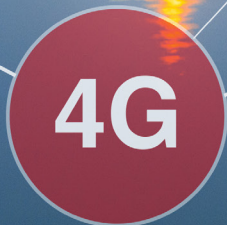
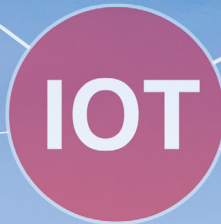


IEEE COMMUNICATIONS MAGAZINE

March 2017, Vol. 55, No. 3

- Mobile and Wireless Technologies for Smart Cities
- Incentives for Mobile Crowd Sensing
- Network Testing and Analytics
- Radio Communications
- Internet of Things



IEEE

IEEE ComSoc
IEEE Communications Society

A Publication of the IEEE Communications Society
www.comsoc.org

While the world benefits from what's new,
IEEE can focus you on what's next.

Develop for tomorrow with
today's most-cited research.

Over 3 million full-text technical documents
can power your R&D and speed time to market.

- IEEE Journals and Conference Proceedings
- IEEE Standards
- IEEE-Wiley eBooks Library
- IEEE eLearning Library
- Plus content from select publishing partners

IEEE Xplore® Digital Library

Discover a smarter research experience.

Request a Free Trial
www.ieee.org/tryieeexplore

Follow IEEE Xplore on  

 **IEEE**
Advancing Technology
for Humanity

Director of Magazines

Raouf Boutaba, University of Waterloo (Canada)

Editor-in-Chief

Osman S. Gebizlioglu, Huawei Tech. Co., Ltd. (USA)

Associate Editor-in-Chief

Tarek El-Bawab, Jackson State University (USA)

Senior Technical Editors

Nim Cheung, ASTRI (China)

Nelson Fonseca, State Univ. of Campinas (Brazil)

Steve Gorshe, PMC-Sierra, Inc (USA)

Sean Moore, Centripetal Networks (USA)

Peter T. S. Yum, The Chinese U. Hong Kong (China)

Technical Editors

Mohammed Atiqzaman, Univ. of Oklahoma (USA)

Guillermo Atkin, Illinois Institute of Technology (USA)

Mischa Dohler, King's College London (UK)

Frank Effenberger, Huawei Technologies Co., Ltd. (USA)

Tarek El-Bawab, Jackson State University (USA)

Xiaoming Fu, Univ. of Goettingen (Germany)

Stefano Gallij, ASSIA, Inc. (USA)

Admela Jukan, Tech. Univ. Carolo-Wilhelmina zu

Braunschweig (Germany)

Vimal Kumar Khanna, mCalibre Technologies (India)

Yoichi Maeda, Telecommun. Tech. Committee (Japan)

Nader F. Mir, San Jose State Univ. (USA)

Seshrathi Mohan, University of Arkansas (USA)

Mohamed Moustafa, Egyptian Russian Univ. (Egypt)

Tom Oh, Rochester Institute of Tech. (USA)

Glenn Parsons, Ericsson Canada (Canada)

Joel Rodrigues, Univ. of Beira Interior (Portugal)

Jungwoo Ryoo, The Penn. State Univ.-Altoona (USA)

Antonio Sánchez Esguevillas, Telefonica (Spain)

Mostafa Hashem Sherif, AT&T (USA)

Tom Starr, AT&T (USA)

Ravi Subrahmanyam, InVisage (USA)

Danny Tsang, Hong Kong U. of Sci. & Tech. (China)

Hsiao-Chun Wu, Louisiana State University (USA)

Alexander M. Wyglinski, Worcester Poly. Institute (USA)

Jun Zheng, Nat'l. Mobile Commun. Research Lab (China)

Series Editors

Ad Hoc and Sensor Networks

Edoardo Biagioni, U. of Hawaii, Manoa (USA)

Ciprian Dobre, Univ. Politehnica of Bucharest (Romania)

Silvia Giordano, Univ. of App. Sci. (Switzerland)

Automotive Networking and Applications

Wai Chen, Telcordia Technologies, Inc (USA)

Luca Delgrossi, Mercedes-Benz R&D N.A. (USA)

Timo Kosch, BMW Group (Germany)

Tadao Saito, University of Tokyo (Japan)

Consumer Communications and Networking

Ali Begen, Cisco (Canada)

Mario Kolberg, University of Sterling (UK)

Madjid Merabti, Liverpool John Moores U. (UK)

Design & Implementation

Vijay K. Gurbani, Bell Labs/Alcatel Lucent (USA)

Salvatore Loreto, Ericsson Research (Finland)

Ravi Subrahmanyam, Invisage (USA)

Green Communications and Computing Networks

Song Guo, University of Aizu (Japan)

John Thompson, Univ. of Edinburgh (UK)

RangaRao V. Prasad, Delft Univ. of Tech. (The Netherlands)

Jinsong Wu, Alcatel-Lucent (China)

Honggang Zhang, Zhejiang Univ. (China)

Integrated Circuits for Communications

Charles Chien, CreoNex Systems (USA)

Zhiwei Xu, SST Communication Inc. (USA)

Network and Service Management

George Pavlou, U. College London (UK)

Juergen Schoenwaelder, Jacobs University (Germany)

Networking Testing and Analytics

Ying-Dar Lin, National Chiao Tung University (Taiwan)

Erica Johnson, University of New Hampshire (USA)

Irena Atov, InClusive Technologies (USA)

Optical Communications

Xiang Liu, Futurewei Technologies, Inc. (USA)

Zuqing Zhu, Univ. Science and Tech. of China (China)

Radio Communications

Thomas Alexander, Ixia Inc. (USA)

Amitabh Mishra, Johns Hopkins Univ. (USA)

Columns

Book Reviews

Piotr Cholda, AGH U. of Sci. & Tech. (Poland)

History of Communications

Steve Weinsten (USA)

Regulatory and Policy Issues

J. Scott Marcus, WIK (Germany)

Jon M. Peha, Carnegie Mellon U. (USA)

Technology Leaders' Forum

Steve Weinsten (USA)

Publications Staff

Joseph Milizzo, Assistant Publisher

Susan Lange, Online Production Manager

Jennifer Porcello, Production Specialist

Catherine Kemelmacher, Associate Editor



IEEE



IEEE ComSoc
IEEE Communications Society

IEEE COMMUNICATIONS MAGAZINE

MARCH 2017, vol. 55, no. 3

www.comsoc.org/commag

- 4 THE PRESIDENT'S PAGE
- 6 BOOK REVIEWS
- 7 GLOBAL COMMUNICATIONS NEWSLETTER
- 11 CONFERENCE CALENDAR
- 224 ADVERTISERS' INDEX

ENABLING MOBILE AND WIRELESS TECHNOLOGIES FOR SMART CITIES: PART 2

GUEST EDITORS: EJAZ AHMED, MUHAMMAD IMRAN, MOHSEN GUIZANI, AMMAR RAYES, JAIME LORET, GUANGJIE HAN, AND WAEI GUIBENE

- 12 GUEST EDITORIAL
- 14 A MULTI-TENANT CLOUD-BASED DC NANO GRID FOR SELF-SUSTAINED SMART BUILDINGS IN SMART CITIES
Neeraj Kumar, Athanasios V. Vasilakos, and Joel J. P. C. Rodrigues
- 22 UAV-ENABLED INTELLIGENT TRANSPORTATION SYSTEMS FOR THE SMART CITY: APPLICATIONS AND CHALLENGES
Hamid Menouar, Ismail Güvenc, Kemal Akkaya, A. Selcuk Uluogac, Abdullah Kadri, and Adem Tuncer
- 30 A UNIFIED URBAN MOBILE CLOUD COMPUTING OFFLOADING MECHANISM FOR SMART CITIES
Daniela Mazza, Daniele Tarchi, and Giovanni E. Corazza
- 38 MOBILE EDGE COMPUTING POTENTIAL IN MAKING CITIES SMARTER
Tarik Taleb, Sunny Dutta, Adlen Ksentini, Muddesar Iqbal, and Hannu Flinck
- 44 5G CONVERGED CELL-LESS COMMUNICATIONS IN SMART CITIES
Tao Han, Xiaohu Ge, Lijun Wang, Kyung Sup Kwak, Yujie Han, and Xiong Liu
- 51 CYBERSECURITY AND PRIVACY SOLUTIONS IN SMART CITIES
Rida Khatoun and Sherali Zeadally

SUSTAINABLE INCENTIVE MECHANISMS FOR MOBILE CROWDSENSING: PART 1

GUEST EDITORS: LINGHE KONG, KUI REN, MUHAMMAD KHURRAM KHAN, QI LI, AMMAR RAYES, MÉROUANE DEBBAH, AND YUICHI NAKAMURA

- 60 GUEST EDITORIAL
- 62 CONGESTION-AWARE COMMUNICATION PARADIGM FOR SUSTAINABLE DENSE MOBILE CROWDSENSING
Wen Sun and Jiajia Liu
- 68 SUSTAINABLE INCENTIVES FOR MOBILE CROWDSENSING: AUCTIONS, LOTTERIES, AND TRUST AND REPUTATION SYSTEMS
Tie Luo, Salil S. Kanhere, Jianwei Huang, Sajal K. Das, and Fan Wu
- 76 A LOCATION-BASED MOBILE CROWDSENSING FRAMEWORK SUPPORTING A MASSIVE AD HOC SOCIAL NETWORK ENVIRONMENT
Md. Abdur Rahman and M. Shamim Hossain
- 86 PROMOTING COOPERATION BY THE SOCIAL INCENTIVE MECHANISM IN MOBILE CROWDSENSING
Guang Yang, Shibo He, Zhiguo Shi, and Jiming Chen
- 93 HySense: A Hybrid Mobile CrowdSensing Framework for Sensing Opportunities Compensation Under Dynamic Coverage Constraint
Guangjie Han, Li Liu, Sammy Chan, Ruiyun Yu, and Yu Yang

2017 IEEE Communications Society Elected Officers

Harvey A. Freeman, *President*
Khaled B. Letaief, *President-Elect*
Luigi Fratta, *VP-Technical Activities*
Guoliang Xue, *VP-Conferences*
Stefano Bregni, *VP-Member Relations*
Nelson Fonseca, *VP-Publications*
Robert S. Fish, *VP-Industry and Standards Activities*

Members-at-Large

Class of 2017

Gerhard Fettweis, Araceli Garca Gomez
Steve Gorshe, James Hong

Class of 2018

Leonard J. Cimini, Tom Hou
Robert Schober, Qian Zhang

Class of 2019

Lajos Hanzo, Wanjiun Liao
David Michelson, Ricardo Veiga

2017 IEEE Officers

Karen Bartleson, *President*
James A. Jeffries, *President-Elect*
William P. Walsh, *Secretary*
John W. Walz, *Treasurer*
Barry L. Shoop, *Past-President*
E. James Prendergast, *Executive Director*
Vijay K. Bhargava, *Director, Division III*

IEEE COMMUNICATIONS MAGAZINE (ISSN 0163-6804) is published monthly by The Institute of Electrical and Electronics Engineers, Inc. Headquarters address: IEEE, 3 Park Avenue, 17th Floor, New York, NY 10016-5997, USA; tel: +1 (212) 705-8900; <http://www.comsoc.org/commag>. Responsibility for the contents rests upon authors of signed articles and not the IEEE or its members. Unless otherwise specified, the IEEE neither endorses nor sanctions any positions or actions espoused in *IEEE Communications Magazine*.

ANNUAL SUBSCRIPTION: \$27 per year print subscription. \$16 per year digital subscription. Non-member print subscription: \$400. Single copy price is \$25.

EDITORIAL CORRESPONDENCE: Address to: Editor-in-Chief, Osman S. Gebizlioglu, Huawei Technologies, 400 Crossing Blvd., 2nd Floor, Bridgewater, NJ 08807, USA; tel: +1 (908) 541-3591, e-mail: Osman.Gebizlioglu@huawei.com.

COPYRIGHT AND REPRINT PERMISSIONS: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limits of U.S. Copyright law for private use of patrons: those post-1977 articles that carry a code on the bottom of the first page provided the per copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For other copying, reprint, or republication permission, write to Director, Publishing Services, at IEEE Headquarters. All rights reserved. Copyright  2017 by The Institute of Electrical and Electronics Engineers, Inc.

POSTMASTER: Send address changes to *IEEE Communications Magazine*, IEEE, 445 Hoes Lane, Piscataway, NJ 08855-1331. GST Registration No. 125634188. Printed in USA. Periodicals postage paid at New York, NY and at additional mailing offices. Canadian Post International Publications Mail (Canadian Distribution) Sales Agreement No. 40030962. Return undeliverable Canadian addresses to: Frontier, PO Box 1051, 1031 Helena Street, Fort Erie, ON L2A 6C7.

SUBSCRIPTIONS: Orders, address changes — IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855-1331, USA; tel: +1 (732) 981-0060; e-mail: address.change@ieee.org.

ADVERTISING: Advertising is accepted at the discretion of the publisher. Address correspondence to: Advertising Manager, *IEEE Communications Standards Magazine*, 3 Park Avenue, 17th Floor, New York, NY 10016.

SUBMISSIONS: The magazine welcomes tutorial or survey articles that span the breadth of communications. Submissions will normally be approximately 4500 words, with few mathematical formulas, accompanied by up to six figures and/or tables, with up to 10 carefully selected references. Electronic submissions are preferred, and should be submitted through Manuscript Central: <http://mc.manuscriptcentral.com/commag-ieee>. Submission instructions can be found at the following: <http://www.comsoc.org/commag/paper-submission-guidelines>. For further information contact Tarek El-Bawab, Associate Editor-in-Chief (telbawab@ieee.org). All submissions will be peer reviewed.



100 ENHANCED C-RAN USING D2D NETWORK

Kazi Mohammed Saidul Huq, Shahid Mumtaz, Jonathan Rodriguez, Paulo Marques, Bismark Okyere, and Valerio Frascolla

INTERNET OF THINGS: PART 3

GUEST EDITORS: CHRISTOS VERIKOUKIS, ROBERTO MINERVA, MOHSEN GUIZANI, SOUMYA KANTI DATTA, YEN-KUANG CHEN, AND HAUSI A. MULLER

108 GUEST EDITORIAL

110 A TRUST CLOUD MODEL FOR UNDERWATER WIRELESS SENSOR NETWORKS

Jinfang Jiang, Guangjie Han, Chunsheng Zhu, Sammy Chan, and Joel J. P. C. Rodrigues

117 A PRIMER ON 3GPP NARROWBAND INTERNET OF THINGS

Y.-P. Eric Wang, Xingqin Lin, Ansuman Adhikary, Asbjorn Grovlen, Yutao Sui, Yufei Blankenship, Johan Bergman, and Hazhir S. Razaghi

124 THE RANDOM ACCESS PROCEDURE IN LONG TERM EVOLUTION NETWORKS FOR THE INTERNET OF THINGS

Tiago P. C. de Andrade, Carlos A. Astudillo, Luiz R. Sekijima, and Nelson L. S. da Fonseca

132 WRONG SIREN! A LOCATION SPOOFING ATTACK ON INDOOR POSITIONING SYSTEMS: THE STARBUCKS CASE STUDY

Junsung Cho, Jaegwan Yu, Sanghak Oh, Jungwoo Ryoo, JaeSeung Song, and Hyoungshick Kim

138 FIRST MILE CHALLENGES FOR LARGE-SCALE IOT

Ahmed Bader, Hesham ElSawy, Mohammad Gharbieh, Mohamed-Slim Alouini, Abdulkareem Adinoyi, and Furaih Alshaalan

146 A COMMUNITY-DRIVEN ACCESS CONTROL APPROACH IN DISTRIBUTED IOT ENVIRONMENTS

Dina Hussein, Emmanuel Bertin, and Vincent Frey

NETWORK TESTING AND ANALYTICS

SERIES EDITORS: YING-DAR LIN, ERICA JOHNSON, AND IRENA ATOV

154 SERIES EDITORIAL

156 FROM LTE TO 5G FOR CONNECTED MOBILITY

Mads Lauridsen, Lucas Chavarra Gimenez, Ignacio Rodriguez, Troels B. Sorensen, and Preben Mogensen

163 TRAFFIC ANALYSIS WITH OFF-THE-SHELF HARDWARE: CHALLENGES AND LESSONS LEARNED

Martino Trevisan, Alessandro Finamore, Marco Mellia, Maurizio Munafo, and Dario Rossi

170 LOAD-STRESS TEST OF MASSIVE HANDOVERS FOR LTE TWO-HOP ARCHITECTURE IN HIGH-SPEED TRAINS

Ali Parichehreh, Umberto Spagnolini, Paolo Marini, and Alberto Fontana

178 NATWATCHER: PROFILING NATS IN THE WILD

Anna Maria Mandalari, Miguel Angel Diaz Bautista, Francisco Valera, and Marcelo Bagnulo

RADIO COMMUNICATIONS:

COMPONENTS, SYSTEMS AND NETWORKS

SERIES EDITORS: AMITABH MISHRA AND TOM ALEXANDER

186 SERIES EDITORIAL

188 ENABLING TECHNOLOGIES TOWARD FULLY LTE-COMPATIBLE FULL-DUPLEX RADIO

Gosan Noh, Hanho Wang, Changyong Shin, Seunghyeon Kim, Youngil Jeon, Hyunchol Shin, Jinup Kim, and Ilgyu Kim

196 ACHIEVING ULTRA-LOW LATENCY IN 5G MILLIMETER WAVE CELLULAR NETWORKS

Russell Ford, Menglei Zhang, Marco Mezzavilla, Sourjya Dutta, Sundeep Rangan, and Michele Zorzi

204 OPPORTUNITIES AND CHALLENGES OF TRIP GENERATION DATA COLLECTION TECHNIQUES USING CELLULAR NETWORKS

Iva Bojic, Yuji Yoshimura, and Carlo Ratti

ACCEPTED FROM OPEN CALL

210 A NOVEL SDN-BASED ARCHITECTURE TO PROVIDE SYNCHRONIZATION AS A SERVICE IN 5G SCENARIOS

Stefano Ruffini, Paola Iovanna, Mats Forsman, and Tomas Thyni

217 AN SDN/NFV-ENABLED ENTERPRISE NETWORK ARCHITECTURE OFFERING FINE-GRAINED SECURITY POLICY ENFORCEMENT

Claas Lorenz, David Hock, Johann Scherer, Raphael Durner, Wolfgang Kellerer, Steffen Gebert, Nicholas Gray, Thomas Zinner, and Phuoc Tran-Gia



“Massive amounts of highly sensitive client data traveling online, 24 hours a day.

And I sleep like a baby at night.”

David Wilner / COO
FRONTEO USA, Inc.
Client since 2012

Meet Spectrum Enterprise. Our thing? Delivering the right data, voice, video and cloud solutions via our nationwide fiber-based network. And all the support you need to succeed. With our superior network and IT infrastructure, you're free to do your thing.

Visit enterprise.spectrum.com/hello
or call 866-313-5812

Spectrum
ENTERPRISE

©2017 Charter Communications. All Rights Reserved. Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply. Subject to change without notice. All trademarks remain property of their respective owners.

REACHING OUT TO THE WORLD

IEEE, and especially ComSoc, offer highly regarded platforms for conferences, publications, education, membership, and other activities aimed at engaging members from industry, academia, and government regardless of where they are on the globe. Over the years, formal processes and organizational structure have evolved to enable best use of this platform, and as a means of reaching out to professionals around the world. However, many of our most successful outreaches have been built upon informal personal relationships, sometimes extending over many years. This month's President's Page by one of our past presidents, Doug Zuckerman, shares some examples of how this outreach is being used to achieve ComSoc's strategic goals, such as strengthening industry engagement.

An active volunteer for more than 30 years, Doug Zuckerman is a past IEEE Division III (Communications Technology) Director, was 2008-2009 President of the IEEE Communications Society, and previously held leadership positions in conferences, publications, and membership development. He received his B.S., M.S., and Eng.Sc.D. degrees from Columbia University, USA, and he is an IEEE Life Fellow. His professional experience, mainly at Bell Labs and Telcordia Technologies, USA, spans the operations, management and engineering of emerging communications technologies, networks, and applications. His work heavily influenced early standards for the management of telecommunications networks. Presently semi-retired, he is still active in standards as a representative to the OpenFog Consortium as a board member. He is also a consulting employee for Vencore Labs. He currently serves on the IEEE Communications Society's Board of Governors and the IEEE Future Directions Committee.



Harvey Freeman



Doug Zuckerman

This was formalized through a memorandum of understanding by which ComSoc represents IEEE, including having a seat on the OpenFog Consortium's Board of Directors. This formed the basis for ComSoc engaging communities across IEEE to proactively pursue conferences, publications, education, and standards activities on fog computing and networking. Some activities fueled by this relationship have included the following:

- IEEE Communications Magazine Feature Topics on Fog
- Fog World Congress (FWC 2017) co-sponsored with the OpenFog Consortium
- Fog panels and keynotes at ICCE, CCNC, PTC, IM, and OFC
- Rejuvenated "Emerging Technology Initiative" in ComSoc on Fog Networking
- Expanded activities by the graduated IEEE Cloud Computing Initiative managed by the IEEE Computer Society
- Increased collaboration with existing IEEE Initiatives on IoT and 5G
- Representation of IEEE at an NSF Grand Challenges workshop on Fog research opportunities
- Exploration of the IEEE Standards Association using the OpenFog Consortium's architectures and frameworks as the basis for new standards on Fog.

The ongoing collaboration with the OpenFog Consortium is a good example of how ComSoc, and IEEE, can provide value to industry and the creation of new revenue opportunities (such as FWC 2017).

ENGAGING INDUSTRY COUNCILS:

PACIFIC TELECOMMUNICATIONS COUNCIL

From their website (www.ptc.org), the "Pacific Telecommunications Council (PTC) is an international community of members from more than 40 countries with a shared vision to promote the development and use of telecommunications and information and communication technologies to enhance the lives of people in the Pacific region." Nearly 20 years ago, then ComSoc President, Tom Plevyak, initiated a relationship with the Council by holding the Society's Management Retreat in conjunction with their Pacific Telecommunications Conference in Honolulu. The win-win scenario was that ComSoc would bolster the "technical" strength of their conference, which already featured a very strong "business" presence from industries and enterprises in the Pacific Rim. In turn, PTC would provide an opportunity for ComSoc to move closer to industry and practitioners who formed the backbone of that event. The conference and trade show continues to be held annually in the Hilton Hawaiian Village in Honolulu. A side benefit of the longstanding PTC relationship was that it introduced us to the local IEEE member community, including eventual establishment of a ComSoc chapter.

As a long-term result of that first meeting, we have since achieved the following tangible outcomes:

- Organized NOMS 2000, the first ComSoc event held in Hawaii
- Organized NOMS 2012 and IEEE GLOBECOM 2009 in Hawaii
- Established PTC as a ComSoc "Related Society" (includes cross-marketing)

BUILDING INDUSTRY CONNECTIONS: OPENFOG CONSORTIUM

In recognition of the growing need for technology architectures and platforms to support IoT, 5G, Artificial Intelligence, and other rapidly evolving paradigm shifts, IEEE had a unique opportunity to come on board early as a participant in the OpenFog Consortium. From the consortium's website (www.openfogconsortium.org):

"The growth in IoT is explosive, impressive – and unsustainable under current architectural approaches. Many IoT deployments face challenges related to latency, network bandwidth, reliability, and security, which cannot be addressed in cloud-only models. Fog computing adds a hierarchy of elements between the cloud and endpoint devices, and between devices and gateways, to meet these challenges in a high performance, open and interoperable way.

"Our work is centered around creating a framework for efficient & reliable networks and intelligent endpoints combined with identifiable, secure, and privacy-friendly information flows between clouds, endpoints and services based on open standard technologies."

The consortium is a collaborative effort involving industry, academia and non-profit organizations such as IEEE. Its members include companies such as AT&T, Cisco, Schneider Electric, Intel, Microsoft, and Hitachi, and universities such as Princeton. The consortium's leadership approached ComSoc during 2015, indicating its desire to enter into a win-win relationship with IEEE.

- Positioned keynotes panels at several PTC events, including most recently PTC '17
- Collaborating with PTC and the IEEE Microwave Theory and Techniques Society on the 2017 International Microwave Symposium to be held June, 2017, at the Honolulu Convention Center.

A second ComSoc Management Retreat was held in Hawaii in conjunction with PTC 2008, and notably ComSoc also held a highly successful third Retreat there in January 2017. Given ComSoc's and IEEE's focus on industry engagement, this Retreat provided a timely opportunity for ComSoc's leadership to meet with the PTC leadership, observe first hand a successful industry event being held in Hawaii, and make personal contact with exhibitors and attendees who may be interested in contributing to IEEE and ComSoc activities.

HELPING IEEE ACTIVITIES IN DEVELOPING REGIONS: RIVF

Much focus in IEEE has been on enabling and supporting technical and professional activities in developing countries and regions. One such region is Southeast Asia. Around 2007, under then ComSoc President Nim Cheung and VP-Society Relations Roberto Saracco, visits with industry and academic leaders were conducted in Vietnam and Thailand. In addition, Nim had encouraged ComSoc President-Elect Doug Zuckerman to represent the Society at an emerging IEEE conference on Research, Innovation, and Visualization of the Future in Communications and Computing (RIVF), held in Hanoi that year. Though this was the fifth in the series, it was the first time it was branded as an IEEE conference. Significantly, the IEEE ComSoc Communications Chapter was inaugurated at RIVF 2007. Going forward, the IEEE Vietnam Section, ComSoc, and the Computational Intelligence Society have been sponsoring and actively contributing to the organization and technical program for this event. Top IEEE and Society leaders have played a key role, e.g., Roberto deMarca (past IEEE President), Vin Piuri (past IEEE VP-Technical Activities), Barry Perlman (past MTT Society President), and Nim Cheung and Doug Zuckerman (past ComSoc Presidents). Major topic areas covered at the most recent RIVF held in Hanoi in November 2016 were: Computational Intelligence and Big Data Analytics; Communications and Networking; Software Engineering and Information Systems; and Image, Language and Speech Processing. In the most recent RIVF, ComSoc President Harvey Freeman and past president Doug Zuckerman represented our Society, with Harvey giving a keynote and Doug serving as RIVF Conference Chair. Their presence also provided an opportunity to meet with a ComSoc Sister Society (REV) Vice President and to discuss issues and opportunities related to the Ministry of Telecommunications.

A detailed conference history from the conference website (<http://rivf2016.tlu.edu.vn/>) is the following:

"Started in 2003, RIVF has become a major scientific event for researchers in the field of Computing and Communication Technologies. In the past, the conference series were held at Institut Francophone International, Ha Noi (2003, 2004), Can Tho University (2005), Ho Chi Minh City University of Technology (2006), Ha Noi University of Science and Technology (2007), Ho Chi Minh City University of Science (2008), Da Nang University of Technology (2009), Ha Noi National University of Science (2010), Ho Chi Minh City University of Technology (2012), Ha Noi National University of Engineering and Technology (2013), and Can Tho University (2015). Since the 9th edition in 2012, RIVF has been held every 18 months approximately, alternating between the northern half and the southern half of Vietnam." Historically, it was at RIVF 2007 the IEEE Vietnam Section was formed, and since then RIVF has been an official IEEE conference."

Some results of this ongoing relationship with colleagues in Vietnam are:

- Active contribution to growth of IEEE and ComSoc technical and professional activities in Vietnam
- Goodwill and friendship among global colleagues
- Recognition of our value to the telecommunications ministry

- Showcasing ComSoc as a dedicated leader in helping developing countries grow their technical and educational activities
- Providing opportunities for participation by IEEE cross-Society initiatives on Cloud and Big Data

It should be noted that ComSoc has been similarly active with another important conference in Vietnam, ATC. From the conference website:

"The International Conference on Advanced Technologies for Communications (ATC) is an annual conference series, co-organized by the Radio Electronics Association of Vietnam (REV) and the IEEE Communications Society (IEEE ComSoc). The goal of the series is twofold: to foster an international forum for scientific and technological exchange among Vietnamese and worldwide scientists and engineers in the fields of electronics, communications and related areas, and to gather their high-quality research contributions."

ACTIVELY CONTRIBUTING TO CONFERENCE GROWTH: IEEE COMCAS

Another conference that top IEEE leadership has shown serious interest in is IEEE COMCAS, the IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems, held every two years in Tel Aviv. This conference, which includes both a high quality technical program and robust industry exhibition, is unique in that it brings together so many related disciplines under a single roof. It provides an opportunity for holistic collaboration across topics covered by the Communications Society, Microwave Theory and Techniques Society, Antennas and Propagation Society, and the Aerospace and Electronic Systems Society. COMCAS is a highly respected global conference that also attracts very strong local participation by the IEEE Israel Section and its Communications, Antennas and Propagation and Microwave Theory and Techniques Chapters, as well as ComSoc's Israeli Sister Society. For at least a half dozen years, Society leaders have worked closely in organizing this conference and contributing to its sustained growth in terms of papers, attendance, exhibits and revenue.

From the COMCAS 2017 conference website (www.comcas.org):

"IEEE COMCAS 2017 continues the tradition of providing a multidisciplinary forum for the exchange of ideas, research results, and industry experience in the areas of microwaves, communications, antennas, solid state circuits, electromagnetic compatibility, electron devices, radar, electronic systems engineering and Bio-Medical Engineering. It includes a technical program, industry exhibits, and invited talks by international experts in key topical areas.

"The conference will take place on 13-15 November, 2017 in Tel Aviv, Israel. The David Intercontinental Hotel on the Mediterranean sea offers an excellent venue for networking and the candid exchange of ideas."

Some results of ComSoc's ongoing relationship with COMCAS are as follows:

- Current and previous Society leaders have helped organize the event and been prominently featured on the conference program
- Offered guidance in working with IEEE MCE and IEEE Legal to assure the conference "ownership" stayed with IEEE
- Helped assure conference surplus was used to support local section/chapter activities in Israel, which in turn resulted in more local patronage for the conference.

GOING FORWARD

This President's Page has touched on just several examples of the value our past and current leaders can provide in reaching out to the world in support of our Society's strategic interests. Much of this outreach is informal and based on personal relationships nurtured over many years. Going forward, we need to assure ongoing engagement by the great resource our past leaders provide through their background, experience, and energy. Their passion and dedication, built over many years, is contagious, and ComSoc will continue encouraging their active contributions going forward.

INTERCLOUD: SOLVING INTEROPERABILITY AND COMMUNICATION IN A CLOUD OF CLOUDS

By Jazib Frahim, Venkata Josyula, Monique J. Morrow, and Kenneth Owens, Cisco Press, 2016, ISBN 978-1-58714-445-5, softcover, 262 pages

Reviewer: Piotr Borylo

The ability to share resources, services, responsibility, and management among cloud providers is the fundamental assumption from the viewpoint of cloud interoperability. This idea is attracting increasing attention as cloud providers are becoming aware that meeting all customer needs without any cooperation is a demanding task. This book regards the issues of seamless and transparent cloud interoperability. Definitions, architectures, and use cases are provided, along with challenges and threats.

The book is divided into nine chapters. Chapter 1 presents fundamentals of the cloud concept, its history, different approaches to virtualization, and preliminary definitions concerning the intercloud topic. Chapter 2 carefully studies the intercloud architecture based on the OpenStack platform, with refer-

ences to currently available solutions. Chapter 3 focuses on business-level considerations about SLA, QoS, the service management cycle, or intercloud management strategies aware of some shadow IT issues. Chapter 4 is especially valuable as it provides information about standardization efforts in the context of intercloud, followed by the Cisco intercloud architecture and use cases based on the OpenStack workflow. In Chapter 5, elements of the operational support system are investigated. In the Cisco intercloud architecture, all the mentioned elements are provided as a service to maintain customer satisfaction and service assurance strategy. Valuable accounting and billing taxonomy related to the intercloud context are provided in Chapter 6. Billing issues are studied for various service models, and remarks are delivered on transfer billing and accounting from the context of traditional clouds to intercloud environments. Chapter 7 addresses security, which is the biggest challenge in the context of the intercloud. Current cloud solutions and threats are studied and mapped to the intercloud architecture. In Chapter 8, the authors propose to consider a cloud as an operating system and moti-

vate this approach carefully. Finally, Chapter 9 describes the use case of migration from traditional stand-alone data centers through the hybrid clouds, to the intercloud. Cisco Hybrid Cloud is referred as a possible solution, being a stepping stone toward the intercloud.

The book presents the concepts, needs, advantages, and challenges regarding cloud interoperability. The assumed high level approach will be most suitable for readers responsible for technology assessment and service development. The authors provide business-level concepts, architectures, and data about standardization efforts. However, the covered practical use cases and workflow examples will also be attractive for network and IT managers. Timeliness is also undoubtedly a strong aspect of the book. Two minor drawbacks must be mentioned. The first one regards the organization of the book, and some improvements in this context will make the book more readable. The second issue concerns Chapters 2 and 5, as both could have been improved to be more easily comprehended by readers. Nevertheless, in summary, I recommend this book as a good and up-to-date source of information on cloud interoperability.

PROPEL YOUR NETWORK R&D TO A HIGHER ORBIT

Technologies

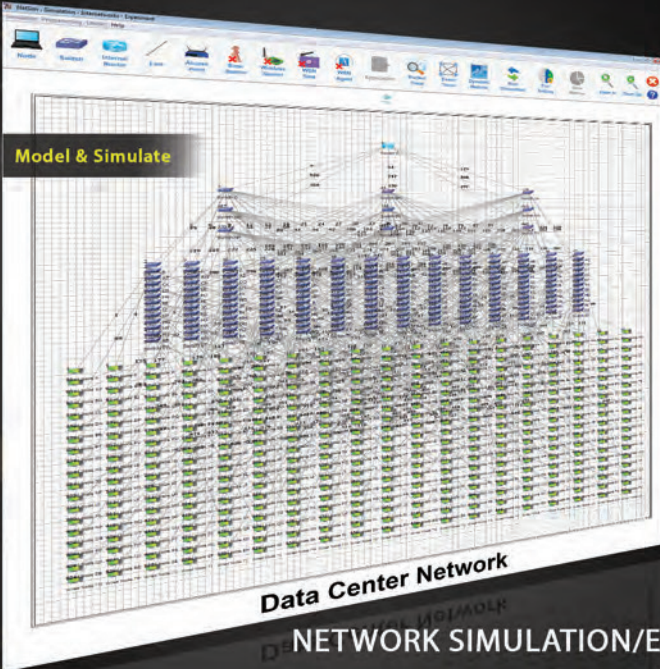
- 802.11 a/b/g/n/ac and e
- MANET
- WSN
- Cognitive Radio
- IOT
- VANETs
- LTE/LTE-A
- Military Radios
- Emulator for connecting real devices and more....

Applications

- Network R&D
- Military Communications
- Network Capacity Studies

Used by

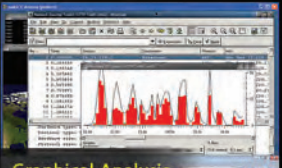
- Universities
- Defence Organizations
- Network Equipment Manufacturers



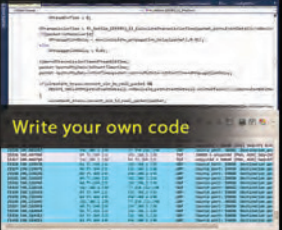
Model & Simulate

Data Center Network


Write to us for a **FREE** Evaluation



Graphical Analysis




Write your own code



Wireshark Packet Capture

Wireshark is a registered trademark of Wireshark Foundation

NETWORK SIMULATION/EMULATION SOFTWARE
With Open Protocol Source Code



Over 300+ customers across 15 countries
www.tetcos.com | sales@tetcos.com | +91 76760 54321



March 2017
ISSN 2374-1082

MEMBERSHIP SERVICES

100 Issues of the New Global Communications Newsletter!

By Stefano Bregni, Vice-President for Member and Global Activities, Editor of the Global Communications Newsletter



Stefano Bregni

This issue of the *Global Communications Newsletter* has a special significance for me: it is Issue No. 100 under my responsibility as Editor!

Almost 10 years ago, I was appointed by Tom La Porta, at that time Director of Magazines of the IEEE Communications Society, to revive our Newsletter, whose publication had been discontinued a couple of years before.

After few months of work to set up the new Editorial Board and solicit the first contributions from ComSoc Chapters, publication resumed. Finally, Issue No. 1 of the new series of the GCN was ready. Ending a long period of absence, the February 2008 issue of *IEEE Communications Magazine* featured again our four light blue pages, opened by my introduction, "The Global Communications Newsletter is Back!".

Since then, the GCN has come a long way. We have worked to improve the variety of contents. We have been publishing more and more articles not exclusively from Chapters but also from other contributors, reporting news and events from all Regions.

CHAPTER REPORT

IEEE ComSoc Iraq Chapter Activities: Serving IEEE ComSoc Members in a Country at War

By Sattar B. Sadkhan, Chair of the IEEE ComSoc Iraq Chapter

The IEEE ComSoc Iraq chapter was established at the end of Nov. 2011. The chapter includes members from academic institutes, ministries (Communication, Science and Technology), and non-government wireless communication companies (especially Asia Cell and Kalimat).

During these past five years the Chapter has organized many scientific activities within Iraq, especially in co-sponsoring national and international conferences and workshops. There were also many scientific activities organized by the Iraq Chapter outside of Iraq, in India, China, and the U.K. Most of these activities were organized and planned by the founder of the ComSoc Iraq Chapter, Dr. Eng. Sattar B. Sadkhan, who is a Senior Member of IEEE, and who served as past chair of the IEEE Iraq Section for the period 2008-2014.

ACADEMIC ACTIVITIES

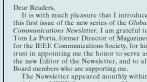
In just one year, from June 2014 up to June 2015, the Chapter organized (co-sponsored) about 15 scientific activities throughout

We also worked on the graphical style. With the issue of October 2014 (No. 71), we abandoned the traditional old-style layout, nearly unchanged since the beginning, for the new sharp look of today. The current graphical layout dresses the articles with a contemporary style, which I hope readers appreciate as I do.

Whenever I have the opportunity, I like to affirm that our GCN is indeed "The Voice of the Chapters". Once again, I cordially invite all Chapter officers to contribute to the GCN by submitting the reports of their best activities. You do a lot of good things in your Chapter: please share with all ComSoc members and let everyone know!

Global
IEEE Communications
Magazine
Newsletter
February 2008

The Global Communications Newsletter Is Back!
By Stefano Bregni, Editor



Dear Readers,
It is with much pleasure that I introduce the first issue of the new series of the Global Communications Newsletter. I am grateful to Tom La Porta, former Director of Magazines for the IEEE Communications Society, for his trust in appointing me the Editor of the Newsletter, and to all Board members who are supporting me.
The Newsletter appeared initially within each issue of IEEE Communications Magazine for a number of years. It was much well appreciated by readers due to the effort and commitment of my predecessor, Nicolas Ono, and of all Regional Correspondents. Nicolas will continue to help as a Regional Correspondent. I also count on his experience and suggestions in my first steps as Editor.
Let me introduce the Regional Correspondents that stepped in now: Jim Ma and Rajan Doshi (USA), Alexander Bhatia (Australia), Milan Radovic (Belgium), Jozsef János (Poland), Marko Jagodic (Slovenia), Hosain Aliji (France), Marko Mladjenovic (Spain), Joseph Boudreau (Canada), Jose Luis Vazquez Gonzalez and Carlos Hinch (Mexico), Igor Armitovic (Paraguay), Jose David Cely (Colombia), Heiko Waldman (Brazil), Ram G. Gupta (India), Stan Zhang (Hong Kong), and Roshanindra Mehta (Malaysia). Their responsibility will be to ensure appropriate coverage of all IEEE Regions by providing timely and interesting contributions from all Chapters and other regional entities.
By resuming publication of the Newsletter, we aim to better serve the global communications community. The Newsletter will provide an excellent opportunity to present news and events related to communications around the world, as well as activities carried out by



IEEE Communications Society Chapters in greater detail.
In general, articles published in the Global Communications Newsletter will not be technical papers or technical surveys. Rather, they will be short articles informing the IEEE Communications Society community about various activities carried out and organized in the four corners of the world by the many volunteers who are the true engine of the Society. Many Chapters organize interesting events several times a year: let our world community know about them! Also, input from telecommunication regional industry operators, and academia may be of great interest to our global community. Examples of suitable articles we plan to publish are: highlights from local ComSoc conferences, reports of Distinguished Lecturer Tours, reports of other technical events organized by IEEE Communications Society Chapters that may be of international interest, and updates on regional telecommunication markets.
I invite all Chapter officers, as well as ComSoc volunteers, to plan to start immediately submitting such articles to the Global Communications Newsletter according to our guidelines. You can submit your contributions to the most appropriate Regional Correspondent or directly to me (email: bregni@ieee.org). The format of submission should be a simple email, including title, possibly a short abstract (< 50 words), and your article attached normally from 50 to 1000 words.
The relevance, timeliness, and interest of reports published in our Newsletter will depend on your cooperation. The willingness of everyone to contribute timely and informative reports are essential to ensure our success. We look forward to receiving your submissions.

Cover page of the Issue No. 1 of the new series of the Global Communications Newsletter, published in the February 2008 issue of the IEEE Communications Magazine.



Activities with the young people

the eight Iraqi cities. It was a great challenge for the Iraq Chapter members to organize these activities when considering the very critical safety status in many cities. The Chapter members took such responsibilities on themselves to organize these activities within many universities. The ComSoc Chapter is fighting against ISIS by continuing to organize activities with any group who wants to cooperate with the Iraq Chapter!

National Scientific Events: In March 2014, a scientific workshop with the theme, "The Role of Information and Communication Technology in Education" was organized at Basra University, in

(Continued on Newsletter page 2)

COMSOC IRAQ CHAPTER/Continued from page 1

Basra City in southern Iraq. The workshop organized by Education College in cooperation with the Iraq ComSoc Chapter. The Chapter Chair delivered the opening lecture at this workshop on the topic, "The Required Infrastructure Communication Technologies to Support e-learning in Iraq".

In April 2015, the ComSoc Chapter, in cooperation with the Kufa University College of Computer and Mathematics, organized a scientific workshop on "E-Criminal". This workshop was one of many scientific activities organized within this university in the past four years in cooperation with the ComSoc Chapter. The Chair of the Chapter delivered the opening Lecture "The e-Criminal: Status and Challenges".

With Waset University, the ComSoc Chapter cooperated in an International Conference organized within the Education College in April 2015. The keynote lecture at the opening ceremony of the conference was given by the ComSoc Chapter Chair on the topic, "Multidiscipline in Information Security".

In February 2015, in Kirkuk City in northern Iraq, a scientific workshop was organized in cooperation with AL-Qalam University College. The Chairman of ComSoc chapter delivered the opening lecture on the "Status of the Infrastructure of Communication Technologies Inside Iraq".

In January 2015, the ComSoc Chapter, in cooperation with Islamic University College in Babylon City, organized a workshop on the topic, "5G Communication Technology". The ComSoc Chapter Chair delivered a lecture on "The Status of Communication Technologies used in IRAQ after 2003". In February 2015, at the same college, the ComSoc chapter organized a training course on "Robotics".

The ComSoc Chapter cooperated with the Iraqi Engineering Council and "Promising Minds" NGO to hold many petition ceremonies for the products of different people of different ages. A ceremony was held on 1 Sept. 2015 in Baghdad, with another ceremony planned for November 2015 at the time of this writing.

International Conferences (Inside Iraq): The First International



Waset International Conference.

Conference on Future Communication Networks (ICFCN'12) was organized in scientific cooperation with Al-Nahrain University in Baghdad at April 2012. Most of the members of the Scientific Committee and Technical Program Committee were Chapter members. The Chapter Chair organized a special session at this conference on the topic, "Iraq Communication Security: Status and Challenges".

On 18-19 December 2013 the Chapter scientific co-sponsored the International Conference on Electrical, Computer, communication, Power, Control Engineering (ICECCPCE'13) in Mosul City in Northern Iraq. One of the keynote lectures was given by the Chapter chair. The Conference was organized by the Mosul Technical College.

Lectures (Outside Iraq): Three lectures were given by the chair of the ComSoc Chapter outside Iraq about the role and activities of the Iraq ComSoc chapter inside and outside Iraq: at KL-University in India on 8-9 February 2012 with the postgraduate students on the status of the IEEE Iraq Section and IEEE Iraq ComSoc



Workshop in Basra City.



ICECCPCE'13 Conference.

COMSOC IRAQ CHAPTER/Continued from page 2

Chapter, and their scientific responsibilities and activities inside Iraq; at Northampton University in the U.K. in October 2013 with the postgraduate students and academic staff of the Computer Engineering College, on the topic “Multidisciplinary in Information Security”; and at Zhejiang Congshang University in China on 26 December 2013 with the undergraduate and postgraduate students, on the topic “Multidisciplinary Prospective in Information Security”.



Visit to a primary school for displaced students, serving more than 150 displaced kids from different cities in North of Iraq, occupied by ISIS- forces since 2014. These families lived in Babylon City.

SCIENTIFIC COOPERATION WITH THE MINISTRY OF COMMUNICATION

A national scientific conference was organized in cooperation with the Ministry of Communication in the capital city of Baghdad in 2011. Many Chapter members participated in the Scientific Committee of this conference. A special session on the topic, “Status of Communication Security in IRAQ after 2003” was organized by the chair of IEEE Iraq ComSoc Chapter.

SCIENTIFIC COOPERATION WITH THE INDUSTRIAL SECTOR IN IRAQ

Iraqi engineers (generally) are in very difficult circumstances, especially after 2003. Most industry institutes and companies ceased operation for many reasons, and this has led to poor relations between the industrial and academic sectors. But even with such a fact, the IEEE Iraq ComSoc Chapter, through its chair (who is a member of the consultant staff on the National Industrial Committee), organized many activities within the Industry Ministry, and two workshops held in mid-2014 at Babylon University with all industrial companies operating in Baghdad and the Mid Euphrates Region. The main goals of this workshop were:

- Plan the “road map” for cooperation among industrial engineers in these companies and academic staffs at the universities in the Mid Euphrates Region.
- Establish opportunities for scientific cooperation among the industrial and academic sectors.
- Create opportunities for the industrial engineering sector to “re-establish the knowledge” through continuing education at the universities.

With all these goals, the ComSoc Chapter members did their best to provide support for the engineering background of the Iraqi industrial sector.

SCIENTIFIC RELATIONS WITH THE OIL MINISTRY

The ComSoc Chapter established scientific relations with the Oil Ministry/Basra Oil Detection company. The first scientific workshop was organized in April 2015 in cooperation with this company and Basra University College for Science and Technology. The topic of the workshop was “Information and Communication Technologies”. The Chapter chair delivered the opening talk about the IEEE Iraq ComSoc Chapter and its role and aims in supporting the scientific requests and activities of the Oil Ministry and different companies within this Ministry.

CONFERENCE REPORT

SoftCOM 2016: Meeting of Academy and Industry

By Dinko Begusic, Nikola Rozic, Pascal Lorenz, Josko Radic, Petar Solic and Matko Saric, University of Split, FESB, Croatia; University of Haute Alsace, France

The 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2016) was held in the attractive ambience of the Radisson Blu Resort Hotel, Split, September 18–20. The Conference was organized by the University of Split, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture (FESB) and Croatian Communications and Information Society (CCIS) under the auspices of the Ministry of Science, Education and Sports, Croatian Academy of Engineering and Croatian Regulatory Agency for Network Industries. The Conference was technically co-sponsored by the IEEE Communications Society (ComSoc).

Researchers and experts from industry, research institutes and universities from 30 countries around the world submitted a total

(Continued on Newsletter page 4)



A plenary talk titled “LOOOM: Defining Control Systems for 5G” has been presented by Sandor Albrecht, PhD, Director of Network Technology, Ericsson Research, Stockholm, Ericsson AB, Sweden. The session has been chaired by P. Lorenz, Univ. of Haute Alsac, France, I. Stupar, Ericsson N. Tesla and D. Begusic, University of Split, Croatia (left to right).

of 170 papers for presentation at SoftCOM 2016. Submitted papers were reviewed by more than 200 scientists from universities, institutes and ICT companies around the world, with 49%

of submitted papers being accepted for presentation within the technical program based on their contribution, relevance, conceptual clearness and overall quality.

At the opening ceremony the participants were welcomed on behalf of the organizers by Prof. Sven Gotovac, Dean of the Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture in Split; Prof. Simun Andelinovic, Rector of the University of Split; Zlatko Zevrnja, Prefect of the County of Split and Dalmatia; Prof. Pascal Lorenz, Chair of the IEEE ComSoc France Chapter; Prof. Mislav Grgic, Chair of the IEEE Croatia Section and the Dean of the Faculty of Electrical Engineering and Computing in Zagreb; and Drazen Lucic, Ph.D., president of the Council of HAKOM. A plenary talk titled "LOOOM: Defining Control Systems for 5G", was presented by Sandor Albrecht, Ph.D., Director of Network Technology, Ericsson Research, Stockholm, Ericsson AB, Sweden.

The technical conference program featured 17 conference sessions, including four special sessions and three symposia: the Symposium on Environmental Electromagnetic Compatibility, the Symposium on Green Networking, and the Symposium on Smart Environment Technologies. The special sessions were focused on hot topics including: RFID Technologies and the Internet of Things, Ad Hoc and Sensor Networks, QoS in Wired and Wireless Networks, and Security and Digital Forensics.

Besides the scientific program, a professional workshop dedicated to the wide spectra of topics in ICT was organized, and six half-day tutorials were organized by worldwide recognized experts.

In conjunction with the SoftCOM 2016 Conference, a Business Forum was organized featuring two workshops and three panel sessions with the participation of managers, executives, experts, government and institution representatives. The Lean Innovation Workshop and the Fifth Workshop on Software Engineering in Practice attracted researchers from academia and professionals from industry to discuss challenges and new developments in the area of communications software production, with a special focus on Cloud based systems. The Lean Innovation Workshop was organized by Marko Bervanakis, and moderated by Toni Mastelic, Ph.D., Ericsson Nikola Tesla, Croatia. The Workshop on Software Engineering in Practice was organized by dr.sc. Darko Huljenic, Ericsson Nikola Tesla, Croatia. The Roundtable discussion on the topic "Development of Broadband Backhaul Infrastructure in Areas Lacking Sufficient Commercial Interest for Investments, using European Structural and Investment Funds (ESI)" was organized by Mario Weber, M.Sc., director



The PhD Forum (awards ceremony and poster presentation shown above) and the Roundtable "Broadband Internet Access" (panel session shown below) have been among the most attractive events.

of the Croatian Regulatory Authority for Network Industries. The Roundtable was particularly interesting for the representatives of local communities preparing projects for development of the broadband access infrastructure of the next generation.

The Roundtable on Entrepreneurship in ICT was organized by Ante Dagelec, M.S. Representatives from academic institutions and professionals from ICT companies discussed practical aspects in entrepreneurship in the area of ICT. The Roundtable included entrepreneurs with different backgrounds and previous experiences. The topics included the "cold start" problem, relations with the government, relations with the university, human resources, software outsourcing, etc.

The Ph.D. Forum provided an opportunity for Ph.D. students to present their work in the areas of ICT related to the SoftCOM 2016 Conference topics to a wider community of researchers from academia and industry. The forum was intended to encourage interaction and networking among Ph.D. students, as well as the audience. The Ph.D. Forum was organized as a poster session, preceded by a fast-paced introduction ("pitch talk") by each student, offering a preview of the posters. The forum involved academics and students from universities from Zagreb, Split, Osijek, and Rijeka. The Forum organized by Prof. Maja Matijasevic, Prof. Dinko Begusic, Asst. Prof. Ognjen Dobrijevic, and Asst. Prof. Petar Solic.

The presentations of the student projects pursued in the frame of the Ericsson Nikola Tesla Summer Camp 2016, were held within a special workshop session that was organized by Sasa Desic, M.Sc. and Goran Gasparovic (Ericsson Nikola Tesla).

The Welcome Reception by the Mayor of the town of Split was organized in the attractive ambience of the 1700 year old Diocletian Palace Basement in Split. The participants also had an opportunity to enjoy a visit to the historic fortress of Klis and the picturesque town of Trogir, which is listed in the UNESCO World Heritage Sites list.

More information about the SoftCOM 2016 Conference may be found at: <http://www.fesb.hr/softcom>

GLOBAL

COMMUNICATIONS

NEWSLETTER

STEFANO BREGNI
Editor

Politecnico di Milano – Dept. of Electronics and Information
Piazza Leonardo da Vinci 32, 20133 MILANO MI, Italy
Tel: +39-02-2399.3503 – Fax: +39-02-2399.3413
Email: bregni@elet.polimi.it, s.bregni@ieee.org

IEEE COMMUNICATIONS SOCIETY

STEFANO BREGNI, VICE-PRESIDENT FOR MEMBER AND GLOBAL ACTIVITIES
CARLOS ANDRES LOZANO GARZON, DIRECTOR OF LA REGION
SCOTT ATKINSON, DIRECTOR OF NA REGION
ANDRZEJ JAJSCZYK, DIRECTOR OF EMEA REGION
TAKAYA YAMAZATO, DIRECTOR OF AP REGION
CURTIS SILLER, DIRECTOR OF SISTER AND RELATED SOCIETIES

www.comsoc.org/gcn
ISSN 2374-1082

UPDATED ON THE COMMUNICATIONS SOCIETY'S WEB SITE
www.comsoc.org/conferences

2017

MARCH

NCC 2017 — Nat'l. Conference on Communications, 2–4 Mar.

Madras, India
<http://ncc2017.org/>

IEEE DYSPAN 2017 — IEEE Dynamic Spread Spectrum Access Symposium, 6–9 Mar.

Baltimore, MD
<http://dyspan2017.ieee-dyspan.org/>

ICIN 2017 — Conference on Innovations in Clouds, Internet and Networks, 7–9 Mar.

Paris, France
<http://www.icin-conference.org/>

NETSYS 2017 — Int'l. Conference on Networked Systems, 13–17 Mar.

Göttingen, Germany
<http://netsys17.uni-goettingen.de/>

IEEE WCNC 2017 — IEEE Wireless Communications and Networking Conference, 19–22 Mar.

San Francisco, CA
<http://wcnc2017.ieee-wcnc.org/>

OFC 2017 — Optical Fiber Conference, 19–23 Mar.

Los Angeles, CA
<http://www.ofcconference.org/>

IEEE CogSIMA 2017 — IEEE Conference on Cognitive and Computational Aspects of Situation Management, 27–31 Mar.

Savannah, GA
<http://cogsima2017.ieee-cogsima.org/>

WD 2017 — Wireless Days 2017, 29–31 Mar.

Porto, Portugal
<http://www.wireless-days.com/>

APRIL

IEEE ISPLC 2017 — IEEE Int'l. Symposium on Power Line Communications and its Applications, 3–5 Apr.

Madrid, Spain
<http://isplc2017.ieee-isplc.org/>

WTS 2017 — Wireless Telecommunications Symposium, 26–28 Apr.

Chicago, IL
<http://www.cpp.edu/~wtsti/>

–Communications Society portfolio events appear in bold colored print.

–Communications Society technically co-sponsored conferences appear in black italic print.

–Individuals with information about upcoming conferences, Calls for Papers, meeting announcements, and meeting reports should send this information to: IEEE Communications Society, 3 Park Avenue, 17th Floor, New York, NY 10016; e-mail: p.oneill@comsoc.org; fax: + (212) 705-8996. Items submitted for publication will be included on a space-available basis.



21-23 September 2017 // Split // Croatia

Call for Papers

The IEEE ComSoc technically co-sponsored 25th International Conference on Software, Telecommunications and Computer Networks (*SoftCOM 2017*) will be held in attractive ambience of the Radisson Blu Resort hotel in Split, Croatia, September 21 to 23.

Authors are invited to submit their original research papers in all areas of communications software, services and applications, telecommunications and computer networks. Accepted and presented papers will be published in the conference proceedings, and submitted to IEEE Xplore.

Business Forum will gather managers, executives, experts, government and institution representatives who will exchange opinions and experiences on a number of hot topics in contemporary and future ICT industry and market including business, technological and social aspects.

General Co-Chairs: Sinisa Krajnovic, *Ericsson AB, Sweden* and Dinko Begusic, *University of Split, FESB, Croatia*

TPC Co-Chairs: Nikola Rozic, *University of Split, FESB, Croatia* and Pascal Lorenz, *University of Haute Alsace, France*

Conference contact: softcom@fesb.hr

More information: <http://softcom2017.fesb.hr>

SYMPOSIA, SPECIAL SESSIONS & WORKSHOPS

- Symposium on Smart Environments & Internet of Things
- Symposium on Green Networking and Computing
- Symposium on Security and Digital Forensics
- Symposium on Evolution of Cloud Computing
- Symposium on QoS in Wired and Wireless network
- Symposium on Ad-Hoc and Sensor Networks
- Symposium on Environmental Electromagnetic Compatibility
- Workshop on IoT in Elderly-Friendly Cities and Healthy Ageing Services

PROFESSIONAL PROGRAM

- 6th Workshop on Software Engineering in Practice
- 23rd Workshop on ICT

Complete manuscript due: **May 20, 2017**
 Notification of acceptance: **July 1, 2017**
 Camera-ready manuscript: **July 25, 2017**

ENABLING MOBILE AND WIRELESS TECHNOLOGIES FOR SMART CITIES: PART 2



Ejaz Ahmed



Muhammad Imran



Mohsen Guizani



Ammar Rayes



Jaime Lloret



Guangjie Han



Wael Guibene

Due to advancements in communication and computing technologies, smart cities have become the main innovation agenda of research organizations, technology vendors, and governments. To make a city smart, a strong communications infrastructure is required for connecting smart objects, people, and sensors. Smart cities rely on wireless and mobile technologies for providing services such as healthcare assistance, security and safety, real-time traffic monitoring, and managing the environment, to name a few. Such applications have been a main driving force in the development of smart cities. Without the appropriate communication networks, it is really difficult for a city to facilitate its citizens in a sustainable, efficient, and safer manner/environment. Considering the significance of mobile and wireless technologies for realizing the vision of smart cities, there is a need to conduct research to further investigate the standardization efforts and explore different issues/challenges in wireless technologies, mobile computing, and smart environments.

In this *IEEE Communications Magazine* Feature Topic (FT), we invited researchers from academia, industry, and government to discuss challenging ideas, novel research contributions, demonstration results, and standardization efforts on enabling mobile and wireless technologies for smart cities. After a rigorous review process, 17 papers were selected to be published in this FT of *IEEE Communications Magazine*. Six of the 17 are published here in Part 2 of the FT.

Self-sustainable smart buildings are expected to be an inherent component of smart cities. To ensure uninterrupted power supply, the authors of “A Multi-Tenant Cloud-Based

DC Nano Grid for Self-Sustained Smart Buildings in Smart Cities” propose a cloud-assisted solution to make intelligent decisions. The authors consider various smart buildings controlled through different data centers, which are connected to the cloud. The performance supremacy of the proposed solution makes it a considerable candidate for real implementation.

The authors of “UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges” highlight the significance of connected and autonomous vehicles. Due to unique characteristics (e.g., mobility, autonomous operation, and communication/processing capabilities), the practicality of unmanned aerial vehicles in various applications and corresponding challenges are investigated to fully automate next generation intelligent transportation systems for smart cities.

Mobile cloud computing is one of the most important emerging technologies for smart cities. To cope with the limited resources of smart mobile devices and meet the requirements of smart city applications, the authors in “A Unified Urban Mobile Cloud Computing Offloading Mechanism for Smart Cities” propose a unified offloading mechanism to jointly manage communication and computing resources for effective load balancing.

Realizing the significance and potentials of mobile edge computing (MEC) in the context of smart cities, the authors in “Mobile Edge Computing Potential in Making Cities Smarter” propose an effective solution to enhance the user’s quality of service experience of video streaming. The proposed solution employs smart MEC architecture and the “Follow-

Me-Edge” concept to allow ubiquitous data access. It helps in reducing core network traffic and achieving ultra-short latency (i.e., 1 ms) for emerging 5G mobile networks.

To support mobile terminals in smart cities, T. Han *et al.* propose vertical (i.e., different tiers) and horizontal (i.e., base stations/access points) converged architecture for heterogeneous wireless networks in “5G Converged Cell-Less Communications in Smart Cities.” Software defined network controllers are used to manage traffic scheduling and resource allocation. The performance gains in terms of coverage probability and energy saving at both base stations and mobile terminals are achieved.

Security and privacy are among the most prominent concerns in smart cities due to the recent proliferation and deployment of heterogeneous technologies. Realizing this fact, the authors in “Cybersecurity and Privacy Solutions in Smart Cities” identify various security vulnerabilities and privacy issues in different application domains. They also discuss various solutions and make some recommendations.

The Guest Editors would like to thank all the involved people, including the contributing authors for their high-quality submissions, the anonymous reviewers for their timely and insightful comments, and the *IEEE Communications Magazine* staff for their continuous support. We believe that the presented contributions in this FT will captivate and spark novel research directions for mobile and wireless technologies for smart cities.

BIOGRAPHIES

EJAZ AHMED has worked as a researcher at C4MCCR, University of Malaya, Malaysia, CogNet Lab, NUST, and CoReNet, Maju, Pakistan. He is an Associate Technical Editor of *IEEE Communications Magazine*, *IEEE Access*, *Springer MJCS*, and *Elsevier JNCA*. He has also served as a Lead Guest Editor for the *Elsevier FGCS Journal*, *IEEE Access*, *Elsevier Computers & Electrical Engineering*, *IEEE Communications Magazine*, *Elsevier Information Systems*, and *Transactions on Emerging Telecommunications Technologies*.

MUHAMMAD IMRAN is currently working at King Saud University and is a visiting scientist at Iowa State University. His research interests include MANETs, WSNs, WBANs, M2M/IoT, SDN, and security and privacy. He has published a number of research papers in refereed international conferences and journals. He serves as a Co-Editor-in-Chief for *EAI Transactions* and Associate/Guest Editor for *IEEE Access*, *IEEE Communications Magazine*, *Computer Networks*, *Sensors*, *IJDSN*, *JIT*, *WCMC*, *AHSWN*, *IET WSS*, *IJAACS*, and *IJITEE*.

MOHSEN GUIZANI [S’85, M’89, SM’99, F’09] received his B.S., M.S., and Ph.D. from Syracuse University. He is currently a professor and the ECE Department Chair at the University of Idaho. His research interests include wireless communications/mobile cloud computing, computer networks, security, and smart grid. He is the author of nine books and 400+ publications. He was the Chair of the IEEE Communications Society Wireless Technical Committee. He served as an IEEE Computer Society Distinguished Speaker.

AMMAR RAYES [S’85, M’91, SM’15] is a Distinguished Engineer focusing on the technology strategy for Cisco Services. His research interests include IoT, network management NMS/OSS, machine learning, analytics, and security. He has authored three books, over 100 publications in refereed journals and conferences on advances in software and networking related technologies, and over 25 patents. He received B.S. and M.S. degrees from the University of Illinois at Urbana and his D.Sc. degree from Washington University, all in electrical engineering.

JAIME LLORET [M’07, SM’10] received his M.Sc. in physics in 1997, his M.Sc. in electronic engineering in 2003, and his Ph.D. in telecommunication engineering in 2006. He is the head of the Communications and Networks research group of the Research Institute IGIC. He is Editor-in-Chief of *Ad Hoc and Sensor Wireless Networks* and *Network Protocols and Algorithms*. He has been General Chair of 36 international workshops and conferences. He is an IARIA Fellow.

GUANGJIE HAN [S’01, M’05] is currently a professor with the Department of Information and Communication Systems, Hohai University, China. His current research interests include sensor networks, computer communications, mobile cloud computing, and multimedia communication and security. He has served on the Editorial Boards of 14 international journals, including *IEEE Access* and *Telecommunication Systems*. He has guest edited a number of Special Issues in IEEE journals and magazines. He is a member of ACM.

WAEL GUIBENE has been a research scientist at Intel Labs since June 2015. He was awarded his Ph.D. from Telecom ParisTech in July 2013. He also holds an M.Eng. and a Master’s degree in telecommunications obtained in 2009 and 2010, respectively. He worked at Eurecom as a research engineer from 2010 to November 2013, and then joined Semtech to work on LoRa systems from 2013 to June 2015. His research activities include IoT, 5G, and wireless communications.

A Multi-Tenant Cloud-Based DC Nano Grid for Self-Sustained Smart Buildings in Smart Cities

Neeraj Kumar, Athanasios V. Vasilakos, and Joel J. P. C. Rodrigues

Energy is one of the most valuable resources of the modern era and needs to be consumed in an optimized manner by intelligent usage of various smart devices, which are major sources of consumption of energy nowadays. With the popularity of low-voltage dc appliances such as-LEDs, computers, and laptops, there is a great need to design new solutions for self-sustainable smart energy buildings containing these appliances.

ABSTRACT

Energy is one of the most valuable resources of the modern era and needs to be consumed in an optimized manner by an intelligent usage of various smart devices, which are major sources of energy consumption nowadays. With the popularity of low-voltage DC appliances such as-LEDs, computers, and laptops, there arises a need to design new solutions for self-sustainable smart energy buildings containing these appliances. These smart buildings constitute the next generation smart cities. Keeping focus on these points, this article proposes a cloud-assisted DC nanogrid for self-sustainable smart buildings in next generation smart cities. As there may be a large number of such smart buildings in different smart cities in the near future, a huge amount of data with respect to demand and generation of electricity is expected to be generated from all such buildings. This data would be of heterogeneous types as it would be generated from different types of appliances in these smart buildings. To handle this situation, we have used a cloud-based infrastructure to make intelligent decisions with respect to the energy usage of various appliances. This results in an uninterrupted DC power supply to all low-voltage DC appliances with minimal dependence on the grid. Hence, the extra burden on the main grid in peak hours is reduced as buildings in smart cities would be self-sustainable with respect to their energy demands.

In the proposed solution, a collection of smart buildings in a smart city is taken for experimental study controlled by different data centers managed by different utilities. These data centers are used to generate regular alerts on the excessive usage of energy from the end users' appliances. All such data centers across different smart cities are connected to the cloud-based infrastructure, which is the overall manager for making all the decisions about energy automation in smart cities. The efficacy of the proposed scheme is evaluated with respect to various performance evaluation metrics such as satisfaction ratio, delay incurred, overhead generated, and demand-supply gap. With respect to these metrics, the performance of the proposed scheme is found to be good for implementation in a real-world scenario.

INTRODUCTION

With the widespread popularity of the Internet of Things (IoT) over the last few years, the concept of smart buildings in smart cities has become popular. A smart building consists of various smart gadgets such as smartphones, cameras, PDAs, and other household appliances, which are Internet-enabled and can be monitored and controlled from remote locations. These smart appliances can communicate and share data with each other using the Internet. The collection of all such smart appliances (commonly known as things/objects) across the globe is called IoT. According to a recent survey [1], there are more than 20 billion such smart objects/things expected to be interconnected with each other for data sharing. These appliances are an integral part of our daily life and can be located in a building called a smart building. The collection of all such smart buildings along with other components, including intelligent transportation systems, e-governance, and e-healthcare, constitute smart cities.

Generally, most of the appliances in a smart building operate on low-voltage DC sources [1]. However, with an evolution in the usage of Internet-enabled smart devices, the power consumption in a smart building has recently increased many times. This has led to the emergence of the use of DC power sources at the distribution level, which was earlier dominated by AC power sources. Many commercial buildings such as shopping malls, government offices, and entertainment parks require uninterrupted power to satisfy users' demands. Hence, for demand side management, there is a requirement for efficient power management at various stages in modern existing infrastructure [1]. However, the traditional power system is AC-based, which requires various phases of AC-DC conversion at various stages during transmission and distribution. This process causes significant power loss during transmission and distribution. This also causes a long delay for power transmission from generation to the consumers located in a community. To remove these problems, one of the solutions is the usage of a DC nano grid in a building so that the building becomes self-sustainable with respect to power generation and consumption. In this type of smart building in a smart city, the renewable energy sources such as-photovoltaic (PV) panels and fuel

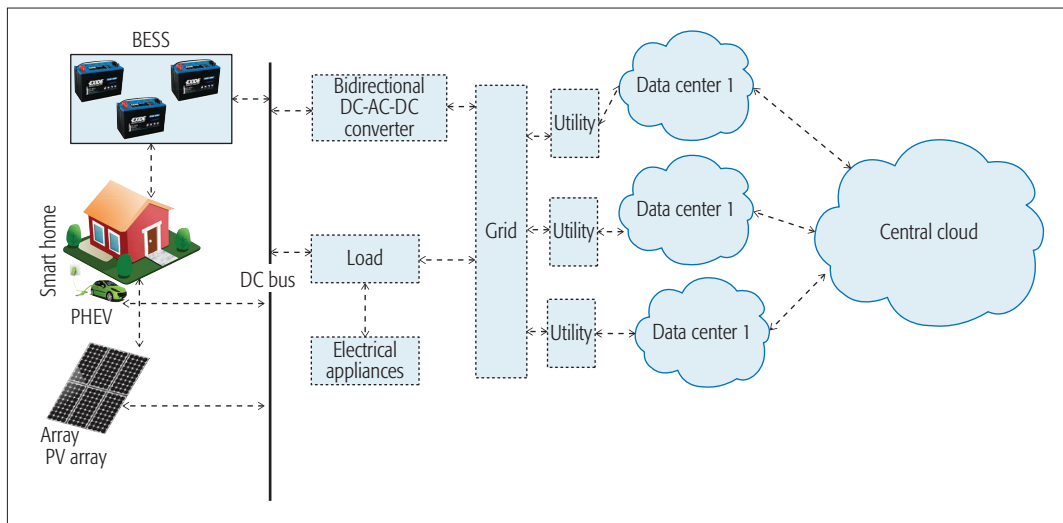


Figure 1. Architecture of the proposed system.

cells can be used as both these type of sources generate DC voltage. On the other hand, wind energy sources can also be used on buildings with suitable AC-DC converters as these sources generate only AC voltage. A nano grid can be AC or DC depending on the power supply sources, but for this article, we have considered only DC power sources that constitute a DC nano grid. The energy generated from these sources can be stored in the battery energy storage system (BESS), which can be used in peak hours for maintaining the balance between demand and supply. This would make most of the modern smart buildings self-sustainable with respect to their energy consumption.

To meet the issue of demand and supply, intelligent decisions need to be made with respect to the effective usage of various smart appliances in a smart building. This requires efficient data mining and data processing at various data centers located at distributed locations. To process such a large collection of data from different buildings, cloud computing is one of the best options. In the proposed solution, we have assumed that there is one data center for each smart city located in a geographical region. These data centers are interconnected with each other and to the central cloud using the Internet for data sharing and load balancing, that is, for energy saving purposes, one of the data centers may be shut down, and its load may be shifted to another data center that is underutilized and may be located in a different locality. However, this type of decision needs to be made by a central controller, which is located on the central cloud in the proposed scheme [1–6].

Figure 1 shows the generalized architecture used in the proposed scheme. In this figure, various cloud data centers are assumed to be connected to the centralized cloud with interconnection to the grid. The smart home in a locality is assumed to have BESS, a PV array, and various charging points used by plug-in hybrid electric vehicles (PHEVs). The power generation sources considered in the proposal generate DC voltage and are connected to the common DC bus. A bidirectional DC-AC-DC converter is also attached to the common bus along with various

electrical appliances, which are considered as loads. Finally, the output produced is connected to the grid. The grid is used only in the worst case when there is a scarcity of the power generated from the renewable energy sources, that is, if demand is high and generation is less from all the renewable energy sources. A PV array generates power that is used by the smart home appliances, and extra unused power is stored in the BESS, which can be used in the peak hours when there is a power crisis. All data centers are used for information dissemination from different communities to the central cloud so that it can be processed with less delay. Hence, in the proposed scheme, each smart building in a community acts as a nanogrid capable of meeting its power requirements from the renewable energy sources. Hence, each building is self-sustainable with respect to the power usage by various appliances in it.

INTEGRATION OF SG AND CLOUD WITH SMART BUILDINGS

As discussed above, with the evolution of IoT, the concept of smart buildings becomes popular. On the other hand, with the widespread usage of smart devices, there is a great need for information exchanges between various smart devices. As these devices are of heterogeneous nature with diverse processing power, collection and processing of such a large database is one of the most challenging tasks to be performed. Moreover, the paradigm shift from the traditional grid to the smart grid (SG) introduces a new challenge with respect to the distributed data managed by the different service providers located in different communities. Hence, there is a need for a centralized controller that monitors all the resources and allocates these to the users as per their demands so that the demand-supply gap can be managed. To store and execute this large database repository, cloud-based infrastructure is required. The cloud computing provides a unique platform for multiple job execution in a virtualized environment so that data can be accessed by users anywhere, even on the fly. Keeping focus on all these major constraints and challenges, we integrate the SG and smart building with a centralized cloud-based infrastructure.

In the proposed scheme each smart building in a community acts as a nano grid capable of meeting its power requirements from renewable energy sources. Hence, each building is self-sustainable with respect to the power usage by various appliances in it.

For the creation of coalitions among multiple tenants, a multi-leader multi-follower Stackelberg game is proposed among the tenants and service providers having a pool of physical machines. Each tenant has a utility function that is based on the available number of resources and demands the additional resources it wants to execute a job.

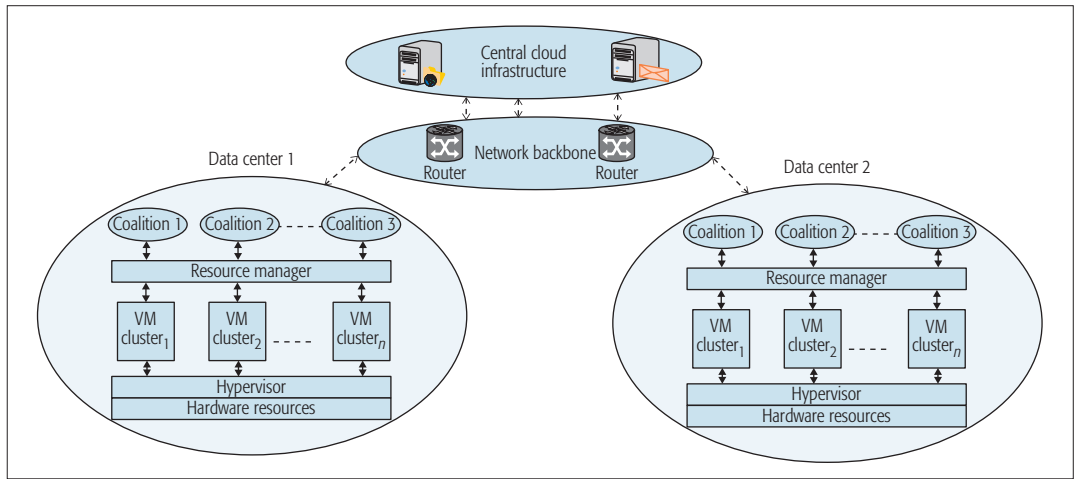


Figure 2. Multi-tenant cloud infrastructure.

RESEARCH CONTRIBUTIONS OF THIS WORK

Based on the above discussion, the main research contributions of this work are summarized as follows.

A DC nano grid for self-sustaining smart buildings is proposed in which all the smart buildings are capable of maintaining their energy needs from renewable energy sources.

For collection of data from various smart buildings in a smart city, cloud data centers are connected to a centralized cloud-based infrastructure. This centralized controller is located at the central cloud, which makes decisions and issues commands for power flow between smart devices in the presence of the centralized cloud controller.

For getting the fast response from the cloud controller, dynamic workflow management is constructed. Using dynamic workflow management, a load-aware scheduling mechanism is designed, the performance of which is evaluated using various evaluation metrics. Based on the power utilization ratio in the load-aware scheduling mechanism, different appliances in the smart home are scheduled.

Finally, for effective resource management, a cluster of virtual resources (e.g., virtual machines) are maintained at the cloud using a multi-tenant cloud-based architecture. This architecture is used to speed up the execution of multiple jobs in the virtual environment used in the proposed scheme.

ORGANIZATION

The rest of the article is structured as follows. The next section illustrates the multi-tenant cloud-based infrastructure used in the proposed scheme. Then we describe how dynamic demand construction along with workflow management are executed in the proposed scheme. How the cluster of virtual machines (VMs) are managed is also explained. Following that, we describe the performance evaluation of the proposed scheme. Finally, we conclude the article with future directions.

MULTI-TENANT CLOUD-BASED INFRASTRUCTURE

This section illustrates the multi-tenant cloud-based infrastructure used in the proposed scheme for fast execution of various jobs in the virtu-

al environment. The virtual environment in the proposed scheme consists of dedicated servers deployed in the data center of the cloud. There may be different data centers located across the globe, and these data centers can share information with one another using the communication infrastructure, which consists of gateway, routers, and network protocols. The underlying hardware infrastructure is assumed to be common in the proposed scheme so that infrastructure-as-a-service (IaaS) can be utilized virtually. Thus, the proposed solution assumes that there is a physical machine.

In the proposed scheme, a coalition of tenants are considered for resource allocation. The coalition of tenants share a pool of resources from the same or different VMs, which may be located on the same or different physical machines. Two types of resources, CPU and memory, are considered in the proposed scheme. For demands generated from multiple tenants, a group of VMs are allocated for faster execution of jobs. At any instant of time, a tenant may have multiple instances of the same or different resources. Per the demand generated for a particular resource, it may release some of the resources for the other tenants. Tenants having the same resource requirements are grouped together for allocation of VMs. For the creation of coalitions among multiple tenants, a multi-leader multi-follower Stackelberg game is proposed among the tenants and service providers having a pool of physical machines. Each tenant has a utility function that is based on the available number of resources and demands the additional resources it wants to execute a job.

Figure 2 describes a multi-tenant architecture for cloud-based infrastructure in the proposed solution. In the proposed scheme, a cluster of tenants are allocated to a group of VMs. The group of VMs are supposed to be located in different geographically located data centers.

DYNAMIC DEMAND CONSTRUCTION

This section illustrates how fluctuating load-aware scheduling activities flow is designed for execution of various jobs in the proposed scheme. A workflow is the complete sequence of activities performed by the controller to make decisions with respect to the job execution, keeping in view

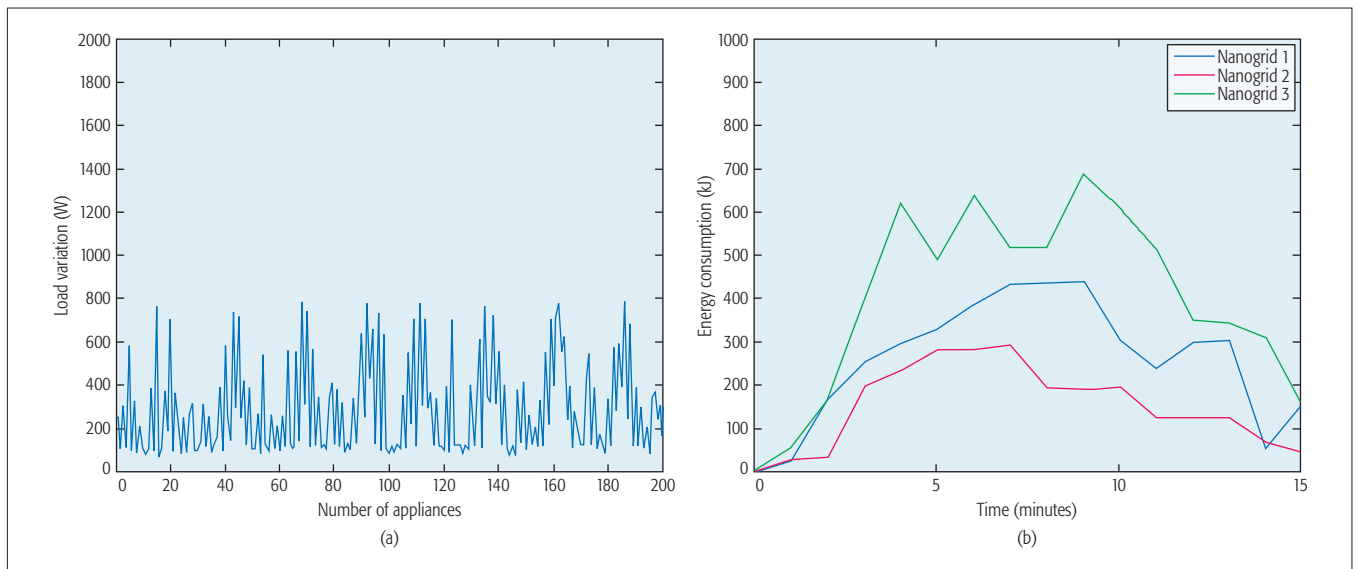


Figure 3. Analysis of a) variation in load with finite number of appliances; b) variation of energy consumption with time.

the availability of resources such as memory and CPUs. Moreover, based on the available power resources and power consumer appliances, an optimized scheduling policy is designed in the proposal.

FLUCTUATING LOAD-AWARE SCHEDULING

This section illustrates how the fluctuating load-aware scheduling activity flow is maintained and designed in the proposed solution. Power generation sources (PGSs) and power consumers (PCs) are assumed to be interconnected with the common bus in the proposed solution. PGSs such as PV panels and wind generation are considered with AC-DC converters to have a common DC bus for all appliances from which power is drawn by various appliances. For this purpose, the power utilization ratio (PUR) of all the appliances is computed as

$$PUR_i = \frac{pow_i}{\sum_{i=1}^n pow_i} \quad (1)$$

$$pow^{tot} = \sum_{i=1}^n pow^{gen}$$

where pow^{tot} is the total power received at the controller from all the sources, and pow^{gen} is the total power generation from all sources. There may be some power losses due to transmission and distribution at various levels. Power utilization ratio is computed based on the power consumed by an appliance pow_i to the aggregated power consumed by all the appliances. The controller in the proposed scheme continuously monitors the status of all appliances' power consumption by maintaining a gap between demand and supply at all times. During any voltage fluctuation at the grid level, it maintains PUR under control for all appliances by providing an extra energy from the battery energy storage system (BESS). The BESS is used in the proposed scheme for storing extra energy generated from all the sources and remains unutilized by various appliances. This extra energy is stored when demand from vari-

ous appliances is less and is used as soon as the demand for power usage grows exponentially in peak hours. Thus, this mechanism reduces the dependence on the grid.

As per Eq. 1, the PUR of all the devices is computed for construction of activity flow scheduling. The controller located at the cloud generates regular alerts of shutting down or operation of various appliances as per the PUR of the devices, which in turn generates an optimized schedule of power consumption of various appliances. Moreover, it also reduces the gap between demand and supply at all times per the demands generated by various tenants across different geographical locations.

As there may be contention due to the multiple requests generated from multiple tenants from different communities, an optimized workflow with respect to the usage of VM based on the current and future loads needs to be designed. In the proposed solution, adaptive load forecasting with respect to the usage of different VMs is designed, which takes care of the current and future load generated from all tenants in a community. The load with respect to the usage of various resources may vary from different tenants, so the requests generated from these tenants produce a variable load at any instant.

CLUSTER OF VM MANAGEMENT

This section illustrates how a cluster of VMs are maintained at the proposed cloud-based infrastructure for fast execution of various jobs. For this purpose, we have taken a case study of three nanogrids in a locality consisting of a number of appliances. The impact of the number of appliances on load variation and energy requirements at any instant of time is studied.

Figures 3a and 3b show how, with an increase in number of appliances, load varies for all three nanogrids. This change in work load may increase the load on the cloud data centers by many times, which may cause improper load distribution among various VMs located at different data centers. Hence, such mismanagement results in a demand and supply gap at cloud data

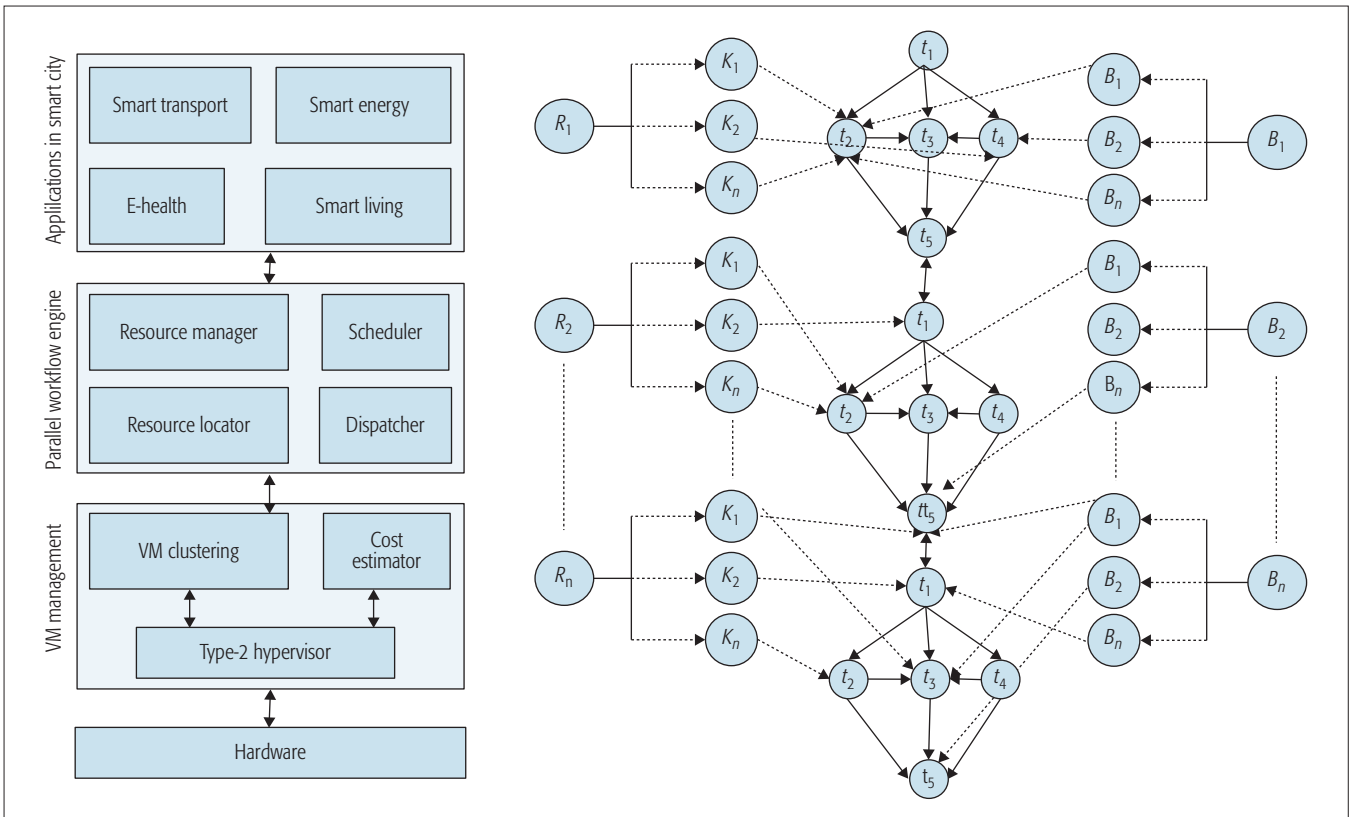


Figure 4. Workflow manager for load balancing.

centers. Thus, there is a requirement for an efficient mechanism to fill this gap by proper VM management.

Most of the time, the major component for energy consumption at the nanogrid is the continuous usage of various appliances. In the proposed solution, we have considered two controllers for making intelligent decisions with respect to the usage of energy. These two controllers are located at the smart building and cloud data centers. These controllers are called smart building controller (SBC) and cloud data controller (CDC). All SBCs receive the signal and commands from a CDC for scheduling of any appliance in the smart building. All SBCs receive commands from the CDC where control algorithms with respect to resource allocation and scheduling are executed. There is a control signal transformation between SBCs and CDC for smooth execution of various applications.

For making a cluster of VMs per the demands generated from various tenants, the PUR of each appliance as computed using Eq. 1 is used. Based on these computed values, the following equation is used for VM state space estimation:

$$VM_i^\psi = \begin{cases} \alpha, & PUR_i < \phi \\ \beta, & PUR_i > \phi \\ \gamma, & PUR_i = \phi \end{cases} \quad (2)$$

where VM_i^ψ is the i th cluster of VMs with ψ being the measure of the current state of the cluster of VMs. ψ may take values depending on the current state of the cluster of VMs, which may be underloaded, overloaded, or saturated with respect to the number of requests processing and current available resources. These conditions are influ-

enced by the PUR of the appliances, which may have values less than, greater than, or equal to a predefined threshold ϕ . Using these VM values, clusters are formed into different groups as specified in Eq. 2.

Once clusters of VMs are formed, clusters of tenants are allocated to these clusters of VMs for job execution. Tenants are clustered into different groups based on the nearest neighbor approach. In this approach, tenants with similar requirements with respect to the resource selection are grouped together in one cluster. The resource requirement is bounded by the service level agreement (SLA) of the job execution. An SLA binds the set of rules and regulations between service provider and consumer with respect to job selection and execution.

As different VMs may be located at different data centers and may have different values of VM_i^ψ , a unified policy with respect to VM migration is applied in the proposed scheme for better network utilization. In the proposed scheme, network cost is computed with respect to the number of incoming requests λ , number of channels μ , and bandwidth available B . Based on these parameters, the current migration cost on the network is computed as follows:

$$cost = \lambda \times \frac{B}{\mu} \quad (3)$$

Using this migration cost, the decisions about the VM management are made. These decisions influence the overall operational cost of the resources in the cloud computing environment. Although there is some migration overhead with respect to the VM migration from one network location to another, for bet-

ter network management and resource utilization one of the best options is always to migrate the VMs from one location to another. This in turn saves considerable energy with respect to the operations such as job scheduling and workflow management.

POWER-AWARE WORKFLOW MANAGEMENT FOR THE SMART CITY

Workflow scheduling is the sequence of activities that need to be performed for successful execution of various tasks in a system. Tasks in the proposed system can be viewed as the tenant's requests for energy satisfaction. Hence, it can be viewed as a directed acyclic graph (DAG) representation where tasks are represented as the nodes of the DAG, and edges represent the dependence of these tasks on various sources of energy such as-BESS, B_i , and renewable energy sources, R_i . Each task t_i needs one of the instances of these resources for successful execution. For example, task t_2 needs resource instances from R_1 and B_1 concurrently, that is, for successful execution of task t_1 , it may take an instance from renewable energy sources or from battery energy storage systems concurrently. Using both options, a task can be executed successfully in the proposed scheme. In Fig. 4, a layered architecture is used for processing tenants' requests for job scheduling in the proposed scheme. On the lower layers, a hardware infrastructure and type-2 hypervisor exist in which VM clustering is done with cost estimation of VM migration from one location to another. These costs are associated with respect to the cost computation of network management and maintenance. Above these layers, there is a parallel workflow engine in which components such as resource manager and resource locator exist. The functions of these components are to manage the resources with respect to the resource finding and allocation for successful execution of various jobs in the proposed scheme. A dispatcher is used to dispatch the job requests to respective VMs for execution. At the top layer of the architecture, all smart applications such as e-health, smart energy, smart transport, and smart living exist, which are typical components of a smart city. The complete sequence of activities performed for successful execution of a task is depicted in the workflow diagram in the proposed multi-tenant architecture [7–14].

PERFORMANCE EVALUATION

For all simulation tests conducted, the topology shown in Fig. 1 was used where a finite number of PHEVs submit their requests for charging from CSs. We evaluate the proposed scheme by using the following performance metrics on ns-2 [15]:

- *Delay incurred for self-sustainability*: This is the time taken to narrow the gap between demand and supply.
- *Energy gap*: This is the difference between the energy generated and consumed by various appliances in a smart building.
- *Overhead generated*: This is the network cost with respect to the VM management for job scheduling and workflow management in the cloud environment.

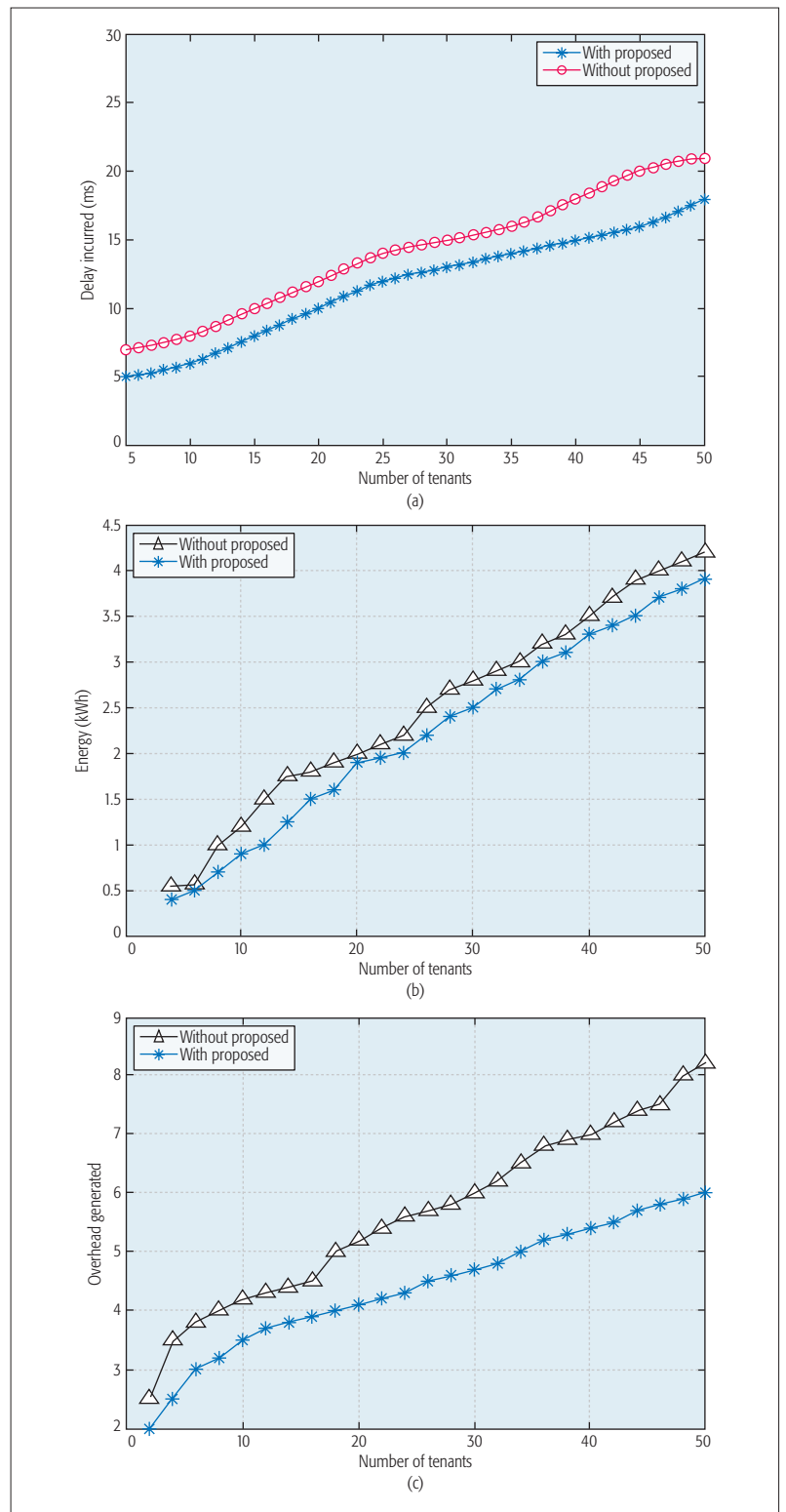


Figure 5. Results for: a) variation of delay incurred with the number of tenants; b) variation of energy gap with the number of tenants; c) variation of overhead generated with the number of tenants.

DELAY INCURRED IN SELF-SUSTAINABILITY

Figure 5a shows how the proposed scheme is successful in managing the gap between demand and supply with respect to the available resources. The control signals with respect to the operations of smart appliances in smart buildings are generated from the cloud-based controller. As can

This article proposed a novel multi-tenant cloud-based nano grid for self-sustain smart buildings. In these buildings, energy is generated from various sources such as-PV panels, and wind generation. The energy generated from these sources is stored and can be converted to dc power supply which can be used by various appliances in the smart buildings.

be seen from the results obtained, the proposed scheme generates less delay with an increase in the number of tenants for self-sustainability of smart buildings. This is mainly due to the fact that the proposed scheme has used an intelligent dynamic workflow construction where the PUR of various devices are used, and hence intelligent decisions are made by the cloud-based controller. Thus, better decisions can be made with respect to energy consumption.

ENERGY GAP

Figure 5b shows how the energy gap between demand and supply is reduced using the proposed scheme. With an increase in the number of tenants, there is an increase in the load on the nanogrids with respect to demand satisfaction. In the proposed scheme, control signals are generated from the cloud-based infrastructure with respect to the energy management at various nanogrids. With an increase in the number of tenants, the demand satisfaction with respect to the energy consumption of various devices is managed from the generation of various renewable energy sources. The extra energy generated from these renewable energy sources is stored at the BESS, which is then used per the requirements of energy generated by various tenants.

OVERHEAD GENERATED

The overhead generated is computed with respect to the control signal generated from the cloud infrastructure for making decisions with respect to energy management. This scenario is depicted in Fig. 5c. An increase in the number of tenants generates additional requests to be satisfied with respect to the energy demands at various nanogrids, but the proposed scheme still manages the load generated from these tenants under a predefined threshold. This is due to the usage of renewable energy sources and energy storage at various nanogrids, which results in overall energy management at various nanogrids. The control signals are generated from the cloud-based infrastructure in which, due to effective VM utilization, less delay is incurred. Hence, the proposed scheme is effective with respect to efficient energy management in the proposed scheme. In the proposed scheme, the cluster of VMs are allocated with respect to the requests generated from a group of tenants. Each individual state of a VM is computed based on the PUR, using which decisions about load management are made. Also, the cost of migration of VMs from one location to another is computed with respect to the resources such as available bandwidth and number of channels. Using these two metrics, VM migration cost is computed.

CONCLUSION

Smart buildings form the backbone of smart cities in modern society. With the introduction of DC nanogrids, these smart buildings are expected to be self-sustaining with respect to their energy requirements. This article proposes a novel multi-tenant cloud-based nanogrid for self-sustaining smart buildings. In these buildings, energy is generated from various sources such as PV panels and wind generation. The energy generated from these sources is stored and can be converted to DC power supply, which can be used by various

appliances in smart buildings. In the worst case, when the requirements for energy are not satisfied from these resources, it is taken from the grid. Moreover, a cloud controller is used to make decisions about the energy automation for various smart buildings that are geographically separated. To speed up the execution of various jobs with respect to the constraints of available resources, a coalition of jobs is formed and allocated to the cluster of VMs. This reduces the execution time of various jobs in the proposed solution. The performance of the proposed solution is evaluated with respect to various metrics where its performance with respect to the selected parameters is found to be satisfactory.

In the future, we will explore machine learning models to be used for efficient energy management in DC nanogrids.

ACKNOWLEDGMENTS

The work of Dr. Neeraj Kumar has been supported by a research project grant from the Council of Scientific and Industrial Research, New Delhi under the Extramural research grant scheme with reference number 22(0717)/16/EMR-II. The work of J. Rodrigues has been supported by Instituto de Telecomunicações, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, by the Government of the Russian Federation, Grant 074-U01, by National Funding from the FCT – Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2013 Project, and by Finep, with resources from Funttel, Grant No. 01.14.0231.00, under the Centro de Referência em Radiocomunicações – CRR project of the Instituto Nacional de Telecomunicações (Inatel), Brazil.

REFERENCES

- [1] S. I. Ganesan *et al.*, "Control Scheme for a Bidirectional Converter in a Self-Sustaining Low-Voltage DC Nanogrid," *IEEE Trans. Industrial Electronics*, vol. 62, no. 10, 2015, pp. 6317–26.
- [2] N. Kumar, N. Chilamkurti, and S. C. Misra, "Bayesian Coalition Game for the Internet of Things: An Ambient Intelligence-Based Evaluation," *IEEE Commun. Mag.*, vol. 53, no. 1, 2015, pp. 48–55.
- [3] N. Kumar, S. Zeadally, S. Misra, "Mobile Cloud Networking for Efficient Energy Management in Smart Grid Cyber-Physical Systems," *IEEE Wireless Commun.*, vol. 23, no. 5, 2016, pp. 100–08.
- [4] D. Dong *et al.*, "Grid-Interface Bidirectional Converter for Residential DC Distribution Systems – Part 2: AC and DC Interface Design with Passive Components Minimization," *IEEE Trans. Power Electronics*, vol. 28, no. 4, 2013, pp. 1667–79.
- [5] Z. Zheng *et al.*, "STAR: Strategy-Proof Double Auctions for Multi-Cloud, Multi-Tenant Bandwidth Reservation," *IEEE Trans. Computers*, vol. 64, no.7, 2015, pp. 2071–83.
- [6] N. Kumar *et al.*, "Playing the Smart Grid Game: Performance Analysis of Intelligent Energy Harvesting and Traffic Flow Forecasting for Plug-In Electric Vehicles," *IEEE Vehic. Tech. Mag.*, vol. 10, no. 4, 2015, pp. 81–92.
- [7] H. Liu and B. He, "F2C: Enabling Fair and Fine-Grained Resource Sharing in Multi-Tenant IaaS Clouds," *IEEE Trans. Parallel and Distrib. Systems*, vol. 27, no.9, 2016, pp. 2589–2602.
- [8] F. Xu *et al.*, "Managing Performance Overhead of Virtual Machines in Cloud Computing: A Survey, State of the Art, and Future Directions," *Proc. IEEE*, vol. 102, no. 1, 2014, pp. 11–31.
- [9] N. Kumar *et al.*, "Intelligent Mobile Video Surveillance System as a Bayesian Coalition Game in Vehicular Sensor Networks: Learning Automata Approach," *IEEE Trans. Intelligent Transportation Systems*, vol. 16, no. 3, 2015, pp. 1149–62.
- [10] X. Dai, J. M. Wang, and B. Bensaou, "Energy-Efficient Virtual Machines Scheduling in Multi-Tenant Data Centers," *IEEE Trans. Cloud Computing*, vol. 4, no. 2, 2016, pp. 210–21.

-
- [11] Ru. Yu et al., "Network Function Virtualization in the Multi-Tenant Cloud," *IEEE Network*, vol. 29, no.3, May 2015, pp. 42-47.
- [12] N. Kumar et al., "Performance Analysis of Bayesian Coalition Game-Based Energy-Aware Virtual Machine Migration in Vehicular Mobile Cloud," *IEEE Network*, vol. 29, no. 2, Mar. 2015, pp. 62-69.
- [13] M. S. Obaidat and P. Nicoplitidis, Eds., *Smart Cities and Homes: Key Enabling Technologies*, Elsevier, 2016.
- [14] A. Gelman et al., *Bayesian Data Analysis*, 2nd ed., CRC Press, 2003.
- [15] N. Kumar et al., "Energy-Efficient Multimedia Data Dissemination in Vehicular Clouds: Stochastic-Reward-Nets-Based Coalition Game Approach," *IEEE Systems J.*, vol. 10, no. 2, 2016, pp. 847-58.

BIOGRAPHIES

NEERAJ KUMAR [M'16] is working as an associate professor in the Department of Computer Science and Engineering, Thapar University, Patiala. He received his M.Tech. from Kurukshetra University, Kurukshetra, Haryana, followed by his Ph.D. from SMVD University, Katra, in computer science and engineering. He was as a postdoctoral research fellow at Coventry University, United Kingdom. He has more than 150 research papers in leading journals and conferences of repute. His research is supported by UGC, DST, CSIR, and TCS. He is an Associate Editor

of the *International Journal of Computer Science*, Wiley, and the *Journal of Networks and Computer Applications*, Elsevier.

ATHANASIOS V. VASILAKOS is a professor with Luleå University of Technology, Sweden. He has served or is serving as an Editor for many technical journals, including *IEEE Transactions on Network and Service Management*, *IEEE Transactions on Cloud Computing*, *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Cybernetics*, *IEEE Transactions on Nanobioscience*, *IEEE Transactions on Information Technology in Biomedicine*, *ACM Transactions on Autonomous and Adaptive Systems*, and the *IEEE Journal on Selected Areas In Communications*. He is General Chair of the European Alliances for Innovation.

JOEL J. P. C. RODRIGUES [S'01, M'06, SM'06] (joeljr@ieee.org) is a professor and senior researcher at the National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí-MG, Brazil, and a senior researcher at the Instituto de Telecomunicação, Portugal. He is the leader of NetGNA Research Group (<http://netgna.it.ubi.pt>), Past Chair of the IEEE ComSoc TCs on eHealth and Communications Software, and a Steering Committee member of the IEEE Life Sciences Technical Community. He is the Editor-in-Chief of three international journals, and a co-author of over 500 papers, two books, and three patents. He is the recipient of several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best paper awards.

UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges

Hamid Menouar, Ismail Güvenc, Kemal Akkaya, A. Selcuk Uluagac, Abdullah Kadri, and Adem Tuncer

Due to their mobility, autonomous operation, and communication/processing capabilities, UAVs are envisaged in many ITS application domains. The authors describe the possible ITS applications that can use UAVs, and highlight the potential and challenges for UAV-enabled ITS for next-generation smart cities.

ABSTRACT

There could be no smart city without a reliable and efficient transportation system. This necessity makes the ITS a key component of any smart city concept. While legacy ITS technologies are deployed worldwide in smart cities, enabling the next generation of ITS relies on effective integration of connected and autonomous vehicles, the two technologies that are under wide field testing in many cities around the world. Even though these two emerging technologies are crucial in enabling fully automated transportation systems, there is still a significant need to automate other road and transportation components. To this end, due to their mobility, autonomous operation, and communication/processing capabilities, UAVs are envisaged in many ITS application domains. This article describes the possible ITS applications that can use UAVs, and highlights the potential and challenges for UAV-enabled ITS for next-generation smart cities.

INTRODUCTION

Intelligent transport systems (ITSs) are considered to be one of the major building blocks of any smart city [1]. Indeed, road infrastructures have been benefiting from information and communication technologies (ICT) for decades. Despite the advanced level of the presently deployed ITS solutions, the technology is continuously evolving. Next generation ITS technologies, such as connected and autonomous vehicles, are finishing their last phase toward large-scale worldwide deployment. Testing of both technologies on public roads has already started in many countries around the world, and serious efforts are ongoing to regulate and mandate such near-future technologies. As the autonomous and inter-connected vehicle penetration in traffic increases, many new services and applications will be enabled.

Unmanned aerial vehicles (UAVs), a.k.a. drones, have been used in the military for many years. Recently, there has been a drastic increase in the use of UAVs in other fields such as precision agriculture, security and surveillance, and delivery of goods and services [2]. For instance, Amazon and Walmart have been working on a new platform that uses UAVs to deliver shipments to customers over the air (<http://www.amazon.com/b?node=8037720011>). Similarly, DHL of Germany and China's largest mailing company have started their experiments with a fleet of UAVs that could deliver around 500 parcels every day. Use of UAVs for daily consumer-oriented services is expanding and becoming a reality.

Automation of the overall transportation system cannot be achieved through only automating the vehicles. Indeed, other components of the road and the end-to-end transportation system, such as the field support team, traffic police, road surveys, and rescue teams, also need to be automated. Automation of those components can be achieved by using smart and reliable UAVs, as shown in Fig. 1. For example, a road support team can be replaced or supported by a set of UAVs that could fly around the location of an incident to provide basic support, or at least to send back a survey report about the situation. Moreover, a traffic police officer can also be replaced or supported by UAVs, which can fly over vehicles on a highway to monitor and report possible traffic violations.

ITS UAVs can provide an efficient means not only to enforce traffic rules and support traffic police on the ground, but also to provide road users with efficient information on traffic (i.e., intelligent traffic management). The ITS UAVs can be enabled with a dedicated short-range communication (DSRC) interface, which will be included in future vehicle models providing vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communications (<http://www.its.dot.gov/DSRC/dsrcfaq.htm>). Such technology will allow the ITS UAVs to communicate through a direct wireless link with vehicles in proximity to better enforce road safety and support traffic efficiency.

Some of the applications that can be enabled by ITS UAVs include, but are not limited to, flying accident report agents, flying roadside units (RSUs), flying speed cameras, flying police eyes, and flying dynamic traffic signals. These examples require multiple UAVs to fly together, collaborate, and coordinate to execute a specific mission. When acting in a group, UAVs could overcome the limitation of their energy efficiency if optimal coordination algorithms are used, for example, to perfectly share the tasks among all UAVs. In the case of a flying accident report agent, as shown in Fig. 1, one UAV could fly to the accident location and issue a report/alert (e.g., video), then

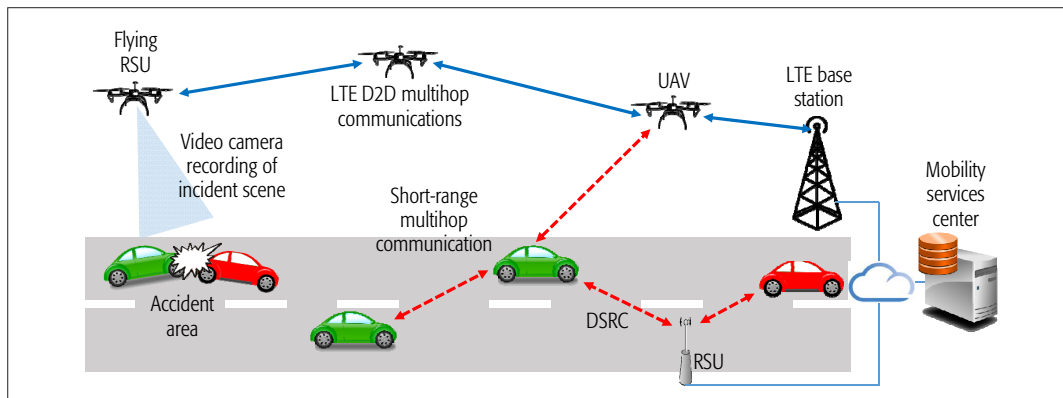


Figure 1. Example usecase scenario for UAV-enabled ITS: UAVs can be used as flying RSUs to capture video recordings of the incident scene and then relay them to a mobility services center.

Vehicles automation is one step forward toward the fully automated transportation networks as there will be still a need to automate other actors of the transport network such as traffic police agents, highway maintenance, and support teams.

land and transmit its report/alarm through other UAVs via device-to-device (D2D) multihop communications. Another nearby UAV or an RSU that has access to the network (e.g., 4G LTE) can then forward the report to the relevant entity. Designing optimal coordination algorithms is one of the challenges that need to be tackled to enable ITS UAVs.

Efficient data routing over flying UAVs, vehicles, and roadside infrastructure is another new research area that should be considered for enabling UAV-enabled ITSs. For example, flying communication nodes (i.e., UAVs) are free to move in a 3D space without restriction to road topology such as in a vehicular network. This brings some flexibility from the data routing point of view, as a flying node can fly to a specific location to strengthen a weak link or fix a broken one. Finally, security and privacy pose serious challenges to UAV-enabled ITS infrastructures within a smart city environment. One particular challenge stems from quick and efficient communication decisions that need to be made among the participants of the UAV-enabled smart city ITS infrastructure. As such, it is difficult to accommodate strong security and privacy mechanisms that are often hungry in terms of processing time. Another pertinent challenge is to preserve the privacy of sensitive information (e.g., location) from vehicles and other drones. Hence, both efficient security and privacy preserving technologies need to be adapted for the UAV-enabled ITS infrastructure in smart cities.

The rest of this article provides an overview of the potential of integrating UAVs with connected and autonomous vehicles to enable fully automated ITSs and discusses related challenges in further detail.

ITS FOR SMART CITIES

Thanks to the advancements in computer engineering and proliferation of ICT, smart cities have recently been transitioning from concept to reality. Smart cities offer improved quality of life for their citizens by providing fully or semi-automated management systems for the assets that exist in the city, such as transportation systems, the electricity network, residential homes, and offices. In future smart cities, almost every object around us will be connected to the Internet via the Internet of Things (IoT) technology [3].

The ITS constitutes one of the oldest smart city technologies, and it has been deployed in many

cities around the world. For example, in Madrid, Spain, all the public transportation systems and components, including train, tramway, buses, and bus stops, are connected to a central control room where data are collected and processed in a real-time manner to provide the end users with smart and efficient services and applications. As a user of public transportation, you can be informed about the bus arrival time at the stop next to your home, which is accurately calculated based on the real-time traffic on the bus route.

The next generation of ITS technology will be enabled by the proliferation of connected and autonomous vehicles. Connected vehicles technology provides vehicles on the same road the means to communicate and exchange real-time data that can be used to improve the safety functionalities and therefore improve road safety. Along with other sensing technologies, connected vehicles can be used to enable driverless vehicles, which will completely change the way we travel. For example, there will be no need to own a car as you could schedule an automatic pickup by an automated car every time you need a ride. Also, there will be no need to waste time searching for a parking spot at the final destination; the automated car can drop you off and go look for a parking spot. Such applications of connected vehicles are already being tested around the world. A large-scale pilot project for connected vehicles in the city of Doha, Qatar, is illustrated in Fig. 2.

Vehicle automation is one step forward toward fully automated transportation networks, but there will still be a need to automate other actors of the transport network such as traffic police agents, highway maintenance, and support teams. The last mile toward fully automated end-to-end transportation systems can be enabled by using automated UAVs.

APPLICATIONS OF UAVS IN SMART CITIES

As explained earlier, there is high potential for UAVs to complement autonomous driving and enable fully automated roads. Many new ITS-related applications could be enabled by using automated UAVs to either help improve traffic, bring better safety and security on the road, or enhance the comfort of the driver. Before being able to utilize UAVs in such applications, there are still some serious issues to tackle. These issues include limited energy, processing capabilities, and signal



Figure 2. Deployment of RSUs and onboard units (OBUs) in Doha, Qatar, to enable testing of vehicle-to-roadside-unit and vehicle-to-vehicle communications.

transmission range. Taking into account the technology revolution in the past decades, there is great potential that the above limitations in UAV utilization will be cleared in the near future. In the following sections we list and describe only a few of these applications.

FLYING ACCIDENT REPORT AGENT

When a traffic accident occurs, the lives of the involved persons depend on the rescue team efficiency, which directly relies on how fast the rescue team can reach the accident scene. When the closest rescue team terminal is located too far from the accident location, the time for the rescue team to reach the scene can be too long. In some cities, the rescue team uses helicopters to reach accidents located in isolated and rural areas. Such a solution has high related cost, making it unsuitable for many cities and scenarios. Traffic congestion on the way to or around the accident location, which can also be caused by the reported accident, is another crucial factor that can delay the rescue team.

In this context, UAVs might be a good complementary solution to help the rescue team reach the accident scene within the shortest time. Indeed, as shown in Fig. 3a, the rescue team can be equipped with an automated UAV that can quickly fly over the traffic until reaching the accident location. It is also possible to have a number of UAV stations deployed around the city from which UAVs can take-off for a mission. In that case, it is required to have some intelligence to select the right UAV station for a specific mission. This selection can be made based on the distance between the accident location and available UAV stations, number of available UAVs at each UAV station, and so on. When the UAV reaches the accident location, it can send a detailed report about the situation, for example, the number of involved persons and their situation along with their profiles, which can be supported by photos and videos. The UAV can also be used to establish a real-time communication channel (voice and video if possible) between the accident site and the rescue team still on their way (and also the team in the control center). Such a communication channel can help the rescue team to provide remote instructions if needed as well. The

Flying Accident Report Agent can also be used to provide the accident site with a first aid kit while waiting for the rescue team to arrive.

FLYING ROADSIDE UNIT

In the near future, our cars will be equipped with DSRC technology to let the vehicles communicate through a DSRC channel (similar to WiFi) with other vehicles and road infrastructure in the surrounding environment. Such an emerging technology becomes efficient when the number of equipped vehicles on the road reaches a certain threshold. At the same time, there will be a need for RSUs to be installed on the road to support the communication among vehicles. Additionally, the RSUs are needed in some places such as intersections to support the DSRC communication, which cannot go through obstacles like nearby buildings. In fact, DSRC operates over 5.9 GHz, which is known to be weak in penetrating obstacles. Most of the RSUs will be installed on the roadside at static locations along with a few mobile RSUs. For example, road operators can equip their maintenance and field service vehicles with RSUs that can operate in both static and mobile modes. If an RSU is installed on a highway maintenance vehicle, it will be in static mode when the maintenance vehicle is parked and then can switch to mobile mode when the vehicle starts driving on the highway.

Similar to a highway maintenance vehicle, a UAV can be equipped with DSRC to enable a flying RSU, as shown in Fig. 3b. The flying RSU can fly to a predefined location to execute a specific application. For example, consider an incident on the highway at a section that is not equipped with any RSU. Then the highway operator in the control center can actuate a UAV to fly to the incident site and land at the appropriate location to broadcast the information over the air and inform all approaching vehicles about the incident.

FLYING POLICE EYE

Traffic police are getting more equipped with the latest technologies to enable safer traffic on the roads. Speed and CCTV cameras remain the most used technologies to enforce traffic rules. If a driver exceeds the speed limit, he/she can be caught by either a static or mobile speed camera, and if a driver runs a stop sign, he/she can be caught by a nearby CCTV camera. As time goes by, the static cameras become less efficient as drivers get to know about them and adjust their driving behaviors when approaching the area under the angles of those cameras. This motivated the adoption of mobile cameras that can be installed at different locations (sometimes unknown locations) to surprise drivers.

Indeed, the latest technologies enable speed cameras to be fully mobile and can be operated while moving. These state-of-the-art mobile speed cameras are usually embedded on police vehicles that drive on the road to catch vehicles violating the traffic rules in the surrounding areas. The same technology can be embedded on a UAV, as in Fig. 3c, to enable a flying speed camera or for other traffic enforcement applications. We can think about fully automated UAVs that are able to execute all or specific tasks of traffic police agents. For example, a UAV can fly over a road and stop a specific vehicle for identity and a regular driv-

ing license check. The UAV can stop a vehicle by holding a traffic light that can be turned to red in front of the vehicle. The same UAV can fly over a highway and catch any vehicles for speeding or breaking traffic rules. Here may arise the issue of the limitation in the maximum speed of a UAV vs. a fast vehicle driving on a highway. This limitation can be overcome by letting the UAV fly at high altitude to get an overview, which compensates the limitation in the speed.

USE OF UAVs FOR ITSs IN SMART CITIES

Use of UAVs for ITS applications, such as roadside condition surveys or counting vehicles in traffic, has recently been getting more attention in the literature [4, 5]. In this section, we study three different aspects for ITS applications of UAV deployment optimization, data routing, and cyber-security and privacy.

UAV LOCATION DEPLOYMENT AND PATH PLANNING

Deployment of RSUs for vehicular ad hoc network scenarios has been studied in earlier works [6, 7]. On the other hand, the use of UAVs as mobile aerial RSUs has not been considered to the best of our knowledge. As shown in Fig. 4a, we envision future ITS deployments that not only consist of ground RSUs, but also flying RSUs that are carried at UAVs. Such flying RSUs will bring the capability of dynamically and optimally placing them using UAVs, considering various cost functions and other criteria. For example, in the case of an accident, UAVs may quickly arrive at the incident scene and collect critical information from nearby vehicles. In order for UAVs to be used for longer time periods in ITS applications, the use of recharge stations will be critical. To solve such an issue, we may either charge UAVs while they are not actively serving, or swap their empty batteries with charged ones to minimize interruptions in UAV utilization. To this end, joint deployment of UAVs, recharge stations, and ground RSUs becomes an intricate optimization problem, as outlined in Fig. 4a.

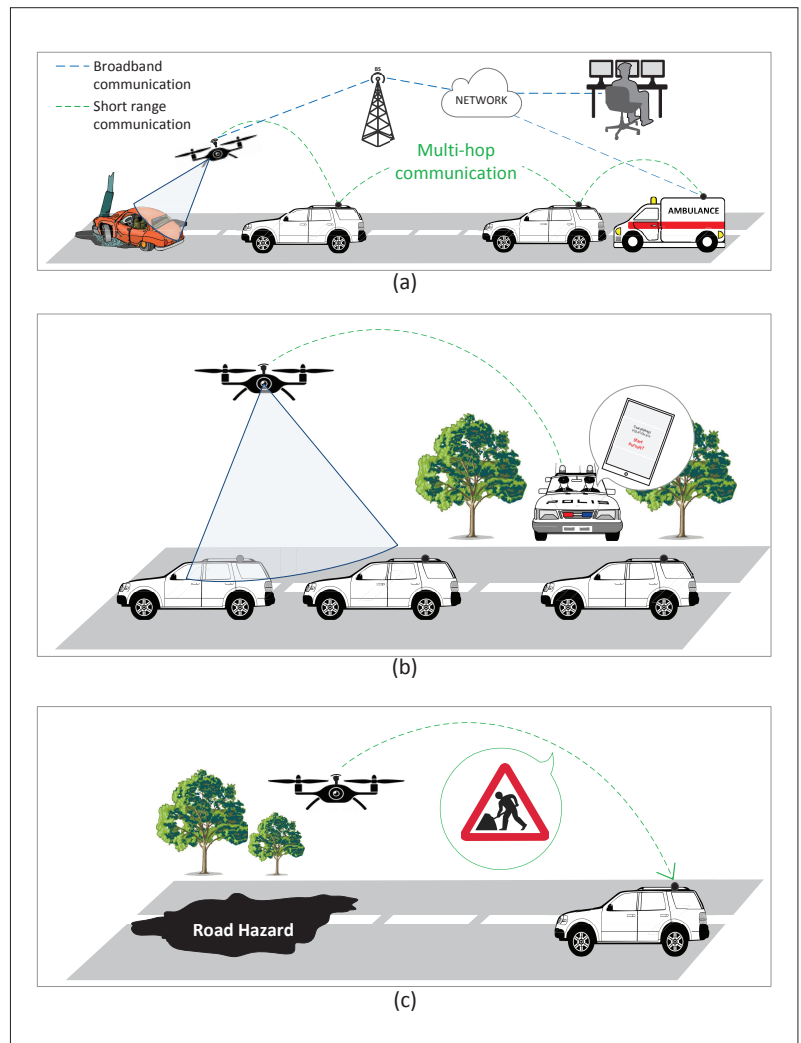


Figure 3. Examples of UAV applications in ITS: a) a UAV is used to provide the rescue team an advance report prior to reaching the incident scene; b) a UAV is used by police to catch traffic violations; c) a UAV is used as a flying RSU that broadcasts a warning about road hazards that have been detected in an area not pre-equipped with an RSU.

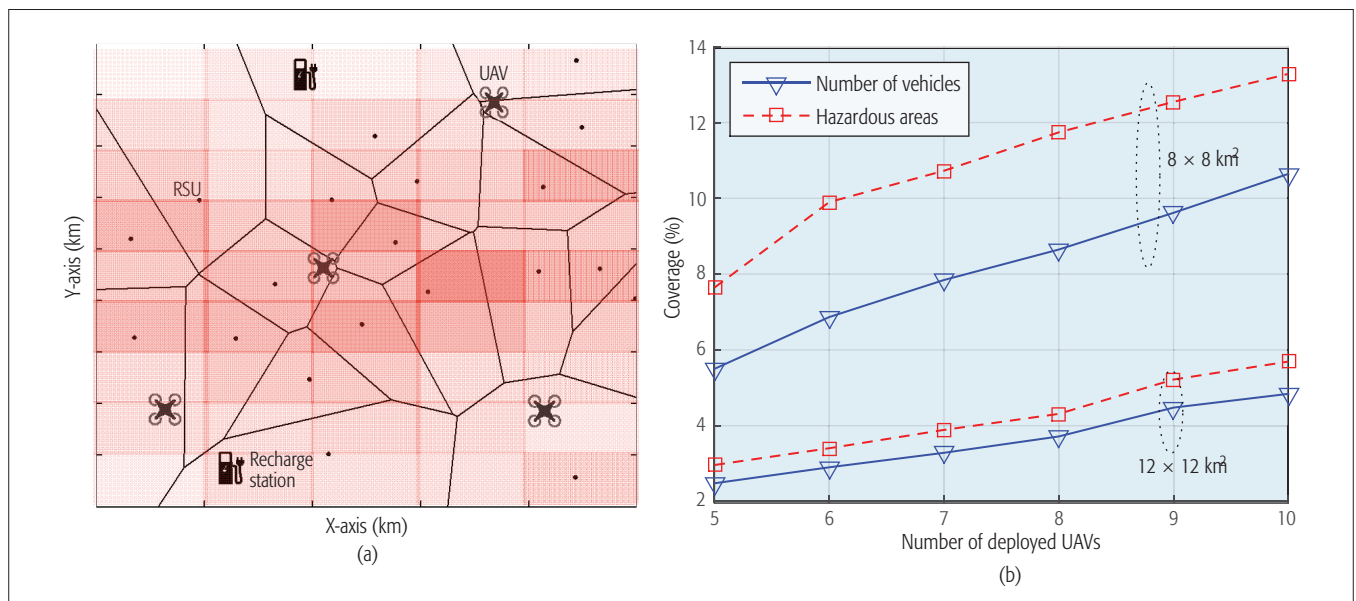


Figure 4. a) Placement of RSUs, UAVs, and recharge stations for ITS scenarios; b) coverage percentage in terms of number of vehicles and hazardous area, due to deployment of varying numbers of UAVs.

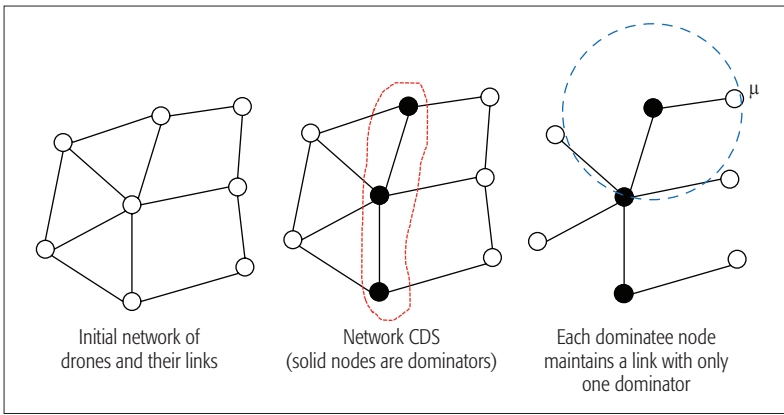


Figure 5. CDS formation for an ad hoc network of UAVs in ITS. The links among black nodes (e.g., dominators) are maintained all the time. The white nodes can have flexibility of moving further as long as they maintain their links with their dominator nodes within their transmission ranges (blue circle.)

Here, we introduce a preliminary framework for deployment optimization of UAVs in ITS scenarios. Let \mathcal{I} and \mathcal{R} denote the set of intersections and set of road segments, respectively, in a road network.

Then UAVs can alleviate deployment costs of RSUs with minimal degradation in performance. More formally, under the given deployment budget constraint B_{tot} , we can define the following optimization problem for joint RSU and UAV emplacement:

$$\begin{aligned} \max \sum_{j=1}^{N_R} \sum_{k=1}^{N_{SS}(R_j)} W_{SS}(j,k) I_{RSU}(j,k) I_{UAV}(j,k) \\ + \sum_{i=1}^{N_I} W_I(i) I_{RSU}(i) I_{UAV}(i), \end{aligned} \quad (1)$$

where N_R and N_{SS} are the total number of road segments and the total number of road sub-segments, respectively, while I_{RSU} and I_{UAV} are indicator functions that are 1 if a sub-segment or intersection is covered by a RSU/UAV and 0 otherwise. Moreover, the weight $W_{SS}(i, j)$ of each sub-segment in road R_i can be written as a function of accident frequency, vehicle count frequency, and connection time for RSU location optimization. A similar metric $W_I(i)$ can also be defined for the intersections. Given this optimization framework, various algorithms, such as genetic algorithms, ant colony optimization, bee colony optimization, and particle swarm optimization, can be used to find the optimum RSU and UAV locations. In [7], a related and simpler problem of deploying only the RSUs has been studied at QMIC, Qatar, without the involvement of UAVs. Among the Knapsack and PageRank algorithms investigated in the article, Knapsack is observed to yield better performance in terms of covering hazardous zones as well as the connectivity of the vehicles for large-scale deployment.

We performed Matlab computer simulations for deployment optimization of UAVs for a representative scenario, and the simulation results are shown in Fig. 4b. We implemented an ITS deployment framework similar to the ITS scenario in [7] where no UAVs have been considered but optimization of RSU placement has been evaluated. Simulations are carried out for urban areas with two different

sizes, $8 \times 8 \text{ km}^2$ and $12 \times 12 \text{ km}^2$. The communication coverage area of UAVs is considered to span a circle with a radius of 500 m (see, e.g., [8]). For simplicity, it is assumed that each sub-segment length is equal to the communication coverage of UAVs. Therefore, dividing roads into sub-segments can better approximate the real map [9] and also provide more UAV deployment choices. For distributing the accidents and vehicles, we consider a distribution where the likelihood of an accident and number of vehicles change from one road/intersection to another. This is a more realistic scenario where accidents are more likely to happen around intersections than in the sub-segments [6]. Numbers of vehicles and accidents are modeled as Poisson distributions.

The results in Fig. 4b show the coverage percentage for the number of vehicles and coverage of hazardous areas under different numbers of UAVs, which are placed in such a way as to maximize Eq. 1. For simplicity, the impact and optimization of RSUs and recharge station placement is not included in the results, and they are left for future work. Hazardous areas have been considered as areas with more traffic accidents. Results show that coverage percentage of hazardous areas is always larger than that of the number of vehicles. For example, if the number of deployed UAVs is increased from 5 to 10 for an $8 \times 8 \text{ km}^2$ area, coverage percentage for vehicles can be improved from 5.6 to 10.6 percent, while the coverage percentage for hazardous areas is improved from 7.8 to 13.4 percent. Moreover, using the same number of UAVs in a larger $12 \times 12 \text{ km}^2$ area significantly reduces the coverage percentages in both scenarios, with a larger degradation in the coverage percentage of hazardous areas. Further work is needed to study different spatial distributions of hazards and traffic densities and deployment optimization techniques of UAVs for different scenarios.

DYNAMIC COORDINATION AND DATA ROUTING

UAVs may act as relaying nodes or traffic monitoring tools in ITS applications for smart cities. In such cases, UAVs need to coordinate the tasks with each other and with the vehicles on the ground. This coordination needs to rely on the ability to maintain communications, in particular among the swarm of UAVs. In other words, the connectivity of the UAV network needs to be maintained at all times. Assuming that the network is modeled as a unit disk graph in 3D, we can maintain such connectivity by building a backbone of the UAV network and keeping it connected at all times.

To enable this, we propose using the notion of a connected dominating set (CDS) from graph theory. The UAVs that will be part of the CDS will need to follow a group-based mobility model based on the destination location. The UAVs that are not part of the CDS will have the flexibility to be connected to the core network (i.e., CDS) via a single link. Their movement will be constrained by their transmission range, as seen in Fig. 5. For safety applications, real-time communication is crucial, and thus, UAV u may only move within the transmission range of its dominator to maintain its connection with the rest of the network. For other application scenarios where real-time communication is not crucial, UAV u may leave that range, collect data, store it, and then come back to for-

ward the data to its *dominator* when it is within the communication range of its dominator.

In terms of end-to-end data routing among UAVs and other vehicles, there is a need for a routing protocol since multiple hops can be exploited due to the limited radio ranges. While vehicular communications plan to rely on the IEEE 802.11p and DSRC standards [10] as the underlying link-layer communication protocol for UAVs, this will not be enough in the case of multiple hops to reach an RSU or other UAVs. There has been extensive research on routing for this type of network in 2D, referred to as mobile ad hoc networks (MANETs). Some of the ideas can be applicable in this context. However, the challenges of 3D environments and mobility patterns need to be taken into account. Despite a large number of works, there are not many standards used today for such multihop routing. IEEE 802.11s is one of the standards that are IP-based and can be used with different MAC layer protocols [11]. The nice feature of this standard is that it can be used with IEEE 802.11p and thus can be interoperable with the upcoming DSRC standards. IEEE 802.11s mesh standard can form a mesh among the UAVs to provide multihop routes to certain destinations. In this case, there will be an RSU acting as the gateway and the remaining UAVs will be the wireless mesh nodes in terms of the 802.11s standard naming conventions. The vehicles will then be able to connect any of these mesh nodes as clients.

CYBERSECURITY AND PRIVACY

The provision of security and privacy for any UAV-enabled smart city ITS infrastructure and its applications in smart cities is extremely important. As future ITS and road safety systems will consist of interconnected systems of heterogeneous systems including UAVs, vehicles, and roadside infrastructure, the UAVs will carry, generate, and hand over valuable sensitive information about the users of these systems among themselves. For instance, vehicle location and speed information can be tracked and leaked to adversaries for malicious purposes. Even benign UAVs can be manipulated to perpetrate attacks on sensitive ITSs and road safety data. Hence, any sensitive data needs to be protected properly against third parties [12].

One promising technique for providing privacy is to utilize the emerging privacy preserving technologies [13, 14] (e.g., homomorphic encryption schemes). A typical scenario of fully homomorphic encryption (FHE) is illustrated in Fig. 6. The user sends the information encrypted with public key pk by function *Encrypt* to the server. The encryption scheme ϵ has an algorithm *Evaluate $_{\epsilon}$* that, given plaintext $\pi_1, \pi_2, \dots, \pi_t$, for any valid ϵ , private, public key pair (sk, pk) , any circuit C , and any ciphertext $\psi_i \leftarrow \text{Encrypt}_{\epsilon}(pk, \pi_i)$, yields $\psi \leftarrow \text{Evaluate}_{\epsilon}(pk, C, \psi_1 \dots \psi_t)$ such that $\text{Decrypt}_{\epsilon}(sk, \psi) = C(\pi_1, \pi_2 \dots \pi_t)$. The server in the cloud does operations on the encrypted numbers by function *Evaluate* with public key pk and outputs ψ . The server sends ψ back to the user. The user then decrypts ψ by function *Decrypt* with his/her private key sk and obtains the result of $C(\pi_1, \pi_2 \dots \pi_t)$. In this way, the server conducts the desired operation for the user without acquiring any plaintext. For example, a vehicle or UAV can authenticate themselves to a particular UAV or roadside infrastructure unit, which should

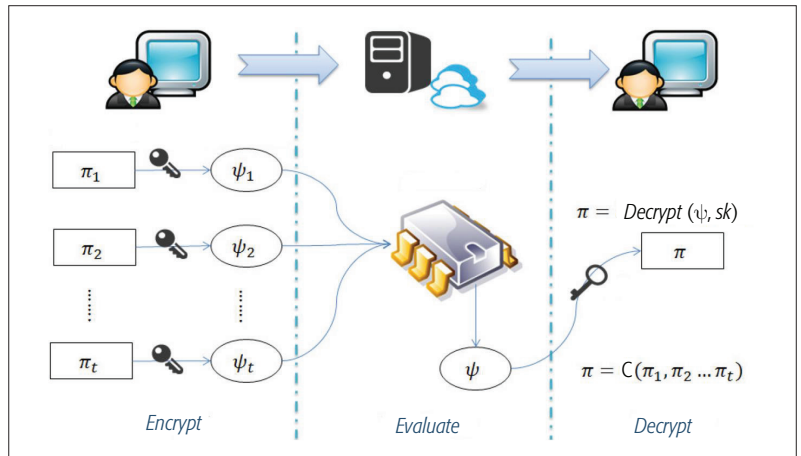


Figure 6. An illustration of Fully Homomorphic Encryption: The user (left) (e.g., UAV, vehicle), the server (right) (e.g., UAV, road-side infrastructure), and fully homomorphic operation ($\psi \leftarrow \text{Evaluate}_{\epsilon}(pk, C, \psi_1 \dots \psi_t)$).

be oblivious to sensitive data such as IDs, locations, and other pertinent data.

Although FHE systems are becoming a viable technology with recent developments on their practicality, specific aspects of UAVs such as swarm, mobility, and autonomy should also be carefully considered in adapting the privacy-preserving technologies.

In addition to privacy, another challenge is to provide flexible and configurable security that can accommodate the needs of different road safety and UAV-enabled ITS applications swiftly. In other words, the fact that decisions need to be made very quickly among the UAVs, RSUs, and vehicles to meet the delay requirements of the ITS applications pose a specific challenge to accommodate strong security and privacy mechanisms that are often hungry in terms of processing time.

DEPLOYMENT ISSUES AND CHALLENGES

There may be several deployment challenges in the utilization of UAVs for ITS applications. Regulations related to operation of UAVs may restrict how UAVs can be used for ITS scenarios. As noted in [15], integration of UAVs into national airspace requires that "UAVs function as if there were a human pilot onboard," and this is ensured through regulations by national authorities. For example, the Federal Aviation Authority (FAA) in the United States requires small UAVs to fly under 400 ft with no obstacles around, maintaining a line of sight between the pilot and the UAV at all times, not flying UAVs within 5 mi from an airport (unless permission is received from the airport and control tower), avoiding endangerment of people or aircraft, and not flying near people and stadiums. On the other hand, there may be the possibility of receiving a Certificate of Waiver or Authorization (COA) from the FAA for getting an exemption on the use of UAVs for ITS applications.

Energy limitation is another challenge. Indeed, the battery life of typical UAVs is usually less than half an hour, which introduces challenges for ITS operations with UAVs due to limited flight time. On the other hand, recent developments in battery technologies such as enhanced lithium-ion batteries and hydrogen fuel cells, more energy-efficient designs of UAVs, and the use of alternative

While UAVs have a potential to be one of the major components of future smart cities, there are also several research and implementation challenges ranging from battery limitations to UAV flight regulations. We expect that academic and industrial research and development activities will pave the way toward effective integration of UAVs into future smart cities.

energy sources such as solar energy to extend flight missions, UAVs may fly on the order of several hours in the future.

Another challenge is linked to the maximum speed a typical UAV can reach when compared to the speed of a vehicle driving on a highway. This can cause issues to some applications like the Flying Police Eye, as the ground speed of a UAV may be less than the speed of a tracked vehicle. Such a challenge can be overcome by letting the UAV fly at a high altitude, benefiting from a high view that can compensate the limitation in the speed.

Similar to any other connected network of nodes, when enabling a network of UAVs we need to be careful about security and privacy. This is obviously another serious challenge when applying UAVs to ITS. Indeed, the consequences may be high if such UAV-based ITS systems or applications are hacked. Finally, truly autonomous operation of UAVs in an ITS scenario is a big challenge, since it requires sensing of humans and obstacles to avoid collisions. In a large-scale ITS scenario with many UAVs, a human supervisor may control a swarm of UAVs that may simultaneously operate in different parts of a city. Since the attention span of a supervisor may be limited, there should be a balance between supervisor intervention and autonomous operation of UAVs. This trade-off is referred to as autonomy spectrum in [16], which provides 10 different levels of UAV swarm control ranging between fully autonomous and fully supervisor-controlled operation.

CONCLUSION

The concept of ITS is expected to move into reality in emerging smart cities. In this article, we study the applications, deployment optimization, and security/privacy challenges for the use of UAVs in ITS scenarios. While UAVs have the potential to be one of the major components of future smart cities, there are also several research and implementation challenges ranging from battery limitations to UAV flight regulations. We expect that academic and industrial research and development activities will pave the way toward effective integration of UAVs into future smart cities.

ACKNOWLEDGMENT

This publication was made possible by NPRP grant #NPRP9-257-1-056 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

- [1] Z. Xiong et al., "Intelligent Transportation Systems for Smart Cities: A Progress Review," *Science China Info. Sciences*, vol. 55, no. 12, 2012, pp. 2908–14.
- [2] I. Bekmezci, O. K. Sahingoz, and S. Temel, "Flying Ad Hoc Networks (FANETs): A Survey," *Ad Hoc Networks*, vol. 11, no. 3, 2013, pp. 1254–70.
- [3] A. Zanella et al., "Internet of Things for Smart Cities," *IEEE Internet of Things J.*, vol. 1, no. 1, Feb. 2014, pp. 22–32.
- [4] W. S. Hart and N. G. Gharaibeh, "Use of Micro Unmanned Aerial Vehicles in Roadside Condition Surveys," *Proc. Transportation Development Institute Congress*, Chicago, IL, Mar. 2011, pp. 80–92.
- [5] P. Cheng, G. Zhou, and Z. Zheng, "Detecting and Counting Vehicles from Small Low-Cost UAV Images," *Proc. ASPRS Annual Conf.*, vol. 3, Baltimore, MD, 2009, pp. 9–13.
- [6] B. Aslam, F. Amjad, and C. C. Zou, "Optimal Roadside Units Placement in Urban Areas for Vehicular Networks," *Proc. IEEE Symp. Computers Commun. (ISCC)*, Cappadocia, Turkey, July 2012, pp. 423–29.

- [7] M. Ben Brahim, W. Drira, and F. Filali, "Roadside Units Placement within City-Scaled Area in Vehicular Ad-Hoc Networks," *Proc. Int'l. Conf. Connected Vehicles and Expo*, Nov. 2014, pp. 1010–16.
- [8] A. Merwaday and I. Guvenc, "UAV Assisted Heterogeneous Networks for Public Safety Communications," *Proc. IEEE Wireless Commun. Networking Conf. Wksp.*, 2015, pp. 329–34.
- [9] Y. Liang, H. Liu, and D. Rajan, "Optimal Placement and Configuration of Roadside Units in Vehicular Networks," *Proc. IEEE VTC*, 2012, pp. 1–6.
- [10] X. Wu et al., "Vehicular Communications Using DSRC: Challenges, Enhancements, and Evolution," *IEEE JSAC*, vol. 31, no. 9, 2013, pp. 399–408.
- [11] T. Imboden, K. Akkaya, and Z. Moore, "Performance Evaluation of Wireless Mesh Networks Using IEEE 802.11s and IEEE 802.11n," *Proc. IEEE Wksp. Convergence among Heterogeneous Wireless Systems in Future Internet in conjunction with ICC '12*, Ottawa, Canada, June 2012.
- [12] P. Perazzo et al., "The Verifier Bee: A Path Planner for Drone-Based Secure Location Verification," *Proc. 2015 IEEE 16th Int'l. Symp. World of Wireless, Mobile and Multimedia Networks*, June 2015, pp. 1–9.
- [13] C. Gentry, *A Fully Homomorphic Encryption Scheme*, Ph.D. dissertation, Stanford Univ., 2009.
- [14] N. Smart and F. Vercauteren, "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes," ser. *Lecture Notes in Computer Science*, Springer, 2010, vol. 6056, pp. 420–43.
- [15] K. P. Valavanis and G. J. Vachtsevanos, "UAV Integration into the National Airspace: Introduction," *Handbook of Unmanned Aerial Vehicles*, 2015, pp. 2113–16.
- [16] G. Coppin and F. Legras, "Autonomy Spectrum and Performance Perception Issues in Swarm Supervisory Control," *Proc. IEEE*, vol. 100, no. 3, 2012, pp. 590–603.

BIOGRAPHIES

HAMID MENOVAR [SM] is a connected vehicles product manager and an R&D expert at Qatar Mobility Innovations Center (QMIC). He is a globally recognized expert in the field of connected vehicles, and his years of experience started with an active contribution in enabling the first connected vehicles field demo by the Car-to-Car Communication Consortium in Europe in 2008, followed by continuous contributions to the standardization and system design, implementation, and validation activities.

ISMAIL GUVENC [SM] has been an associate professor at North Carolina State University since August 2016. His recent research interests include 5G wireless networks, UAV communications, and heterogeneous networks. He has published more than 130 conference/journal papers, several standardization contributions, three books, and over 30 U.S. patents. He is a recipient of the 2015 NSF CAREER Award, 2014 Ralph E. Powe Junior Faculty Award, and 2006 USF Outstanding Dissertation Award.

KEMAL AKKAYA [SM] is an associate professor in the Department of Electrical and Computer Engineering at Florida International University. He leads the Advanced Wireless and Security Lab and is an area editor of the *Elsevier Ad Hoc Network Journal*. His current research interests include security and privacy, and protocol design. He has published over 120 papers in peer reviewed journal and conferences. He received the "Top Cited" article award from Elsevier in 2010.

SELÇUK ULUĞAÇ [SM] is an assistant professor at Florida International University, leading the CPS Security Lab and conducting research in security and privacy of IoT. He is a recipient of the 2015 US NSF CAREER, 2015 US Air Force Summer Faculty Fellowship, and 2007 Georgia Tech Outstanding Teaching Assistant Awards. Currently, he serves on the Editorial Boards of the *Elsevier Journal of Network and Computer Applications* and *IEEE Communications Surveys & Tutorials*.

ABDULLAH KADRI [SM] received his M.E.Sc. and Ph.D. degrees in electrical engineering from the University of Western Ontario, Canada, in 2005 and 2009, respectively. Between 2009 and 2012, he worked as a research scientist at QMIC, Qatar University. In 2013, he became a senior R&D expert focusing on R&D activities related to intelligent sensing and monitoring using mobility sensing. His research interests include wireless communications, the Internet of Things, and smart sensing.

ADEM TUNCER has been an assistant professor in the Computer Engineering Department at Yalova University, Turkey, since 2013. His recent research interests include artificial intelligence, heuristic optimization techniques, and path planning and localization of mobile robots and UAVs.

Networking • Conference Discounts • Technical Publications • Volunteer



Special Member Rates

50% off Membership for new members.

Offer valid March through 15 August 2017.

Member Benefits and Discounts

Valuable discounts on IEEE ComSoc conferences

ComSoc members save on average \$200 on ComSoc-sponsored conferences.

Free subscriptions to highly ranked publications*

You'll get digital access to IEEE Communications Magazine, IEEE Communications Surveys and Tutorials, IEEE Journal of Lightwave Technology, IEEE/OSA Journal of Optical Communications and Networking and may other publications – every month!

*2015 Journal Citation Reports (JCR)

IEEE WCET Certification program

Grow your career and gain valuable knowledge by Completing this certification program. ComSoc members save \$100.

IEEE ComSoc Training courses

Learn from industry experts and earn IEEE Continuing Education Units (CEUs) / Professional Development Hours (PDHs). ComSoc members can save over \$80.

Exclusive Events in Emerging Technologies

Attend events held around the world on 5G, IoT, Fog Computing, SDN and more! ComSoc members can save over \$60.

If your technical interests are in communications, we encourage you to join the IEEE Communications Society (IEEE ComSoc) to take advantage of the numerous opportunities available to our members.

Join today at www.comsoc.org

A Unified Urban Mobile Cloud Computing Offloading Mechanism for Smart Cities

Daniela Mazza, Daniele Tarchi, and Giovanni E. Corazza

The authors develop the UMCC framework, introducing a mobile cloud computing model describing the flows of data and operations taking place in the smart city. In particular, they focus on the proposal of a unified offloading mechanism where communication and computing resources are jointly managed, allowing load balancing among the different entities in the environment, delegating both communication and computation tasks in order to satisfy the smart city application requirements.

ABSTRACT

The increasing urbanization level of the world population has driven the development of a smart city geographic system, conceived as a fully connected wide area characterized by the presence of a multitude of smart devices, sensors, and processing nodes aimed at distributing intelligence into the city. At the same time, the pervasiveness of wireless technologies has led to the presence of heterogeneous networks, operating simultaneously in the same city area. One of the main challenges in this context is to provide sustainable solutions able to jointly optimize the data transfer, exploiting heterogeneous networks, and the data processing, exploiting heterogeneous devices, for managing smart city applications for citizens' communities. In this article, the UMCC framework is developed, introducing a mobile cloud computing model describing the flows of data and operations taking place in the smart city. In particular, we focus on the proposal of a unified offloading mechanism where communication and computing resources are jointly managed, allowing load balancing among the different entities in the environment, delegating both communication and computation tasks in order to satisfy the smart city application requirements. This allows us to cope with the limited battery power and computation capacity of smart mobile devices and plays a key role in a smart environment where wireless communication is of utmost relevance, particularly in the mobility and traffic control domains.

INTRODUCTION

According to the *World Urbanization Prospect* (<http://esa.un.org/unpd/wup/>) published by the United Nations, more than half of the population currently lives in urban areas, and about 70 percent will be city people by 2050. At the same time as urbanization, an extraordinary phenomenon concerning information and communication technology (ICT) is happening: according to the *Visual Networking Index* (<http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html>), the number of connected devices in mobility has overtaken the number of people in the world, and by 2018 it will be over 10 billion, including machine-to-machine (M2M) modules in the Internet of Things (IoT). Mobile data traffic is expected to increase about 11 times in the next five years.

Urbanization and ICT expansions are finding a relevant convergence point in the smart city concept, the icon of a sustainable and livable city, projecting the ubiquitous and pervasive computing paradigms to urban spaces, focusing on developing city network infrastructures, optimizing traffic and transportation flows, lowering energy consumption, and offering innovative services. It is through ICT that smart cities are truly turning *smart* [1], in particular, exploiting smart mobile devices (SMDs) in a mobile cloud computing (MCC) context [2]. However, the huge amount of data generated in a smart city environment could be overwhelming due to the rising and diversified quality of service (QoS) requirements of city services in relation to the computation time and energy consumed by the devices. In order to face the explosion of big data to be stored and elaborated in a smart city, mobile devices need to be supported by cloud and fog computing structures [3], allowing optimized load sharing in the network for both data storage and processing features.

For this reason, a new urban framework, named urban MCC (UMCC), is developed herein. While in [4–6] specific solutions were introduced and analyzed, here the full system view is provided with requirements and an optimization framework. UMCC can be thought of as the technological nervous system, allowing the networks and information flows of the city to enjoy a better urban way of life. UMCC is composed of different network and computing elements, having heterogeneous requirements and capabilities. Within it, the offloading process emerges as the opportune method for balancing the workload in a twofold way: On one hand, *network offloading* [7] distributes data traffic among the different wireless access technologies within the heterogeneous network (HetNet) environment. On the other hand, *computation offloading*, or *cyberforaging* [8], delegates computing functions to the cloud. In this context, a novel unified offloading mechanism can be envisaged. By means of the UMCC framework, data can be stored and processed by resource-rich devices using dynamic cell association for delegating workload, thus shortening execution time, extending battery life, and exploiting the possibility to preserve data in the cloud. The proposed framework implements a unified offloading mechanism that allows optimization of the system by offloading both communication

Reference	Objective	Strengths	Weaknesses w.r.t. UMCC
[9]	Cloud-edge-beneath (CEB) architecture	Scalable ecosystem useful for the smart city's massive scale of devices	Mostly focused on architectural aspects
[10]	Cloud-assisted data fusion	Efficient selection of nodes with respect to link quality	Mostly focused on data collection
[11]	Device-to-device-based architecture	Adds D2D communication to cloud, with increased traffic capacity	Mostly focused on the global traffic increase
[12]	Mobile as a representer (MaaR)	User-centric characterization using proactive behavior	Mostly focused on a holistic perspective

Table 1. State of the art summary.

and computing tasks in order to satisfy the smart city application requirements.

The unified offloading operation, within the UMCC framework, can be driven by a purposefully defined utility function where throughput, energy efficiency, latency, and computing performance are taken into account. Several works have already analyzed the characteristics of MCC offloading. In Table 1 the strengths and weaknesses with respect to UMCC of some of the most important works are summarized.

The rest of the article is organized as follows. In the next section, the main requirements of a smart city environment are introduced, focusing on some specific applications. Then UMCC framework is introduced, focusing on the main constitutive entities. Following that, the offloading mechanism taking advantage of the UMCC framework is discussed. In the final section, conclusions are drawn.

REQUIREMENTS OF SMART CITY APPLICATIONS

There are many taxonomies trying to define key smart city areas, where social aims, care for the environment, and economic issues are related and interconnected. The European Research Cluster on the Internet of Things (IERC) has identified in [13] a list of applications in different IoT domains, including the smart city domain. Moreover, the Net!Works ETP has issued a white paper [14] aiming to identify the major topics of smart cities that will influence the ICT environment. Furthermore, a relevant document aiming to categorize and define the different applications has been released by the European Telecommunications Standards Institute (ETSI), where several application types have been specified focusing on their bandwidth requirements [15].

Taking into account all the relevant aforementioned essays, we selected some important smart city applications in order to identify their requirements and then to leverage the UMCC. Each application can be defined through the services provided to citizens, concerning the requirements in terms of:

- **Latency:** the amount of time required by a certain application between the event happening and the event being acquired by the system
- **Energy consumption:** the energy consumed for executing a certain application locally or remotely
- **Throughput:** the amount of bandwidth required by a specific application to be reliably executed in the smart city environment

- **Computing:** the amount of computing processes requested by a certain application
- **Exchanged data:** the amount of input, output, and code information to be transferred by means of the wireless network
- **Storage:** the amount of storage space required for storing the sensed data and/or the processing application
- **Users:** the number of users needed to achieve reliable service

The QoS of a certain application can be seen as a function where each requirement plays a role less or more important depending on the application type. In the following, we list some of the most influential smart city applications by highlighting their technological requirements and characteristics, while in Table 2, the considered application types and the significance of their requirements are summarized.

Mobility: All the components in an intelligent transportation system could be connected to improve transportation safety, relieve traffic congestion, reduce air pollution, and enhance driving comfort. The necessary throughput, the computational load, and the amount of data to exchange are high, whereas we can think of storage as a secondary requirement, unless for security recording.

Healthcare: Intelligent and connected medical devices, monitoring physical activity and providing efficient therapy management by using patients' personal devices, could be connected to medical archives and provide information for medical diagnosis. In this case, there are relatively low requirements regarding energy consumption, throughput, and number of users, whereas the requirements in terms of latency, computation, exchanged data, and storage are high.

Disaster Recovery: In a disaster relief scenario people are faced with the destruction of infrastructures, and local citizens are asked to use their mobile phones to photograph the site. In this case there are relatively low requirements regarding throughput, whereas it is important to have a quick response and to save the energy of the devices.

Energy: Energy saving can take advantage of the cloud basically thanks to smart grid systems, aimed at transforming the behavior of individuals and communities toward more efficient and greener use of electric power.

Waste Management: Automatically generated schedules and optimized routes that take into account an extensive set of parameters could be

All the components in an intelligent transportation system could be connected to improve transportation safety, relieve traffic congestion, reduce air pollution and enhance comfort of driving. The necessary throughput, the computational load and the amount of data to exchange are high, whereas we can think the storage as a secondary requirement, unless for security recording.

To perform this triple role, mobile devices must become part of an infrastructure that is constituted by different cloud topologies and, at the same time, have to exploit heterogeneous wireless link technologies, allowing to address the different requirements of a smart city scenario.

Application	Requirements						
	Latency	Energy	Throughput	Computing	Exchanged data	Storage	Users
Mobility	Restrictive	Variable	Restrictive	High	High	Variable	High
Healthcare	Restrictive	Non-restrictive	Non-restrictive	High	High	High	Low
Disaster recovery	Restrictive	Restrictive	Non-restrictive	High	High	High	Variable
Energy	Non-restrictive	Non-restrictive	Non-restrictive	High	High	High	High
Waste management	Non-restrictive	Restrictive	Non-restrictive	Low	Low	Low	Low
Tourism	Non-restrictive	Restrictive	Non-restrictive	High	High	High	Variable

Table 2. Summary of smart city applications and requirements.

planned not only looking at the current situation, but also considering the future outlook. We can expect non-restrictive requirements of latency and throughput, and resource-poor devices have to be taken into consideration. The requirements related to data to be exchanged, load of computation, storage, and number of users are not critical.

Tourism: Augmented reality and social networks are the characteristics of applications that take more advantage of the cloud, which also becomes useful for mobile users sharing photos and video clips, tagging their friends in popular social networks. We can expect non-restrictive requirements for latency and throughput, and resource-poor devices have to be taken into consideration. There is a great amount of data to be exchanged; load of computation and storage and number of users are variable.

By comparing the above described applications, it is possible to highlight that a smart city scenario is composed of several heterogeneous services with different requirements. However, it is possible to note that most of them require high computational complexity and a very high amount of data to be exchanged in order to be executed. Moreover, it should be noted that in a smart city scenario multiple services coexist, increasing the system requirements even more. This is at the base of the proposed UMCC architecture, which, benefiting from a joint distributed computing and communication infrastructure, can be implemented through the use of heterogeneous cloud computing and wireless networks.

UMCC FRAMEWORK

UMCC sprang from MCC, which has gained increasing interest in recent years due to the possibility of exploiting both cloud computing and mobile devices for enabling a distributed cloud infrastructure [2]: on one hand, the cloud computing idea has been introduced as a means for allowing remote computation, storage, and management of information, and on the other hand, mobility allows us to gain from the most modern smart devices and broadband connections to create a distributed and flexible virtual environment. At the same time, recent advances in wireless technologies are defining a novel pervasive scenario where several wireless HetNets

interact, giving users the ability to select the best radio access among those in a certain area. As a consequence, the development of UMCC is introduced, gaining from both computing and wireless communication technologies. In the following, the three pillars at the base of the proposed UMCC framework are discussed.

SMART MOBILE DEVICES

By analyzing the technology systems underlying a smart city framework, mobile devices can be considered in a three-fold way:

- *Sensors:* They can acquire different types of data regarding the users and the environment, transmitting a large amount of information to the cloud in real time by means of wireless communication systems.
- *Nodes:* They can form distributed mobile clouds where the neighboring mobile devices are merged for resource sharing, becoming an integral part of the network.
- *Outputs:* They can make the citizens aware of results and consequently able to make decisions, or become actuators without need of human intervention.

To perform this triple role, mobile devices must become part of an infrastructure that is constituted by different cloud topologies and, at the same time, have to exploit heterogeneous wireless link technologies, allowing the different requirements of a smart city scenario to be addressed. This infrastructure starts from the concept of MCC, where the cloud works as a powerful complement to resource-constrained mobile devices.

CLOUD TOPOLOGIES

In relation to the previously described SMD roles, we take into account various cloud topologies. This is a different categorization with respect to the classical as a service taxonomy used for cloud computing, that is, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). It looks at the different interactions among the nodes that form the cloud instead of the services provided by the cloud itself, so we can distinguish among centralized cloud, cloudlet, distributed mobile cloud, and a combination of them, as shown in Fig. 1.

Centralized Cloud: A centralized cloud provides citizens the ability to interact remotely, for

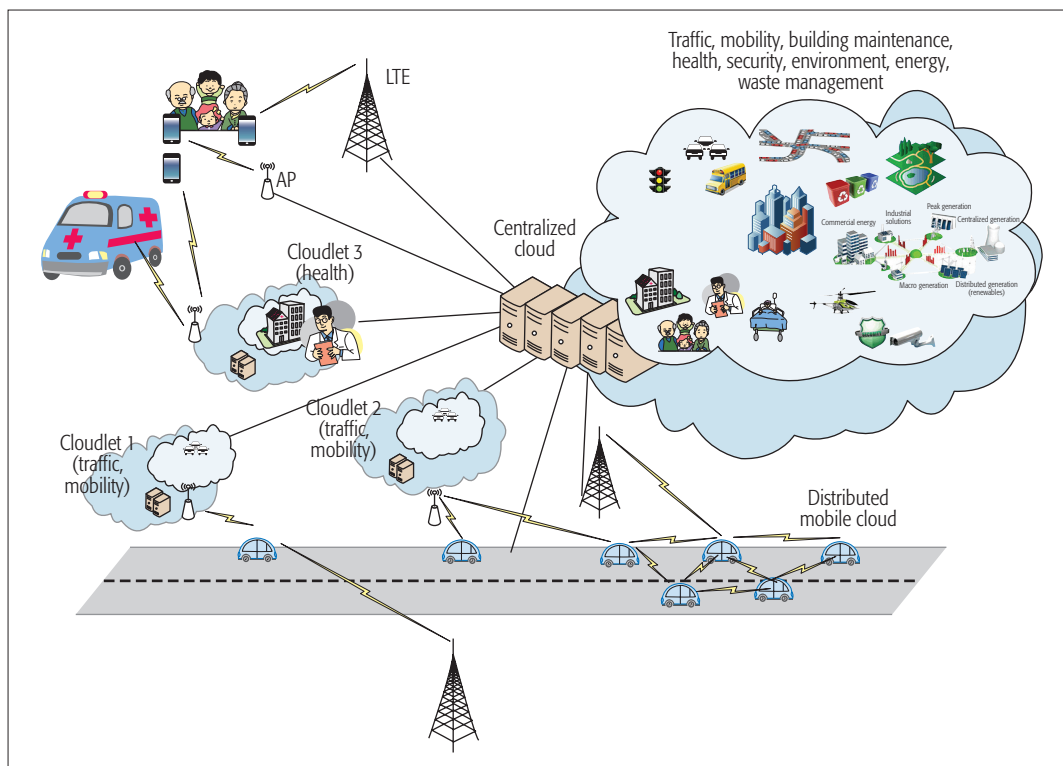


Figure 1. Cloud topologies in the UMCC framework: centralized cloud, cloudlet and distributed mobile cloud.

example, for accessing open data delivered by the public administrations. It refers to the presence of a remote cloud computing infrastructure having a huge amount of storage space and computing power, virtually infinite, offering the major advantage of elasticity of resource provisioning.

Cloudlet: Cloudlets are fixed small cloud infrastructures installed between mobile devices and the centralized cloud, limiting their exploitation to users in a specific area. Their introduction allows decrease in the latency of the access to cloud services by reducing the transfer distance at the cost of using smaller and less powerful cloud devices.

Distributed Mobile Cloud: A third configuration can address the issue of non-persistent connectivity, whereas both the previous concepts must assume a durable state of connection. In a distributed mobile cloud, the neighboring mobile devices are pooled together for resource sharing [12].

The proposed UMCC framework foresees the joint exploitation of the aforementioned topologies.

HETEROGENEOUS ACCESS TECHNOLOGIES

One of the most active trends in wireless networks is the presence of a heterogeneous access platform allowing several types of devices with multiple network interfaces to select from among them the most suitable. Such a forthcoming scenario, introducing a higher degree of pervasiveness, allows, especially in a smart city scenario, the enabling of access for a multitude of different devices, from high-end broadband user devices to narrowband M2M devices.

Such network deployment, comprising a mix of low-power nodes underlying the conventional homogeneous macrocell network, by deploying additional small cells within the local area range and bringing the network closer to users, can

significantly boost the overall network capacity through better spatial resource reuse. Inspired by the attractive features and potential advantages of HetNets, their development has gained much momentum in the wireless industry and research communities during the past few years toward fifth generation (5G) concepts.

TOWARD A UNIFIED OFFLOADING MECHANISM

The UMCC approach foresees the definition of a scenario where smart city applications can jointly exploit the three cloud topologies, as shown in Fig. 2, by distributing and performing among the different parts composing the framework, and wireless HetNet access technologies deployed in the urban area. The application requested by a specific SMD, named the requesting SMD (RSMD), is partitioned and distributed among the different clouds using the available access networks or computed locally (Fig. 2).

The main issue is that for transferring data from the requesting mobile device to the selected cloud topology, a certain time is required. This mostly depends on some communication parameters of the selected access network, such as the end-to-end throughput, the amount of users, and the QoS management of a certain transmission technology between the user device and each type of cloud processing unit. Moreover, the access networks themselves could already be used by SMDs belonging to the smart city scenario, as well as other devices using wireless infrastructures. This involves the necessity of designing a proper offloading method that, by modeling both computing and communication resources as a single unique resource, allows the computing/communication load to be distributed fairly among the different clouds and access networks.

Such network deployment, comprised of a mix of low-power nodes underlying the conventional homogeneous macrocell network, by deploying additional small cells within the local-area range and bringing the network closer to users, can significantly boost the overall network capacity through a better spatial resource reuse.

Whenever a smart city application has to be performed, a citizen within the UMCC can select among different MCC infrastructures, aiming to respect the requirements of the specific application depending on their features. The distribution depends on the application requirements and the UMCC features.

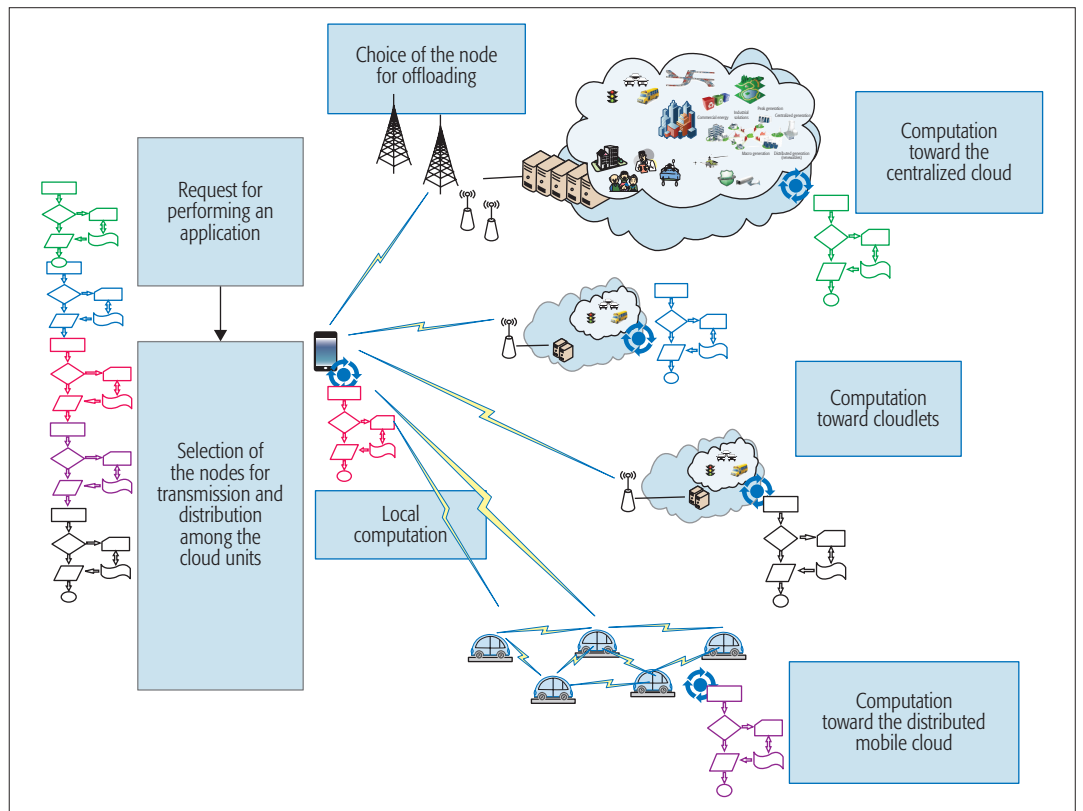


Figure 2. The process of distributing and performing the application among different parts of the UMCC.

Hence, when an RSMD needs to select the cloud infrastructures to be used for computing a smart city application, two main elements have to be taken into account:

- The processing and storage devices – smart mobiles, individually or together forming distributed mobile clouds, and cloud servers, constituting the cloudlets and the centralized cloud
- The wireless transmission equipment – different access networks entailing diverse transmission speeds in relation to their own channel capacity and to the number of linked devices

In Fig. 2, the UMCC framework is sketched by representing the functional flows of the architecture. Whenever a smart city application has to be performed, a citizen within the UMCC can select among different MCC infrastructures, aiming to respect the requirements of the specific application depending on their features. The distribution depends on the application requirements and the UMCC features.

Computation, storage, and transmission features: The features of the selected processing and storage devices, considered individually or in a group forming cloud/cloudlets, are:

- *Processing speed:* the speed of a device or a group of devices for processing the applications
- *Storage capacity:* the amount of storage space provided by a device or a group of devices

At the same time, the features of the transmission equipment to be taken into account are:

- *Channel capacity:* The nominal bandwidth of a certain communication technology that can be accessed by a certain device

- *Priority/QoS management:* The ability of a certain communication technology to manage different QoS and/or priority levels
- *Communication interfaces:* The number of communication interfaces of each device, which impacts the possibility of selecting among the available HetNets

UMCC OFFLOADING MODEL

Let us focus on one RSMD running an application, App , defined through the number of operations to be executed, O , the amount of data to be exchanged, D , and the amount of data to be stored, S . An application can be seen as a smart city service that can be executed either locally or remotely by exploiting the cloud infrastructures. Furthermore, each application has many requirements regarding QoS levels. Among others, the most important are:

- The maximum accepted latency, T_{App} , intended as the interval between when a task of the application is requested and its results are acquired
- The minimum level of energy consumption, E_{App} , that the RSMD needs to use for performing the application itself
- The throughput η_{App} , intended as the minimum bandwidth that the application takes to be performed

The first acting entity in the system is the RSMD, characterized by certain features that are involved in the offloading operation: the power to compute applications locally, P_l , the power used for transferring data toward clouds, P_{tr} , the power for idling during the computation in the cloud, P_{id} , the computing speed to locally perform the computation, f_l , and its storage availability, H_l . Further-

Entity	Connectivity	Storage	Throughput	Energy	Time latency
$App = App(O, D, S, T_{App}, E_{App}, h_{App})$	–	S	η_{App}	O, D, E_{App}	O, D, T_{App}
$Dev = Dev(P_i, P_{Tr}, P_{id}, f_i, H_i, pos_{dev}(x, y))$	$pos_{dev}(x, y)$	H_i	–	P_i, P_{Tr}, P_{id}, f_i	f_i
$C_{cc} = C_{cc}(f_{cc})$	–	–	–	f_{cc}	f_{cc}
$C_{cl} = C_{cl}(f_{cl}, H_{cl}, pos_{cl}(x, y), \eta_{cl}, n_{cl}, r_{cl})$	$pos_{cl}(x, y), n_{cl}, r_{cl}$	H_{cl}	η_{cl}	f_{cl}, η_{cl}	η_{cl}, f_{cl}
$MD = MD(f_{MD}, H_{MD}, pos_{MD}(x, y), \eta_{MD}, n_{MD}, r_{MD})$	$pos_{MD}(x, y), n_{MD}, r_{MD}$	H_{MD}	η_{MD}	f_{MD}, η_{MD}	η_{MD}, f_{MD}
$Nod = Nod(pos_{Nod}(x, y), \eta_{Nod}, n_{Nod}, r_{Nod})$	$pos_{Nod}(x, y), n_{Nod}, r_{Nod}$	–	η_{Nod}	η_{Nod}	η_{Nod}

Table 3. Summary of entities and relations in the UMCC -involved features and requirements.

more, the time-varying position of the device also plays an important role in the system interactions.

The different types of clouds considered in the Smart City are characterized by their computing speed to perform the computation, that is, f_{cc} for the centralized cloud and f_{cl} for cloudlets. Additionally, while the storage availability of the centralized cloud can be considered infinite, therefore not constraining in the interaction, the storage availability H_{cl} of each cloudlet has to be taken into consideration.

The distributed cloud is a set of SMDs, each characterized by its specific features in the same way as the RSMD, even if the role played by the SMDs is not a request for but a provision of service. Furthermore, we are considering the system from the point of view of the RSMD. Thus, the involved features are connectivity, computation, and storage for the data exchange, that is, the computing speed f_{MD} , the storage availability H_{MD} , the position $pos_{MD}(x, y)$, the throughput η_{MD} , the number of devices that can be connected to each SMD n_{MD} , and their coverage range r_{MD} .

While connection to cloudlets can be made only through the unique access point (AP) that can be considered built into each cloudlet, and the connection to the SMDs of the distributed cloud can be made directly, the nodes of the HetNet offer different alternatives to connect toward the centralized cloud. For each involved node, it is possible to define the position of the node $pos_{Nod}(x, y)$, the end-to-end throughput in bits per second between the user and the exploited node η_{Nod} , the number of devices available to connect n_{Nod} , and the range of availability of the node r_{Nod} .

Table 3 summarizes the entities and the characteristics described above. They are in a certain relationship due to some physical and logical bounds that are derived from the following considerations.

In order to distribute the computing and communication loads among the different elements, the system has to evaluate which HetNet nodes, cloudlets, and SMDs are available. On one hand, there are M available HetNet nodes Nod for communication offloading toward the centralized cloud, and N cloudlets C_{cl} and K SMDs able to offer computation offloading capabilities to the RSMD. On the other hand, the system has to distribute, by means of all these entities, different

percentages α_i of operations O , β_i of data D , and γ_i of memory S , to all the available nodes, cloudlets, and devices.

The requirements related to the applications, and the associated QoS, can be respected by optimizing the application partitioning and node/cloud association based on the features of the processing and storage devices and of the transmission devices introduced earlier; this corresponds to designing a unified offloading mechanism that, by taking into account both computing and communication resources and their relationships, as listed in Table 3, as a whole, can distribute the loads to the different devices of the environment.

In this context a utility function aiming to optimize the application-dependent QoS can be introduced, acting as input for the offloading procedure by selecting the best cloud and communication infrastructures, as shown in Fig. 3. The model constraints are derived from the observation that the sum of the offloaded fractions must be equal to 1; thus, the optimization problem becomes

$$\max_{\alpha_{Xi}, \beta_{Xi}} \left\{ \begin{array}{l} w_E f(E_{RSMD}(\alpha_{Xi}, \beta_{Xi})) \\ + w_T f(T_{RSMD}(\alpha_{Xi}, \beta_{Xi})) \\ + w_\eta f(\eta_{RSMD}(\alpha_{Xi}, \beta_{Xi})) \end{array} \right\} \quad (1a)$$

$$\text{s.t. } \alpha_0 + \sum_{i=1}^M \alpha_{HNi} + \sum_{i=1}^N \alpha_{CLi} + \sum_{i=1}^K \alpha_{MDi} = 1 \quad (1b)$$

$$\sum_{i=1}^M \beta_{HNi} + \sum_{i=1}^N \beta_{CLi} + \sum_{i=1}^K \beta_{MDi} = 1 \quad (1c)$$

The above equation corresponds to maximizing a utility function defined as a weighted sum of the functions related to the energy consumed, the time spent, and the throughput achieved by the RSMD, with constraints on the amount of operations and data to be shared among the different entities. By doing this, the system performs a unified offloading mechanism by jointly considering the communication and computing resources. In particular, the overall throughput can be evaluated as the sum of the throughput values η_{Xi} achievable through each node of the scenario. The throughput η_{Xi} is related to the number of SMDs η_{Xi} connected to the i th node and the channel capacity BW_{Xi} of the i th node, and can be

While the connection to the cloudlets can be made only through the unique access point (AP) that can be considered built-in in each cloudlet, and the connection to the SMDs of the distributed cloud can be made directly, the nodes of the HetNet offer different alternatives to connect towards the centralized cloud.

With respect to the latency, it can be evaluated as the sum of the local computing, the data transfer time toward and from the cloud/cloudlets, and the idle time during the offloaded computation. With respect to the consumed energy, it can be derived from the latency, as the weighted sum of each latency components by the power consumed in each state.

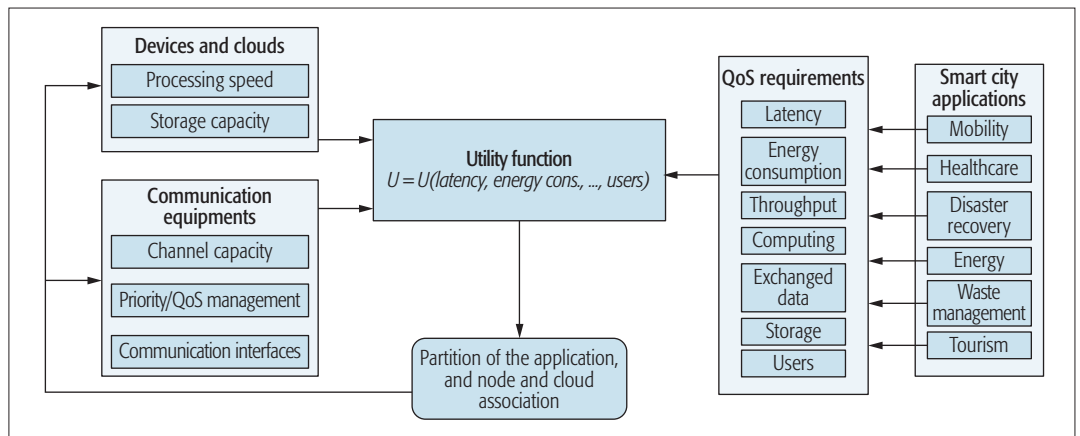


Figure 3. The utility function acts for distributing and performing the application in different parts of the urban MCC.

expressed by resorting to the Shannon Formula. With respect to the latency, it can be evaluated as the sum of the local computing, the data transfer time toward and from the cloud/cloudlets, and the idle time during the offloaded computation. With respect to the consumed energy, it can be derived from the latency as the weighted sum of each latency component by the power consumed in each state.

In Fig. 3, the functional blocks of the UMCC offloading mechanism, based on a utility function optimization, are represented. On one hand, the smart city applications define specific requirements, while the cloud topologies in a certain scenario set their features. The utility function aims to select those cloud topologies and access networks that allow to respect the requirements by setting an optimized distribution of the application itself. The optimization of the partition and the node association will impact again on the UMCC features to be used by the other applications.

The maximization of the introduced utility function could be a nontrivial optimization problem, depending on the considered number of applications and devices acting in the selected scenario. Toward this goal, different methods to find an optimal or sub-optimal solution of the objective function can be employed.

A Greedy Approach: If the offloading operation is advantageous with respect to the local computation, the cell association scheme allows the “best” node to be selected from the list of those available; such a list can be completed by each SMD that sorts each possible access node based on a self-calculated objective function [4]. If the offloading cost is lower than the cost of local computation, the SMD will connect to the node that minimizes the cost function; otherwise, it will locally compute the application.

A Cluster Based Approach: The idea is to divide the urban area in subareas having range r ; each SMD can share resources only with the other SMDs, cloudlets, and HetNet access points placed in the same subarea. This approach, even if suboptimal, can simplify the problem by reducing the amount of concurrent devices that are involved in the offloading; in [5] a cluster-based optimization model is proposed, where the cluster size plays a significant role in optimizing the problem while keeping the complexity low.

Biased Randomization: A different approach can be resorting to probabilistic algorithms based on biased randomization techniques [6]. In this problem setting, the most promising node concerning the potential increase in system efficiency has to be selected. The biased randomization techniques work by introducing a biased or oriented random effect on the possible solutions of a problem, allowing the best solution to be chosen from a set of possible alternatives that are close to the global optimal. In [6] a biased randomization algorithm is proposed, allowing us to approach the optimal solution by gaining from a heuristic algorithm, hence keeping the complexity low while approaching the optimal solution. In [6], it is also possible to note that such an approach is feasible from the implementation point of view, allowing a quasi-optimal solution in a reduced amount of time.

CONCLUSIONS

In this article we develop the UMCC framework, a concept that supports the smart city vision for the optimization of the QoS of various types of smart city applications. By exploiting the heterogeneous types of applications and devices typical of a smart city environment, and from the heterogeneous computing and communication infrastructure that composes the technological nervous system of the smart city, the proposed UMCC framework makes it possible to optimize the system performance, respecting the application requirements, by performing a suitable partial offloading mechanism. Based on the performance shown in specific applications, we can be optimistic about the practical effectiveness of UMCC.

ACKNOWLEDGMENT

This work has been partially supported by the project “GAUCHO – A Green Adaptive Fog Computing and Networking Architecture” funded by MIUR under PRIN Bando 2015.

REFERENCES

- [1] M. Dohler *et al.*, “Smart Cities,” Guest Editorial, *IEEE Commun. Mag.*, vol. 51, no. 6, June 2013, pp. 70–71.
- [2] H. T. Dinh *et al.*, “A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches,” *Wireless Commun. Mobile Computing*, vol. 13, no. 18, Dec. 2013, pp. 1587–1611.

- [3] F. Bonomi *et al.*, "Fog Computing: A Platform for Internet of Things and Analytics," *Big Data and Internet of Things: A Roadmap for Smart Environments*, ser. *Studies in Computational Intelligence*, N. Bessis and C. Dobre, Eds., Springer, 2014, vol. 546, pp. 169–86.
- [4] D. Mazza, D. Tarchi, and G. E. Corazza, "A User-Satisfaction Based Offloading Technique for Smart City Applications," *Proc. IEEE GLOBECOM 2014*, Austin, TX, Dec. 2014.
- [5] D. Mazza, D. Tarchi, and G. E. Corazza, "A Cluster Based Computation Offloading Technique for Mobile Cloud Computing in Smart Cities," *Proc. IEEE ICC 2016*, Kuala Lumpur, Malaysia, May 2016.
- [6] D. Mazza *et al.*, "Supporting Mobile Cloud Computing in Smart Cities via Randomized Algorithms," *IEEE Systems J.*, accepted for publication.
- [7] A. Aijaz, H. Aghvami, and M. Amani, "A Survey on Mobile Data Offloading: Technical and Business Perspectives," *IEEE Wireless Commun.*, vol. 20, no. 2, Apr. 2013, pp. 104–12.
- [8] X. Ma *et al.*, "When Mobile Terminals Meet the Cloud: Computation Offloading as the Bridge," *IEEE Network*, vol. 27, no. 5, Sept./Oct. 2013, pp. 28–33.
- [9] Y. Xu and A. Helal, "Scalable Cloud-Sensor Architecture for the Internet of Things," *IEEE Internet of Things J.*, vol. 3, no. 3, June 2016, pp. 285–98.
- [10] F. H. Bijarbooneh *et al.*, "Cloud-Assisted Data Fusion and Sensor Selection for Internet of Things," *IEEE Internet of Things J.*, vol. 3, no. 3, June 2016, pp. 257–68.
- [11] M. Jo *et al.*, "Device-to-Device-Based Heterogeneous Radio Access Network Architecture for Mobile Cloud Computing," *IEEE Wireless Commun.*, vol. 22, no. 3, June 2015, pp. 50–58.
- [12] D. Huang, T. Xing, and H. Wu, "Mobile Cloud Computing Service Models: A User-Centric Approach," *IEEE Network*, vol. 27, no. 5, Sept. 2013, pp. 6–11.
- [13] O. Vermesan and P. Friess, *Internet of Things – From Research and Innovation to Market Deployment*, River Publishers, 2014.
- [14] L. M. Correia and K. Wunstel, "Smart Cities Application and Requirements," white paper, Net!Works European Technology Platform, May 2011.
- [15] ETSI Std. TR 103 055, "Electromagnetic Compatibility and Radio Spectrum Matters (ERM); System Reference Document (SRdoc): Spectrum Requirements for Short Range Device, Metropolitan Mesh Machine Networks (M3N) and Smart Metering (SM) Applications," 2011.

BIOGRAPHIES

DANIELA MAZZA received her Master's degrees in electronic engineering and communication science and her Ph.D. degree in electronics, telecommunications, and information technologies engineering from the University of Bologna, Italy. She is an expert on system optimization in public administration organizational contexts at Emilia Romagna Local Government, Italy. Her research interests include services to citizens, including solutions for distributed multimedia systems and services management in the context of smart city. She possesses more than 15 years of

experience in local government organizations and has worked as a project manager for technological packaging businesses since 1991.

DANIELE TARCHI [S'99, M'05, SM'12] received his M.Sc. degree in telecommunications engineering and Ph.D. degree in informatics and telecommunications engineering from the University of Florence, Italy, in 2000 and 2004, respectively. He is currently an assistant professor at the University of Bologna. His research interests include the telecommunication area, with particular interests in resource allocation and link adaptation algorithms in wireless and satellite networks. He has been involved in several national projects as well as European projects, and has been active in several industry funded projects. He is an Editorial Board member for *IEEE Wireless Communications Letters* and *IEEE Transactions on Vehicular Technology*, and has been an Editorial Board member for *Wiley Wireless Communication and Mobile Computing*, *Hindawi Journal of Engineering*, and the *Scientific World Journal*, and has served as an Associate Editor for *IEEE Transactions on Wireless Communications*. He was Symposium Chair at IEEE Wireless Communications and Networking Conference 2011 and at IEEE GLOBECOM 2014, and Workshop Co-Chair at IEEE ICC 2015.

GIOVANNI EMANUELE CORAZZA [M'92, SM'07] is currently a full professor with the Alma Mater Studiorum, University of Bologna, a member of the Alma Mater Board of Directors, the founder of the Marconi Institute for Creativity (2011), a member of the Marconi Society Board of Directors, and a member of the Board of the 5G Infrastructure Association. In the years 2012–2016 he was a member of the Board of the 5G Infrastructure Association and the Vice-Chairman of the NetWorld2020 European Technology Platform. He was head of the Department of Electronics, Computer Science and Systems (DEIS) in 2009–2012, the chairman of the School for Telecommunications in 2000–2003, the chairman of the Advanced Satellite Mobile Systems Task Force (ASMS TF), and the founder and chairman of the Integral Satcom Initiative, a European technology platform devoted to satellite communications. He has authored or co-authored more than 260 papers. His research interests include wireless and satellite communications, mobile radio channel characterization, the Internet of Things, navigation and positioning, estimation and synchronization, spread spectrum and multicarrier transmission, and scientific creative thinking. He served as an Editor on Communication Theory and Spread Spectrum for *IEEE Transactions on Communications*, 1997–2012. He was the recipient of the Marconi International Fellowship Young Scientist Award in 1995, the IEEE 2009 Satellite Communications Distinguished Service Award, the 2013 Newcom Best Paper Award, the 2002 IEEE Vehicular Technology Society Best System Paper Award, the Best Paper Award of the IEEE International Symposium on Spread Spectrum Techniques and Application (ISSSTA) 1998, the IEEE International Conference on Telecommunication 2001, and the 2nd International Symposium on Wireless Communication Systems 2005. He was the General Chairman of IEEE ISSSTA 2008, ASMS 2004–2012 Conferences, and MIC Conference 2013.

The proposed UMCC framework makes it possible to optimize the system performance by respecting the application requirements by performing a suitable partial offloading mechanism. Based on the performance shown in specific applications, we can be optimistic about the practical effectiveness of UMCC.

Mobile Edge Computing Potential in Making Cities Smarter

Tarik Taleb, Sunny Dutta, Adlen Ksentini, Muddesar Iqbal, and Hannu Flinck

The authors propose an approach to enhance users' experience of video streaming in the context of smart cities. The proposed approach relies on the concept of MEC as a key factor in enhancing QoS. It sustains QoS by ensuring that applications/services follow the mobility of users, realizing the "Follow-me-Edge" concept.

ABSTRACT

This article proposes an approach to enhance users' experience of video streaming in the context of smart cities. The proposed approach relies on the concept of MEC as a key factor in enhancing QoS. It sustains QoS by ensuring that applications/services follow the mobility of users, realizing the "Follow Me Edge" concept. The proposed scheme enforces an autonomic creation of MEC services to allow anywhere anytime data access with optimum QoE and reduced latency. Considering its application in smart city scenarios, the proposed scheme represents an important solution for reducing core network traffic and ensuring ultra-short latency through a smart MEC architecture capable of achieving the 1 ms latency dream for the upcoming 5G mobile systems.

INTRODUCTION

Over the years, technology has served humanity by providing sustainable technical solutions to the social problems faced by society. In recent years, the research communities have been working on optimizing the technological infrastructure and maximizing the efficiency of services for citizens to meet their changing needs for smarter living. Society has evolved, and in the present era of smartphones, we have a new concept, the smart city," which is increasingly gaining in importance. Smart cities are expected to improve the quality of life for their citizens, leveraging advanced information and communications technologies (ICT). Smart cities are also expected to provide their citizens with a variety of innovative services, ranging from education and healthcare to augmented and immersive reality; for example, for the support of tourism. Indeed, deployed services in smart cities will involve not only smartphones and tablets, but also utility meters, washing machines, thermostats, refrigerators, sensors for environmental monitoring, and so on; in short, the different components of the Internet of Things (IoT) ecosystem.

The next generation mobile systems, commercially known as fifth generation (5G), aims to accelerate the development of smart cities, by not only increasing the data delivery rates but also accommodating the expected high numbers of IoT devices to be used by smart city services and applications [1, 2]. Besides, thanks to its elasticity and agility, 5G will be able to support numerous smart services, which cannot be supported by cur-

rent network architectures [3, 4]. This includes immersive reality and tactical applications, and services with highly strict requirements in terms of ultra-short latency and high responsiveness.

5G systems will rely on technologies such as Network Function Virtualization (NFV), Software Defined Networking (SDN), and cloud computing to attain system's flexibility and true elasticity [1, 4]. Among these technologies, cloud computing has tremendously advanced enabling diverse services. However, it remains limited against emerging applications (e.g., tactile Internet and augmented reality) that require ultra-short latency. Cloud is also limited against computation-intensive applications running on power/CPU-constrained user equipment (e.g., mobile gaming) that need to partially run their computation in the cloud while ensuring response times (i.e., for other parts of the code running on the user equipment) in the range of milliseconds. These limitations are principally due to the centralized cloud computing architecture. Mobile edge computing (MEC), interchangeably known as fog computing (originating from the cloudlet concept [5]), represents a vital solution to these limitations. Indeed, it reforms the cloud hierarchy by pushing computing resources in the proximity of mobile users (i.e., at the mobile network edge). There are high expectations for MEC and 5G, when efficiently integrated, to improve the quality of life of residents in smart cities. This underpins the focus of this article, wherein we show how MEC will enable emerging services for smart cities, focusing on an augmented reality use case involving streaming of high definition (HD) video, which is for the support of tourism in smart cities. The overall objective is to demonstrate how high quality of service (QoS) can be maintained regardless of the mobility of users through the use of MEC, more particularly through the concept of Follow Me Edge (FME — similar in spirit to the Follow Me Cloud concept [1, 6]). FME ensures that the service constantly follows the user and that the user is always serviced from the closest edge. As discussed later, the fundamental observations made about the envisioned use case are highly applicable to other services requiring ultra-short latency, such as immersive reality and tactical applications.

The remainder of this article is organized as follows. The following section presents the state of the art. Then we describe our proposed FME framework along with the supporting mecha-

nisms. For the sake of performance evaluation, in the next section we portray the experimental setup and discuss the obtained results. The article concludes in the final section with a summary recapping the main findings.

STATE OF THE ART

The key idea beneath MEC is to place storage and computation resources at the network edge, in the proximity of users. Accordingly, data processing can be pushed from far remote cloud to the edge. By processing data locally and accelerating data streams through various techniques (i.e., caching and compression), MEC reduces the traffic bottleneck toward the core network. Besides, it helps shorten end-to-end latency, enabling the offload of important computation load from power-constrained user equipment to the edge. As discussed in the executive briefing of the European Telecommunications Standards Institute (ETSI) MEC initiative,¹ edge computing shall enable new computation-intensive services and shall yield promising business models. It also represents a fault resilient solution for its decentralized architecture [7].

Given its potential, MEC has been gaining lots of momentum among industries and within the researcher community [8]. Important standardization activities have been initiated. Indeed, to standardize the specifications of MEC across mobile operators and vendors in the value chain, ETSI formed a new ISG group in 2014 and came up with different industry specifications.² The specifications highlight the different service scenarios whereby MEC can be beneficial. For video streaming services, it was recommended to apply intelligent video acceleration schemes using video analytics and video management applications within MEC. The research work in [9] proposes a two-hop network whereby edge architecture enhances data transfer rate and throughput for video streaming compared to remote cloud. The work in [10] exploits network assisted adaptive streaming applications for multimedia content delivery inside MEC to enhance Quality of Experience (QoE). The research study in [11] proposes an architecture with distributed parallel edges to increase QoE for content delivery. The research work in [12] makes use of edges as caches along with proxies to store media content. It also enforces computation offloading to increase the lifetime of mobile devices. In [7], edges function independently as small-scale data centers on their own and are used for video caching and streaming.

In all the above research work, MEC is deemed to be a promising solution for handling video services. Its limitations in terms of resource control and orchestration have also been highlighted as important challenges. In smart city scenarios, users' mobility and the need for dynamic service migration add to these challenges. Most research works on the latter consider traditional cloud environments [1, 6]. In [13], migration of edges has been proposed using a Markov decision process approach to determine optimal solutions for service placement.

To the best of the authors' knowledge, mobility support and migration of service in terms of video content delivery have not been considered yet. In the remainder of this article, we describe and showcase an innovative deployment scenario on how

a user's experience on video streaming can be enriched using MEC in spite of the user's mobility.

FOLLOW ME EDGE

USE CASES

To support tourism in smart cities, many use cases, involving video streaming from the edge, could be considered. In the following, we consider two representative use cases, one implying edge migration:

Use Case 1: Robert from England visits Helsinki for the first time. He visits the white church, likes it, takes a video of it, comments on it in his native language (i.e., English), and streams it to an edge placed near the white church. Some time later, Eric, also from England and a member of Robert's social network (e.g., Facebook), visits the same church and receives an invitation to view Robert's generated video and hear what Robert said about the location. Eric may further comment on the video, indicating whether he liked it, or post a new video about the location. In this use case, videos about a certain attractive location are cached at edges in the vicinity of that location and streamed to people visiting that location when there is interest or when there is linkage with the video publisher. Mapping the most popular videos with Google Streetview may also be considered. The video streaming as well as the relevant operations (comment, like/dislike, etc.) take place at the corresponding edges near the visited sites.

Use Case 2: Robert visits the city of Hamburg. To explore the city, he takes a sightseeing bus. He uses interactive glasses that recognize historical monuments (e.g., tourist attractions) and accordingly receives introductory video about these monuments in the format of high definition (HD) video. The video can be streamed from either a remote cloud or the edge. As the path to the remote cloud involves multiple hops, some being nearly congested, high resolutions of the video cannot be guaranteed unless it is streamed from the edge. Furthermore, to prevent jitter and the associated degradation in QoE, the video must always be streamed from the nearest edge to Robert. In this use case, Robert's user equipment receives a portion of the video from the nearest edge A. As the bus gets far away from edge A and closer to edge B, the video along with the streaming virtual network function are migrated to edge B, and the remaining portion of the video streams to Robert from edge B. This edge migration occurs in a manner transparent to Robert, who continues enjoying the video without any disruption in the video stream and with no degradation in the perceived QoE.

While the above use cases focus on video streaming services, similar use cases with the same requirements can be derived for augmented reality services. In this work, we consider using lightweight virtualization technologies (i.e., container), and introduce container migration to meet the above mentioned use cases, with more focus on the edge mobility aspect of use case 2.

FME ARCHITECTURE

The proposed architecture is based on the two-tier principle, wherein the cloud service provider (CSP) gives access, through an appropriate application programming interface (API) [14], to a content provider or a third party over-the-top (OTT) service

The key idea behind MEC is to place storage and computation resources at the network edge, in the proximity of users. Accordingly, data processing can be pushed from a far remote cloud to the edge. By processing data locally and accelerating data streams through various techniques, MEC reduces the traffic bottleneck toward the core network.

¹ https://portal.etsi.org/portals/0/tbpages/mec/docs/mec_executive_brief_v1_28-09-14.pdf

https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1_18-09-14.pdf

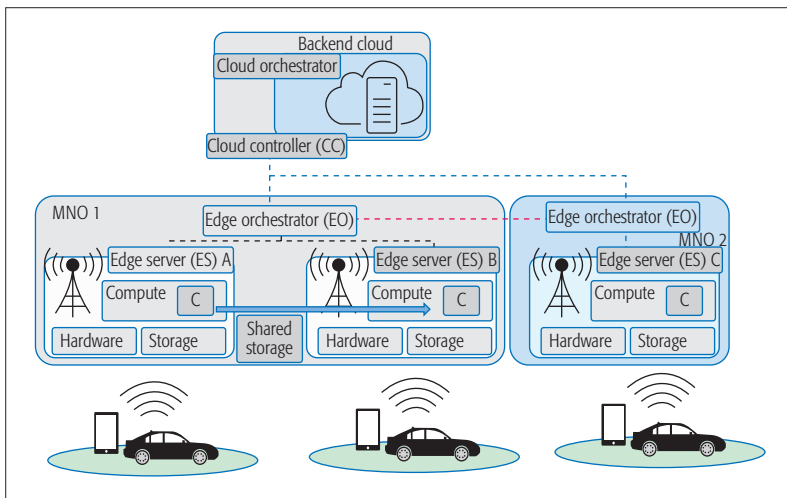


Figure 1. The envisioned mobile edge computing architecture.

to use the cloud resource to deploy its application. The cloud has its own orchestrator to manage the cloud infrastructure and its resources. An additional component is considered: the cloud controller (CC). Considering the business functionality, CC is involved in maintaining the service level agreement (SLA) with the OTT providers and mobile network operators (MNOs). The agreement deals with access rights and policies on the entity's authority. The edge server (ES) belongs to the MNO's network, where it is managed and controlled by the edge orchestrator (EO). Every MNO has its own EO, managing its own set of ES clusters. Figure 1 depicts inter/intra-MNO edge network. The dotted lines represent the agreement level connection among CSP, MNO, EO, and ES.

The ES is hosted on virtual machines on top of the existing server hardware residing in the MNO's edge network node. The ES has its own compute and storage. The compute node is responsible for hosting container-based applications on the edge. The storage is used to keep images of the application containers. For an intra-edge network, additional shared storage is needed to ensure live migration of containers between edge compute nodes. Linux-based containers (LCs) can be employed to make the system lightweight and help in easily deploying service packages. LCs run applications/services provided from the edge, while EO is in charge of deploying, controlling, and migrating containers.

Referring to use case 2, when Robert connects to ES A to watch an HD video introducing Hamburg, he may initially be served from the backend cloud. As stated earlier, this may incur jitter and may limit the video resolution. To cope with this issue, the EO may instantiate a container on the connected ES compute node with built-in streaming and transcoding virtualized functionality [14, 15]. Subsequently, it may store the relative content from the backend cloud into the ES's local storage. Robert will then be served the HD version of the video stream from the ES. Considering the case of HTTP-based video streaming, the EO can fetch the entire media content on one go or may fetch only a certain number of video chunks at a time. Consequently, as the content will be served from one hop away, the user's perceived quality is expected to greatly improve. For applications involving OTT services,

the established SLA may help in performing this task with a pre-agreed negotiation between the OTT provider and the MNO. In this case, the EO inside the MNO will get access rights from the OTT service at the beginning of the process. The EO will then create the replica and bring the service to the edge.

Although the content is now served from the nearest edge, after some time the connection with the mobile user may begin experiencing degradation as the length of the path to the served MEC increases. To maintain the same quality, it is vital that the content moves along the physical mobility of users in an FME fashion [6]. To realize the FME vision, the EO needs to keep updated information about its resources and the user locations. The latter may be obtained using the MEC's active device location tracking functionality, based on which a user's velocity and direction may be derived. Taking this into consideration, the EO may estimate the latency between the user and the current edge, and compare it with the latency between the same user and the target edge. Once deemed appropriate, the EO may trigger live migration of the container in a proactive manner. This will consist of migrating the video streaming service along with its contents. Upon successful container migration, the user may then be served from the new ES, which will ensure low latency access to the content. The above described migration process will be repeated along the track whenever required.

Migration can happen using various techniques. In the case of live video streaming, service continuity and bare minimum disruption are of prime concern. To perform seamless live migration, the service state has to be maintained in order to ensure that no data is lost. This is achieved by transferring the entire memory content of the running instance (i.e., container) from the source ES to the target ES. The source ES keeps track of which memory blocks are modified while the transfer is in progress. Once this initial transfer is complete, the changes that have occurred in the meantime are transferred again. This continues until the newly built instance becomes exactly identical to the old one. This ensures that after the migration process is complete, the video starts from the exact point rather than overlapping. Indeed, in the case of mishandled memory, data loss happens. This incurs overlap in video play-time, where the user may have to watch the same content again (from the span when the migration started). Moreover, the migration duration should not be too long. If the duration is too long, it might be that by the end of the migration either the user has moved away from the ES location or the played video is almost over. To overcome these constraints, separate shared storage has to be considered. Normally migration takes place by copying memory blocks. Thus, if the blocks are dumped at a shared location attached to the new ES, service transfer becomes faster than in the case considering local storage. Although async mode configuration of shared storage is even faster than sync mode, we propose the use of sync mode to maintain data integrity. In sync mode the data saved in the storage location is confirmed before processing the next request from the ES. In async mode, the requests are processed without proper confirmation. It yields better response time

but at the cost of possible data corruption, which may introduce a glitch in the played video.

So far, the proposed scheme deals with latency reduction and mobility within the network of the same MNO/edge. If the user moves out of the network of an edge provider to the edge of another provider, the SLA shall be used. The SLA should enforce an integrated architecture where the EO handover, shared storage concept, and service migration are considered. In this case, the source EO may hand over the control to the target EO (in a separate MNO's network) and permit service migration. If it is not possible, then during the MNO crossover phase, the content will be served from the back-end cloud temporarily until the new EO again caches the service in its own compute node.

It is worth noting that smart caching and migration can considerably enhance the overall system performance and reduce the migration cost [16]. The caching concept can be enhanced further by considering the remaining duration of the content. If there is no possibility to store the whole content (due to storage space), only the next few chunks of the remaining video may be cached. Moreover, if the video is almost at the end (i.e., the remaining play time less than the migration time), the container/service migration may be simply omitted.

PERFORMANCE EVALUATION

Figure 2 portrays the testbed environment we have built to simulate edge-based video streaming and its mobility considering use case 2. The testbed is built using one Ubuntu 14.04.3 LTS desktop and two laptops with the same host operating system. Virtualbox is used to implement the testbed on a desktop workstation machine. The desktop machine hosts three virtual machines (VMs) inside the virtual box environment. VM1 is used as a gateway for the entire network to access the Internet. VM2 is used to simulate the cloud environment deploying a Devstack-based cloud, which provides all-in-one (i.e., controller, compute, network, and storage on the same node) with an Ubuntu instance running inside it. The Ubuntu cloud instance hosts an HTTP live streaming (HLS) server. The ffmpeg open source server, for both streaming and transcoding, are built in separate VMs. The media contents (HLS fragments) are generated using ffmpeg transcoding servers, and are then streamed using an ffmpeg streaming server (hosted in a separate VM). The floating IP address of the instance was chosen from the same IP subnet range of the edge cluster, so the ES can access the data from the cloud VM. The CC function was omitted, as the SLA level implementation was not considered in the testbed. VM3 was configured using Proxmox VE and acts as edge cluster controller — EO. VM3 also includes a DHCP server with authentication. To automate the orchestration process, a script is used to:

- Monitor the session changeover of the clients from one edge to the other using the authentication server logs
- Handle the container migration

The entire cluster of edges is formed by integrating two additional VMs (i.e., VM4 and VM5) with the EO. VM4 and VM5 are hosted inside laptops to emulate ESs. The connectivity between the VMs is extended using an Ethernet switch. VM4 and VM5 use the same virtual environment as the EO. To ensure that the laptops (VM4 and VM5)

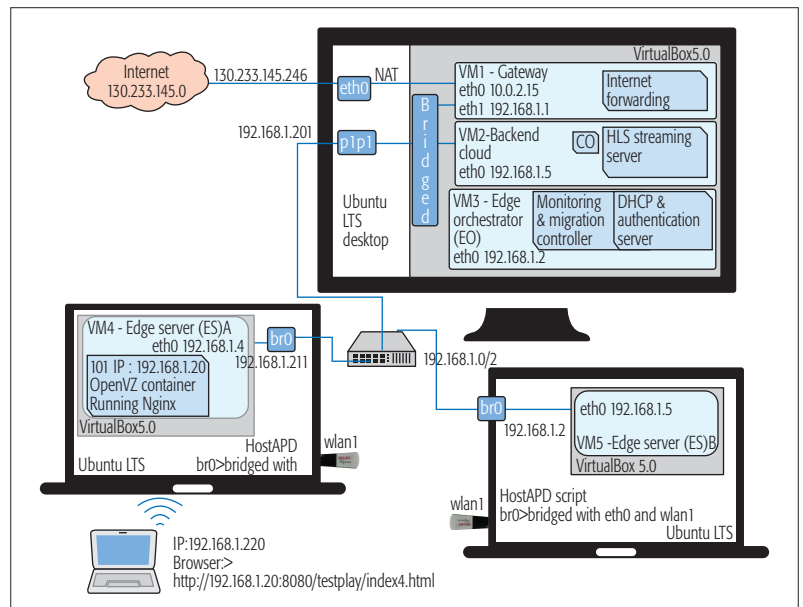


Figure 2. Envisioned testbed setup.

act as edge access points, the wireless LAN interface was configured using Host-apd in IEEE 802.11 master mode. The container is created inside VM4. We use Openvz containers for the testbed. The containers are built with Ubuntu cloud minimal image using Nginx as the web server. Nginx is configured to serve as reverse proxy to the back-end cloud HLS server with caching and streaming functionality. It is worth recalling that the objective of these tests is to validate the use of MEC to ensure high-quality HD video streaming service to mobile users. Therefore, the focus of these tests is on caching content and live delivery of the multimedia content closer to the user at the edge.

To perform the test, one container is instantiated in Edge1 with all the features explained above. When a user (using a smartphone or laptop) connects to the network through SSID, the user is assigned an IP from the same IP subnet pool of the ES. The user connectivity log along with the MACID of the user are saved in a database of the EO. The user launches a browser and starts browsing the video, using the URL of the streaming sever hosted at the container. To implement minimum security, the user is given authorization to only browse data from the container. Upon connecting for the first time, the container forwards the request to the cloud VM, and the multimedia content is served from the back-end cloud. Simultaneously, it caches the relevant media contents and stores them for further use to the container. For the next requests to the same video, the container makes use of its own streaming functionality to serve the user by using cached contents regardless of the fact that the cloud is accessible or not. Accordingly, this implements the concept of bringing the content closer to the user and making the backend core free from the traffic.

To simulate mobility, laptops are placed at a distance from a multihop network. During the video playback, the user device is deliberately moved from the first edge toward the second edge connected to the next hop in the network. The user automatically connects to Edge2. As soon as the wireless connectivity handover takes place, the logs are generated inside the EO. Upon

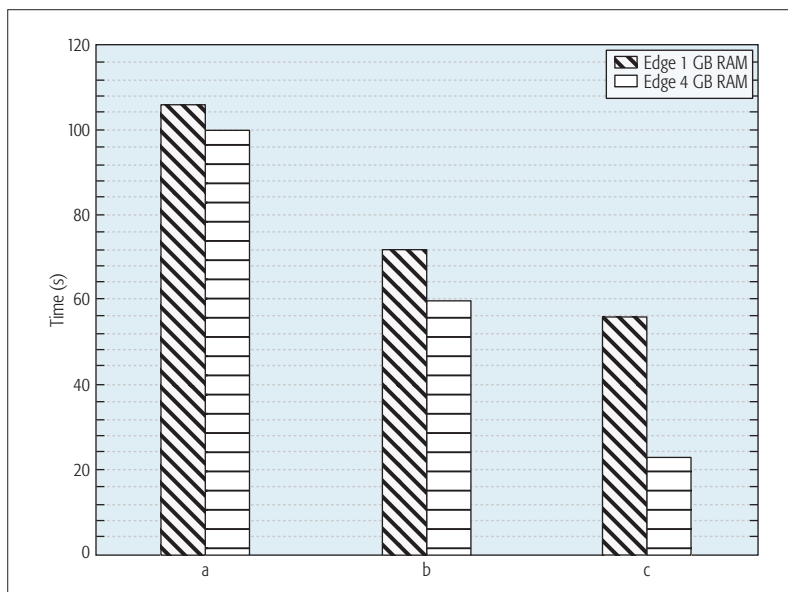


Figure 3. Live migration time using local storage: a) with streaming online mode; b) without streaming offline mode; c) blank container.

detecting the client's connectivity, the script in charge of automating the service migration gathers the client info (i.e., MACID), compares it to the database, identifies the same client's movement to a new edge, and subsequently triggers the live migration of the container from the old ES to the next one to which the client is directly connected. For Openvz, the live content delivery is done using checkpoint/restore in userspace (CRIU). It performs `vz-dump` (memory block dump) to save the state and uses `rsync` (i.e., incremental file transfer utility) to transfer the file to the target location. It performs a dual-level operation to prevent data loss. First, pre-copy starts from the point at which the migration is initiated. Once completed, the container initialization is started in the new edge along with post-copy. Herein, post-copy represents transfer of the residual amount of changes that occurred in the memory block during this small interval. As service auto-start is already enabled, once this data transfer operation is done, the container is automatically started in the target edge, and the old one is released. The user remains unaware of this fact and enjoys normal streaming. Throughout the migration time, the container IP address remains the same, ensuring no service downtime (i.e., the session remains active) during this span.

For service migration, the test is performed with two types of storage. In the first type, the whole operation is performed using local storage (i.e., service migration within a federated edge network). The `vz-dump` files are first copied to the local storage, then synced with the target ES node, the container is initialized in that target node, and after post-copy the migration is completed. However, this method causes high delays. To achieve better performance with minimum response, the second type is implemented. A network file system (NFS) server is used as shared storage for the operation. The NFS server is installed inside the EO, and the shared space is defined for the cluster nodes. The shared storage is used only for `vz-dump` files. During migra-

tion, the copied memory files are stored in the shared location. As the target node can access the shared location directly, it reduces the content delivery to the edge, resulting in faster response.

In Fig. 3, we plot the migration duration of one container for three different conditions:

- With streaming online mode — streaming in use and the client watching the video
- Without streaming offline mode — streaming in use and the client is not watching the video with no changes in the memory blocks
- Blank container with two different types of ES

The migration latency is plotted considering local storage. The migration latency of a blank container is plotted to showcase how much added services impact the migration time. From the results, we can observe that when video streaming is not active, the content migration takes less time compared to the case when the video is being streamed. Moreover, for an ES with higher RAM capacity, the migration duration is shorter. This is attributable to the fact that copying memory pages takes less time with higher RAM, leading to a slight decrease in the overall duration.

Figure 4 plots the migration duration when considering various ways to share the storage among edges. The test is performed with two different sizes of containers, one small and another big, to investigate if container size affects migration duration. We clearly remark that the container size merely affects the migration latency. Besides, we observe that shared-sync mode achieves shorter latency in comparison to local mode. Furthermore, the shared storage, if configured in shared-async mode, reduces the duration of the migration closer to 10 s. In this last mode, the video experienced a single glitch of 1~2 s. We explain this by the fact that data corruption took place during async mode, resulting in reduced quality of experience (QoE) [17]. The results obtained through this evaluation reveal that the storage type and memory capacity have high impact on the migration latency.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this article, we propose a framework that leverages MEC to support diverse applications in smart city scenarios. To always ensure high QoE, the Follow Me Edge concept is introduced. According to this concept, services move across edge servers as per the movement of their respective users. The proposed framework is validated using a real-life testbed. Edge mobility was tested using different storage types, different container sizes, and different edge resources.

Interesting results were obtained, suggesting migration latency depends on the different techniques used. The obtained results also demonstrate that short migration latency does not necessarily guarantee high QoE. It becomes apparent that the complexity of the system arises as a trade-off between short migration latency at the cost of possible data loss. Based on the obtained results, it can be concluded that a mechanism to select the right combination of techniques to be used for efficiently migrating a service is of vital importance. This defines one of the authors' future research directions in this area.

ACKNOWLEDGMENTS

This work was partially supported by the TAKE 5 project funded by the Finnish Funding Agency for Technology and Innovation (TEKES) and in part by the Finnish Ministry of Employment and the Economy. It is also partially supported by the European Union's Horizon 2020 research and innovation programme under the 5G!Pagoda project with grant agreement no. 723172.

REFERENCES

- [1] T. Taleb, A. Ksentini, and A. Kobbane, "Lightweight Mobile Core Networks for Machine Type Communications," *IEEE Access*, vol. 2, Oct. 2014, pp. 1128–37.
- [2] T. Taleb and A. Kunz, "Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions," *IEEE Commun. Mag.*, vol. 50, no. 3, Mar. 2012.
- [3] T. Taleb et al., "EASE: EPC as a Service to Ease Mobile Core Network," *IEEE Network*, vol. 29, no. 2, Mar. 2015, pp. 78–88.
- [4] T. Taleb, "Toward Carrier Cloud: Potential, Challenges, and Solutions," *IEEE Wireless Commun.*, vol. 21, no. 3, June 2014, pp. 80–91.
- [5] U. Shaukat et al., "Cloudlet Deployment in Local Wireless Area Networks, Motivation, Taxonomies, and Open Research Challenges," *J. Network Computer Applications*, vol. 62, Feb. 2016, pp. 18–40.
- [6] A. Ksentini, T. Taleb, and F. Messaoudi, "A LISP-Based Implementation of Follow Me Cloud," *IEEE Access*, vol. 2, Oct. 2014, pp. 1340–47.
- [7] H. Chang et al., "Bringing the Cloud to the Edge," *Proc. IEEE INFOCOM Wksp.*, Toronto, Ontario, Canada, May 2014.
- [8] A. Ahmed and E. Ahmed, "A Survey on Mobile Edge Computing," *Proc. IEEE 10th Int'l. Conf. Intelligent Systems Control*, India, May 2016.
- [9] D. Fesehaye et al., "Impact of Cloudlets on Interactive Mobile Cloud Applications," *Proc. IEEE 16th Int'l. Conf. Enterprise Distributed Object Computing*, Beijing, China, Sept. 2012.
- [10] J. Fajardo, I. Taboada, and F. Liberal, "Improving Content Delivery Efficiency through Multi-Layer Mobile Edge Adaptation," *IEEE Network*, vol. 29, no. 6, Dec. 2015, pp. 40–46.
- [11] W. Zhu et al., "Multimedia Cloud Computing," *IEEE Signal Processing Mag.*, vol. 28, no. 3, May 2011, pp. 59–69.
- [12] Y. Jararweh et al., "Resource Efficient Mobile Computing Using Cloudlet Infrastructure," *Proc. IEEE 9th Int'l. Conf. Mobile Ad Hoc Sensor Networks*, Dalian, China, Dec. 2013.
- [13] S. Wang et al., "Dynamic Service Migration in Mobile Edge Clouds," *Proc. IFIP Networking Conf.*, Toulouse, France, May 2015.
- [14] P. Frangoudis et al., "An Architecture for On-Demand Service Deployment over a Telco CDN," *IEEE ICC '16*, Kuala Lumpur, Malaysia, May 2016.
- [15] T. Taleb, A. Ksentini, and R. Jantti, "Anything as a Service for 5G Mobile Systems," *IEEE Network*, vol. 30, no. 6, Dec. 2016, pp. 84–91.
- [16] T. Taleb and A. Ksentini, "An Analytical Model for Follow Me Cloud," *Proc. IEEE GLOBECOM*, Atlanta, GA, Dec. 2013.
- [17] S. Dutta, T. Taleb, and A. Ksentini, "QoE-Aware Elasticity Support in Cloud-Native 5G Systems," *Proc. IEEE ICC '16*, Kuala Lumpur, Malaysia, May 2016.

BIOGRAPHIES

TARIK TALEB is currently a professor at the School of Electrical Engineering, Aalto University, Finland. He has worked as senior researcher and 3GPP standards expert at NEC Europe Ltd. Prior to his work at NEC, until March 2009, he worked as an assistant professor at the Graduate School of Information Sciences, Tohoku University, Japan, in a lab fully funded by KDDI. He received his B.E. degree in information engineering with distinction, and his M.Sc. and Ph.D. degrees in information sciences from Tohoku University in 2001, 2003, and 2005, respectively. His research interests lie in the field of architectural enhancements to mobile core networks (particularly 3GPP's), mobile cloud networking, mobile multimedia streaming, and social media networking. He has also been directly engaged in the development and standardization of the Evolved Packet System. He is a member of the IEEE Communications Society Standardization Program Development Board and serves as Steering Committee Chair of the IEEE Conference on Standards for Communications and Networking. He has received many awards for his many contributions to the area of mobile networking.

SUNNY DUTTA obtained his M.Sc. and Bachelor's degree from the School of Electrical Engineering, Aalto University, Finland, and the West Bengal University of Technology, India, in 2016 and 2006, respectively. Prior to his Master's studies, he worked

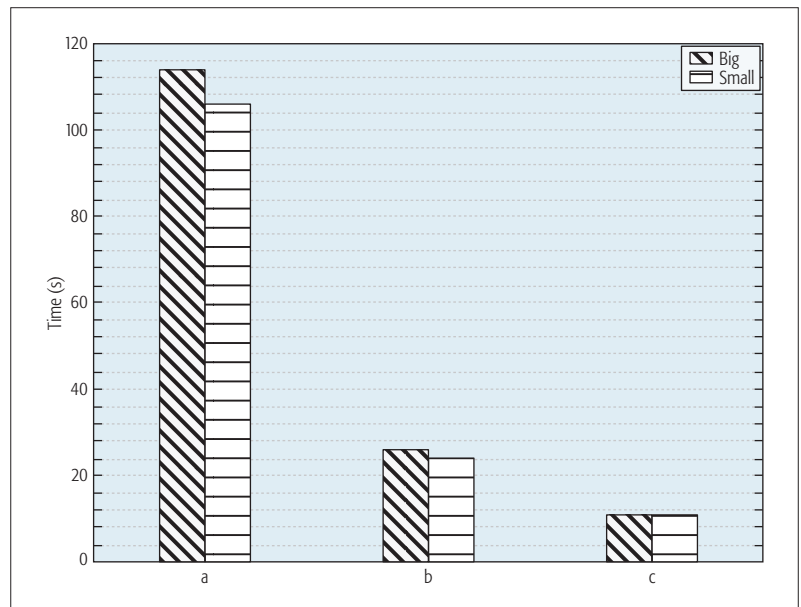


Figure 4. Live migration latency: a) local storage; b) shared sync storage; c) shared async storage.

as an engineer assuming different roles in network administration, energy automation, and smart grid communication network infrastructure. His present research focus includes MEC, NFV, SDN, and multimedia content delivery.

ADLEN KSENTINI received his M.Sc. degree in telecommunication and multimedia networking from the University of Versailles Saint-Quentin-en-Yvelines, and his Ph.D. degree in computer science from the University of Cergy-Pontoise in 2005, with a dissertation on QoS provisioning in IEEE 802.11-based networks. From 2006 to 2015, he worked at the University of Rennes 1 as an assistant professor. During this period, he was a member of the Dionysos Team with INRIA, Rennes. Since March 2016, he has been working as an assistant professor in the Communication Systems Department of EURECOM. He has been involved in several national and European projects on QoS and QoE support in future wireless, network virtualization, cloud networking, and mobile networks. He has co-authored over 100 technical journal and international conference papers. He received the best paper award from IEEE IWCMC 2016, IEEE ICC 2012, and ACM MSWiM 2005. He has been acting as TPC Symposium Chair for IEEE ICC 2016 and 2017 and IEEE GLOBECOM 2017. He was a Guest Editor of *IEEE Wireless Communications*, *IEEE Communications Magazine*, and two issues of *ComSoc MMTC Letters*. He has been on the Technical Program Committees of major IEEE Com-Soc, ICC/GLOBECOM, ICME, WCNC, and PIMRC conferences.

MUDDESAR IQBAL is working as a senior lecturer in mobile computing at the Computer Science and Informatics Division, School of Engineering, London South Bank University. He has been a principal investigator, co-investigator, technical lead, project manager, coordinator, and focal person of more than 10 internationally teamed R&D and capacity building training projects with total funding of over £1 million from different international organizations. He has co-founded and successfully launched a startup called SwanMesh Networks Ltd that was initially established in the United Kingdom to commercialize his Ph.D. project and now has over six years of design and development experience. Over the last few years, he has been actively involved in R&D projects in the area of mobile cloud computing and other open source networking technologies for applications in healthcare, disaster management, and community networks. He has won two awards from the Association of Business Executives UK while tutoring on computing modules.

HANNU FLINCK is a research manager at Nokia Bell Labs Espoo, Finland. Before that he worked with Nokia Research Center and the Technology and Innovation unit of Nokia Networks in various positions. He has been actively participating in a number of EU research projects. He received his M.Sc. degree (1986) and Lic.Tech. degree (1993) in computer science and communication systems from Aalto University (at that time known as Helsinki University of Technology). His current research interests include mobile edge computing, SDN, and content delivery in mobile networks, particularly in 5G networks.

5G Converged Cell-Less Communications in Smart Cities

Tao Han, Xiaohu Ge, Lijun Wang, Kyung Sup Kwak, Yujie Han, and Xiong Liu

Ubiquitous information service converged by different types of heterogeneous networks is one of the fundamental functions for smart cities. Considering the deployment of 5G ultra-dense wireless networks, 5G converged cell-less communication networks are proposed to support mobile terminals in smart cities.

ABSTRACT

Ubiquitous information service converged by different types of heterogeneous networks is one of fundamental functions for smart cities. Considering the deployment of 5G ultra-dense wireless networks, 5G converged cell-less communication networks are proposed to support mobile terminals in smart cities. To break obstacles of heterogeneous wireless networks, the 5G converged cell-less communication network is vertically converged in different tiers of heterogeneous wireless networks and horizontally converged in celled architectures of base stations/access points. Moreover, the software defined network controllers are configured to manage the traffic scheduling and resource allocation in 5G converged cell-less communication networks. Simulation results indicate the coverage probability and the energy saving at both base stations and mobile terminals are improved by the cooperative grouping scheme in 5G converged cell-less communication networks.

INTRODUCTION

Smart cities are the evolution trends of future cities, which involve many aspects of daily life in cities, including e-businesses, intelligent transportation systems, telemedicine, metropolis management, security surveillance, logistics management, social networks, community services, and so on. To brace for the above services, smart cities have been employing various wireless communication technologies and networks, including Bluetooth, ZigBee, RF identification (RFID) wireless technologies, wireless cellular networks, wireless local area networks (WLANs), radio broadcasting networks, wireless sensor networks, body area networks, and many others [1]. These wireless communication technologies along with fiber communication networks and cable networks form the ubiquitous networks for smart cities. Furthermore, these different types of heterogeneous wireless networks are expected to support mobile Internet, the Internet of things (IoT), cloud computing [2], and big data in smart cities.

In future smart cities, the different types of information need to be smoothly transmitted by different types of heterogeneous wireless networks with high data rate and low energy consumption. In this case, simple interconnection with different types of heterogeneous wireless

networks cannot support the ubiquitous information services of future smart cities. Furthermore, the mobile converged network has been proposed to satisfy the high data rate and low energy consumption [3]. Compared to the simple interconnection scheme, a new network architecture needs to be proposed for the convergence of heterogeneous networks based on different transmission technologies in smart cities. In general, there are two levels of heterogeneity of communication networks in smart cities. One of the levels refers to the different transmission technologies among Bluetooth, ZigBee, WLAN, millimeter-wave, and even visible light communication (VLC) [4], while another level of heterogeneity is related to different configurations and parameters of the same transmission technology; for example, a heterogeneous cellular network consists of a macrocell tier, a few microcell tiers, and femto-cell tiers [5]. Conventional communication networks, including cellular networks and WLANs, have a distinct characteristic, that is, there are regional areas around base stations (BSs) or access points (APs), in which mobile terminals have to access the network via its associated BS or AP. Such an area can be defined as a "cell" associated with a BS in cellular networks, or just a "covered area" associated with an AP in WLANs. In this article, both of them are called cells for the sake of convenience. In conventional heterogeneous cellular scenarios, a mobile terminal has to hand over vertically among heterogeneous network tiers, or horizontally among adjacent cells in the same tier. As a consequence, it is required to perform complicated switching and routing algorithms across various types of heterogeneous networks. In some recent research, software defined networking (SDN), which was introduced to wired networks many years ago, has been using in managing complicated mobile networks and performing the traffic routing in new generation networks [6], and SDN is also suitable to manage complicated heterogeneous networks [7] such as fifth generation (5G) networks in smart cities. Some research shows that SDN can be improved to manage dynamic links such as access network links or 5G backhaul links, which are widely required in coordinated multipoint transmission networks [8]. To realize ubiquitous and universal network services in smart cities, we try to use SDN technology to break the technology gaps and regional strictness in both vertically tiered and horizontally celled heteroge-

neous networks to support the ubiquitous information services in smart cities.

The most important contribution of this article is to show that a 5G converged cell-less communication scheme is proposed to meet rising challenges in smart cities, such as heterogeneous wireless transmission technologies and interference. Numerical results indicate that the proposed 5G converged cell-less communication network has better coverage performance and higher energy efficiency compared to conventional cellular networks. In the following section the architecture and model of cell-less communication networks are introduced for smart cities. The performance of the 5G converged cell-less communications is then investigated by evaluating the performance of coverage and energy efficiency. The future challenges of the 5G converged cell-less communications in smart cities are then discussed. The conclusion is drawn in the final section.

ARCHITECTURE AND MODEL OF CELL-LESS COMMUNICATIONS IN SMART CITIES

FROM CELLED NETWORKS TO CELL-LESS NETWORKS

There are many challenges for mobile and wireless communications in smart cities. Based on the development of 5G communication systems, some of issues involving with the urban scenarios are described as follows.

- The huge demand of data rate causes ultra-densified BS/AP deployment. There are three main approaches for 5G communication systems to increase data rate significantly: the wider spectrum of millimeter-wave transmission, the greater spatial diversity of massive multiple-input multiple-output (MIMO), and the more spatial density of BSs/APs. Deploying more BSs/APs can serve more high-data-rate-demanding users and thereby provide a higher achievable data rate in terms of per unit area in smart cities. The higher density of BSs/APs makes the cell coverage smaller as the distance between BSs/APs is reduced to tens of meters for satisfying the high data rate demand in smart cities [9].

- The movement of mobile terminals in modern metropolitan scenarios becomes more complex and volatile. In a prosperous city, the movement of mobile nodes is varied and complicated [10]. In smart cities, a mobile terminal with data transmission can be a mobile phone carried by a pedestrian, a navigation device installed on a moving car, or a PDA used on a high-speed train. What is more, various types of mobile nodes make the mobility situation even harder to handle. For example, there are completely different communication requirements between the scenarios of densified RFID labels going through a gate and a mobile high definition surveillance camera moving around in a disaster scene.

- In urban areas, buildings and trees become obstacles to wireless communications. The wireless communication channels are very different between indoor and outdoor environments. The designers of mobile communication systems have to consider the obvious impact of obstacles, especially for the millimeter-wave wireless transmission in the emerging 5G communication networks, which is of very short wavelength and hard to diffract in smart cities.

With regard to the above demands of mobile communications in smart cities, current heterogeneous networks based on different types of communication technologies face many issues for the ubiquitous information services in smart cities; some of them are listed below.

Issue of Network Convergence: To overcome problems of the vertical and horizontal handover and routing across tiers, how to converge the heterogeneous networks becomes a critical issue. It is hard to seamlessly converge the prevailing wireless transmission technologies and communication networks. Instead, they interconnect with each other; hence, many issues regarding routing and protocols remain in heterogeneous wireless networks.

Issue of Load Balancing in Cell Networks: Along with the decreasing cell size, the traffic loads of cells get more and more unbalanced. Moreover, the traffic load of smart cities obviously fluctuates over the space and time domains. The fluctuation of traffic load in the space domain is caused by the stochastic spatial distribution of communication nodes in smart cities; for example, the data centers of smart cities are stochastically distributed in different places. The fluctuation of traffic load in the time domain is created by the mobility of terminals scheduled by the work and life in smart cities [11]. For the improvement of signal-to-interference-plus-noise ratio (SINR) in wireless communications, the sizes of cells in mobile networks get smaller to gain higher data rate matching the terminal's higher data rate demand. As we know, a bigger cell can smooth the random fluctuation in the space domain. When the size of a cell gets smaller in 5G networks, the traffic load balance issue emerges for smart cities.

Issue of Handover: When the cell size is reduced to tens of meters in 5G cellular networks, quickly moving terminals lead to frequent handovers in 5G cellular networks and additional latency is inevitable for wireless communications. When the handover occurs between different types of heterogeneous wireless networks, a large amount of overhead in wireless networks will decrease the data exchanging efficiency.

Issue of Interference: In an interference-limited conventional cellular network, the increase of BS/AP density does not lead to the increase of the average interference indicator [12]. However, the densified BSs/APs under complicated electromagnetic environments in smart cities may face highly correlative interference or noise, and hence the performance of some adjacent BSs/APs drops significantly [13]. It is an important concern to eliminate spatially correlative interference in the dense wireless networks of smart cities.

From what we have discussed above, deploying conventional cellular networks cannot solve the above issues and satisfy the ubiquitous information services in smart cities. To solve these problems caused by heterogeneity of networks and ultra-density of BSs/APs, we propose to use converged "cell-less" communication networks instead of "celled" networks to support the mobile users in smart cities.

Figure 1 illustrates a conventional cellular network and a cell-less network in urban scenarios. As shown in the figure, a mobile terminal in the

When the cell size is reduced to tens of meters in 5G cellular networks, the quickly moving terminals lead to frequent handovers in 5G cellular networks and additional latency is inevitable for wireless communications. When the handover occurs between different types of heterogeneous wireless networks, a large amount of overhead in wireless network will decrease the data exchanging efficiency.

When there are data to be sent to a specified mobile terminal, the SDN controller in the cloud decides which one or more of the BSs are chosen to form a cooperative group to perform downlink joint transmission, considering the location and channel status around the terminal.

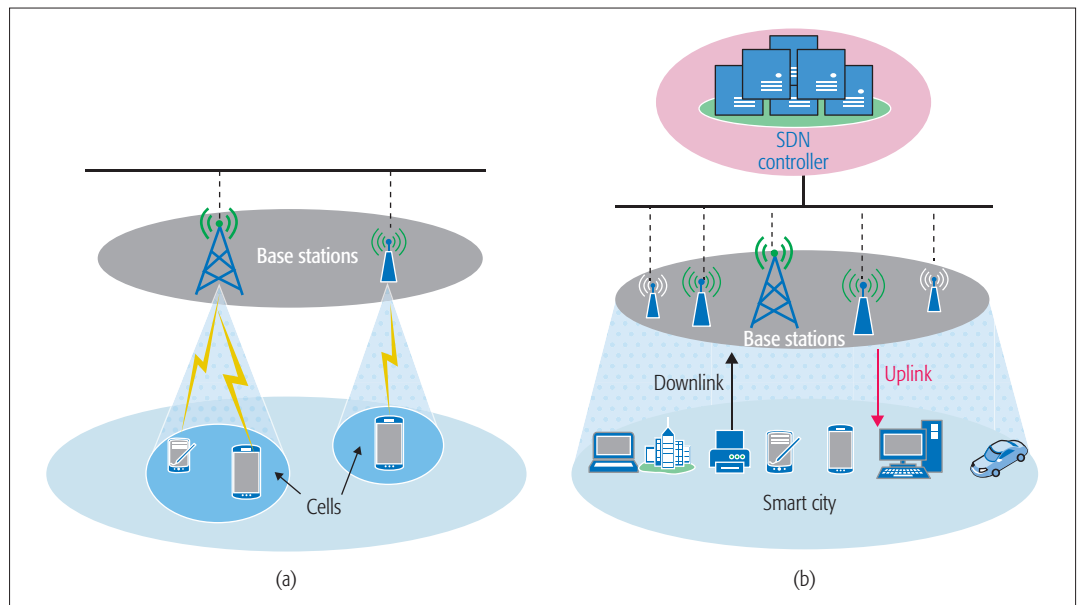


Figure 1. From a conventional cellular network to a cell-less network: a) conventional cellular network; b) cell-less network.

conventional cellular network always associates with one and only one BS/AP, while a terminal in a cell-less network does not associate with any BS/AP. In this case, the terminal in a cell-less network can flexibly communicate with one or more BSs/APs if necessary. In the following parts of the article, we explain the architecture and transmission model of cell-less communication networks.

ARCHITECTURE OF CELL-LESS COMMUNICATION NETWORKS IN SMART CITIES

To match the requirements of huge data rate, ultra-high density, high mobility, and low energy consumption of wireless networks in smart cities, a 5G converged cell-less communication network is proposed in this article. In the novel cell-less scheme shown in Fig. 2, a mobile terminal can choose to access one or more BSs/APs by different uplinks and downlinks considering wireless channel status and its demands, or choose not to access any BS/AP when the mobile terminal is idle. That is, a mobile terminal does not associate with any BSs/APs before it starts to transmit data. In such a case, BSs/APs need not maintain a list of associated mobile terminals; instead, the SDN controller decides which one or more BSs/APs perform the data transmission for the mobile terminal by the control link shown in Fig. 2. Moreover, the SDN controller creates dynamic backhaul links and downlinks/uplinks as well for the joint transmission or reception group of BSs/APs such that they can cooperate with other members in the same group to support joint transmission and reception for a specified mobile terminal. The cell-less scheme supports the adaptive adjustment of the number of BSs/APs by the requirements of the mobile terminal and the wireless channel status in different environments. Therefore, the overhead caused by handover is reduced, and the coverage probability is guaranteed for the mobile terminal. Moreover, the traffic load balancing is achieved by resource scheduling in a large-scale network, which is performed by the SDN controller of converged cell-less communication net-

works. Furthermore, the traffic load fluctuation in spatial and temporal domains is decreased for smart cities. In this cell-less scheme, the SDN controller and core routers form the SDN cloud, in which the control plane is driven by cloud computing, while routers and the instantaneous backhaul links form the data plane in the cloud.

TRANSMISSION MODEL OF CELL-LESS WIRELESS COMMUNICATIONS

To implement the unassociated transmission between BSs/APs and mobile terminals in cell-less wireless communications, it is necessary to change the access method. Mobile terminals update their locations and channel status around them to the SDN cloud in case the communication to BSs/APs is necessary. As shown in Fig. 3, a mobile terminal transmits the data by broadcasting when it wants to send the uplink data. Nearby BSs/APs receive the data, then forward the data to the joint reception controller in the cloud where the data transmitted from the mobile terminal are jointly decoded. When there are data to be sent to a specified mobile terminal, the SDN controller in the cloud decides which one or more of the BSs are chosen to form a cooperative group to perform downlink joint transmission, considering the location and channel status around the terminal.

Compared to the conventional celled networks, the 5G converged cell-less communication networks have many advantages, listed below.

Seamless Convergence of Heterogeneous Networks: Adopting not only interconnection but also data convergence in terms of transmission environments and user requirements, the cell-less communication networks provide a compelling mechanism to fulfill convergence across tiers and combine their respective advantages as well.

Superior Traffic Load Management: By cooperation of dynamically grouped BSs/APs in the cell-less scheme, the cell-less communication network can allocate traffic load to BSs/APs under the schedule of the SDN controller.

Avoiding Frequent Handovers: In a converged cell-less communication network, a mobile terminal need not associate with any fixed BS. Hence, frequent handovers between cells are avoided, which is conducive to the decrease of outage and latency in converged cell-less communication networks.

Improving of Coverage and Energy Efficiency: When the fixed cell association scheme is given up in heterogeneous wireless networks, the converged cell-less communication networks reorganize the association scheme between the mobile terminals and the BSs/APs in terms of the requirements from users and wireless environments in smart cities. When the flexible grouped cooperative communication is performed, improved coverage probability is expected for a mobile terminal in converged cell-less communication networks. Moreover, when suitable BSs/APs are selected for joint transmission and reception, the energy consumption is also expected to be optimized.

COVERAGE AND ENERGY EFFICIENCY OF CONVERGED CELL-LESS COMMUNICATION NETWORKS

BS GROUPING SCHEME FOR CONVERGED CELL-LESS COMMUNICATIONS NETWORKS

How to form a cooperative group of BSs/APs is a critical issue in converged cell-less communication networks. In general, the grouping scheme depends on the spatial distribution of BSs/APs and the wireless channel environments in smart cities. The basic criteria of cooperative BSs/APs grouping are suggested as below.

Simplicity: Considering the ultra-dense deployment of BSs/APs in smart cities, it is suggested that each station/point serves only one mobile terminal at any time if possible, but one BS/AP is allowed to serve more than one mobile terminal if there may be congestion in high traffic load scenarios.

Economy: As infrequently as possible, BSs/APs are selected to form a cooperative group, given that the group of BSs/APs meet the user data rate demand.

Uniformity between Grouping for Uplinks and Downlinks: The SDN controller will always try to keep the same group for both uplink and downlink transmission if possible. However, the BSs/APs of the cooperative groups for uplinks and downlinks can be different from each other, especially when mobile terminals move quickly.

Employing Backhaul Multicast Capability if Possible: In order to reduce the backhaul overhead, the downlink data is transmitted to the cooperative group by multicast methods if possible.

Mobility Prediction for Adjacent Mobile Terminals: When the BSs/APs are grouped for active mobile terminals, it is necessary to acquire the distribution of adjacent active and inactive mobile terminals and predict the transmission and reception actions of adjacent active mobile terminals. Furthermore, the size of a cooperative group is optimized to avoid traffic congestion at a hotspot.

Pre-Grouping of BSs/APs: Considering that there may be frequent grouping of cooperative BSs/APs in high traffic load scenarios, a pre-group-

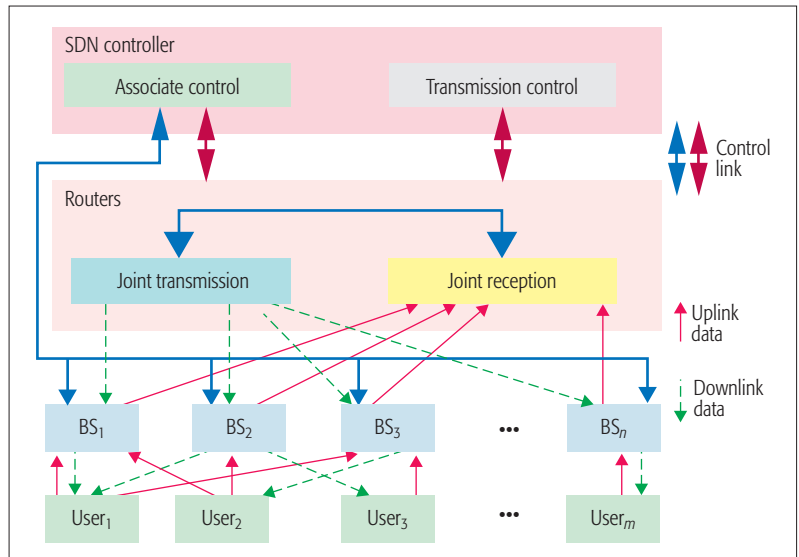


Figure 2. Cell-less association relations and data transmission are under the control of the SDN controller.

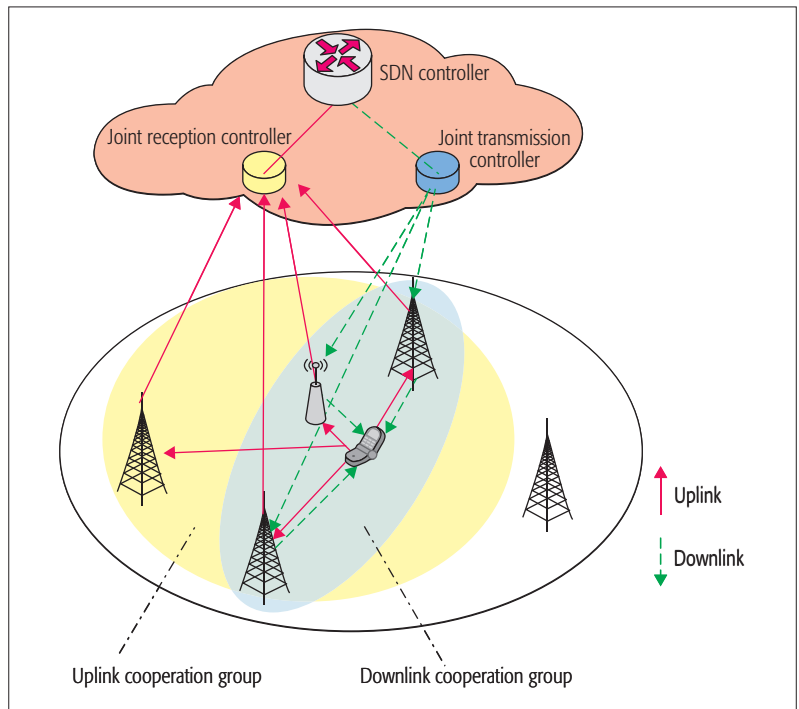


Figure 3. Transmission model of a cell-less network.

ing scheme is required to accelerate the grouping speed of cooperative BSs/APs. The pre-grouping scheme is designed by evaluating recent cooperative grouping results to reduce the computational complexity of a cooperative grouping algorithm.

Generally speaking, for the indoor scenario where terminals hardly move, a cooperative BS/AP group need not be adjusted frequently, while frequent adjustments must be done for quickly moving terminals outdoors. To maintain the quality of communication for fast moving terminals, more BS/AP candidates are beneficial for BS/AP grouping in downlink transmission. Moreover, to maintain a consistent quality of communication, the grouping size should be adjusted when the data rate demands of the users vary.

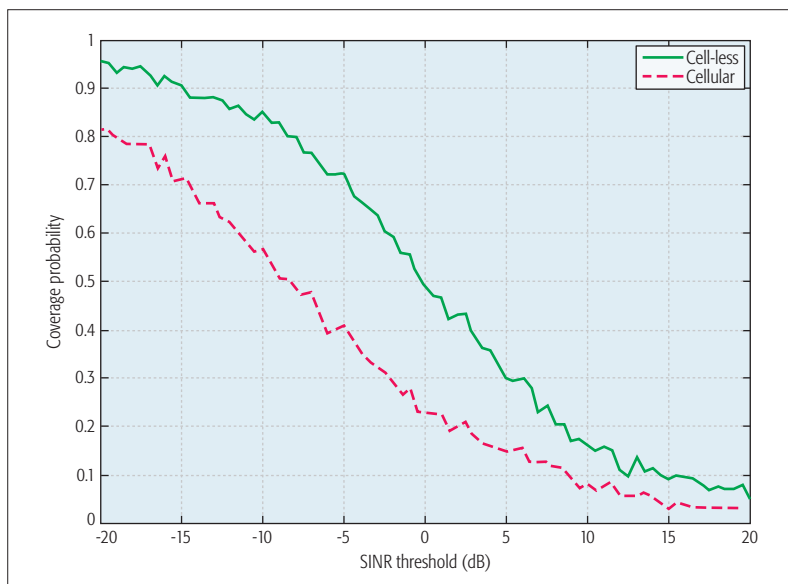


Figure 4. Coverage probabilities of cellular and cell-less networks.

COVERAGE PROBABILITIES IN CONVERGED CELL-LESS COMMUNICATION NETWORKS

As we know, ultra-dense BSs/APs can be deployed to achieve high data rate in smart cities. Moreover, the coverage of every BS/AP will be reduced by massive MIMO and millimeter-wave communication technologies. In this case, the cooperative grouping scheme is a reasonable approach to satisfy the coverage requirement of mobile terminals in smart cities.

Without loss of generality, in our illustrative example, 50 BSs are randomly deployed into a plane of 50 m × 50 m. Moreover, 30 BSs are configured as members of active cooperative groups. A typical user is assumed to be located at the central location in the plane. For the sake of simplicity, the nearest 10 BSs around the typical user are configured to be candidates for cooperative grouping in converged cell-less communication networks. The size limit of the cooperative group is no more than three BSs in converged cell-less communication networks. If there is no idle BS among the candidate BSs, the nearest BS to the typical user is selected to transmit data even if this BS is active in another cooperative group. The coverage probability is analyzed by Monte Carlo simulations in Fig. 4. The results indicate that the coverage probability of the illustrative converged cell-less communication networks is higher than the coverage probability of conventional cellular networks when the SINR threshold of a user terminal is configured as -15 dB~5 dB. The reason is that the cooperative group formed by local BSs can significantly reduce the interference among BSs by converting the interference within the group into the useful signal.

ENERGY EFFICIENCY IN CONVERGED CELL-LESS COMMUNICATION NETWORKS

A large number of BSs/APs are ultra-densely deployed in smart cities. Hence, there is redundancy in BSs/APs when the traffic load is low in some scenarios, such as offices in the middle of the night. The converged cell-less communication network provides a flexible BS/AP sleeping

scheme to decrease the energy consumption in smart cities, which is controlled by the SDN cloud computing. The detailed BS/AP sleeping scheme is explained as follows:

- A BS/AP can be configured in several states including transferring, ready, listening, and sleeping. When a BS/AP is in the transferring state, the BS/AP can transmit data to the specified user terminal or probably quit the active cooperative group due to the dynamic grouping scheme. After that, the BS/AP enters ready state.
- When a large amount of data are transferred, the transmission power can be dynamically allocated among the members of a cooperative group according to the channel status between the user and the BSs/APs. A deliberate power allocation scheme will make sense to save energy.
- In low traffic load scenarios, for example, an office at midnight, some BSs/APs can enter sleeping state from ready or listening state to save as much energy as possible. To guarantee the coverage probability of converged cell-less communication networks, the active BSs/APs adaptively increase the coverage area by increasing the transmission power or grouping more cooperative members if necessary.

Utilizing the same illustrative simulation scenario in Fig. 4, 20 active BSs are selected randomly for transferring or ready state, and the other BSs are configured in sleeping state in converged cell-less communication networks. When a BS is sleeping, its neighbor BSs are configured to serve active users to guarantee coverage probability in this area. Considering small BSs in 5G mobile communication systems, the consumption power of BSs is configured as 10, 50, 80, and 200 mW corresponding to the sleeping, listening, ready, and transferring states, respectively. The energy saving of converged cell-less communication networks with respect to the number of sleeping BSs considering different numbers of cooperative BSs is illustrated in Fig. 5a. Numerical results indicate that the energy saving of BSs increase with the increase of the number of sleeping BSs in the illustrative converged cell-less communication networks. Moreover, the cooperative group of two BSs achieves the maximum energy saving of BSs compared to the cooperative groups of three and four BSs in converged cell-less communication networks.

Without loss of generality, the original transmission power of a mobile terminal is configured as 100 mW, and then first, the received data rate in non-joint reception scenario can be obtained by simulation. When the joint reception scheme is adopted in converged cell-less communication networks, the mobile terminal can adaptively adjust the transmission power to acquire the same data rate as the non-joint reception scenario. When the joint reception is configured at uplinks, the energy saving of a mobile terminal is shown in Fig. 5b. Numerical results show that the energy saving of a mobile terminal increases with the increase of the number of cooperative BSs in the illustrative converged cell-less communication networks. These results imply that the converged cell-less communication networks save energy not only at BSs but also at the mobile terminals.

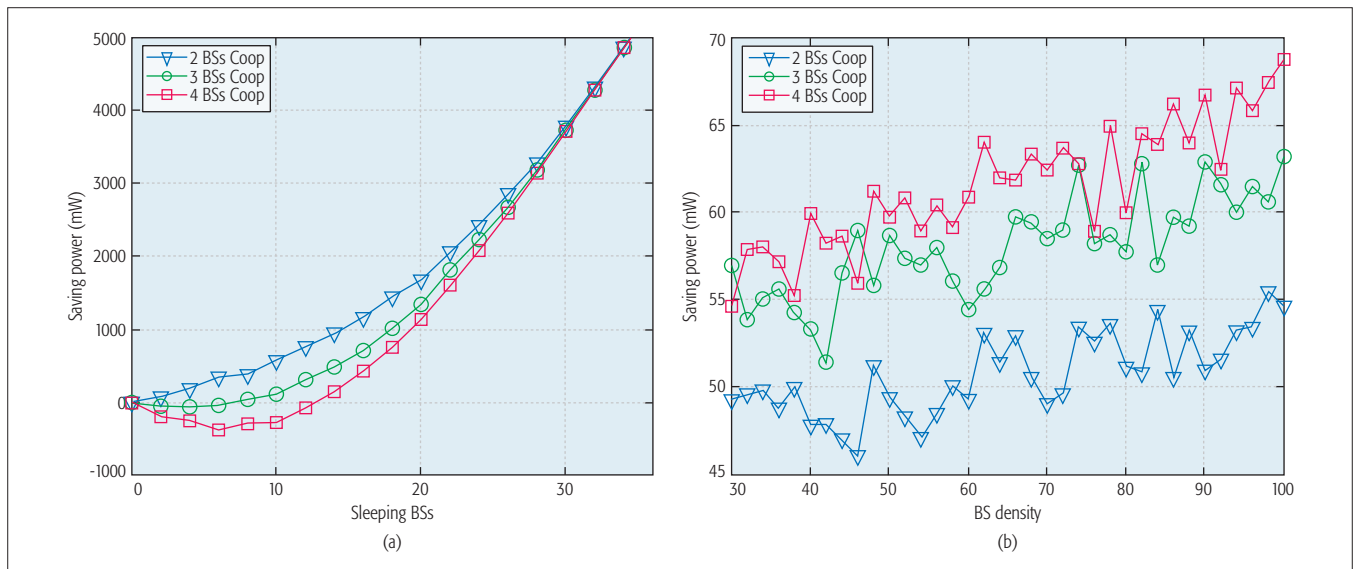


Figure 5. Energy saving in cell-less networks: a) energy saving of mobile terminals; b) energy saving of mobile terminals.

FUTURE CHALLENGES FOR CONVERGED CELL-LESS COMMUNICATIONS IN SMART CITIES

COOPERATION IN ULTRA-DENSIFIED WIRELESS TRANSMITTERS

In the future smart cities, there will be not only a larger number of BSs but also many other WLAN APs and IoT nodes. In this case, these wireless transmitters are ultra-densely deployed in smart cities. All these wireless transmitters could be converged to provide information to users by a cell-less network architecture. The cooperative communication in ultra-densified wireless transmitters is an attractive solution for converged cell-less communication networks. However, the association relationship of the cooperative group cannot be fixed in advance considering heterogeneous wireless transmitters in different wireless networks. In this article, we discuss the potential grouped solutions and validate the advantages in the mobile user coverage probability and the energy saving in smart cities. Anyway, there are still many challenges that need to be investigated. An example is how to trade off the complex and efficiency metrics in cooperative schemes of converged cell-less communication networks. When the large data rate is available for mobile terminals, how to realize the backhaul traffic in converged cell-less communication networks is a great challenge, especially considering different transmission capacities of heterogeneous wireless networks [14]. The cooperative backhaul solution is a potential solution to satisfy the requirements of big data collection and environment awareness in smart cities. As a consequence, the investigation of cooperative backhaul schemes in converged cell-less communication networks is an emerging issue for future smart cities.

DATA AND CONTROL INFORMATION IN SMART CITIES

To support the cooperative transmission in converged cell-less communication networks, part of the control information needs to be separated from the transmission data; then the common data could easily be transmitted and converged in smart cities. Considering the difference among

heterogeneous wireless networks and the architecture of converged cell-less communication networks, it is an important challenge to design a compatible protocol for converged cell-less communication networks. Moreover, the information and data in smart cities have different priorities and security levels. In this case, the control information of transmission data cannot be separated in some specified scenarios of smart cities, for reasons such as personal privacy and public security. Therefore, a special scheme may need to be included in 5G converged cell-less communications for smart cities. At the technology level, it is also a troubling problem to execute a single special scheme in all heterogeneous devices, especially if these devices belong to different owners.

CLOUD AND CACHE COMPUTING IN CONVERGED CELL-LESS COMMUNICATIONS

As discussed in this article, cell-less communications provide a flexible solution in coverage and energy efficiency for future smart cities. Cell-less communications can solve the heterogeneous issues at the physical level. To match the advantages brought by cell-less communications, the cloud and cache computing schemes are expected to collaborate with cell-less communications in smart cities. How to cover the cloud, cache, and cell-less communication into the uniform architecture for supporting smart cities is a true challenge for researchers around the world. One possible way is to cover the above three architectures by converged data information. However, there are different definitions and understandings for the data and information in cloud, cache, and cell-less communications in smart cities. More studies need to be carried out to investigate the converged cloud, cache, and cell-less communications. Consequently, smart cities will be a good platform to build the dream of converged cloud, cache, and cell-less communications [15].

CONCLUSION

The information and data generated from different types of heterogeneous wireless networks are converged to provide ubiquitous service in smart

Considering there should be many complicated factors in the future smart cities, such as the high demand caused by crowded people, the serious obstacle due to a lot of buildings and the heavy interference in dense streets, the converged cell-less communication networks can play a critical role.

cities. To support mobile users in smart cities, the idea of converged cell-less communication networks is proposed to break away from the conventional celled architecture of cellular networks and support a flexible mobile user association scheme considering the application requirements and wireless channel status. With the deployment of 5G ultra-dense wireless networks in smart cities, the cooperative group communication is designed for the 5G converged cell-less communication networks. Simulation results indicate that the coverage probability and the energy saving at BSs and mobile terminals are improved in 5G converged cell-less communication networks. Based on the analysis and illustrative results, it can be concluded that the converged cell-less communication scheme is a promising way to match the high demand for coverage and rate in future smart cities because of its flexibility and unitarity. Considering there should be many complicated factors in future smart cities, such as the high demand caused by crowded people, the serious obstacle of a lot of buildings, and heavy interference in dense streets, the converged cell-less communication networks can play a critical role because they can converge different communication technologies and provide seamless transmission, and thus improve coverage and energy efficiency by reducing unnecessary interference. With the development of smart cities, 5G networks still need to be further investigated for solving new challenges in smart cities.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of the International Science and Technology Cooperation Program of China (grants 2015DFG12580 and 2014DFA11640), the National Natural Science Foundation of China (NSFC) (grants 61471180 and 61210002), the Hubei Provincial Department of Education Scientific research projects (No. B2015188), the Fundamental Research Funds for the Central Universities (HUST grants 2015XJGH011 and 2015MS038), a grant from Wenhua College (No. 2013Y08), the National Research Foundation of Korea-Grant funded by the Korean Government (Ministry of Science, ICT and Future Planning)NRF-2014K1A3A1A20034987, the EU FP7-PEOPLE-IRSES (Contract/Grant Nos. 318992 and 610524), and the EU H2020 project (Grant No. 723227). This research is supported by the China international Scientific and Technological Cooperation Base of Green Communications and Networks (No. 2015B01008).

REFERENCES

- [1] M. Chen *et al.*, "Smart Clothing: Connecting Human with Clouds and Big Data for Sustainable Health Monitoring," *ACM/Springer Mobile Networks and Applications*, DOI: 10.1007/s11036-016-0745-1, 2016.
- [2] M. Chen *et al.*, "AIWAC: Affective Interaction through Wearable Computing and Cloud Technology," *IEEE Wireless Commun.*, vol. 22, no. 1, Feb. 2015, pp. 20–27.
- [3] T. Han *et al.*, "Mobile Converged Networks: Framework, Optimization, and Challenges," *IEEE Wireless Commun.*, vol. 21, 2014, pp. 34–40.
- [4] P. Lynggaard and K. E. Skouby, "Deploying 5G-Technologies in Smart City and Smart Home Wireless Sensor Networks with Interferences," *Wireless Personal Commun.*, vol. 81, no. 4, Mar. 2015, pp. 1399–1413.
- [5] A. Cimmino *et al.*, "The role of Small Cell Technology in Future Smart City Applications," *Trans. Emerging Telecommun. Technologies*, vol. 25, no. 1, 2014, pp. 11–20.

- [6] M. Chen *et al.*, "Software-Defined Mobile Networks Security," *ACM/Springer Mobile Networks and Applications*, DOI: 10.1007/s11036-015-0665-5, 2016.
- [7] S. Sun *et al.*, "An Intelligent SDN Framework for 5G Heterogeneous Networks," *IEEE Commun. Mag.*, vol. 53, no. 11, Nov. 2015, pp. 142–47.
- [8] T. Han *et al.*, "Small Cell Offloading through Cooperative Communication in Software-Defined Heterogeneous Networks," *IEEE Sensors J.*, vol. 16, no. 20, Oct. 2016, pp. 7381–92.
- [9] X. Ge *et al.*, "5G Ultra-Dense Cellular Networks," *IEEE Wireless Commun.*, vol. 23, no. 1, Feb. 2016, pp. 72–79.
- [10] F. Giust *et al.*, "Distributed Mobility Management for Future 5G Networks: Overview and Analysis of Existing Approaches," *IEEE Commun. Mag.*, vol. 53, no. 1, Jan. 2015, pp. 142–49.
- [11] X. Ge *et al.*, "User Mobility Evaluation for 5G Small Cell Networks Based on Individual Mobility Model," *IEEE JSAC*, vol. 34, no. 3, Mar. 2016, pp. 528–41.
- [12] H. S. Dhillon *et al.*, "Modeling and Analysis of K-Tier Downlink Heterogeneous Cellular Networks," *IEEE JSAC*, vol. 30, no. 3, Apr. 2012, pp. 550–60.
- [13] T. Han *et al.*, "Interference Minimization in 5G Heterogeneous Networks," *ACM/Springer Mobile Networks and Applications*, vol. 20, 2015, pp. 756–62.
- [14] X. Ge *et al.*, "5G Wireless Backhaul Networks: Challenges and Research Advances," *IEEE Network*, vol. 28, 2014, pp. 6–11.
- [15] M. Chen, "Towards Smart City: M2M Communications with Software Agent Intelligence," *Multimedia Tools and Applications*, vol. 67, no. 1, 2013, pp. 167–78.

BIOGRAPHIES

TAO HAN [M'13] (hantao@hust.edu.cn) received his Ph.D. degree in information and communication engineering from Huazhong University of Science and Technology (HUST), Wuhan, China, in December, 2001. He is currently an associate professor with the School of Electronic Information and Communications, HUST. His research interests include wireless communications, multimedia communications, and computer networks. He is currently serving as an Area Editor for the *EAI Endorsed Transactions on Cognitive Communications*.

XIAOHU GE [M'09, SM'11] (xhge@hust.edu.cn) is currently a full professor with the School of Electronic Information and Communications at HUST and an adjunct professor with the Faculty of Engineering and Information Technology at the University of Technology Sydney (UTS), Australia. He received his Ph.D. degree in information and communication engineering from HUST in 2003. He is the director of the China International Joint Research Center of Green Communications and Networking. He has published more than 110 papers in international journals and conferences. He served as the General Chair for the 2015 IEEE International Conference on Green Computing and Communications (IEEE GreenCom). He has served as an Editor for *IEEE Transactions on Green Communications and Networking* and other publications.

LIJUN WANG [M'16] is pursuing her Ph.D. degree with Wuhan University, China. She is currently an associate professor with the Faculty of Information Science and Technology, Wenhua College, Wuhan, China. Her research interests include wireless communications and multimedia communications.

KYUNG SUP KWAK received his Ph.D. degree from the University of California at San Diego in 1988. He worked for Hughes Network Systems and IBM Network Analysis Center, and is now with Inha University, Korea, as the Inha Hanlim Fellow Professor. He served as the President of Korean Institute of Information and Communication Sciences in 2006, and the President of Korea Institute of Intelligent Transport Systems in 2009. His research interests include mobile communications and wireless sensor networks including nano networks.

YUJIE HAN received his Bachelor's degree in communication and information systems from HUST in 2012, where he is currently working toward his Master's degree. His research interests include cooperative communication, stochastic geometry, and heterogeneous networks.

XIONG LIU received his Bachelor's degree in electronic information and communication from HUST in 2015, where he is currently pursuing his Master's degree. His research interests include vehicular networks, non-orthogonal multiple access, and cognitive radio.

Cybersecurity and Privacy Solutions in Smart Cities

Rida Khatoun and Sherali Zeadally

ABSTRACT

The increasing proliferation and deployment of ICT in the infrastructure of cities has increased interest in smart cities. The long-term objective of a smart city is to enhance the quality of services provided to citizens and ultimately improve their quality of life. However, incorporating ICT opens up various security and privacy issues in smart cities, along with the people living in them. We briefly present the fundamental design concepts of a smart city and review recent smart city initiatives and projects. After identifying several security vulnerabilities and privacy issues within the context of smart cities that must be addressed, we then discuss various privacy and security solutions, recommendations, and standards for smart cities and their services.

INTRODUCTION

Many cities around the world risk becoming barely livable within a few years as their infrastructures are stretched to their limits in terms of scalability, environment, and security while they adapt to support population growth (9.7 billion in 2050 according to the UN-Habitat United Nations [UN] program — <http://unhabitat.org>). Today, urban territories have complex economic and environmental crises. In fact, this urban evolution will convey both benefits and challenges. Economies will be under increased pressure; energy consumption will increase exponentially; the environment will be challenged; healthcare and education systems will demand new approaches; public safety will be further challenged; and the potential for future cyberattacks against cities is high. Without innovative solutions, this situation can lead to further environmental degradation and poverty. We need to rethink the models of access to resources, transport, waste management, and energy management [1]. Hence, smart, cost-effective, scalable, innovative solutions that can address the problems of urbanization are needed. There are six components that underpin most smart city models: government, economy, mobility, environment, living, and people. All these components help a smart city to achieve multiple benefits that include the following.

Efficient Urban Services: These provide improved transport conditions including comfort, shorter waiting times, better access to information, reduced travel time, reduced CO₂ emissions, optimized operations of municipal services (fast

and effective response to the demands of citizens [users]), and reduced response times in case of failures of city services/systems or theft.

Smart Buildings Services: These offer reduced costs of electricity and water bills by providing information about an individual's consumption in real time, enabling buildings to make use of renewable energy, managing the energy consumption of buildings through a smart grid (e.g., anticipating consumption), and automating all building functions (heating and cooling, security, and lighting).

Cyberspace Services: These support timely and high-quality information to citizens, providing quick and efficient responses to the requests of citizens (e.g., through electronic operations), providing various types of services to citizens, including cloud computing and remote data storage.

As mentioned earlier, a smart city offers several solutions to the various problems faced by urban development and city management. However, the smart delivery of services depends on information and communication technology (ICT) as a critical component. In fact, there are risks and challenges invoked by introducing ICT into the infrastructure of a city. Citizens increasingly use unsafe WiFi networks to access their emails, e-banking, and so on, thereby exposing themselves to various types of cyberattacks such as man in the middle (MITM), cracking, and denial of service (DoS) attacks. On the other hand, new critical infrastructures of cities are likely to be exposed to attacks that could cause severe denial of service to cities and industrial sites, and impede the delivery of other services. Cybersecurity is one of the major distinguishing characteristics that can be used to classify safe cities around the world. The Safe Cities Index (SCI — http://safecities.cope.economist.com/wp-content/uploads/sites/5/2015/06/Safe_cities_index_2015_EIU_report-1.pdf) is often used, and it relies on an index comprising more than 40 quantitative and qualitative indicators relying on four facets: digital security, health security, infrastructure safety, and personal safety.

The actual supervisory control and data acquisition (SCADA) systems are based on old software platforms that can be susceptible to intrusions and attacks, thereby compromising these systems' security criteria. In 2010, the Stuxnet virus [2] targeted the SCADA systems of one of the Iranian nuclear centrifuges. The goal of Stuxnet was to intercept and modify the data sent from and to

The authors briefly present the fundamental design concepts of a smart city and review recent smart city initiatives and projects. After identifying several security vulnerabilities and privacy issues within the context of smart cities that must be addressed, they then discuss various privacy and security solutions, recommendations, and standards for smart cities and their services.

The purpose of health-care services is to help people live healthy by providing access to a range of facilities. In a smart city, public health professionals often need to access the medical information of patients at any time and from anywhere through connected devices, especially when circumstances do not allow for the physical presence of a specialist or in case of unforeseen disasters.

the programmable logic controllers (PLCs) in the nuclear reactors. Stuxnet was successful in causing real physical damage to the Iranian SCADA systems. By 2010 more than 90,000 Stuxnet infections were reported in 115 countries. According to the 2015 Dell Security Annual Threat Report (<https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf>), in 2014, the number of attacks on SCADA systems increased from 91,676 in January 2012 to 163,228 in January 2013, and 675,186 in January 2014. Intelligent vehicles are also vulnerable to serious cybersecurity attacks. In 2015, two cybersecurity researchers published a report (http://illmatics.com/Remote_Car_Hacking.pdf) showing how someone can wirelessly control a Jeep Cherokee after shattering the vehicle's Uconnect system. In 2014, Proofpoint Inc. (<http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799>) published a report on Internet of Things (IoT)-based cyberattacks involving household smart devices. The report showed that 750,000 malicious emails (spam) were sent from more than 100,000 devices, including home networking routers, televisions, and refrigerators. In 2016, Dyn (a company that provides DNS services) suffered from a denial of service attack caused by tens of thousands of connected objects to saturate its infrastructure. The attack resulted in Dyn's inability to provide the DNS service (<https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-to-daysmassive-internet-outage/>). Hence, IoT networks are increasingly being used as an attack platform by malicious attackers.

These attacks and their impact show how seriously we should take security into consideration in critical infrastructures in order to protect data confidentiality, users' privacy, and the safety of human life. To address these aforementioned challenges, cities need to be "smart." As ICT is vulnerable to threats, the smart city should be immune against such attacks and vulnerabilities. In this work, we explore the security architecture of a smart city, and its requirements and challenges. We also highlight some cybersecurity challenges while exploring research opportunities that need more attention to enable the development and adoption of smart cities in the future.

The remainder of this article is organized as follows. In the next section, we describe the smart city design and its deployment. Following that, we present the cybersecurity solutions needed for different sectors of a smart city. Then we describe research works and challenges for privacy protection in smart cities. Finally, we conclude the article.

SMART CITY DESIGN AND DEPLOYMENT

For its general foundation, a smart city's architecture must represent and consider the following components.

GOVERNMENT SECTOR

E-governance is the performance of a government through the electronic medium. E-government allows citizens to fulfill their civic and social responsibilities through a web portal. The main goals of e-government services include: providing access to all information services through official government websites; achieving efficient coordi-

nation among all government departments; providing flexible communication methods to citizens using various types of Internet applications such as email, SMS, chat, and social media; providing information on sentiments of citizens and giving early warnings when something is wrong [3]; and eliminating government paperwork. According to a recent report [4] of the UN, in 2014, all 193 UN member states had national websites, but most of them remain below the desired levels of e-government. In France, the digital France 2012–2020 project (France Numrique 2012–2020) [5] is a government initiative that aims to put France among the major digital nations through digital actions. In this context, the open government partnership (OGP — <http://www.opengovpartnership.org/>), an international organization supported by 69 countries, provides an international platform to encourage governments to be more open and responsive to citizens. Recently, OGP launched the International Open Data Charter that defines the best practices for the release of governmental open data.

HEALTHCARE SECTOR

Healthcare services in a smart city can also benefit from smart connected devices. The purpose of healthcare services is to help people live healthy by providing access to a range of facilities. In a smart city, public health professionals often need to access the medical information of patients at any time and from anywhere through connected devices, especially when circumstances do not allow for the physical presence of a specialist or in case of unforeseen disasters. Remote healthcare can be realized through the utilization of smart devices wirelessly connected to health centers and a data analytics system. However, there are numerous challenges facing the implementation of healthcare services [6]: coordination among healthcare providers, insurance in case of mistakes or errors, high energy consumption by the new healthcare system, interactions among hospitals requiring common languages or new protocols, high-quality interoperable systems, and process standardization. The Health 2.0 (<http://www.health2con.com/>) project is a good example of a healthcare initiative that promotes and exchanges experiences of new technologies in healthcare. In this context, several health startups (<http://tech.eu/features/1472/health-startup-europe/>) are emerging that focus on digital health activity in Europe. To adopt smart healthcare systems, we need more clearly defined methodologies and guidelines to be implemented in hospitals and medical centers.

CRITICAL INFRASTRUCTURE SECTOR

A smart grid is a system built on advanced ICT-based infrastructures that manages electricity in a sustainable, reliable, and economic manner. It is an intelligent electricity network using computers and sensors placed in the grid. In the United Kingdom, more than 7 million smart meters will be installed during the next year in households under a new project called Smart Meters — Project Spark funded by the European Investment Bank and six other commercial banks. It is the largest existing smart meters installation project in Europe in this field to date. One of the world's most modern and intelligent electricity grids is

Project/location	Funding	Duration	Goals	Main partners
France Numrique/ France	French government	2012–2020	Facilitate the growth of digital small and medium-sized enterprises (SMEs). Introduce high-speed broadband and improve the quality of mobile access. Diversify uses and digital services. Renovate governance and ecosystem of the digital economy.	French Ministry of the Economy, Finance and Industry
Spark/United Kingdom	European Union via European Investment Bank (EIB)	2016–2020	Reduction of greenhouse gas	Department of Energy and Climate Change (DECC)
CenterPoint Energy Houston Electric (CEHE's) smart grid/ United States	Investment grant program		Reduce the following: greenhouse gas and pollutant emissions, meter-reading costs, maintenance costs, duration of outages, and theft costs	U.S. Department of Energy
Smart Grid Gotland (SGG)/Sweden	Swedish Energy Agency	2012–2015	Increase the hosting capacity for wind power, and participation in the electricity market.	ABB, Ventyx, Schneider Electric, Royal Institute of Technology (KTH), Svenska Kraftnt, GEAB, and Vattenfal
Yokohama Smart City Project (YSCP)/Japan	Ministry of Economy, Trade and Industry (METI)	2010–2015	Low-carbon city, hierarchical energy management systems (EMS), sensitive photovoltaic (PV) generation	Tokyo Institute of Technology, Toshiba, Mitsubishi, and Hitachi
SCOOP@F/France	Ministry of Sustainable Development and European Union	2014–2018 (parts 1 and 2)	Improve the safety of road users and road workers during maintenance projects. Traffic management.	PSA-Peugeot, Renault, Cerema, IFSTTAR, Telecom ParisTech, Orange
UR: BAN/Germany	Federal Ministry of Economics and Energy	2012-2015	Cognitive assistance, connected traffic systems, and human factors in traffic	Adam Opel, Audi, BMW, Volkswagen, and other companies. Fraunhofer Institute, TUM, Kassel University, other universities/institutes.
AdaptIVe/Germany	European Union	2014–2017	Achieve real advances in safe automated driving. Legal context of automated driving in future cities and the classification of automated systems from a legal perspective.	Volkswagen, BMW, RENAULT, Volvo, Peugeot Citron, Ford R&A, and other companies. University of Trento, University of Leeds, and other universities/institutes.
Green Vision/United States	State and federal funding	2007–2022	Ten goals have been defined, including reducing energy use by 50 percent, 100 percent energy from renewable sources, reuse of water, zero-emission lighting, and 100 percent public vehicles running on alternative fuels	Universities, private companies, and regional agencies

Table 1. Recent projects and initiatives related to smart cities around the world.

actually in progress on the Swedish island of Gotland. This project (<http://www.smartgridgotland.se/>), called Smart Grid Gotland (SGG), intends to integrate large amounts of renewable energy sources (RESs) into the network while maintaining reliability. SGG will increase the hosting capacity for wind power and test the sale of energy by households from solar or wind power under market driven conditions. In the United States, the results of CenterPoint Energy Houston Electric's (CEHE's) smart grid project (https://www.smartgrid.gov/project/centerpoint_energy_hous-

[ton_electric_llc_smart_grid_project.html](https://www.smartgrid.gov/project/centerpoint_energy_houston_electric_llc_smart_grid_project.html)) show the benefits of the smart grid approach: improved distribution system reliability (avoiding dozens of millions of customer outage minutes), reduced meter reading costs, reduced operating and maintenance costs (decreased by approximately \$55 million in 2013), reduced truck fleet fuel usage, and reduced costs from theft detection such as unusual consumption (a cost reduction of \$2 million in 2013). To monitor and control distributed components in a power system, the latter needs a SCADA system.

In a smart city, an IT infrastructure underpins the design of buildings' control systems, including light and motion sensors, water heaters and coolers, escalators, gas and smoke detectors, water leak detectors, security and access systems. The integration and interconnection of these control systems with other systems will increase the security concerns for building operations, occupants and owners.

SMART BUILDINGS SECTOR

In a smart city, innovative and smart buildings are required for various reasons: improving residents' comfort, efficient operation of the building's systems (i.e., elevators, water pipes, gas pipes), and reduction in energy consumption. In a smart building, a building automation system (BAS) automatically controls the heating, air conditioning, lighting, and other systems. In its report titled *Global Smart Buildings Forecast 2013–2018*, IDC Energy Insights expects that the smart building technology market will grow from \$7.3 billion in 2014 to \$21.9 billion in 2018. As for the promotion of technologies for smart buildings, it has been demonstrated that fuel cell technology [7] will enable smart buildings to provide their own electricity with 50 percent less CO₂ emissions. Fuel cell technology is currently being tested at various locations around the world such as Amsterdam's smart city projects and on environmentally friendly vehicles. Solar technology has also made significant strides (e.g., PV cells that convert light energy into electricity) in the past decade. Recently, new design approaches have emerged based on nanophotonics where nano-antennas are exploited for guiding and localizing light at the nanoscale [8, 9].

TRANSPORTATION SECTOR

Half of humanity today lives in cities. Mobility in big cities leads to several problems, such as traffic congestion, and increased pollution and energy consumption. To alleviate these problems, one solution is intelligent transportation systems (ITSs). In a smart city, ITSs offer multiple services, such as reducing mobility by facilitating transport mode selection, optimizing trip planning and management, detecting drivers exhibiting malicious behaviors, improving driver and passenger safety, reducing CO₂, making available parking places information known on smartphones, and tracking cars. Hence, vehicular communication is a key technology in smart cities. ITS technologies and services have been developed over a number of years in research projects by different research communities and standardization organizations such as IEEE and the European Telecommunications Standards Institute (ETSI), the Car2Car Communication Consortium, or the U.S. National Highway Traffic Safety Administration (NHTSA). In Germany, 31 partners from industry and academia are working on the user-centric assistance systems and network management (UR: BAN) project (<http://urban-online.org/en/urban.html> — 2012–2015). This project's goal is to introduce human factors into the traffic system to receive information much earlier, which will help anticipate traffic situations, predict behavior, and detect hazardous traffic situations. Further, the European research project (<https://www.adaptive-ip.eu/>) Automated Driving Applications & Technologies for Intelligent Vehicles (AdaptIVe) in Wolfsburg, Germany, aims to improve safety for automated driving. In this project special attention is given to the legal aspects of automated driving in future cities and the classification of automated systems from a legal perspective.

In Table 1 we highlight specific developments related to smart cities in Asia, Europe, and North America.

CYBERSECURITY SOLUTIONS

For the many components of a smart city's design, we must also consider the cybersecurity solutions needed.

CRITICAL INFRASTRUCTURES

During the last few years, industrial control systems (ICSs) are increasingly connected to the Internet. ICSs can be found in various infrastructures, including nuclear power plants, chemical plants, oil refineries, railway signaling systems, wind turbines, and so on. Many supervising systems such as SCADA and communication protocols have been designed for ICSs. The SCADA system consists of multiple hardware modules and devices such as the front-end processors (FEPs), engineering workstations, servers, telephone lines, remote terminal units (RTUs), and programmable logic controller (PLC). These devices are controlled through specific SCADA system protocols such as Modbus/TCP, EtherNet/IP, and the Distributed Network Protocol (DNP). However, these protocols were originally designed without any security measures. Exploiting vulnerabilities in a SCADA system can cause significant disruption in the delivery of its services. In SCADA systems, the DNP3 and Modbus protocols allow the supervisory system to have remote devices (e.g., PLCs) that are used to control machines and processes, such as the flow of cooling water in a nuclear reactor, motors, and sensors. Actually, engineers need access to these PLC devices from diverse locations. DNP3 is a communication protocol standardized by IEEE for electric power systems. Modbus is the most widely rolled out industrial control communications protocol (designed in 1979 by Modicon). Unfortunately, security measures were not taken into consideration in the initial design of DNP3 and Modbus. Consequently, these protocols are often vulnerable to cyberattacks such as unauthorized command execution, MITM attacks, DoS, and replay attacks. For example, by default, DNP3 does not provide any authentication mechanisms between the master and the remote devices, which can lead to dangerous consequences in a critical infrastructure such as a water distribution system, a gas distribution system, or a nuclear reactor.

Recently, the open intrusion detection system (IDS) Snort, version 2.9.2, has added preprocessors to support the DNP3 and Modbus protocols in detecting intrusions and attacks against DNP3 and Modbus. A new design architecture of a firewall for systems that use the ModBus and DNP3 protocols using critical state distance (a metric to compute the distance between the current profile and a critical one) was proposed in [10]. However, critical states need to be described in advance, and the firewall does not automatically learn the configuration of the SCADA system. A lot of attention has been given to the data integrity, and some to authentication and confidentiality.

SMART BUILDINGS

Cyber-attacks are threatening banks, companies, and government networks. In a smart city, an IT infrastructure underpins the design of buildings' control systems, including light and motion sensors, water heaters and coolers, escalators, gas

Characteristics	Description	Standards and recommendations
Organizational	<ul style="list-style-type: none"> • Develop a backup and recovery plan • Manage passwords • Open feedback sessions • Define the standards, tools, safety procedures and rules for the community • Develop policies regarding passwords and configurations 	<ul style="list-style-type: none"> • Five Best Practices to Improve Building Management Systems (BMS), Schneider Electric • IET standards: Resilience and Cyber Security of Technology in the Built Environment • Frost & Sullivan's Cybersecurity in Smart Buildings, 2015 • Measurement Science Roadmap for Net-Zero Energy Buildings
Technical	<ul style="list-style-type: none"> • Provide physical security for equipment, network cable, and servers • Encrypt network traffic with robust symmetric algorithms such as AES and Blowfish • Use a secure connection such as a VPN for remote accesses • Secure any wireless network with WPA2 protocol • Deploy IDS in building • Use a centralized authentication, authorization, and accounting (AAA) server such as a RADIUS server • Deploy a firewall at every transition point • Use strong authentication methods such as biometric or smart cards 	<ul style="list-style-type: none"> • ANSI/TIA-862, Building Automation Systems Cabling Standard • GSA Guide to Specifying Interoperable Building Automation and Control Systems Using ANSI/ASHRAE Standard 135-1995, BACnet • Security requirements of IoT-based smart buildings using RESTful web services • BSI Federal Office for Information Security • Schneider Electric
Human	<ul style="list-style-type: none"> • Comprehensive training program for developers and administrators. • Inform and raise awareness of safety issues • Alert and advise users where there are threats • Embed continuity plans and disaster recovery 	—
Legal	<ul style="list-style-type: none"> • Respect legal aspects of security • Use safety standards and follow-up recommendations of the national cybersecurity agencies and actors of IT security • Good practices of ICT use • Performance standards 	—

Table 2. Security standards and recommendations for cybersecurity of smart buildings.

and smoke detectors, water leak detectors, security, and access systems. The integration and interconnection of these control systems with other systems will increase the security concerns for building operations, occupants, and owners. In a smart building the threat could be the disruption of video surveillance, electrical distribution, lighting, emergency power, access control, elevators, fire systems, HVAC, climate control, monitoring, and so on. Any connected device using some software is vulnerable, and the hack can be performed remotely through the Internet. An attacker can easily hack a smart TV by using an MITM attack (<https://iicybersecurity.wordpress.com/2015/07/07/how-to-easily-hack-your-smart-tv-samsung-and-lg/>) because there are actually no anti-viruses or anti-malware solutions available for smart TVs, and for some TV brands the authentication procedure only needs an IP address, a media access control (MAC) address, and a hostname for authentication, which is easy to spoof. Cyberattacks can come from many sources: originating inside or outside a company, executed by terrorists, and so forth. Various communication protocols are actually used in smart buildings:

- BACnet is a communication protocol standardized by the American National Standards Institute (ANSI) and the International Standards Organization (ISO) (ISO 16484-5) since 2003 for building automation and control networks. It defines a number of data link/physical layers.
- KNX is standardized under EN 50090 and ISO/IEC 14543; it is an Open System Interconnection (OSI)-based network communications protocol for intelligent buildings.
- Factory Instrumentation Protocol (FIP) is a European standard (EN 50170-3) used for

the interconnection of devices in automated systems. It defines several application/data link/physical layers.

However, all these protocols have no cybersecurity measures to protect buildings against cyberattacks or intrusions. Hence, strong security measures must be applied in smart buildings. These measures must be applied as part of a complete security architecture. Table 2 summarizes the security characteristics that must be applied in an intelligent building management system (BMS).

ITS

The IEEE 1609.2 standard proposed various methods of securing WAVE messages against eavesdropping and spoofing. These methods include public key cryptography, elliptic curve cryptography (ECC), specific WAVE certificates, and hybrid encryption. However, IEEE 1609.2 does not address the issue of user authentication and privacy. In [11] the authors showed a close correlation between the start and end points of a vehicle's trips and the vehicle owner's home address, which can lead to vehicle tracking. Current standardization efforts (http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp1_security.pdf) focus on approaches based on asymmetric cryptography. Messages are authenticated with the Elliptic Curve Digital Signature Algorithm (ECDSA) and the public key certificate issued by a long-term certificate authority (LTCA). Each vehicle also has a pseudorandom certificate issued temporarily by a pseudorandom certificate authority (PCA). Changing pseudonyms frequently offers a good solution for location privacy [12]. However, if the pseudonyms are changed at an inappropriate time or position, such a solution might become inefficient.

E-health devices supporting healthcare applications face several constraints such as the computational limitations because of low-speed processors in sensors and smartphones, memory limitations, energy limitations, and concerns about mobility. Therefore, further research into novel, robust security algorithms is needed.

E-GOVERNMENT

As mentioned previously, e-governance is a modern system adopted by governments using ICT to link government institutions to each other and to private institutions. Several countries have tried e-government to offer high-quality e-government services to their citizens. However, according to the United Nations e-government survey (<http://www.unpan.org/e-governme>) in 2014, the majority of citizens are concerned about privacy and security when using e-government services. The main challenges e-government must overcome are privacy, trust, and availability in terms of security. In fact, the security of e-governance includes traditional security services (authentication, confidentiality, integrity, and availability), with more emphasis on data privacy and business continuity management. In the final report of the European project STOA, "Security of eGovernment Systems," 11 security policies were defined. More attention was given in this project to the privacy in e-governance such as building a "Privacy by Design" knowledge base, stimulating technical and legal solutions to enhance privacy, and making privacy impact assessments of e-government systems mandatory and public.

E-HEALTH

E-health medical services are supported by electronic processes and communication. Also, healthcare professionals share patients' data among them and tele-monitor patients' health through smartphones, and patients can have e-prescriptions. E-health allows the public dissemination of medical information about a country's health situation and manages health crises through the use of information systems to measure, monitor, and make decisions. Actually, many research efforts have focused on the use of wireless medical networks to enable and improve the quality of care and remote medical monitoring. These networks, also called wireless body area networks (WBANs), are characterized by the mobility of their nodes, a network's easy deployment, and its self-organization, which allows elderly people, people at risk, and patients with chronic disease to be monitored. However, these networks open up new technological challenges in terms of security and privacy. For example, transmitting an electrocardiogram (ECG) signal without encryption will have a big impact on privacy. Commonly used methods include discrete cosine transform (DCT), wavelet transform, and adaptive Fourier decomposition (AFD) algorithms [13]. However, for e-health applications, the performance of these methods depends on the compression efficiency (i.e., the ratio between the original signal and the recovered one), reconstruction quality (the difference between the original signal and the recovered one), and computation complexity. Finding an efficient solution remains a serious challenge. On the other hand, shifting to the cloud environment and storing patient health data in third-party servers remains a serious threat to data privacy. Homomorphic encryption enables modification of the encrypted data without decrypting it. Homomorphic encryption is a very good candidate for e-health in the cloud as it makes the data hosted in the cloud incomprehensible to the provider and others during transmission or processing. The

efficiency of Somewhat Homomorphic Encryption (SwHE) has been proven in medical and financial applications [14]. The ISO/TS 18308 standard defines security and privacy for medical records. E-health devices supporting healthcare applications face several constraints such as the computational limitations because of low-speed processors in sensors and smartphones, memory limitations, energy limitations, and concerns about mobility. Therefore, further research into novel, robust security algorithms that minimize resource consumption and maximize security performance (along with efficient energy use) is needed.

INTERNET OF THINGS

According to [15], there are various key IoT challenges such as heterogeneity, interoperability, scalability, security and privacy, reliability, lack of understanding of new business models, and numerous competing technology standards – International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Study Groups, Internet Engineering Task Force (IETF) Working Groups, ISO, International Electrotechnical Commission (IEC), ISO/IEC Joint Technical Committee 1 (JTC1), IEEE Working Groups, World Wide Web Consortium (W3C), Third Generation Partnership Project (3GPP), Object Management Group (OMG), Open Mobile Alliance (OMA), and others – that must be addressed in the future. In an IETF draft (<https://tools.ietf.org/html/draft-ietf-dice-profile-17>), the authors define the security architecture and security services (authentication, key exchange, and data integrity) of IoT, and its deployment model. They propose what is actually considered be the most suitable protocol for IoT, which is Constrained Application Protocol (CoAP) over Datagram Transport Layer Security (DTLS). CoAP is a lightweight application layer protocol particularly suited for constrained IP networks because of its low bandwidth requirements; it helps to increase reliability (by reducing fragmentation at layer 2) and reduce latency in low-power wireless networks such as IEEE 802.15.4. Along with IoT standardization perspectives, there is a need to integrate emerging technologies such as cloud computing, big data, software defined networking (SDN), and network functions virtualization (NFV) with IoT. However, this integration brings risks and vulnerabilities from a security perspective.

Generally, the introduction of ICT in smart cities leads to various security and privacy concerns, summarized in Table 3 along with possible countermeasures.

As shown in Fig. 1, we identified four main challenges for a cybersecurity architecture for smart cities: sophisticated attacks, software product bugs and vulnerabilities, legislation issues, and complexity. Sophisticated attacks are due to hardware capabilities, virtualization, and advanced cryptography techniques that are increasingly being used in network attacks. Software products with security vulnerabilities exist because of poor/defective software design, configuration errors, and/or insecure isolation techniques. As for legislation issues, laws for smart cities cannot be developed and applied properly if existing laws are not reviewed in light of new demands (e.g., user privacy, smart cities leadership, and law

interoperability) in smart cities. Finally, security requirements, new attacks, and legislation issues together further increase the complexity of managing a smart city.

PRIVACY PROTECTION IN SMART CITIES

For any technology, the rights of citizens should be guaranteed anywhere and anytime. Despite the benefits of smart cities services, privacy breaches are becoming worrisome within the context of smart cities. In fact, most services of a smart city are based on ICT. Sometimes users (especially adolescents and the elderly) are not familiar with security issues, and they become perfect targets for attackers when they interact with many smart cities services through their smartphones, tablets, and computers, revealing personal data such as gender, age, and location. Thus, this section focuses on privacy issues within smart cities. We first define privacy issues; then we present and compare different privacy models. Finally, we briefly discuss current privacy regulations in different countries.

PRIVACY ISSUES

To understand the significance of privacy challenges in smart cities, we use the following example. A vehicle's license plate can be connected to the vehicle owner's identity. Hence, the trajectory of a vehicle can easily be traced even if all communications between the vehicle and infrastructure are encrypted and each device is authenticated by others. This is against the common notion of privacy, which includes the right of people to lead their lives in a manner that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbor's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera. In a smart city, future vehicles will have various communication capabilities that include Internet access, GPS, an electronic tolling system, and RFID. Connected devices in a vehicle will store lots of personal information and have various communication capabilities. In a smart city, the number of connected devices will be very high. The data collected by IoT will allow data consumers to understand the behaviors of data owners or use the data to derive highly personal information, including daily habits.

PRIVACY MODELS

In an information system there are three main operations: data transfer, storage, and processing. Privacy concerns can occur during any of these operations, which can affect the user's behavior. Services may be associated with the user's location, which can raise privacy concerns. The authors in [16] proposed the Where, Who, What (W3) privacy model for location-based services (LBS). In [17], a three-layer model of user privacy was proposed to build privacy-friendly systems. For example, in a smart city, privacy-preserving techniques allow two companies to compare their activities without disclosing to each other their strategic or critical data. The authors in [18] proposed an approach based on linear algebra operations such as matrix multiplications to solve linear systems and compute the correlation between distributed datasets. The proposed solution is efficient and theoretically secure. However, on a large scale the performance of this solution is not

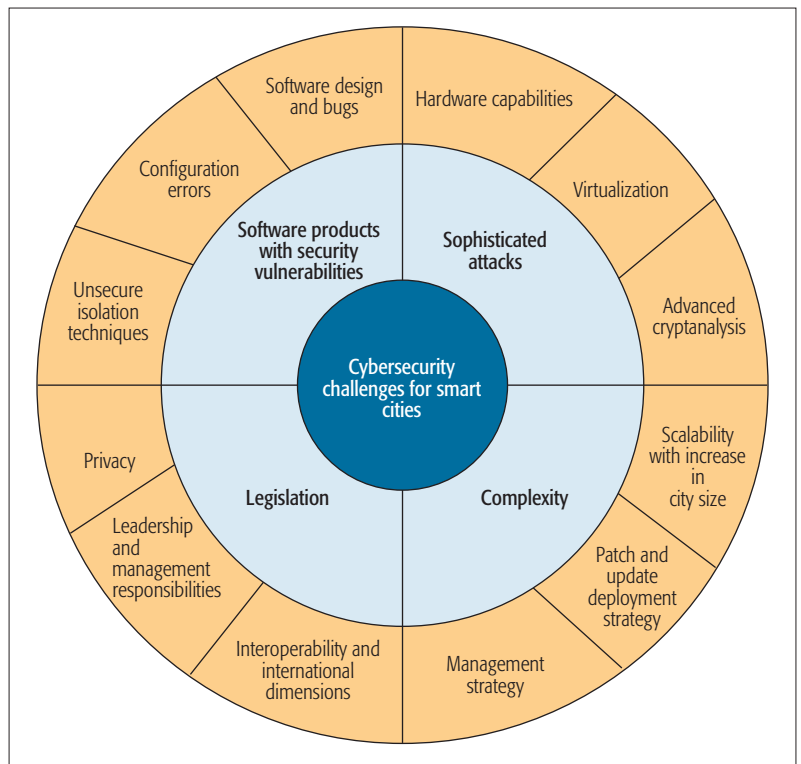


Figure 1. Cybersecurity challenges for smart cities.

reliable because it depends on a trusted initializer that must send data to the parties involved before protocol execution. Unfortunately, privacy-preserving techniques do not address constraints such as the frequent change of members and untrusted third parties (cloud providers). Hence, privacy preservation remains a significant challenge that requires further investigation.

Legislation is important to guarantee privacy within smart cities. Recently, the British Parliament initiated a bill [19] that would allow intelligence services to get unlimited access to users' Internet navigation data. Under this law, intelligence agencies can legally intercept and decrypt people's communications; service providers can store users' navigation data for 12 months; and police can also legally hack computers, networks, and mobile phones. However, Microsoft, Facebook, Google, Yahoo, and Twitter indicated their disapproval of this project. Human Rights Watch (<https://www.hrw.org/news/2015/11/09/uk-surveillance-bill-threat-privacy>) argued that this kind of project is dangerous and too intrusive because it threatens citizens' privacy in the United Kingdom. In France, a new surveillance law (Loi n° 2015-912 du 24 juillet 2015) was approved in July 2015. The new law allows intelligence agencies to monitor communications (emails and phone calls) of suspected persons.

CONCLUSION

The main objective of a smart city is to enhance the quality of services provided to citizens to improve their quality of life. However, ensuring security and privacy are significant challenges for our future cities. Here, we have described some of the basic concepts of smart cities, and highlighted recent major initiatives, developments, research, and industrial projects related to smart

cities in different countries. We then identify risks and challenges for smart cities in different sectors such as industrial control systems, intelligent transport systems, the Internet of Things, and e-health. In looking toward the future, we underscore that in smart cities, privacy and public safety remain a central concern that need more legal, scientific, and political consideration. To make this technology as beneficial and trustworthy as possible for public adoption, it is imperative to fight against cybercrime in smart cities. This will

require ongoing efforts and support from all stakeholders including politicians, governments, legal institutions, energy providers, network operators, vehicle manufacturers, cloud providers, research laboratories, and industry.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their valuable comments and suggestions, which helped us to improve the quality and presentation of this work.

Sector	Threats	Countermeasures
Smart buildings sector	<ul style="list-style-type: none"> • Infection by malware • Systems failure • Fraud by staff and unauthorized users • Controlling the fire system • Causing physical damage such as flooding • Disrupting building temperature (overheating or overcooling) • Damaging or controlling the lifts • Open windows and doors • Modifying smart meters • Opening parking gates • Disabling water and electricity supplies • Starting/stopping the irrigation water system • Stopping the renewable energy systems (RES) 	<ul style="list-style-type: none"> • Two-factor authentication and one-time passwords for stronger authentication (Imprivata OneSign, Comodo Security Solutions, and STMicroelectronics Secure MCU) • IoT forensics (DigiCert IoT PKI Solutions, and Symantec solutions) • Threat and risk modeling • Data backup and recovery solutions to ensure reliability and continuity of services (CommScope solutions, Socomec solutions, Johnson Controls, and Newron System)
Transport sector	<ul style="list-style-type: none"> • Sending false emergency messages • Disrupting a vehicle's braking system • Stopping the vehicle's engine • Triggering false displays in the vehicle's dashboard • Disrupting the vehicle's emergency response system • Changing GPS signals 	<ul style="list-style-type: none"> • Public key infrastructure (PKI), digital certificates (ECDSA) and data encryption solutions (ECIES and AES) • Misbehavior detection solutions • Pseudorandom identities
Government sector	<ul style="list-style-type: none"> • Preventing of cybercrime • Identity theft • Disrupting critical infrastructures • Fiscal fraud • Altered files 	<ul style="list-style-type: none"> • Data leakage prevention (Symantec, Fortinet) • Risk assessment (MEHARI, EBIOS) • Insider threat analysis • Awareness training
Healthcare sector	<ul style="list-style-type: none"> • Modifying patients record or information • Exposing sensitive data unintentionally • Disrupting the monitoring system • Disrupting the emergency services • Sending false information • Jamming attacks • Sending an emergency alert • Eavesdropping sensitive information 	<ul style="list-style-type: none"> • Secured WiFi networks to guarantee safe handling of confidential information and personal data (AirTight Networks solutions, Aerohive security solutions) • Risk assessment (Rapid7 solutions, Health Security Solutions, SafeNet's data security solutions, Stanley security solutions, Intel healthcare security solutions)
Energy sector	<ul style="list-style-type: none"> • Spoofing addresses and user names • Unauthorized access and controls • Zero day attacks • Botnets (Zeus, ZeroAccess, Conficker, etc.) • Denial of service and distributed denial of service (DDoS) 	<ul style="list-style-type: none"> • Intrusion detection and prevention techniques (Radflow, Snort) • Risk assessment (MEHARI, EBIOS) • Insider threat analysis • Cybercrime intelligence
Financial sector	<ul style="list-style-type: none"> • Loss of privacy • Accounting fraud • Disrupting business processes • Accessing confidential company information • Accessing confidential customer information • Damaging reputation(s) • Defacing websites • Financial and reputation concerns due to fraud and data leakage • Denial of service and DDoS • Phishing • Mobile banking exploitation • SQL injection • Trojan 	<ul style="list-style-type: none"> • Anti-malware solutions (McAfee, Symantec) • Encrypted files and firewalling • Fraud detection and prevention techniques (NICE Actimize, Lexisnexis, Kount Complete, Signifyd, Fraud Guardian) • Risk assessment (MEHARI, EBIOS) • Insurance to mitigate cybercrime Risk • Cybercrime intelligence (RSA CyberCrime Intelligence Service, ThreatMetrix Advances Cybercrime Prevention, SurfWatch vC-Suite, IBM Enterprise Insight Analysis)

Table 3. Security and privacy concerns and countermeasures in smart cities.

REFERENCES

- [1] R. Khatoun and S. Zeadally, "Smart Cities: Basic Concepts, Architectural Issues, and Research Opportunities," *Commun. ACM*, vol. 59, no. 8, Aug. 2016, pp. 46–57.
- [2] Symantec Security Response Report: W32.Stuxnet Dossier, v. 1.4, Feb. 2011.
- [3] L. Berntzen, "Smart Cities, Smart Buildings, Smart Users," Keynote, DigitalWorld 2015, Lisbon, Portugal, Feb. 24th, 2015.
- [4] UN E-Government Survey 2014, "E-Government for the Future We Want," <http://www.un.org/desa>
- [5] France numérique 2012: bilan et perspectives, <http://www.entreprises.gouv.fr>
- [6] H. Demirkan, "A Smart Healthcare Systems Framework," *IT Professional*, vol. 15, no. 5, Sept.–Oct. 2013, pp. 38–45.
- [7] L. Valverde, C. Bordons, and F. Rosa, "Integration of Fuel Cell Technologies in Renewable-Energy-Based Microgrids Optimizing Operational Costs and Durability," *IEEE Trans. Industrial Electronics*, vol. 63, no. 1, Jan. 2016, pp. 167–77.
- [8] G. Akselrod et al., "Probing the Mechanisms of Large Purcell Enhancement in Plasmonic Nanoantennas," *Nature Photonics*, 2014.
- [9] X. Zhou et al., "Selective Functionalization of the Nanogap of a Plasmonic Dimer," *ACS Photonics*, vol. 2, no. 1, 2015, pp. 121–29.
- [10] I. N. Fovino et al., "Critical State-Based Filtering System for Securing SCADA Network Protocols," *IEEE Trans. Industrial Electronics*, vol. 59, no. 10, Oct. 2012, pp. 3943–50.
- [11] B. Hoh et al., "Achieving Guaranteed Anonymity in GPS Traces via Uncertainty-Aware Path Cloaking," *IEEE Trans. Mobile Computing*, vol. 9, no. 8, Aug. 2010, pp. 1089–1107.
- [12] R. Lu et al., "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Trans. Vehic. Tech.*, vol. 61, no. 1, Jan. 2012, pp. 86–96.
- [13] J. Ma, T. Zhang, and M. Dong, "A Novel ECG Data Compression Method Using Adaptive Fourier Decomposition with Security Guarantee in e-Health Applications," *IEEE J. Biomedical Health Informatics*, vol. 19, no. 3, May 2015, pp. 986–94.
- [14] J. H. Cheon and J. Kim, "A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption," *IEEE Trans. Info. Forensics Security*, vol. 10, no. 5, May 2015, pp. 1052–63.
- [15] M. Carugi, "Considerations on the IoT Standardization Landscape and ITU-T Perspectives," Proc. IoT 360 Summit 2015, Technology Track, Session on "Standardization in IoT," 27 Oct. 2015, Roma, Italy.
- [16] P. A. Prez-Martnez, and A. Solanas, "W3-Privacy: The Three Dimensions of User Privacy in LBS," *Proc. 12th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing*, May 2011.
- [17] S. Spiekermann and L. F. Cranor, "Engineering Privacy," *IEEE Trans. Software Engineering*, vol. 35, no.1, Jan.–Feb. 2009, pp. 67–82.
- [18] B. David et al., "Unconditionally Secure, Universally Composable Privacy Preserving Linear Algebra," *IEEE Trans. Info. Forensics Security*, vol. 11, no. 1, Jan. 2016, pp. 59–73.
- [19] Draft Investigatory Powers Bill, Nov. 2015.

BIOGRAPHIES

RIDA KHATOUN received his M. Sc in computer engineering and his Ph.D. from the University of Technology of Troyes (UTT), France, in 2004 and 2008. He is currently an associate professor at Telecom ParisTech. His research interests include DDoS attack detection and defense, intrusion detection systems, and mobile ad hoc network security.

SHERALI ZEADALLY received his Bachelor's degree in computer science from the University of Cambridge, United Kingdom, and his doctoral degree in computer science from the University of Buckingham, United Kingdom. He is an associate professor in the College of Communication and Information at the University of Kentucky. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, United Kingdom.

SUSTAINABLE INCENTIVE MECHANISMS FOR MOBILE CROWDSENSING: PART 1



Linghe Kong

Kui Ren

Muhammad Khurram Khan

Qi Li

Ammar Rayes



Mérouane Debbah

Yuichi Nakamura

Mobile devices are explosively growing in our daily lives. These mobile devices are widely equipped with sophisticated embedded sensors, such as accelerometers, digital compasses, gyroscopes, GPS, microphones, and cameras. The emerging paradigm of crowdsensing allows this large number of mobile devices to measure phenomena of common interest, which provides a new societal fashion of data sensing and sharing. A typical crowdsensing application leverages the ubiquitous mobile devices and the pervasive wireless network infrastructure to collect and analyze sensed data far beyond the scale of what was possible before. The incentive mechanism is the most critical concern in the development of mobile crowdsensing. Classic incentive mechanisms attract numerous participants by competitive payment designs. However, to achieve sustainable crowdsensing, advanced incentive mechanisms need to pay attention to not only the payment but also many other designs such as energy conservation and secure communications. Although plenty of incentive mechanisms have been developed for mobile crowdsensing, many challenges still remain to be addressed. It is important to explore this timely research topic to support the promise of crowdsensing in practice.

This Feature Topic (FT) gathers articles from the industrial and research communities on sustainable incentive mechanisms for mobile crowdsensing. The primary goal is to push the theoretical and practical bounds for deeper understanding of fundamental algorithms, modeling, and positioning over the next decade, and analysis techniques from industry and academic viewpoints on these challenges, thus fostering

new research streams to be addressed in the future. After a rigorous review process, six papers have been selected to be published in this March 2017 FT of *IEEE Communications Magazine*.

The first article in this FT, "Congestion-Aware Communication Paradigm for Sustainable Dense Mobile Crowdsensing" by Sun *et al.*, investigates the imbalanced utilization problem of wireless bandwidth resources in mobile crowdsensing, which may exacerbate the communication performance, in particular in areas with high density of users. In order to address the issue, the authors propose a congestion-aware communication paradigm. The proposed paradigm efficiently achieves load balance and reliable communication in mobile crowdsensing.

The second article, "Sustainable Incentives for Mobile Crowdsensing: Auctions, Lotteries, Trust and Reputation Systems" by Luo *et al.*, studies design principles of incentive mechanisms with respect to the sustainability issue. It covers a wide spectrum of incentive mechanisms including auctions, lotteries, trust and reputation systems, as well as some potential mechanisms such as games, contract theory, and market-driven mechanisms.

The next article, "A Location-Based Mobile Crowdsensing Framework Supporting Massive Ad Hoc Social Network Environment," describes a framework that can create an ad hoc social network of millions of people and provide context-aware serious game services as an incentive. While interacting with different services, the massive crowd shares a rich trail of geo-tagged multimedia data, which acts as a crowdsourcing eco-system. This framework can solve many

real-life problems such as reaching a person in a crowd within the shortest possible time, isolating significant events, and finding lost individuals.

In order to increase participation in mobile crowdsensing, the fourth article, “Promoting Cooperation by Social Incentive Mechanism in Mobile Crowdsensing,” develops a social incentive mechanism to incentivize the social friends of the existing participants. The proposed mechanism can be applied to various scenarios where the contributions to the quality of sensing among participants are mutually dependent. Moreover, the authors provide a case study to illustrate that the proposed mechanism is more cost-effective than the traditional incentive mechanism.

Motivated by inadequate sensing opportunities with sparse mobile users, “HySense: A Hybrid Mobile Crowd-Sensing Framework for Sensing Opportunities Compensation under Dynamic Coverage Constraint” by Han *et al.*, proposes a hybrid framework which utilizes mobile devices and static sensor nodes to provide uninterrupted sensing service. HySense is designed as a mobile service oriented architecture entailing four stages: recruiting, sensing, uploading, and calibrating, in order to achieve sustainable crowdsensing.

The sixth article, “Enhanced C-RAN Using a D2D Network” by Huq *et al.*, leverages the cloud radio access network (C-RAN) technology to address the issue of exponentially growing data traffic in mobile networks. The authors propose a novel device-to-device (D2D) approach for C-RAN networks such that it can effectively reduce the front-haul delays. In particular, the proposed approach meets the objectives of 5G in terms of latency, capacity, energy efficiency, mobility and cost.

In closing, we would sincerely like to thank all the people who significantly contributed to this FT, including the contributing authors, the anonymous reviewers, and the *IEEE Communications Magazine* publications staff. We believe that the research findings presented in this FT will stimulate further research and development ideas in mobile crowdsensing.

BIOGRAPHIES

LINGHE KONG is currently a research professor in the Department of Computer Science and Engineering at Shanghai Jiao Tong University, China. Before that, he was a postdoctoral researcher at Columbia University, McGill University, and Singapore University of Technology and Design. He received his Ph.D. degree from Shanghai Jiao Tong University. His research interests include software defined wireless networks, sensor networks, mobile computing, the Internet of Things, and smart energy systems.

KUI REN [F] is a professor of computer science and engineering at the State University of New York at Buffalo. He received his Ph.D. degree from Worcester Polytechnic Institute. His current research interests span cloud and outsourcing security, wireless and wearable systems security, and mobile sensing and crowdsourcing. Kui is a Distinguished Lecturer of IEEE, a member of ACM, and a past board member of the Internet Privacy Task Force, State of Illinois.

MUHAMMAD KHURRAM KHAN [SM] is currently working as a full professor at King Saud University, Kingdom of Saudi Arabia. He is the Editor-in-Chief of *Springer Telecommunication Systems* and full-time Editor/Associate Editor of several ISI-indexed international journals/magazines. His research areas of interest are cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management. He is a Fellow of the IET, the BCS, and the FTRA.

QI LI received his Ph.D. degree from Tsinghua University. Now he is an associate professor of the Graduate School at Shenzhen, Tsinghua University. He has worked at ETH Zurich, UTSA, CUHK, Chinese Academy of Sciences, and Intel. His research interests are in network and system security, particularly in Internet security, mobile security, and security of large-scale distributed systems. He is currently an Editorial Board member of *IEEE TDSC*.

AMMAR RAYES received his Ph.D. degree in electrical engineering from Washington University, St. Louis, Missouri. He is currently a Distinguished Engineer at Cisco Systems, San Jose, California. He is the Founding President of the International Society of Service Innovation Professionals. He is an Editor-in-Chief of the *Advances of Internet of Things Journal*. He was a recipient of the Outstanding Graduate Student Award in Telecommunications at Washington University.

MÉROUANE DEBBAH [F] received his Ph.D. degree from Ecole Normale Supérieure de Cachan. Currently, he is the vice-president of Huawei France R&D and director of the Mathematical and Algorithmic Sciences Lab. His research interests lie in fundamental mathematics, algorithms, statistics, and information and communication sciences research. He is a WWRF Fellow and a member of the academic senate of Paris-Saclay.

YUICHI NAKAMURA received his Ph.D. from the Graduate School of Information, Production and Systems, Waseda University, in 2007. He is currently a general manager at Green Platform Research Labs, NEC Corp. He is also a guest professor with the National Institute of Informatics and a Chair of IEEE CAS Japan Joint Chapter. He has more than 25 years of professional experience in electronic design automation, network on chip, signal processing, and embedded software development.

Congestion-Aware Communication Paradigm for Sustainable Dense Mobile Crowdsensing

Wen Sun and Jiajia Liu

It is of great necessity to consider the imbalanced utilization of wireless resources in the design of a communication paradigm in mobile crowdsensing to meet the stringent QoS requirements. To this end, the authors propose a congestion-aware communication paradigm for sustainable dense mobile crowdsensing in order to achieve efficient load balancing and reliable communication in mobile crowdsensing.

ABSTRACT

Mobile crowdsensing, as an emerging sensing paradigm, relies significantly on wireless communication networks to provide QoS guaranteed data transmission among smartphone users on phenomena of common interest. The explosively growing number and varieties of smartphones impose heavy burdens on the communication infrastructures of mobile crowdsensing. The communication performance of crowdsensing may deteriorate in some high-density areas due to the overwhelming communication requests, while the wireless bandwidth in other areas may not be fully utilized with sporadic and infrequent communication requests. Therefore, it is of great necessity to consider the imbalanced utilization of wireless resources in the design of a communication paradigm in mobile crowdsensing to meet the stringent QoS requirements. To this end, in this article we propose a congestion-aware communication paradigm for sustainable dense mobile crowdsensing in order to achieve efficient load balancing and reliable communication in mobile crowdsensing.

INTRODUCTION

Mobile crowdsensing, as an emerging sensing paradigm, enables individuals or communities to sense and share their local information about phenomena of common interest, based on ever more capable smartphones with a rich set of embedded or accessible sensors and powerful communication capabilities. In mobile crowdsensing, besides a great variety of applications (e.g., environmental monitoring, transportation, human behavior study), wireless communication is of significance to realize mobile pervasive data exchange and data processing.

The explosive growth in the number and capabilities of smartphones makes mobile crowdsensing an unprecedented dense large-scale sensing paradigm, resulting in heavy burdens on wireless communication networks. According to Ericsson's mobility report [1], the number of global smartphone users had already reached 3.2 billion in 2015. By 2021, there will be 6.3 billion smartphone users worldwide, without taking into account other portable smart devices. In the meantime, a great variety of embedded and accessible sensors are available for mobile devices, which generate huge amounts of data. For instance, the *Samsung Galaxy S5* has at least 14 different embedded sensors including accelerator, gyroscope, magnetometer, proximity sensor, light sensor, barometer, heart rate

monitor, fingerprint sensor, microphone, and camera. Based on the mobile data forecast from Cisco [2], global mobile data will exceed 30 exabytes per month by 2020.

The existing wireless communication technologies and paradigms are unable to provide enough bandwidth and coverage to the huge number of mobile devices in dense mobile crowdsensing. For instance, in multimedia applications, each YouTube user will upload data with an average data rate of 5.6 Mb/s for a high resolution video stream. Even the metro network with 100 Gb/s links developed by Verizon is only able to support 18,000 users, which is a quite limited number in a large-scale mobile crowdsensing application [3].

New communication technologies and paradigms have been developed for the next generation of wireless networks, and paradigms typically fall into three categories: centralized communication, opportunistic communication, and device-to-device (D2D)-enabled communication. The centralized communication paradigm, as the most widely used paradigm, requires each mobile user to connect with the service provider for contribution or consumption [4, 5]. It provides reliable transmission, but cannot fully utilize the channel capacity. The opportunistic communication paradigm enables data transmission among mobile users through intermittent connections when they are in short range of each other. It works well in delay-tolerant scenarios where network communication is expensive or unavailable [6]. The D2D-enabled communication paradigm enables direct communication of two mobile users with the assistance of the infrastructure. However, these communication paradigms cannot be applied directly in real-time dense crowdsensing applications due to the specific characteristics of mobile crowdsensing, such as the stringent and various requirements on quality of service (QoS), privacy, budgets, and so on. For example, some real-time required scenarios, such as cloud game systems, have strict delay limitations on interaction, and users with multimedia data processing need traffic transmission at low expense.

Imbalanced utilization of wireless resources is another important characteristic in mobile crowdsensing. Particularly, mobile users are likely to congregate in some areas, such as taxi waiting points, shopping malls, and central business district streets during rush hour, while in other areas, mobile users may be sporadic. This leads to imbalanced usage of the wireless communi-

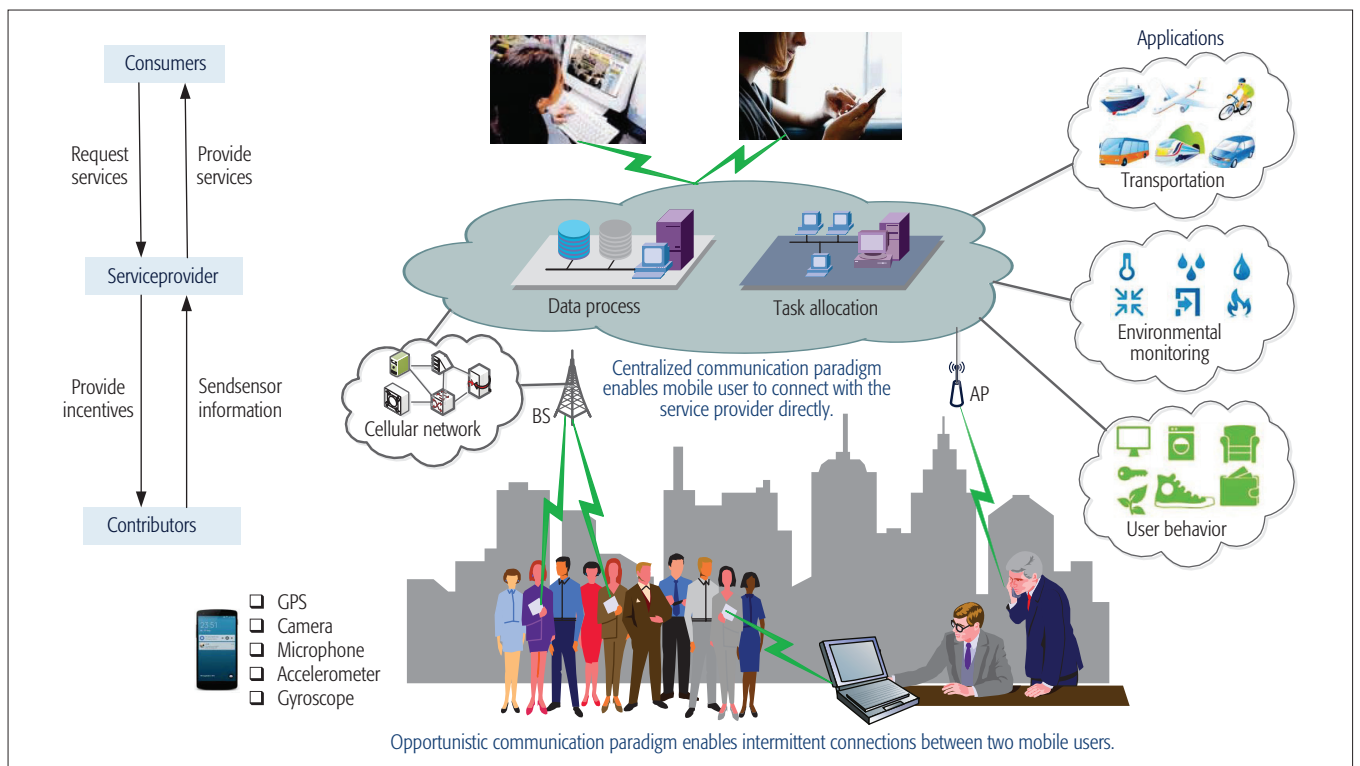


Figure 1. Illustration of the architecture of mobile crowdsensing. Contributors submit their sensor data to the service provider for data processing and task allocation, which in turn provides services to consumers. The applications include transportation, environmental monitoring, and user behavior study.

resources where some base stations (BSs) are overwhelmed with massive communication requests while others have sporadic connections. Therefore, it is of great necessity to design a reliable communication paradigm considering the load balancing problem in mobile crowdsensing. However, few works have considered the load imbalance in dense mobile crowdsensing, taking advantage of the wisdom of crowds. In this article, we propose a congestion-aware D2D-enabled incentive framework to achieve efficient load balancing and provide real-time reliable communications in mobile crowdsensing.

The remainder of this article is organized as follows. We overview the basics and the existing communication paradigms of the mobile crowdsensing system. We propose a congestion-aware communication paradigm. Preliminary numerical results are shown. Finally, we conclude the article.

COMMUNICATION PARADIGM FOR DENSE MOBILE CROWDSENSING

BASICS OF MOBILE CROWDSENSING

Figure 1 shows the typical architecture of mobile crowdsensing, which consists of three entities: contributor, consumer and service provider. The service provider processes and aggregates data from contributors, and provide services to consumers [7]. Typically, the consumers request the service provider for a sensing task with the specific requirements and the remuneration they would like to pay. The service provider publishes the sensing task according to the consumers' demand (i.e., the content and requirement of the sensing task), such as accuracy and coverage, as well as price [8]. The contributors decide whether to

participate in the sensing task depending on the price the service provider offers and the sensing cost in terms of time consumption, mobile data charge, battery consumption, and so on. There is a negotiation process on pricing between the contributors and the service provider, which is referred to as the incentive process. Then, after that process, the service provider serves the consumers. In some cases, the roles of consumers are negligible, and contributors work toward an overall objective instead of separate objectives for each consumer, such as enlarging the overall sensing coverage [9]. In general, "mobile user" is used as a general term that refers to either a contributor or a consumer.

Wisdom of crowds: One of the generic characteristics of crowdsensing is to fuzzify the wisdom of crowds, which reveals that the aggregation of information from a group of people often results in better decisions than those made by a single person. Moreover, crowds may move around driven by incentives, which means that given appropriate incentives, the spatial distribution of mobile nodes (i.e., mobile users) could be changed. However, the involvement of crowds may bring uncertainty in data gathering, as the willingness of humans is quite complex depending on user profiles. Thus, we need to consider user profiles when designing an incentive scheme and try to take advantage of the wisdom of crowds to assist the communication paradigm.

Traffic imbalance: In urban environments, driven by social reasons, crowds are likely to congregate together in some areas (e.g., taxi waiting points, shopping malls), while in other areas, mobile users may be sporadically present. From the perspective of networks, the mobility of

Communication paradigm	Reference	Application description	Application category	Real-time	Dense users	Traffic balancing
Centralized communication paradigm	Zhou <i>et al.</i> [11]	Bus arrival time prediction system based on mobile crowdsensing	Transportation	Yes	No	No
	Mahali project [5]	Use GPS signals that penetrate ionosphere for weather monitoring	Environmental monitoring	Yes	No	No
	QueueSense [12]	A queuing recognition system to help users to plan their routes	User behavior study	Yes	Yes	No
Opportunistic communication paradigm	Ma <i>et al.</i> [6]	Discover geographic characteristics from Twitter	User behavior study	No	No	No
	LifeTie [14]	Exploit opportunistic collaboration of pedestrians for hikers' safety	User behavior study	No	No	No
	Sun <i>et al.</i> [15]	A practical and optimized communication mechanism for direct phone-to-phone data transfer	User behavior study	Yes	No	No

Table 1. The communication paradigms of mobile crowdsensing in various applications with different communication considerations.

crowds leads to traffic imbalance in wireless network resource allocations. In a congested area, some communication requests may not be served in time, resulting in performance deterioration. Imbalanced traffic load is time-variant as the social reasons may vary dynamically. Thus, a feasible communication paradigm should be adaptive to the congestion situation.

COMMUNICATION PARADIGMS IN MOBILE CROWDSENSING

Communication paradigms in mobile crowdsensing typically fall into three categories: centralized, opportunistic, and D2D-enabled. Table 1 summarizes some existing works on communication paradigms in mobile crowdsensing in terms of application categories, the requirements of real time and density, and the consideration of imbalanced network resources.

Centralized Communication Paradigm: The centralized communication paradigm, as the most widely used paradigm for mobile crowdsensing, enables each mobile user to connect to the service provider for contribution or consumption [10, 11]. The service provider aggregates the data from contributors for crowd wisdom and service delivery. Typically, the centralized communication paradigm fits large-scale and real-time applications where communication infrastructures are well developed and deployed. In the case of imbalanced traffic load, the centralized communication paradigm cannot work well.

Li *et al.* [12] presented QueueSense, a queuing recognition system, to help users detect the waiting time in public places (e.g., supermarkets, amusement parks). QueueSense clients on smartphones provide automatic queuing recognition and deliver this information to the service provider, which detects queuing behavior in various scenarios. The system follows the centralized communication paradigm, where the service provider operates a platform that connects an indefinite number of consumers to an indefinite number of contributors. The relevance between the contributors and consumers are learned by the service provider, which then incentivizes the contributors according to the requirements of the consumers.

In large-scale mobile crowdsensing, where the communication infrastructure may not provide reliable communication service to all the mobile users, Hachem *et al.* [13] proposed an approach to decrease the participation of mobile users given sufficient accuracy of the collected information. Only a subset of mobile users is allowed to

contribute their sensing data when other devices, capable of providing similar data, are in the presence of overlapping locations.

Opportunistic Communication Paradigm: The opportunistic communication paradigm leverages the mobility of crowds to communicate with each other and share data messages during their interaction time. This paradigm can be applied in some scenarios where network communication is expensive or unavailable (e.g., dead spots of network coverage). The advantage of this paradigm is that a centralized communication server or infrastructure is not required, which reduces the workload of cellular networks in dense areas [6]. However, the opportunistic communication paradigm relies on the mobility of crowds, and cannot be applied in delay-intolerant applications.

The opportunistic communication paradigm has been deployed in disaster rescue applications, where network coverage is poor. Chen *et al.* [14] presented LifeTie, a prototype of a social-network-inspired mobile crowdsensing application, to ensure hikers' safety. NFC tags are attached to a mountain as an infrastructure. Hikers on the mountain trigger NFC tags nearby in the range of a few inches using their NFC-enabled mobile phones to check if there is any shelter nearby or leave a message for rescue. However, the deployment and maintenance of NFC tags on mountains are difficult, especially when most hiking areas are deserted. Also, as the NFC tags are not interconnected, the rescue information may not be delivered quickly and effectively.

In order to enable the opportunistic communication between smartphones automatically, Sun *et al.* [15] developed a communication mechanism for direct communication between smartphone users by automatically setting the phones between normal mode and hotspot mode. Results show that the proposed communication solution reduces communication delay time in some specific scenarios, which paved the way for opportunistic communication in mobile crowdsensing.

D2D-Enabled Communication Paradigm: Both the centralized and opportunistic communication paradigms cannot be applied in real-time dense crowdsensing scenarios. The D2D-enabled communication paradigm provides direct and real-time communication between two mobile users with the assistance of the infrastructure. The D2D-enabled communication paradigm is beneficial for large-scale dense crowdsensing, as it could alleviate the workload burdens of communication

infrastructure in dense areas, while providing reliable communication in spite of the opportunistic interactions between two mobile users. Note that the imbalanced workload problem in dense mobile crowdsensing could take advantage of this flexibility and reliability. We propose a congestion-aware D2D-enabled incentive framework to balance the workload of mobile crowdsensing and provide real-time communications.

THE PROPOSED CONGESTION-AWARE COMMUNICATION PARADIGM

In this section, we propose a congestion-aware D2D-enabled communication paradigm for dense mobile crowdsensing in order to alleviate the overloading problem. Assume that in the application area, some eNBs are overwhelmed with massive communication requests (referred to as congested eNBs), while others have infrequent and sporadic connections (referred to as uncongested eNBs). The proposed paradigm aims to offload a requesting mobile user (either a contributor or a consumer without specific remarks) from a congested eNB to an adjacent uncongested eNB through human mobility (step 1) or a D2D-enabled communication (steps 2 and 3).

Figure 2 illustrates an example of steps 1, 2, and 3 of the proposed congestion-aware communication paradigm. The application area is covered by macrocells with picocells. eNBs connect to the service provider. Each eNB gets global knowledge from the service provider about its neighboring eNBs, such as location, the congestion situation of these neighboring eNBs, and the information of their connected mobile users. Contributor 1 is an example of step 1, where the congested eNB1 incentivizes contributor 1 to move to the coverage of uncongested eNB2 to re-establish connection. Contributor 2 shows an example of step 2, where eNB3 incentivizes contributor 2 to work as a relay for contributor 3. In step 3, contributor 4 or contributor 5 in a congested eNB establishes direct communication with consumer 1 or consumer 2.

Step 1. A congested eNB first tries to offload a requesting mobile user to an adjacent uncongested eNB by taking advantage of human mobility. Note that the position of a mobile user could be determined by human willingness. The service provider could incentivize a mobile user to move to another location to contribute data through a specific pico eNB or macro eNB by providing an appropriate incentive. Particularly, when a mobile user requests for connection to a congested eNB, the eNB searches for a neighboring uncongested eNB with the shortest distance from the position of the requesting mobile user. Then the current eNB incentivizes the mobile user to move to the coverage of the target eNB by providing an extra incentive in terms of monetary or credits depending on the deviation distance. In the case of several eNBs with the same deviation distances, the mobile user just determines an eNB according to his/her preference. The service provider calculates the incentive depending on the real-time situation, given the budget limitation of the service provider. As the exact incentive is related to the user profile and congestion situation, we introduce the *congestion factor* here and study the incentive through a case study.

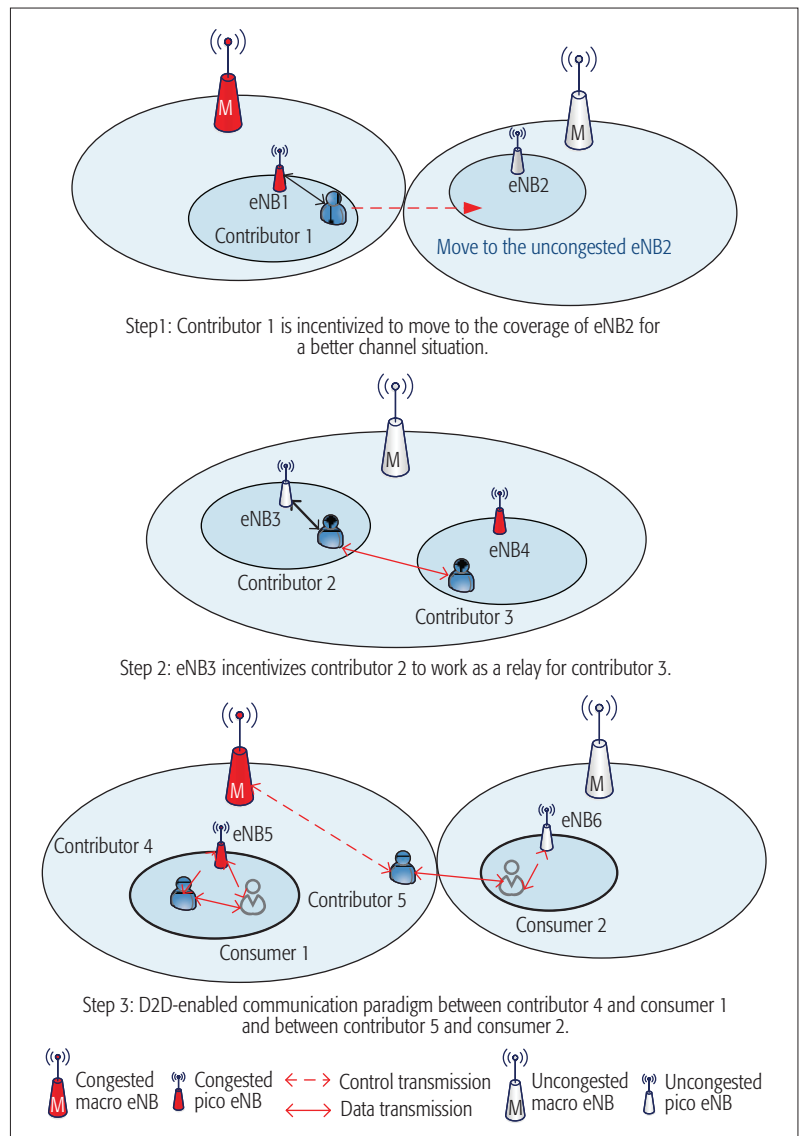


Figure 2. Illustration of steps 1, 2, and 3 of the proposed congestion-aware communication paradigm. Contributor 1 is an example of step 1, where the congested eNB1 incentivizes contributor 1 to move to the coverage of uncongested eNB2 to re-establish connection. Contributor 2 shows an example of step 2, where eNB3 incentivizes contributor 2 to work as a relay for contributor 3. In step 3, contributor 4 or contributor 5 in a congested eNB establishes direct communication with consumer 1 or consumer 2.

We introduce a congestion factor that is proportional with the traffic load of the eNB. The amount of the incentive from an eNB should be inversely proportional to the congestion factor of the eNB, that is, $p_i \propto x_i^{-1}$, where p_i is the payment for user i , and x_i is the congestion factor of the eNB with which user i connects. Although it is inversely proportional with the congestion factor, the exact value is also related to the budget of the service provider, the daily expense of the mobile users and the related consuming time, and the deviation distance.

After the mobile user moves to the coverage of the target eNB, it establishes connections and uploads the sensor data. If mobile users are unwilling to move to another location for the sensing task or step 1 could not achieve the expected performance improvement, the procedure turns to step 2.

Step 2. The congested eNB tries to offload the

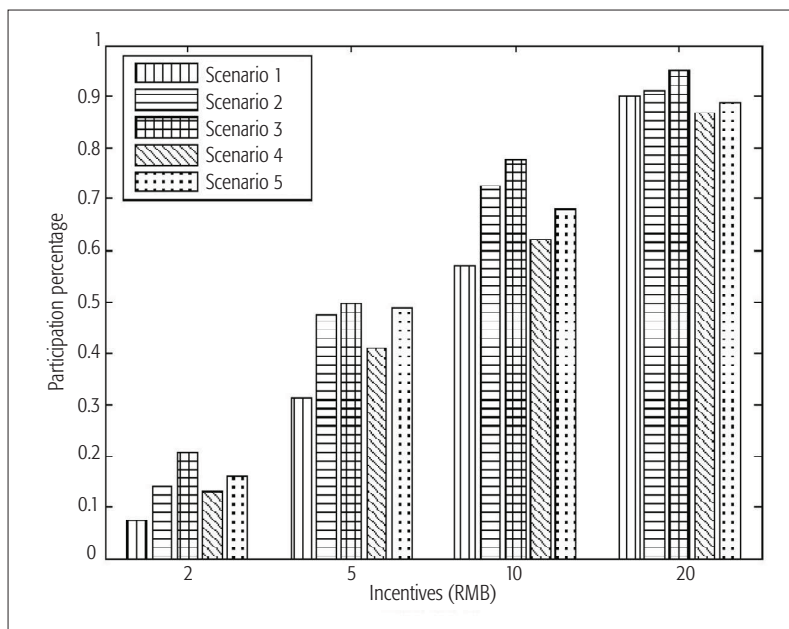


Figure 3. The participation percentage in different congestion scenarios in the case study according to different incentives. Scenarios 1 to 5 are set for students representing 5 different congestion scenarios. Incentives are to pay the student a remuneration of 2, 5, 10, or 20 RMB for the sensing task.

requesting mobile user to an adjacent uncongested eNB by relaying the traffic of the mobile user to an adjacent eNB through another mobile user. Particularly, when an uncongested eNB receives the communication requests from an adjacent congested eNB, it determines the best relay mobile user based on the location of the connected mobile users. Then it encourages the potential relay mobile user to help relay the communications with an appropriate incentive. If the chosen relay accepts the relay request, it responds to the request with a message. Otherwise, the uncongested eNB determines another potential relay for incentive. Then the uncongested eNB informs the congested eNB, and the congested eNB informs the initial mobile user to transmit to the determined relay mobile user.

For the relay nodes, the service provider pays them an incentive to compensate the sensing cost in terms of mobile data charge, battery drain, privacy risk, and inconvenience. The service provider helps establish the control link, while it also provides the privacy protection. In case mobile users are unwilling to work as relays or step 2 could not achieve the expected performance improvement, the procedure turns to step 3.

Step 3. The congested eNB tries to offload the requesting mobile user by establishing direct communication among contributors and consumers. In particular, after the current eNB receives the characteristic information of the mobile users including spatio-temporal information, the service provider matches the requests to find appropriate pairs of consumers and contributors within the coverage. If a consumer happens to request information from a neighboring contributor, the service provider informs the two entities that they could communicate directly. After receiving the control command, the contributor sends the sensor information to the corresponding consumer directly.

Note that as sensor information typically has

spatio-temporal expiration range, it makes sense to establish direct communication between contributors and the corresponding consumers, especially for traffic that does not need the process of the service provider. It is likely that there is an appropriate pair of contributor and consumer in the same vicinity. The channels used by the D2D communication could be reused again some range away in order to improve the spectrum efficiency.

PERFORMANCE EVALUATION

In this section, we present the numerical results of the proposed congestion-aware communication paradigm. Note that incentive for mobile users to move to another location or work as relay (steps 1 and 2) relies heavily on human willingness, and may differ depending on different user profiles in different time periods. We first conduct a case study at the university scale to learn the relevant aspects regarding incentives. After that, we compare the performance improvement brought by each step of the proposed paradigm.

A CASE STUDY ON INCENTIVES FOR THE PROPOSED COMMUNICATION PARADIGM

In the case study, 130 volunteer students at Xidian University are required to complete a sensing task with a certain incentive. The case study lasts for one week. The sensing task asks students to take a photo of a specific item at pre-determined locations. The sensing task may need them to deviate from their planned track and move to another location. Scenarios 1 to 5 are set as different routes to alleviate congestion where the deviation distances in scenarios 1 to 5 are 1200, 600, 180, 530, and 200 m, respectively. For scenarios 1, 2, and 3, students are encouraged to change their usual lunch canteen for an incentive, while scenarios 4 and 5 incentivize the volunteers to move to another location, especially for a sensing task.

Figure 3 shows the participation percentage of the volunteers in the case study who are willing to complete the specific sensing task according to different congestion scenarios. Incentive is set as a remuneration of 2, 5, 10, and 20 RMB for the sensing task according to the board expenses of college students. As can be seen from Fig. 3, the percentage of students who are willing to move to another location for a sensing task changes with the given incentive as well as the deviation distance. Generally, the participation percentage decreases when the route distance increases. It is also noted that it costs less to incentivize a participant to deviate from their regular route for daily needs (e.g., change a lunch location) than that especially for sensing tasks. We also conducted a survey on how much credits could encourage a student to work as a relay. The results show that given twice the mobile charges, 86 percent of students are willing to help deliver others' data for one-time sensing task, and 77 percent for long-term relay services.

NUMERICAL RESULTS

In order to compare the performance improvement brought by each step of the proposed congestion-aware paradigm, we consider a scenario that is covered by macrocells with picocells. The coverage area of a macrocell is assumed to be circles with radius of 200 m, while a picocell

has a radius of 100 m. Each eNB has frequency resources of 50 orthogonal channels. Three hundred mobile users are deployed in the coverage area. Moreover, the maximum distance allowed for D2D communication between a contributor and consumer pair is set to 30 m. The revenue of the service provider is proportional to the addition of the traffic of the contributors minus the cost of incentives. The participation percentage is achieved from the aforementioned case study.

Figure 4 shows the revenue of the service provider in the centralized paradigm, steps 1, 2, and 3 of the proposed congestion-aware scheme. As can be seen, the revenue of the service provider is improved by the proposed scheme. In the centralized paradigm, the revenue of the service provider is fixed, and will not change with the number of users as the available channels are already occupied. Thus, the service provider is unable to allocate a new channel for newcomers. For step 1, the revenue of the service provider is improved as the available channels in the uncongested eNB can be utilized by the users from the congested eNB. The revenue of step 2 is slightly higher than that of step 1 as relay-enabled communication could further utilize the wireless resources of the uncongested eNB, while some mobile users may be unwilling to work as relays due to privacy concerns. Thus, a mobile crowdsensing system shall enhance the privacy measurements and incentives to encourage cooperation. This could be done by employing virtual currency or based on a reputation mechanism. The incentives for mobile users to move to another location or work as relays reduce the revenue of the service provider in steps 1 and 2. The revenue of the service provider in step 3 is significantly improved as frequency channels can be reused, while the cost for incentive is relatively low in step 3.

CONCLUSION

In this article, the communication paradigms in sustainable dense mobile crowdsensing have been investigated. We propose a congestion-based D2D-enabled communication paradigm, which takes advantage of the intelligence of crowds to achieve efficient load balancing and reliable communication in mobile crowdsensing. Since mobile crowdsensing is becoming the mainstream data collection method, it is important to pay more attention to a load balancing scheme leveraging on human intelligence in the future.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (61372073, 61373043, 61202394, 61472367, 61432015, 61601357), in part by China 111 Project (B16037), and in part by the Fundamental Research Funds for the Central Universities (JB161502, XJS16045).

REFERENCES

- [1] Ericsson Mobility Report, <https://www.ericsson.com/res/docs/2016/ericssonmobility-report-2016.pdf>, 2016.
- [2] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015 to 2020 White Paper, tech. rep. <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>, 2016.
- [3] Y. Xiao et al., "Lowering the Barriers to Large-Scale Mobile Crowdsensing," *Proc. ACM HotMobile '13*, 2013.

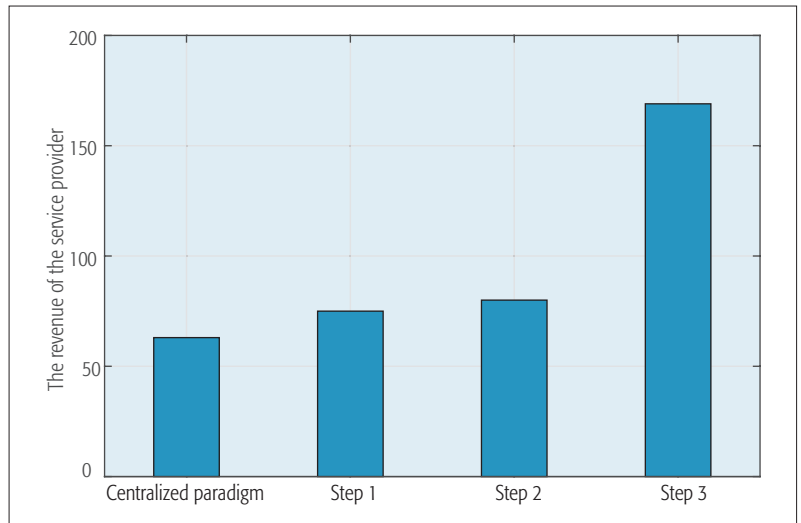


Figure 4. The revenue of the service provider for the scheme without offloading consideration, comparing that of steps 1, 2, and 3 of the proposed congestion-aware communication paradigm.

- [4] Y. Lu, S. Xiang, and W. Wu, "Taxi Queue, Passenger Queue or No Queue?" *Proc. EDBT'15*, 2015.
- [5] V. Pankratius et al., "Mobile Crowd Sensing in Space Weather Monitoring: the Mahali Project," *IEEE Commun. Mag.*, vol. 52, no. 8, Aug. 2014, pp. 22–28.
- [6] H. Ma, D. Zhao, and P. Yuan, "Opportunities in Mobile Crowd Sensing," *IEEE Commun. Mag.*, vol. 52, no. 9, Sept. 2014, pp. 29–35.
- [7] D. Yang, G. Xue, and X. Fang, "Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing," *Proc. ACM MobiCom '12*, 2012.
- [8] J. Lee and B. Hoh, "Sell Your Experiences: A Market Mechanism Based Incentive for Participatory Sensing," *Proc. IEEE PerCom '10*, 2010.
- [9] L. Kong et al., "Surface Coverage in Sensor Networks," *IEEE Trans. Parallel and Distrib. Systems*, vol. 25, no. 1, 2014, pp. 234–43.
- [10] T. Kumrai et al., "An Incentive-Based Evolutionary Algorithm for Participatory Sensing," *Proc. IEEE GLOBECOM '14*, 2014.
- [11] P. Zhou, Y. Zheng, and M. Li, "How Long to Wait? Predicting Bus Arrival Time with Mobile Phone Based Participatory Sensing," *IEEE Trans. Mobile Computing*, vol. 13, no. 6, 2014, pp. 1228–41.
- [12] Q. Li, Q. Han, and L. Sun, "Collaborative Recognition of Queuing Behavior on Mobile Phones," *IEEE Trans. Mobile Computing*, vol. 15, no. 1, 2016, pp. 60–73.
- [13] S. Hachem, A. Pathak, and V. Issamy, "Probabilistic Registration for Large-Scale Mobile Participatory Sensing," *Proc. PerCom '13*, 2013.
- [14] P. Chen et al., "When Crowdsourcing Meets Mobile Sensing: A Social Network Perspective," *IEEE Commun. Mag.*, vol. 53, no. 10, Oct. 2015, pp. 157–63.
- [15] X. Sun et al., "Participatory Sensing Meets Opportunistic Sharing: Automatic Phone-to-Phone Communication in Vehicles," *IEEE Trans. Mobile Computing*, vol. 15, no. 10, 2015, pp. 2550–63.

BIOGRAPHIES

WEN SUN [S'11, M'16] (sunwen@xidian.edu.cn) is currently an associate professor with the School of Cyber Engineering, Xidian University. She received her Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2014, and her B.E. degree from Harbin Institute of Technology in 2009. Her research interests cover a wide range of areas including body sensor network, IoT, participatory sensing, and 5G.

JIAJIA LIU [S'11, M'12, SM'15] (liujiajia@xidian.edu.cn) is currently a full professor at the School of Cyber Engineering, Xidian University. His research interests cover wireless mobile communications, FiWi, IoT, and more. He has published more than 50 peer-reviewed papers in many prestigious IEEE journals and conferences, and currently serves as an Associate Editor for *IEEE Transactions on Communications* and *IEEE Transactions on Vehicular Technology*, an Editor for *IEEE Network*, and a Guest Editor of *IEEE Transactions on Emerging Topics in Computing* and the *IEEE Internet of Things Journal*. He is a Distinguished Lecturer of IEEE ComSoc.

Sustainable Incentives for Mobile Crowdsensing: Auctions, Lotteries, and Trust and Reputation Systems

Tie Luo, Salil S. Kanhere, Jianwei Huang, Sajal K. Das, and Fan Wu

The authors provide an exposition of design principles of six incentive mechanisms, drawing special attention to the sustainability issue. They cover three primary classes of incentive mechanisms: auctions, lotteries, and trust and reputation systems, as well as three other frameworks of promising potential: bargaining games, contract theory, and market-driven mechanisms.

ABSTRACT

Proper incentive mechanisms are critical for mobile crowdsensing systems to motivate people to actively and persistently participate. This article provides an exposition of design principles of six incentive mechanisms, drawing special attention to the sustainability issue. We cover three primary classes of incentive mechanisms: auctions, lotteries, and trust and reputation systems, as well as three other frameworks of promising potential: bargaining games, contract theory, and market-driven mechanisms.

INTRODUCTION

Mobile crowdsensing (MCS) is a new crowdsourcing technique that exploits the sensing capabilities of personal mobile devices, such as smartphones and wearables, to collect data from a large group of individuals. It is advantageous in low deployment cost and vast geographic coverage, and has found numerous applications in diverse domains including transportation, environment monitoring, smart city, and pervasive healthcare. However, MCS systems often face the challenge of *insufficient participation* due to two reasons:

- Sensing incurs nontrivial costs to participants in terms of battery consumption, mobile data usage, time, and effort.
- Sensor-data collection may not have direct benefit to participants, but often requires long-term commitment.

Therefore, designing proper *incentive mechanisms* is pivotal to motivate the crowd to participate in and sustain MCS.

This tutorial article provides an exposition of six incentive mechanisms (Fig. 1) that can be applied to MCS. This area of study is fascinating due to its interdisciplinary nature: auctions and lotteries are deeply rooted in microeconomics, while trust and reputation systems are a subject of artificial intelligence by tradition; bargaining games, contract theory, and market-driven mechanisms all sit on the boundary between economics and computer science. This article elaborates the first three mechanisms in length due to their wide adoption in the literature, but we also summarize the salient technical features of the other three because of their promising potential.

Compared to its predecessor, *crowdsourcing*, MCS shares many characteristics with it, but at the same time has several unique features. MCS typically involves *location dependency* (geo-tagged data) and *temporal continuity* (collecting data continuously over an extended period), and each individual worker only participates in a few *micro-tasks*. These features have significant impact on the incentive mechanism design, which we elaborate. In particular, the temporal continuity also engenders the *sustainability* issue, where workers may not follow through the entire campaign but drop out in the interim. This is under-explored in the literature and is one of the foci of this article. A broader scope of sustainability, which encompasses other topics such as energy efficiency, security, and privacy, warrants several other lines of rigorous research.

PRELIMINARIES OF MECHANISM DESIGN

Mechanism design concerns stipulating a set of rules such that players will act to the designer's preference. Therefore, mechanism design is also known as *reverse game theory*, since game theory concerns reasoning about players' strategy choices given a set of rules.

However, the space of designing the set of rules appears to be infinite, making the problem seemingly intractable. This issue was remarkably alleviated due to the introduction of the *revelation principle*, which says that any arbitrary mechanism can be replicated by an *incentive-compatible direct mechanism*. Here, a direct mechanism is one in which players directly tell their *types* (i.e., *private information* such as cost) to the designer, and is incentive-compatible (IC) if truth-telling is optimal for every player. Thus, the revelation principle allows us to restrict our attention to direct mechanisms only, which are a much smaller class compared to the original design space. Another important property that needs to be satisfied by a mechanism is individual rationality (IR), which means that one should only gain or maintain his/her utility by participating.

In practice, a player's type is often unknown to other agents and the mechanism designer, who hence have to reason about the unknowns using prior (often probabilistic) beliefs. This is called an *incomplete-information* setting and is dealt with by *Bayesian mechanism design*.

The classic mechanism design theory, which is rooted in economics, focuses on characterizing the existence and uniqueness of equilibria. Its recent marriage with computer science gave birth to the theory of *algorithmic mechanism design*, which focuses more on how to reach a desired equilibrium through polynomial-time algorithms with an emphasis on *computational efficiency*.

AUCTION

Auction is one of the most widely used incentive mechanism design frameworks in MCS. A standard auction consists of an auctioneer who sells some goods and a group of bidders who place bids to buy the goods. The auctioneer determines:

- An *allocation rule*, which specifies “who gets what,” that is, who win the auction and what goods are allocated to them
- A *payment rule*, which dictates “who pays how much”

A classic example is a *Vickrey auction*, where there is a single good, and the allocation rule is that the highest bidder gets the good, and the payment rule is that the highest bidder pays the second-highest bid. While seemingly simplistic, Vickrey auction possesses three very desirable properties: dominant-strategy incentive-compatibility, maximal social welfare, and computational efficiency.

When auctions are applied to MCS, the buyer and seller roles are often swapped: the bidders are now mobile users or *workers* who want to *sell* sensory data, and the auctioneer *buys* sensory data from them. This is often referred to as a *reverse auction* model, in which the allocation rule determines the winners (who are qualified to sell data), and the payment rule determines the size of payment to each winner.

Standard auctions can be categorized into *winner-pay* and *all-pay* auctions according to who pays the bids. To allow this taxonomy to also cover reverse auctions, we generalize “paying” bids to “fulfilling” bids. Thus, fulfilling a bid in standard auctions means paying one’s bidding price, and in reverse auctions means surrendering a selling item. In MCS, the latter corresponds to completing a sensing task or submitting sensor data.

WINNER-PAY AUCTIONS

In a winner-pay auction, only the winners (selected by the allocation rule) need to pay or fulfill the bids. This conforms to intuition and has been widely applied in the MCS literature.

For example, in [1], n participants bid their respective desired payments b_i for performing a sensing task requested by a service provider. The service provider (i.e., auctioneer) implements:

- An allocation rule that selects the lowest m out of the n bidders as the winners
- A payment rule that pays the m winners their respective bids b_i

This is essentially a first-price sealed-bid auction that does not satisfy IC, as a bidder could overbid ($> c_i$ where c_i is his/her true sensing cost) and gain higher payoff.

However, what is interesting in [1] is how the issue of *sustainability* is addressed. The authors observed that, as winner selection is based on b_i , which is lower bounded by c_i , the auction tends to separate participants into constant winners and

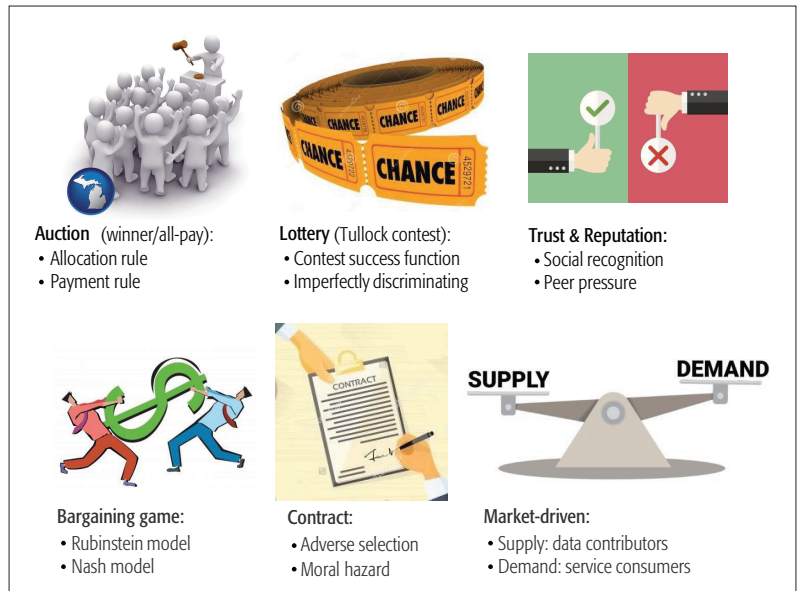


Figure 1. Six incentive mechanism frameworks with their key elements.

losers according to their c_i after multiple rounds. Thus, the loser group may start to *drop out* as they would see little chance to win. The resultant shrinking participant pool would then induce the winners to increase bids, which implies a higher cost to the service provider and impact the sustainability of the campaign.¹ To solve this problem, [1] gives “virtual participation credit” α to each losing participant after each round, such that his/her bid b_i in the next round will be treated as $b'_i = b_i - k_i\alpha$, where k_i is the number of his/her consecutive losing rounds. Hence, a loser gets a higher chance to win subsequently while his/her payment remains b_i .

Another winner-pay auction that specifically addresses sustainability is [2], which selects winners by combining their locations (for better geographic coverage) and reported sensing costs. To provide long-term incentives, the auction aims to satisfy a *participatory constraint*: the average frequency that a user is selected must be no less than his/her “dropout threshold.” Unlike [1], the auction [2] satisfies the IC constraint by adopting a *VCG auction*.

A VCG auction is an extension of the classic Vickrey auction for selling multiple goods, which corresponds to allocating multiple sensing tasks in MCS. A VCG auction allocates goods to the set of bidders whose bids maximize the social welfare (total goods value); in MCS, this means allocating tasks to workers whose sensing costs minimize the total cost. As for the payment rule, each bidder i pays his/her *externality*, that is, the maximum welfare if i were absent minus the current welfare (when i is present) of others.

ALL-PAY AUCTIONS

In an all-pay auction (APA), all the bidders need to pay or fulfill the bids regardless of who wins the auction. This appears to be unnatural, and indeed, APA is rarely used in practice for selling traditional goods. But in fact, it exists in reality pervasively, but in a nonobvious form. For example, in political campaigns, job promotions, R&D competitions, and sports, all candidates exert vast effort

¹ Strategic workers could do better by *underbidding* in earlier rounds so as to “elbow out” other workers and, thereafter, increase bids to gain higher payoff in the long run. However, in reality, workers are generally *myopic*, as also (implicitly) assumed by [1].

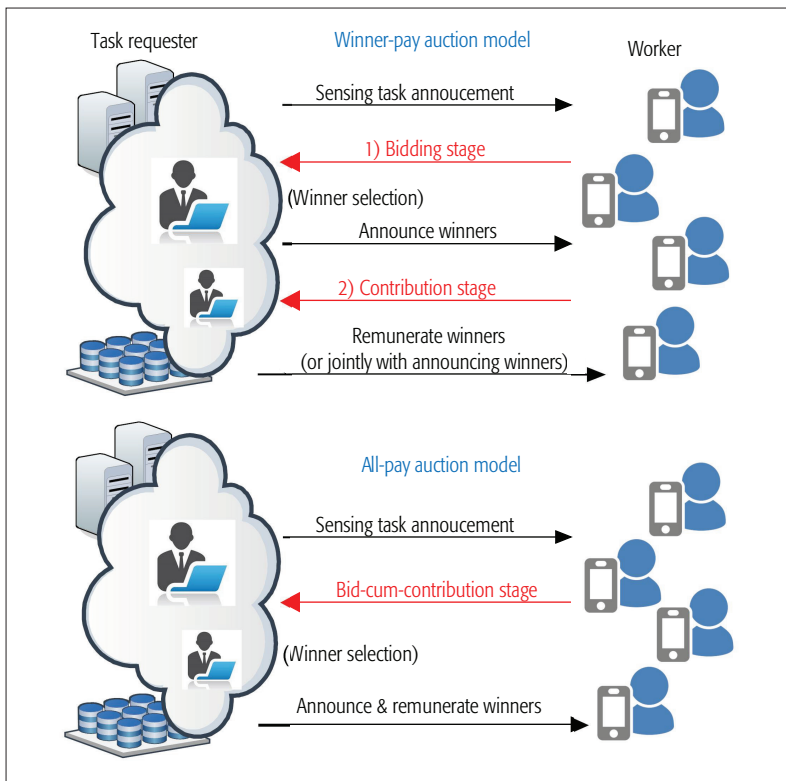


Figure 2. Winner-pay auction vs. all-pay auction in MCS.

(fulfilling bids) without knowing who will eventually win the competition. The theoretical foundation of APA is based on the notion of *expected utility*, which incorporates a *winning probability* into the utility function and thereby makes all-pay equivalent to winner-pay auctions in principle.

The first work that applies APA to MCS is [3], where the APA is conducted as follows. After a task requester announces a sensing task, interested workers can straightaway participate in performing the task (e.g., move to specific locations and collect sensor data). Upon completion of the task (or after a predefined period), the task requester selects a winner based on performance (amount/quality of collected sensor data) and rewards him/her. This is all-pay since non-winners have also surrendered their sensing data (and effort).

Compared to the winner-pay genre, APA has three desired advantages, as partially covered in [4]. The first is *simplicity*. A winner-pay auction consists of two stages (Fig. 2): a *bidding stage* in which bidders submit bids to indicate their *intent* to participate (e.g., how much sensor data to collect and how much payment they desire) and a *contribution stage* in which only the winners (a subset chosen from all the bidders) perform the sensing task. In contrast, an APA compresses these two stages into a single *bid-cum-contribution stage*, in which all workers contribute straightaway without bidding their intent. For a requester, such an MCS campaign is simpler to organize. For workers, they no longer need to contrive a plan or intent just for doing a micro-task like sensor data collection; rather, they can quickly start and then “plan on the go” (e.g., the amount of data). This offers more flexibility and is better suited to the ad hoc and “micro-task” based nature of MCS.

The second advantage is *risk-free* of bid non-fulfillment. Since a bid in winner-pay auctions is merely an intent to participate, there is little guarantee that the winning bids selected in the first stage will be fulfilled in the second stage. On the other hand, bids in APA are all fulfilled upfront (as actual contributions), which nullifies the risk.

The third advantage is *obliviousness to truthfulness*. This is a special merit when applying APA to MCS, as APA does not exhibit it by itself. This merit says that IC, which is a main challenge in mechanism design, is technically irrelevant to all-pay MCS. The reason is that both the allocation and payment rules of all-pay MCS are no longer based on bids of intent but on bids of actual contributions, which are directly observable and cannot be lied about. This liberates mechanism designers from the IC constraint and allows them to focus on other important goals such as revenue maximization, IR, and computational efficiency.

However, APA also has a disadvantage, which is more of a psychological rather than a technical one. That is, although the fact that APA entails a *sunk cost* to every bidder makes no mathematical difference in terms of *expected utility*, it demands the bidders to be fully *rational*. More specifically, APA can only guarantee nonnegative payoff *in expectation* but not on every *realization*, unlike winner-pay auctions. In other words, APA offers a weaker “sense of security” to workers. One remedy is to employ behavioral economics and marketing strategies, as suggested by [4].

Table 1 summarizes the above comparison.

SUSTAINABILITY

As mentioned earlier, the temporal continuity of MCS causes a critical sustainability issue in which participants may drop out due to lack of long-term commitment. One way to retain participants is to run the original “grand” auction in multiple iterations, each over shorter periods, such that the remuneration cycle is reduced and more winners can be selected. However, under such a scheme, many workers may keep losing successive rounds and thus still quit in frustration.

Therefore, we suggest three modifications to traditional auction design to improve sustainability. First, redesign the *allocation rule* by determining winners using one of the following:

- The (possibly time-discounted) *cumulative contribution* of each non-winner rather than his/her contribution in the current round alone
- A *discriminatory winning probability*, which is a function of previous losing rounds, such that losers are “subsidized” with higher winning odds subsequently.

Second, redesign the payment rule such that the reward is *adaptive* to the losing history of a winner. An example can be found in [3, 4], which introduce an *adaptive prize* to vary with a winner’s cumulative contribution so that workers are incentivized to contribute more than the case of fixed reward.

Third, although theory shows no definitive advantage between single and multiple prizes in terms of revenue (total contribution) [5], we recommend the use of multiple prizes for MCS. This is because it curbs “starvation,” especially when the crowd size is large, and is user-friendly.

Another feature related to sustainability is the *microscopic nature of MCS tasks*, as mentioned earlier. This feature calls for a *minimal participation procedure*, as otherwise it tends to outweigh the task itself and thereby prompts participants to leave. This advocates an all-pay auction as a more favorable choice due to its one-stage bidding process.

LOTTERY

Auctions have been extensively studied in economics for decades, and (primarily because of that) are widely adopted in the MCS literature as an incentive mechanism. However, a recent critique undertaken by [6] points out that auctions may not always be a good fit for MCS due to their *perfectly discriminating* nature. Intuitively, it means that one must outbid everyone else in order to win; in other words, auctions are so competitive that “weaker” (lower-type) bidders will *never* win. Thus, while auctions could be a superior choice for crowdsourcing that solicits prime quality from strong players, they may not suit MCS well, which aims to engage “grassroots” to perform very simple tasks like sensor data collection, where massive participation is of the foremost priority to achieve a required geographic coverage.

Lottery — or its generalized form *Tullock contest* — is shown by [6] to be a good alternative to resolve this issue. A Tullock contest is a probabilistic game in which the winner is not determined by the rank of bids but by a probability, specified by a contest success function (CSF) $p_i = b_i^r / \sum_j b_j^r$. Here, b_i is bidder i 's bid and r is a constant exponent. When $r = 1$, it yields a lottery, which is the simplest form of Tullock contests.

The most salient feature of Tullock contests is that they are *imperfectly discriminating*: as bids only determine winning probabilities, *everyone has a chance to win*, no matter how “weak” he/she is. This is very attractive to ordinary workers who often constitute the majority of MCS participants, which is not necessarily the case in crowdsourcing in general. Therefore, as evidenced even by reality, many countries run national lotteries in which millions of people participate.

Table 2 summarizes the above comparison, indicating that auction and lottery are two *complementary* mechanisms. When applied to MCS, a typical lottery is conducted in an all-pay fashion, in the sense that all the bids are actual contributions.

Tullock contests are inherently more sustainable than auctions, because imperfect discriminating allows for a more even distribution of winning positions and thereby helps participant retention. To further improve sustainability, one way is to incorporate historical losing records into the bid b_i or the power exponent r in the CSF, such that the CSF gives favorable bias toward persistent losers. Another way is to use the *adaptive payment rule* described earlier, for which [6] provides a detailed reference.

TRUST AND REPUTATION SYSTEMS

Auctions and Tullock contests tend to use financial incentives, which may be less effective when:

- The amount is insignificant (e.g., due to the “micro-ness” of MCS tasks).

	Winner-pay MCS	All-pay MCS
Procedure	Two stages: bidding and contribution	Single stage: bidding cum contribution
Risk of bid nonfulfillment	Yes	No
Has challenge of satisfying IC	Yes	No
Workers' sense of security	Stronger	Weaker
Revenue (total contribution)	Equal (by the <i>revenue equivalence theorem</i> under standard assumptions)	

Table 1. Comparison of winner-pay and all-pay MCS.

	Auction	Lottery/Tullock contest
Winner selection	Perfectly discriminating	Imperfectly discriminating
Competitiveness/barrier to entry	High	Low
Typical size of participant pool	Small	Large
Contribution level from each individual player	High	Low
Suitable applications	Those favoring quality over quantity (e.g., effort/ knowledge-intensive crowdsourcing, contests)	Those favoring quantity over quality (e.g., micro-task crowdsourcing, MCS)
Suitable players	Strong players (who are of higher types)	Ordinary players
Revenue (total contribution)	No conclusive comparison (contingent on problem settings)	

Table 2. Comparison of auction and lottery.

- The task has moral implications (e.g., collecting healthcare-related data for seniors). Another issue is *financial sustainability*, which we address in market-driven mechanisms.

A widely used non-monetary incentive mechanism is trust and reputation systems. Trust is a local and subjective measure of the relationship between two persons/agents, and can be derived from direct or indirect past interactions. Reputation is a global and rather objective measure by aggregating all other people's trust with respect to a particular person. Trust and reputation have enormous influence on *social recognition* and *peer pressure*, and hence are effective and sustaining sources of motivation as backed up by both scientific research and practice (e.g., Quora and Stack-Overflow).

A well-known online trust and reputation system is the *Beta reputation system* [7]. It uses a modified expected value of the Beta distribution to model the extent to which a user i trusts another user j , as $T(i, j) = [g(i, j) - b(i, j)] / [g(i, j) + b(i, j) + 2]$, where $g(i, j)$ and $b(i, j)$ are the number of “good” and “bad” feedbacks i gave to j , respectively. The reputation of j is then an aggregated value of all the feedback combined, that is, $R_j = (g_j - b_j) / (g_j + b_j + 2)$ where $g_j = \sum_i g(i, j)$ and $b_j = \sum_i b(i, j)$.

Trust and reputation can be used in MCS to incentivize workers to contribute more trust-

The sustainability issue arises when some workers constantly fail to achieve an agreement with the requester and fall back to their status-quo payoffs. This can be improved by giving higher bargaining power to “loyal” workers and workers who successively fail.

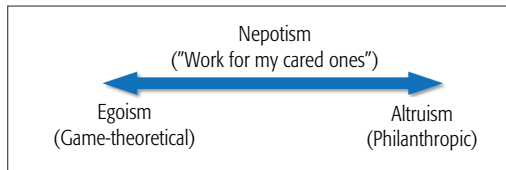


Figure 3. *Nepotism* [9] strikes a trade-off between egoism and altruism, aiming to capture human nature in a more realistic manner.

worthy data. For example in [8], the authors use a fuzzy inference system to determine the trust of contribution, given the quality of contributed data and the trust-of-participant. If the output trust is higher than a threshold, the reputation of the participant will increase, otherwise it will decrease. The reputation is then used as a scaling factor of reward, thereby incentivizing each worker to improve his quality of contribution and to contribute more.

Another trust and reputation based incentive mechanism for MCS is simple endorsement web (SEW) [9]. It is a *social network* that connects participants using an *endorsement* relationship, where Alice endorses Bob if she trusts Bob to be a “good” contributor, or because of benefit derived from nepotism.

Nepotism is a notion introduced by [9] to capture human nature more realistically, striking a trade-off between *egoism* (as assumed by game-theoretical economists) and *altruism* (as argued for by philanthropists and humanitarians). Nepotism states that people could behave in the interest of a specific group of people whom they care about (e.g., family and close social connections), rather than being categorically egoistic or altruistic (Fig. 3).

Nepotism can be used in social-network-based MCS to create incentives. For example, this can be realized by a *revenue-sharing scheme* [9] in which a worker who contributes sensor data and thereby earns a reward (e.g., reputation points) needs to share the reward with his/her endorsers. As a result, endorsers become *beneficiaries* of the contributor. Thus, if (very likely) a contributor is endorsed by some of his/her “nepotic” social connections, a new incentive is created for the contributor: “work for your cared (or loved) ones” (besides yourself).

For completeness (to cover non-nepotic cases as well), endorsement is designed to be a *mutually beneficial relationship*, where a contributor with more endorsers is deemed by SEW as more trustworthy, and will receive higher reward.

Trust and reputation systems are generally more sustainable than monetary incentive mechanisms, due to the void of financial burden and the long-term social influence. On the other hand, a major challenge to trust and reputation systems is the *cold-start problem* (i.e., the difficulty of inferring the trustworthiness of a user during bootstrapping). There is a large literature on this topic, which is out of the scope of this article.

OTHER INCENTIVE MECHANISMS

We discuss three additional incentive mechanisms that are less common in the MCS literature but have great potential nevertheless.

BARGAINING GAMES

A bargaining game concerns how to divide certain surplus (cooperation benefit) between two players. There are two classic bargaining models. The *Rubinstein bargaining model* takes a strategic approach to model the bargaining procedure as a *sequential game*, in which the two players alternately propose offers until one accepts the offer proposed by the other. The *Nash bargaining model* takes an axiomatic approach to focus on deriving an outcome that satisfies certain axioms [10]. Such an outcome is a tuple (r_1, r_2) that maximizes the Nash product, $(u_1(r_1) - u_1(d_1))(u_2(r_2) - u_2(d_2))$, where, r_1 and r_2 are the two players’ shares of the total surplus, respectively, $u_1(\cdot)$ and $u_2(\cdot)$ are their utility functions, and d_1 and d_2 are their status quo payoffs if an agreement is not achieved.

MCS involves multiple workers, and we can apply a bargaining model by letting the task requester bargain with each worker separately while taking into account other workers. Using the Nash model as an example (e.g., [11]), let us suppose a task requester has a sensing task of value v and a worker is interested in undertaking it. The requester wants a share r_1 as profit, and the worker wants a share r_2 as reward, where $r_1 + r_2 \leq v$. If the bargain fails (say with a probability p), they both fall back to their status quo payoffs, which are typically 0 for the worker but can be positive for the requester. The reason is that, with probability $1 - p$, the requester can reach an agreement with one of the other workers. This implies that $d_1 > 0$ and $d_2 = 0$, which then allows us to formulate and optimize the Nash product. Depending on the players’ risk profiles, the utility functions $u_1(\cdot)$ and $u_2(\cdot)$ may be nonlinear.

The sustainability issue arises when some workers constantly fail to achieve an agreement with the requester and fall back to their status quo payoffs. This can be improved by giving higher bargaining power to “loyal” workers and workers who successively fail. One way to achieve this is to generalize the Nash product to $(u_1(r_1) - u_1(d_1))^\alpha (u_2(r_2) - u_2(d_2))^{1-\alpha}$ to create the asymmetric bargaining power case, where $\alpha < 0.5$ gives an advantage to player 2. Another way is to make the worker’s status quo payoff d_2 a function of his/her loyalty or bargaining history.

Moreover, as the bargaining process itself creates no surplus but can be costly, we can improve sustainability by automating the bargaining process using software. This is a non-theoretical tweak but can be very useful in practice.

CONTRACT THEORY

Contract theory [12] deals with two players who take very different roles. One player, called a *principal*, has all the bargaining power and spells out a contract, which may contain a list of contract items. The other, called an *agent*, can only accept or reject the contract or accept a specific contract item, without counter-offering as in bargaining.

There are two main contract models: the *adverse selection* model, in which the agent has certain *hidden information* that the principal tries to elicit, and the *moral hazard* model, in which the agent could exert some *hidden effort* that is of economic value to the principal, and the principal tries to induce a desired effort level at minimal cost.

In the context of MCS, we consider each pairing of a worker and the task requester. In the adverse selection case, the hidden information may be the worker's sensing cost. The requester can offer a menu of contract items, each being a (cost, remuneration) tuple. To induce the worker to pick the contract item corresponding to his/her true sensing cost (i.e., to satisfy IC), the requester needs to pay an *information rent*, which is the difference between the remuneration and the cost. See [13] for an example of how to set the rent. In the moral hazard model, the requester aims to elicit a certain sensing effort from a worker so as to produce a sensing quality that maximizes the data value v minus the worker's remuneration. As the effort is hidden and the quality is not a deterministic function of effort, the optimal contract is an insurance that gives the worker the entire effort-dependent v while requiring the worker to pay a fixed "deductible." However, if the worker is risk-averse, the requester needs to also offer a quality-linked incentive and make a trade-off between incentive and insurance based on the worker's risk profile.

Sustainable contracts can be achieved in two ways. First, the contract can adopt an *installment scheme* rather than one-off payment: only after the worker has collected a certain portion of the total target amount of sensing data (with certain quality) will a corresponding portion of the total remuneration be paid to the worker. This not only motivates workers to follow through the entire campaign, but also shortens their waiting period and curbs impatience. Second, in the adverse selection model, the remuneration can include a bonus component on top of information rent to reward long-term workers; in the moral hazard model, this bonus can be incorporated into either the insurance or the incentive.

MARKET-DRIVEN MECHANISMS

Monetary incentives may encounter *financial sustainability* as mentioned earlier, where constant payments to workers could impose a stringent burden on budget. One solution is market-driven mechanisms, which exploit the supply-demand interaction to create incentives and shed the financial burden from MCS systems.

To run a market-driven mechanism, the MCS system first needs to create a market. Specifically, given that supply is provided by MCS workers, the goal is to create demand (i.e., attract consumers). This can be achieved by:

- Offering a compelling informational service over the collected sensor data (e.g., via data analytics)
- Simply providing the raw data if it bears considerable value to certain users

The next step is to design a market-driven mechanism using one of the following models. In a *fine-grained* model, each service request from a consumer can be mapped to a specific set of data contributions. For example, a consumer may query "the average traffic speed of Road-7 in the past hour." In such cases, the market can distribute the consumer's payment to workers who contributed data to that particular spatio-temporal (S-T) window. As illustrated in Fig. 4, a requester who made a query at S-T point t_1^s pays workers who made the set of contributions $\{q_{(1)}, q_{(2)},$

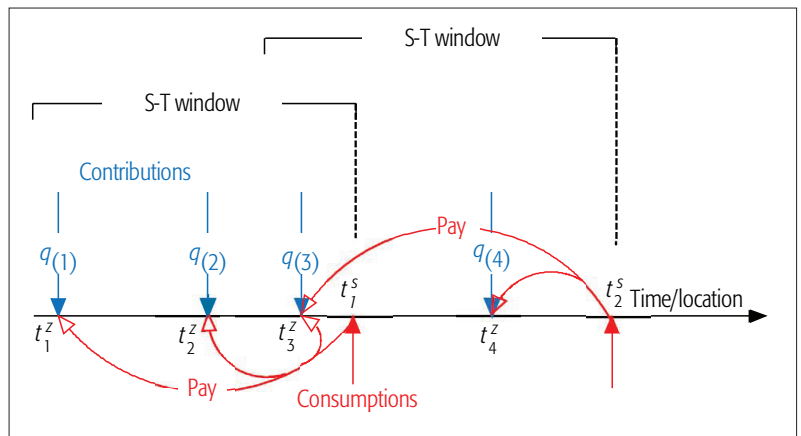


Figure 4. Fine-grained model for market-driven mechanisms [14].

$q_{(3)}$, and a query at t_2^s pays to the set $\{q_{(3)}, q_{(4)}\}$. *Dynamic pricing* [14] can also be integrated to determine the payment to each individual worker.

In a *coarse-grained* model, each consumption is serviced by mining a large set of data or multi-datasets; it is not possible or practical to pinpoint which particular contributions are used and to what extent. Therefore, supply and demand can be calculated on a macro basis using statistical methods to determine pricing and payment distribution.

In both models, it is possible that each user plays a dual role of both data contributor and service consumer. A corresponding incentive scheme is provided in [15], which does not use monetary payments.

Market-driven mechanisms thus improve sustainability by shedding financial burden from the system. They are also advantageous in their inherent ability to regulate *supply imbalance* between popular and unpopular areas, or peak and non-peak hours. This is achieved by charging a higher price to spatiotemporal regions with lower supply but higher demand, and vice versa, which incentivizes workers to move to system-desired regions to perform MCS tasks.

SUMMARY, CHALLENGES, AND OPPORTUNITIES

Is there a rule of thumb as to which incentive mechanism fits which particular MCS applications? The answer is embedded above and summarized here. In general, auctions suit effort/knowledge-intensive applications, while lotteries suit micro-task scenarios. Trust and reputation systems are best when the task has strong moral and social implications, while market-driven mechanisms are a superior choice when the sensing data have great commercial value; both mechanisms have good financial sustainability. Bargaining games suit the situation when workers and the task requester have comparable bargaining power, while contracts are preferred when the task requester dominates the decision making.

While research in the area of incentive mechanism design is rich, the fundamental assumption of human rationality often faces challenges in reality. A relaxation of this assumption is the notion of *bounded rationality*, which has led to rising activities on *behavioral economics*. Another challenge is *collusion* among agents, which significantly complicates the design but meanwhile introduces a very interesting problem to solve. *Heterogene-*

While research in the area of incentive mechanism design is rich, the fundamental assumption of human rationality often faces challenges in reality. A relaxation of this assumption is the notion of bounded rationality, which has led to rising activities on behavioral economics.

ity and *inter-correlation* of agent types pose additional challenges by often precluding closed-form solutions. Moreover, non-quasilinear utility functions and uncertain risk profiles have been much less studied and are worth future exploration.

ACKNOWLEDGMENTS

This work was supported in part by the U.S. National Science Foundation under grants CNS-1545037 and CNS-1545050, in part by the General Research Fund Project CUHK 14206315, and in part by A*STAR Singapore under SERC grant 1224104046.

REFERENCES

- [1] J-S. Lee and B. Hoh, "Sell Your Experiences: A Market Mechanism Based Incentive for Participatory Sensing," *Proc. IEEE PerCom*, 2010, pp. 60–68.
- [2] L. Gao, F. Hou, and J. Huang, "Providing Long-Term Participation Incentive in Participatory Sensing," *Proc. IEEE INFOCOM*, 2015, pp. 2803–11.
- [3] T. Luo, H-P. Tan, and L. Xia, "Profit-Maximizing Incentive for Participatory Sensing," *Proc. IEEE INFOCOM*, 2014, pp. 127–35.
- [4] T. Luo *et al.*, "Incentive Mechanism Design for Crowdsourcing: An All-Pay Auction Approach," *ACM Trans. Intell. Sys. Tech.*, vol. 7, no. 3, 2016, pp. 35:1–26.
- [5] D. Sisak, "Multiple-Prize Contests: the Optimal Allocation of Prizes," *J. Economic Surveys*, vol. 23, 2009, pp. 82–114.
- [6] T. Luo *et al.*, "Crowdsourcing with Tullock Contests: A New Perspective," *Proc. IEEE INFOCOM*, 2015, pp. 2515–23.
- [7] A. Jøsang and R. Ismail, "The Beta Reputation System," *Proc. 15th Bled Electronics Commerce Conf.*, 2002.
- [8] H. Amintoosi and S. S. Kanhere, "A Reputation Framework for Social Participatory Sensing Systems," *Mobile Net. Appl.*, vol. 19, no.1, 2014, pp. 88–100.
- [9] T. Luo, S. S. Kanhere, and H-P. Tan, "SEW-ing A Simple Endorsement Web to Incentivize Trustworthy Participatory Sensing," *Proc. IEEE SECON*, 2014, pp. 636–44.
- [10] A. Muthoo, "Bargaining Theory with Applications," Cambridge Univ. Press, 1999.
- [11] S. He *et al.*, "Toward Optimal Allocation of Location Dependent Tasks in Crowdsensing," *Proc. IEEE INFOCOM*, 2014, pp. 745–53.
- [12] P. Bolton and M. Dewatripont, *Contract Theory*, MIT Press, 2005.
- [13] L. Duan *et al.*, "Motivating Smartphone Collaboration in Data Acquisition and Distributed Computing," *IEEE Trans. Mobile Comp.*, vol. 13, no. 10, Oct. 2014, pp. 2320–33.

[14] C-K. Tham and T. Luo, "Quality of Contributed Service and Market Equilibrium for Participatory Sensing," *IEEE Trans. Mobile Comp.*, vol. 14, no. 4, 2015, pp. 829–42.

[15] C-K. Tham and T. Luo, "Fairness and Social Welfare in Service Allocation Schemes for Participatory Sensing," *Computer Networks*, Elsevier, vol. 73, 2014, pp. 58–71.

BIOGRAPHIES

TONY T. LUO is a programme lead, scientist, and principal investigator at I2R, A*STAR Singapore. He received his Ph.D. in electrical and computer engineering from the National University of Singapore. He was a Best Paper Award recipient at ICTC 2012 and a Best Paper Award nominee at IEEE INFOCOM 2015. He has served as Program Chair for several conferences and Guest Editor for several journals, and delivered a tutorial at IEEE ICC 2016.

SALIL KANHERE [SM] is an associate professor at the University of New South Wales, Australia. He received his Ph.D. from Drexel University. His research interests include pervasive computing, crowdsourcing, the Internet of Things, privacy, and security. He has published over 150 peer-reviewed articles and delivered over 20 tutorials and keynote talks on these research topics. He is a Senior Member of ACM. He was a recipient of the Humboldt Research Fellowship in 2014.

JIANWEI HUANG [F'16] is an associate professor in the Department of Information Engineering at the Chinese University of Hong Kong. He has received eight international Best Paper Awards, including the IEEE Marconi Prize Paper Award in Wireless Communications 2011. He has co-authored five books, including the textbook *Wireless Network Pricing*. He has served as the Chair of IEEE TCCN and MMTTC. He is an IEEE ComSoc Distinguished Lecturer and a Thomson Reuters Highly Cited Researcher.

SAJAL K. DAS [F] is the chair of the Computer Science Department and Daniel St. Clair Endowed Chair at Missouri University of Science and Technology. His current research includes crowdsensing, incentive mechanisms, wireless sensor networks, cyber-physical systems, smart healthcare, smart grid, and mobile and pervasive computing. He has a Ph.D. in computer science from the University of Central Florida.

FAN WU is an associate professor at Shanghai Jiao Tong University. His research interests include wireless networking and mobile computing. He has published more than 100 peer-reviewed papers in technical journals and conference proceedings. He is a recipient of the first class prize from the Natural Science Award of China Ministry of Education, the NSFC Excellent Young Scholars Program, and the ACM China Rising Star Award.

IEEE Global Communications Conference

4-8 December 2017 // Singapore • Global Hub: Connecting East and West

CALL FOR PAPERS

The 2017 IEEE Global Communications Conference (GLOBECOM) will feature a comprehensive technical program including 13 symposia, tutorials, workshops and an industrial program featuring prominent keynote speakers, technology and industry forums and vendor exhibits.

TECHNICAL SYMPOSIA

- Ad Hoc and Sensor Networks
- Cognitive Radio and Networks
- Communication and Information System Security
- Communication QoS, Reliability and Modeling
- Communication Software, Services and Multimedia Applications
- Communication Theory
- Green Communications Systems and Networks
- Mobile and Wireless Networks
- Next-Generation Networking and Internet
- Optical Networks and Systems
- Signal Processing for Communications
- Wireless Communication
- Selected Areas in Communications
 - Access Networks and Systems
 - Big Data
 - Data Storage
 - e-Health
 - Internet of Things
 - Molecular, Biological, and Multi-scale Communication
 - Power Line Communications
 - Satellite and Space Communications
 - Smart Grid Communications
 - Social Networks

Please address questions regarding the Technical Symposia to Technical Program Committee (TPC) Chair: Ying-Chang Liang (liangyc@ieee.org), and TPC Co-Chairs: Teng Joon Lim (eleltj@nus.edu.sg) and Chengshan Xiao (xiaoc@mst.edu). Accepted and presented technical and workshop papers will be published in the IEEE GLOBECOM 2017 Conference Proceedings and submitted to IEEE Xplore®. See the website for author requirements of accepted authors. Full details of submission procedures are available at www.ieee-globecom.org.

TUTORIALS

Proposals are invited for half-day tutorials in communications & networking. Please address questions regarding tutorials to Tutorial Chair: **Rui Zhang (elezhang@nus.edu.sg)**.

IMPORTANT DATES

Symposia Papers
1 April 2017

Tutorial Proposals
15 March 2017

ORGANIZING COMMITTEE

General Chair

Dim-Lee Kwong (I2R, Singapore)

General Vice Chairs

Shiang Long Lee
(Singapore Technologies, Singapore)
Pak Lum Mock (Starhub, Singapore)

Executive Chair

Lawrence Wong (NUS, Singapore)

Executive Vice Chairs

Ying-Chang Liang
(UESTC, China & I2R, Singapore)
Sumei Sun (I2R, Singapore)

TPC Chair

Ying-Chang Liang
(UESTC, China & I2R, Singapore)

TPC Co-Chairs

Teng Joon Lim (NUS, Singapore)
Chengshan Xiao (Missouri S&T, USA)

Tutorial Chair

Rui Zhang (NUS, Singapore)

Tutorial Co-Chairs

Lingyang Song (PKU, China)
Stefano Bregni (Politecnico Milano, Italy)

Workshop Chair

Tony Quek (SUTD, Singapore)

Workshop Co-Chairs

Wei Zhang (UNSW, Australia)
Gang Wu (UESTC, China)

A Location-Based Mobile Crowdsensing Framework Supporting a Massive Ad Hoc Social Network Environment

Md. Abdur Rahman and M. Shamim Hossain

The authors address one of the key challenges of engaging a massive ad hoc crowd by providing sustainable incentives. The incentive model is based on a context-aware cyber-physical spatio-temporal serious game with the help of a mobile crowdsensing mechanism. To this end, this article describes a framework that can create an ad hoc social network of millions of people and provide context-aware serious-game services as an incentive.

ABSTRACT

This article addresses one of the key challenges of engaging a massive ad hoc crowd by providing sustainable incentives. The incentive model is based on a context-aware cyber-physical spatio-temporal serious game with the help of a mobile crowd sensing mechanism. To this end, this article describes a framework that can create an ad hoc social network of millions of people and provide context-aware serious-game services as an incentive. While interacting with different services, the massive crowd shares a rich trail of geo-tagged multimedia data, which acts as a crowdsourcing eco-system. The incentive model has been tested on the mass crowd at the Hajj since 2014. From our observations, we conclude that the framework provides a sustainable incentive mechanism that can solve many real-life problems such as reaching a person in a crowd within the shortest possible time, isolating significant events, finding lost individuals, handling emergency situations, helping pilgrims to perform ritual events based on location and time, and sharing geo-tagged multimedia resources among a community of interest within the crowd. The framework allows an ad hoc social network to be formed within a very large crowd, a community of interests to be created for each person, and information to be shared with the right community of interests. We present the communication paradigm of the framework, the serious game incentive model, and cloud-based massive geo-tagged social network architecture.

INTRODUCTION

With the recent advancements of smartphone technologies, people carry smartphones as an alternative to their home computer. One of the key powers of a smartphone is that it can sense the context of a user or his/her surroundings and provide necessary services based on location, time, and personalized needs [1]. A large proportion of the population nowadays are familiar with smartphone technologies and use them for day-to-day affairs. For example, both Facebook and Google have crossed the billion landmark of mobile social network users. Hence, not only can people who carry smartphones consume location-aware services but they can also take part in crowdsensing activities and share data with

their social networks of interest [2]. Furthermore, people carry smartphones as a personal digital assistant, for instance, while walking, at rest, running, bike riding, driving, or on a bus or train [3]. Recent crowdsensing applications leverage this smartphone ubiquity to support innovative solutions over a very large coverage region that were previously not achievable, thereby advancing the domain of mobile crowdsensing research [2]. Using mobile crowdsensing, many interesting phenomena can be observed in real time, such as live auto traffic and navigation map in a city, live weather reports based on smartphone user observations, sentiment analysis from uploaded multimedia content, multimedia annotation and tagging, emergency and disaster management, multi-lingual translation, city noise map generation, location-based news sharing through multimedia, rich multimedia data reports from an accident scene, and collaborative city map updating, to name a few [4].

Mobile crowdsensing allows a query or task to be outsourced by a requester to a very large crowd, sometimes called *crowdsourtees*, through a global crowdsensing platform running a cloud computing framework [5]. The requester then receives complex results back within a defined amount of time. One of the distinguishing characteristics of mobile crowdsensing is that it augments the sensing capabilities of smartphones with human computation because humans carry smartphones. As a result, a query or task can leverage different crowdsensing paradigms such as opportunistic and participatory sensing, personal sensing, group sensing, community sensing, location-aware sensing, and context-aware sensing [6, 15].

To seamlessly integrate the requester and crowdsourtees, it is necessary to use a crowdsensing framework [3] that allows a requester to pose a query and crowdsourtees to reply with sensing results. There are several challenges that must be addressed by the different parties involved in mobile crowdsensing in order to obtain the desired output because both requester and crowdsourtees need sustainable motivation through incentives, rewards, and returns, whether intrinsic or extrinsic, financial or non-financial [2]. In a crowdsensing environment, everybody pays some cost and hence expects some return [6]. For example, a requester has

to spend a significant amount of time designing tasks, either developing them from scratch or paying to post the tasks to a crowdsensing platform, finding workers with the right skills, coordinating the workflow, analyzing the quality and quantity of the returned crowd sensed data, ranking the crowdsourcees for future recruitment, and providing appropriate and sustainable incentives to the workers while considering their own profits.

The crowdsourcees use their smartphone resources, time, energy, and intelligence, and they also compromise their privacy and expose their personal social network to the outside world at the expense of their own communication costs. Hence, a strong mobile crowdsensing platform has to be designed that can address the challenging needs of mobile crowdsourcing within a very large crowd [7]. In addition, depending on the crowdsensing application, smartphone workers might share a massive volume of multimedia such as geo-tagged text, audio, video, and images to the crowdsensing platform that need to be processed in real time. Hence, designing a crowdsensing platform based on the application type is a challenging task [8].

To support mobile crowdsensing activities, each mobile crowdsensing system leverages a smartphone application in which a requester can communicate with the appropriate audience. Although some existing crowdsensing platforms such as Amazon Mechanical Turk or CrowdFlower [9] allow workers to be found, creating an ad hoc crowd social network just for the purpose of crowdsensing, this issue poses additional challenges. Existing crowdsensing applications hire skilled and in-demand labor online through already established online platforms while offering other crowdsensing features through a separate smartphone application. Alternatively, the hiring platform can be used as a component within the crowdsensing framework [10]. However, this approach is not suitable for very large gatherings such as the Hajj, Olympic Games, and other ad hoc scenarios where the crowd comes together for a short while from all over the world, stays in a city, and then permanently leaves.

In this article, we present our novel multilingual crowdsensing framework that embeds a set of free smartphone-based services that are needed for pilgrims to perform the pilgrimage while they stay in the city of Makkah. The framework also allows each pilgrim and city resident taking part in the crowdsensing activities to leverage incentives. The incentives are embedded within the framework in the form of a set of free services. Because most pilgrims are perform their pilgrimages for the first time in their lives, the crowdsensing framework adopts a spatio-temporal serious game, or game-with-a-purpose (GWAP) initiatives [12], the details of which are discussed in the design section.

The rest of the article is structured as follows. At first, we discuss the background and challenges of the proposed crowdsensing. Then we present the system design of the framework. Next, we describe the crowdsensing experience and lessons learned from the deployment of the system followed by the concluding remarks.

BACKGROUND AND CHALLENGES

Hajj is a yearly gathering where more than 3 million people from around the world congregate for a week in the Holy City of Makkah to perform spatio-temporal ritual activities [11]. Each ritual must be performed within a geographical boundary (Fig. 1) and within a certain time period, and is referred to in this article as a *spatio-temporal* activity. The crowd is composed of males, females, and children of all ages, although a large percentage are older in age. One of the unique characteristics of this crowd is that they mostly come only once in their lifetime to the pilgrimage; they have different languages, cultures, daily needs, health conditions, educational backgrounds, and social needs. Each pilgrim is part of a small group that has a team leader from his/her country, and each small group then becomes part of a larger group that has a group leader. The geographical location of the venue where the crowd gathers, the diversity of the crowd and its organizing authorities, the size of the crowd (Fig. 1), and the type of sensing services required by the crowd are unique needs that the crowdsensing system must address.

Some of the key aspects of the crowdsensing framework are as follows:

REQUESTER AND CROWDSOURCEES

The following are the actors of the crowdsensing system:

- Pilgrims and their accompanying group members
- Pilgrimage organizers and group leaders
- The family members of each pilgrim around the world
- The friends of each pilgrim around the world
- Existing social networks on Facebook, Google, Twitter, Instagram, and so on
- Medical facilities, hotels, and other similar service providers
- The Makkah municipality, different Saudi ministries that handle pilgrims, and other governments and their respective ministries that deal with pilgrims

CROWDSENSING SERVICES

The following are some key needs, challenges, and features of the crowdsensing services:

- Because Makkah is going through incremental but rapid structural changes, there are numerous missing addresses. Hence, existing mapping services such as Google, Yahoo, and ESRI together do not cover more than 40 percent of the city road networks. Thus, it is hard for a pilgrim to identify him/herself with respect to a certain geo-location. The only way of localizing oneself is through a GPS location. Fortunately, more than 80 percent of pilgrims come with smartphones with a built-in GPS sensor.

- Because the crowd is mostly elderly people from all over the world, despite having a smartphone as a companion, many of them are unaware of mapping, location sharing, and other crowdsensing tools.

- Because almost all the rituals take place on open land (Fig. 1), where all the pilgrims must travel from one geographical location to another within a predefined time duration, each pilgrim needs personalized crowdsensing services. Exam-

The geographical location of the venue where the crowd gathers, the diversity of the crowd and its organizing authorities, the size of the crowd, and the type of sensing services required by the crowd are unique needs that the crowdsensing system must address.

Because many smart-phone users who come for pilgrimage from around the world are elderly, designing a semantic and user friendly crowdsensing client side application is a challenging task. Another challenge is the social diversity and inter-pilgrim and intra-pilgrim requirements, which we term as user context.

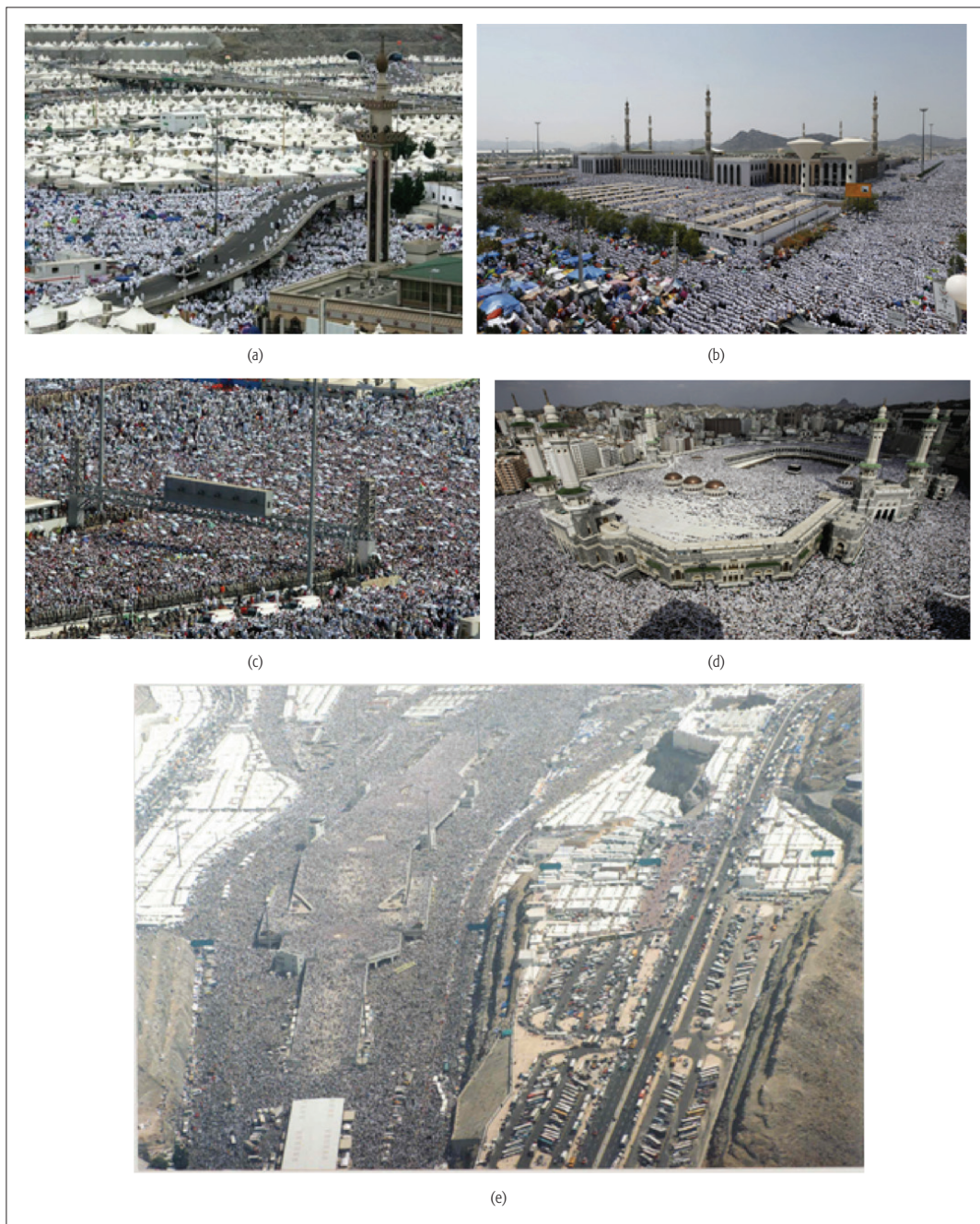


Figure 1. Sample crowd in a tiny region with key ritual geo-zone locations that every pilgrim has to attend for a certain amount of time: a) Mina; b) Arafat; c) Muzdalifah; d) Haram; e) Jamarat.

ples of free crowdsensing services are services that locate fellow pilgrims and family members (as all of them have the same color clothing), locate tents (as all the tents look alike), find important points of interest such as hotels and restaurants, locate nearby taxis and nearby hospitals, present the weather and news, provide translation, identify areas with accidents and congestion nearby or on the route (e.g., more than 700 pilgrims died in a stampede during Hajj in 2015).

- When a pilgrim is lost, his/her social network such as his/her family members, group or team leader, country representative, local city municipality, and other communities of interest might leverage location-based crowd sourcing services to find him/her.

- Because every year a new crowd appears, the crowdsensing framework has to quickly set up the social network by creating small and large groups and then allowing each pilgrim or other actors to join as ordinary or leader members. Existing social network models fail to handle such pilgrim dynamics. The pilgrims generally form a social network model in which the network is formed on an ad hoc basis; the size of the network grows as the crowd starts the pilgrimage and diminishes as the pilgrims leave the gathering place.

- With the help of the crowd, the city municipality would like to build the digital road network and enrich the digital map with all the points of interest (POIs). The digital map should consist of items such as POI descriptions with geo-tagged

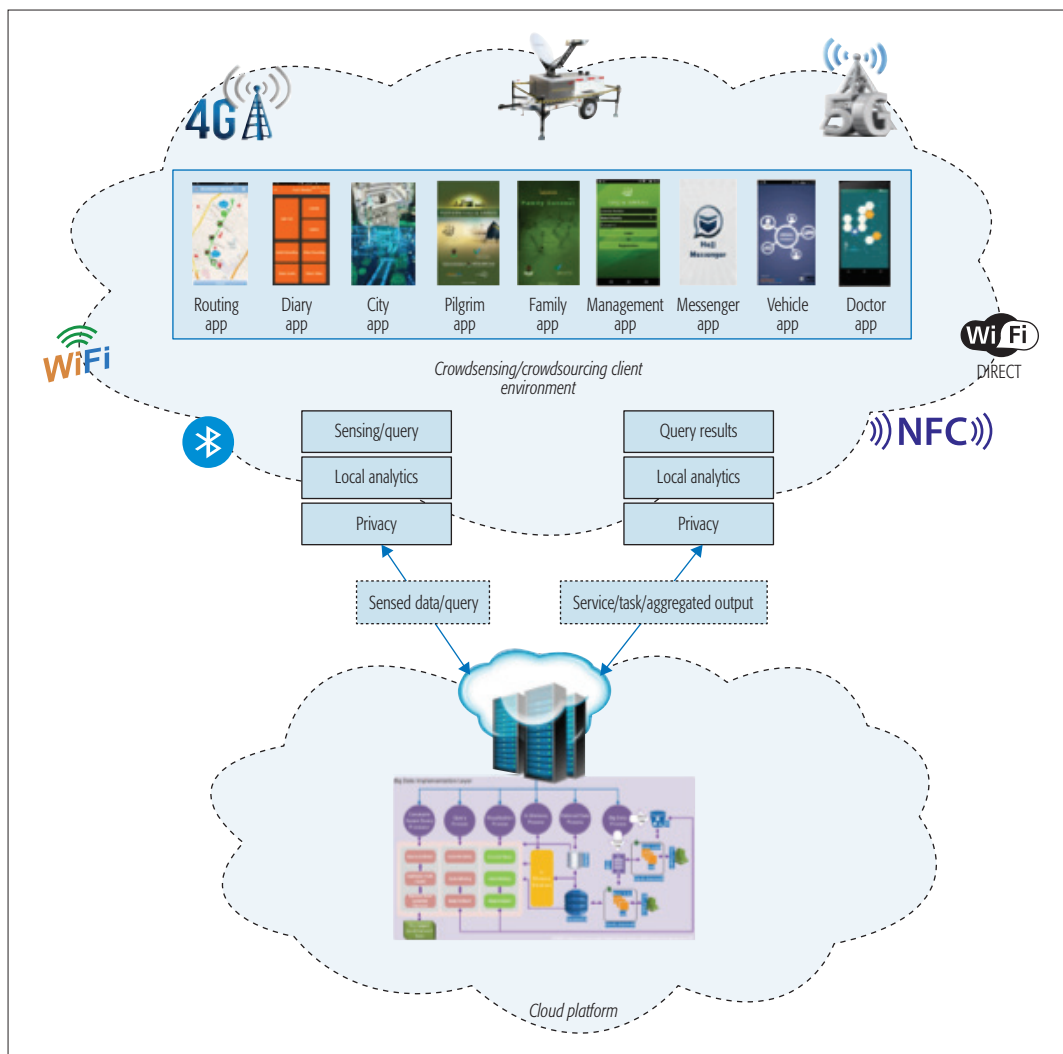


Figure 2. Mobile crowdsensing environment.

images, audio and video, POI ratings, a city noise map, live city traffic, tourist POIs, city-wide restaurants and facilities, free parking slots, the best route to a POI, multimedia reports on accidents, and garbage collection spots. The city will provide these free map-based services, which will be enriched through the crowdsensing framework, to the pilgrims and city residents.

- The crowdsensing platform should have both smartphone applications for different actors and a cloud platform that can process a massive amount of crowdsensing multimedia data and generate appropriate query results.

- The crowdsensing platform should embed an incentive mechanism that is sustainable and can attract the actors mentioned above through free mobile services, which is equivalent to different forms of intrinsic, extrinsic, and other social incentives.

SYSTEM DESIGN

Because many smartphone users who come for pilgrimage from around the world are elderly, designing a semantic and user-friendly crowdsensing client side application is a challenging task [13]. Another challenge is the social diversity and inter-pilgrim and intra-pilgrim requirements, which we call user context. The inter-pilgrim context is

the difference in user context between any two pilgrims at any given time, while the intra-pilgrim user context is the change in user context of one pilgrim over time. Hence, a context-aware crowdsensing framework supports the recommendation of a subset of social ties, often called a community of interest (COI), and services to a user, the automatic execution of a service for a user, and tagging of context-to-information to support later retrieval.

CONTEXT-AWARE CROWDSENSING CLIENT ENVIRONMENT

The following smartphone applications with free services have been designed to attract different actors and encourage them to contribute to the crowdsensing system. We designed nine crowdsensing and crowdsourcing single sign-on applications (for iOS, Android, and the Web), as shown in Fig. 2, that support various actors when they perform different crowdsensing tasks. These applications were envisioned to support various communication paradigms such as Wi-Fi, 4G mobile communication, Bluetooth Low Energy, Wi-Fi Direct, and other emergency Internet access point based communications. For example, the experimental 5G network is envisioned as providing near infinite bandwidth, always connected capability, and context-aware service support. Using

We designed nine crowdsensing and crowdsourcing single sign-on applications that support various actors when they perform different crowdsensing tasks. These applications were envisioned to support various communication paradigms such as Wi-Fi, 4G mobile communication, Bluetooth low energy, Wi-Fi direct, and other emergency Internet access point based communications.

The management application was designed for agencies, ministries, and governments around the world, including Saudi Arabia. This application can be used to locate any pilgrim in real time in case they are lost. It also helps to locate the mass movements of the pilgrims throughout the Hajj, provided a pilgrim gives his/her authorization.

these applications, different actors can form an ad hoc social network. We have worked with the Saudi government and other government agencies and ministries around the world that facilitate pilgrims to distribute the apps before pilgrimage is even started. When the pilgrims reach the pilgrimage location, they start enriching their ad hoc social network through the day-to-day use of different applications, communicate with their COI, and consume services or take part in multimedia location-based crowdsensing services. We briefly describe different sensing and crowdsourcing features supported by each of these applications.

Pilgrim App: This app contains many spatio-temporally context-aware incentive services for the pilgrims. Because pilgrimage is the objective, altruism is found to be the greatest motivator for each pilgrim, in addition to access to lifesaving free services. For example, it offers the location and time for each pilgrim, defines the geo-zones, and offers the necessary and recommended rituals as well as other services. This motivates each pilgrim to continuously use the application and take part in the crowdsensing activities. Some of the incentivized services are as follows:

- 10 free SMSs per day in which pilgrims can share geo-tagged multimedia with their COI on topics such as complaints, health issues, or POI reviews.
- Because of their similar dress and tents, a very large number of pilgrims get lost. This app enables lost individuals to be located with a real-time route augmented with crowdsourced multimedia data.
- Location of the optimum route to more than 30,000 POIs with live offline map-based browsing.
- A service that allows pilgrims to update the traffic in either opportunistic mode or participatory mode, share incident images and video, add missing road names to the map, and report empty parking slots, trash locations, construction work, or obstacles on the road, and earn credit in terms of free daily services and SMSs.
- An emergency service that shows nearby police stations, fire departments, and ambulances as well as a navigational path in real time.
- A service that shares a privacy-protected location with a COI via other applications.

Family App: This application was designed to keep the pilgrim connected to his/her relatives throughout his/her stay in Saudi Arabia. The relatives of pilgrims are notified whenever pilgrims enter different ritual boundaries. Assuming proper authorization is set, a pilgrim and his/her COI can see their live locations at any moment of time and can interact through the respective apps by sharing geo-tagged text, audio, video, and images via a messenger app.

Management App: The management application was designed for agencies, ministries, and governments around the world, including Saudi Arabia. This application can be used to locate any pilgrim in real time in case they are lost. It also helps to locate the mass movements of the pilgrims throughout the Hajj, provided a pilgrim gives his/her authorization. It provides a mechanism by which a pilgrim can complain about the

services and health issues directly to the respective authorities. Authorities can also interact with the pilgrims through SMS, MMS, and a messenger app. Authorities can share the POIs like bus or rendezvous points and tent location through the app.

Messenger App: This application provides single sign-on actors the facilities to chat and share location-aware text, images, and audio and video messages with their COI in a multipoint-to-multipoint conferencing mode.

Vehicle App: This application connects vehicles with related pilgrims, drivers of public and private vehicles, family members of vehicle owners, companies of public vehicles, and administration. Vehicle owners and drivers can announce their locations through the application, and pilgrims and city residents can discover vehicle or taxi locations within a certain perimeter, chat with drivers, negotiate prices and routes, book single or multiple seats, and announce their pickup location(s).

Doctor App: Most pilgrims come to perform the rituals in their old age with one or many types of disease such as diabetes, high blood pressure, heart problems, or asthma. In an emergency, a pilgrim might be unable to explain his/her current location properly because of the language barrier and lack of a proper addressing mechanism. Hence, it is very difficult for an ambulance, doctors, or authorities to locate a patient. If a pilgrim falls ill, the app can help by showing nearby ambulance locations and sharing the current location and health condition of the pilgrim. The system can share the status to *nearby* friends who are online. The system can also send notifications to family app contacts.

City App: This is a real-time monitoring system so that the Makkah city authorities can monitor and manage all involved entities during the Hajj. This is a visualization and analytics tool for the municipality that receives a stream of real-time data from the suites of smartphone crowdsensing modules.

Routing App: Because a large percentage of the pilgrims do not know how to use maps because of their advanced age, this app allows the current location of two individuals to be geo-tagged and augmented with multimedia to determine a route. It uses crowdsourced multimedia along the route as POIs so that users can easily locate each other among millions of similar looking pilgrims and tents.

CYBER PHYSICAL SERIOUS GAMES AS INCENTIVES

We defined geo-caching game elements within the crowdsensing environment, which includes both cyber and physical scenarios. A pilgrim can play the cyber game before he/she starts his/her pilgrimage through virtual space. Once he/she arrives at the pilgrimage venue, the physical game starts, which is architecturally like Nintendo's Pokémon Go. The two scenarios are briefly explained below.

Scenario 1: Users in A Cyber World:

1. A pilgrim has to solve a spatio-temporal puzzle in the context of Hajj in a cyber world. The game environment consists of maps with the actual POIs of the physical holy landscape and digital



Figure 3. a) Multimedia geo-tagged trail to a certain POI or route recorded by a user in the physical world and shared with social networks; b) people in the game environment or the physical world can follow these trails.

road network. Once he/she completes one Hajj task at a particular location (broken down into mandatory, recommended, and optional ritual activities by time and geo-zone), he/she has to perform the next task by visiting the next location using allowable modes for travel (by air, walking, or a vehicle), times, and sequences. This journey continues until a pilgrim wins the game (by being in certain locations in a specific order). The system shows him/her a path to the next step from the current state.

2. The game environment maps each virtual POI with the actual location and elevation of the objects in the holy land, thanks to our crowd-sourced POI collection apps.

3. A pilgrim can share his/her location and geo-tagged multimedia messages with others in the COI of the game environment in case he/she needs guidance or is lost at any geo-location.

4. The game environment is capable of showing a physical crowd and the player's social network as virtual objects in a leaderboard to pilgrims while they perform the rituals (Fig. 3b).

For example, a pilgrim will be able to view real-life traffic and a number of cars on a certain road while he/she roams around.

5. Once the pilgrim finishes all the parts of the puzzle, he/she gets an accolade, badge, and views his/her score. The system shows the mistakes with details such as the location of the mistake, type of mistake, and correct way of doing the step.

6. The game can be played using gaming hardware such as Oculus Rift, Virtuix Omni, MYO, Google Glass, LEAP, and Kinect2.

7. A user can play the above steps as many times as needed before he/she starts the actual pilgrimage.

8. The game can have multiple levels. For example, in Level 1 (basic level), the user is provided a virtual environment with almost no crowd so that he/she can clearly visualize all related POIs. Factors such as "user gains expertise" or "time taken to complete a level" will determine if a player moves to the next level. The difficulty of a level is changed by adding virtual/real crowds and shorter completion times.

We defined geo-caching game elements within the crowdsensing environment, which includes both cyber and physical scenarios. A pilgrim can play the cyber game before they start their pilgrimage through virtual space. Once they arrive at the pilgrimage venue, the physical game starts, which is architecturally like Nintendo's Pokémon Go.

A special add-in mode was designed for users who need special medical observation. For example, while they play multiple levels of the game, their heart-beat, pulse rate, blood pressure can be recorded. These measurements can be analyzed to generate automatic recommendations and/or a special consultation before the user actually plans their real-time activities.

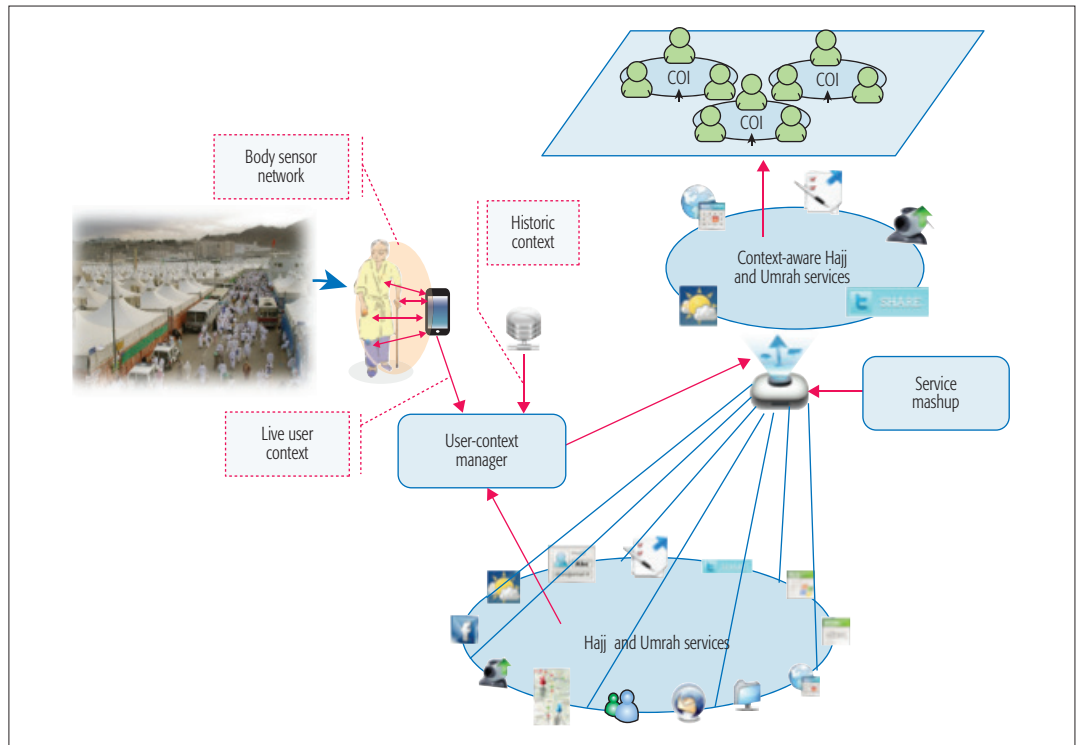


Figure 4. Context-aware crowdsourcing environment.

9. The game can operate in a recording mode that saves all activities in any format and can be played if assistance is required for performing all the activities in real time.

10. The game also has sharing options, so if one needs specific help, the shared component provides guidance.

11. A special add-in mode was designed for users who need special medical observation. For example, while they play multiple levels of the game, their heartbeat, pulse rate, and blood pressure can be recorded. These measurements can be analyzed to generate automatic recommendations and/or a special consultation before the user actually plans his/her real-time activities.

12. The game shows other users' experiences and statuses that can be viewed any time in a leaderboard (in game mode as well as in real time).

Scenario 2: Users in the Physical World:

1. This scenario starts as soon as the pilgrim reaches the actual region where the pilgrimage needs to be performed. The game has to be played physically. If one has family members or other persons of interest accompanying him/her on the pilgrimage, they can play the game together (multi-player game), thereby producing a spatio-temporal massive online real-time geo-caching game.

2. Users face tasks similar to those discussed in scenario 1, except for the fact that the user is in the physical world.

3. Pilgrims generally come in groups. Whenever one pilgrim in a group finishes a ritual in one place, he/she can leave a message and share a trail of his/her events so that others in the group can follow the trail (Fig. 3). The full multimedia sensory data stream along with video and audio can be used to re-create the Hajj experience. Geo tracks can be used to draw the journey path on

the map. All the data collected can be used to provide the completely immersive experience of visiting a place another pilgrim or can be shared with family members around the world.

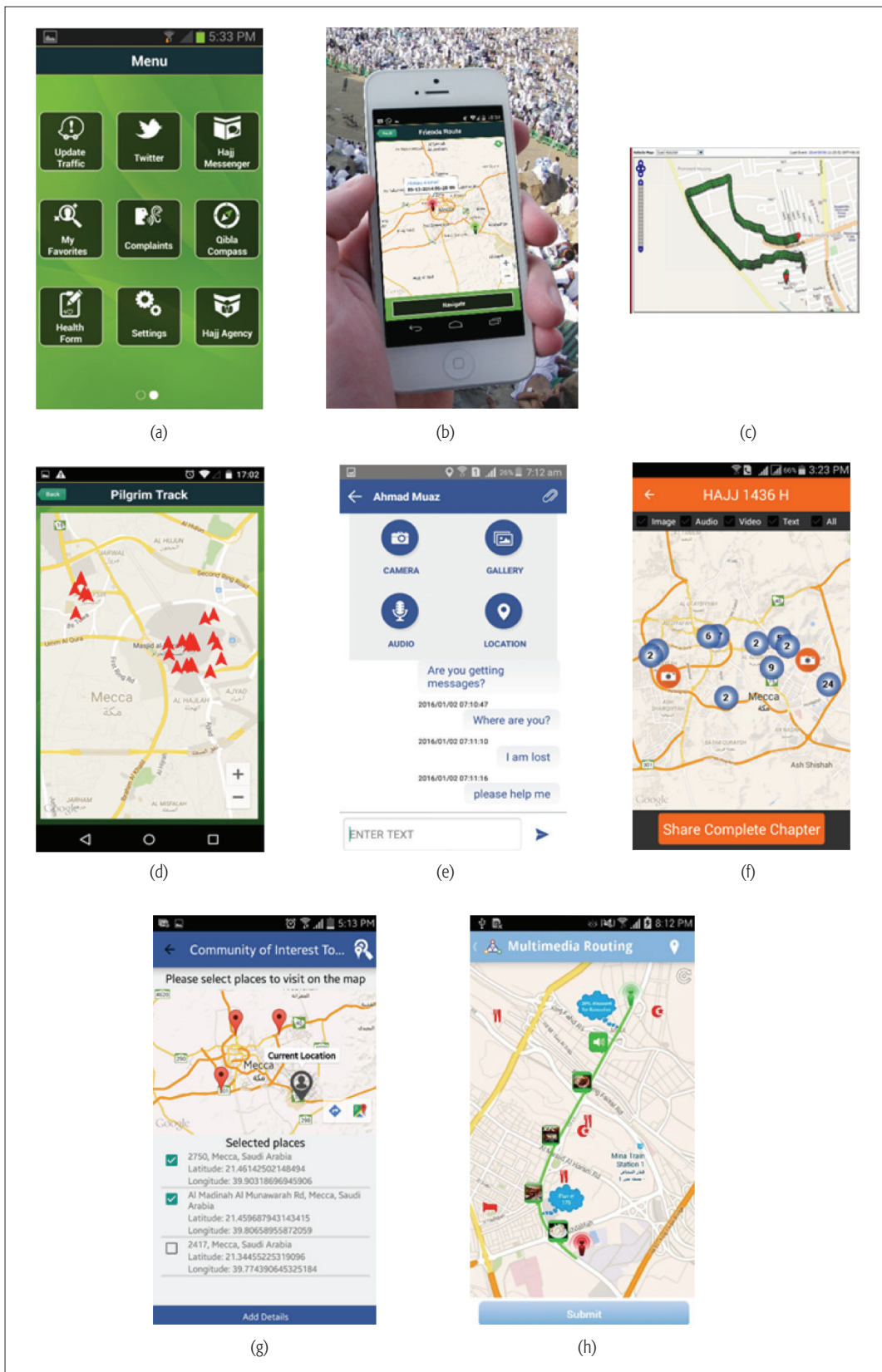
4. If there are no shared components with any of the COI members, the user can log on to his/her account and download his/her pre-recorded activities as performed in scenario 1.

CONTEXT-AWARE CROWDSOURCING ENVIRONMENT

Figure 4 shows the high-level context-aware crowd sensing/sourcing environment. The smartphone apps are designed to probe a user's current context (location, time, events from mobile sensors, onboard or attached, and mined user social network data), read past contexts, capture user queries or tasks posted from other users, and provide a subset of available services and tools to connect to a subset of the user's social ties through mobile applications.

CROWDSOURCING CLOUD ENVIRONMENT

All the crowdsourcing applications we have designed require a big data cloud that supports both real-time and offline multimedia data processing as well as spatio-temporal query analysis and visualization of very big data. We have used Amazon's big data Web services architecture to deal with multiple applications for multiple entities. The architecture is able to handle multimedia data, spatio-temporal data, and relational data with the support of S3 for storage, SQS for queue management, EC2 for scalability, RDS for relational data management, and DynamoDB for noSQL data management (to name some key technologies). We used Open Street Map for offline mapping and routing using PostGreSQL as the backend database in addition to Google Maps for the online maps. For messaging services and push messages consisting of multimedia and location



All the crowdsourcing applications we have designed require a big data cloud that supports both real-time and offline multimedia data processing as well as spatio-temporal query analysis and visualization of very big data. We have used Amazon's big data Web services architecture to deal with multiple applications for multiple entities.

Figure 5. User interfaces for different crowdsourcing smartphone application suites: a) sample user interfaces for crowdsourcing, crowdsensing, and free services in the pilgrim app; b) sample incentive mechanism in which a pilgrim can see his/her live location as well as those of the COI members with respect to ritual geo-zones; c) family members can see the trails of a pilgrim in real time; d) the city can visualize the real-time trails of a sub-group or larger group of pilgrims from a certain country; e) multimedia messenger for sharing text, audio, images, and short videos; f) multimedia POIs that can be visualized or shared with the crowd; g) location-aware crowdsourced and crowd sensed collaborative taxi application; h) while navigating toward a POI or another person, crowdsourced geo-tagged multimedia is shown on the route.

In order to validate the crowdsourcing paradigm, we first introduced the suite of applications to different Hajj stakeholders in May 2014 in six languages. Since then, we have received tremendously positive feedback that motivated us to constantly update our system by taking into consideration the reviews and suggestions of the crowd.

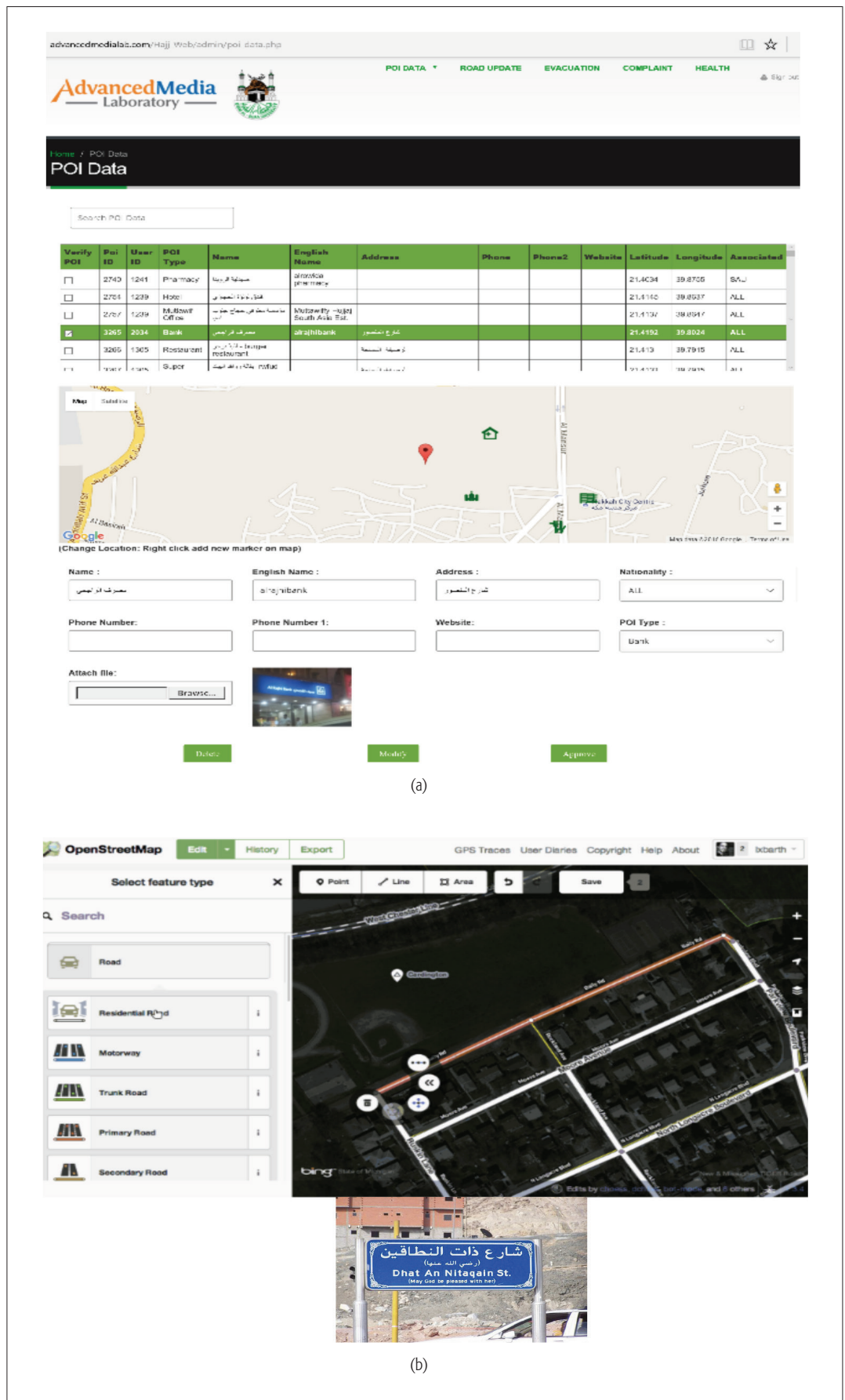


Figure 6. Admin volunteers performing a human intelligence task (HIT) from a web admin by: a) approving, editing, or rejecting points of interests uploaded by the crowd; b) adding/editing a road name based on a crowd submitted picture from the on-site location.

information, we use the Google Cloud Messaging service and Apple Push Notification service, while the SMS services are provided by Twilio.

REAL-LIFE EXPERIENCE

In order to validate the crowdsourcing paradigm, we first introduced the suite of applications to different Hajj stakeholders in May 2014 in six languages. Since then, we have received tremendously positive feedback that motivated us to constantly update our system by taking into consideration the reviews and suggestions of the crowd. More than 20,000 users have downloaded different application suites. Thanks to S. Basalamah, F. Allaf, F. Ur Rehman, A. Ahmad, B. Sadiq, D. Hossain, and S. Abdullah for their great support. Around 100 local volunteers have been helping us to analyze, clean, and publish the crowd data for public usage [14].

Figure 5 shows some of the most popular services along with their user interfaces and usage scenarios, while Fig. 6 shows the human intelligence tasks performed by paid volunteers who analyze, modify, and approve the crowd submitted POIs (Fig. 6a) and missing road name data (Fig. 6b). Using the developed services, pilgrims can consume location- and time-aware services, form ad hoc communication networks with millions of people and share information via geotagged multimedia. The developed suite of smartphone applications enables the crowdsensing and crowdsourcing activities described in this article.

CONCLUSION

In this article, we present our crowdsourcing and crowdsensing framework designed for a very large ad hoc crowd. The framework offers a suite of applications as free services to incentivize the crowd. To make it sustainable, the framework uses both smartphone and human intelligence to collect, analyze, personalize, and share the crowd-sourced data with the different stakeholders of a tiny city that hosts about 3 million tourists for about a week. The proposed crowdsourcing paradigm is designed to deal with people who speak many different languages and from each country around the world by forming an ad hoc social network and then providing context-aware services to each person. This work has given us insight and motivated us to work further in understanding such unique crowd dynamics and enhancing incentive models to engage the crowd in consuming and sharing information as well as using the crowd's intelligence to provide services to the crowd and the city.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, for funding this work through the research group project no. RGP-228. The corresponding author is M. Shamim Hossain.

REFERENCES

- [1] R. K. Ganti, F. Ye, and H. Lei, "Mobile Crowdsensing: Current State and Future Challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, Nov. 2011, pp. 32–39.
- [2] D. Yang et al., "Incentive Mechanisms for Crowdsensing: Crowdsourcing With Smartphones," *IEEE/ACM Trans. Net.*, vol. 24, no. 3, June 2016, pp. 1732–44.
- [3] T. Luo et al., "Incentive Mechanism Design for Heterogeneous Crowdsourcing Using All-Pay Contests," *IEEE Trans. Mobile Computing*, no. 1, pp. 1, doi:10.1109/TMC.2015.2485978.
- [4] N. D. Lane et al., "A Survey of Mobile Phone Sensing," *IEEE Commun. Mag.*, vol. 48, no. 9, Sept. 2010, pp. 140–50.
- [5] P. Cheng et al., "Task Assignment on Multi-Skill Oriented Spatial Crowdsourcing," *IEEE Trans. Knowledge and Data Engineering*, vol. 28, no. 8, Jan. 2016, pp. 2201–15.
- [6] G. Cardone et al., "ParticipAct: A Large-Scale Crowdsensing Platform," *IEEE Trans. Emerging Topics in Computing*, vol. 4, no. 1, Mar. 2016, pp. 21–32.
- [7] S. Ji, T. Chen, "Incentive Mechanisms for Discretized Mobile Crowdsensings," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, Jan. 2016, pp. 146–61.
- [8] J. Xu, J. Xiang, and D. Yang, "Incentive Mechanisms for Time Window Dependent Tasks in Mobile Crowdsensing," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, Nov. 2015, pp. 6353–64.
- [9] P. Kucherbaev et al., "Crowdsourcing Processes: A Survey of Approaches and Opportunities," *IEEE Internet Computing*, vol. 20, no. 2, 2016, pp. 50–56.
- [10] O. Feyisetan et al., "Improving Paid Microtasks through Gamification and Adaptive Furtherance Incentives," *Proc. 24th Int'l. Conf. World Wide Web*, New York, NY, 2015, pp. 333–43.
- [11] A. Ahmad et al., "ST-Diary: A Multimedia Authoring Environment for Crowdsourced Spatio-Temporal Events," *Proc. 23rd ACM SIGSPATIAL*, Seattle, WA, Nov. 3–6, 2015.
- [12] H. Xie et al., "Incentive Mechanism and Protocol Design for Crowdsourcing Systems," *52nd Annual Allerton Conf. Commun., Control, and Computing*, UIUC, IL, Oct. 1–3, 2014, pp. 140–47.
- [13] A. I. Chittilappilly, L. Chen, and S. Amer-Yahia, "Survey of General-Purpose Crowdsourcing Techniques," *IEEE Trans. Knowledge and Data Engineering*, Apr. 2016.
- [14] M. Zhang et al., "Quality-Aware Sensing Coverage in Budget Constrained Mobile Crowdsensing Networks," *IEEE Trans. Vehic. Tech.*, 2015.
- [15] L. Kong et al., "Embracing Big Data with Compressive Sensing: A Green Approach in Industrial Wireless Networks," *IEEE Commun. Mag.*, vol. 54, no. 10, Oct. 2016, pp. 53–59.

BIOGRAPHIES

M. SHAMIM HOSSAIN [SM'09] (mshossain@ksu.edu.sa) is an associate professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He has authored or co-authored more than 120 publications. He was the recipient of the 2016 ACM *Transactions on Multimedia Computing, Communications and Applications* Best Paper Award. He is on the Editorial Boards of *IEEE Access*, *Computers and Electrical Engineering* (Elsevier), the *Games for Health Journal*, and the *International Journal of Multimedia Tools and Applications* (Springer). Currently, he serves as a lead Guest Editor of *IEEE Communications Magazine*, *IEEE Transactions on Cloud Computing*, *Future Generation Computer Systems* (Elsevier), *Computers and Electrical Engineering* (Elsevier), and *Cluster Computing* (Springer).

MD. ABDUR RAHMAN (m.arahman@bnc.edu.sa) is an assistant professor in the Department of Computer Science, Prince Mugrin Bin Abdulaziz University, Madinah Al Munawwarah, Kingdom of Saudi Arabia. He received his Ph.D. degree in electrical and computer engineering from the University of Ottawa, Canada, in 2011. He has authored and co-authored around 85 publications. He has six U.S. patents issued and a couple pending. He has served as a member of the Organizing and Technical Committees of several international conferences and workshops. Recently, he received three best paper awards from ACM and IEEE conferences.

This work has given us insight and motivated us to work further in understanding such unique crowd dynamics and enhancing incentive models to engage the crowd in consuming and sharing information as well as using the crowd's intelligence to providing services to the crowd and the city.

Promoting Cooperation by the Social Incentive Mechanism in Mobile Crowdsensing

Guang Yang, Shibo He, Zhiguo Shi, and Jiming Chen

The authors introduce a novel approach, called the social incentive mechanism, which, surprisingly, incentivizes the social friends of the participants who perform the sensing tasks. The basic idea is to leverage the social ties among participants to promote global cooperation. Since the incentive that a participant receives largely relies on the behaviors of his/her social friends, participants have the motivation to impact their friends' behaviors through their social relationships in order to gain a higher payoff.

ABSTRACT

An incentive mechanism is important for mobile crowdsensing to recruit sufficient participants to complete large-scale sensing tasks with high quality. Previous incentive mechanisms have focused on quantifying participants' contribution to the quality of sensing and provide incentives directly to them. In this article, we introduce a novel approach, called the social incentive mechanism, which, surprisingly, incentivizes the social friends of the participants who perform the sensing tasks. The basic idea is to leverage the social ties among participants to promote global cooperation. Since the incentive that a participant receives largely relies on the behaviors of his/her social friends, participants have the motivation to impact their friends' behaviors through their social relationships in order to gain a higher payoff. This approach is applicable to many scenarios where the contributions to the quality of sensing among participants are interdependent, such as data aggregation. We have provided a case study which shows that the social incentive mechanism is more cost-effective than traditional incentive mechanisms.

INTRODUCTION

Generally speaking, mobile crowdsensing leverages the power of mobile participants with smart devices, including smartphones, smart wristbands, smart watches, and so on, to sense the information of interest from a large area. A popular example of mobile crowdsensing is fine-grained air quality monitoring, in which participants use their smart devices to measure the air quality around the city and upload their sensed data to the mobile crowdsensing platform. Compared to traditional sensor networks, there are many advantages of data collection by mobile crowdsensing [1–3]. First, sensing coverage is unprecedented, since smart devices carried by participants are distributed everywhere in the city. What is more, the mobility of participants further extends the sensing coverage. Second, the cost for installation and maintenance of sensors is trivial in mobile crowdsensing, since these sensors are embedded in off-the-shelf smart devices. Third, with mobile crowdsensing, vast heterogeneous data can be aggregated to provide more comprehensive sensing services.

Although promising, there are some fundamental issues in mobile crowdsensing, among which the incentive mechanism has received the

most attention. Since smart devices are owned by mobile users, rather than the mobile crowdsensing platform, we need to encourage the participation of mobile users (i.e., these who own smart devices). Clearly, when mobile participants are performing their sensing tasks, they will consume their time, battery energy, and mobile data; that is, participants will incur certain costs for participating in crowdsensing. Therefore, a crowdsensing platform can barely attract sufficient participants to fulfill tasks without proper incentives. In this sense, an incentive mechanism, which determines the reward for participants to complete their tasks, is critical to guarantee the performance of crowdsensing.

In most previous studies, large-scale sensing tasks are first decomposed into a set of independent sensing tasks. Then the crowdsensing platform allocates these tasks to participants by providing incentives to them directly for what they have performed. Clearly, such mechanisms can motivate the participants to get involved in crowdsensing and provide high-quality sensing data in the independent task scenarios. However, in practice, there are many sensing applications where the quality of sensing tasks are interdependent (e.g., data aggregation applications). It is therefore difficult to decide the incentive for each individual due to the unknown quality of sensing that each participant contributes. If all participants are awarded with the same incentive, this could encourage them to report sensing data at the least cost, which leads to overall poor performance in terms of quality of sensing. Existing results fall short, and a new incentive mechanism is pressing needed for this application scenario.

Since the quality of sensing is interdependent among a collection of sensing tasks performed by independent participants, it is desired to stimulate cooperation among participants. In practice, the number of participants who perform tasks with interdependent quality of sensing (referred to as interdependent tasks hereafter) could be very large. Most participants may not be willing to cooperate with strangers. Therefore, it is difficult to include all participants in cooperation. Notice that participants may have social friends due to the popularity of social networks. It is more feasible to design an incentive mechanism that encourages social friends to cooperate with each other so that the social welfare and the utility of each participant can be increased simultaneously.

In this article, we propose a novel incentive

This work was supported in part by NSFC under grant No. 61402405, and Zhejiang Provincial Natural Science Foundation of China under grant No. LR16F020001.

Digital Object Identifier:
10.1109/MCOM.2017.1600690CM

The authors are with Zhejiang University. Zhiguo Shi is the corresponding author.

mechanism, called the social incentive mechanism, which was first introduced in [4] to promote cooperation among rational and selfish participants for an energy consumption scenario. In the social incentive mechanism, the incentives are given to the social friends of the participant instead of rewarding him/her directly. In such a way, what a participant gains totally depends on his/her social friends. Therefore, each participant has the motivation to encourage his/her social friends to provide high-quality sensing data. Since each participant has a different set of social friends, such local cooperation leads to global cooperation (Fig. 1), which results in near-optimal social welfare. We formally formulate this social incentive mechanism for mobile crowdsensing with interdependent tasks. We show that with the social incentive mechanism, cooperation among participants can be reached. Further, compared to existing incentive mechanisms, the budget needed by the social incentive mechanism to reach the cooperation is much lower.

The main contributions of this article can be summarized as follows:

- We introduce a new incentive mechanism, the social incentive mechanism in mobile crowdsensing, where incentives are provided to the participants' social friends to stimulate cooperation, rather than directly incentivizing participants themselves.
- We provide a framework, showing how to design an efficient social incentive mechanism for mobile crowdsensing with interdependent tasks. A case study is provided to demonstrate that the performance of the proposed incentive mechanism is better than traditional incentive mechanisms.

EXISTING INCENTIVE MECHANISMS IN MOBILE CROWDSENSING

In this section, we summarize existing incentive mechanisms in mobile crowdsensing, shown in Fig. 2. The existing literature can first be categorized according to the different objectives of sensing applications (optimizing data quality, maximizing sensing coverage, protecting privacy, etc.). They can be further divided by their role in designing incentive mechanisms: platform-leading and market-driven. The platform-leading incentive mechanisms are further classified based on the mathematical approaches (e.g., auction, contract). The market-driven incentive mechanisms are mainly designed to balance the supply and demand. Lastly, all incentive mechanisms can be designed in either online or offline ways.

First, in order to meet various requirements in different scenarios, researchers have proposed various incentive mechanisms with objectives varying from optimizing data quality [5] to maximizing sensing coverage [6] to protecting privacy [7], and so on. Taking sensing coverage as an example, consider the case where the platform wants to collect information about how many roads are in poor condition. Thus, the quality of information received by the platform is largely dependent on the sensing coverage. Therefore, the incentive mechanism should encourage participants to sense in various areas. These reporting data of a new location will receive a high reward.

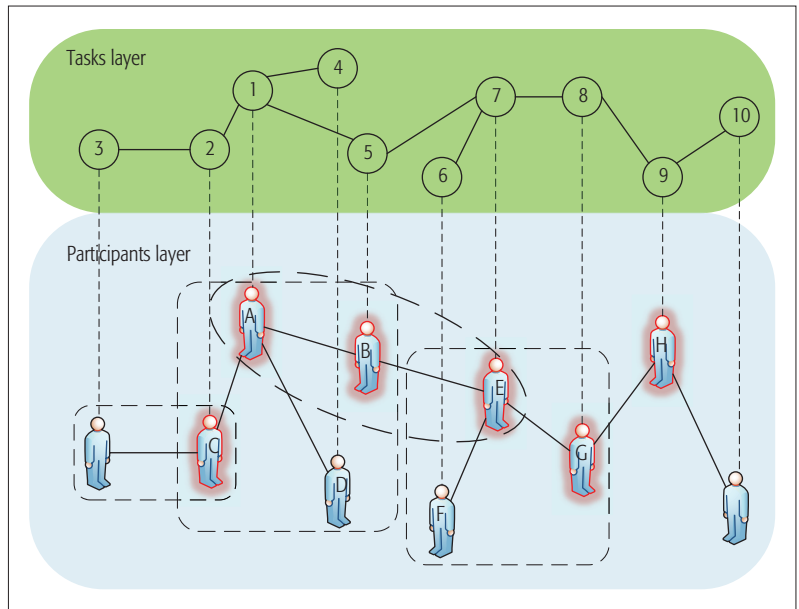


Figure 1. Cooperation propagation through social relationships. Links between the tasks layer and participants layer mean that a task is performed by a participant. Tasks are connected to each other due to interdependence, while participants are connected to each other by social relationships. Participant A, performing task 1, needs to cooperate with B, C, and D, shown in the dashed box. Further, B also needs to cooperate with E. Then E needs to cooperate with F and G. In this way, the cooperation can propagate through social relationships among participants, which results in global cooperation.

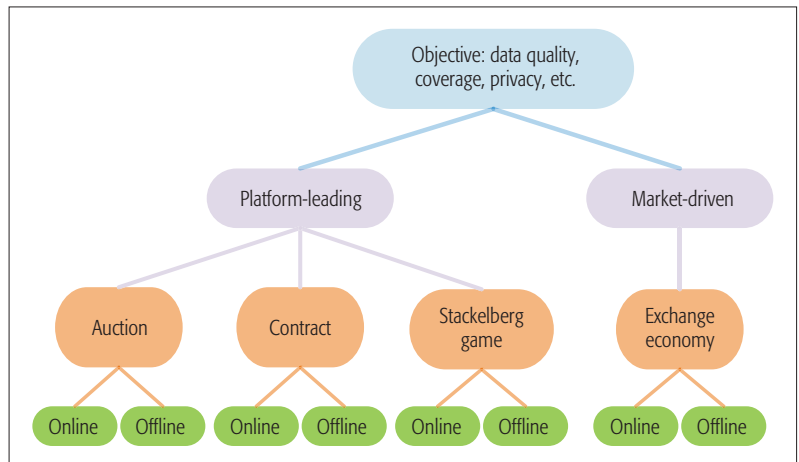


Figure 2. A summary of existing works on incentive mechanisms in mobile crowdsensing.

Since there are multiple entities in mobile crowdsensing systems, previous studies can then be classified into platform-leading [5, 7–11, 13] and market-driven [12, 14]. Platform-leading means that the reward of tasks is determined by the platform. Clearly, the platform can take the initiative to maximize its payoff by adjusting tasks' rewards. Market-driven is a fair situation where the reward of a task is determined on the relation between supply and demand. That is, if there are many participants performing one certain task, the reward will decrease because of redundant supply. If there are many requests for a certain service, the reward of the corresponding task will increase. Note that both platform-leading and

The most popular market-driven approach is based on exchange economy theory. The utilities of both participants and service requesters interact through the relation between supply and demand. The incentive mechanism is designed to maximize the social welfare on condition that the market is clear.

market-driven approaches need to consider individual rationality (IR), that is, any participant's payoff must be nonnegative.

Auction is one of the most common approaches in platform-leading incentive mechanisms. In auction, participants have to submit their bids for candidate sensing tasks, and the platform chooses some participants as auction winners according to various requirements. Besides IR, an auction-based incentive mechanism must guarantee truthfulness, which means that a participant cannot improve his/her utility using an untrue cost as his/her bid. Existing studies on this include reverse auction [8], all-pay auction [9], Tullock auction [10], and so on. In reverse auction (i.e., the roles of participants and auctioneer are reversed), participants are data sellers, while the platform is the data buyer. In [8], Yang *et al.* proposed a reverse-auction-based incentive mechanism for the user-centric model, where participants who are selected as auction winners will upload their data and receive their rewards from the platform. Different from common reverse auction, all-pay auction and Tullock auction are new, where the platform forces all participants to upload their sensing data in advance. In [9], the authors proposed an all-pay auction-based incentive mechanism for the scenario where participants have asymmetric beliefs. The only auction winner is the one with the greatest contribution, who will get a high reward, while other participants gain nothing. A Tullock auction is similar to an all-pay auction. The only difference is that the winner in a Tullock auction is determined stochastically. The one contributing the largest value has the biggest probability to win. Both all-pay and Tullock auctions are efficient to eliminate participants' free-riding. That is, participants cannot trickily receive profit without contributing. Although no participants except the winner get any reward in all-pay and Tullock auctions, the feasibility lies in the expected individual rationality (i.e., a participant has nonnegative expected payoff).

The contract is another popular approach in platform-leading approaches. Its basic idea is to classify participants into different types, and design a set of contract items for participants of different types. A contract can overcome information asymmetry, that is, the platform may not know the actual cost of performing tasks by participants, due to the lack of private information such as preferences and valuations. A feasible contract ensures that participants of each type will choose the same kind of contract items to maximize their payoffs; meanwhile, the platform can maximize its own payoff. In [11], Duan *et al.* proposed a contract-based incentive mechanism for distributed computing in crowdsourcing where the contract is a set of task quota and reward pairs. Each participant selects one of the contract items and performs the corresponding amount of the task to obtain the reward.

The Stackelberg-game-based incentive mechanism is also a popular approach in platform-leading incentive mechanisms. Typically, in the context of mobile crowdsensing, the platform is the leader who will first provide a total reward (which will be divided by participants) to recruit participants. Participants, acting as followers, will decide whether to participate in crowdsensing. Refer-

ence [11] focused on the scenario where the platform wants to build a database, and proposed a Stackelberg-game-based incentive mechanism for data acquisition. Participants who upload their information will share this reward uniformly. Reference [8] designed an incentive mechanism for a crowdsourcing-centric model in which participants' strategies are the sensing time. The reward is divided according to participants' sensing time instead of equal distribution as in [11].

The most popular market-driven approach is based on exchange economy theory. The utilities of both participants and service requesters interact through the relation between supply and demand. The incentive mechanism is designed to maximize the social welfare on condition that the market is clear. In [12], Tham *et al.* proposed a market-based approach for crowdsensing taking data quality into account, and proved the existence of the market equilibrium.

All the incentive mechanisms can work either offline or online. An offline mechanism refers to the case where participants are already in the platform and wait for the platform's recruitment. The platform needs to design an effective incentive mechanism to conduct the crowdsensing process. In contrast, an online mechanism means that participants come to the platform one by one. If not being recruited, a participant will leave. Participants will inform the platform of the tasks in which they are interested and the corresponding reward they expect upon arrival. The platform needs to make a decision at once on whether to recruit this participant or wait for another participant with a lower cost [13]. The key challenge is how to design an efficient algorithm with guaranteed performance.

As seen in Fig. 2, none of the existing incentive mechanisms take the social relationship among participants into consideration. As we consider a quite different scenario where the quality of sensing is interdependent, we propose a novel social incentive mechanism, aiming to promote cooperation among participants in crowdsensing.

SYSTEM MODEL

We consider large-scale sensing applications where the quality of sensing for sensing tasks is interdependent. An example of such a scenario is the data aggregation, where sensing reports from different participants are fused to serve a common objective [15]. Clearly, the quality of sensing that the platform can receive depends on how many participants share their information.

Define the participant set as $N = \{x_1, x_2, \dots, x_N\}$. Participant i in the crowdsensing system has his/her own strategy x_i , which indicates the workload that participant i wants to perform, or the contribution that participant i wants to make. x_i , for example, can be seen as the amount of sharing information. Further, define X as all participants' strategies (i.e., strategy profiles) and X_{-i} as the strategies excluding participant i . As the quality of sensing tasks are interdependent, the utility that participant i can receive is defined as $v_i(1 \cdot X_{-i})$, where \cdot is the product operator, and

$$1 \cdot X_i = \sum_{j \neq i, j \in N} x_j.$$

Note that here participant i 's own contribution is

trivial for providing service for himself/herself. The reason is that in our scenario, exactly what the participant needs is others' sharing sensing data. For example, consider that a driver wants to make a good route plan. This driver already knows his/her own GPS information. However, this cannot help make a route plan. What the driver wants to know is whether there is a traffic jam along the selected path. The platform gathers drivers' GPS information to provide such road condition service. If the driver is informed of another driver's GPS information, he/she will know traffic state, and manage to have a wise route plan. That is, this driver can only benefit from others' information. We assume that $v_i(1 \cdot X_{-i})$ is an increasing and concave function with $v_i(0) = 0$ to capture the marginal effect. Performing a task will certainly incur a cost for a participant, such as consuming their time, battery energy, and mobile data. Define $cost_i(x_i)$ as the cost of participant i for performing a task with strategy x_i . Here, we assume that $cost_i(x_i)$ is an increasing and convex function with $cost_i(0) = 0$ and $cost_i'(0) = 0$ to indicate the increasing marginal cost for making a greater contribution. Taking the data aggregation as an example, the more information a participant shares, he/she will consume more battery energy and mobile data. At the same time, it will cost more time to sense and upload these sensing data, which will further increase the cost. We define a participant's payoff as the benefit from others (i.e., the service provided by the platform) minus the cost of performing tasks, i.e., $u_i = v_i(1 \cdot X_{-i}) - cost_i(x_i)$. Besides, define the sum of all participants' payoffs as the social welfare S , that is,

$$S = \sum_{i=1}^N u_i.$$

For a better understanding, the service can be seen as a positive externality. Externality is a concept from microeconomics, in which a participant's utility is affected by others' strategies. Note that in our scenario, participants need to cooperate with each other to obtain a higher utility v_i . On the other hand, to bring down the cost, a rational participant may not have enough motivation to perform their own tasks. Define x_i^* as the best strategy for participant i , which maximizes participant i 's payoff u_i . It is easy to see $x_i^* = 0$. Therefore, each rational participant will never contribute sensing data in the Nash equilibrium. Define $X^* = 0$ as the strategy profiles in the Nash equilibrium.

From this dilemma, we can see that noncooperation among rational and selfish participants results in low-level social welfare. The awful consequence is exactly what we should avoid in practice. The basic reason for this dilemma is that participants act individually without considering others' utility, while the quality of sensing tasks is interdependent.

SOCIAL INCENTIVE MECHANISM

In this section, we propose the social incentive mechanism framework to promote cooperation for interdependent tasks in mobile crowdsensing.

As we all know, participants are connected through their social relationships in daily life, and they can affect each other through the social ties.

Note that a social relationship between participant i and participant j here means i and j are friends or acquaintances. Topologically, there is an undirected link between participant i and j , as can be seen in Fig. 1. Since each participant relies on others' behaviors for a higher payoff, they have the motivation to cooperate with each other. It is shown in [4] that with the social relationship, participants can exert pressure on their social friends so that their behaviors will become better. We exploit this principle to promote cooperation between a participant and his/her social friends in this article. Further, participants have varying social relationships. Thus, a participant's friends also need to cooperate with their social friends. In this way, the cooperation can propagate through social relationships. This means such local cooperation of each participant can finally lead to global cooperation.

First, we define X^o as the strategy profiles that maximize social welfare (i.e., optimal social strategies). Define $Nbr(i)$ as the set of participant i 's social friends. Clearly, we have $i \in Nbr(j)$. As participant i 's utility v_i depends on other participants' strategies, participant i has the motivation to exert pressure on his/her social friends to cooperate for a higher payoff. Define p_{ij} as the pressure that participant i exerts on participant j (given i and j are social friends). Further, define p_i^+ as the pressure exerted by participant i on all his/her friends,

$$p_i^+ = \sum_{j \in Nbr(i)} p_{ji}.$$

On the other hand, participant i will also receive pressure exerted by his/her friends, defined as p_i^-

$$p_i^- = \sum_{j \in Nbr(i)} p_{ji}.$$

If there is a gap between participant i 's current strategy and his/her social optimal strategy, he/she will suffer a disutility because of social pressures p_i^- , which can be modeled as a function of the gap $|x_i^o - x_i|$ and the pressure exerted on him/her p_i^- . This indicates that the pressure helps regulate participants' asocial behaviors. Besides, if a participant's strategy is exactly social optimal, the pressure exerted on him/her is null. For simplicity, we use the product of the gap and pressure to indicate this disutility,

$$- \sum_{j \in Nbr(i)} p_{ji} |x_i^o - x_i|.$$

Further, define P as the pressure profiles. Exerting pressure on friends will naturally incur a cost, since the friendship may be affected, or there is a cost to inform friends to cooperate. Thus, a participant's payoff will also be impacted by the cost of exerting pressure on his/her friends. Define c_i as the per unit pressure cost for participant i to exert pressure on his/her friends. We assume that c_i is neither too high (in case no one has the motivation to exert the pressure to his/her friends) nor too low (in case every participant exerts large enough pressure and the social welfare is maximized).

Thus, to determine a strategy, each participant will first exert pressure to promote cooperation among his/her social friends. For participant i , he/she needs to decide how much pressure to exert (i.e., decide p_i^+). Then participant i observes the

Participants have varying social relationships.

Thus, a participant's friends also need to cooperate with their social friends. In this way, the cooperation can propagate through social relationship. This means such local cooperation of each participant can finally lead to global cooperation.

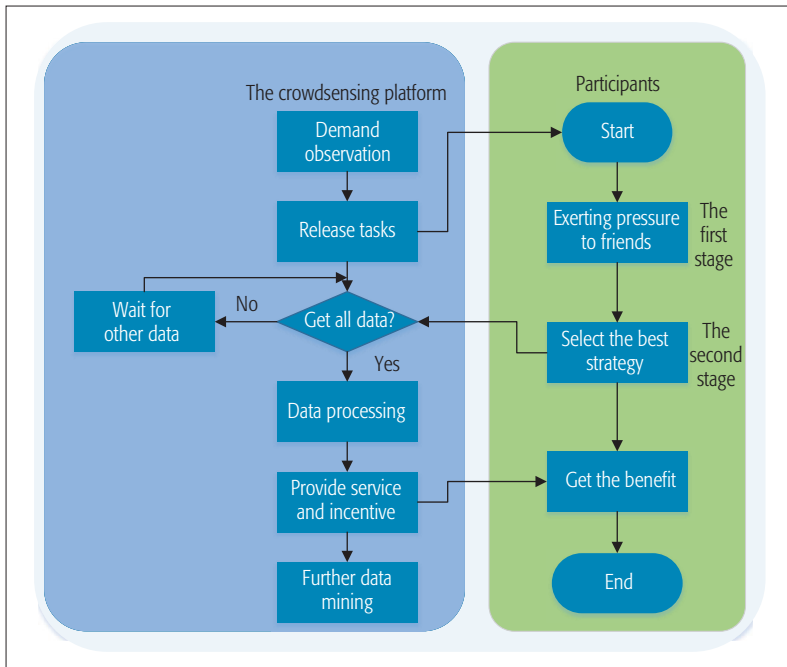


Figure 3. The work flow of the social incentive mechanism.

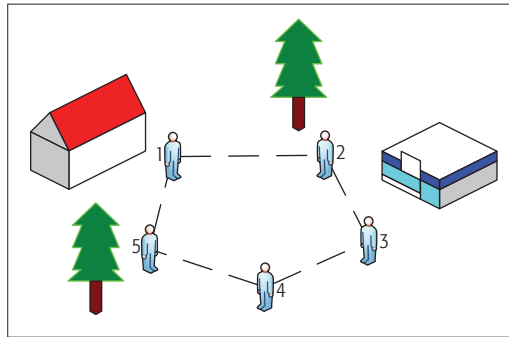


Figure 4. A simple case study. In our case study, there are five people, each of whom only has a relationship with the two closest people shown by the dashed lines. They want to know the ranking of their amount of exercise in the small society.

pressure p_i^- exerted on himself/herself. Next, participant i will choose a strategy to maximize his/her payoff.

Clearly, an incentive mechanism is needed to encourage participants to exert pressure so that participants' strategies approximate the social optimal. In the social incentive mechanism, a participant is indirectly incentivized, which is quite different from traditional incentive mechanisms. That is, a participant's reward depends on his/her social friends' behaviors, which can be seen as compensation for exerting pressure. Briefly speaking, if a participant chooses a selfish strategy, he/she will suffer disutility because of pressure from his/her social friends. On the other hand, if he/she chooses a cooperative strategy, his/her social friends will get a high incentive, and the disutility will decrease at the same time. Thus, each participant is motivated to cooperate with others in our social incentive mechanism. When $j \in Nbr(i)$, participant i 's incentive r_{ji} for exerting pressure on participant j can be defined as a function of

the difference between participant j 's strategy x_j and j 's strategy in Nash equilibrium x_j^* , for example, $r_{ji} = x_j - x_j^*$. In this way, participant i has the motivation to exert pressure on participant j to gain more incentive r_{ji} and a higher utility v_i . The total incentive r_i that participant i can receive is the sum of incentives for exerting pressure on all his/her friends,

$$r_i = \sum_{j \in Nbr(i)} r_{ji}.$$

Thus, the payoff of participant i can be defined as

$$U_i = v_i(1 - X_{-i}) - \text{cost}_i(x_i) - \sum_{j \in Nbr(i)} p_{ji} |x_i^o - x_i| - c_i \sum_{j \in Nbr(i)} p_{ij} + r_i.$$

We summarize the work flow of the social incentive mechanism in Fig. 3.

To implement the social incentive mechanism, the platform should first derive the raw equilibrium strategy profiles X^* and the social optimal strategy profiles X^o . In what follows, participants in the crowdsensing should calculate their best information sharing level $x_i^*(p_i^-)$ under any pressure p_i^- . Further, participants need to derive their best exerting pressure level p_i^+ based on $X^*(p_i^-)$. In this sense, pressure level profiles P is determined. Based on P , the information sharing level profiles $X^*(p^-)$ can also be determined. Finally, to guarantee $X^*(p^-) = X^o$, the platform can determine its incentive to participants.

To summarize, we model the incentive mechanism design process, the exerting pressure process, and the choosing strategy process as a three-stage Stackelberg game, where the platform is the leader and participants are followers in our scenario. In the first stage, the platform declares the incentive mechanism. In the second stage, participants determine how much pressure to exert on their social friends. In the third stage, participants determine their strategies independently. The basic idea is to employ backward induction and derive the best response. Specifically, we first determine the participants' strategy profiles under any pressure profile according to participants' best responses. We then can derive the pressure profile that maximizes participants' payoffs. The social incentive mechanism is determined to ensure that the participants' strategy profiles are exactly the social optimal strategies.

CASE STUDY

In this section, we conduct a simple case study to demonstrate the performance of the social incentive mechanism. For this, we consider the case where five participants want to know each other's amount of exercise, as shown in Fig. 4. Thus, they can know the ranking. Each participant only has a social relationship with two other participants who live nearby. Next, in this scenario, we compare the proposed social incentive mechanism with the traditional incentive mechanisms.

In the traditional incentive mechanisms, the system treats participants individually. In order to avoid sporadic and infrequent contributions, the system provides incentives for participants who complete their tasks. In this case, participants directly get the incentive for their contributions. In our scenario, a participant receives the incentive

from the system as a reward for changing his/her strategy from the strategy profiles in Nash equilibrium (which is $X^* = 0$). Each participant will find his/her best strategy to maximize his/her payoff.

An efficient incentive mechanism should guarantee that all participants' choices are exactly the social optimal strategies. Under this goal, we implement the social incentive mechanism according to an earlier section. Further, denote the budget of a traditional incentive mechanism and the social incentive mechanism as B_T and B_S , respectively. Obviously,

$$B_T = \sum_i r_i \text{ and } B_S = \sum_i \sum_{j \in Nbr(i)} r_{ji}.$$

The simulation results are shown in Figs. 5 and 6.

From Fig. 5, we can see that without the social pressure and incentives, the best response for each participant is $x_i = 0$, while the social optimal strategy is $x_i = 1$. With the social pressure only, the best response is $x_i = 0.39$ for each participant, and the pressure level in the Nash equilibrium is $p_{ij} = 0.39$ for each participant. Thus, we can see that the Nash equilibrium with only pressure still does not reach Pareto optimality. In this sense, it is essential to provide an efficient incentive mechanism to motivate the optimal behaviors among participants.

A traditional incentive mechanism gives reward directly to the participant himself/herself. With the traditional incentive, the budget of the platform is 10 (i.e., $B_T = 10$). In contrast, exploring the power of social relationships and encouraging participants to exert pressure on their social friends, the budget of the social incentive mechanism is only 3 (i.e., $B_S = 3$). Thus, the social incentive mechanism is more cost effective.

Further, we evaluate the impact of cost c on the budget and participant's payoff, which is shown in Fig. 6. We can see that when the cost for exerting pressure is small enough ($c = 0.25$), the strategy of a participant is exactly the social optimal strategy (i.e., $x_i = x^o = 1$). Besides, there is no need to give incentives at this time in our social incentive mechanism (i.e., $B_S = 0$). On the other hand, the traditional incentive mechanism has the constant budget 10. Also, we can see that when the cost for exerting pressure on friends is quite high, the budget is higher than the traditional incentive mechanism. This means when participants are unfamiliar with each other, or when it is hard to communicate with each other, the social incentive mechanism is not a good choice. However, in practice, the cost c will not be very high since it is convenient to communicate with friends via social networks these days. Therefore, the social incentive mechanism is more cost-efficient to promote cooperation and yield near-social-optimal solution.

CONCLUSION

In this article, we have proposed a novel incentive mechanism for mobile crowdsensing, which leverages the power of social relationships to promote cooperation. First, we provide a brief summary about existing incentive mechanisms. Different from these works, we then focus on the scenario where the quality of sensing tasks are interdependent and illustrate the dilemma in that scenario. We propose a framework for designing the social incentive mechanism to promote cooperation in

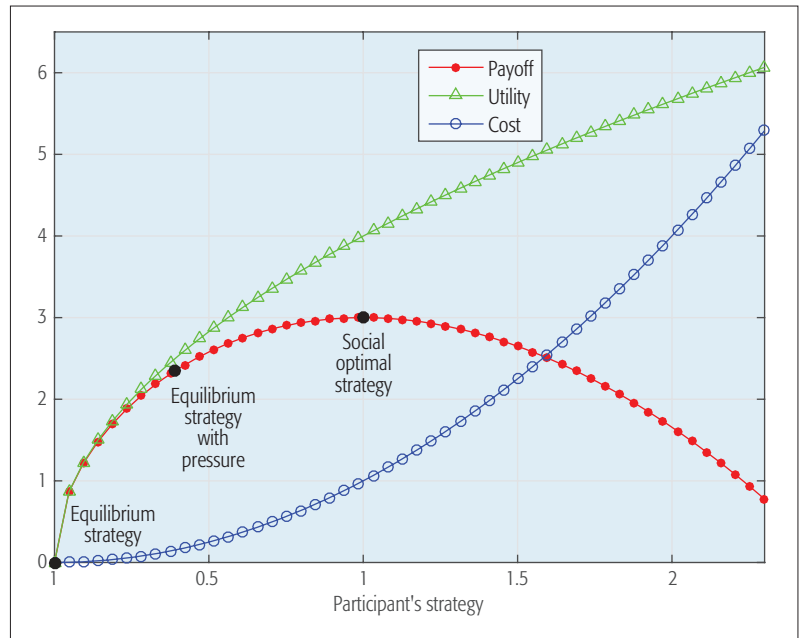


Figure 5. Payoff with the same strategy for all participants.

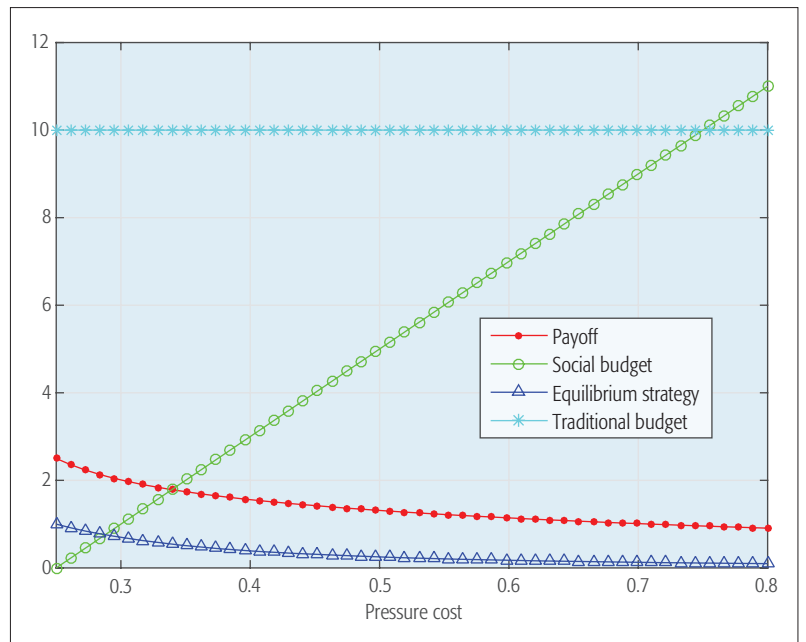


Figure 6. Impact of pressure cost c .

crowdsensing. Further, we provide a primary case study. The results show that the social incentive mechanism is more cost-effective to promote cooperation and yield a near-social-optimal solution. For future work, we plan to study the structure of participants' social relationships to explore some statistical properties, which may help to design incentive mechanisms for mobile crowdsensing. In a nutshell, this article has explored the power of social relationships and has introduced a new perspective for designing incentive mechanisms in mobile crowdsensing.

ACKNOWLEDGMENT

We thank Prof. Xiaofan Wang from Shanghai Jiaotong University for fruitful discussion on the social incentive mechanism.

The results shows that the social incentive mechanism is more cost-effective to promote cooperation and yield near-social-optimal solution. For future direction, we plan to study the structure of participants' social relationship to explore some statistical properties, which may help to design incentive mechanisms for mobile crowdsensing.

REFERENCES

- [1] S. He *et al.*, "Near-Optimal Allocation Algorithms for Location-Dependent Tasks in Crowdsensing," *IEEE Trans. Vehic. Tech.*, to appear, DOI: 10.1109/TVT.2016.2592541.
- [2] G. Yang, S. He, and Z. Shi, "Leveraging Crowdsourcing for Efficient Malicious Users Detection in Large-Scale Social Networks," *IEEE Internet of Things J.*, to appear, DOI: 10.1109/JIOT.2016.2560518.
- [3] J. Chen *et al.*, "Utility-based Asynchronous Flow Control Algorithm for Wireless Sensor Networks," *IEEE JSAC*, vol. 28, no. 7, Sept. 2010, pp. 1116–26.
- [4] A. Mani, I. Rahwan, and A. Pentland, "Inducing Peer Pressure to Promote Cooperation," *Sci. Rep.*, vol. 3, no. 1735, Apr. 2013.
- [5] W. Sun and C.-K. Tham, "An Information-Driven Incentive Scheme with Consumer Demand Awareness for Participatory Sensing," *Proc. IEEE SECON*, 2015, pp. 319–26.
- [6] H. Xiong *et al.*, "Crowdtasker: Maximizing Coverage Quality in Piggyback Crowdsensing Under Budget Constraint" *Proc. IEEE Percom*, 2015, pp. 55–62.
- [7] Q. Li and G. Cao, "Providing Privacy-Aware Incentives in Mobile Sensing Systems," *IEEE Trans. Mobile Comp.*, vol. 15, no. 6, June 2016, pp. 1485–98.
- [8] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive Mechanisms for Crowdsensing: Crowdsourcing With Smartphones," *IEEE/ACM Trans. Network*, vol. 24, no. 3, June 2016, pp. 1732–44.
- [9] T. Luo *et al.*, "Incentive Mechanism Design for Heterogeneous Crowdsourcing using All-Pay Contests," *IEEE Trans. Mobile Comp.*, vol. 15, no. 9, Sept. 2016, pp. 2234–46.
- [10] T. Luo *et al.*, "Crowdsourcing with Tullock Contests: A New Perspective," *Proc. IEEE INFOCOM*, 2015, pp. 2515–23.
- [11] L. Duan *et al.*, "Motivating Smartphone Collaboration in Data Acquisition and Distributed Computing," *IEEE Trans. Mobile Comp.*, vol. 13, no. 10, Oct. 2014, pp. 2320–33.
- [12] C.-K. Tham and T. Luo, "Quality of Contributed Service and Market Equilibrium for Participatory Sensing," *IEEE Trans. Mobile Comp.*, vol. 14, no. 4, Apr. 2015, pp. 829–42.
- [13] X. Zhang *et al.*, "Free Market of Crowdsourcing: Incentive Mechanism Design for Mobile Sensing," *IEEE Trans. Parallel and Distrib. Comp.*, vol. 25, no. 12, Dec. 2014, pp. 3190–3200.
- [14] T. Luo and C.-K. Tham, "Fairness and Social Welfare in Incentivizing Participatory Sensing," *IEEE SECON*, 2012, pp. 425–33.
- [15] L. Kong *et al.*, "Embracing Big Data with Compressive Sensing: A Green Approach in Industrial Wireless Networks," *IEEE Commun. Mag.*, vol. 54, no. 10, Oct. 2016, pp. 53–59.

BIOGRAPHIES

GUANG YANG (yangg2015@zju.edu.cn) received his B.Sc. degree in electronic information science and technology from Lanzhou University, China, in 2015. He is currently pursuing his Ph.D. degree in the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China. His current research interests include crowdsensing/sourcing and mobile social networks.

SHIBO HE (s18he@ipc.zju.edu.cn) is currently a professor with Zhejiang University. His research interests include the Internet of Things, crowdsensing, and big data. He serves on the Editorial Boards of several journals including *IEEE Transactions on Vehicular Technology*. He served as Symposium Co-Chair for IEEE ICC 2017, Finance & Registration Chair for ACM MobiHoc 2015, and TPC Co-Chair for IEEE ScalCom 2014.

ZHIGUO SHI (shizg@zju.edu.cn) received his B.S. and Ph.D. degrees in electronic engineering from Zhejiang University in 2001 and 2006, respectively. Since 2006, he has been a faculty member with the College of Information and Electronic Engineering, Zhejiang University, where he is currently a full professor. Now he is serving as an Editor for *IEEE Network* and *IET Communications*.

JIMING CHEN (cjm@zju.edu.cn) is currently a full professor with the College of Control Science and Engineering and vice director of the State Key Laboratory of Industrial Control Technology, Zhejiang University. His research interests include sensor networks, networked control, and cyber security.

HySense: A Hybrid Mobile CrowdSensing Framework for Sensing Opportunities Compensation under Dynamic Coverage Constraint

Guangjie Han, Li Liu, Sammy Chan, Ruiyun Yu, and Yu Yang

ABSTRACT

Mobile crowdsensing is a novel sensing paradigm enabled by the proliferation of mobile devices. Since crowdsensing applications are driven by sufficient users, advanced incentive mechanisms have been designed to enhance users' willingness to participate in sensing tasks. However, incentive mechanisms only provide adequate sensing opportunities on the condition that the available user base is large. If existing users are fewer than the required number of participants, incentive mechanisms will lose efficacy. This article proposes a hybrid framework called HySense to compensate for inadequate sensing opportunities solely provided by incentive mechanisms. Within each sensing cycle, HySense combines mobile devices with static sensor nodes to generate uniformly distributed space-time data under the constraint of field coverage. To balance sensing opportunities among different geographic regions, redundant users are efficiently migrated from densely populated areas to sparsely populated areas. HySense utilizes calibration mode for checking whether the participants' behavior patterns are consistent with the sensing task queue. Therefore, any change caused by unforeseen accidents can be dealt with in advance.

INTRODUCTION

Following the explosive growth in the number of mobile devices, a large quantity of sensors mounted on mobile devices are available for information perception. Besides good sensing capabilities, sensor-equipped mobile devices are capable of performing data storage, processing, and uploading through internal chips and wireless network interfaces. These indicate that if the potential of existing mobile devices can be fully exploited, large-scale and fine-grained sensing can be realized without deploying additional sensor nodes. The resulting mobile crowdsensing (MCS) has been proposed as a novel sensing paradigm, which utilizes pervasive mobile devices in social scale to perform complex sensing tasks [1, 2].

Compared to wireless sensor networks, MCS

systems are also sensor-based and inclined to use wireless communication technology. However, there is no deployment cost issue in MCS because sensor data are not provided by hundreds of sensor nodes but by pervasive mobile devices in people's daily lives [3, 4]. These pervasive mobile devices include smartphones, wearable devices, and so on. MCS systems recruit users of these mobile devices to contribute their resources for crowdsensing tasks. As long as enough users are recruited, the realization of large-scale sensing can be ensured. However, whether and when to participate in sensing tasks are up to users' willingness. Generally, for saving location privacy as well as resources of mobile devices (e.g., communication, computation, and energy), users tend to refuse participation in data sensing and sharing [5]. Thus, it is essential for MCS systems to motivate users to share their sensing capabilities.

Researchers have developed several incentive mechanisms for attracting users to participate in MCS. The proposed solutions fall into three categories: entertainment-based strategies, service-based strategies, and reward-based strategies [6]. Entertainment-based strategies motivate participants by turning sensing tasks into games. Participants can experience enjoyment when performing sensing tasks. Service-based strategies stipulate that a user who wants to benefit from the service provided by an MCS system is required to become a service provider first. Reward-based strategies pay participants who make contributions for sensing tasks. Auction mechanisms are widely adopted to negotiate the cost of reward. These existing methods feed MCS systems with sufficient numbers of participants based on a strong assumption that existing users are more than the least expected number of participants. In fact, the number of available users is time-varying. The assumption cannot be satisfied all the time.

According to the biological clock of human beings, few users are available to be recruited in the middle of the night. When the number of users is less than the threshold level that ensures the minimum sensing quality, even if all the users are recruited as participants by incentive

The authors propose a hybrid framework called HySense to compensate for inadequate sensing opportunities solely provided by incentive mechanisms. Within each sensing cycle, HySense combines mobile devices with static sensor nodes to fulfill dynamic coverage constraints in terms of time and space. To balance sensing opportunities among different geographic regions, redundant users are efficiently migrated from densely populated areas to sparsely populated areas.

Due to the involvement of human beings in MCS, the realization of crowdsensing applications is driven by both temporal and spatial distribution of mobile device users. Owing to the regularity of human behavior patterns, the change of population density in different districts follows certain rules. We have collected some statistics to show spatial and temporal distribution of online smartphone users.

mechanisms, crowdsensing applications fail to offer reliable services. Thus, purely using incentive mechanisms cannot support crowdsensing applications, which operate around the clock. To compensate for inadequate sensing opportunities solely provided by incentive mechanisms, this article proposes a hybrid framework called HySense to integrate the advantages of participatory sensing and opportunistic sensing. HySense consciously enables sensor nodes as alternatives when mobile users are unavailable. User migration is allowed in HySense to balance sensing opportunities among different regions. A calibration mode is designed for checking whether participants' behavior patterns are consistent with task scheduling. HySense is suitable for all-day crowdsensing applications under the constraint of dynamic coverage.

STATE OF THE ART

Recent studies on mobile crowdsensing have enabled many crowdsensing applications and services, such as social interaction sensing, urban noise monitoring, mapping geographic locations, mobile object discovery, and road traffic/public transport monitoring. To support the above-mentioned applications, corresponding crowdsensing frameworks that involve participatory management, energy conservation, mobility prediction, programming interface, and so on have been designed.

Most existing crowdsensing frameworks follow three main stages, "recruiting-sensing-uploading." In the stage of recruiting, advanced incentive mechanisms are designed to identify well suited participants. Besides attracting enough participants to undertake subsequent sensing tasks, incentive mechanisms are required to minimize the incentive cost. In [7], Reddy *et al.* propose a recruitment framework for participatory sensing data collection. The framework selects participants from volunteers based on historic participation behavior. A reputation model is established to evaluate participants' willingness and diligence in data sensing and collection. The framework is designed to support crowdsensing applications that have made systematic guidelines for data collection.

In the stage of sensing, sensing accuracy and resource usage form a contradictory pair. Sensing accuracy can be improved through adding participants to the area of interest, increasing the frequency of data upload, and so on. However, the improvement of sensing accuracy incurs much resource usage at the same time. Thus, it is essential to design intelligent task assignment algorithms to make a trade-off between sensing accuracy and resource usage. In [8], Cardone *et al.* propose a geo-social crowdsensing platform. The platform consists of an Android mobile app and an infrastructure-side server. The former is designed to ease the delivery of crowdsensing tasks, while the latter functions as an administrator who manages crowdsensing tasks and associated incentives. For a specific geo-socially modeled region, the platform provides a good dimensioning of involved participants and sensing accuracy.

In the final stage, concerns are focused on reducing the cost of data upload. Due to huge volumes of data generated on the social scale, some

previous work aggregates sensor data through fusion computation on local mobile devices [9]. Besides, the existence of spatial correlation makes it feasible to upload part of the data while deducing the rest [10]. In [11], Wang *et al.* propose an energy-efficient mobile crowdsensing framework called effSense for cost-effective data uploading. EffSense empowers non-data-plan users and data plan users to upload data via different network gateways. By offloading data to low-power Bluetooth/WiFi gateways, the energy consumption concerned by non-data-plan users can be reduced. For data plan users, they are advised to piggyback data on a call so that the cost of data uploading can be saved by 55–65 percent.

OPPORTUNISTIC CHARACTERISTICS OF HUMAN DISTRIBUTION

Due to the involvement of human beings in MCS, the realization of crowdsensing applications is driven by both temporal and spatial distribution of mobile device users [12, 13]. Due to the regularity of human behavior patterns, the change of population density in different districts follows certain rules. We have collected some statistics to show spatial and temporal distribution of online smartphone users. In a civic center, new urban district, and suburb, we recorded the number of mobile device users who use 4G service to access a network at different times of three days. To guarantee the generalization of our findings, statistics were collected at the beginning, middle, and end of a month.

The areas of the study involve three districts, Zhonglou, Xinbei, and Wujin, in Changzhou, Jiangsu Province, China. Zhonglou district is located in the downtown area of Changzhou. It consists of 4423 cells. Xinbei is a new urban district located at the urban-rural fringe. There are 4541 cells within its territory. Wujin district is located in the outskirts of Changzhou. It is a university town that comprises 5957 cells. In Fig. 1, we recorded the number of mobile device users who use 4G service to access the network every three hours on May 5, May 15, and May 25, 2015. It can be observed that from 0:00 a.m. to 6:00 a.m., the number of online users in each district is much lower than that at other times of the day. The number of users peaked at noon and remained relatively stable from 9:00 a.m. to 21:00 p.m.. In the same period, there are great disparities in the number of users among the three districts. As a university town, Wujin has the largest number of users, with college students making up the majority. Zhonglou has more users than Xinbei because the downtown area attracts a larger population flow than a new urban district.

Statistics suggest that in the daytime, urban districts have more chance than suburbs to recruit sufficient numbers of participants. In the middle of the night, a small user base makes it difficult to recruit enough participants even though there are incentive mechanisms. On the other hand, imbalanced spatial distribution of population creates opportunities to compensate users in suburbs through user migration.

Inspired by the above-mentioned statistical analysis, we propose a hybrid framework called HySense. HySense possesses three characteristics.

First, within each sensing cycle, redundant users are efficiently migrated from densely populated areas to sparsely populated areas. Second, sensor nodes are introduced to compensate for insufficient sensing opportunities solely provided by incentive mechanisms. Third, uploaded sensor data is ensured to be evenly distributed over geographic regions.

HYBRID MOBILE CROWDSENSING FRAMEWORK

OVERVIEW

HySense is designed as a mobile service oriented architecture (SOA) that entails four stages: recruiting, sensing, uploading, and calibrating. The four stages are not carried out in sequence but interact with each other through feedback scheduling. Figure 2 is an overview of HySense. Components in HySense are entities connected by arrows. When an upper entity needs to obtain service or output from a lower entity, the workflow transition is represented by one-way arrows joining the two entities. If two entities are connected by a two-way arrow, it means the two entities form a feedback. In the feedback, the output of the upper entity will reversely work on the lower entity. The main innovative characteristics of HySense are as follows:

- Since the number of mobile device users is uneven in times of day and night, HySense involves sensing opportunities compensation in the phase of recruiting.
- HySense uses trigger time and trigger location to schedule sensing tasks so that batch upload of data from local areas can be avoided.
- Combining user recruiting and migration, HySense fulfills the dynamic coverage and balances sensing opportunities among different geographic regions.
- Due to subjective human initiative, participants might refuse to accomplish sensing tasks as planned. Calibration mode is designed to deal with participants backing out in advance.

DYNAMIC COVERAGE CONSTRAINT

A complex crowdsensing application comprises multiple sensing tasks. For ease of organization and management, MCS systems prefer to divide time into equal-length cycles and require each task to be finished in one cycle. The duration of one sensing cycle depends on the expected sampling frequency. In HySense, the duration of each sensing cycle is treated as a time restriction. Within the time limit, HySense needs to finish participant recruitment, task assignment, and task schedule by leveraging participatory and opportunistic sensing.

We use a practical implementation of an MCS-based project to clarify the design ideas behind HySense. Reviewing that in the CBD area of Abidjan, Cote d'Ivoire, 13 cellular towers are installed in the range of 7 km². With the help of a telecom operator, the city government released a series of MCS tasks through third generation (3G) cellular network infrastructure. The MCS tasks were aimed at monitoring air quality in the CBD area. The corresponding MCS system asked citizens of Abidjan

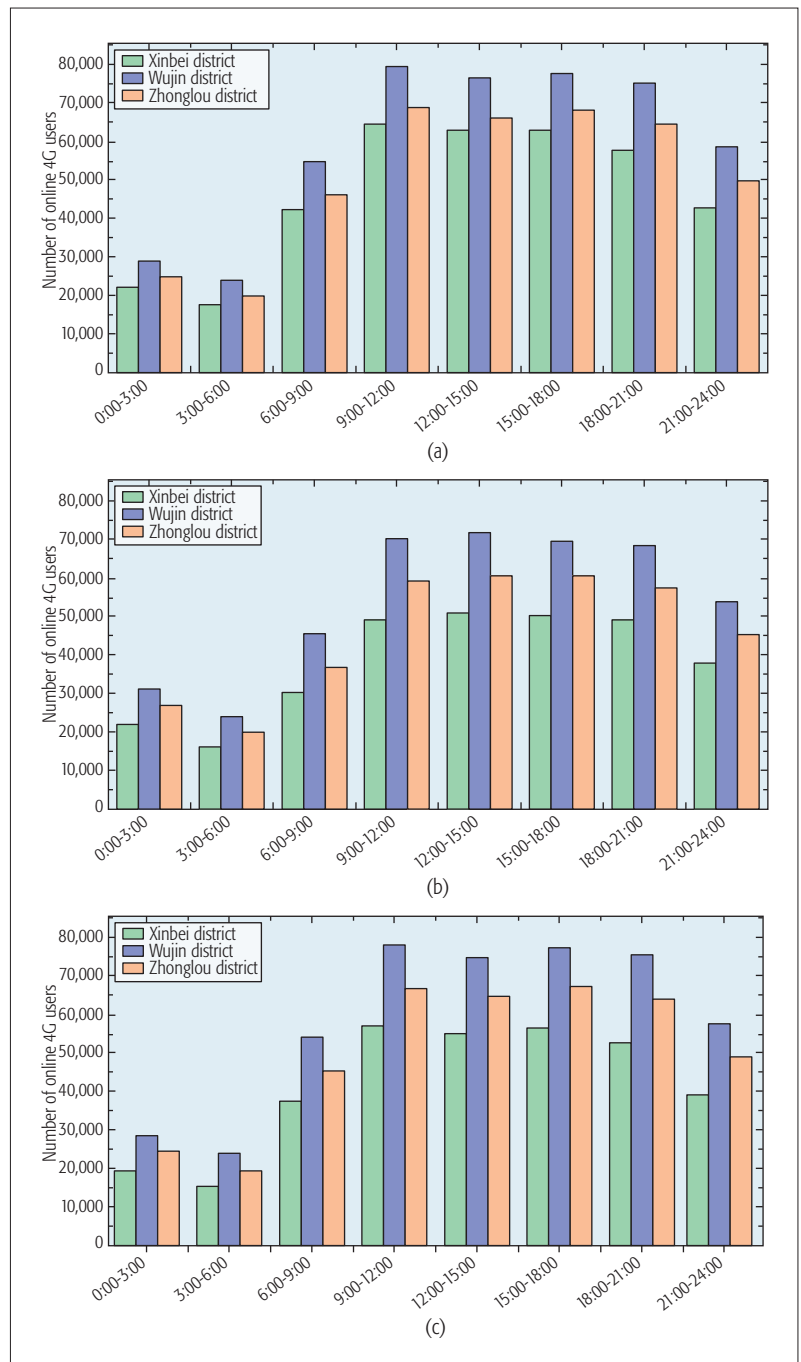


Figure 1. Trend of online 4G users in Changzhou, China: a) May 5, 2015; b) May 15, 2015; c) May 25, 2015.

to update the air quality every two hours (sensing cycle) for two weeks. To prevent biased measurements, the system requires at least 40 mobile users to upload sensor data, covering all 13 cells in each cycle. Since the distribution of users is time-varying in different cells, HySense provides two methods to assess the availability of users in terms of geographic and temporal coverage.

Geographic coverage is based on collective participant mobility [14, 15]. When a cellular tower receives the least required number of sensor data scattered across the cell, the air quality of the cell can be evaluated. However, due to the cluster behavior pattern of human beings, sensor data might be limited to a particular spatial

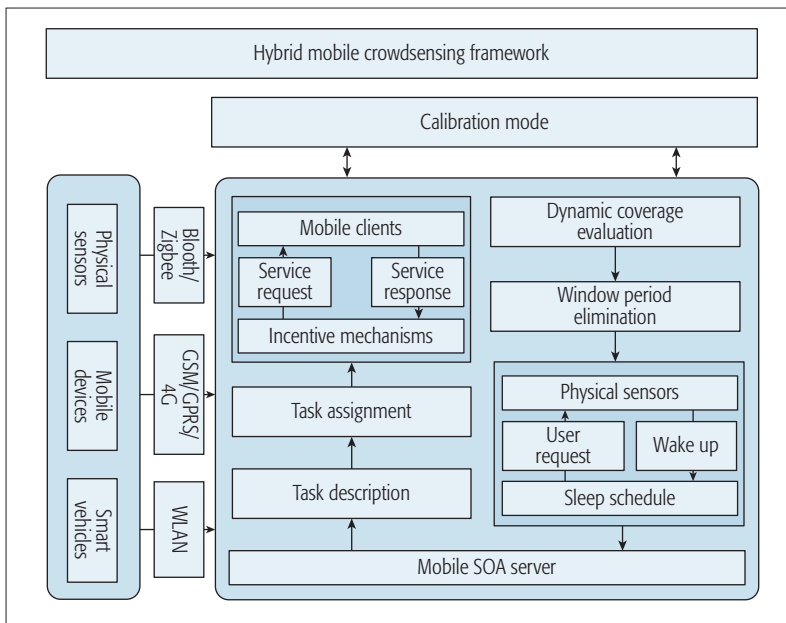


Figure 2. Overview of the hybrid mobile crowdsensing framework.

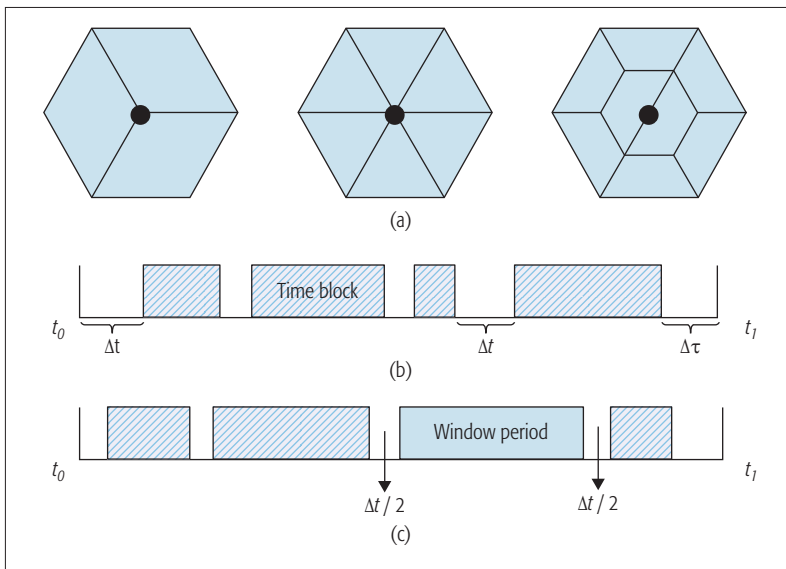


Figure 3. Dynamic coverage constraint in MCS.

region. For example, shopping malls are more likely to gather more people than parks. This spatial region is called a hotspot. Simply using data generated in a hotspot to evaluate an entire cell is biased. To make data evenly generated in the cell, we propose to divide cells into microcells. The uploaded sensor data is required to be evenly distributed to each microcell. The division of cells ensures a low spatial correlation between two neighbor microcells. The number of microcells is determined by the area of the cell. Figure 3a shows the generation of microcells through different partitioning schemes.

Given that sensor data have timestamps attached, temporal coverage refers to that within each sensing cycle; the timeline is evenly occupied by timestamps with restricted interval. Temporal coverage prevents biased monitoring results caused by bulk upload sensor data at a certain point in time. In HySense, we introduce

time blocks to evaluate the quality of temporal coverage. It is assumed that the duration of a sensing cycle is T , and the least required number of sensor data is N . Then each sensor data is required to be uploaded within T/N on average. The generation of a time block is as follows. From the moment of t_s to the moment of t_d , the interval time span is $t_{int} = t_d - t_s$. If the number of uploaded data is no less than $\lceil t_{int} * N/T \rceil$, the corresponding time block can be generated to occupy the timeline from t_s to t_d . As shown in Fig. 3b, the condition of full temporal coverage is that within a sensing cycle, the interval between the beginning of the first time block and the start time is no more than Δt , the interval between the end of the last time block and end time is no more than Δt , and the interval between adjacent time blocks is no more than Δt . If any interval mentioned above is exceeded, such an interval is called a window period. There is a $\Delta t/2$ gap between the window period and its adjacent time block. Figure 3c illustrates the existence of a window period when the interval between adjacent time blocks exceeds Δt .

TASK ASSIGNMENT POLICIES

HySense is a hybrid framework that integrates a sensor network system into classic MCS systems. Chicago provides a referential model of sensor network system deployment in urban areas. In Chicago, sensor nodes are installed on lamp-posts to collect environment information. These nodes do not violate privacy because they do not record medium access control (MAC) and Bluetooth addresses of mobile devices. Utilizing the above-mentioned model, smartphones along with sensor nodes are able to provide sensor data in HySense. Since sensor nodes are energy constrained but easy to control, while smartphones are rechargeable but it is hard to ensure stable sensing quality, HySense prioritizes the use of smartphones to enable large-scale applications and introduces sensor nodes as alternatives when sensing opportunities are inadequate or cannot be provided in time. Meanwhile, the dynamic coverage problem is addressed in HySense through feedback scheduling.

Initially, HySense splits tasks into smaller, manageable subtasks. A complete subtask involves data sensing and uploading. Each subtask is described by a tuple that consists of its trigger time and trigger position. Through an incentive mechanism (e.g., auction-based), subtasks can be assigned to candidate participants. According to candidate participants' claim to different subtasks, a task list can be created. HySense utilizes tuples of each subtask from the list to evaluate the quality of temporal and geographic coverage, respectively. Then HySense can deal with the window period during which no data is uploaded.

ELIMINATION OF WINDOW PERIOD

Since the population changes over time, before the arrival of a window period, HySense still has opportunities to narrow or even eliminate the window period. Thus, HySense keeps recruiting users to participate in sensing tasks that are to be triggered during the window period. As time goes, new users might be added to narrow

ID	Name	Latitude	Longitude	Value	Region	Time
5	Gangyu glass store	41.929118	123.398584	114	0_1	5/04/2015 14:00:00
6	Jinhong supermarket	41.927316	123.398584	99	0_1	5/04/2015 14:00:00
7	Tangxuan capitals	41.92841	123.398584	104	0_1	5/04/2015 14:00:00
8	Boya teaching building	41.931905	123.398584	110	0_2	5/04/2015 14:00:00
9	Laboratory building	41.932019	123.398584	93	0_3	5/04/2015 14:00:00
10	Yixin teaching building	41.931898	123.398584	127	0_4	5/04/2015 14:00:00
11	Comprehensive service building	41.93163	123.398584	96	0_5	5/04/2015 14:00:00

Table 1. The format of a sensing record.

the window period. HySense sets a time threshold t_{th} to limit the maximum length of recruiting time. If the window period cannot be eliminated t_{th} before the arrival of the window period, HySense believes that it cannot recruit enough participants in time. HySense calculates the current length of the window period t_w and turns to schedule sensor nodes as alternatives. The number of sensor nodes used to eliminate the window period is $\lceil T_w * N/T \rceil$.

HySense allows redundant users' migration for eliminating neighbor cells' window periods. In the process of candidate participants recruitment, HySense judges which cell has a surplus of users and no window period, it communicates with its neighbor cells C_{nei} through cellular towers. Then C_i will receive tuples of the subtasks scheduled to be triggered during the C_{nei} ' window period. HySense allows redundant users who fail to apply for subtasks in C_i to be turned into candidate participants in C_{nei} . These users determine whether to accept the subtasks based on their travel plan and traffic mode. When a user applies for subtasks in C_{nei} , the cellular tower in C_i will send notification messages of user migration to C_{nei} , so C_{nei} can narrow the window period and refresh task lists.

EXCEPTIONAL CASE HANDLING

To improve task execution reliability, we design a calibration mode in HySense. In the calibration mode, HySense protects against malicious users who successfully apply for a subtask but refuse to do it. On the other hand, if an unforeseen event occurs and normal users cannot perform their tasks as planned, HySense can deal with such a problem in advance.

HySense requires each participant to periodically upload his/her current position. According to location history, HySense judges whether the participant is approaching the task trigger location and whether the participant can arrive there before the trigger time. If a participant refuses to report its position three times in succession, HySense considers the participant as a malicious user. The subtask applied by the participant will be removed in the task queue and reassigned by HySense. For normal participants who report positions in time, HySense first removes the participants whose mobility traces are further away from trigger locations. The remaining participants need to be evaluated as to whether they can arrive at

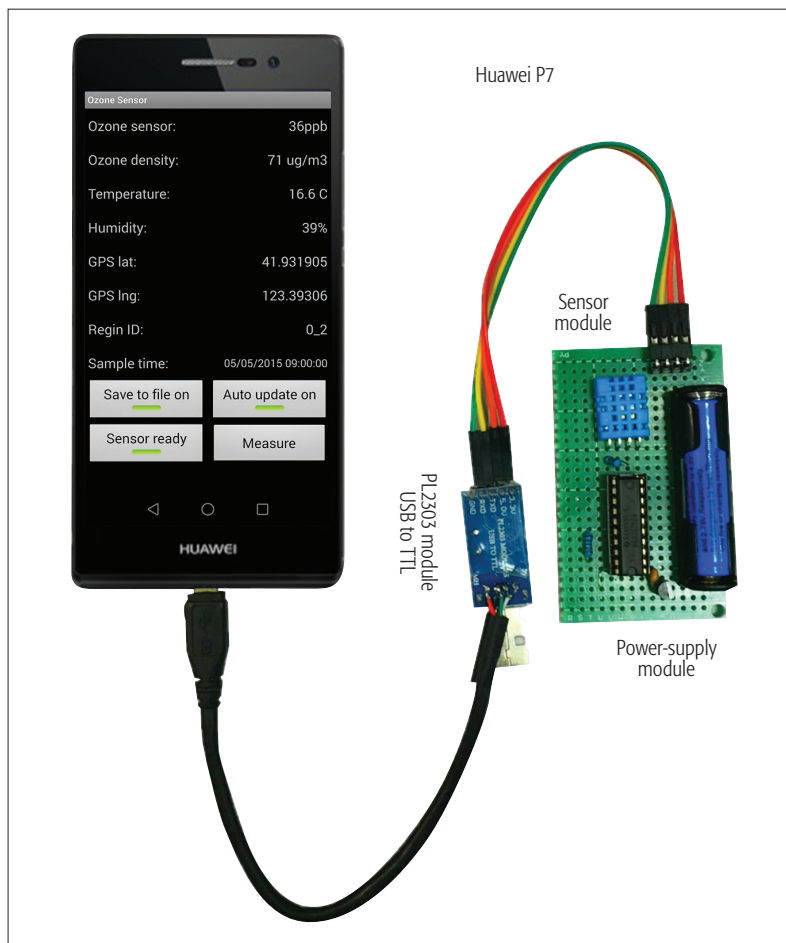


Figure 4. Mobile hardware device for ozone sensing.

trigger locations in time. HySense uses average movement speed of participants as the evaluation criterion. Since elapsed time equals the reporting period, while distance information can be provided by location history, average speed can be obtained through the moved distance divided by the elapsed time. HySense keeps updating participants' average speed and the interval between current instant and trigger time. If the product of current interval and current speed is less than the distance between current position and trigger location, HySense considers that the participant cannot finish the task in time. From the current instant, HySense recruits additional users near the trigger location to take over the subtask. At t_{th}

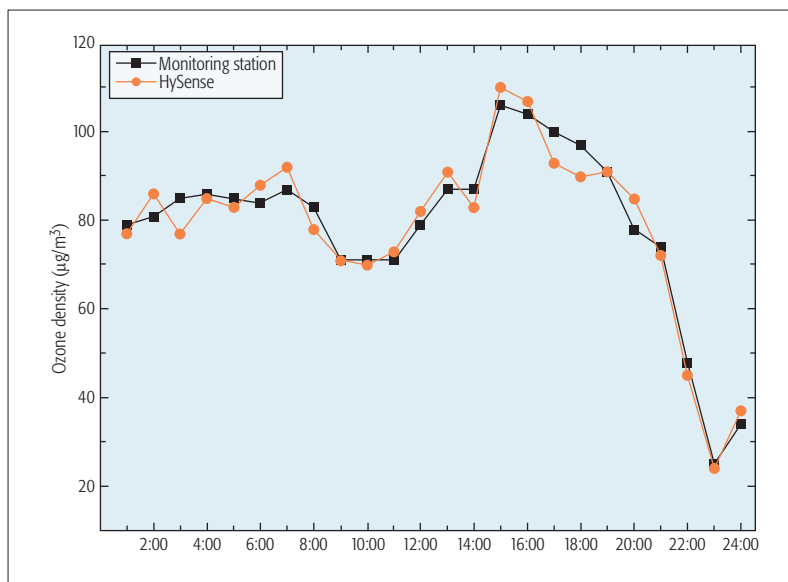


Figure 5. Concentration distribution of ozone on May 5, 2015.

before trigger time, if no users are willing to take over the subtask, HySense turns to waking up sensor nodes as alternatives.

SYSTEM EVALUATION

We evaluate the performance of HySense in terms of precision because it is of particular concern to crowdsensing applications. A prototype of HySense is implemented to realize the application of ozone concentration monitoring at Liaoning University, Shenyang, China. The experiment ran for one month from 4 May 2015 to 5 June 2015. To validate the precision of HySense, in the experiment, we use ozone data from a monitoring station located in the university as the reference standard.

We set the sensing cycle to be one hour. Default parameters Δt and T_{th} are set to be eight minutes and five minutes, respectively. As shown in Fig. 4, we designed a specific hardware device to make ozone monitoring feasible for mobile users. It can be observed that an external sensor module is connected to a smartphone by a USB/R232 bidirectional converter like PL2303. The sensor module is powered by battery. HySense asked at least 80 participants from 300 volunteers who held the smartphones to upload sensor data, covering all 20 microcells in each cycle. One hundred fifty MiCS-OZ-47 ozone sensor nodes are also evenly deployed on the university campus for sensing opportunities compensation.

Table 1 shows the format of the sensing record collected by mobile users. Each record includes name, latitude, longitude, sensor value, microcell ID, and timestamps. The precision of HySense can be revealed by comparing its output to the monitoring station. Figure 5 illustrates the value of ozone obtained by HySense and the monitoring station on May 5, 2015. It can be observed that HySense performs steadily and accurately around the clock.

CONCLUSION

In this article, we have proposed a hybrid framework named HySense to combine mobile crowdsensing with static sensing. Besides incentive

mechanisms, HySense introduces sensor nodes to compensate for inadequate sensing opportunities. Within each sensing cycle, the window period is eliminated so that temporal coverage can be ensured around the clock. Redundant user migration is allowed in HySense to balance sensing opportunities among different regions. To improve task execution reliability, we designed a calibration mode for checking whether the participants' behavior patterns are consistent with task queues. Any change in task queues can be dealt with in advance. In further research, we will pay more attention to establishing a prediction model of population. Through the prediction of future crowds in certain regions, HySense has more agility and adjustable space to schedule mobile users.

ACKNOWLEDGMENT

The work is supported by the Qing Lan Project and the National Natural Science Foundation of China under Grant No. 61572172, the Fundamental Research Funds for the Central Universities, No. 2016B10714, the Changzhou Sciences and Technology Program, No. CE20165023 and No. CE20160014, and the Six talent peaks project in Jiangsu Province, No. XYDXXJS-007. This research is also supported by a strategic research grant from City University of Hong Kong, No. 7004615.

REFERENCES

- [1] E. Macias, A. Suarez, and J. Lloret, "Mobile Sensing Systems," *Sensors*, vol. 13, no. 12, 2013, pp. 17,292–17,321.
- [2] R.K. Ganti, F. Ye, and H. Lei, "Mobile Crowdsensing: Current State and Future Challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, 2011, pp. 32–39.
- [3] H. Ma, D. Zhao, and P. Yuan, "Opportunities in Mobile Crowd Sensing," *IEEE Commun. Mag.*, vol. 52, no. 8, Aug. 2014, pp. 29–35.
- [4] B. Guo et al., "Mobile Crowd Sensing and Computing: The Review of an Emerging Human-Powered Sensing Paradigm," *ACM Comp. Surveys*, vol. 48, no. 1, 2015, article 7.
- [5] H. Xiong et al., "EEMC: Enabling Energy-Efficient Mobile Crowdsensing with Anonymous Participants," *ACM Trans. Intell. Sys. Tech.*, 2015, vol. 6, no. 3, article 39.
- [6] X. Zhang et al., "Incentives for Mobile Crowd Sensing: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 1, 2016, pp. 54–67.
- [7] S. Reddy, D. Estrin, and M. Srivastava, "Recruitment Framework for Participatory Sensing Data Collections," *Int'l. Conf. Pervasive Comp.*, 2010, pp. 138–55.
- [8] G. Cardone, L. Foschini, and P. Bellavista, "Fostering Participation in Smart Cities: A Geo-Social Crowdsensing Platform," *IEEE Commun. Mag.*, vol. 51, no. 6, June 2013, pp. 112–19.
- [9] C. Wietfeld, C. Ide, and B. Dusza, "Resource Efficient Mobile Communications for Crowd-Sensing," *51st ACM Design Automation Conf.*, 2014, pp. 1–6.
- [10] L. Kong et al., "Embracing Big Data with Compressive Sensing: A Green Approach in Industrial Wireless Networks," *IEEE Commun. Mag.*, vol. 54, no. 10, Oct. 2016, pp. 53–59.
- [11] L. Wang et al., "effSense: A Novel Mobile Crowd-Sensing Framework for Energy-Efficient and Cost-Effective Data Uploading," *IEEE Trans. Sys., Man, and Cybernetics.: Sys.*, vol. 45, no. 12, 2015, pp. 1549–63.
- [12] X. Hu et al., "Multidimensional Context-Aware Social Network Architecture for Mobile Crowdsensing," *IEEE Commun. Mag.*, vol. 52, no. 6, June 2014, pp. 78–87.
- [13] D. Zhao et al., "COUPON: A Cooperative Framework for Building Sensing Maps in Mobile Opportunistic Networks," *IEEE Trans. Parallel Distrib. Sys.*, vol. 26, no. 2, 2015, pp. 392–402.
- [14] P. Sharma, S. M. Salapaka, and C. L. Beck, "Entropy-Based Framework for Dynamic Coverage and Clustering Problems," *IEEE Trans. Automated Control*, vol. 57, no. 1, 2012, pp. 135–50.
- [15] R. Yu et al., "RAQ-A Random Forest Approach for Predicting Air Quality in Urban Sensing Systems," *Sensors*, vol. 16, no. 1, 2016, article 86.

BIOGRAPHIES

GUANGJIE HAN [S'01, M'05] (hanguangjie@gmail.com) is currently a professor with the Department of Information & Communication Systems at Hohai University, China. He finished his work as a postdoctoral researcher with the Department of Computer Science at Chonnam National University, Korea, in 2008. From October 2010 to 2011, he was a visiting research scholar with Osaka University, Suita, Japan. He has served as an Editor of *IEEE Access*, *Telecommunication Systems*, *IJAHUC*, *TIS*, and *JIT*. His current research interests include sensor networks, green computing, cloud computing, and mobile computing.

LI LIU (liulihuc@gmail.com) is currently pursuing his Ph.D degree from the Department of Internet of Things Engineering at Hohai University. He received his B.S. degree in internet of Things engineering from Hohai University in 2014. His current research interests are connectivity and coverage for wireless sensor networks.

SAMMY CHAN [S'87-M'89] (eeschan@cityu.edu.hk) received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and his Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995.

From 1989 to 1994, he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994, he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

RUIYUN YU (yury@mail.neu.edu.cn) received his M.S. degree in computer science in 2004 and B.E. degree in mechanical engineering in 1997, both from Northeastern University, China. Currently he is a professor with the Computing Center of Northeastern University, China. His research interests include wireless ad hoc communication, efficient routing and data processing in sensor networks, and industrial wireless networking technology. From September 2006 to October 2007, he worked as a visiting researcher in the Center for Research in Wireless Mobility and Networking at the University of Texas at Arlington.

YU YANG (yy388@cs.rutgers.edu) is a graduate student in the Department of Computer Science at Rutgers University. He received his B.E. degree from Northeastern University. His research interests include mobile and pervasive computing, vehicular networks, and urban computing.

Enhanced C-RAN Using D2D Network

Kazi Mohammed Saidul Huq, Shahid Mumtaz, Jonathan Rodriguez, Paulo Marques, Bismark Okyere, and Valerio Frascolla

The authors show, together with standardization aspects, how combining C-RAN and D2D technologies can help to solve the delay issue and fulfill most of the targets specified for 5G networks in terms of delay, capacity, energy efficiency, mobility, and cost.

ABSTRACT

With the surge in smartphone sensing, wireless networking, and mobile social networking techniques, mobile crowdsensing (MCS) has become a promising paradigm for 5G networks. An MCS system's service quality heavily depends on the platform, which brings the users under a common cloud with very low delay. Therefore, MCS needs a new platform that brings the best not only from the user's perspective, but also from the operator's perspective. In this article, we propose a novel architecture for MCS by combining two technologies, those being C-RAN and D2D. C-RAN is a promising enabling technology that can at the same time cope with the ever increasing mobile traffic demand and reduce the surging costs experienced by service operators. In spite of the many advantages offered by C-RAN, one of the main concerns for operators is its associated fronthaul delay. To handle such delay, we come across this D2D solution in C-RAN networks. D2D is adopted as an effective candidate for very low delay between links and has already provided evidence of its potential for novel business opportunities. This article shows, together with standardization aspects, how combining C-RAN and D2D technologies can help to solve the delay issue and fulfill most of the targets specified for 5G networks in terms of delay, capacity, energy efficiency, mobility, and cost.

INTRODUCTION

The demand for wireless mobile data has continued to rise, leading to a surge in the number of smart devices in use throughout the world. They are usually equipped with a rich set of sensors, including GPS, microphone, camera, accelerometer, and gyroscope, among others. As a consequence, these devices generate a huge amount of data, and according to an Ericsson report [1], on average a laptop will generate 11 GB, a tablet 3.1 GB, and a smartphone 2 GB of data per month by the end of 2018. Mobile crowdsensing (MCS) [2] has come onto the scene recently as a promising large-scale data sensing collection paradigm where the collection is usually performed by smartphones. It is a method that provides the pervasiveness of sensor-equipped mobile devices such as smartphones to collect data. The enormous amount of data is then shared and sent to an MCS central collector that is running on the cloud (as show in Fig. 1). Mobile crowdsensing is projected to become one of the most important technologies contributing to healthcare, moni-

toring, logistics, and organization in future smart cities. This huge process of data collection is impeded by current delay tolerance in MCS. To alleviate this delay, we are proposing the novel idea of cloud RAN (C-RAN)-based device-to-device (D2D) networking. D2D is one of the key technologies that can reduce the delay in current MCS systems. In D2D communications mode [3], devices can communicate with each other without the intervention of base stations and provide less delay between devices. Along with D2D, C-RAN will provide reduced signaling overhead and a reduction in the capital expenditure (CAPEX) and operating expenditure (OPEX) of an overall MCS system. Moreover, C-RAN and D2D will be a part of the fifth generation (5G) network and expected to fulfill most 5G requirements. There is already a general consensus on the requirements of a 5G network, which are [4]:

- **Capacity:** 1000× increase in area capacity
- **Delay:** 1 ms round-trip time (RTT) delay
- **Energy:** 100× improvement in energy efficiency in terms of Joules/bit
- **Cost:** 10–100× reduction in cost of deployment
- **Mobility:** Seamless indoor/outdoor mobility and always-on connectivity for high-throughput users

C-RAN is one of the highly anticipated 5G enabling technologies that can optimize network performance and reduce CAPEX/OPEX for the next generation wireless systems [5]. It has a centralized entity to support advanced joint radio resource and mobility management. The C-RAN access separates the baseband units (BBUs) from radio front-ends, also called remote radio heads (RRUs), using a transport link, which is known as the fronthaul (FH), as shown in Fig. 1a. This new framework enables centralized and cooperative techniques. In addition to controlling multi-cell and multi-user in unison, C-RAN is also well equipped for system deployment with multi-radio access technologies (RATs) and multi-layer network coexistence, referred to as heterogeneous networks (HetNets) [6]. Along with its many advantages, C-RAN also has some inherent drawbacks, the most relevant of which for our study is the user plane delay, mainly due to the FH effects, meaning the RTT from C-RAN to end users (C-RAN ↔ FH ↔ users). To alleviate this delay problem, we propose tighter integration of D2D into C-RAN.

D2D is adopted as an effective and efficient candidate for very low delay in 5G [7]. D2D communication can serve as a candidate paradigm to

Feature name	CoMP	C-RAN	D2D	D2D: C-RAN
Standardization	3GPP Release 11-12	IEEE	3GPP Release 11-12	3GPP and IEEE
Frequency band	Licensed bands	Licensed bands	Licensed bands	Licensed/unlicensed bands
Max Transmission distance	500 m	100 m / 1000 m ¹	20 m	100 m/1000 m
Capacity ²	Good (500–600 Mb/s)	Good (500-600 Mb/s)	Very good (1 Gb/s)	Excellent (2 Gb/s)
Delay	>1 ms	>1 ms	“Zero delay”	“Zero delay”
Uniformity of service provision	No	No	Yes	Yes
Application	Improved capacity at cell edge. Longer battery life of handsets. Complete operator control.	Improved capacity and coverage at cell center and edge. More energy efficient than CoMP.	Improved capacity and coverage at cell center and edge. More energy-efficient than CoMP and C-RAN. Relaying in cellular networks, safety in public services, sharing in context based applications.	Combination of C-RAN and D2D.
Infrastructure	Within licensed bands, a central controlling unit such as eNB is used for transferring data.	Within licensed bands, a radio controlling cloud is used for transferring data.	Data transfer between users occurs directly, be it licensed or unlicensed bands.	Data transfer between users occurred in licensed bands directly. It is managed by a cloud central controller.
Expenses	CAPEX: Subsidized hardware. Commissioning new cell sites and towers. OPEX: Communication haul (i.e., FH). Leasing and electric power consumption of the cell site. Operational cost of eNBs.	CAPEX: Subsidized C-RAN (BBU) hardware. Installing new RRU. OPEX: Communication haul (i.e., FH). Leasing and electric power consumption of the cell site. Operational cost of RRUs.	CAPEX: no expenses since users are using their devices, which are of similar terminal types. OPEX: usage of battery of the device.	Combination of C-RAN and D2D.

¹ 100 m is for mmWave at 60 GHz and 1000 m is for fiber.

² These values are calculated under ideal channel and traffic condition and with 2×2 MIMO using 20 Mhz of bandwidth.

Table 1. Comparison of technologies.

improve spectrum efficiency as well. In fact, by reusing the spectrum, two D2D users can form a direct data link without the need for routing through base stations (BSs) and core networks (CN). In D2D, reducing the distance between transmitters and receivers also makes a cellular system more energy-efficient. Moreover, D2D communication is the perfect candidate for centralized location-based services that enable efficient, flexible, and secure applications, including social networking applications. These affect users' interests, locations, and mobility, all important elements in D2D communications.

All of the above have led us to develop a new communication architecture called D2D-based C-RAN. The combination between C-RAN and D2D will be a game changer for future 5G systems, which will provide more answers than questions w.r.t. the coexistence of different types of communication protocols, services, and devices within a single network. This novel architecture can help solve most of the problems related to emerging 5G systems (capacity, delay, energy efficiency, CAPEX/OPEX, and mobility). Table 1 shows a comparison of D2D-based C-RAN with existing LTE-Advanced (LTE-A) technologies, like cooperative multipoint (CoMP), also taking into consideration the main architectural blocks of the communication network, like the evolved NodeB (eNB).

The rest of the article is organized as follows. We describe the state of the art of the topics in focus, we elaborate on the standardization activities of C-RAN and D2D, and explain the overall architecture and protocol stack of D2D-based C-RAN networks, we give an overview on system models along with simulation results, and finally, future research directions and concluding remarks are provided.

STATE OF THE ART

So far, data offloading from mobile CNs has been an active area of research from industrial and academic stakeholders, as a means toward virtualization by transferring heavy computational operations to resourceful cloud servers, also promoting novel services that far exceed traditional mobile devices' processing power. For example, [8] presents two data offloading approaches, which are currently used in most of the literature:

- Reducing the execution time of mobile applications using remote cloud resources, for example, by offloading selected computing tasks executed on mobile devices to the cloud
 - Enabling nearby devices (mobile devices or small cell BSs or WiFi) to work collaboratively as cloud resource providers
- Similarly, [9] presents a two-layered HetNets

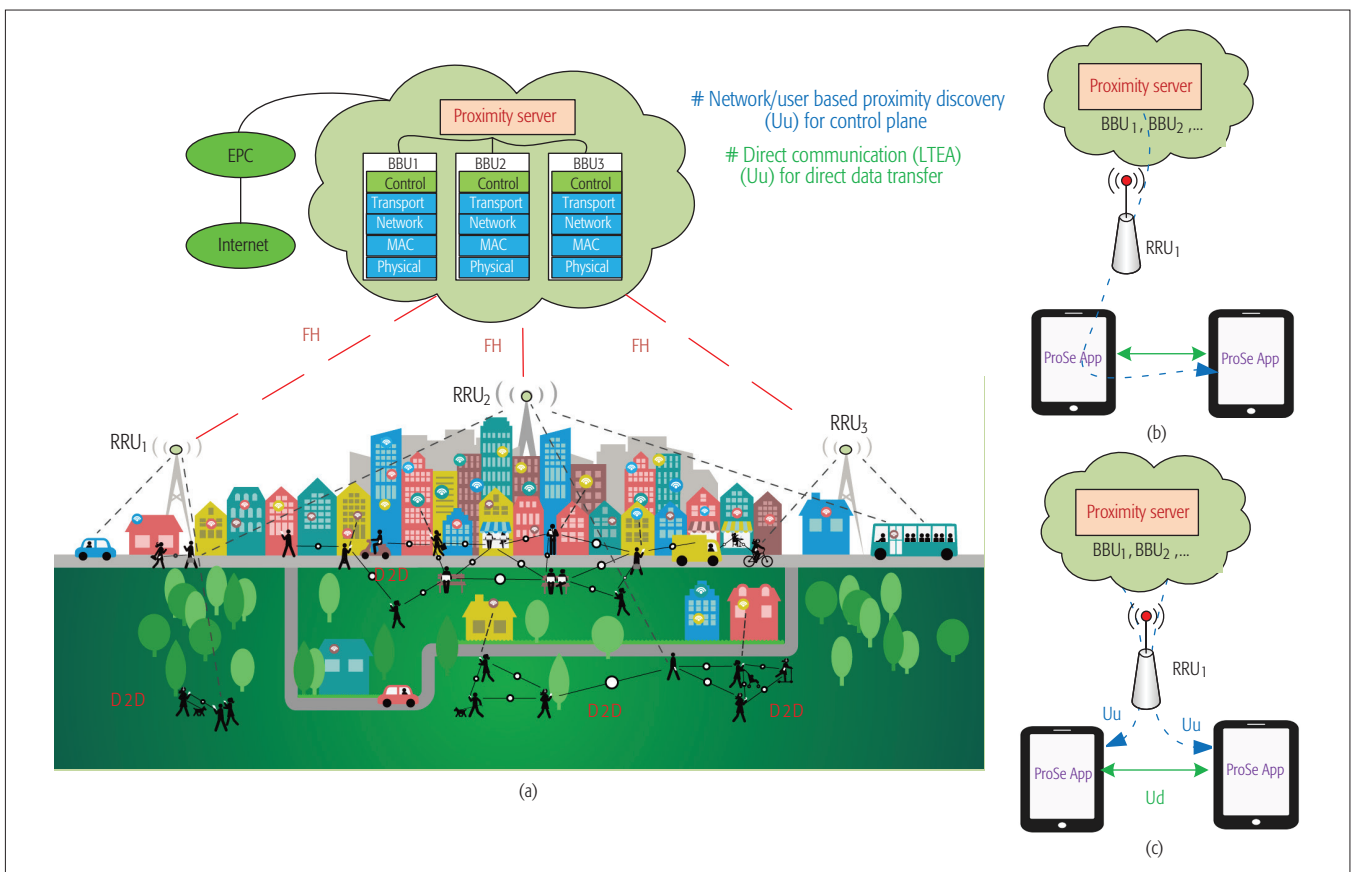


Figure 1. Novel D2D based C-RAN Scenario for MCS: a) novel D2D-based scenario; b) cloud core architecture for D2D; c) cloud access architecture for D2D.

architecture where mobile cloud computing is utilized, focusing more on the cloud computing phenomenon in terms of service provisioning rather than RAN perspective. A new load balance factor is introduced in [10] for D2D assisted HetNets, which provides a novel framework for D2D offloading. Finally, the seminal work [3] introduces cellular D2D communications just as a means to introduce offloading techniques and to improve the signal-to-interference-plus-noise ratio.

All the above mentioned works either consider D2D or cloud based mechanism to offload the traffic from mobile CN. To the best of our knowledge, this article is the first effort to take the best of both technologies, proposing a novel syndicate architecture for offloading traffic from the CN.

STANDARDIZATION ACTIVITIES

C-RAN will most probably be standardized by IEEE. The IEEE standards body 802.15 started the P802.15 [11] project in January 2014 on C-RAN fronthauling, common public radio interface (CPRI) [12], user plane, control plane, transport mechanisms, and synchronization techniques. This project is still in its infancy; nevertheless, China Mobile [5] already started proprietary C-RAN networks deployment, as well as several service providers and equipment manufacturers. An alignment of the work done in IEEE with the work ongoing in other relevant standards bodies is still an open point and will be one of the main focuses of the activities in 2016. D2D standardization activities, ruled by the Third Generation Partnership Project (3GPP), and in that context

called “proximity services,” started in 2011 under Release 12 with Work Item (WI) “FS_ProSe” and Technical Report (TR) 22.803, which created three new TRs (36.843, 23.703, and 33.833), on radio, architectural, and security aspects, respectively. Due to the large number of Stage 1 service requirements defined, it was decided to limit the Release12 normative work to a set of basic functionalities, e.g. broadcast (public safety) communication and D2D discovery in network coverage [13], by both enhancing existing Technical Specifications (TSs) and creating new TSs (23.303, 24.333 and 24.334). In 2014 Release 12 was frozen, and the non-addressed Stage 1 requirements and Stage 2/3 normative text moved to Release 13, frozen at the end of 2016. Among the D2D features currently under definition one can mention WLAN interworking, service continuity, handling of relays, and more refined discovery mechanisms. Finally, it is worth highlighting that the D2D work done so far focused on new functionalities only for the LTE access technology, briefly touching on WLAN interworking but leaving 3G and 2G aspects for future 3GPP Releases.

D2D-BASED C-RAN ARCHITECTURE

The proposed novel architecture is divided into two main parts, as shown in Fig. 1.

C-RAN

We consider a smart city scenario, focusing on a use case where most of the users are in close proximity and communicate with each other using their user equipment (UE) via D2D connection

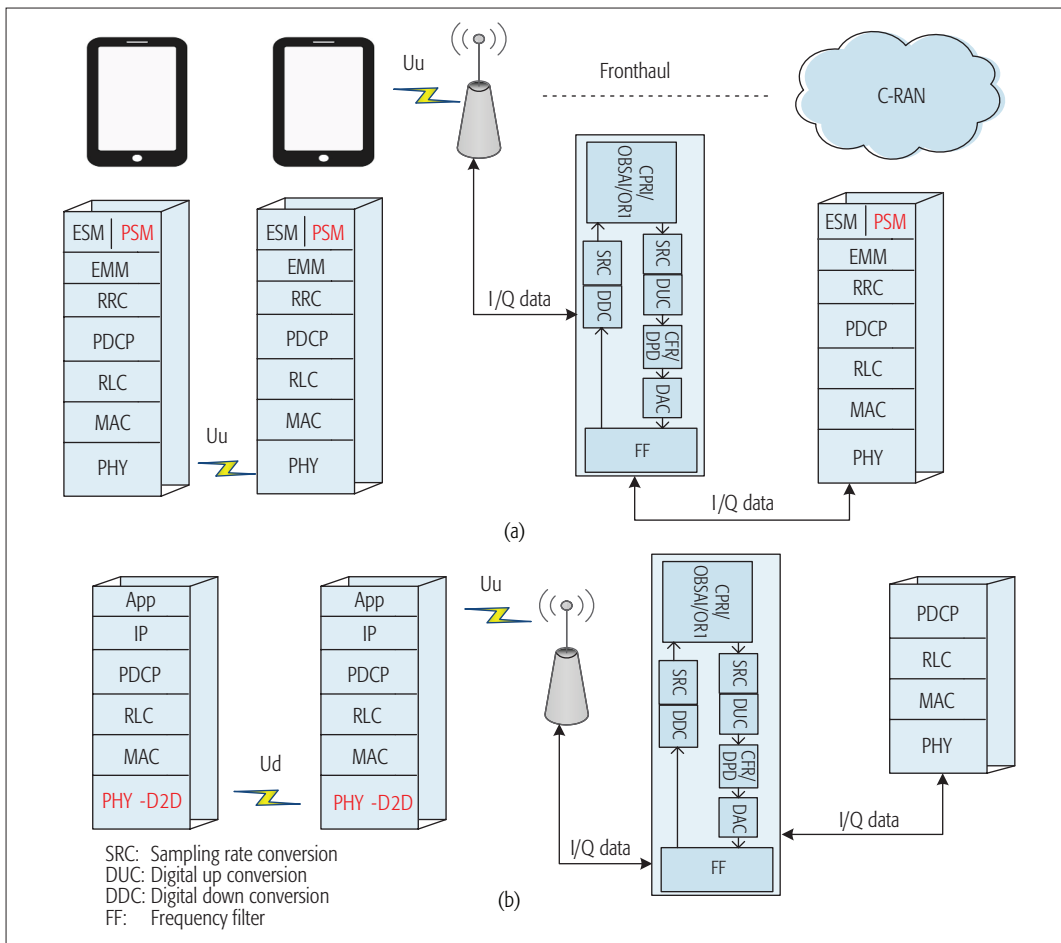


Figure 2. C-RAN-based D2D protocol stack: a) C-RAN-based D2D: control plane protocol; b) C-RAN-based data plane protocol.

(UE1 ↔ UE2). Along with D2D users, we also consider normal cellular users who communicate via RRUs (UE1 ↔ RRU ↔ UE2). RRUs are deployed for radio coverage and can be picocells or microcells depending on the specific use case under consideration, but for the sake of simplicity we refer to them all as RRUs in this article. An RRU is only used to transfer radio signaling, whereas all other signaling processing/baseband processing – physical (PHY), medium access control (MAC), transport, and control) – is done in the C-RAN.

In C-RAN, baseband processing is centralized and shared among sites in a virtualized BBU pool. This means that it is very much able to adapt to smart city non-uniform traffic and utilizes the available resources (i.e., the BSs) more efficiently. Not only are fewer BBUs needed in C-RAN compared to the traditional architecture, but also C-RAN has the potential to decrease the cost of the network operation, because power and energy consumption are reduced. New BBUs can be added and upgraded easily, thereby improving scalability and easing network maintenance. Virtualized BBU pools can be shared by different network operators, allowing them to rent RAN as a cloud service. Therefore, mechanisms introduced for LTE-A to increase spectral efficiency, interference management, and throughput, such as enhanced inter-cell interference coordination (eICIC) and CoMP, are greatly facilitated.

In spite of several advantages, one of the main disadvantages of C-RAN is the user plane delay due to the FH, which should be less than 1 ms according to 5G. To alleviate this delay problem, we propose D2D integration into C-RAN.

D2D NETWORK

D2D proposes to be a “zero delay” technology for 5G networks and will solve the FH delay problem in C-RAN. To enable D2D communication in a C-RAN architecture, we propose a proximity server that resides inside the C-RAN, with interfaces connected to each BBU as shown in Fig. 1a.

The proximity server functionality can be split up into two portions, proximity discovery and direct communication, as shown in Fig. 1b. The major function of proximity discovery is to discover users that are in proximity. This discovery mechanism can be user-assisted or network-assisted, which can also perform as a standalone application to users such as in social networking where a direct communication does not need to be triggered. Direct communication is initiated when proximity discovery is not needed to transfer data [7, references therein].

For the control plane in the access network of C-RAN, the cellular access link (Uu) is utilized by proximity, whereas for the data plane a novel direct mobile communication interface (Ud) is required for direct communication between devices, as shown in Fig. 1c.

D2D proposes to be a “zero delay” technology for 5G networks and will solve the FH delay problem in C-RAN. To enable D2D communication in a C-RAN architecture, we propose a proximity server which resides inside the C-RAN, with interfaces connected to each BBUs.

C-RAN-BASED D2D PROTOCOL STACK

Figure 2 shows the layers, interfaces, and protocols that compose the control plane and the data plane of an LTE-A architecture, extended to include D2D C-RAN functionalities by the blocks highlighted with red characters. The LTE-A non-access stratum can be decomposed into several sublayers, the main ones being EPS Mobility Management (EMM) and EPS Session Management (ESM) [14]. In order to handle the D2D bearer management in C-RAN, as shown in Fig. 2a, a proximity services (ProSe) management (PSM) entity is introduced, thus giving rise to an enhanced FH connection that we call “extended control plane.” Each D2D user is also connected to an RRU over the Uu interface. The RRU sends and receives I/Q data, caters for the interface to the C-RAN via fiber, and executes digital processing, digital-to-analog and analog-to-digital conversions, power amplification, and filtering.

The PSM procedures establish and manage the direct radio path bearer. In contrast to presently available LTE-A systems, where the radio bearer is ended at the eNB and the UE, the termination point of the direct radio path communication is located at the two D2D UEs’ side. Therefore, the configuration of PSM rendered by the C-RAN to

both UEs should be compatible with each other. In addition, the adjustment of radio link handover, measurement, and monitoring is required to adapt direct path aspects.

Figure 2b focuses on the data plane protocols of an LTE-A system and brings in the novel interface named Ud for the data plane, which is enhanced at the PHY layer with D2D functionalities [15]. Radio bearers — one or more than one — are established for the data plane transmission over direct path transmission. The PHY, MAC, radio link control (RLC) and packet data convergence protocol (PDCP) layers of the wireless protocol stack for these radio bearers are all ended at the respective UE side.

SYSTEM MODEL AND SIMULATION RESULTS

In order to efficiently analyze the performance of D2D-based C-RAN, we have enhanced an existing system level simulator (SLS) with a centralized cloud entity that control all the baseband processing [7], an RRU which acts as an antenna, and a D2D users’ pair. We provide key simulation parameters in Table 2.

Moreover, we also enhanced the following key performance indicators (KPIs) to evaluate the performance of the proposed system. Those are explained in the following.

End-to-End Delay: This performance metric relates to the network delay (RTT), which is measured as the time between a packet being available at the transmitter and the availability of this packet at the receiver in milliseconds.

Throughput (with ideal FH): The average throughput per cell is defined as the sum of the total amount of bits being successfully received by all active users in the system divided by the product of the number of cells being simulated in the system and the total amount of time spent in the transmission of these packets (the simulation time for LTE is TTI (1 ms)). The mathematical expression is given in the following:

$$\text{Throughput} = \frac{\sum_{c=1}^c \sum_{u=1}^U b_c^u}{N_{\text{cells}} \times T_{\text{sim}}} \quad (1)$$

where

N_{cells} is the total number of cells being simulated.

T_{sim} is the simulation time per run.

b_c^u is the number of bits received with success user u in cell c .

Throughput (with Non-Ideal FH): The average throughput per cell is defined as the sum of the total amount of bits being successfully received by all active users in the system divided by the product of the number of cells being simulated in the system, the total amount of time spent in the transmission of these packets (the simulation time for LTE is TTI = 1 ms), and the delay of FH link (10 ms).

DELAY ANALYSIS

Figure 3 shows the end-to-end (E2E) delay experienced by the devices. The number of cellular users in each cell is 30, and they are distributed in close proximity. In this result we use a non-ideal FH link, which can increase E2E delay up to 10 ms. There are a total of 20 D2D pairs in each cell,

Name	Parameter	
System	LTE-A, 20 MHz, 2.6 GHz	
Resource block (RB)	100	
Duplexing method	Cellular: FDD (downlink)	
	D2D: FDD (uplink using TDD timeslot)	
Mode selection	Shortest distance (cellular or D2D)	
Resource allocation	Fixed allocation	
Channel estimation	Perfect	
Channel models	Between D2D	$40 \log_{10} d[m] + 30 + 30 \log_{10}(f [\text{MHz}] + 49)$
	RRU → D2D	$36.7 \log_{10} d[m] + 40.9 + 26 \log_{10}(f [\text{MHz}]/5) + \alpha_{\text{shadowing}}$
	RRU → CU	$36.7 \log_{10} d[m] + 40.9 + 26 \log_{10}(f [\text{MHz}]/5) + \alpha_{\text{shadowing}}$
Retransmission	HARQ	
Scheduler of eNB	Proportional fairness (PF)	
Power control	Adaptive power	
Traffic	Full buffer	
Fronthaul	Ideal (no delay)/ non-ideal (10 ms delay)	
Maximum transmit power	RRU = 30 dBm	
	Cellular Tx_Power = 24 dBm	
	D2DTx_Power = 9 dBm	
Noise figure	5 dBm for BS/9 dBm for D2D receiver	
Thermal noise density	-174 dBm/Hz	
User speed	Static	

Table 2. Simulation parameters.

and they are separated from each other at 20 m. It is interesting to know that for a higher number of user devices, the delay also increases in traditional C-RAN networks, where data traffic goes through BBUs, while in D2D mode the delay stays almost constant as the number of devices increases thanks to direct data transfer between devices. With these results one can conclude that D2D-enabled C-RAN mode demonstrates the improvement for delay-sensitive 5G networks.

THROUGHPUT ANALYSIS

Figure 4 shows the average throughput of the system with and without ideal FH. For this simulation, we consider 20 D2D pairs and 20 cellular users (CUs). We also assume a fixed resource allocation between CUs and D2D users. There are 100 resource blocks (RBs) in LTE 20 MHz band, which were divided equally among CUs and D2D users (50 RBs each). Each of these RBs is then assigned to their corresponding users via a proportional fairness scheduler. CUs on 50 RBs communicate using a cellular link (UE1 ↔ RRU ↔ UE2), while D2D use a direct link (UE1 ↔ UE2).

When only CUs with ideal FH are deployed, the average throughput of the system is around 10 Mb/s, but when this scenario is enhanced with D2D, the average throughput raises to 20 Mb/s. This increase in throughput is due to the inclusion in the C-RAN network of D2D, which, thanks to its capability of direct communication, enhances the average system throughput of the system. Moreover, if shared resource allocation schemes between CUs and D2D with some interference cancellation mechanism are considered, the average throughput of the system increases even further.

When simulations with the non-ideal FH are run, a delay of 10 ms is experienced and CUs throughput drops to around 5 Mb/s. This is due to the FH delay: the greater the delay, the lower the throughput. But for the D2D case, throughput remains the same, because in D2D data is transferred directly between devices, and therefore there is sort of a “zero delay,” but still under the control of C-RAN, which is a benefit in terms of mobility and handover.

POWER CONSUMPTION ANALYSIS

In this subsection, we provide power consumption analysis for our envisioned scenario, which is shown in Fig. 5.

Power Consumption for C-RAN-Based D2D:

The power consumption comparison of the C-RAN with D2D communication against the conventional small cell associated with a macro BS deployment is shown in Fig. 5a. It can be seen that the power consumption of the conventional small cell deployment scenario increases as the radius of the cell increases, while that of the C-RAN with D2D communication remains unchanged. This is due to the fact that the number of small cells increases in the conventional small cell deployment as the cell radius increases, and each of them increases the power consumption. Meanwhile, only the central cloud BBU unit in the C-RAN with D2D communication is the power consumption source. It is observable that the conventional small cell deployment has about three times higher power consumption than that

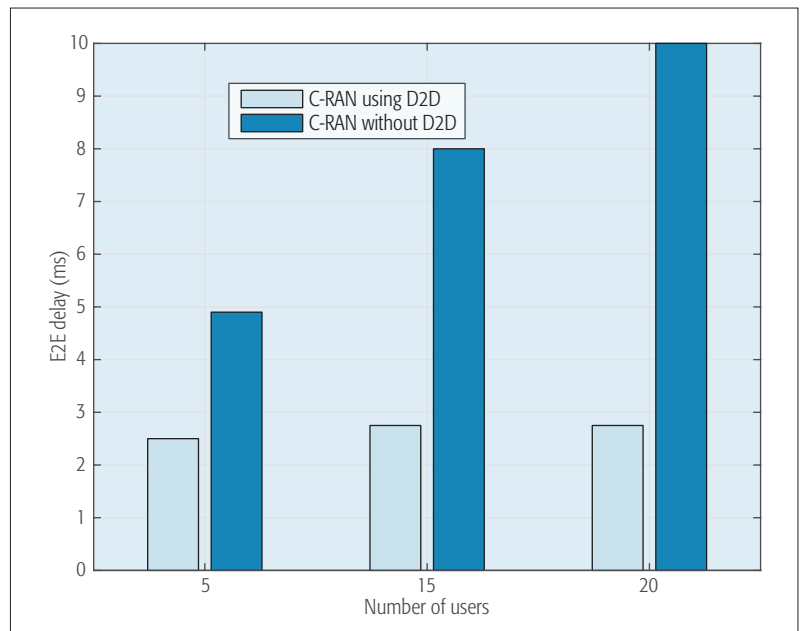


Figure 3. Delay comparison.

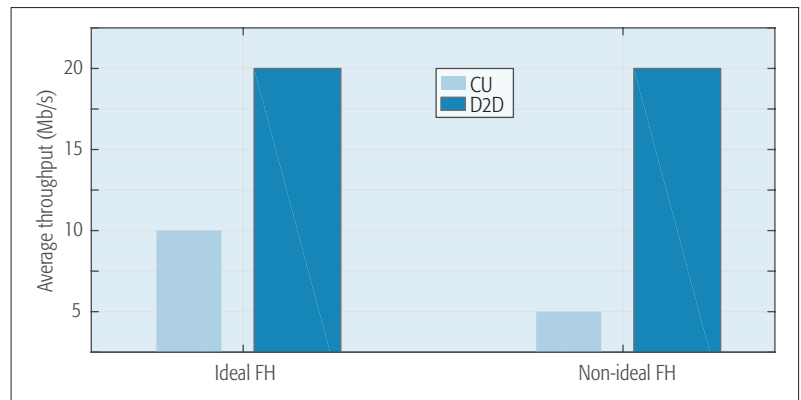


Figure 4. Average throughput vs. ideal-/non ideal-FH.

of the C-RAN with D2D communication, depending on the radius of the cell.

Different Types of FH Power Consumption for C-RAN: Figure 5b shows the total power consumption for a given area throughput of three different types of FH technologies: fiber, millimeter-wave (mmWave), and microwave links. The power consumption is measured with respect to area power consumption and is expressed as a function of the area throughput. We find that the fiber FH consumes the least power among the considered FH technologies. Therefore, from a total power consumption standpoint, an optical-fiber-based hauling solution for an FH system is the most suitable. Finally, it is also clear that the mmWave technology proves to be a very convenient option, with performance similar to the fiber FH.

FUTURE RESEARCH DIRECTIONS

The proposed D2D-based C-RAN technology framework offers several advantages for MCS: it reduces the signaling overhead when compared to deployed small cells, and acts as a means of enhancing the mobility management. However, there are also some challenges that remain to

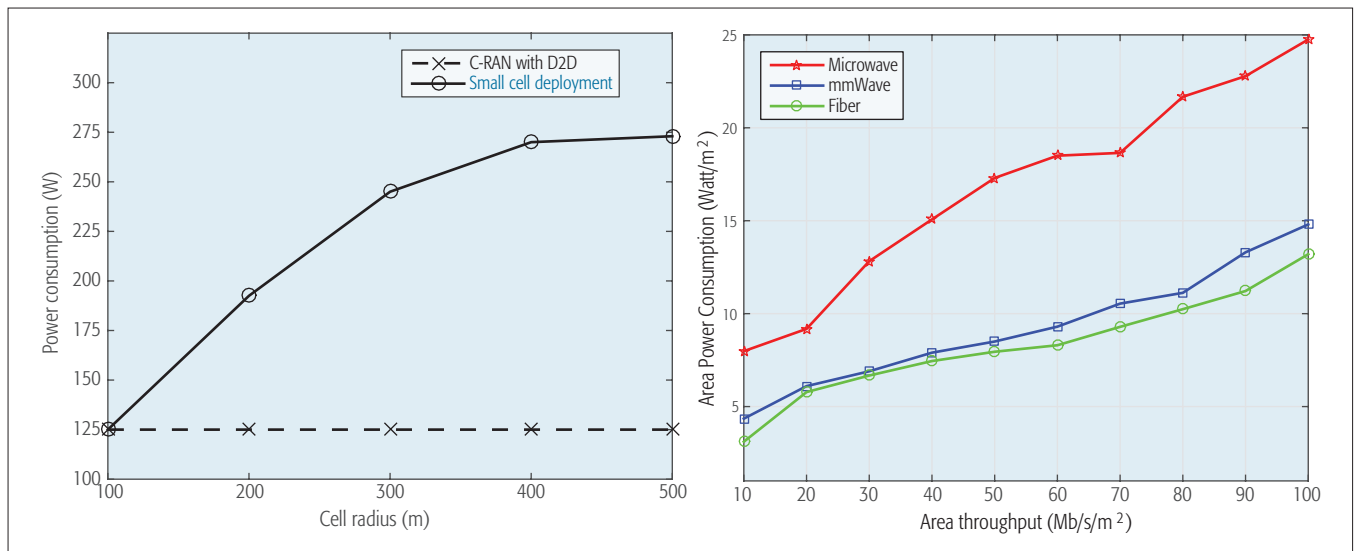


Figure 5. Power consumption for C-RAN-based D2D: a) power consumption vs. cell radius; b) power consumption for different types of FH.

be addressed, especially in terms of interference management. In fact, D2D-based C-RAN has evolved into randomly created on-demand small cells, a setup that increases interference among the cells. Another challenge to solve is the problem of jointly optimizing resources in the communication haul and access network for D2D-based C-RAN small cells.

Moreover, actual C-RAN could provide an additional opportunity for energy efficiency since the centralization of the baseband processing might save energy, especially if the latest advances on green data centers techniques are leveraged. The amount of energy consumption by the circuitry needed for C-RAN is still unknown; therefore, how to deal with this is a big research challenge.

Other topics of future research are backhauling aspects, mmWave communication [16], and cross-layer optimizations in C-RANs, aiming to enable even more opportunities for D2D-based networks. Finally, designing resource management algorithms that incorporate tighter frequency reuse in D2D-based C-RAN will have a significant impact on future research for capacity enhancement.

CONCLUSIONS

This article proposes a novel framework for MCS applications that incorporates D2D features within a C-RAN communication system. A description of the current status of standardization activities of both C-RAN and D2D is offered, as well as a detailed overview of the architecture of a D2D-based C-RAN system, focusing on the enhancements brought to the FH link, from both the data plane and control plane perspectives of the LTE-A protocol stack. Finally, the effectiveness of the newly proposed architecture is demonstrated by system-level simulations to help mobile stakeholders assess the gains of a C-RAN architecture incorporating D2D functionalities. We believe this novel architecture can provide a significant step ahead toward an effective realization of some of the requirements that are shaping the vision of future 5G systems.

ACKNOWLEDGMENT

The research leading to these results received funding from the European Commission H2020 programme under grant agreement no. 671705 (SPEED-5G project). Kazi Mohammed Saidul Huq would also like to acknowledge the Fundação para a Ciência e a Tecnologia (FCT) of Portugal; Reference No. SFRH/BPD/110104/2015.

REFERENCES

- [1] Ericsson, "Mobility Report," June 2013, <http://www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf>, accessed 14 Dec. 2016.
- [2] R. K. Ganti, F. Ye, and H. Lei, "Mobile Crowdsensing: Current State and Future Challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, Nov. 2011, pp. 32–39.
- [3] A. Osseiran et al., "Advances in Device-to-Device Communications and Network Coding for IMT-Advanced," *ICT-MobileSummit 2009 Conf. Proc.*, Santander, Spain, June 2009.
- [4] NGMN, "5G White Paper," Mar. 2015, <http://www.ngmn.org/5g-white-paper.html>, accessed 14 Dec. 2016.
- [5] China Mobile Research Institute, "C-RAN: The Road Towards Green-RAN," White Paper, 2011, http://labs.chinamobile.com/cran/wp-content/uploads/CRAN_white_paper_v2_5_EN.pdf, accessed 14 Dec. 2016.
- [6] M. Peng et al., "Heterogeneous Cloud Radio Access Networks: A New Perspective for Enhancing Spectral and Energy Efficiencies," *IEEE Wireless Commun.*, vol. 21, no. 6, Dec. 2014, pp. 126–35.
- [7] S. Mumtaz, K. M. S. Huq, and J. Rodriguez, "Direct Mobile-to-Mobile Communication: Paradigm for 5G," *IEEE Wireless Commun.*, vol. 21, no. 5, Oct. 2014, pp. 14–23.
- [8] D. Mazza, D. Tarchi, and G. E. Corazza, "A Partial Offloading Technique for Wireless Mobile Cloud Computing in Smart Cities," *2014 Euro. Conf. Networks and Commun.*, June 2014, pp. 1–5.
- [9] H. Hu and R. Wang, "User-Centric Local Mobile Cloud-Assisted D2D Communications in Heterogeneous Cloud-RANs," *IEEE Wireless Commun.*, vol. 22, no. 3, June 2015, pp. 59–65.
- [10] M. Jo et al., "Device-to-Device-Based Heterogeneous Radio Access Network Architecture for Mobile Cloud Computing," *IEEE Wireless Commun.*, vol. 22, no. 3, June 2015, pp. 50–58.
- [11] T. Kürner, "Information on Backhauling/Fronthauling," IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs), Jan. 2014, <https://mentor.ieee.org/802.15/dcn/14/15-14-0025-01-0thz-information-on-backhauling-fronthauling.pdf>, accessed: 14-Dec-2016.
- [12] CPRI, "The industry initiative for a Common Public Radio Interface (CPRI)," <http://www.cpri.info>, accessed 14 Dec. 2016.
- [13] Qualcomm Inc., "Work Item Proposal for Enhanced LTE Device to Device Proximity Services," 3GPP doc. RP-142311, Dec. 2014, http://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_66/Docs/RP-142311.zip, accessed 14 Dec. 2016.

- [14] M. J. Yang *et al.*, "Solving the Data Overload: Device-to-Device Bearer Control Architecture for Cellular Data Off-loading," *IEEE Vehic. Tech. Mag.*, vol. 8, no. 1, Mar. 2013, pp. 31–39.
- [15] 3GPP, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification (release 12)," TS 36.321, V13.0.0, Feb. 2016; http://www.etsi.org/deliver/etsi_ts/136300_136399/136321/13.0.0.00_60/ts_136321v130000p.pdf, accessed 14 Dec. 2016.
- [16] L. Kong *et al.*, "Millimeter-Wave Wireless Communications for IoT-Cloud Supported Autonomous Vehicles: Overview, Design, and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, Jan. 2017, pp. 62–68.

BIOGRAPHIES

KAZI MOHAMMED SAIDUL HUQ [M] is a senior research engineer at the Instituto de Telecomunicações, Pólo de Aveiro, Portugal. He received his Bachelor's degree in computer science and engineering from Ahsanullah University of Science & Technology, Bangladesh, in 2003. He obtained his Master's and Ph.D. degrees in electrical engineering from Blekinge Institute of Technology, Sweden, in 2006 and the University of Aveiro, Portugal, in 2014, respectively. His research activities include 5G paradigm, backhaul, D2D communication, energy-efficient wireless communication, radio resource management, and MAC layer scheduling. He is the author of several publications including papers in conferences and journals, and a book and book chapters.

SHAHID MUMTAZ [SM] (smumtaz@av.it.pt) has more than seven years of wireless industry experience and is currently working as a senior research scientist and technical manager at Instituto de Telecomunicações Aveiro, Portugal, in the 4Tell group. Prior to his current position, he worked as a research intern at Ericsson and Huawei Research Labs. He received his M.Sc. and Ph.D. degrees in electrical and electronic engineering from Blekinge Institute of Technology Karlskrona, Sweden, and the University of Aveiro. His research interests lie in the field of architectural enhancements to 3GPP networks (i.e., LTE-A user plane and control plane protocol stack, NAS, and EPC), 5G related technologies, green communications, cognitive radio, cooperative networking, radio resource management, cross-layer design, backhaul/fronthaul, heterogeneous networks, M2M and D2D communication, and baseband digital signal processing. He has more than 80 publications in international conferences, journals, and book chapters.

JONATHAN RODRIGUEZ [SM] received his Master's degree in electronic and electrical engineering and Ph.D. from the University of Surrey, United Kingdom, in 1998 and 2004, respectively. In 2002, he became a research fellow at the Centre for Communication Systems Research and was responsible for coordinating Surrey's involvement in European research projects under Frameworks 5 and 6. Since 2005, he has been a senior researcher at the Instituto de Telecomunicações, where he founded the

4TELL Wireless Communication Research Group in 2008. He was the project coordinator and technical manager of the FP7 C2POWER and FP7 COGEU projects, respectively, and currently acts as coordinator of several national and international projects. He is the author of more than 250 scientific publications, and has served as General Chair for several prestigious conferences and workshops, and has carried out consultancy for major manufacturers participating in DVB-T/H and HS-UPA standardization. He is a Chartered Engineer (CEng IET). His research interests include green communications, network coding, cognitive radio, cooperative networking, radio resource management, and cross-layer design

PAULO MARQUES received his Licenciatura, Master's degree, and Ph.D. from the University of Aveiro in 1998 and 2006, respectively. He is a senior researcher at the Instituto de Telecomunicações. During 2006 he was a visiting researcher at Trinity College Dublin, Ireland, working on reconfigurable radio systems. He has been involved in several national and European research projects: the IST projects SAMBA, ASILUM, MATRICE, 4MORE, and ORACLE, where he acts as work package leader on "sensing and interference evaluation." He is currently the project coordinator of COGEU and technical manager of C2POWER. His research interests include advanced signal processing techniques for wireless communications and cognitive radio networks. His current focus is on the development of efficient sensing algorithms to exploit spectral opportunities in dynamic spectrum systems. He has published extensively in these areas and is an active reviewer for several scientific journals. He is a member of the IEEE P1900.6 standardization group with voting rights

BISMARCK OKYERE obtained a double M.Sc. in electrical engineering and information technology from Universität Karlsruhe (now Karlsruhe Institute of Technology) and Politecnico di Torino in 2009. He was a recipient of the Erasmus Mundus Scholarship. He has over six years' protocol stack development experience working with Intel. He is currently involved in the Speed-5G EU project. His research interests include cognitive radio, efficient MAC schemes, and more.

VALERIO FRASCOLLA obtained his M.Sc. and Ph.D. in electrical engineering from Ancona University, Italy. Since 2006, in Germany, he has worked in different roles for Comneon, Infineon, and finally Intel, where he is funding and innovation manager. He has expertise in mobile platforms system architecture and requirements management, standard bodies attendance, and innovation program management, using the latest agile methodologies. He has contributed to several research projects (EASY-C, ADEL, MiWaveS, SPEED-5G, mmMAGIC, FUTEBOL, 5G-MiEdge, 5GChampion). He has a track record of technical excellence, is an author of several papers and an invited speaker to international venues, and serves as a member of numerous Technical Program Committees. His research interests are hardware/software co-design, mobile edge computing and 5G systems design.

INTERNET OF THINGS: PART 3



Christos Verikoukis



Roberto Minerva



Mohsen Guizani



Soumya Kanti Datta



Yen-Kuang Chen



Hausi A. Muller

The Internet of Things (IoT) is seen as a set of vertical application domains that share a limited number of common basic functionalities. In this view, consumer-centric solutions, platforms, data management, and business models have to be developed and consolidated in order to deploy effective solutions in the specific fields. The availability of low-cost general-purpose processing and storage systems with sensing/actuation capabilities coupled with communication capabilities are broadening the possibilities of IoT, leading to open systems that will be highly programmable and virtualized, and will support large numbers of application programming interfaces (APIs). IoT emerges as a set of integrated technologies — new, exciting solutions and services that are set to change the way people live and produce goods. IoT is regarded by many as a fruitful technological sector in order to generate revenues. IoT covers a large wealth of consumer-centric technologies and is applicable to an even larger set of application domains. Innovation will be nurtured and driven by the possibilities offered by the combination of increased technological capabilities, new business models, and the rise of new ecosystems.

This Feature Topic (FT) addresses several promising approaches to sensors, actuators, and new consumer devices. New communication capabilities (from short range to LPWAN to 4G and 5G networks, with NB-IoT). In addition, there are new communication protocols and the exploitation of NFV/SDN for better communications; new solutions for large distributed systems (e.g., combination of cloud, grid, and edge/fog computing); new business models and ecosystems; and consumer-centric aspects including IoT application development, utilization of semantics, and security, privacy, and trust.

This timely FT has gathered articles from a wide range of perspectives in different industrial and research communities of IoT.

In response to the Call for Papers, 103 high-quality manuscripts were received, and after a very careful review process six outstanding papers have been selected for Part 3 of this FT, giving an overview of recent developments in underwater communications, NB-IoT, random access for IoT applications in cellular networks, security, and access control mechanisms.

Using underwater wireless sensor networks (UWSNs) has many challenges since it is very different from normal WSNs. In addition, ensuring security and safety of UWSNs increases those challenges. In the first article, J. Jiang, G. Han, C. Zhu, S. Chan, and J. P. C. Rodrigues study the problem of trust establishment between nodes in UWSNs. They show that existing trust management mechanisms do not apply underwater. Then they introduce a trust cloud model that is suitable for trust management under water.

In the second article, Y.-P. Wang, X. Lin, A. Adhikary, A. Grövlén, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi provide an overview of the 3GPP standard of NB-IoT. They cover deployment flexibility, low device complexity, long battery lifetime, support of massive number of devices, and significant coverage extension beyond existing cellular technologies. Then they cover several open areas for future evolution of NB-IoT.

The radio access network (RAN) can be overloaded if we allow a large number of IoT devices to access the medium simultaneously. T. P. C. de Andrade, C. A. Astudillo, L. R. Sekijima, and N. L. S.da Fonseca, in the third article, review the LTE random access procedure and its support for IoT applications. Then they assess the RAN performance of the standard overload control schemes suggested by 3GPP.

In the fourth article J. Cho, J. Yu, S. Oh, J. Ryoo, J. Song, and H. Kim investigate potential security risks involved in location-based smart services offered by retail stores to their customers by providing as a case study a comprehensive security analysis of the recently launched Starbucks service called Siren Order.

The random access procedures when a large number of connected IoT devices is connected to cellular networks is studied in the fifth article by A. Bader, H. ElSawy, M. Gharbieh, M.-S. Alouini, A. Adinoyi, and F. Alshalan. Based on experimental data and system-level simulations, they demonstrate that it is essential to revisit the status quo of random access procedures in large-scale IoTs.

In the sixth article, D. Hussein, E. Bertin, and V. Frey discuss open issues for security and access control mechanisms in distributed IoTs. They propose a novel community-driven access control framework and demonstrate it in a developed prototype in a user-friendly manner.

BIOGRAPHIES

CHRISTOS VERIKOUKIS [S'95, M'04, SM'07] (cveri@cttc.es) got his Ph.D. from Universitat Politècnica de Catalunya (UPC) in 2000. He is currently a Fellow Researcher at CTTC, head of the SMARTECH Department, and an adjunct associate professor at the University of Barcelona. He has published 106 journal papers and over 170 conference papers. He is also a co-author of three books, 14 chapters in other books, and two patents. He is currently Chair of the IEEE ComSoc CSIM Technical Committee.

ROBERTO MINERVA holds a Ph.D. in computer science and telecommunications from Telecom Sud Paris, France, and a Master's degree in computer science from Bari University, Italy. He is the Chairman of the IEEE IoT Initiative, an effort to nurture a technical community and to foster research in IoT. He is at TIMLab, involved in activities on SDN/NFV, 5G, big data, and architectures for IoT. He is the author of papers published in international conferences, books, and magazines.

MOHSEN GUIZANI [S'85, M'89, SM'99, F'09] received his B.S. (with distinction) and M.S. degrees in electrical engineering, and M.S. and Ph.D. degrees in computer engineering from Syracuse University in 1984, 1986, 1987, and 1990, respectively. He is currently a professor and the Electrical and Computer Engineering Department Chair at the University of Idaho. He currently serves on the Editorial Boards of several international technical journals. He is the author of nine books and more than 450 publications in refereed journals and conferences.

SOUMYA KANTI DATTA is a research engineer at EURECOM and a co-founder of an IoT startup, Future Tech Lab. His research focuses on innovation, standardization, and development of next-generation technologies in mobile computing, IoT, M2M communication, and security. He is an active member of the IEEE Consumer Electronics Society and W3C. He has published more than 40 papers in top IEEE conferences and journals. Currently he is involved in oneM2M and the W3C Web of Things Group.

YEN-KUANG CHEN [F'12] received his Ph.D. degree from Princeton University. He is a principal engineer at Intel Corporation, Santa Clara, California. His research areas span from emerging applications that can utilize the true potential of IoT to computer architecture that can embrace emerging applications. He has 50+ U.S. patents, 20+ pending patent applications, and 90+ publications. He is the Editor-in-Chief of the *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*. He is a Distinguished Lecturer of the IEEE Circuits and Systems Society, 2016–2017.

HAUSI A. MULLER is a professor in the Department of Computer Science and associate dean of research in the Faculty of Engineering at the University of Victoria. He is a member of the IEEE Computer Society Board of Governors and the 2016–2017 Vice-President of the IEEE CS Technical and Conference Activities Board. His research interests include software engineering, software evolution, IoT, smart cyber physical systems, and self-adaptive systems. He is a Fellow of the Canadian Academy of Engineering.

A Trust Cloud Model for Underwater Wireless Sensor Networks

Jinfang Jiang, Guangjie Han, Chunsheng Zhu, Sammy Chan, and Joel J. P. C. Rodrigues

The authors study the problem of trust establishment between nodes in UWSNs. They first give a detailed overview of existing trust management mechanisms. Since UWSNs possess specific characteristics, it is noted that those existing mechanisms are not applicable for UWSNs. They then introduce a trust cloud model that is suitable for trust management in UWSNs.

ABSTRACT

Nowadays, the study of underwater WSNs (UWSNs) has become a hot topic. However, UWSNs have not been fully utilized in the complex underwater environment, since there are some difficulties in controlling mobile sensor nodes and underwater environment conditions. In addition, how to ensure the security of UWSNs and the safety of underwater mobile sensor nodes has not been solved well. In this article, we study the problem of trust establishment between nodes in UWSNs. We first give a detailed overview of existing trust management mechanisms. Since UWSNs possess specific characteristics, it is noted that those existing mechanisms are not applicable for UWSNs. We then introduce a trust cloud model that is suitable for trust management in UWSNs.

INTRODUCTION

Over the past few years, underwater wireless sensor networks (UWSNs) have gained much attention from researchers due to their wide applications in many underwater scenarios (oceanographic data collection, marine environment monitoring, ocean target surveillance, underwater assisted navigation, disaster forecast and prevention, etc.). As a kind of collaborative network, in almost all applications of UWSNs, sensor nodes are required to participate in the collaboration, while malicious attackers can seriously threaten the operation of UWSNs. Therefore, secure communication and collaboration among sensor nodes are needed to ensure the efficiency of UWSNs [1, 2].

Until now, there have mainly been three kinds of security mechanisms: intrusion protection, intrusion detection, and intrusion tolerance. As the first line of defense against malicious attackers, intrusion protection mechanisms use encryption algorithms, key management, and authentication technologies to prevent adversary invasion. They can resist external attacks well, but once the malicious attackers obtain secret keys and successfully initiate internal attacks, intrusion protection mechanisms lose their effectiveness.

Intrusion detection mechanisms aim to detect and identify malicious attackers that have successfully invaded the network. However, intrusion detection mechanisms usually work after the initiation of malicious attacks. It is difficult to

detect malicious intruders as soon as possible; thus, real-time detection needs to be improved. Intrusion tolerance mechanisms try to protect networks while allowing the existence of malicious intruders. As the third line of defense, intrusion tolerance is considered to be an efficient security mechanism, and many new algorithms and technologies have been proposed to further improve network security.

Trust management is an important part of intrusion tolerance mechanisms. As an effective complement to traditional cryptography, trust management is widely used in the Internet, terrestrial WSNs (TWSNs), point-to-point (P2P) networks, ad hoc networks, social networks, e-commerce, and so on. However, different application environments have different functional requirements for trust mechanisms. Traditional trust management mechanisms cannot be directly used in UWSNs. Due to the unique characteristics of the underwater environment and acoustic communication, the research on trust management mechanisms in UWSNs faces more challenges. In this article, we first give a detailed overview of existing trust management mechanisms, which are divided into seven categories according to the different theories or methods that are used to calculate trust. Each kind of trust management mechanism is presented in detail and compared carefully. Then this article proposes a novel trust evaluation algorithm, called the Trust Cloud Model (TCM), which can be used in mobile UWSNs. The new algorithm improves the trust calculation accuracy, and increases the successful communication rate of sensor nodes.

In the remainder of this article, we first review existing trust management schemes. Then we describe how the *cloud* mathematical concept is used to evaluate the trust relationship for underwater sensor nodes. We give the details of our proposed TCM, which is a new trust model for UWSNs. We evaluate the proposed model using various performance metrics. Finally, we conclude the article.

TRUST MANAGEMENT SCHEMES

As an important complement to traditional security defense based on cryptography, a trust management mechanism has a significant advantage in the identification of malicious nodes, and many trust management mechanisms have been proposed for WSNs [3]. The common practice of

trust management is to first collect trust evidence, according to the behaviors of sensor nodes and then adopt some mathematical methods to deal with the trust evidence to further determine whether the node is credible or not. In this section, we divide existing trust management mechanisms into the following seven categories according to the different theories or methods that are used to calculate trust.

Trust management based on subjective logic.

In 2008, subjective logic was first adopted for trust computation [4]. The concepts of evidence space and concept space are introduced to describe and establish trust relationships. In addition, a set of logical operators are defined to calculate the trust values of sensor nodes. Subjective logic can also be adopted to study group trust relationship establishment. According to different group relations, direct trust and recommendation trust are measured. In 2014, Ren *et al.* [5] proposed a novel trust model based on subjective logic for intermittent connected networks. A set of trust similarity functions were defined to detect abnormal trust values so as to further improve trust evaluation accuracy. However, how to accurately obtain trust evidence has not been discussed in this kind of trust management mechanism.

Trust management based on Bayesian theory.

In 2004, Ganeriwal *et al.* proposed a trust mechanism based on Bayesian theory named Reputation-Based Framework for High Integrity Sensor Networks (RFSN) [6]. To the best of our knowledge, this was the first trust model proposed for WSNs, where sensor nodes monitor communication behaviors of their neighbor nodes. The amounts of successful and unsuccessful communication are counted for trust evidence, and are further used to obtain trust values of sensor nodes by using the Bayesian formula. At present, the trust model based on Bayesian theory is the most extensively used trust mechanism in WSNs. However, only considering successful or unsuccessful communication to evaluate trust is not reliable since communication behavior in UWSNs is easily affected by the environment.

Trust management based on probability theory.

In 2006, Crosby *et al.* proposed a trust calculation model based on probability theory [7]. First, through a simple statistical method, the relevant trust evaluation factors are obtained. Then the trust values of sensor nodes are calculated by the weighted algorithm. The proposed trust model is simple and has low computational complexity. However, the calculation is based on local monitoring, ignoring recommendations from other nodes in the network. In addition, it is hard to accurately obtain trust evaluation through the weighted algorithm, since it is difficult to determine the exact size of each weight value in UWSNs.

Trust management based on fuzzy logic. In 2010, Chen *et al.* [8] studied the fuzzy nature of trust, and proposed a trust management mechanism based on fuzzy logic. Trust has subjectivity and fuzziness. In the trust management mechanism based on Bayesian theory and probability theory, randomness is used to express fuzziness, and the probability statistics method is adopted to calculate trust values of nodes. In the trust management mechanism based on fuzzy

logic, the fuzzy logic inference rule is established to express the subjectivity and fuzziness of trust, which can solve the problem of inaccurate trust calculation caused by the subjective fuzzy information. However, this kind of trust mechanism cannot provide a specific quantitative method for trust values. How to quantify the fuzzy trust relationship to specific trust values needs further study.

Trust management based on D-S evidence theory.

D-S evidence theory is an important method in uncertainty reasoning, since it can directly express "inaccuracy" and "uncertainty." In 2011, Feng *et al.* [9] proposed a trust model based on node behaviors and D-S evidence theory. D-S evidence theory can describe the uncertainty of trust well. However, the computational complexity of D-S evidence theory is high, and grows exponentially with the increasing number of sensor nodes. Therefore, it is not suitable for resource constrained UWSNs. Another drawback of this kind of trust model is that it may not be possible to get the right result when conflict evidence is synthesized.

Trust management based on entropy theory.

Entropy is a measurement of information uncertainty. In 2006, Sun *et al.* [10] introduced entropy theory into trust evaluation for ad hoc networks. In 2008, Dai [11] *et al.* applied entropy theory for trust evaluation in TWSNs. In 2015, to solve the complex recommendation information processing problem, Zhang *et al.* [12] proposed a trust model based on entropy and recommendation chain classification. First, based on node honesty, recommendation chains are classified into different categories. Then direct trust and recommendation information are aggregated based on entropy theory. Compared to the traditional subjective model, trust management mechanisms based on entropy theory can get rid of trust fuzziness better and obtain accurate trust evaluation.

Trust management mechanism based on cloud theory.

In 1995, Li *et al.* proposed a cloud model based on the traditional fuzzy set theory and probability statistics theory [13]. In 2009, Ma [14] introduced a trust cloud into TWSNs, and put forward a cloud-based trust model (CBTM). CBTM does not take timeliness of trust into account. In addition, using the average method to evaluate trust values of sensor nodes is not reasonable. In 2014, Xu *et al.* designed a lightweight cloud model (LCT) for TWSNs [15]. The proposed trust model is simple: each sensor node can establish an independent LCT and carry out a comprehensive assessment of trust for its neighbor nodes. Cloud theory is mainly used for trust combination and transfer calculation. It can describe the uncertainty of trust well. However, how to obtain trust evidence and how to calculate trust values according to the trust evidence have not been resolved; moreover, in the process of trust combination and trust transfer calculation, conflict trust, trust repeated calculation, and the timeliness of trust are not taken into account. In addition, all the proposed trust models based on cloud theory are designed for the terrestrial environment, which cannot be directly used in UWSNs. Therefore, in this article, we introduce a trust model based on cloud theory for UWSNs.

As an important complement to the traditional security defense based on cryptography, a trust management mechanism has a significant advantage in the identification of malicious nodes, and many trust management mechanisms have been proposed for WSNs.

The mathematical concept cloud can well describe the uncertainty of qualitative and quantitative values. In our TCM, we use clouds to evaluate trust relationships for underwater sensor nodes, since they possess fuzziness and randomness.

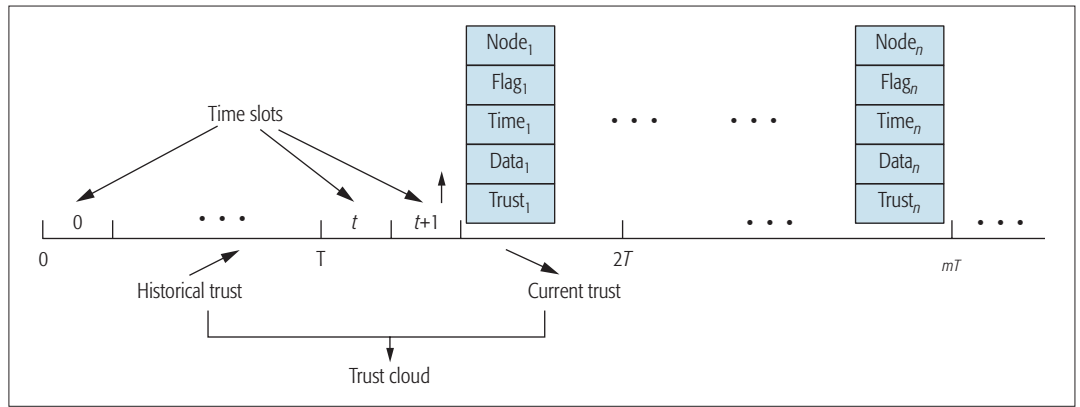


Figure 1. The sliding time window.

SYSTEM MODEL

NETWORK MODEL

In the UWSN, there are n sensor nodes, denoted by $s_i \in S$, where $S = \{s_i\}_{i=1}^n$. Each sensor node s_i is randomly deployed at position p_i . We assume that all sensor nodes have the same communication range. The communication radius is r . Only when the distance $d(p_i, p_j)$ between two sensor nodes s_i and s_j satisfies $d(p_i, p_j) \leq r$ can the two nodes directly communicate with each other. We call them one-hop neighbor nodes. The location of any sensor node can be obtained by possibly using GPS or other techniques such as triangulation or localization. In TCM, trust is periodically evaluated by using a sliding time window, as shown in Fig. 1. In each time slot, the information of *node*, *flag*, *time*, *data*, and *trust* is obtained, where *node* is the target node of current communication, *flag* records the communication status (successful or unsuccessful), *time* is the current

time, and *data* is the attribute data of the target node obtained in the process communication process. The attribute data is analyzed as trust evidence, which is further used to calculate trust. The calculated trust is recorded in *trust*.

CLOUD MODEL

The mathematical concept cloud can describe the uncertainty of qualitative and quantitative values well. In our TCM, we use clouds to evaluate trust relationships for underwater sensor nodes, since they possess fuzziness and randomness. For any trust attribute X , if $\forall x \in X$, where X is a trust evaluation domain denoted with accurate value, there is a mapping μ satisfying $\mu : X \rightarrow [0, 1]$, $x \rightarrow \mu(x) \in [0, 1]$; then the distribution of X in the domain X is called cloud.

A model could consist of three digital features (E_x, E_n, E_e) to describe transformation between qualitative and quantitative values. E_x is the expected value of the attribute (i.e., the mean

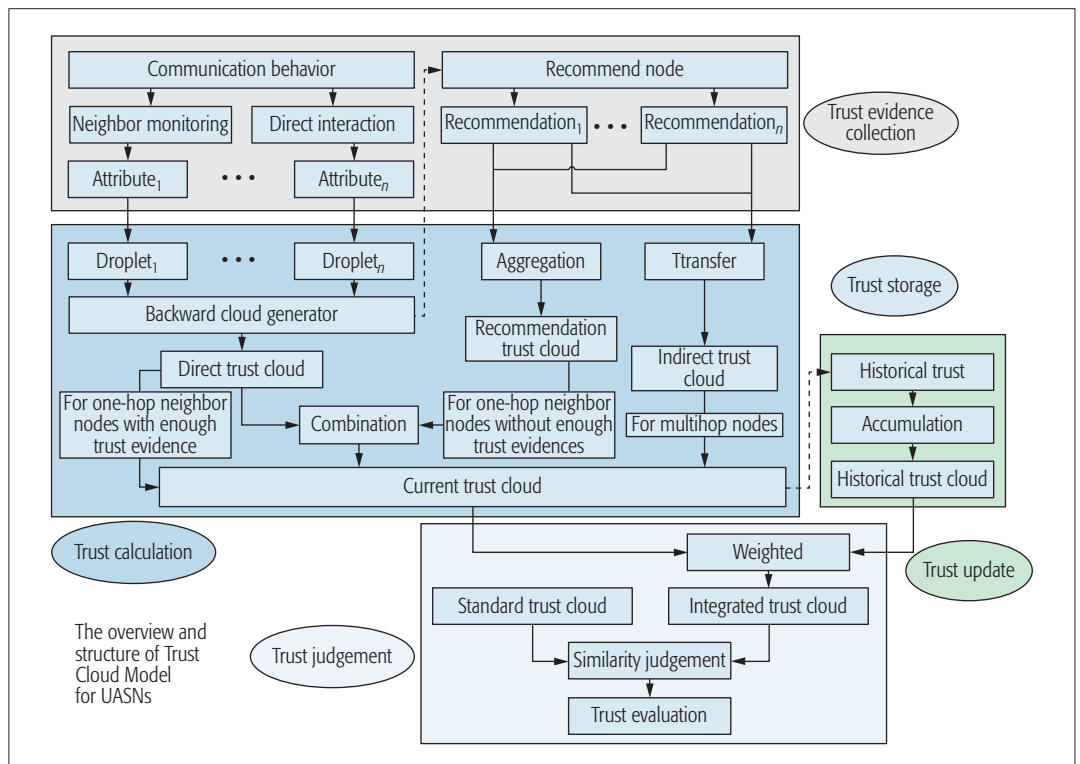


Figure 2. The architecture of TCM.

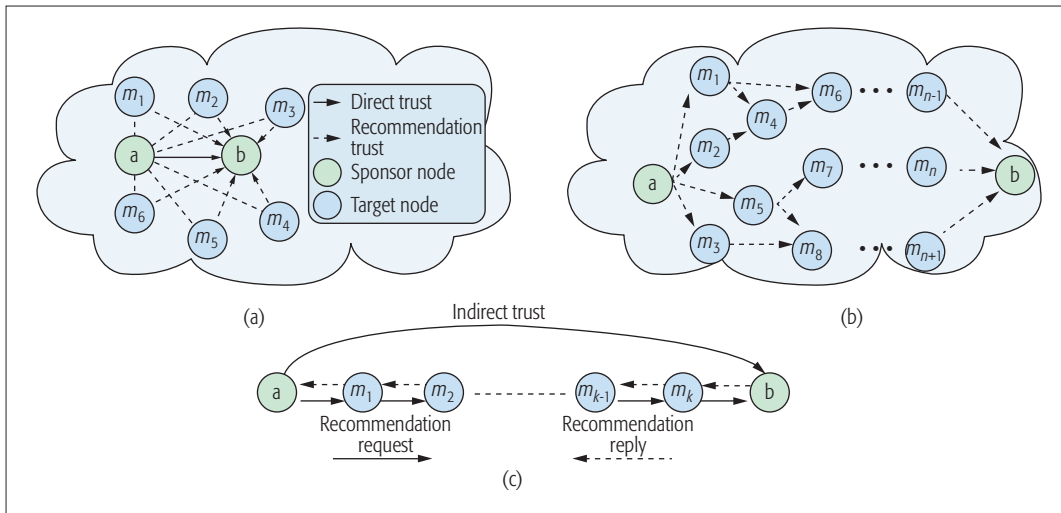


Figure 3. The detail of TCM.

value). E_n is the entropy of the attribute, which reflects the ambiguity of E_x . E_e is the hyper entropy of the attribute, which indicates the uncertainty of E_n . Each cloud is composed of a lot of cloud drops. A single cloud drop cannot express any specific meaning or feature. But a cloud that consists of a number of drops can be a feature of a qualitative concept. For any x_i , we can calculate (E_{xi}, E_{ni}, E_{ei}) based on the Backward Cloud Generator as follows:

Step 1. Calculating the mean \bar{x}_i and the variance S^2 of x_i ,

$$\bar{x}_i = \frac{1}{n} \sum_{i=1}^n x_i, S^2 = \frac{1}{n-1} \sum_{i=1}^n (\bar{x}_i - x_i)^2$$

Step 2. Calculating E_{xi} , $E_{xi} = \bar{x}_i$

Step 3. Calculating E_{ni}

$$E_{ni} = \sqrt{\frac{\pi}{2}} \times \frac{1}{n} \sum_{i=1}^n |E_{xi} - x_i|$$

Step 4. Calculating E_{ei}

$$E_{ei} = \sqrt{S^2 - E_{ni}^2}$$

METHODS OF TRUST EVIDENCE COLLECTION

In this section, we introduce TCM in detail. Figure 2 presents a work flow of TCM. The detailed operation is presented as follows:

TRUST EVIDENCE COLLECTION

The first step of trust management is the collection of trust evidence. As shown in Fig. 3, according to nodes' communication behaviors, trust evidence is collected. There are two methods for trust evidence collection: neighbor nodes monitoring and direct information interaction. In UWSNs, abnormal acoustic communication (e.g., packet loss, packet error, and abnormal energy consumption) can be used as trust evidence to establish a trust model. A UWSN is characterized by narrow bandwidth, high bit error rate, and packet loss rate. In order to make full use of acoustic channel bandwidth, malicious packet error and packet loss must be avoided; thus, abnormal packet error and loss are used as trust evidence. In addition, as a kind of resource constrained network, a UWSN is especially limited by energy; thus, abnormal energy consumption is also taken into account.

The trust model is used to quantify trust relationships between sensor nodes. Based on the quantified results and similarity judgment, a sensor node can judge whether another node is trustworthy or not. Thus, in the operation of the UWSN, only trustworthy nodes are selected to use for data transmission.

At the beginning of network deployment, there is no past communication between sensor nodes; thus, no trust evidence is available. In this case, we need to initialize the trust values of nodes. Here, we assume that all the sensor nodes are trustworthy at the beginning.

DIRECT TRUST CLOUD ESTABLISHMENT

Trust calculation is the core module in the trust management mechanism. In TCM, three kinds of trust are calculated: direct trust, recommendation trust, and indirect trust. For one-hop neighbor nodes, direct trust can be calculated based on their direct communication experiences. Based on trust evidence, trust attributes are calculated to obtain cloud drops, which can be used to establish direct trust cloud based on the backward cloud generator. If there is enough trust evidence between one-hop neighbor nodes, only direct trust is calculated for establishing a trust relationship.

RECOMMENDATION TRUST CLOUD ESTABLISHMENT

In UWSNs, underwater sensor nodes freely float with the ocean currents. The neighborhood of a sensor node changes from time to time. In the same neighborhood, the trust values can share with each other to provide recommendation. In a different neighborhood, the trust values can be transferred to obtain indirect trust. For neighbor nodes without direct communication or enough direct interaction experiences, recommendations from other nodes are required to establish recommendation trust. The nodes that provide recommendations are called recommenders. The calculated direct trusts stored in the recommender are used for recommendations. Then direct and recommendation trusts are combined as the current trust cloud.

INDIRECT TRUST CLOUD ESTABLISHMENT

For multihop nodes, indirect trust clouds are established. In the process of trust transfer, in order to limit the path length of trust transfer and save energy consumption of recommendation, the six degrees of separation rule is adopted to establish recommendation links, which are used to transfer commendations for multihop sensor nodes.

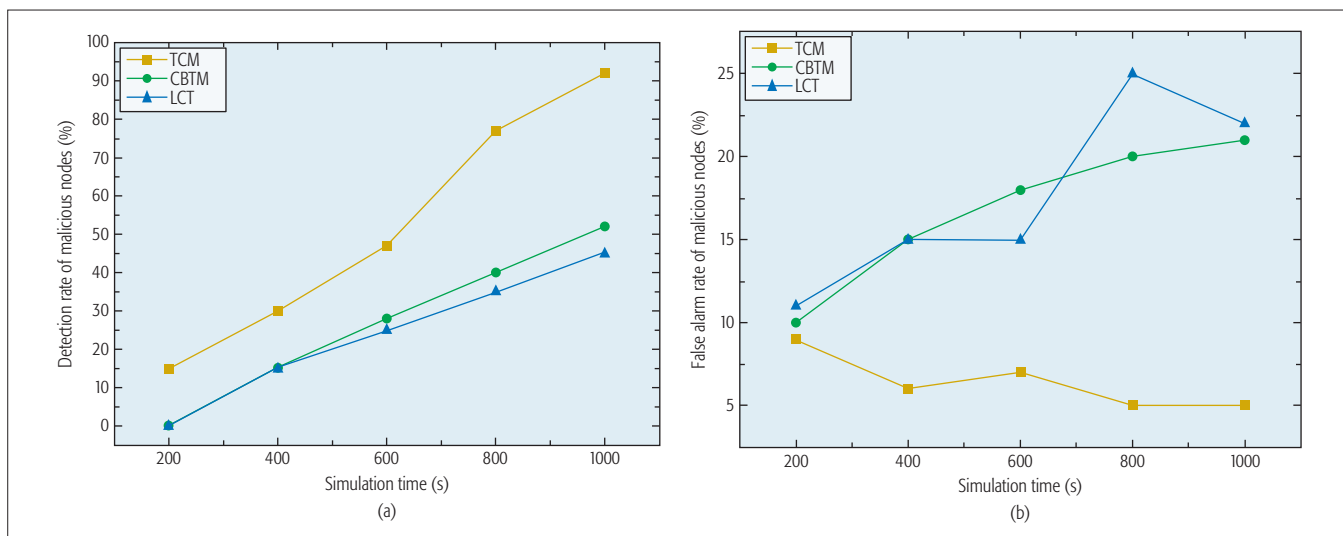


Figure 4. Comparison of the expected trust value.

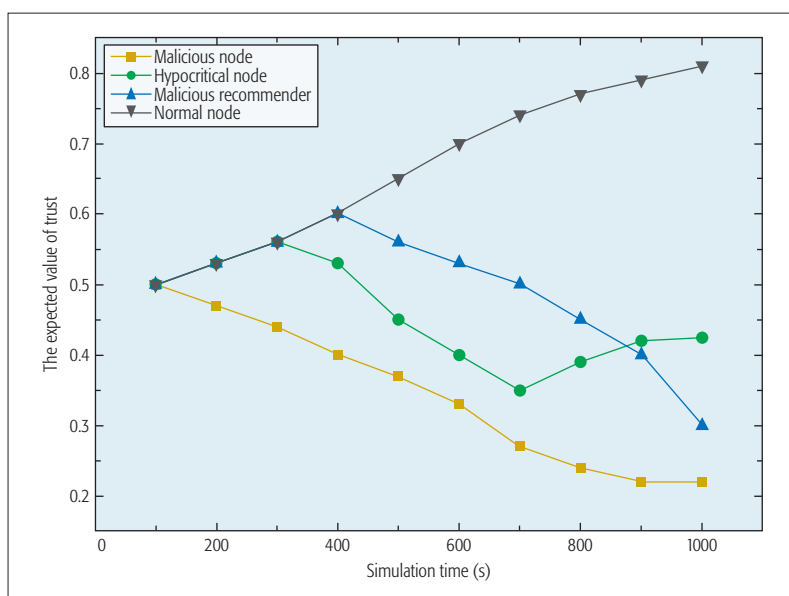


Figure 5. Comparison of the detection rate and false alarm rate.

TRUST CLOUD UPDATE

Trust has two aspects of dynamic characteristics: first, the trust relationship between sensor nodes changes in a dynamic environment; second, trust decays over time. In the first case, due to dynamic ocean currents and unstable acoustic communication, the sensor nodes with interrupted communication due to an intermittently connected acoustic link may easily be mistaken as malicious nodes. Thus, a redemption factor is introduced to control normal communication. If the value of a sensor node's trust is lower than the defined redemption factor, it will be forbidden from participating in communication until its trust value returns to normal. The redemption factor can also be used to avoid the excluded malicious nodes quickly joining the network again. In the second case, a memory factor is introduced to describe the time decay characteristic. The trust trails off along with time; thus, the trust closer to the current time can be given a higher weight, and the historical trust is assigned with a lower weight.

TRUST JUDGMENT AND EVALUATION

The trust model is used to quantify trust relationships between sensor nodes. Based on the quantified results and similarity judgment, a sensor node can judge whether another node is trustworthy or not. Thus, in the operation of the UWSN, only trustworthy nodes are selected to use for data transmission.

SIMULATIONS

The simulation is conducted using the Matlab simulator. The number of normal sensor nodes is 100. The number of malicious nodes ranges from 10 to 100 with an increment of 10 each time. All the sensor nodes are randomly deployed over a network size of 500 m × 500 m. The transmission radius of each node is set as 50 m. We evaluate the performance of TCM in the following three aspects:

1. The performance of malicious node detection
2. The performance of trust value calculation
3. The performance of data transmission

THE PERFORMANCE OF MALICIOUS NODE DETECTION

The detection rate and false alarm rate of malicious nodes are compared in Figs. 4a and 4b, respectively. TCM outperforms CBTM and LCT because CBTM and LCT do not take timeliness of trust into account. In addition, using the direct average method to evaluate trust values of sensor nodes is not reasonable.

THE PERFORMANCE OF TRUST VALUE CALCULATION

In order to evaluate the performance of TCM, four kinds of sensor nodes (normal nodes, malicious nodes, hypocritical nodes, and malicious recommender) are simulated. The communication behaviors of normal nodes have been good; thus, their trust values gradually rise along simulation time. On the contrary, malicious nodes' trust values rapidly decrease with communication time. This is because malicious nodes lose many packets, which introduces unsuccessful communication. As shown in Fig. 5, even they stop performing malicious behaviors; it is hard for them to obtain high trust values. Hypocritical nodes first pretend to be normal nodes, and thus they are

evaluated with higher trust values. However, their trust values will rapidly decrease once they launch malicious attacks. The malicious recommender can be detected and will not continue to be used in the following trust evaluation. These results meet the requirements of slow establishment and rapid destruction of trust evaluation.

THE PERFORMANCE OF DATA TRANSMISSION

As shown in Fig. 6, in the same environment, the rate of successful communication under TCM is higher than that of the other two trust models. The rate of successful communication decreases with the increasing number of malicious nodes. However, TCM can be robust against malicious attacks. When the ratio of malicious nodes grows from 10 to 50 percent, we can get a higher communication success rate and the trend is relatively flat, indicating that TCM can suppress a certain number of malicious nodes.

CONCLUSION

In this article, we have presented a detailed survey of existing trust management mechanisms. Since UWSNs possess specific characteristics, we introduce a new trust cloud model that is suitable for trust management in UWSNs. The research of trust management for UWSNs is still in its infancy; there are still many challenges remaining wide open for future investigation:

1. The challenge of underwater acoustic communication. The underwater environment is complex and dynamic, which leads to poor stability of underwater acoustic communication. How to effectively obtain trust evidence and accurately evaluate trust values is one of the key issues in trust management mechanisms. In addition, the instability of underwater acoustic communication makes UWSNs more vulnerable to various types of network attacks, which brings new challenges for network security.

2. The challenge of node mobility. In UWSNs, the positions of sensor nodes change with ocean water flow. Thus, communication behaviors and trust relationships between sensor nodes also constantly change, which causes a lot of difficulties for trust assessment.

3. The challenge of sparse node deployment. UWSNs are always used to monitor a large-scale scenario, and sensor nodes are usually sparsely deployed. In this case, sensor nodes are far away from each other, so the number of direct communication or information exchange between them is not enough to accurately evaluate trust relationship. How to carry out trust management under the condition of insufficient trust evidence becomes a new problem to be solved.

ACKNOWLEDGMENTS

The work is supported by the Qing Lan Project and the National Natural Science Foundation of China under Grant No. 61572172 and No. 61602152, the Fundamental Research Funds for the Central Universities, No. 2016B10714 and No. 2016B03114, the Changzhou Sciences and Technology Program, No.CE20165023 and No.CE20160014, and the Six talent peaks project in Jiangsu Province, No.XYDXXJS-007. This research is also supported by a strategic research grant from City University of Hong

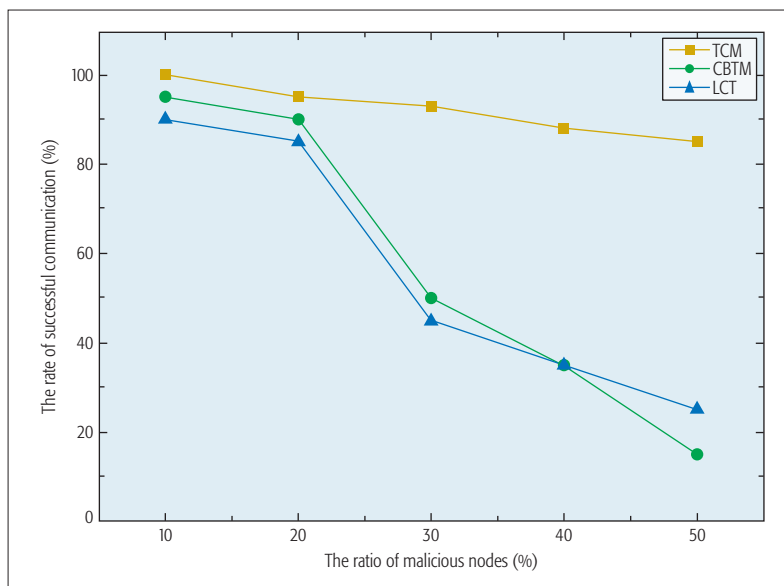


Figure 6. Comparison of the successful communication rate.

Kong, No. 7004615. This work has been supported by National Funding from the FCT – *Fundação para a Ciência e a Tecnologia* through the UID/EEA/500008/2013 Project, by the Government of Russian Federation, Grant 074-U01, and by Finep, with resources from Funttel, Grant No. 01.14.0231.00, under the Radio-communication Reference Center (*Centro de Referência em Radiocomunicações – CRR*) project of the National Institute of Telecommunications (*Instituto Nacional de Telecomunicações – Inatel*), Brazil.

REFERENCES

- [1] G. Han et al., "Secure Communication for Underwater Acoustic Sensor Networks," *IEEE Commun. Mag.*, vol. 53, no. 8, Aug. 2015, pp. 54–60.
- [2] G. Han et al., "Routing Protocols for Underwater Wireless Sensor Networks," *IEEE Commun. Mag.*, vol. 53, no. 11, Nov. 2015, pp. 72–78.
- [3] G. Han et al., "An Attack-Resistant Trust Model Based on Multidimensional Trust Metrics in Underwater Acoustic Sensor Networks," *IEEE Trans. Mobile Comp.*, vol. 14, no. 12, 2015, pp. 2447–59.
- [4] A. Josang, R. Hayward, and S. Pope, "Optimal Trust Network Analysis with Subjective Logic," *Int'l. Conf. Emerging Security Info., Systems and Technologies*, 2008, pp. 179–84.
- [5] Y. Ren et al., "A Novel Approach to Trust Management in Unattended Wireless Sensor Networks," *IEEE Trans. Mobile Comp.*, vol. 13, no. 7, 2014, pp. 1409–23.
- [6] S. Ganeriwal, L. K. Balzan, and M. B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," *ACM Trans. Sensor Networks*, 2004, pp. 66–77.
- [7] G. Crosby et al., "A Framework for Trust-Based Cluster Head Election in Wireless Sensor Networks," *2nd IEEE Wksp. DSSNS*, 2006, pp. 13–22.
- [8] C. Chen, R. Wang, and L. Zhang, "The Research of Subjective Trust Model Based on Fuzzy Theory in Open Networks," *Acta Electronica Sinica*, vol. 11, 2010, pp. 2505–09.
- [9] R. Feng et al., "Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory," *Sensors*, vol. 11, no. 2, 2011, pp. 1345–60.
- [10] Y. Sun et al., "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," *IEEE JSAC*, vol. 24, no. 2, 2006, pp. 305–17.
- [11] H. Dai, Z. Jia, and X. Dong, "An Entropy-Based Trust Modeling and Evaluation for Wireless Sensor Networks," *ICESS*, 2008, pp. 27–34.
- [12] L. Zhang et al., "Dynamic Trust Model Based on Recommendation Chain Classification in Complex Network Environment," *J. Commun.*, vol. 36, no. 9, 2015, pp. 55–64.
- [13] D. Li, H. Meng, and X. Shi, "Membership Clouds and Membership Cloud Generators," *J. Comp. R&D*, vol. 32, no. 6, 1995, pp. 15–20.

-
- [14] B. Ma, "Cross-Layer Trust Model and Algorithm of Node Selection in Wireless Sensor Networks," *ICCSN*, 2009, pp. 812–15.
- [15] X. Xu *et al.*, "Representation for Uncertainty Trust of WSN Based on Lightweight-Cloud," *J. Commun.*, vol. 35, no. 2, 2014, pp. 63–69.

BIOGRAPHIES

JINFANG JIANG (jiangjinfang@hhu.edu.cn) is currently a lecturer with the Department of Information & Communication Systems, Hohai University, Changzhou, China. She received her Ph.D. degree from the Department of Computer Science from Hohai University in 2015. Her current research interests are security, localization, and routing for sensor networks.

GUANGJIE HAN [S'01, M'05] (hanguangjie@gmail.com) is currently a professor in the Department of Information & Communication System at Hohai University. He finished his work as a postdoctoral researcher with the Department of Computer Science at Chonnam National University, Korea, in 2008. He received his Ph.D. degree in the Department of Computer Science from Northeastern University, Shenyang, China, in 2004. He has served as an Editor of *IEEE Access* and *Telecommunication Systems*.

CHUNSHENG ZHU [S'12] (cszhu@ece.ubc.ca) is a postdoctoral research fellow in the Department of Electrical and Computer Engineering, University of British Columbia, Canada. He received his Ph.D. degree in electrical and computer engineer-

ing from the University of British Columbia in 2016. His current research interests mainly include wireless sensor networks, cloud computing, the Internet of Things, social networks, and security.

SAMMY CHAN [S'87, M'89] (eeschan@cityu.edu.hk) received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and his Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994, he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994, he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

JOEL J. P. C. RODRIGUES [S'01, M'06, SM'06] (joeljr@ieee.org) is a professor at the Inatel, Brazil and senior researcher at IT, Portugal. He has been a professor at UBI, Portugal, and a visiting professor at UNIFOR. He is the leader of the NetGNA Research Group (<http://netgna.it.ubi.pt>), the President of the scientific council at ParkUrbis @C Covilhã Science and Technology Park, the Past-Chair of the IEEE ComSoc TCs on eHealth and Communications Software, and a Steering Committee member of the IEEE Life Sciences Technical Community. He is the Editor-in-Chief of three international journals and an Editorial Board member of several journals. He has authored or coauthored over 500 papers in refereed international journals and conferences, 3 books, and two patents.

A Primer on 3GPP Narrowband Internet of Things

Y.-P. Eric Wang, Xingqin Lin, Ansuman Adhikary, Asbjörn Grövlén, Yutao Sui, Yufei Blankenship, Johan Bergman, and Hazhir S. Razaghi

ABSTRACT

Narrowband Internet of Things (NB-IoT) is a new cellular technology introduced in 3GPP Release 13 for providing wide-area coverage for IoT. This article provides an overview of the air interface of NB-IoT. We describe how NB-IoT addresses key IoT requirements such as deployment flexibility, low device complexity, long battery lifetime, support of massive numbers of devices in a cell, and significant coverage extension beyond existing cellular technologies. We also share the various design rationales during the standardization of NB-IoT in Release 13 and point out several open areas for future evolution of NB-IoT.

INTRODUCTION

Use cases for machine-type communications (MTC) are developing very rapidly. There has been enormous interest in integrating connectivity solutions with sensors, actuators, meters (water, gas, electric, or parking), cars, appliances, and so on [1, 2]. The Internet of Things (IoT) is thus being created and constantly expanded. IoT consists of a number of networks that may have different design objectives. For example, some networks only intend to cover a local area (e.g. one single home), whereas some networks offer wide-area coverage. The latter case is being addressed in the Third Generation Partnership Project (3GPP). Recognizing the importance of IoT, 3GPP has introduced a number of key features for IoT in its latest release, Release 13 (Rel-13). EC-GSM-IoT [3] and LTE-eMTC [4] aim to enhance existing Global System for Mobile Communications (GSM) [5] and Long Term Evolution (LTE) [6] networks, respectively, for better serving IoT use cases. Coverage extension, user equipment (UE) complexity reduction, long battery lifetime, and backward compatibility are common objectives. A third track, Narrowband IoT (NB-IoT) [7], shares these objectives as well. In addition, NB-IoT aims to offer deployment flexibility, allowing an operator to introduce NB-IoT using a small portion of its existing available spectrum. NB-IoT is designed mainly for targeting ultra-low-end IoT applications.

NB-IoT is a new 3GPP radio access technology in the sense that it is not fully backward compatible with existing 3GPP devices. It is, however, designed to achieve excellent coexistence per-

formance with legacy GSM and LTE technologies. NB-IoT requires 180 kHz minimum system bandwidth for both downlink and uplink, respectively. The choice of minimum system bandwidth enables a number of deployment options. A GSM operator can replace one GSM carrier (200 kHz) with NB-IoT. An LTE operator can deploy NB-IoT inside an LTE carrier by allocating one of the physical resource blocks (PRBs) of 180 kHz to NB-IoT. As will become clear later in this article, the air interface of NB-IoT is optimized to ensure harmonious coexistence with LTE, and thus such an “in-band” deployment of NB-IoT inside an LTE carrier will not compromise the performance of LTE or NB-IoT. An LTE operator also has the option of deploying NB-IoT in the guard-band of the LTE carrier.

NB-IoT reuses the LTE design extensively, including the numerologies, downlink orthogonal frequency-division multiple access (OFDMA), uplink single-carrier frequency-division multiple access (SC-FDMA), channel coding, rate matching, interleaving, and so on. This significantly reduces the time required to develop full specifications. Also, it is expected that the time required for developing NB-IoT products will be significantly reduced for existing LTE equipment and software vendors. The normative phase of the NB-IoT work item in 3GPP started in September 2015 [7] and the core specifications were completed in June 2016. The physical layer specifications of NB-IoT are included in [8–10]. Commercial launch of NB-IoT products and services is expected to be around the beginning of 2017.

In this article, we provide a state-of-the-art overview of the air interface of NB-IoT with a focus on the key aspects where NB-IoT deviates from LTE. In particular, we highlight the NB-IoT features that help achieve the aforementioned design objectives. The remainder of this article is organized as follows. First, transmission schemes and deployment options are given. We then describe the physical channels of NB-IoT. Resource mapping is described, with an emphasis on how orthogonality with LTE is achieved when deploying NB-IoT inside an LTE carrier. Procedures such as cell search, random access, scheduling, and hybrid automatic repeat request (HARQ) are detailed. The article highlights NB-IoT performance, and the final section provides a conclusion.

We describe how NB-IoT addresses key IoT requirements such as deployment flexibility, low device complexity, long battery lifetime, support of massive numbers of devices in a cell, and significant coverage extension beyond existing cellular technologies. We also share the various design rationales during the standardization of NB-IoT in Release 13 and point out several open areas for the future evolution of NB-IoT.

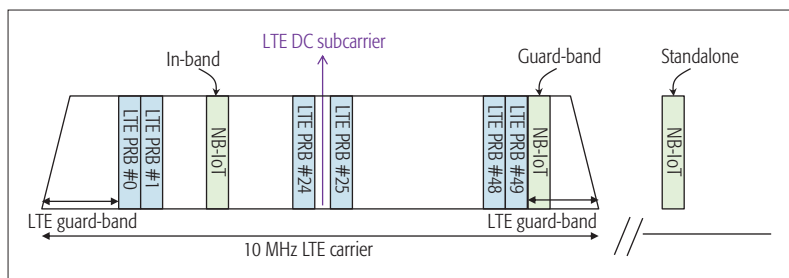


Figure 1. Examples of NB-IoT stand-alone deployment and LTE in-band and guard-band deployments.

TRANSMISSION SCHEMES AND DEPLOYMENT OPTIONS

DOWNLINK TRANSMISSION SCHEME

The downlink transmission scheme of NB-IoT is based on OFDMA with the same 15 kHz subcarrier spacing as LTE [8]. Slot, subframe, and frame durations are 0.5 ms, 1 ms, and 10 ms, respectively, identical to those in LTE. In essence, an NB-IoT carrier uses one LTE PRB in the frequency domain (i.e., 12 15 kHz subcarriers) for a total of 180 kHz. Reusing the same OFDMA numerology as LTE ensures good coexistence performance with LTE in the downlink. For example, when NB-IoT is deployed inside an LTE carrier, the orthogonality between the NB-IoT PRB and all the other LTE PRBs is preserved in the downlink.

ULINK TRANSMISSION SCHEME

The uplink of NB-IoT supports both multi-tone and single-tone transmissions [8]. Multi-tone transmission is based on single-carrier frequency-division multiple access (SC-FDMA) using the same 15 kHz subcarrier spacing and 0.5 ms slot as LTE. Single-tone transmission supports two numerologies, 15 kHz and 3.75 kHz. The 15 kHz numerology is identical to LTE and thus achieves the best coexistence performance with LTE in the uplink. The 3.75 kHz single-tone numerology uses 2 ms slot duration. Like the downlink, an uplink NB-IoT carrier uses a total system bandwidth of 180 kHz.

DEPLOYMENT OPTIONS

NB-IoT may be deployed as a standalone carrier. It may also be deployed within the LTE spectrum, either inside an LTE carrier or in the guard band. These different deployment scenarios are illustrated in Fig. 1. The deployment scenario, standalone, in-band, or guard-band, however, should be transparent to a user equipment (UE) when it is first turned on and searches for an NB-IoT carrier. Similar to existing LTE UEs, an NB-IoT UE is only required to search for a carrier on a 100 kHz raster. An NB-IoT carrier that is intended for facilitating UE initial synchronization is referred to as an anchor carrier. The 100 kHz UE search raster implies that for in-band deployments, an anchor carrier can only be placed in certain PRBs.

Figure 1 illustrates the deployment options of NB-IoT with a 10 MHz LTE carrier. The PRB right above the DC subcarrier (i.e., PRB #25) is centered at 97.5 kHz. Since the LTE DC subcarrier is placed on the 100 kHz raster, the center of PRB#25 is 2.5 kHz from the nearest 100 kHz grid. Similarly, PRBs #30, #35, #40, and #45 are all centered at 2.5 kHz from the nearest 100 kHz

grid. It can be shown that for an LTE carrier of 10 or 20 MHz, there is a set of PRBs that are all centered at 2.5 kHz from the nearest 100 kHz grid, whereas for an LTE carrier of 3, 5, or 15 MHz, the PRBs are centered at least 7.5 kHz away from the 100 kHz raster. A PRB that is no more than 7.5 kHz away from the 100 kHz raster may be used as an NB-IoT anchor carrier. Further, an NB-IoT anchor carrier should not be any of the middle six PRBs of the LTE carrier. This is because LTE synchronization and broadcast channels occupy many resource elements in the middle six PRBs, making it difficult to use these PRBs for NB-IoT.

Similar to the in-band deployment, an NB-IoT anchor carrier in the guard-band deployment needs to have center frequency no more than 7.5 kHz from the 100 kHz raster. NB-IoT cell search and initial acquisition are designed for a UE to be able to synchronize to the network in the presence of a raster offset up to 7.5 kHz.

Multi-carrier operation of NB-IoT is supported. Since it suffices to have one NB-IoT anchor carrier for facilitating initial UE synchronization, the additional carriers do not need to be near the 100 kHz raster grid. These additional carriers are referred to as secondary carriers.

PHYSICAL CHANNELS

DOWNLINK

NB-IoT provides the following physical signals and channels in the downlink:

- Narrowband primary synchronization signal (NPSS)
- Narrowband secondary synchronization signal (NSSS)
- Narrowband physical broadcast channel (NPBCH)
- Narrowband reference signal (NRS)
- Narrowband physical downlink control channel (NPDCCH)
- Narrowband physical downlink shared channel (NPDSCH)

Unlike LTE, these NB-IoT physical channels and signals are primarily multiplexed in time. Figure 2 illustrates how the NB-IoT subframes are allocated to different physical channels and signals. Each NB-IoT subframe spans over one PRB in the frequency domain and 1 ms in the time domain.

NPSS and NSSS are used by an NB-IoT UE to perform cell search, which includes time and frequency synchronization, and cell identity detection. Since the legacy LTE synchronization sequences occupy six PRBs, they cannot be reused for NB-IoT. A new design is thus introduced.

NPSS is transmitted in subframe #5 in every 10 ms frame using the last 11 OFDM symbols in the subframe. NPSS detection is one of the most computationally demanding operations from a UE's perspective. To allow efficient implementation of NPSS detection, NB-IoT uses a hierarchical sequence. For each of the 11 NPSS OFDM symbols in a subframe, either p or $-p$ is transmitted, where p is the base sequence generated based on a length-11 Zadoff-Chu (ZC) sequence with root index 5 [8]. Each of the length-11 ZC sequences is mapped to the lowest 11 subcarriers within the NB-IoT PRB.

NSSS has 20 ms periodicity and is transmitted in subframe #9, also using the last 11 OFDM sym-

Even numbered frame	Subframe number									
	0	1	2	3	4	5	6	7	8	9
	NPBCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPSS	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NSSS
Odd numbered frame	Subframe number									
	0	1	2	3	4	5	6	7	8	9
	NPBCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPSS	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH	NPDCCH or NPDSCH

Figure 2. Time multiplexing of NB-IoT downlink physical channels and signals.

bols that consist of 132 resource elements overall. NSSS is a length-132 frequency domain sequence, with each element mapped to a resource element. NSSS is generated by element-wise multiplication between a ZC sequence and a binary scrambling sequence [8]. The root of the ZC sequence and binary scrambling sequence are determined by narrowband physical cell identity (NB-PCID). The cyclic shift of the ZC sequence is further determined by the frame number modulo 8.

NPBCH carries the master information block (MIB) and is transmitted in subframe #0 in every frame. A MIB remains unchanged over the 640 ms transmission time interval (TTI).

NPDCCH carries scheduling information for both downlink and uplink data channels. It further carries the HARQ acknowledgment information for the uplink data channel as well as paging indication and random access response (RAR) scheduling information. NPDSCH carries data from the higher layers as well as paging message, system information, and RAR message. As shown in Fig. 2, there are a number of subframes that can be allocated to carry NPDCCH or NPDSCH. To reduce UE complexity, all the downlink channels use the LTE tail-biting convolutional code (TBCC) [9]. Furthermore, the maximum transport block size of NPDSCH is 680 bits [10]. In comparison, LTE without spatial multiplexing supports a maximum TBS greater than 70,000 bits.

An NRS is used to provide phase reference for the demodulation of the downlink channels. NRSs are time-and-frequency multiplexed with information bearing symbols in subframes carrying NPBCH, NPDCCH, and NPDSCH, using eight resource elements per subframe per antenna port. NB-IoT supports up to two NRS ports.

UPLINK

NB-IoT includes the following channels in the uplink:

- Narrowband physical random access channel (NPRACH)
- Narrowband physical uplink shared channel (NPUSCH)

NPRACH is a newly designed channel since the legacy LTE physical random access channel (PRACH) uses a bandwidth of 1.08 MHz, more than NB-IoT uplink bandwidth. One NPRACH preamble consists of four symbol groups, with each symbol group comprising one CP and five symbols [8]. Two CP lengths, 66.67 μ s and 266.7 μ s, are specified. Each symbol, with fixed symbol value 1, is modulated on a 3.75 kHz

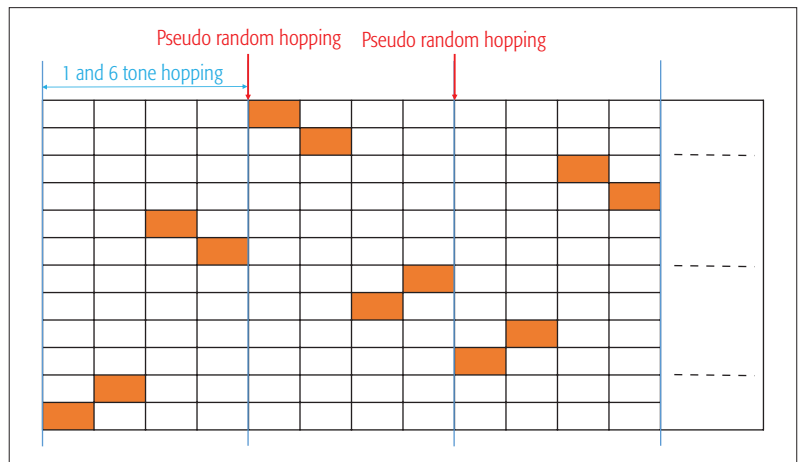


Figure 3. An illustration of NPRACH frequency hopping.

subcarrier. However, the tone frequency index changes from one symbol group to another. The waveform of NPRACH preamble is referred to as single-tone frequency hopping. An example of NPRACH frequency hopping is illustrated in Fig. 3.

NPUSCH has two formats. Format 1 is used for carrying uplink data and uses the same LTE turbo code for error correction. The maximum transport block size of NPUSCH Format 1 is 1000 bits [10], which is much lower than that in LTE. Format 2 is used for signaling HARQ acknowledgment for NPDSCH, and uses a repetition code for error correction. NPUSCH Format 1 supports multi-tone transmission. In this case, the UE can be allocated with 12, 6, or 3 tones. While only the 12-tone format is supported by legacy LTE UEs, the 6-tone and 3-tone formats are introduced for NB-IoT UEs who, due to coverage limitation, cannot benefit from higher UE bandwidth allocation. Moreover, NPUSCH supports single-tone transmission based on either 15 or 3.75 kHz numerology. To reduce peak-to-average power ratio (PAPR), single-tone transmission uses $\pi/2$ -binary phase shift keying (BPSK) or $\pi/4$ -quadrature phase shift keying (QPSK) with phase continuity between symbols.

NPUSCH Format 1 has 7 OFDM symbols/slot, one of which is the demodulation reference symbol (DMRS). NPUSCH Format 2 also has 7 OFDM symbols/slot, but uses 3 symbols as DMRS. DMRSs are used for channel estimation.

Table 1 summarizes the NB-IoT physical channels and their differences from their LTE counterparts.

RESOURCE MAPPING

In this section, we describe how NB-IoT resource mapping is designed to ensure the best coexistence performance with LTE if deployed inside an LTE carrier. In essence, the orthogonality to LTE signals is preserved by avoiding mapping NB-IoT signals to the resource elements already used by the legacy LTE signals. An example is illustrated in Fig. 4, in which each column indicates resource elements in one OFDM symbol. There are 12 resource elements per OFDM symbol corresponding to 12 subcarriers. As shown, for the standalone and guard-band deployments, no LTE resource needs to be protected; thus, NPDCCH, NPDSCH, and NRS can utilize all the resource elements in one PRB pair. However, for in-band deployment, NPDCCH, NPDSCH, and NRS cannot be mapped to the resource elements taken by LTE cell-specific reference symbols (CRS) and LTE physical downlink control channel (PDCCH). NB-IoT is designed to allow a UE to learn the deployment mode (standalone, in-band, or guard-band) as well as the cell identity through initial acquisition. Then the UE can figure out which resource elements

are used by LTE. With this information, the UE can map NPDCCH and NPDSCH symbols to available resource elements. On the other hand, NPSS, NSSS, and NPBCH are used for initial synchronization and master system information acquisition. These signals need to be detected without knowing the deployment mode. To facilitate this, NPSS, NSSS, and NPBCH avoid the first three OFDM symbols in every subframe as these resource elements may be used by LTE PDCCH. Furthermore, NPSS and NSSS signals overlapping with resource elements taken by LTE CRS are punctured at the base station. Although the UE is not aware of which resource elements are punctured, NPSS and NSSS can still be detected by correlating the received punctured synchronization signal with the non-punctured signal since the percentage of punctured resource elements is relatively small. NPBCH is rate-matched around LTE CRS. However, this requires the UE to figure out the location of CRS resource elements, which is dependent of LTE physical cell identity (PCID). The relationship of the values of PCID and NB-PCID used by the same cell is such that the UE can use NB-PCID to determine the LTE CRS locations.

CELL SEARCH AND INITIAL ACQUISITION PROCEDURE

When a UE is powered on for the first time, it needs to detect a suitable cell to camp on, and for that cell, obtain the symbol, subframe, and frame timing as well as synchronize to the carrier frequency. In addition, due to the presence of multiple cells, the UE needs to distinguish a particular cell on the basis of an NB-PCID.

NB-IoT is intended to be used for very low-cost UEs and at the same time provide extended coverage for UEs deployed in environments with high penetration losses (e.g., the basement of a building). Such low-cost UEs are equipped with low-cost crystal oscillators that can have an initial carrier frequency offset (CFO) as large as 20 ppm. Deployment in-band and in guard-bands of LTE introduces an additional raster offset (2.5 or 7.5 kHz) as explained earlier, giving rise to an even higher CFO. Despite this large CFO, a UE should also be able to perform accurate synchronization at very low signal-to-noise ratio (SNR).

Synchronization in NB-IoT follows similar principles as the synchronization process in LTE, but with changes to the design of the synchronization sequences in order to resolve the problem of estimating large frequency offset and symbol timing at very low SNR. Synchronization is achieved through the use of NPSS and NSSS. The NPSS is used to obtain the symbol timing and the CFO, and the NSSS is used to obtain the NB-PCID and the timing within an 80 ms block.

For UEs operating at very low SNR, an auto correlation based on a single 10 ms received segment would not be sufficient for detection. As a result, an accumulation procedure over multiple 10 ms segments is necessary. Because of the inherent NPSS design, the accumulation can be performed coherently, providing sufficient signal energy for detection.

After the synchronization procedure is complete, the UE has knowledge of the symbol timing, the CFO, the position within an 80 ms block, and

	Physical channel	Relationship with LTE
Downlink	NPSS	<ul style="list-style-type: none"> • New sequence for fitting into one PRB (LTE PSS overlaps with middle six PRBs) • All cells share one NPSS (LTE uses 3 PSSs)
	NSSS	<ul style="list-style-type: none"> • New sequence for fitting into one PRB (LTE SSS overlaps with middle six PRBs) • NSSS provides the lowest 3 least significant bits of system frame number (LTE SSS does not)
	NPBCH	<ul style="list-style-type: none"> • 640 ms TTI (LTE uses 40 ms TTI)
	NPDCCH	<ul style="list-style-type: none"> • May use multiple PRBs in time, i.e. multiple subframes (LTE PDCCH uses multiple PRBs in frequency and 1 subframe in time)
	NPDSCH	<ul style="list-style-type: none"> • Use TBCC and only one redundancy version (LTE uses Turbo Code with multiple redundancy versions) • Use only QPSK (LTE also uses higher order modulations) • Maximum transport block size (TBS) is 680 bits. (LTE without spatial multiplexing has maximum TBS greater than 70000 bits, see [9]) • Supports only single-layer transmission (LTE can support multiple spatial-multiplexing layers)
Uplink	NPRACH	<ul style="list-style-type: none"> • New preamble format based on single-tone frequency hopping using 3.75 kHz tone spacing (LTE PRACH occupies 6 PRBs and uses multi-tone transmission format with 1.25 kHz subcarrier spacing)
	NPUSCH Format 1	<ul style="list-style-type: none"> • Support UE bandwidth allocation smaller than one PRB (LTE has minimum bandwidth allocation of 1 PRB) • Support both 15 kHz and 3.75 kHz numerology for single-tone transmission (LTE only uses 15 kHz numerology) • Use $\pi/2$-BPSK or $\pi/4$-QPSK for single-tone transmission (LTE uses regular QPSK and higher order modulations) • Maximum TBS is 1000 bits. (LTE without spatial multiplexing has maximum TBS greater than 70000 bits, see [9]) • Supports only single-layer transmission (LTE can support multiple spatial-multiplexing layers)
	NPUSCH Format 2	<ul style="list-style-type: none"> • New coding scheme (repetition code) • Uses only single-tone transmission

Table 1. Summary of NB-IoT physical signals and channels and their relationship with the LTE counterparts.

the NB-PCID. The UE then proceeds to the acquisition of the MIB, which is broadcast in subframe #0 of every frame carried by NPBCH. The NPBCH consists of eight self-decodable sub-blocks, and each sub-block is repeated eight times, so each sub-block occupies subframe #0 of eight consecutive frames. Therefore, one NPBCH codeword is distributed over 64 frames (i.e., 640 ms) using subframe 0. The design is intended to enable successful acquisition for UEs in deep coverage.

After the symbol timing is known and the CFO is compensated for, in the in-band and guard-band deployment there is still an additional raster offset which can be as high as 7.5 kHz. The presence of raster offset results in either overcompensation or undercompensation of the carrier frequency. As a result, the symbol timing drifts in either the forward or backward direction depending on whether the carrier frequency was overcompensated or undercompensated. This may cause a severe degradation in the performance of NPBCH detection if the NPBCH is not detected on the first try. For example, an unsuccessful detection of NPBCH in the first attempt introduces a latency of 640 ms before the next NPBCH detection attempt. A 7.5 kHz raster offset leads to a symbol timing drift of 5.33 μ s (assuming a carrier frequency of 900 MHz), which is greater than the duration of the cyclic prefix. As a result, the downlink orthogonality of OFDMA is lost. A solution to this problem comes at the expense of a small increase in computational complexity, where the UE can perform “hypothesis testing” over the set of possible raster offsets to improve the detection performance.

RANDOM ACCESS

In NB-IoT, random access serves multiple purposes such as initial access when establishing a radio link and scheduling request. Among others, one main objective of random access is to achieve uplink synchronization, which is important for maintaining uplink orthogonality in NB-IoT.

To serve UEs in different coverage classes that have different ranges of path loss, the network can configure up to three NPRACH resource configurations in a cell. In each configuration, a repetition value is specified for repeating a basic random access preamble. UE measures its downlink received signal power to estimate its coverage level, and transmits a random access preamble in the NPRACH resources configured for its estimated coverage level. To facilitate NB-IoT deployment in different scenarios, NB-IoT allows flexible configuration of NPRACH resources in a time-frequency resource grid with the following parameters:

- Time domain: periodicity of NPRACH resource and starting time of NPRACH resource in a period
- Frequency domain: frequency location (in terms of subcarrier offset) and number of subcarriers

It is possible that in early NB-IoT field trials and deployment, some UE implementations may not support multi-tone transmission. The network should therefore be aware of UE multi-tone transmission capability before scheduling uplink transmission. To support this, the network can partition the NPRACH subcarriers in the frequency domain into two non-overlapping sets. A UE can select

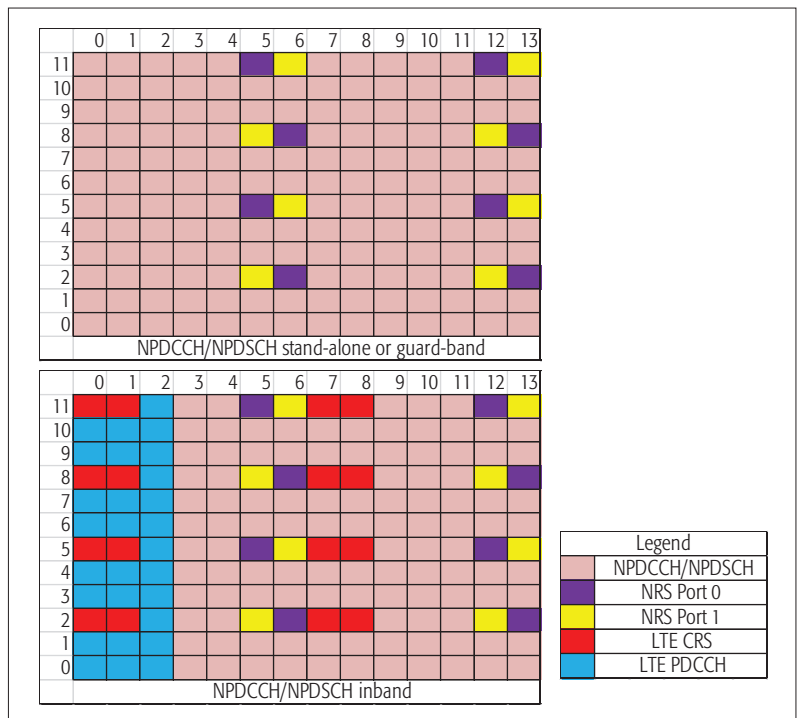


Figure 4. NPDCCH/NPDSCH resource mapping example.

one of the two sets to transmit its random access preamble to signal whether or not it supports multi-tone transmission.

In summary, UE determines its coverage level by measuring downlink received signal power. After reading system information on NPRACH resource configuration, the UE can determine the NPRACH resource configured and the number of repetitions needed for its estimated coverage level and transmit power. Then the UE can transmit repetitions of the basic single-tone random access preamble back to back within one period of the NPRACH resources. The remaining steps in the random access procedure are similar to LTE, and we omit the details here. Additional information about NB-IoT random access can be found in [11].

SCHEDULING AND HARQ OPERATION

To enable low-complexity UE implementation, NB-IoT allows only one HARQ process in both downlink and uplink, and allows longer UE decoding time for both NPDCCH and NPDSCH. An asynchronous, adaptive HARQ procedure is adopted to support scheduling flexibility. An example is illustrated in Fig. 5. A scheduling command is conveyed through a downlink control indicator (DCI), which is carried by NPDCCH. NPDCCH may use aggregation level (AL) 1 or 2 for transmitting a DCI [8, 10]. With AL-1, two DCIs can be multiplexed in one subframe; otherwise, one subframe only carries one DCI (i.e., AL-2), giving rise to a lower coding rate and improved coverage. Further coverage enhancement can be achieved through repetition. Each repetition occupies one subframe. DCI can be used for scheduling downlink data or uplink data. In the case of downlink data, the exact time offset between NPDCCH and the associated NPDSCH is indicated in the DCI. Since IoT

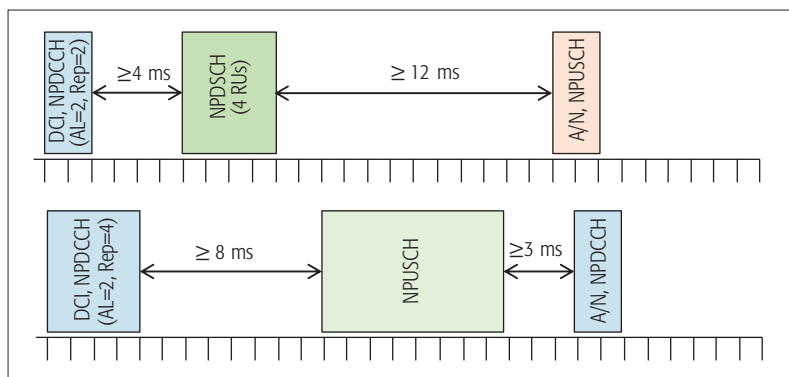


Figure 5. Timing relationship operation (each unit corresponds to one sub-frame).

devices are expected to have reduced computing capability, the time offset between the end of NPDCCH and the beginning of the associated NPDSCH is at least 4 ms [10]. In comparison, LTE PDCCH schedules PDSCH in the same TTI. After receiving NPDSCH, the UE needs to send back a HARQ acknowledgment using NPUSCH Format 2. The resources of NPUSCH carrying the HARQ acknowledgment are also indicated in DCI [10]. The time offset between the end of NPDCCH and the start of the associated HARQ acknowledgment is at least 12 ms [10]. This allows a UE ample decoding time.

Similarly, uplink scheduling and HARQ operation are also illustrated in Fig. 5. The DCI for an uplink scheduling grant needs to specify which subcarriers a UE is allocated [10]. The time offset between the end of NPDCCH and the beginning of the associated NPUSCH is at least 8 ms [10]. After completing the NPUSCH transmission, the UE monitors NPDCCH to learn whether NPUSCH is received correctly by the base station, or a retransmission is needed.

PERFORMANCE

IoT use cases are characterized by requirements such as data rate, coverage, device complexity, latency, and battery lifetime. These are thus important performance metrics. Furthermore, according to [12], IoT traffic is forecast to have compounded annual growth rate of 23 percent between 2015 and 2023. It is therefore important to ensure that NB-IoT has good capacity to support such growth in the years to come.

PEAK DATA RATES

NPDSCH peak data rate can be achieved by using the largest TBS of 680 bits and transmitting it over 3 ms [10]. This gives 226.7 kb/s peak layer 1 data rate. NPUSCH peak data rate can be achieved by using the largest TBS of 1000 bits and transmitting it over 4 ms [10]. This gives 250 kb/s peak layer 1 data rate. However, the peak throughputs of both downlink and uplink are lower than the above figures when the time offsets between DCI, NPDSCH/NPUSCH, and HARQ acknowledgment are taken into account.

COVERAGE

NB-IoT achieves a maximum coupling loss 20 dB higher than LTE Rel-12 [12–14]. Coverage extension is achieved by trading off data rate through

increasing the number of repetitions. Coverage enhancement is also ensured by introducing single subcarrier NPUSCH transmission and $\pi/2$ -BPSK modulation to maintain close to 0 dB PAPR, thereby reducing the unrealized coverage potential due to power amplifier backoff. NPUSCH with 15 kHz single-tone gives a layer 1 data rate of approximately 20 b/s when configured with the highest repetition factor (i.e., 128) and the most robust modulation and coding scheme (MCS). NPDSCH gives a layer 1 data rate of 35 b/s when configured with repetition factor 512 and the most robust MCS. These configurations support close to 170 dB coupling loss. In comparison, the Rel-12 LTE network is designed for up to approximately 142 dB coupling loss [14].

DEVICE COMPLEXITY

NB-IoT enables low-complexity UE implementation by the designs highlighted below:

- Significantly reduced transport block sizes.
- Support only one redundancy version in the downlink.
- Support only single-stream transmissions.
- Only single antenna is required at the UE.
- Support only single HARQ process.
- No need for a turbo decoder at the UE.
- No Connected mode mobility measurement is required. A UE only needs to perform mobility measurement during Idle mode.
- Low sampling rate due to lower UE bandwidth.
- Allow only half-duplex frequency-division duplexing operation.
- No parallel processing is required. All the physical layer procedures occur in a sequential manner.

The coverage objective is achieved with 20 or 23 dBm power amplifier, making it possible to use an integrated power amplifier in the UE.

LATENCY AND BATTERY LIFETIME

NB-IoT targets latency-insensitive applications. However, for applications like sending alarm signals, NB-IoT is designed to allow less than 10 s latency [3]. NB-IoT aims to support long battery life. For a device with 164 dB coupling loss, a 10-year battery life can be reached if the UE transmits 200 bytes of data a day on average [3].

CAPACITY

NB-IoT supports massive IoT capacity by using only one PRB in both uplink and downlink. Sub-PRB UE scheduled bandwidth is introduced in the uplink, including single-subcarrier NPUSCH. Note that for a coverage limited UE, allocating higher bandwidth is not spectrally efficient as the UE is power limited rather than bandwidth limited. Based on the traffic model in [3], NB-IoT with one PRB supports more than 52,500 UEs per cell [3]. Furthermore, NB-IoT supports multiple carrier operation. Thus, more IoT capacity can be added by adding more NB-IoT carriers.

CONCLUSION

In this article, a description of NB-IoT radio access is given. We emphasize how radio access is designed differently compared to LTE, and how it is designed to fulfill the performance requirements of IoT such

as significant coverage extension, low device complexity, long battery lifetime, and supporting a massive number of IoT devices. Further enhancements of NB-IoT in the next 3GPP Release are ongoing in 3GPP, including, for example, introducing low-complexity multicast functionality, for rolling out firmware updates and enhancing positioning accuracy, which is important to many IoT applications. NB-IoT is a step toward building the fifth generation (5G) radio access technology intended for enabling new use cases like machine type communications. NB-IoT devices, after deployment, are expected to remain in the network for many years, likely beyond network migration toward 5G. It is thus important to design 5G radio access technology to coexist well with NB-IoT and its evolutions. It is also important to ensure that NB-IoT continues to evolve toward meeting all 5G requirements for IoT, minimizing any need to introduce a new 5G IoT technology, which may cause market fragmentation and reduce the benefit of economy of scale. NB-IoT ushers in ultra-low-cost devices and has enough capacity to support a massive number of these devices in a cell. This is also a step toward the fog network [15] as these devices, although individually simple and low-cost, collectively form significant capability in terms of sensing, intelligence, storage, and computing.

REFERENCES

- [1] "Cellular Networks for Massive IoT," Ericsson White Paper, Jan. 2016; https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf, accessed Oct. 6, 2016.
- [2] H. Shariatmadari et al., "Machine-Type Communications: Current Status and Future Perspectives toward 5G Systems," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2015, pp. 10–17.
- [3] 3GPP TR 45.820, "Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things," v. 13.1.0, Nov. 2015, http://www.3gpp.org/ftp/Specs/archive/45_series/45.820/45820-d10.zip, accessed Oct. 6, 2016.
- [4] Ericsson and Nokia Networks, "Further LTE Physical Layer Enhancements for MTC," RP-141660, 3GPP TSG RAN Meeting #65, Sept. 2014; http://www.3gpp.org/ftp/tsg_ran/tsg_ran/TSGR_65/Docs/RP-141660.zip, accessed Oct. 6, 2016.
- [5] P. Stuckmann, *The GSM Evolution: Mobile Packet Data Services*, Wiley, 2003.
- [6] E. Dahlman, S. Parkvall and J. Sköld, *4G: LTE/LTE-Advanced for Mobile Broadband*, Oxford, Academic Press, 2011.
- [7] Qualcomm, Inc., "Narrowband IoT (NB-IoT)," RP-151621, 3GPP TSG RAN Meeting #69, Sept. 2015; http://www.3gpp.org/ftp/tsg_ran/TSR_RAN/TSGR_69/Docs/RP-151621.zip, accessed Oct. 6, 2016.
- [8] 3GPP TS36.211, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Physical Channels and Modulation," v. 13.3.0, Sept. 2016, http://www.3gpp.org/ftp/Specs/archive/36_series/36.211/36211-d30.zip, accessed Oct. 8, 2016.
- [9] 3GPP TS36.212, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Multiplexing and channel coding," v. 13.3.0, Sept. 2016; http://www.3gpp.org/ftp/Specs/archive/36_series/36.212/36212-d30.zip, accessed Oct. 8, 2016.
- [10] 3GPP TS36.213, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Physical Layer Procedures," v13.3.0, Sept. 2016; http://www.3gpp.org/ftp/Specs/archive/36_series/36.213/36213-d30.zip, accessed Oct. 8, 2016.
- [11] X. Lin, A. Adhikary, and Y.-P. E. Wang, "Random Access Preamble Design and Detection for 3GPP Narrowband IoT systems," to appear, *IEEE Wireless Commun. Letters*.
- [12] "Ericsson Mobility Report, on the Pulse of the Networked Society," Ericsson White Paper, June 2016; <https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf>, accessed Oct. 6, 2016.
- [13] A. Adhikary, X. Lin and Y.-P. E. Wang, "Performance Evaluation of NB-IoT Coverage," *Proc. IEEE VTC-Fall*, Montreal, Canada, Sept. 18–21, 2016.
- [14] TR 36.888 v12.0.0, "Study on Provision of Low-Cost Machine-Type Communications (MTC) User Equipments (UEs) Based on LTE," June 2013; http://www.3gpp.org/ftp/Specs/archive/36_series/36.888/36888-c00.zip, accessed Oct. 6, 2016.
- [15] F. Bonomi et al., "Fog Computing and Its Role in the Internet of Things," *Proc. ACM Wksp. Mobile Cloud Computing*, Helsinki, Finland, Aug. 17, 2012.

BIOGRAPHIES

Y.-P. ERIC WANG (eric.y.p.wang@ericsson.com) received his Ph.D. degree in electrical engineering from the University of Michigan, Ann Arbor, in 1995. Since then he has been a member of Ericsson Research. He was a technical leader at Ericsson during the concept development and standardization of NB-IoT. He served as an Associate Editor for *IEEE Transactions on Vehicular Technology* from 2003 to 2007. He has contributed to more than 50 conference and journal articles.

XINGQIN LIN (xingqin.lin@ericsson.com) received his Ph.D. degree in electrical and computer engineering from the University of Texas at Austin (UT Austin) in 2014. He is currently a research engineer with the Radio Access Technologies team at Ericsson Research, Santa Clara, California. He received the MCD fellowship from UT Austin. He held summer internships at Alcatel-Lucent Bell Labs, Nokia Siemens Networks, and Qualcomm CR&D. He serves as an Editor of *IEEE Communications Letters*.

ANSUMAN ADHIKARY (ansuman.adhikary@ericsson.com) received his B.Tech. degree from Indian Institute of Technology, Kharagpur (2003), his M.Tech. degree from Indian Institute of Technology, Kanpur (2009), and his Ph.D. degree from the University of Southern California, Los Angeles (2014), all in electrical engineering. He was a research engineer at Ericsson Research USA 2014–2016, and is currently working as a systems engineer at Qualcomm India, Hyderabad. His research interests lie in the areas of wireless communications and information theory.

ASBJØRN GRØVLEN (asbjorn.groflen@ericsson.com) received an M.Sc. degree in electrical engineering from the Norwegian University of Science and Technology, Trondheim, Norway, in 1994. He currently works as a researcher in standardization at Ericsson Sweden attending 3GPP RAN WG1 with a focus on MTC related topics and most recently on New Radio (5G). Previously, he held similar positions at Nokia, Renesas, and Broadcom. He served as a Rapporteur during the standardization of NB-IoT in 3GPP Release 13.

YUTAO SUI (yutao.sui@ericsson.com) received his Ph.D. degree in communication systems from Chalmers University of Technology, Gothenburg, Sweden. His main research interests are in design and analysis of physical layer algorithms, multiple access, vehicular small cells, and massive machine type communication. He is currently a standardization researcher at Ericsson, Stockholm, Sweden, with focus on machine type communication related standardization works.

YUFEI BLANKENSHIP (yufei.blankenship@ericsson.com) received her Ph.D. degree in electrical engineering from Virginia Tech in 2000. From 2000 to 2007, she was with Motorola Labs, working on physical layer standardization with an emphasis on channel coding. She is currently a standards researcher with Ericsson. For 3GPP LTE Release 13, her focus was in the areas of MTC and NB-IoT.

JOHAN BERGMAN (johan.bergman@ericsson.com), M.Sc., is a researcher at Ericsson AB, Stockholm, Sweden. Since 2005, he has been working with physical layer standardization for 3G HSPA and 4G LTE in 3GPP. As Rapporteur for 3GPP Release 13/14 Work Items, he has been a driver for the technical work to standardize the new LTE-based features dedicated to machine type communications.

HAZHIR SHOKRI RAZAGHI (hazhir.shokri.razaghi@ericsson.com) received his Master's degree in electrical engineering from the Royal Institute of Technology, Stockholm, Sweden. He joined Ericsson in 2013 and has been working on different aspects of LTE technology since then. Currently he is working on the physical layer aspect of machine type communication and Internet of Things (IoT). Most of his work is in regard to 3GPP standardization.

NB-IoT ushers in ultra-low cost devices and has enough capacity to support a massive number of these devices in a cell. This is also a step toward the Fog network [15] as these devices, although individually simple and low-cost, collectively form significant capability in terms of sensing, intelligence, storage, and computing.

The Random Access Procedure in Long Term Evolution Networks for the Internet of Things

Tiago P. C. de Andrade, Carlos A. Astudillo, Luiz R. Sekijima, and Nelson L. S. da Fonseca

The authors review the LTE random access procedure and its support for IoT applications. They also assess the performance of the RAN overload control schemes proposed by 3GPP, taking into consideration the interaction between the random access procedure and packet downlink control channel resource allocation.

ABSTRACT

Network connectivity is a key issue in the realization of IoT, and LTE cellular technology is the most promising option for the provisioning of such connectivity. However, in LTE networks, a large number of IoT devices trying to access the medium can overload the RAN. In this article, we review the LTE random access procedure and its support for IoT applications. We also assess the performance of the RAN overload control schemes proposed by 3GPP, taking into consideration the interaction between the random access procedure and packet downlink control channel resource allocation.

INTRODUCTION

In the Internet of Things (IoT), tens of billions of devices with sensing, computing, and communication capabilities will improve our daily life and create new business opportunities [1]. Various sectors will benefit from the information exchange in IoT, such as transportation, health care, and manufacturing, as well as the development of smart cities, smart grid, and smart home. Devices will be interconnected by a diverse communication infrastructure, with connectivity being a key issue for the realization of IoT.

Machine-to-machine (M2M) communication, or machine-type communication (MTC) technology, will enable the interaction of IoT devices. Technologies using unlicensed frequency bands and featuring low power consumption for a short transmission range, such as RF identification, Zigbee, Bluetooth Low Energy, and low-power WiFi, have been designed to support M2M applications. However, in order to provide coverage for wide areas, which is a key requirement for various IoT applications, these technologies rely on multihop packet forwarding, as well as the addition of backhaul links. Moreover, these technologies are prone to interference because of the use of the unlicensed spectrum, which reduces the reliability and availability of these systems, and increases communication delays [2].

To overcome some of these limitations, long-range, low-power communication technologies, known as low-power wide area, such as Sigfox, LoRa, Weightless, and Long Term Evolution (LTE),¹ are gaining momentum in the IoT connectivity landscape [3], with the LTE cellular technology being the most suitable solution for the

interconnection of IoT devices due to its wide coverage, security, licensed spectrum, and simplicity of management. By using LTE technology for MTC, mobile network operators (MNOs) can leverage their investment in 4G LTE networks to provide IoT connectivity.

Traditionally, cellular networks were designed to support human-to-human (H2H) communications. However, the requirements of IoT M2M communication and the energy limitation of devices impose additional requirements for the cellular networks. For example, severe congestion can occur when a massive number of transmitting devices attempt to access the network simultaneously. Moreover, the connection-oriented communication in traditional cellular networks can generate excessive signaling overhead for transmitting small data packets generated by IoT applications. Consequently, quality of service (QoS) provisioning for human-type communication (HTC) and MTC can be jeopardized.

In order to make the LTE technology more suitable for M2M communications, 3GPP LTE-standard Releases 11, 12, and 13 included different features to support MTC applications, known as LTE for MTC (LTE-M), as well as a new technology, known as Narrowband LTE (NB-LTE).

This article focuses on the radio access network (RAN) overload problem, especially the problem of congestion arising from a massive number of MTC devices trying simultaneously to access the LTE network. The evolution of the LTE standard for the support of IoT applications is reviewed, especially a variety of proposals impacting the random access procedure. The performance of the main approaches for the amelioration of the RAN overload problem [4] is shown. This article considers the interaction of the random access procedure and packet downlink control channel (PDCCH) resource allocation, which has not been undertaken previously. Results derived via extensive simulations show that the RAN overload problem has been underestimated. We show that physical and PDCCH constraints strongly impact the network performance during the random access procedure. Based on these findings, we present key research directions for the improvement of the performance of the random access procedure of LTE to enhance the access by the massive number of devices expected in IoT scenarios.

¹ In this article, we use LTE to refer to all technologies based on Third Generation Partnership Project (3GPP) LTE standards (Release 8 and beyond).

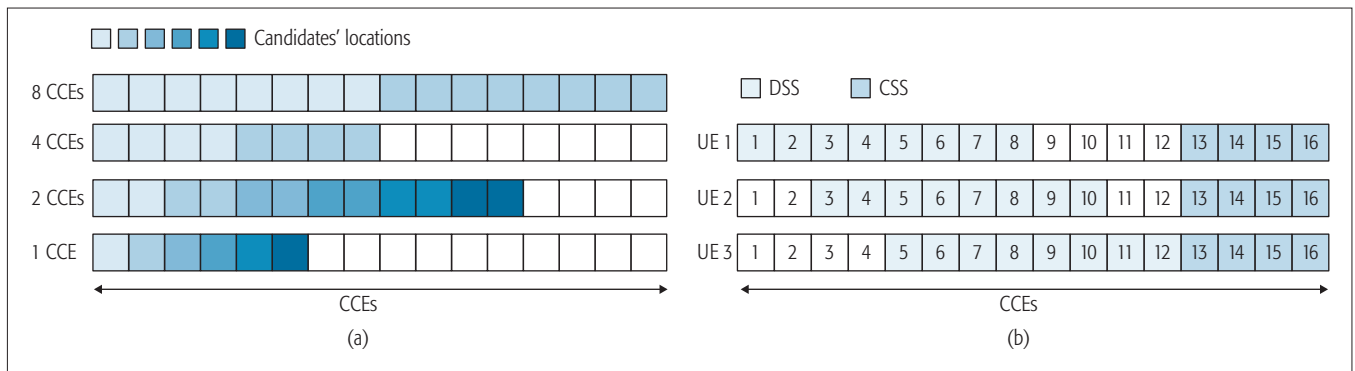


Figure 1. Constraints to the PDCCH resource allocation in LTE networks: a) PDCCH search space candidates; b) overlap on PDCCH for different UEs.

LTE PACKET DOWNLINK CONTROL CHANNEL

In the PDCCH, downlink control Information (DCI) messages are transmitted carrying downlink assignment, uplink grants, and random access related messages. Assignments are used to convey the information needed to receive data from the evolved NodeB (eNB) on the physical downlink shared channel (PDSCH), whereas grants allow user equipments (UEs) to transmit data to the eNB on the packet uplink shared channel (PUSCH). The PDCCH uses up to the first three orthogonal frequency-division multiplexing (OFDM) symbols of each subcarrier.

Each DCI message can use 1, 2, 4, or 8 control channel elements (CCEs) (aggregation levels), depending on the message format and channel quality. The DCI messages are sent on the PDCCH, but the UE does not know a priori information about the exact location of its messages. Each UE applies blind decoding on a specific set of CCEs in two regions of the PDCCH, the common search space (CSS) and the dedicated search space (DSS) to determine which, if either, contains DCI message(s) to the device. Each UE will monitor 6 candidate locations at aggregation levels 1 and 2, as well as 2 candidate locations at levels 4 and 8, as illustrated in Fig. 1a.

One problem with the design of the PDCCH is that the eNB cannot freely use all available CCEs to schedule DCI messages, which can only be scheduled on the specific PDCCH resources of the intended UE. Thus, there can be an overlap in the resources allocated for the UEs on the PDCCH if there are few CCEs or a large number of UEs in the cell, as illustrated in Fig. 1b.

LTE RANDOM ACCESS PROCEDURE

The random access procedure is performed by a UE in the following cases:

- Upon initial access to the network
- Upon arrival of uplink data at the UE buffer if no radio resources have been assigned to request uplink resources
- During handover
- Upon radio failure to re-establish a connection
- When the UE is not synchronized with the eNB

There are two types of random access (RA) procedures: contention-free and contention-based. The former is used to perform handover, whereas the latter is used otherwise. The four-way

handshake contention-based RA procedure is described below.

The UE first transmits a preamble (msg1) message on the random access channel during the first random access opportunity (RAO) after the triggering of the random access procedure. The eNB periodically informs the UEs about a set of up to 64 orthogonal preamble sequences from which the UE can make a choice. Collisions occur when two or more UEs transmit the same preamble sequence during the same RAO. However, the eNB does not detect such collisions during this step.

The second step is the transmission of a random access response (RAR) (msg2) message by the eNB, addressed to the random access temporary identifier (RA-RNTI) over the downlink shared channel. A DCI message is thus scheduled on the CSS of the PDCCH to indicate the PDSCH resources in which the RAR message was transmitted. This message contains a timing advance command and an uplink grant for the transmission of a message in the following step. If the UE device that sent a preamble sequence does not receive an msg2 message from the eNB within a certain period of time, it enters a backoff period again, trying to access the network once this period has expired.

Then the UE transmits a layer 2/3 (L2/L3) (msg3) message on the uplink shared channel. The message is addressed to the RA-RNTI and carries either the identity of the UE, if it is in the connected radio resource control (RRC) state, or a temporary UE identity (if the UE is in the idle RRC state). If two or more UEs have chosen the same preamble sequence in a RAO, they will receive the same grant in the RAR message, and thus, all their L2/L3 message transmissions will collide. A contention resolution (msg4) message is then sent to each UE on which msg3 message was successfully received by the eNB.

LTE RAN ENHANCEMENT FOR MTC AND ITS IMPLICATIONS FOR RANDOM ACCESS PROCEDURE PERFORMANCE

This section provides a brief review of the efforts by 3GPP to support MTC, highlighting UE categories and capabilities, as well as the implications of these efforts for the random access procedure.

ENHANCEMENT FOR MTC

3GPP Release 11 focuses on RAN overload control schemes [4], which can improve network reliability in the face of a massive number of simul-

The 3GPP Release 12 introduces a new LTE UE device category (Cat. 0) for MTC devices to potentiate LTE penetration into restrictive MTC markets. This new category decreases the cost and complexity of the LTE chipset. It features a single receiver, 1 Mb/s maximum bit rate, and half-duplex operation.

aneous attempts to access the network. Most of these solutions are based on the barring of access of devices or the splitting of random access radio resources between different UE device classes. Moreover, an enhanced PDCCH (ePDCCH) structure has been proposed. By using the ePDCCH, a portion of the resources dedicated to the PDSCH is used for conveying control resources. It can alleviate the shortage of control resources resulting from a massive number of devices [5].

3GPP Release 12 introduces a new LTE UE device category (Cat. 0) for MTC devices to potentiate LTE penetration into restrictive MTC markets. This new category decreases the cost and complexity of the LTE chipset. It features a single receiver, 1 Mb/s maximum bit rate, and half-duplex operation, which can achieve a 50 percent reduction in complexity and a 30 percent reduction in cost when compared to a Cat. 1 chipset.

Two important features for MTC devices are introduced in 3GPP Release 13: enhanced coverage and Cat. M1, a new low-complexity UE device category. The Cat. M1 reception bandwidth has been reduced to 1.4 MHz. This release also introduces coverage levels and physical channel repetitions to improve coverage and allows the relaxation of hardware requirements. These cost reductions and coverage enhancements allow MNOs to cover a larger number of IoT applications with LTE technology. Since the legacy PDCCH is spread across the entire bandwidth, a new PDCCH design, the MTC PDCCH, has been developed to support this new category. However, the uplink channel, including the physical random access channel (PRACH), remains the same as for UE Cat. 0 and above.

The final 3GPP enhancement for MTC is called NB-LTE [6], which will operate with a 200 kHz channel bandwidth. Consequently, other UE device categories will be introduced in future releases, further reducing the cost of the MTC device. Such a new category should reduce the complexity of hardware by at least 80 percent in comparison with the hardware of a Cat. 1 UE. This technology aims to support ultra-low-complexity and low-throughput IoT applications via LTE cellular systems. Although NB-LTE still makes extensive use of the higher-layer user plane, it represents a “clean slate” approach,² in which many aspects of the physical layer of the LTE technology will be changed. In the uplink, the duration of OFDM symbol, slot, and subframe will be six times longer than its LTE counterpart. Thus, an NB-LTE subframe (M-subframe) is now 6 ms rather than the 1 ms in the traditional LTE system. Even though NB-LTE has the possibility of 64 preamble sequences available as well as the random access procedure with four messages, it remains basically the same as for the standard LTE technology; the MTC PRACH occupies two M-subframes (12 ms) and uses different preamble sequence signals. Depending on the level of coverage, which determines the number of repetitions required, up to six M-subframes may be needed to transmit the preamble sequence. Six devices is the maximum number that can be scheduled in an M-subframe. The Narrowband IoT technology, which is similar to NB-LTE, was recently included in 3GPP Release 13.

IMPLICATIONS ON THE RANDOM ACCESS PROCEDURE

Although the ePDCCH was proposed to alleviate the shortage of control resources, this channel still has two important limitations during the random access procedure. One limitation is that the ePDCCH is configured in the UE only after the establishment of the RRC connection [7]. As a consequence, devices in idle RRC state (usually when the device performs its initial access) cannot use this channel during the random access procedure; moreover, the eNB must rely exclusively on the PDCCH to allocate the control messages to random-access-related messages. The second limitation is that the ePDCCH supports only UE-specific DCI allocations, which means it cannot be used to allocate control resources to RAR messages. Another issue is the reduction in the capacity to transmit data on the downlink as a consequence of resource sharing with the PDSCH. This can have an impact on the performance of downlink-intensive HTC users in a scenario with coexisting M2M/H2H communications.

The main difference between the ePDCCH and the MTC PDCCH of UE Cat. M1 is that the latter also supports CSS allocation, thus allowing the base station to allocate resources to RAR messages in the MTC PDCCH. The enhanced coverage feature in 3GPP Release 13 increases access delay due to repetition of the transmissions.

Although NB-LTE devices perform the random access procedure as described earlier, 3GPP considered that advanced RAN overload control schemes will not be required, due to the adoption of a simple mechanism based on an access class barring (ACB) bitmap. Moreover, the delay during the random access procedure may increase significantly since only a single device can be scheduled per millisecond on average. In traditional LTE networks, however, devices can transmit not only 3 msg3/ms on average but also conventional downlink/uplink data. However, this is not expected to affect performance, since Narrowband IoT applications are generally delay-tolerant, and the NB-LTE system will not share resources with legacy LTE users. Thus, those IoT applications with a QoS requirement or throughput constraints will use Cat. M1 chipsets or above.

Based on this analysis, we now focus on the interaction between the random access procedure and the PDCCH. Therefore, the insights arising from this article can be generalized to all LTE-M technologies, including Releases 11, 12, and 13.

STATE OF THE ART IN RAN OVERLOAD CONTROL FOR LTE NETWORKS

Different approaches have been proposed to counteract the RAN overload problem, most of which were proposed by 3GPP in [4]. This section briefly discusses some novel solutions that use more robust approaches, solutions that do not use a combination of 3GPP proposed schemes, but rather more innovative ones. These approaches have emerged as a consequence of the limitations of the existing solutions in the LTE standards.

An approach for handling massive MTC traffic by using a dense network was proposed in [8]. Femtocells are used to decrease the access delay

² There is no agreement in 3GPP whether NB-LTE is a clean slate approach or not.

Scheme	Benefits	Limitations	Challenges	Overhead
Access class barring	Different access probability values can be configured to deal with different PRACH loads.	Low flexibility to provide device differentiation	Determination of the barring probability based on the PRACH load	Low computational processing and low number of message exchanges
EAB	Access differentiation can be provided with fine granularity.	Access classes are either completely barred or unbarred and only delay-tolerant devices are supported.	Determination of the PRACH load and selection of the barred and unbarred classes	Moderate computational processing and moderate number of message exchanges
SB	Collisions are solved faster and it is backward compatible with traditional backoff scheme.	Inefficient under high PRACH load conditions	Definition of the scheme settings based on the device requirements	Very low computational processing and very low number of message exchanges
RRS	HTC is not affected by MTC.	Inefficient when there is unbalanced load between MTC and HTC	Dynamic allocation of RA resources for each device type	Very low computational processing and very low message exchanges
Slotted access	Dedicated RA slots for individual devices or group of devices	The number of unique RA slots is proportional to the RA cycle length. The PRACH is overloaded when the number of devices is greater than the total number of unique RA slots.	Effective allocation of RA slots to devices/groups	Low computational processing and messages exchange
Pull-based	Overload on PRACH can be effectively mitigated.	Unexpected surge of access requests cannot be handled.	Mechanism to decrease the load in the paging channel	High number of message exchanges in the core network and paging channel
Distributed queuing	Infinite number of simultaneous devices can ideally be handled.	Only delay-tolerant devices are supported.	Access delay increases as the number of devices increases.	High computational processing and high number of message exchanges
Femto-cell-based	Low energy consumption; support for high number of simultaneous devices	Lack of access differentiation; low outdoor coverage	Differentiation of users' attempts	Huge cost of the approach for MNOs

Table 1. Summary of the RAN overload control schemes proposed by 3GPP.

as well as energy consumption. However, this is not a cost-effective solution and is not practical in real IoT scenarios.

Another solution, proposed in [3], is distributed queuing (DQ)-based. It supports an infinite number of contending devices over PRACH. It has clear advantages over the conventional RA procedure; delays and energy consumption are reduced more than they are in the 3GPP RAN overload control schemes. Nevertheless, the access delay is greater than that required by delay-sensitive IoT applications.

In [9], two methods for the management of critical and emergency alarm messages in LTE networks are proposed. They require dedicated preambles for alarm devices as well as specific modifications of both the eNB and UE. Each message is mapped on either a predefined index or a sequence of preambles, depending on the method used. Although such methods can significantly reduce the time required for notification of an alarm to the eNB, they require excessive PRACH resources (i.e., RAO) every millisecond as well as the reservation of a set of preambles for use only by these applications. Table 1 shows a summary of the RAN overload control schemes [4].

PERFORMANCE EVALUATION

To evaluate the performance of different RAN overload control schemes, a special module was developed for the LTE-Sim simulator, which includes detailed implementation of the random access procedure, described next. The collision of

preambles can only be detected when a UE does not receive the msg4 message within the waiting time window. Thus, the UEs can send msg3 messages in the same PUSCH resources, even though this leads to collisions. In addition, whenever an msg3 message is retransmitted, the contention resolution timer is restarted. The PDCCH CSS and DSS mechanisms were also implemented. This inclusion reduces the region in which the eNB can allocate control information to each UE as well as increasing blocking on the PDCCH, when two or more UEs use the same region. The processing latency for each step of the RA procedure was introduced, following the specifications in [10].

We validated this new module by comparing its output with the metric values given by the 3GPP TR 37.868 MTC simulation model [4]. To provide a fair comparison, however, it was necessary to assume that the eNB does not decode simultaneous transmission of the same preamble, and, therefore does not send the uplink grant for those preambles as assumed in [4]. This comparison is displayed in Table 2, on the columns "LTE-Sim Module" and "3GPP TR 37.868," respectively. The last column of Table 2 shows the impact of the inclusion of the above-mentioned realistic assumptions in the enhanced simulation model. Simulations considered scenarios with 5000, 10,000, and 30,000 UEs, with the number of connection requests over a period of 10 s following a $Beta(3, 4)$ distribution as proposed in [4].

Tables 3 and 4 show the configuration param-

Metric	3GPP TR 37.868			LTE-Sim module			Enhanced LTE-Sim module		
	5000	10,000	30,000	5000	10,000	30,000	5000	10,000	30,000
Number of devices per cell	5000	10,000	30,000	5000	10,000	30,000	5000	10,000	30,000
Access success probability	100%	100%	29.5%	100%	100%	29.6%	100%	87.95%	14.93%
Average access delay (ms)	29.06	34.65	76.81	29.67	35.95	80.43	46.05	108.59	156.12
10th percentile access delay (ms)	15	15.25	15.89	15.02	15.39	16.52	17.19	20.97	19.83
90th percentile access delay (ms)	51.61	65.71	174.39	52.80	66.56	176.64	98.13	247.04	336.72
Number of preamble transmission	1.56	1.77	3.49	1.62	1.83	3.56	1.66	2.92	3.86
Preamble collision probability	0.45%	1.98%	47.76%	0.46%	1.96%	47.70%	0.44%	7.30%	53.21%
msg2 blocking probability	–	–	–	0%	0.73%	4.52%	0.03%	31.60%	63.66%

Table 2. Validation of our simulation model and the impact of realistic considerations on the performance of a traditional random access scheme.

eters used in the simulations. The following metrics were considered in the analysis: access probability, defined as the ratio between a fully complete RA and the total number of RAs triggered; average delay, defined as the time elapsed from the transmission of the first msg1 message to the reception of an msg4 message, considering only successful accesses; preamble collision ratio, which is the ratio between the number of events when two or more devices send the same msg1 message (collision) and the overall number of msg1 messages available during the period; CCE utilization, which is the ratio between the number of CCEs used on the PDCCH and the overall number of available CCEs in the PDCCH; and msg2 blocking probability, which is the ratio between the number of dropped msg2 messages to send msg3 and the number of this type of msg2 messages that joined the eNB queue.

Table 2 shows that the results for the enhanced LTE-Sim module differ from those of the other models due to consideration of realistic assumptions in both the detection of preamble sequence collisions and the allocation of control resources, with the access success probability decreasing while the preamble collision probability and the access delay increase. One of the reasons for the increase in the average access delay is the consideration that preamble collisions will only be detected when the msg4 message is not received. This increases the number of detected preambles, thus increasing the msg2 blocking probability. The dropping of the msg2 messages due to timeout of the timer is the main factor for the decrease in the access probability. This blocking occurs mainly when various UEs are trying to access the network at the same time (or in a short period) and the eNB does not have enough resources during the time window to send the msg2 messages. Another reason for the increased delay is the delay in the downlink grant for msg4 message on the PDCCH. This happens when the PDCCH resources for the allocation of msg4 message destined to a UE are already allocated to other UE msg4 messages, resulting in the postponement of the transmission of the msg4 message despite the existence of available resources on the PDCCH.

Under light loads, all schemes achieved 100 percent access, except some losses when using the Fixed-EAB (F-EAB) scheme (Fig. 2a). More-

over, the F-EAB scheme imposed the greatest average access delay, some 2.8 times greater than those of the second slowest scheme (the fixed-ACB [F-ACB]), and 46 times greater than the smallest delay imposed by the LTE scheme (Fig. 2b). No scheme produced a preamble collision probability greater than 1 percent (Fig. 2c), which suggest that few attempts using the same preamble were sent. However, the CCE utilization exceeded 20 percent in 6 schemes, the F-ACB scheme being the one with lowest utilization, only 11 percent (Fig. 2d). Although the operation of both ACB schemes is quite similar, the fixed approach imposes a greater average access delay than does the adaptive one. Since the barring probability varies as a function of the network load, and few preamble collisions occur on the network, it is possible to conclude that the variation in blocking probability is of little relevance, remaining most of the time in 0, thus allowing the preamble transmissions. The F-EAB scheme produces high msg2 blocking probability values as a consequence of numerous simultaneous access attempts (Fig. 2e). The other schemes spread access attempts along the timeline, decreasing the intensity of access attempts.

Under medium loads, the F-ACB, adaptive-ACB (A-ACB), adaptive-EAB (A-EAB), and specific backoff (SB) schemes also achieved an access ratio of almost 100 percent, despite a decrease in this ratio for certain other schemes (Fig. 2a). Such a high access probability is due to the fact that these schemes spread in time the attempts to transmit the preambles, thus avoiding collisions. However, such a high access success ratio leads to a considerable increase in delay, which reaches as high as 35 times (Fig. 2b). The access ratio of F-EAB decreased to 68 percent due to the period required for altering the unbarred class. The longer the period, the greater is the number of devices waiting to attempt access after the change of unbarred class. This procedure degrades the performance when compared to the performance of the LTE scheme. Such an increase is due to the large number of devices trying to use the same preamble in an attempt to access the network. Moreover, the CCE utilization of all schemes increased, reaching 50 percent for the conventional scheme, which shows that more msg4 messages were transmitted (Fig. 2d). The msg2

LTE	
Backoff period	20 ms
F-ACB	
Barring factor	0.9
Barring time	4 s
A-ACB	
Barring factor	Adaptive
Barring time	4 s
Monitoring period	500 ms
Update period	500 ms
F-EAB	
Round period	500 ms
ON/OFF	Always ON
A-EAB	
Round period	500 ms
ON/OFF	Adaptive
Update period	500 ms
RRS	
# preambles to HTC	22
# preambles to MTC	30
SB	
Backoff period HTC	20 ms
Backoff period MTC	960 ms

Table 3. RAN overload control schemes configuration.

blocking probability of all schemes increased, but the ACB schemes produced the lowest probability value, only 0.5 percent (Fig. 2e). However, this low value of the F-ACB scheme is achieved at the expense of high access delay (Fig. 2b). Conversely, the A-ACB scheme obtained msg2 blocking probability as low as 2.95 and 1.8 percent, respectively, while providing low access delays (Fig. 2b).

Under heavy loads, the access ratio decreases dramatically for some schemes. For the adaptive ACB scheme, the access ratio decreased 25 percent, while for the RACH resource separation (RRS) scheme, it decreased more than 90 percent (Fig. 2a). The separation of preambles according to the type of device (MTC or HTC) implies a reduction in the number of preambles for MTC devices and a consequent increase in the preamble collision probability (Fig. 2c). The preamble collision probability of the conventional scheme is 45 percent, while the preamble collision probability of the RRS scheme is 60 percent. As a consequence of the variation of barring probability, the preamble collision probability of the adaptive ACB scheme is only 15 percent. Despite the

Parameter	Value
System bandwidth	5 MHz
Frame structure	FDD
PRACH configuration Index	6
Max. preamble retransmissions	10
Number of msg2 per subframe	3
Total preamble sequences	52
RAR window size	5 ms
Contention resolution timer	48 ms
Max. msg3 retransmissions	5
Number of CCEs	16

Table 4. Simulation parameters.

F-ACB preamble collision probability of only 13 percent, the access probability achieves only 44 percent, and the CCE utilization is equal to 29 percent (Figs. 2b and 2d). Moreover, there is a slight increase in the CCE utilization over what is found for the scenario with 10,000 UEs for the F-ACB scheme, which suggests saturation of the networks. All the schemes produced an msg2 blocking probability lower than 40 percent, showing limitation of the capacity for sending RAR. For the ACB and EAB schemes, the fixed approach dropped more msg2 messages than did the adaptive one (Fig. 2e).

In summary, the performance of the RA procedure depends on the number of competing UEs and their generated traffic. For networks with a small number of UEs, the LTE scheme is more appropriate, since it provides a good trade-off between access ratio and delay. For instance, 100 percent of access is possible with a delay of only 47 ms. For networks with a large number of UEs generating delay-tolerant traffic, the recommendation is the employment of the adaptive ACB scheme, since it produces the greatest access ratio, although this access is delayed.

CHALLENGES AND RESEARCH DIRECTIONS

Although progress has been made in reducing the impact of the RAN overload problem, several challenges remain to be overcome, especially those related to the support of delay-sensitive IoT applications. This section discusses three key challenges originating from the need to provide some kind of guarantee to limit delays during the random access procedure as these can reach several seconds under heavy load conditions and control resources' influence on the performance.

QoS-AWARE RAN OVERLOAD CONTROL

Existing RAN overload control mechanisms do not provide QoS guarantees for delay-sensitive IoT applications. It is necessary to investigate new ways to reduce the random access delay as well as increase the chances of access of IoT devices [11]. For example, the adaptation of the distributed queuing approach for QoS provisioning has great potential for handling a very large number of devices but reducing the access delay. The

Existing RAN overload control mechanisms do not provide QoS guarantees for delay-sensitive IoT applications. It is necessary to investigate new ways to reduce the random-access delay as well as increasing the chances of access of IoT devices.

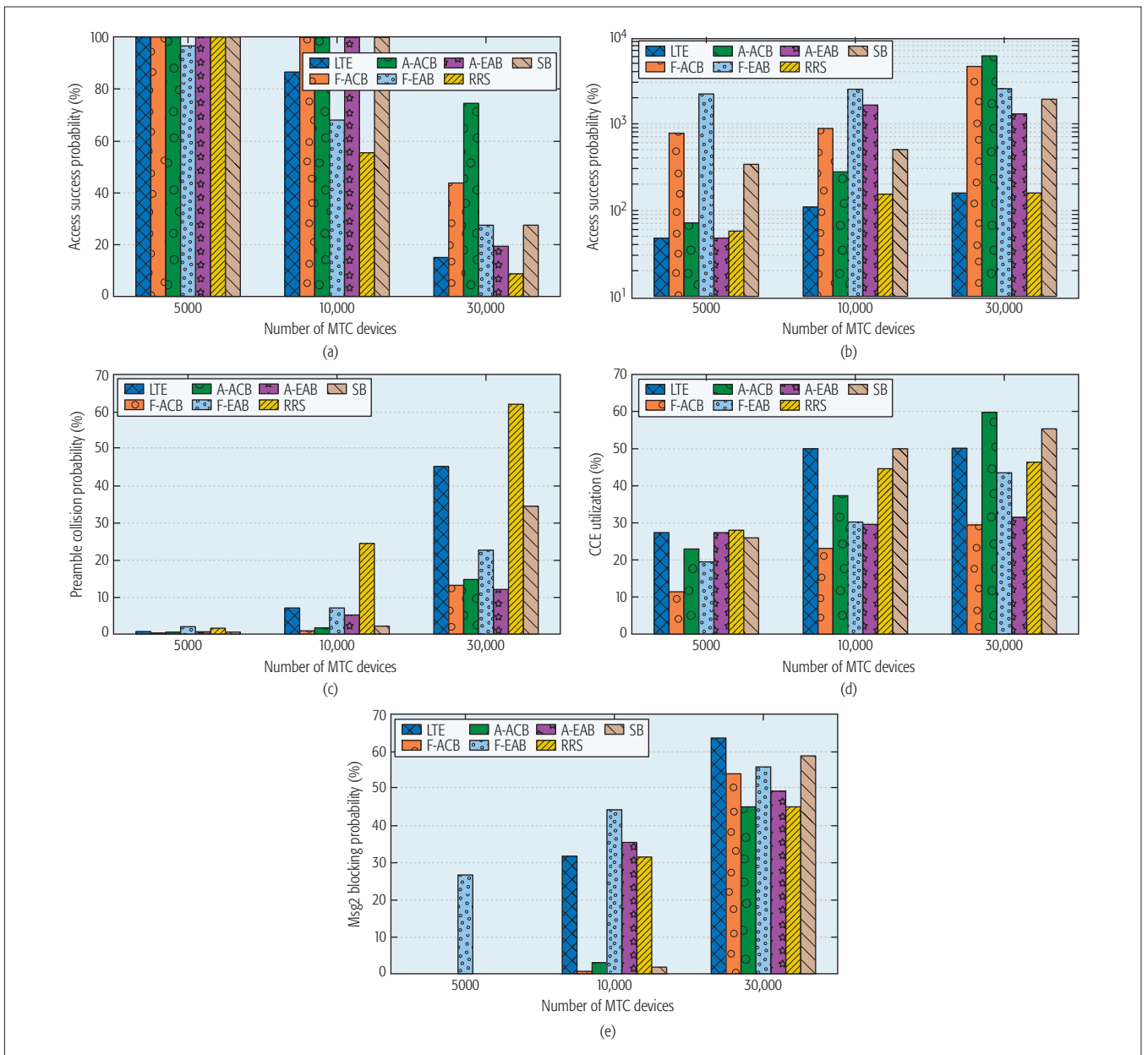


Figure 2. Performance of the 3GPP RAN overload control schemes vs. the number of MTC devices: a) access success probability; b) average access delay; c) preamble collision probability; d) CCE utilization; e) msg2 blocking probability.

challenge is finding a way to differentiate access on the basis of class. The state-of-the-art methods differentiate classes by means of preamble sequence reservation (e.g., the RRS scheme and the two methods proposed in [9]) or configuration of random access parameters (e.g., the SB scheme and the ACB mechanism in [12]), but these methods are not scalable and affect performance. An interesting option is to prioritize preamble transmissions by means of their transmit power level [13]. Another option that could be combined with various existing schemes would be the use of the QoS class identifier (QCI) available in LTE technology rather than the device type to provide greater flexibility to the random access procedure [14].

QoS-AWARE PDCCH RESOURCE ALLOCATION

A QoS-aware PDCCH scheduler can also improve performance during random access. QoS awareness in the allocation of control

resources can further improve the performance of a network during periods of access attempt by a massive number of users [15]. In fact, the PDCCH scheduling algorithm can have great impact on the network performance in MTC/HTC coexisting scenarios [15]. Moreover, 3GPP does not standardize any PDCCH scheduling algorithm, but rather leaves this option to the vendor to implement its own solutions. Thus, PDCCH schedulers can make a real difference in the IoT market. PDCCH schedulers typically give high priority to msg2 and msg4 messages regardless of the QoS required by a device with control resources shared by downlink assignments, uplink grants, and msg2 and msg4 messages. Thus, PDCCH policies taking QoS requirements of all control messages into consideration can improve network performance and maximize resource utilization.

RANDOM-ACCESS-AWARE PACKET SCHEDULING

With large delays in network access, the performance of delay-sensitive IoT applications is degraded. The packets generated by delay-sensitive applications do not receive adequate service differentiation. Even though various M2M schedulers reserve certain physical resource blocks (PRBs) for MTC devices and implement some sort of prioritization for them, existing schedulers do not take into consideration the time consumed for access of the channel. Typically, LTE schedulers estimate the delay of device packets on the basis of arrival time of the request at the base station, thus ignoring delays in random access in the production of schedules. However, this can lead to less urgent packets receiving grants unless random access awareness is considered.

CONCLUDING REMARKS

The RAN became the bottleneck of an LTE system when a very large number of MTC devices transmit within a short time interval. In this article, the performance of the LTE random access procedure for IoT connectivity has been analyzed. The impact of LTE enhancements on the random access procedure for MTC is highlighted. RAN overload control schemes standardized by 3GPP and novel approaches for supporting massive access to IoT devices over LTE networks have been reviewed, and the performance of those schemes standardized by 3GPP under realistic assumption in both the PRACH and control resource allocation are assessed. Extensive simulation results indicate that the RAN overload problem has been underestimated due to use of unrealistic assumptions in previous work. Based on these observations, directions for future research to ameliorate the RAN overload have been presented.

ACKNOWLEDGMENTS

This work was supported in part by the CNPq Brazilian research agency and Motorola Mobility.

REFERENCES

- [1] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 4th qtr. 2015, pp. 2347–76.
- [2] S. Andreev *et al.*, "Understanding the IoT Connectivity Landscape: A Contemporary M2M Radio Technology Roadmap," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2015, pp. 32–40.
- [3] A. Laya *et al.*, "Goodbye, ALOHA!," *IEEE Access*, vol. 4, 2016, pp. 2029–44.
- [4] 3GPP, "Technical Specification Group Radio Access Network; Study on RAN Improvements for Machine-type Communications," TR 37.868, Sept. 2011.
- [5] S. Ye, S. H. Wong, and C. Worrall, "Enhanced Physical Downlink Control Channel in LTE Advanced Release 11," *IEEE Commun. Mag.*, vol. 51, no. 2, Feb. 2013, pp. 82–89.
- [6] 3GPP, "Technical Specification Group GSM/Edge Radio Access Network; Cellular System Support for Ultra-Low Complexity and Low Throughput Internet of Things (CIoT)," TR 45.820, Nov. 2015.
- [7] T. Tirronen *et al.*, "Telecommunications Apparatus and Method Relating to a Random Access Procedure," Dec. 11, 2014, wO Patent App. PCT/SE2013/050,647; <http://www.google.com/patents/WO2014196908A1?cl=en>.
- [8] M. Condoluci *et al.*, "Toward 5G Densets: Architectural Advances for Effective Machine-Type Communications Over Femtocells," *IEEE Commun. Mag.*, vol. 53, no. 1, Jan. 2015, pp. 134–41.
- [9] M. Condoluci *et al.*, "Enhanced Radio Access and Data Transmission Procedures Facilitating Industry-Compliant Machine-Type Communications over LTE-Based 5G Networks," *IEEE Wireless Commun.*, vol. 23, no. 1, Feb. 2016, pp. 56–63.
- [10] 3GPP, "LTE; Feasibility Study for Further Advancements for E-UTRA," TS 36.912, Jan. 2016.
- [11] O. Arouk, A. Ksentini, and T. Taleb, "Group Paging-Based Energy Saving for Massive MTC Accesses in LTE and Beyond Networks," *IEEE JSAC*, vol. 34, no. 5, May 2016, pp. 1086–1102.
- [12] J. S. Vardakas *et al.*, "Performance Analysis of M2M Communication Networks for QoS-Differentiated Smart Grid Applications," *2015 IEEE GLOBECOM Wksp.*, Dec. 2015, pp. 1–6.
- [13] T. Kim, K. S. Ko, and D. K. Sung, "Prioritized Random Access for Machine-to-Machine Communications in OFDMA Based Systems," *IEEE ICC 2015*, June 2015, pp. 2967–72.
- [14] T. P. C. de Andrade, C. A. Astudillo, and N. L. S. d. Fonseca, "Random Access Mechanism for RAN Overload Control in LTE/LTE-A Networks," *IEEE ICC 2015*, June 2015, pp. 5979–84.
- [15] T. P. C. de Andrade, C. A. Astudillo, and N. L. S. da Fonseca, "Allocation of Control Resources for Machine-to-Machine and Human-to-Human Communications over LTE/LTE-A Networks," *IEEE Internet of Things J.*, vol. 3, no. 3, June 2016, pp. 366–77.

BIOGRAPHIES

TIAGO P. C. DE ANDRADE received his MSc. and BSc. degrees in computer science from the State University of Campinas (UNICAMP), Brazil, in 2013 and 2009, respectively. Currently, he is a Ph.D. student in computer science at the Institute of Computing, UNICAMP. His current research interests are in machine-to-machine communications, device-to-device communication, quality of service, and energy efficiency mechanisms for 4G/5G cellular networks.

CARLOS A. ASTUDILLO received his B.Sc. degree in electronics and telecommunications engineering from the University of Cauca (UNICAUCA), Popayán, Colombia, in 2009 and his M.Sc. degree in computer science from UNICAMP in 2015, and is currently working toward his Ph.D. degree at the Institute of Computing, UNICAMP. In 2010, he was a Young Researcher with the New Technologies in Telecommunications R&D Group (GNNT), UNICAUCA, supported by the Colombian Administrative Department of Science, Technology and Innovation. His current research interests include quality of service and energy-efficient mechanisms in machine-to-machine communications and mobile backhauling for 4G/5G cellular networks.

LUIZ R. SEKIJIMA is an undergraduate student in computer engineering at the Institute of Computing, UNICAMP. His current research interest is in energy-efficient mechanisms for 4G cellular networks and the Internet of Things.

NELSON L. S. DA FONSECA received his Ph.D. degree from the University of Southern California in 1994. He is a full professor at Institute of Computing, UNICAMP. He is the IEEE ComSoc Vice-President of Publications. He has served as Vice-President of Member Relations, IEEE ComSoc Director of Conference Development, Director of Latin America Region, and Director of Online Services. He is past Editor-in-Chief of *IEEE Communications Surveys & Tutorials*. He is a Senior Editor of *IEEE Communications Magazine*.

An interesting option is to prioritize preamble transmissions by means of their transmit power level. Another option that could be combined with various existing schemes would be the use of the QoS class identifier available in LTE technology rather than the device type to provide greater flexibility to the random access procedure.

Wrong Siren! A Location Spoofing Attack on Indoor Positioning Systems: The Starbucks Case Study

Junsung Cho, Jaegwan Yu, Sanghak Oh, Jungwoo Ryoo, JaeSeung Song, and Hyoungshick Kim

Thanks to indoor proximity technologies, it is possible to introduce location-based smart services to customers, for example, transmitting identifiable signals that represent the locations of stores. The authors investigate a potential security risk involved in such technologies: physical signals used as identifiers can be captured and forged easily with today's widely available IoT software for implementing location spoofing attacks.

ABSTRACT

The Internet of Things interconnects a mass of billions of devices, from smartphones to cars, to provide convenient services to people. This gives immediate access to various data about the objects and the environmental context — leading to smart services and increased efficiency. A number of retail stores have started to adopt IoT enabled services to attract customers. In particular, thanks to indoor proximity technologies, it is possible to introduce location-based smart services to customers, for example, transmitting identifiable signals that represent the locations of stores. In this article, we investigate a potential security risk involved in such technologies: physical signals used as identifiers can be captured and forged easily with today's widely available IoT software for implementing location spoofing attacks. We highlight this security risk by providing a case study: an in-depth security analysis of the recently launched Starbucks service called *Siren Order*.

INTRODUCTION

Tracking the physical locations of objects (e.g., a user's smartphone) could be applied to the Internet of Things (IoT) to make them more convenient and attractive to users. There are many practical applications utilizing the geographical locations of things; some applications allow customers to locate various points of interests (POIs) including retail stores, tourist attractions, public transportation stations, and so on; other applications focus on marketing and help vendors push advertisements to potential clients when they are within a specific range of a geographic location.

For example, in order to help their customers avoid queues, Starbucks Korea recently introduced a mobile pre-ordering and payment service called *Siren Order*. This service allows customers to remotely place their orders and pay in advance for those orders using their smartphones without contacting a cashier at a Starbucks store. For this service, a customer's Starbucks app needs to identify the particular Starbucks store where the customer wants to pick up the order. Unfortunately, GPS does not often work well for this scenario when the customer is already inside a

building (i.e., the Starbucks store). Therefore, an indoor positioning system can alternatively be used for this kind of pre-ordering/payment service.

A large number of available sensors built into a thing (e.g., smartphone) — RF technology such as Wi-Fi, Bluetooth, and RFID, ultrasound, GPS, infrared, and magnetic fields — can be used for tracking people and objects within a geographical space [1]. For instance, IndoorAtlas (<http://www.indooratlas.com>, accessed 10 October 2016) uses magnetic technology, Wi-Fi, and Bluetooth to provide an indoor positioning service. Skyhook (<http://www.skyhookwireless.com>, accessed 10 October 2016) uses GPS and Wi-Fi to deploy geofences. Recently, Broadcom (<http://www.broadcom.com>, accessed 10 October 2016) developed an indoor positioning technology using fifth generation (5G) Wi-Fi (802.11ac).

Despite the benefits of indoor positioning systems for both customers and retailers, this technology may pose serious security and privacy threats. Several studies [2, 3] demonstrated that indoor positioning systems might be vulnerable to location spoofing attacks at the physical layer. Tippenhauer *et al.* [4] particularly introduced several kinds of attacks targeted at WLAN-based positioning systems through the security analysis of a WLAN-based positioning system such as Skyhook. They showed that Skyhook is vulnerable to location spoofing attacks by jamming and replaying localization signals to deceive WLAN clients into believing that they are at a position which is different from their actual physical position, and suggested some mitigation techniques (e.g., using the unique characteristics of access points).

In this article, we demonstrate that a different type of indoor positioning system using high-frequency audio signals can also be vulnerable to similar location spoofing attacks, through a deep analysis of the *Siren Order* service in Starbucks stores. We found that an attacker can easily record the unique audio signal used for identifying a Starbucks store, and then broadcast that signal in another store to deceive victims into placing their orders at the place where the attacker is located. Therefore, the item being ordered can be intercepted by an attacker. Such attacks might, in turn, negatively influence customers'

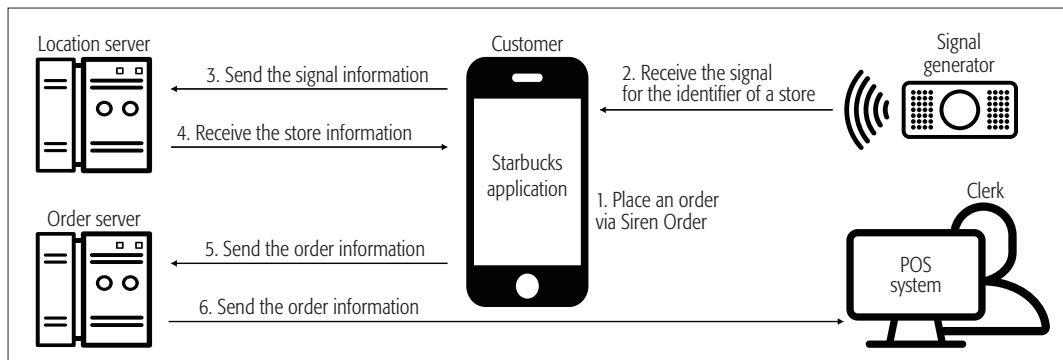


Figure 1. Overview of the process of Siren Order.

attitude and behavior toward indoor positioning systems and may seriously damage the reputation of the company using the system. We demonstrated the feasibility of a successful attack exploiting the real-world service called Siren Order. This implies that many real-world indoor positioning systems might be badly designed without considering security threats at the physical layer. To improve the status quo, we suggest practical ways to address such vulnerabilities.

The remainder of this article presents our in-depth security analysis and discusses Siren Order. We first explain how Siren Order works in detail, and then discuss the feasibility of a location spoofing attack against that service.

WHAT IS SIREN ORDER?

Starbucks Korea launched a new mobile pre-ordering service, called Siren Order, with the Starbucks mobile app, which has been made available for both iOS and Android platforms. The goal of this service is to allow customers to order in advance, saving them waiting time before picking up their order at a store location. Unlike Mobile Order & Pay, which was launched in the United States, using smartphones' GPS functionality to identify the Starbucks store nearest to a customer's location, an indoor positioning system is used to implement the Siren Order service. Even when a customer inside a Starbucks store tries to place an order through the Starbucks app, the Siren Order service (i.e., the Starbucks mobile app) can identify in which Starbucks store the customer placed the order.

For the Siren Order service, high-frequency audio signals that are mostly inaudible to human ears have been used. This technology has some benefits compared to conventional RF-based indoor positioning systems. In general, audio signals are easily absorbed into walls. That is, user locations can be determined at room-level precision with high accuracy because those signals cannot pass through walls or windows. This is very useful to precisely identify in which store the customer is actually located.

Figure 1 shows the overall process of Siren Order. The Siren Order system consists of five components: a customer's Starbucks app, location server, order server, point-of-sale (POS) system, and signal generator. A typical use of this system would be as follows:

1. A customer places an order via the Starbucks app and pays for the selected item.



Figure 2. Signal generator.

2. The app turns on the microphone in the customer's smartphone and then records the audio signals, which come from the signal generator installed in a Starbucks store (see an example in Fig. 2).
3. When the recording ends, the app analyzes the captured audio signal and submits a query with the signal data to the location server.
4. After receiving that query, the location server finds the Starbucks store matched with the signal data, and sends the Starbucks store information to the Starbucks app.
5. After receiving the query response, the Starbucks app sends the order information to the order server.
6. Finally, this order information is processed at the order server and relayed to the POS system at the Starbucks store for placing the order to the cashier at the store.

We collected audio signals from four different Starbucks stores and found that the audio signals used in Siren Order typically range from 18 to 20 kHz, which humans cannot hear. The collected audio signals have uniquely different periodic patterns, although all patterns are commonly repeated every 1.25 s (i.e., five time units). Figure 3 shows one of the audio signals recorded in a Starbucks store. As shown in Fig. 3, one period of the signal is composed of two parts — start flag (the first time unit) and store ID (the remaining time units).

In general, audio signals are easily absorbed into walls. That is, user locations can be determined with room-level precision with high accuracy because those signals cannot pass through walls or windows. This is very useful to precisely identify which store the customer is actually located at.

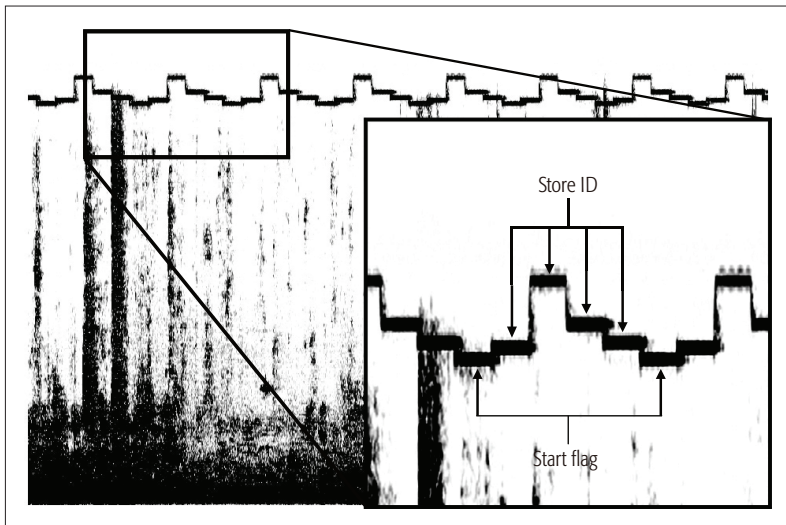


Figure 3. A recorded audio signal in a Starbucks store.

IMPLEMENTATION OF A LOCATION SPOOFING ATTACK

We describe our implementation of a location spoofing attack against *Siren Order*. As mentioned earlier, a signal generator at a Starbucks store continuously emits a unique audio signal to represent the store's identifier. The goal of our attack is to deceive a victim's Starbucks app at store S_1 into believing that the app is at store S_2 in which an attacker is located. When an order is placed at S_2 instead of S_1 , the attacker can illegally intercept the item that the victim ordered in store S_1 . Therefore, such attack attempts will inevitably harm the reputation of Starbucks since the attacker can control customers' orders freely and/or disrupt the whole service.

Figure 4 illustrates an overview of our attack. In our attack, there are two attackers: attacker A_1 in store S_1 and attacker A_2 in store S_2 . A_2 has recorded the signal transmitted from S_2 , and delivers it to A_1 via any communication channel. After receiving the signal from A_2 , A_1 broadcasts it again (i.e., by playing the recorded signal through an audio player) to its neighbors (i.e., potential victims) in S_1 . To succeed in this attack, a victim's device must receive A_1 's signal instead of the authentic signal transmitted from S_1 's signal generator. This can be achieved simply by jamming at the physical layer (e.g., loudly playing the signal to represent S_2 's identifier). If A_1 's signal is more powerful than the signal from the transmitter at S_1 , the attacker can interfere and overpower the signal from S_1 . As a result, a victim's Starbucks app in S_1 receives the attacker's signal representing S_2 's identifier and unknowingly transmits that signal to the location server with which the Starbucks app communicates. Thereafter, the location server finds the store information about S_2 in response to the received signal and replies to the victim's Starbucks app; the Starbucks app blindly believes that it is in S_2 . Therefore, if the victim places an order through her Starbucks app, this order is processed at S_2 in spite of the user's original intent (to place the order at S_1) in which attacker A_2 is located. This is a typical scenario for our location spoofing attack.

As a proof of concept, we performed a location spoofing attack on real Starbucks stores. In our implementation, we used QuickTime Player (<https://support.apple.com/kb/PH22585>, accessed 10 October 2016) for recording signals and Adobe Audition CC (<http://www.adobe.com/products/audition.html>, accessed 10 October 2016) for filtering out unnecessary signals, which are widely affordable and popular.

In our experiment, we first recorded a signal in Starbucks store A and then applied a band-pass filter (in Adobe Audition CC) between 18 and 20 kHz to the recorded signal data to isolate the high-frequency part, which is a typical range used for *Siren Order*. In another Starbucks store, B, two participants were recruited to play the roles of "victim" and "attacker," respectively. The attacker simply amplified the audio signal (previously recorded at store A) and broadcasted it to overpower the signal data emitted from store B's generator. When the victim was located around the attacker (e.g., within about 3 m), the victim's Starbucks app believed that the victim was in store B. Finally, we confirmed that location spoofing attacks can be successfully performed in real-world settings when the victim tried to place an order through his Starbucks app; his order was inappropriately placed at store B, although he was in store A (our demonstration video clip is available at <https://youtu.be/oN9kB169lvE>, accessed 10 October 2016).

The main goal of this experiment is not to damage Starbucks' business or reputation. We conducted this experiment to show the feasibility of location spoofing attacks on new indoor positioning systems through a case study. We already reported the discovered problem to the Starbucks developers and suggested a fix based on our observations.

COUNTERMEASURES

How can we fix this problem in indoor positioning systems? In this section, we discuss some possible mitigation techniques against such attacks.

FRESHNESS OF AUDIO SIGNALS

Location spoofing is basically a kind of *replay attack*. Therefore, we need to verify the freshness of messages to prevent location spoofing attacks. A number of distance-bounding protocols have already been proposed for this purpose. Brands and Chaum [5] proposed the first distance-bounding protocol against a type of replay attack called Mafia fraud [6]. Hancke and Kuhn [7] also proposed a distance-bounding protocol against a terrorist fraud [6], which was a modified version of Mafia fraud. Furthermore, Reid *et al.* [8] proposed an advanced distance-bounding protocol based on a symmetric key cryptosystem, taking advantage of the security strengths of Brands' and Chaum's protocol and the efficiency of Hancke's and Kuhn's protocol. However, those distance-bounding protocols are not suitable for the indoor positioning system in *Siren Order* where one-way communication from a signal generator to a Starbucks app is only allowed because in the aforementioned protocols, challenge-response message pairs should be repeatedly exchanged to obtain

meaningful statistical information about the physical distance between the sender and the recipient. To overcome this limitation in our application, we present a distance-bounding protocol based on a synchronized timestamp.

Our main idea is to include a timestamp in the signals used for an indoor positioning system to limit the lifetime of recorded signals. We briefly describe this with the following notation. In a protocol that is used by S_1 and S_2 , " $S_1 \rightarrow S_2: x$ " implies that S_1 sends message x to S_2 . The symbols G , a , and S represent the signal generator, Starbucks app, and Starbucks server, respectively. E is a symmetric encryption algorithm (e.g., AES). $k_{S_1S_2}$ is a secret symmetric session key to be shared by two parties S_1 and S_2 . For data input x , $E_k(x)$ denotes the data value resulting from E 's encryption operation on x using the encryption key k . t_P is a timestamp generated by a party P . id_G is a signal to identify a signal generator G installed at a Starbucks store. Notation $||$ denotes the concatenation operation. We assume that an encryption key k_{GS} is securely shared between G and S , and G and a have a synchronized time clock that can be maintained via coordinated universal time (UTC). A reliable connection to the Internet is needed for G and a to use a clock synchronization mechanism on the Internet. This assumption could be acceptable because it is expected that most sensor devices such as G would be connected to the Internet in the near future.

Unlike the existing system, in our proposed protocol, G generates its timestamp t_G and broadcasts the encrypted signal $E_{k_{GS}}(id_G || t_G)$ instead of the plaintext signal id_G in its Starbucks store as follows:

$$G \rightarrow A: E_{k_{GS}}(id_G || t_G)$$

After receiving $E_{k_{GS}}(id_G || t_G)$ from G , a immediately generates its own timestamp t_A and then relays $E_{k_{GS}}(id_G || t_G)$ with the generated t_A to S . We assume that the communication channel between G and S is securely protected. This assumption is practical and reasonable because G and S communicate via the Internet against an attacker who can eavesdrop any wireless signals in the Starbucks store.

$$A \rightarrow S: E_{k_{GS}}(id_G || t_G) || t_A$$

After receiving $E_{k_{GS}}(id_G || t_G) || t_A$ from a , S decrypts the encrypted part $E_{k_{GS}}(id_G || t_G)$ only with the shared key k_{GS} and verifies its freshness. For the verification, S calculates the time difference between t_G and t_A . If the difference is less than a pre-determined threshold δ , the received query message is accepted, and the corresponding Starbucks store information is sent to a ; otherwise, this query is rejected. If the Starbucks customer relays an outdated message $E_{k_{GS}}(id_G || t_G)$ (which has been replayed by a location spoofing attack) to S , the time difference between t_G and t_A would be quite large.

Suffice it to say that it is important to choose a proper δ to make location spoofing attacks difficult while guaranteeing a low false alarm rate for legitimate customers. We claim that a consider-

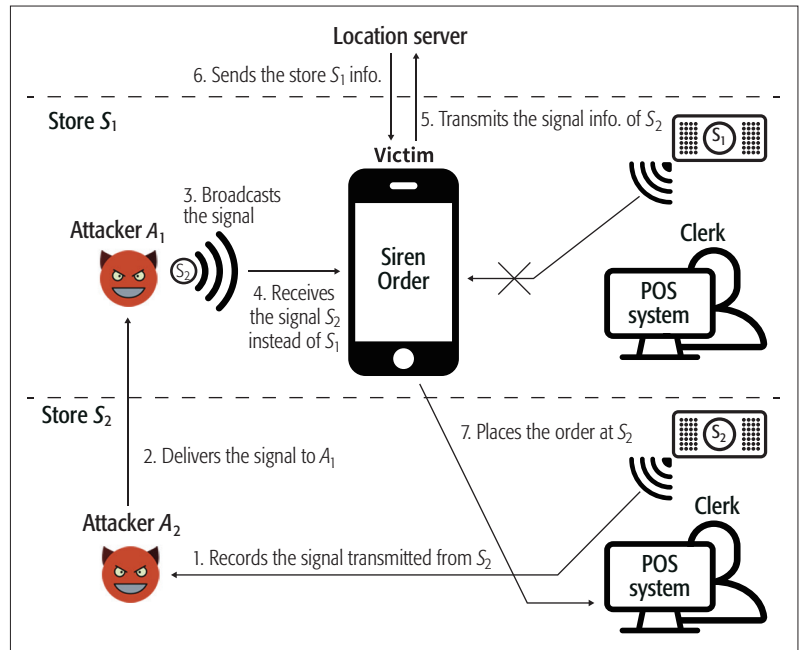


Figure 4. Overview of the location spoofing attack on Siren Order.

able amount of processing time will be required to perform a location spoofing attack in this scenario. If an attacker tries a location spoofing attack, the attacker's timestamp can be approximately calculated as follows:

In this equation, t_{sound_1} is the amount of time taken from a signal generator to an attacker's recording device; t_{record} is the amount of time taken for recording the audio signal in a digital format; $t_{internet}$ is the amount of time taken to deliver a recorded signal from an attacker A_2 in store S_2 to another attacker A_1 in store S_1 ; and t_{sound_2} is the amount of time from an attacker's audio player to a victim's Starbucks app. Note that t_A can also be represented as $t_G + t_{sound_1}$, which might be significantly less than t_{attack} . To prevent location spoofing attacks, we need to find a proper threshold δ that satisfies the following equation. To simplify the equation, we assume that t_{sound_1} is equal to t_{sound_2} as follows:

$$t_{sound} < \delta < 2 \cdot t_{sound} + t_{record} + t_{internet}$$

Now suppose that the distance from a signal generator to a customer's smartphone is 10 m. In this case, if we assume that the speed of sound is 343.2 m/s, t_{sound} can approximately be calculated to be roughly 29.1 ms. To show that there is a practically reasonable δ for the proposed mitigation technique in a real-world situation (i.e., $2 \cdot t_{sound} + t_{record} + t_{internet} \gg 29.1$ ms), we conducted a simple experiment with two laptops with a non-congested 100 Mb/s Wi-Fi connection to a LAN connected to the Internet via a Gigabit-speed link. The first and second laptops were used to simulate attackers A_1 and A_2 , respectively, in Fig. 4. We used an audio streaming application named Nicecast to efficiently deliver the recorded audio signal from the first laptop to the second laptop. We recorded the input sound stream and receiver's output sound stream synchronously. A short audio signal was generated and delivered to

In order to deploy our mitigation methods in such existing IoT platforms, a platform has to support at least two features: location and security. As these widely used IoT platforms support location and security functions, our mitigation methods can easily be integrated into existing IoT platforms.

simulate a location spoofing attack. After receiving the sound signal, the second laptop produced the same sound signal from its speaker. We measured the total processing time for those steps to approximately measure $2 \cdot t_{\text{sound}} + t_{\text{record}} + t_{\text{internet}}$. We repeated this 20 times to obtain statistically meaningful results. The mean time spent on each simulation was 2.1 s, ranging from 1.9 s to 2.9 s, which implies that there is a significant gap between t_{sound} (29.1 ms) and $2 \cdot t_{\text{sound}} + t_{\text{record}} + t_{\text{internet}}$ (2.1 s). Therefore, in practice, we can find a reasonable δ to mitigate location spoofing attacks.

However, efficient and accurate time synchronization is not easy in the real world. For example, Network Time Protocol (NTP) [9] provides limited accuracy because the packet propagation delay varies depending on network conditions. Fortunately, our experimental results (2.1 s vs. 29.1 ms) show that the proposed method does not require a highly accurate time synchronization model. An inaccuracy of a few milliseconds, which could be incurred by NTP, seems well tolerated in the proposed solution.

TRANSACTION AUTHENTICATION

The main problem, or the reason for this attack, is the absence of a verification process when an order is picked up. We can simply fix this problem by introducing an additional procedure for transaction authentication. That is, we require that a customer provides a proof of transaction before picking up an order. It is a secure way to authenticate whether someone who is trying to pick up the order is the legitimate customer of the order being placed.

For example, when a customer places an order via **Siren Order**, the customer's Starbucks app can generate a 4-digit random number as a one-time password and send it to a clerk through the **Siren Order** service. This number is then required to pick up the order for the purpose of verifying the customer who placed the order. This technique helps protect the customer's order against an attacker who wants to steal the ordered product. It is very difficult for an attacker to obtain the randomly generated number, although capturing any signals in the air is possible. Without modifying the existing system, this verification procedure might be added with a software patch to the Starbucks app. However, it is likely to degrade the usability of the **Siren Order** service as customers and clerks should check the validity of the generated random number for each order. Therefore, we need to conduct a user study to investigate the usability of this newly proposed procedure.

CONCLUSION

In recent years, indoor positioning systems are gaining popularity in the market to provide the location information of people and devices in a building. Several different types of technologies have been introduced, but their security issues have not been explored thoroughly.

In this article, we point out a security risk called *location spoofing* associated with indoor positioning systems by providing a proof-of-concept case study that implements a well designed location spoofing attack against the Starbucks pre-order

service called **Siren Order**, which can cause severe disruption in the service. To mitigate such attacks, we discuss two possible mitigation strategies.

There are many IoT platforms, for example, Mobius based on oneM2M global IoT standards [10] and IoTivity open source platform based on OCF (<https://openconnectivity.org>, accessed 10 October 2016). In order to deploy our mitigation methods into such existing IoT platforms, a platform has to support at least two features: location and security. As these widely used IoT platforms support location and security functions, our mitigation methods can easily be integrated into existing IoT platforms.

As part of our future work, we plan to implement the proposed mitigation techniques and further investigate the performance and usability of those solutions by conducting user studies.

ACKNOWLEDGMENTS

This work was supported in part by the NRF Korea (No. 2014R1A1A1003707), the ITRC (IITP-2016-R0992-16-1006), and ICT R&D program (No. B0717-16-0116, No. B0184-15-1001). The authors would like to thank all the anonymous reviewers for their valuable feedback.

REFERENCES

- [1] Y. Gu, A. Lo, and I. Niemegeers, "A Survey of Indoor Positioning Systems for Wireless Personal Networks," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 1, 2009, pp. 13–32.
- [2] L. Lazos, R. Poovendran, and S. Capkun, "ROPE: Robust Position Estimation in Wireless Sensor Networks," *Proc. 4th Int'l. Symp. Info. Processing in Sensor Networks*, 2005.
- [3] S. Capkun and J. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," *Proc. 24th Annual Conf. IEEE Comp. Commun. Societies*, 2005.
- [4] N. O. Tippenhauer et al., "Attacks on Public WLAN-Based Positioning Systems," *Proc. 7th Int'l. Conf. Mobile Systems, Applications, and Services*, 2009.
- [5] S. Brands and D. Chaum, "Distance-Bounding Protocols," *Proc. Wksp. Theory and Application of Cryptographic Techniques*, 1993.
- [6] Y. Desmedt, "Major Security Problems with the 'Unforgeable' (feige)-fiat-shamir proofs of Identity and How to Overcome Them," *SecuriCom*, 1988.
- [7] G. P. Hancke and M. G. Kuhn, "An RFID Distance Bounding Protocol," *Proc. 1st Int'l. Conf. Security and Privacy for Emerging Areas in Commun. Networks*, 2005.
- [8] J. Reid et al., "Detecting Relay Attacks with Timing-Based Protocols," *Proc. 2nd ACM Symp. Info., Comp. and Commun. Security*, 2007.
- [9] D. Mills et al., "RFC 5905: Network Time Protocol version 4: Protocol and Algorithms Specification," IETF tech. rep., 2010.
- [10] J. Swetina et al., "Toward a Standardized Common M2M Service Layer Platform: Introduction to oneM2M," *IEEE Wireless Commun.*, vol. 21, no. 3, June 2014, pp. 20–26.

BIOGRAPHIES

JUNSGUNG CHO (js.cho@skku.edu) received his B.S. degree from the Department of Computer Engineering, Korea University of Technology and Education, in 2014. He is currently a graduate student with the Department of Computer Science and Engineering, Sungkyunkwan University, Korea, supervised by Hyoungshick Kim. His current research interests include usable security, mobile security, IoT security, and security engineering.

JAEGWAN YU (jaegwan@skku.edu) received his B.S. degree from the Department of Electrical and Information Engineering, Korea University, in 2015. He is currently a graduate student with the Department of Platform Software, Sungkyunkwan University, supervised by Hyoungshick Kim. His current research interests include network security, software security, and security engineering.

SANGHAK OH (osh09@skku.edu) received his B.S. degree from the Department of Software, Sungkyunkwan University, in

2015. He is currently a graduate student with the Department of Platform Software, Sungkyunkwan University, supervised by Hyoungshick Kim. His current research interests include network security, software security, and security engineering.

JUNGWOO RYOO [M] (jryoo@psu.edu) is a professor of information sciences and technology at Pennsylvania State University. His research interests include information security and assurance, software engineering, and computer networking. He received a Ph.D. in computer science from the University of Kansas.

JAESEUNG SONG (jssong@sejong.ac.kr) is an assistant professor in the Computer and Information Security Department at Sejong University. He holds the position of oneM2M Test Working Group Chair. Prior to his current position, he worked for NEC

Europe Ltd. and LG Electronics in various positions. He received a Ph.D. from Imperial College London in the Department of Computing, United Kingdom. He holds B.S. and M.S. degrees in computer science from Sogang University. He is a member of IEEE.

HYOUNGSHICK KIM (hyoung@skku.edu) received his B.S. degree from the Department of Information Engineering, Sungkyunkwan University, his M.S. degree from the Department of Computer Science, Korea Advanced Institute of Science and Technology, Daejeon, and his Ph.D. degree from the Computer Laboratory, University of Cambridge, United Kingdom, in 1999, 2001, and 2012, respectively. He is currently an assistant professor with the Department of Software, Sungkyunkwan University. His current research interests include usable security and security engineering.

First Mile Challenges for Large-Scale IoT

Ahmed Bader, Hesham ElSawy, Mohammad Gharbieh, Mohamed-Slim Alouini, Abdulkareem Adinoyi, and Furaih Alshaalan

The authors shed light on the random access dilemma and present a case study based on experimental data as well as system-level simulations. Accordingly, a case is built for the latent need to revisit random access procedures. A call for action is motivated by listing a few potential remedies and recommendations.

ABSTRACT

The Internet of Things is large-scale by nature. This is not only manifested by the large number of connected devices, but also by the sheer scale of spatial traffic intensity that must be accommodated, primarily in the uplink direction. To that end, cellular networks are indeed a strong first mile candidate to accommodate the data tsunami to be generated by the IoT. However, IoT devices are required in the cellular paradigm to undergo random access procedures as a precursor to resource allocation. Such procedures impose a major bottleneck that hinders cellular networks' ability to support large-scale IoT. In this article, we shed light on the random access dilemma and present a case study based on experimental data as well as system-level simulations. Accordingly, a case is built for the latent need to revisit random access procedures. A call for action is motivated by listing a few potential remedies and recommendations.

INTRODUCTION

A plethora of application scenarios are rapidly emerging within the context of the Internet of Things (IoT) in possibly every industrial and market vertical [1]. As such, it is large in scale by design [2]. A recent report from ABI Research predicts that 75 percent of the growth in wireless connections between today and the end of the decade will come from non-hub devices, that is, sensor nodes and accessories [3]. Accordingly, the wireless infrastructure should be able to accommodate unprecedented traffic levels that are essentially a blend of human-type and machine-type communications. While the common perception of IoT dwells in the low-bandwidth delay-tolerant quadrant, there is growing evidence of IoT application scenarios that thrive in the totally opposite quadrant, that is, high-bandwidth delay-intolerant [4, 5]. This primarily appears in applications demanding real-time transmission of video and rich multimedia streams. Consequently, the large-scale nature of the IoT stems not only from the massive number of devices but also from the amount of the uplink (UL) traffic it is poised to generate. Hence, it is crucial to study the spatiotemporal dynamics of the IoT based on the spatial density of the IoT devices as well as the traffic requirement per device. This leads to the notion of spatial traffic intensity in the context of the IoT. This perception is further illustrated by means of shedding some light on the growing domains of IoT applications.

There are a few natural technology contenders for addressing the scalability challenges of the IoT era, including LTE, Wi-Fi, and LoRa, among others. While each may have its own potential, LTE is better positioned to handle key trade-offs pertinent to ubiquity, mobility, scalability, and latency. However, cellular networks (including LTE) are mainly designed to address massive downlink (DL) traffic demands, while the IoT is fiercely pushing the envelope on the UL interface. Articulated differently, the IoT is expected to exert tremendous pressure on LTE networks, particularly in the UL direction.

To that end, there is a long-standing challenge that has been inherited by the IoT from its machine-to-machine (M2M) predecessor, and still persists: random access (RA) procedures [6]. Particularly, devices with UL traffic need to go through an RA procedure prior to resource allocation and packet scheduling via the base stations (BSs) [sesia2009lte]. As the number of devices and traffic intensity grows, contention over scarce RA resources escalates substantially. This can be the cause of excessive access delays leading to frequent packet drops [7]. An empirical case study is presented supporting such an argument. The study highlights the detrimental effect that RA inefficiency may have on the ability to meet UL traffic demands, not limited to IoT devices but actually overall.

To accommodate large-scale IoT, refining RA procedures and addressing their limitations in LTE networks bear paramount importance. This article discusses the need to rigorously model RA procedures in LTE in light of spatial distribution of devices as well as the traffic demand per device. Within that context, researchers have already started to look into combined stochastic geometry and queueing theory models to capture such spatiotemporal dynamics [8, 9]. This combined model abstracts the IoT network to a network of spatially distributed and interacting queues, in which the interaction resides in the mutual interference between the devices. In other words, the service rate of one queue depends on the number of other active queues and their relative locations from the test queue.

The marriage between queueing theory and stochastic geometries offers insightful views that can be used when designing the radio access networks. For example, design engineers can identify combinations of temporal traffic intensity and spatial device density beyond which the network becomes unstable. Within this context, instability refers to the situation where the probability

of queue overflow is one. This occurs when the RA process invokes substantial delay such that the packet service rate becomes less than the packet arrival rate. The call for action is clear: it is essential to revisit the status quo of RA procedures. Indeed, there are straightforward remedies to circumvent shortcomings pertaining to RA procedures. Furthermore, additional potential solutions are highlighted, while also pinpointing some promising research directions.

IOT IMPLICATIONS ON LTE NETWORKS

GROWING UPLINK TRAFFIC DEMAND

There is a growing list of application scenarios that are expected to generate overwhelming upstream demand. Two examples of “uplink-centric” service categories are highlighted in this section.

The first one relates to crowds and venue management. During events, venue owners and event organizers can benefit from the IoT paradigm to hook up a massive array of IP-enabled cameras covering the crowds. These cameras can be fixed at strategic locations [10] or mounted aboard unmanned aerial vehicles (UAVs) for flexible and dynamic monitoring. Video streams are analyzed in real time in order to classify a crowd (e.g., gender, age, ethnicity) or estimate its parameters (e.g., density and flow intensity) [11]. In fact, crowded venues can be associated with many other flavors of IoT-driven applications. Some of them are UL-centric and may well fall in the high-bandwidth delay-intolerant quadrant illustrated in Fig. 1.

On a different IoT wavefront, live video streaming might be a crucial ingredient for future cyber-physical systems (CPSs). With the rocket speed advancements in UAVs, new horizons are currently being explored. For example, we can now imagine public safety personnel and emergency responders performing critical field missions while being aided by clusters of UAV agents [12]. In fact, Qualcomm and AT&T have recently announced UAV connectivity trials with the objective of better serving emerging IoT needs in logistics, search and rescue, and inspection sectors.¹

The industrial IoT (IIoT) may also entail some bandwidth-hungry applications. Conscious of safety and operational integrity, many energy production plants are installing vision-based equipment. Coupled with arrays of gas and temperature sensors, tomography cameras help energy plant operators detect anomalies in the underlying physical/chemical process and react in a timely manner. Also within the context of the IIoT, there is growing attention to machinery health management. This entails online monitoring of rotating parts (turbines, engines, fin fans) by means of characterizing the vibration in the frequency domain. Similarly, ultrasonic corrosion/erosion measurements are periodically carried out on hydrocarbon transmission pipelines to ensure their integrity. While such types of measurements can be delay-tolerant, they generate an appreciable amount of upstream traffic.

LOWER TRANSMISSION EFFICIENCY

We are already in the fifth generation (5G) era, the next evolution wave of cellular networks. 5G networks are not only envisioned to offer tangible

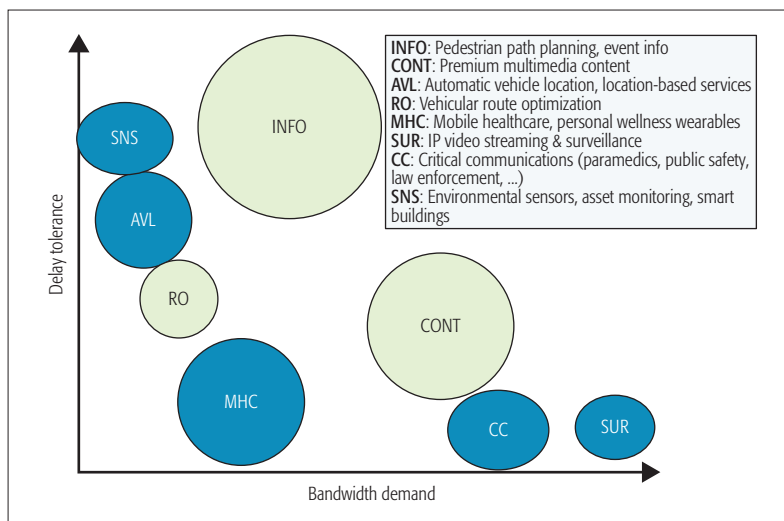


Figure 1. Examples of services that can be associated with the management of events and venues in massively crowded contexts. Lightly colored bubbles correspond to downlink-centric applications, while the dark bubbles correspond to uplink-centric ones. The size of the bubble reflects the relative number of connections typically expected.

performance improvement in terms of data rate, network capacity, energy efficiency, and latency, but also to offer support for large-scale IoT. There are indeed tangible efforts to address the growing spatial traffic intensity over LTE cellular networks. Some notable examples are massive multiple-input multiple-output (MIMO) antenna techniques, non-orthogonal multiple access, and extreme network densification. Together, these technologies promise magnitude of order UL capacity gains [13]. However, these technologies can mainly be exploited to boost the data-serving capacity but have minimal impact on improving RA performance.

The LTE standard requires the IoT devices and user equipment (UE) to undergo RA procedures twice. The first corresponds to the transition from idle (RRC_IDLE) state to connected (RRC_CONNECTED) state. A device that has been idle for some time needs to synchronize once again with a base station (BS). The second step is required to send a resource scheduling request (SR) to the BS [7]. In LTE, RA is dominantly contention-based. Therefore, it is prone to collisions when the number of UL connection requests is quite high, as in the large-scale IoT case. Accordingly, many devices do not get the opportunity to successfully complete the RA process in the first place. As such, RA may well be a bottleneck preventing full exploitation of all the available capacity to be provided by novel 5G technologies.

To validate such an argument, the UL throughput is simulated for various levels of device intensity. The exercise considers machine-type as well as human-type traffic. The goal of the simulation is to explore the effect of congestion/collisions on the RA UL radio resources as the number of UEs grows. The simulation is not built from scratch but rather takes into consideration historical user traffic profiles and user mobility trends from an active cellular network deployment in a massively crowded geographical locale. It is in essence an extrapolation of network behavior measured for low to moderate device intensities. A carrier

¹ <https://www.qualcomm.com/news/releases/2016/09/06/qualcomm-and-att-trial-drones-cellular-network-accelerate-wide-scale>

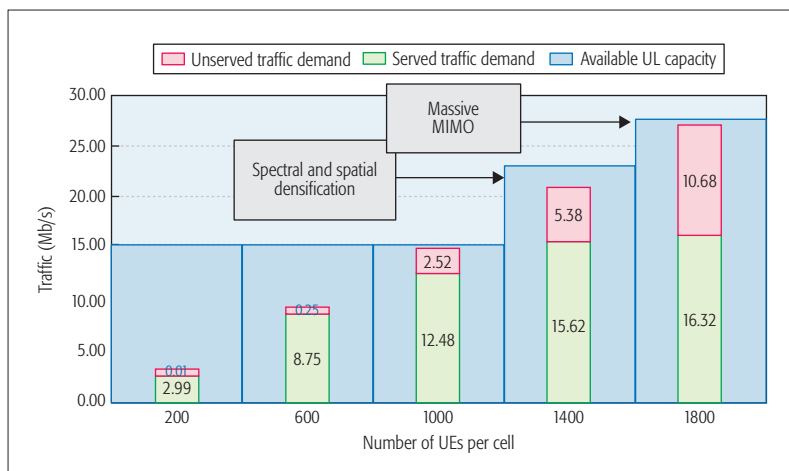


Figure 2. At low to moderate device counts, minimal to negligible levels of collisions occur on the RA radio resources. However, mobile networks are already past this phase: the number of devices in a small cell is rapidly growing beyond 1000.

bandwidth of 10 MHz is assumed throughout the exercise.

Results are depicted in Fig. 2. The achievable UL capacity is computed based on signal-to-noise-plus-interference ratio (SINR) distributions typically seen in small cells. As the number of devices grows, the available capacity needs to be boosted to accommodate the increase in traffic demand. The amount of served and unserved traffic is stacked and plotted for various device counts.

As shown in the figure, even for low to moderate device counts (200–600), there is a small percentage of unserved traffic. Articulated differently, while there is an ample remainder of unused UL capacity, part of the traffic demand is never served. Collisions *do* occur, and therefore frames are occasionally dropped by devices. The percentage of unserved traffic grows evidently with the increase in the number of devices. For instance, 16.8 percent of the traffic demand is unserved when the number of devices is 1000, while as much as 39.6 percent of traffic is dropped when the number of devices is 1800.

These results clearly underline the challenges as the IoT rollout picks up. While the IoT is a long-awaited business opportunity for operators, it may be a serious threat to the quality of service (QoS) if this issue is not rapidly tackled. Before attempting to do so, there is an obvious need first to rigorously model the RA process. In the absence of such models, any attempt to develop solutions or propositions cannot be evaluated properly. Accordingly, a combined stochastic geometry and queueing model is discussed in the next section.

RANDOM ACCESS MODELING AND PERFORMANCE EVALUATION

By far, stochastic geometry lends itself as a very powerful tool for modeling large-scale wireless networks [14]. However, traffic-agnostic spatial models are not sufficient to understand the RA behavior. Hence, combining queueing theory and stochastic geometry is advocated to give a unified overview of the spatio-temporal performance

of the network. Stochastic geometry takes care of topological aspects, while queueing theory incorporates protocol state as well as queue state awareness in the models.

COMBINED STOCHASTIC GEOMETRY AND QUEUEING MODEL

For simplicity, it can be assumed that BSs are spatially distributed according to a homogeneous Poisson point process (PPP). Similarly, the devices are spatially distributed via an independent PPP with intensity \mathcal{U} . Four standards-based RA schemes are modeled.

Baseline: This scheme defines only one protocol state in which the device persistently sends the RA request with the same power as long as there is a UL packet to transmit.

Power Ramping: This scheme defines multiple protocol states based on the transmit power used by the device. Particularly, the device increases its power in each RA attempt to increase the success probability until the maximum allowable power threshold is reached. Once successful, the device repeats the same strategy next time starting from the initial (i.e., smallest) power control threshold.

Backoff: The backoff scheme defines multiple protocol states that defer transmissions to control RA contention. Particularly, the device goes for a deterministic backoff state for N time slots followed by a probabilistic backoff state with probability $1 - q$ after each RA failure. The backoff scheme is generic. It captures deterministic backoff by setting $q = 1$, random backoff by setting $N = 0$, and generic combinations of both deterministic and random backoff states by setting $N > 1$ and $q < 1$.

Combined: The power ramping and backoff schemes can be combined together simply by ramping the transmit power whenever the device backs off after a failed attempt. It is worthwhile mentioning that the baseline scheme is a special case of the power ramping scheme (i.e., by setting $M = 1$) and also a special case of backoff scheme (i.e., by setting $N = 0$ and $q = 1$).

Each IoT device in the network is abstracted via a two-dimensional Markov model, as illustrated in Fig. 3 for the power ramping and backoff schemes. In essence, this two-dimensional Markov model captures the temporal evolution of the queue and protocol states, which can estimate the intensity of active/idle devices as well as the average number of packets per queue. Using the two-dimensional queue/protocol state model, more insights about the networks can be obtained such as:

- Intensity of active devices at each protocol state
- Transmission success probability
- Average waiting time before successful RA
- Average queue length
- Conditions for network stability

PERFORMANCE EVALUATION

The LTE standard specifies 64 Zadoff-Chu (ZC) orthogonal sequences to be used by devices in the RA process [7]. It is assumed that the IoT/user device intensity is high enough that there would be multiple active devices in each BS using the same sequence. It can be shown that the devices interfering on the same ZC sequence constitute a

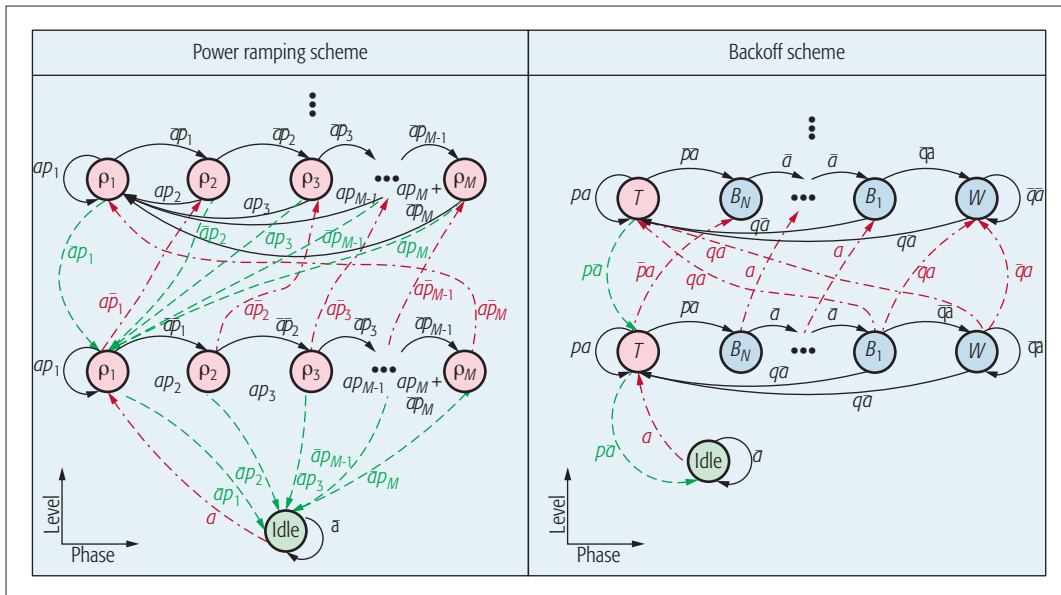


Figure 3. A schematic diagram for RA schemes is developed based on a discrete-time Markov chain (DTMC). For the power ramping scheme, p_m is the RA access success probability from device in state m , the midpoint of $p_m = 1 - p_m$, and p_m is the power control parameter. For the backoff scheme, T denotes the transmission state, B_1, B_2, \dots, B_N denote the deterministic backoff states, and W denotes the random backoff state that occurs with probability q . The level represents the number of packets in the queue, and the phase corresponds to the protocol states. Green indicates empty queue and hence idle state (not transmitting), red indicates a non-empty queue while in a transmission state, and blue indicates a non-empty queue in a backoff state. The packet arrival probability is denoted as a and its complement is denoted as $\bar{a} = 1 - a$.)

PPP with intensity proportional to the ratio of the probability of transmission to the number of available ZC sequences.

To transmit their RA requests, all of the devices use full inversion power control. That is, each device controls its transmit power such that the average signal power received at the corresponding serving BS is equal to a certain threshold. The implicit assumption here is that devices have sufficient transmit power headroom to execute the inversion power control. This assumption is justified by the sufficiently small BS footprints driven by the foreseen 5G network densification [13]. Large-scale IoT is typically expected to go in conjunction with highly dense BS deployment modes such that the average cell radius is small enough. Hence, it can be safely assumed that there would be enough headroom.

All BSs are assumed to have an open access policy, and hence, each of the devices is assumed to request Internet access from its nearest BS. A power-law path loss model and a Rayleigh fading environment are considered. All the channel gains are assumed to be independent of each other, independent of the spatial locations, and identically distributed (by virtue of the inversion power law). In this model, Rayleigh fading is considered.

While a case study with full technical details is available in [15], it is worthwhile to offer a high-level description of the analytical framework. The cornerstone is the computation of the transmission success probability, which is a function of the SINR. Using stochastic geometry, SINR, which depends on the intra-cell and inter-cell interference, is characterized in terms of the intensity of active devices and their protocol states.

It is noted that the transmission probability

for each device is not trivially equal to one since some devices may be in backoff states or even idle if they have empty buffers. This is the point where the employed two-dimensional Markov model is exploited to find the intensity of the devices operating at each protocol state. Under PPP distribution and equiprobable usage of ZC sequences, all devices have identically and independently distributed queue and protocol states. Furthermore, it is noteworthy that there is a causality problem between the Markov model solution and the stochastic geometry analysis due to the interdependence between the queue transition probabilities and the network interference. This causality problem can be solved via an iterative solution.

Based on the above, the performance of the four RA schemes can be investigated. Optimum values of N and q in the backoff and combined RA scheme are selected via an exhaustive search. The criterion for optimality is minimization of the waiting time. The BS density used in the evaluation is 50 BS/km². One of the key metrics considered for performance evaluation is network stability. For each value of device-to-BS density ratio there is a maximum frame arrival rate beyond which the network becomes unstable. This means that the frame arrival rate will be larger than the RA service rate.

Analytical and simulation results have shown that all four RA schemes – more or less – have the same stability region. As such, their performance measured in terms of waiting time or average queue length are tightly coupled during stability [15]. This is mainly due to the fact that the success probability is sufficiently high during stability. As such, most of the devices maintain

One of the key metrics considered for performance evaluation is network stability. For each value of device-to-BS density ratio, there is a maximum frame arrival rate beyond which the network becomes unstable. This means that the frame arrival rate will be larger than the RA service rate.

empty buffers and remain in idle mode. Hence, the RA resources are not congested, and there is no need to impose sophisticated techniques to regulate the RA process.

Figure 4 portrays the stability region for the combined RA scheme. The curve can be used to reinforce what should be an intuitive insight: allocating more radio resources for the RA process has a highly profound effect. For instance, changing the RA Configuration Index from 3 to 9 as per Third Generation Partnership Project (3GPP)

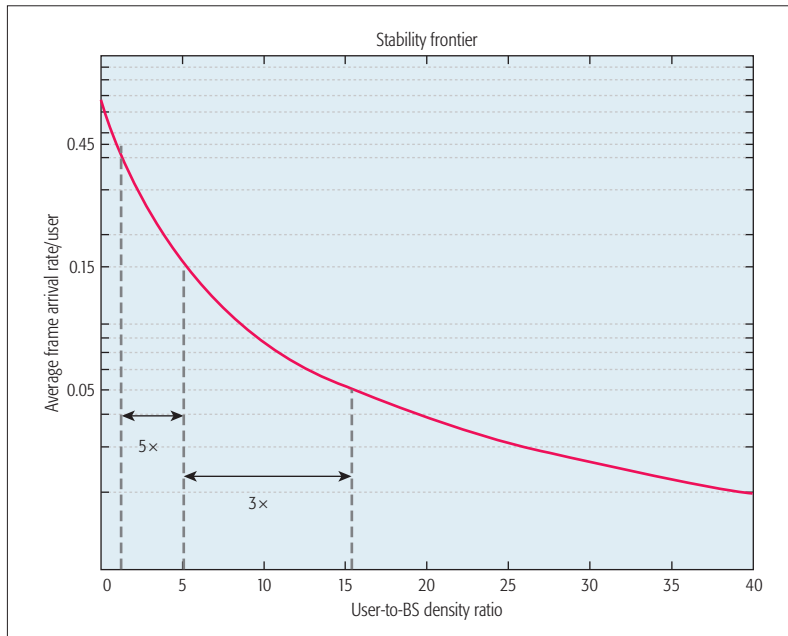


Figure 4. Stability region shown for the combined scheme, where the network is stable when operated below the curve. In this numerical example, the detection threshold at the BS is assumed to be -8 dB (corresponding to rich scattering moderately mobile environment as per the 3GPP Technical Specification). Power inversion law is assumed to target -105 dBm at the BS, ramped up to -95 dBm with a step of 2 dB.

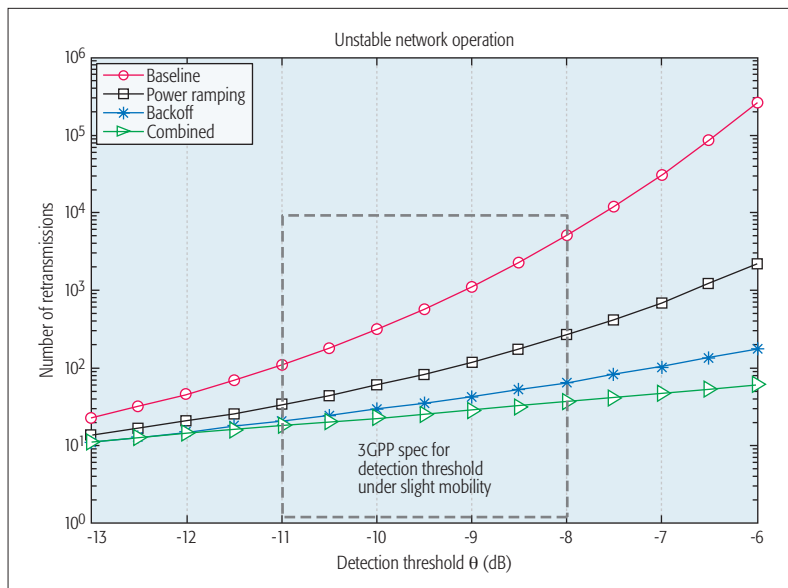


Figure 5. It is quite challenging to keep the network within the confines of stability. Peaks of traffic and user intensities can occur. In such circumstances, it is advised to revert to the combined RA scheme or otherwise work on strengthening the detection capability of the BS.

Technical Specification 36.211, Table 5.7.1-2, increases the number RA slots per frame from 1 to 3. Assuming a 10 MHz channel, the contribution of the RA allocation to the physical layer (PHY) overhead increases slightly from 1 up to 3 percent. However, by doing so, the BS is now able to handle $3\times$ – $5\times$ larger frame arrival rates while still operating in the stability region, as evident from Fig. 4.

However, inevitably there will be situations where bursts of UL traffic or peaks in user intensities drive the network toward instability. In this case, RA resources quickly become congested such that the RA scheme starts to play a major role in the network performance. Consequently, it is worthwhile to contrast the four schemes in terms of expected number of retransmissions before success. In such circumstances, the combined RA scheme differentiates itself very clearly, as shown in Fig. 5. It is clear from the figure that the combined scheme features consistently lower numbers of retransmissions than the other schemes, particularly as the detection threshold requirement increases.

In practice, the range of detection thresholds is typically confined between -11 and -8 dB (as per Tables 8.4.2.1-1 and 8.4.2.1-2 in 3GPP Technical Specification 36.104). The said tables specify the detection threshold for multipath channels under slight mobility for the cases of 2 and 4 receive antennas at the base station. Having said that, equipment vendors have one of two options when the network faces unstable conditions:

- Introduce an RA scheme that is slightly more sophisticated than the baseline one.
- Invest in enhancing the detection capability of the base station by a couple of dBs. This will enforce network stability in which all schemes impose similar behavior.
- Change the RA Configuration Index, which allocates more RA slots per frame.

POTENTIAL REMEDIES AND RECOMMENDATIONS

Now that we quantitatively know the limits of the RA process in LTE, it is time to contemplate possible remedies and enhancements. A few propositions are outlined herewith starting with the most obvious ones. Potential challenges and drawbacks associated with each proposition are also highlighted.

QUICK WINS

It has already been demonstrated that allocating more radio resources for RA pays off significantly. In practice, however, scheduling UL traffic on resource blocks that are spectrally adjacent to the physical random access channel (PRACH) has been avoided. This has been mainly to reduce unwanted adjacent interference whose impact is even more drastic when RA power ramping is exercised. As such, a BS should schedule those data resource blocks to devices that enjoy good radio conditions so as to minimize the effect of adjacent RA interference.

It is also worthwhile pointing out that allocating spectrally adjacent blocks for RA increases computational complexity at the BS side due to parallelized processing [7]. Nonetheless, we believe such additional computational burden can

be perceived as an affordable penalty for the sake of handling a large number of connections.

Another quick win is to simply keep the majority if not all devices in the RRC_CONNECTED state. This will significantly cut down the load on the RA process. In fact, transitioning devices into the RRC_IDLE state was primarily motivated in the early days by the need to relax the computational load of resource scheduling and allocation on the BS. However, this should not be worrisome anymore! The radio access network (RAN) is expected to soon become significantly more computationally powerful thanks to cloud-based architectures and network functions virtualization (NFV).

One additional proposition is to streamline the RA process by simply combining its two stages (i.e., piggyback the SR to the RRC transition request). The problem here is that the RA preamble signal is not designed in the first place to bear any useful information. As such, there is a need to investigate RA preamble waveforms, which can be information to be extracted by BSs.

Finally, the network can work toward shaving user intensity or traffic arrival peaks by invoking more RA-sensitive handover algorithms. Rather than basing handover solely on data serving capacity metrics, RA stability metrics can also be jointly considered.

BANDWIDTH SHARING

A potential route to resolving RA congestion directly stems from optimization of resource allocation for data transmission. The ability to serve devices with higher modulation schemes intuitively correlates to lessening the rate of RA attempts. Our experience shows that for a fixed UL traffic volume, a tangibly lower number of connections can be exploited to increase the available UL capacity at the BS. This is further explained in the sequel.

As a widely practiced approach, resource scheduling on the UL is performed irrespective of the UL channel response. However, for more efficient channel-aware scheduling to be feasible, UL channel sounding has to take place. Unless the number of connections is low enough, the sounding overhead becomes prohibitive. One proposition to lower the number of connections would be to cluster devices and IoT devices within a confined proximity. Data from cluster members is forwarded through an elected or BS-assigned cluster head over unlicensed spectrum.

On the other hand, there are a couple of drawbacks here. The first relates to interference in the unlicensed domain due to over-grazing (i.e., excessive use) of the spectrum for device-to-device (D2D) data forwarding. It also entails fairness issues regarding battery depletion rates and tariffing. Other well-known challenges encompass the need for intrusive changes to the back-end accounting and billing system in order for fair tariffing. Also, the overhead pertaining to cluster formation, particularly in light of mobility, should not be overlooked.

COORDINATED RANDOM ACCESS

To avoid over-grazing of the unlicensed spectrum, a “coordinated random access” approach is proposed herewith and depicted in Fig. 6. Under this approach, cluster members only exchange infor-

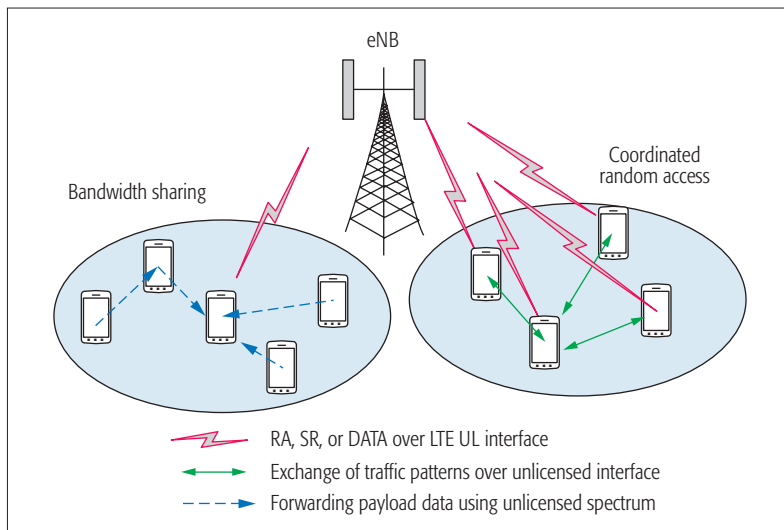


Figure 6. Two proposed approaches for relaxing contention rates over the PRACH in LTE networks.

mation about their traffic profiles with the goal of amicably agreeing to an RA schedule. As a result, the rate of RA collisions caused by devices belonging to one cluster can be potentially driven down to zero. In contrast to the bandwidth sharing approach, each cluster member here takes responsibility to transmit its data on its own. Clearly, the advantage of coordinated RA is light use of the unlicensed D2D spectrum, since it is only utilized to exchange informational messages in contrast to forwarding of the actual data payload. It is intuitive to state that the coordinated RA approach is more efficient than the former at higher device and/or traffic intensities.

While this scheme may well prove to have merit, it is quite challenging to implement in a non-invasive manner. In other words, adjustments have to be incorporated into the LTE specification and implemented on a mobile chipset to support its operation. Furthermore, this approach is more feasible for small cells. For larger cells, the number of coordination clusters increases, thus reducing the amount of mutual information across clusters. As a result, this diminishes the ability to avoid collisions.

Finally, it is crucial to point out that both approaches (bandwidth sharing and coordinated RA) may face serious scrutiny due to their security threats and vulnerability to attacks. Measures to circumvent these limitations are indeed an interesting area of research.

CONCLUSIONS

The IoT is going to be large in scale by nature. A wide array of applications with different mobility, latency, and traffic requirements will be associated with the IoT. To entertain such a diverse set of requirements, LTE technology is often perceived as a perfect candidate. Nevertheless, LTE is soon going to be plagued by unprecedented congestion on random access resources. Live network measurements and simulations carried out in this work confirmed the validity of this claim. As such, a combined stochastic geometry and queueing model is developed so as to better model and design RA procedure in terms of spatio-temporal traffic intensity. Furthermore, a few potential

The IoT is going to be large in scale by nature. A wide array of applications with different mobility, latency, and traffic requirements will be associated with the IoT. To entertain such a diverse set of requirements, LTE technology is often perceived as a perfect candidate. Nevertheless, LTE is soon going to be plagued by unprecedented congestion on random access resources.

remedies and recommendations for relaxing RA congestion are also highlighted.

REFERENCES

- [1] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 4th qtr. 2015, pp. 2347–76.
- [2] D. Miorandi *et al.*, "Internet of Things: Vision, Applications and Research Challenges," *Elsevier Ad Hoc Networks*, vol. 10, no. 7, 2012, pp. 1497–1516.
- [3] C. Drubin, "The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020," *Microwave J.*, vol. 57, no. 10, no. 51, Aug. 2014.
- [4] M. Polese *et al.*, "On the Evaluation of LTE Random Access Channel Overload in a Smart City Scenario," *Proc. 2016 IEEE ICC*, Kuala Lumpur, Malaysia, May 2016.
- [5] S. Alvi *et al.*, "Internet of Multimedia Things: Vision and Challenges," *Ad Hoc Networks*, vol. 33, Oct. 2015, pp. 87–111.
- [6] D. T. Wiriatmadja and K. W. Choi, "Hybrid Random Access and Data Transmission Protocol for Machine-to-Machine Communications in Cellular Networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, Jan 2015, pp. 33–46.
- [7] S. Sesia, I. Toufik, and M. Baker, *LTE: The UMTS Long Term Evolution*, Wiley Online Library, 2009.
- [8] Y. Zhong *et al.*, "On the Stability of Static Poisson Networks under Random Access," *IEEE Trans. Commun.*, accepted 2016.
- [9] M. Gharbieh *et al.*, "Tractable Stochastic Geometry Model for IoT Access in LTE Networks," *Proc. IEEE GLOBECOM '16*, Washington, DC, Dec. 2016.
- [10] J. Boyd, "Real-Time Crowd Simulator Could Help Prevent Deadly Stampedes," *IEEE Spectrum*, Aug. 2016.
- [11] S. A. M. Saleh, S. A. Suandi, and H. Ibrahim, "Recent Survey on Crowd Density Estimation and Counting for visual Surveillance," *Elsevier Engineering Applications of Artificial Intelligence*, vol. 41, May 2015, pp. 103–14.
- [12] J. Fink, A. Ribeiro, and V. Kumar, "Robust Control of Mobility and Communications in Autonomous Robot Teams," *IEEE Access*, vol. 1, May 2013, pp. 290–309.
- [13] J. G. Andrews *et al.*, "What Will 5G Be?," *IEEE JSAC*, vol. 32, no. 6, June 2014, pp. 1065–82.
- [14] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic Geometry for Modeling, Analysis, and Design of Multi-Tier and Cognitive Cellular Wireless Networks: A Survey," vol. 15, no. 3, 2011, pp. 996–1019.
- [15] M. Gharbieh *et al.*, "Spatiotemporal Stochastic Modeling of IoT Enabled Cellular Networks: Scalability and Stability Analysis," *ArXiv e-prints*, Sept. 2016.

BIOGRAPHIES

AHMED BADER [M'10, SM'13] (ahmed.bader@kaust.edu.sa) received his B.S. degree from the University of Jordan in 2003, his M.S. degree from The Ohio State University in 2006, and his Ph.D. degree from Telecom ParisTech, France, in 2013, all in electrical engineering. He has more than 10 years of experience in the wireless industry and has previously held positions at Emerson and Siemens. Since 2013, he has been with King Abdullah University of Science and Technology (KAUST) in Saudi Arabia where he is spearheading multiple applied research projects that have led to several patent-pending technologies. He is also a co-founder of Insyab Wireless, a Dubai-based company designing real-time connectivity solutions for unmanned systems. His research interests are mainly in the domain of large-scale wireless networks.

HESHAM EL SAWY [S'10, M'14] (hesham.elsawy@kaust.edu.sa) received his B.Sc. degree in electrical engineering from Assiut University, Egypt, in 2006, his M.Sc. degree in electrical engi-

neering from the Arab Academy for Science and Technology, Cairo, Egypt, in 2009, and his Ph.D. degree in electrical engineering from the University of Manitoba, Winnipeg, Canada, in 2014. Currently, he is a postdoctoral fellow with the Computer, Electrical, and Mathematical Sciences and Engineering Division, KAUST and an adjunct member at the School of Computer Science & Engineering, York University, Canada. During the period of 2006–2010, he worked at the National Telecommunication Institute, Egypt, where he conducted professional training at both the national and international levels, as well as research on network planning. From 2010 to 2014, he worked with TRTech, Winnipeg, Canada, as a student researcher. For his academic excellence, he has received several academic awards, including the NSERC Industrial Postgraduate Scholarship during the period of 2010–2013, and the TRTech Graduate Students Fellowship in the period of 2010–2014. He also received the best paper award at the ICC 2015 Workshop on Small Cells and 5G Networks. He was recognized as an exemplary reviewer by *IEEE Transactions on Communications* in 2015 and 2016. His research interests include statistical modeling of wireless networks, stochastic geometry, and queueing analysis for wireless communication networks.

MOHAMMAD GHARBIEH received his B.Sc. degree (Hons.) in electrical engineering from the University of Jordan, Amman, in 2016. He has been a visiting student with the Computer, Electrical, and Mathematical Sciences and Engineering (CEMSE) Division, KAUST, since 2016. His research interests are mainly statistical modeling of wireless networks, stochastic geometry, queueing theory applications for communications, and cross-layer protocol design.

MOHAMED-SLIM ALOUINI [S'94, M'98, SM'03, F'09] received his Ph.D. degree in electrical engineering from the California Institute of Technology (Caltech), Pasadena, in 1998. He served as a faculty member at the University of Minnesota, Minneapolis, and then at the Texas A&M University at Qatar, Education City, Doha, before joining KAUST as a professor of electrical engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.

ABDULKAREEM ADINOYI received his B.Eng., M. S., and Ph.D. in electrical engineering, from the University of Ilorin, Nigeria, in 1992, King Fahd University of Petroleum and Minerals, Saudi Arabia, in 1998, and Carleton University, Canada, in 2006, respectively. He has worked in the industry (as an engineer, researcher, and consultant) and academia (as a lecturer and assistant professor). He is an inventor of three patents in radio resource management in relay-based OFDMA networks. Between January 2004 and December 2006, he worked in the European Union 6th Framework integrated project WINNER. He is currently at Swedtel Arabia as a senior telecom consultant for Saudi Telecommunications Company (STC). His current research and work scope covers mobile broadband technologies (e.g., cooperative communications, LTE, NB-IoT, LTE-Advanced, and 5G) and emerging mobile network-based services and applications (e.g., the Internet of Things, smart cities, and intelligent transport systems).

FURAIH ALSHAALAN is the GM of R&D at STC. He is an accomplished technology development and management professional with a balanced combination of managerial and technical experience. His experience spans over 25 years in the telecom industry. At STC, he leads, directs, and guides the adoption of new network technologies, including HSPA/HSPA+, LTE/LTE-Advanced, and NFV. He received his Ph.D. in electrical engineering from King Saud University, Riyadh, in 2011. He obtained Bachelor's and Master's degrees in electrical engineering from King Fahd University of Petroleum and Minerals. He has attended many executive management courses.



IEEE WCET™

**IEEE WIRELESS COMMUNICATION
ENGINEERING TECHNOLOGIES
CERTIFICATION**



Join an Elite Group of Professionals Working in Wireless



IEEE WCP
*IEEE Wireless
Communications
Professional*

**Globally Recognized
Emblem of Achievement**

WWW.IEEE-WCET.ORG

IMPORTANT DATES

SPRING APPLICATION DEADLINE
31 March 2017 by 23:59 UTC

SPRING TESTING WINDOW
17 April - 13 May 2017

FALL APPLICATION DEADLINE
8 SEPTEMBER 2017 by 23:59 UTC

FALL TESTING WINDOW
25 September - 21 October 2017

A Community-Driven Access Control Approach in Distributed IoT Environments

Dina Hussein, Emmanuel Bertin, and Vincent Frey

The authors propose utilizing a community-based structure to define the notion of access rights in a distributed IoT environment. With this structure, within a given community of smart objects sharing a common mission, access rights are to be evaluated based on the community norms by smart objects with sufficient resources on behalf of those with resource limitations.

ABSTRACT

The distributed Internet of Things is emerging in the literature as a new paradigm for IoT where remotely controlled smart objects can act on their own to sense/actuate, store, and interpret information either created by them or within the surrounding environment. This paradigm calls for novel security and access control mechanisms to enable smart objects with various resource limitations to evaluate a claimed access right from external entities without relying on central authorization systems. This article proposes utilizing a community-based structure to define the notion of access rights in a distributed IoT environment. With this structure, within a given community of smart objects sharing a common mission, access rights are to be evaluated based on the community norms by smart objects with sufficient resources on behalf of those with resource limitations. A novel, community-driven, access control framework is proposed in addition to a prototype to demonstrate access control granting in a user-friendly manner.

INTRODUCTION

Where and how should access control (AC) be exercised in the Internet of Things (IoT)? Vint G. Cerf [1] deliberates on some possible AC methods for IoT. Cerf discusses the idea of placing AC at the edge of the network, particularly at the device level or the device controller level. In this sense, devices should be able to evaluate an external source's authorization to command, access, or gain control over them. Along the same lines, Roman *et al.* [2] provided the concept of distributed IoT as an element of the future IoT. Distributed IoT can be characterized by two main principles: edge intelligence, in which parent nodes are able to delegate authority decisions to entities at a lower level, and collaboration among diverse entities to reach a certain goal.

In daily social life, the distribution of rights and obligations is typically addressed through the notion of community, which is formalized within the philosophy of social science. Bhaskar *et al.* [3] notably provide this seminal definition: "Community is conceptualized as an identifiable, restricted enduring (if typically evolving) coherent grouping of people who share some set of (usually equally evolving) concerns."

This conceptualization of communities, as we argue in this article, is helpful to clarify the notion of rights in distributed IoT. That is, the vision of

edge intelligence as proposed in the literature [1, 2] is hardly possible to achieve by smart objects (SOs) with limited capabilities. Thus, relying on a community-based structure would enable SOs that share common missions and have sufficient resources to make authorization decisions on behalf of those with less capability. Additionally, this community structure would enable a finely tuned set of AC policies to be stored and managed locally to fit the goals of the community. From a computational perspective, the overhead required to process and enforce AC policies at the individual device level will be scaled down when policies are designed to secure access to a community of devices sharing common missions and therefore access requirements. Finally, external entities that, temporarily or permanently, share a common mission and are capable of providing sufficient assertions to prove compliance to the community rules can be entitled to get a key to enable access to the community.

The structure of a community, however, is different from the social structures proposed by the social Internet of Things (SIoT) paradigm [4]. SIoT suggests building a social structure composed of diverse entities, not necessarily driven by common goals and missions, to facilitate SOs' navigability and services discovery in a manner similar to social network services (SNS).

This article proposes a community structure for distributed IoT environments in order to manage AC rights. We define an IoT community as composed of the following elements:

- An evolving set of SOs, each one having a specific position within the community according to its resource capability (sensor, actuator, controller, etc.)
- A set of shared goals that defines the mission statement of the community
- A set of policies defining the rights and obligations toward the community

Community capability-based access control (COCapBAC) is proposed in this article where AC is managed at the level of IoT communities sharing the same mission (e.g., entertaining guests in a smart home, managing kitchen and cooking appliances). At the bootstrapping stage, a community is created with one or more resource-capable IoT objects, named gatekeepers, that have the role of making AC decisions on behalf of other resource-constrained objects in the community. Additionally, owning a community key token, named capability, enables access to devices and resources within the

Project	Security model	Applications/ use cases	Design principle
iCore (http://www.iot-icore.eu/)	A model-based security toolkit, Seckit, is proposed	Smart home, city, meeting, and business	Virtual objects (VO) to represent real-world objects
BUTLER (www.iot-butler.eu/)	A centralized authorization protocol based on OAuth2.0 standard	Smart cities, health, home, shopping, and transport	Distributed and cross-domain network of networks
GAMBAS (http://www.gambas-ict.eu/)	A policy-based access control mechanism	Smart city and transport	Adaptive middleware for distributed behavior-driven services
IoT@Work (https://www.iot-at-work.eu/)	A capability-based access control mechanism	Industrial automation	Distributed and cross-domain IoT
RERUM (https://ict-rerum.eu/)	Public key infrastructure (PKI)-based authorization for objects with limited resources	Smart transport, environment monitoring, energy management at home	Distributed and cross-domain framework for smart city
COMPOSE (http://www.compose-project.eu/)	Security control policies configured by regular users	Smart city, shopping, and territory	VOs are considered, that is, service objects
OpenIoT (http://www.openiot.eu/)	Access control server module	Smart city	Cloud-based IoT sensing services, "sensing as a service"
IoT6 (http://iot6.eu/)	Datagram transport layer security (DTLS)	Smart building	IPv6 architecture to achieve IoT interoperability
IoT-A (http://www.iot-a.eu/public)	Access control policies	Smart cities	Distributed, cross-domain platform
Sociotal (http://sociotal.eu/)	A distributed capability-based AC approach	Smart communities, cities	Distributed IoT platform

Table 1. Security approaches in European (Framework Programme 7, FP7) projects.

community without the need to issue and validate tokens prior to each access attempt.

The rest of the article goes as follows. We review the current state of the art and related works. We present our COCapBAC approach and framework. A use case is implemented later to demonstrate our approach in a daily life scenario. We provide a discussion on AC principles for future-driven IoT paradigms. Finally, the article is concluded.

STATE OF THE ART

SECURITY AND PRIVACY IN IOT

Security and privacy in the IoT arena are emerging, crucial topics, which are widely tackled by a number of review articles in the literature. Roman *et al.* [2] define and compare security challenges and requirements in centralized vs. distributed IoT environments. Similarly, Sicari *et al.* [5] summarize contributions of articles tackling IoT security. Vasilomanolakis *et al.* [6] provide taxonomy for the main security requirements in IoT and their subcomponents. Among the common research challenges and open issues found in the previously mentioned survey articles are the need to provide scalable security and AC mechanisms for devices with limited capabilities. Also, there is the challenge of achieving horizontal security approaches for cross-domain IoT [5]. That is, in many IoT scenarios, objects that belong to certain security domains might need to access data produced in another domain. Moreover, in mission-critical application scenarios, like in an enterprise, data generated by IoT objects at different security levels may only be meant for accessing by selected employees. Thus, there is a need for building cross security domain AC in IoT.

In addition to research articles, European proj-

ects are also concerned with security and AC for IoT. As summarized in Table 1, we surveyed the contributions of European FP7 projects that have particularly addressed this topic. It is worth mentioning here that within these projects we did not detect novel challenges, security, or AC models beyond the current state of the art.

ACCESS CONTROL IN IOT

One of the most common AC models is the AC list (ACLs), in which access rights are centrally specified and assigned to concerned subjects. This approach becomes a burden to manage and deploy with the increasing number of IoT objects [7].

Role-based AC (RBAC) emerged to propose an additional layer: assigning rights to roles, instead of granting those rights directly to subjects; thus, these roles can be assigned to the subjects requesting access [8]. This approach reduces the effort of managing AC rules; however, its scalability is a big challenge, given the need to assign roles to a big number of IoT object.

Attribute-based AC (ABAC) addresses the problem of managing a huge number of rules by giving the possibility to use a combination of various attributes concerning a requested subject (i.e., location, temperature, etc.) to generate dynamic access policies, and therefore potentially reduce the number of static AC rules associated with each resource [9]. For instance, the location of the IoT object in addition to the object owner identity could be combined dynamically to allow/or deny access to a certain building. The potentially large number of attributes that need to be understood and managed in order to establish dynamic policies is one of ABAC's biggest challenges.

One problem common to ACL, RBAC, and ABAC is centralization, as a central entity is

Among the advantages of capability-based AC is the support for delegation of access rights from a subject to another. Additionally, it supports the revocation of granted capability token and the granularity of access permission level.

responsible for making authorization decisions, combining attributes, and enforcing access policies. However, in a distributed IoT these models may not meet the requirements.

A capability-based security model was provided a long time ago in the literature [10, 11]. A capability can be defined as a self-contained key or a token that references a target object, resource, or information along with an associated set of access rights.

Holding a capability token enables access to only the information and resources that are necessary for the holder's legitimate purpose, as stated within the capability token held.

The capability-based authorization approach offers flexibility that can meet the requirements of various IoT architectures. In which a central party is responsible for issuing the capability token, whereas validating the correctness of this capability token is either the responsibility of an intermediate party different than the issuing one (for a centralized architecture) or the responsibility of requested SOs themselves (for distributed architecture). Among the advantages of capability-based AC is support for delegation of access rights from one subject to another. Additionally, it supports the revocation of a granted capability token and the granularity of the access permission level [12].

CAPABILITY-BASED AC IN IOT

Anggorojati *et al.* [12] provide a vision for an identity and capability-based AC model to handle authority delegation in cross-domain IoT environments in which a central entity in each domain is in charge of authorizing a delegation request from a delegator to a delegate. This approach relies mainly on a central entity for asserting a delegation request. This centralization makes the approach susceptible to single point of failure (SPOF) issues.

Hernández-Ramos *et al.* [13] provide a study for a capability-based AC in a distributed IoT environment where capability issuance and authorization take place without intermediate entities implementing AC logic. That is, IoT objects are capable of evaluating an access authorization request and thus make a decision whether to grant or deny access permission. This fully distributed approach, however, does not consider entities with limited resources, which are not capable of making authorization decisions.

Gusmeroli *et al.* [14] provide a proposal for capability-based AC in a distributed IoT environment, where users can manage AC processes for their owned IoT objects by generating electronic capability tokens. This proposed mechanism supports AC rights delegation from one user to another where the IoT objects are located at the edge to activate granted access with no mechanism to detect the validity or correctness of the token itself. Additionally, users need information and communications technology (ICT) skills for generating capability tokens, delegating or revoking capability tokens given to other users.

CAPABILITY-BASED AC ARCHITECTURE IN LITERATURE

In this section we summarize the different capability-based AC approaches proposed in the literature along with our proposed approach. Figures 1a and 1b illustrate the different kinds of capability-based AC approaches proposed in the literature.

Centralized Capability-Based AC Approach:

In this approach capability issuance, as well as validation, takes place at a central point (Fig. 1a). The authorization server (AS) is responsible for acting as a certificate authority (CA) to issue capability tokens, as well as a policy decision point (PDP) to evaluate and make authorization decisions. This approach starts with the requesting entity (subject) requesting a capability token in order to get authorized access to another entity (object). After evaluating the AC policies, a capability token is issued specifying access rights toward the requested object. Then, prior to each access attempted by the subject, the capability token has to be presented once again to the central AS to verify its validity and to avoid forgery before allowing or denying access to the object. However, the centralized approach is susceptible to SPOF issues. In addition, the centralized approach is not compatible with different implementation choices in cross security domains.

Distributed Capability-Based AC Approach:

In this approach capability issuance takes place centrally, whereas capability validation is enforced via distributed PDPs embedded at the device or gateway level (Fig. 1b). This approach begins with the subject requesting a capability token from the CA where a centralized AS is taking the CA responsibility. After making a capability authorization decision and issuing a capability token, this capability token has to be locally verified by the target object. AC decisions are hence made and enforced via PDP and policy enforcement point (PEP) roles embedded in target objects. This approach brings forward the challenge of managing access policies and rules per device in the network, especially in big-scale IoT networks. In addition to the challenge of embedding PDP in resource limited objects.

TOWARD A COMMUNITY-DRIVEN CAPABILITY AC APPROACH

THE COCAPBAC APPROACH

In COCapBAC, the authorization decision is split between:

1. The CA (for asserting a subject's attributes)
2. The AS (for issuing CO capability tokens)
3. CO gatekeepers (for validating the correctness of a CO capability token against forgery)

These gatekeepers are chosen among the most capable objects of a given community.

In the first phase the subject will send an attribute assertion request to a CA of choice and trust by the AS (mobile operator, location service, IoT device manufacturer, etc.). The goal of this request is to receive a certificate signing the authenticity of the subjects' attributes (e.g., mobile phone number, current location, device manufacturer code). In the second phase, the subject will send an access request to the CO gatekeeper along with the signed attributes, which will transfer the request and attributes to the AS. The AS is responsible for acting as a PDP for evaluating a CO access request. In the third phase, after validating the signed attributes, the AS will generate a CO capability token and transfer it back to the CO gatekeeper, which will forward it to the subject (Fig. 1c).

Each time the subject holding a CO capability token is requesting access to an SO, it will present the CO capability token to the CO gatekeeper. The CO gatekeeper acts as a PEP to execute AC

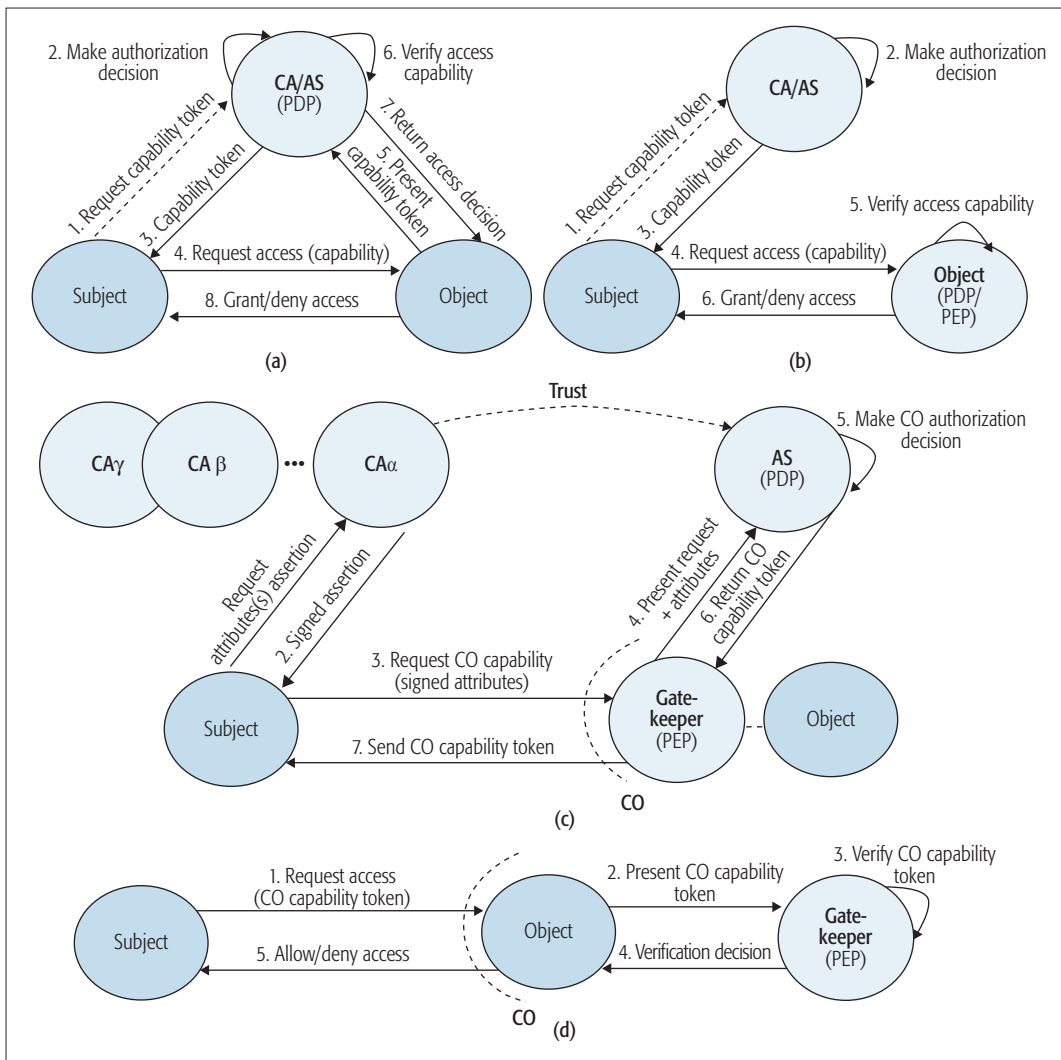


Figure 1. Different approaches for capability-based AC: a) centralized capability-based approach; b) distributed capability-based approach; c) community-driven capability approach; d) using a community capability to get access to a community object.

policies within a CO. Such policies are managed by the AS. After validation of the correctness of the token, the CO gatekeeper will allow/deny access to the requested SO (Fig. 1d).

COCAPBAC FRAMEWORK

Figure 2 depicts the main elements of the COCapBAC framework that are responsible for issuing and validating a capability token. Most of the elements types are borrowed from well established schemas like SAML¹ and XACML.² Additionally, most of the definitions used are provided by the Internet Engineering Task Force (IETF) Policy Framework Working Group [15].

Authorization Server: It is responsible for authorizing access to a community. For this purpose, it registers SO attributes and AC policies. It also has a capability token manager, which is responsible for delivering capability tokens

Policy Decision Point: This is embedded within the AS, and is responsible for evaluating applicable policies and rendering capability authorization decisions.

Certificate Authority: It is responsible for providing assertions to a subject requesting access to a target (CO or SO) managed by a given AS. As dis-

cussed before, each entity can rely on any CA to provide the required assertion given that this chosen CA is trusted by the AS. For this purpose and upon request for an assertion made by a subject, the assertion manager in the CA will require further authorization steps before providing an assertion (these steps are not in the scope of this article).

Community Gatekeeper: This is responsible for enforcing an access authorization decision made by AS inside the CO. For this purpose, it registers attributes of SOs that are part of a community as well as community policies (which are pre-specified at the AS).

Policy Enforcement Point: It is embedded within a CO gatekeeper and responsible for enforcing CO decisions sent by the PDP. It also validates the correctness of a capability token against interception from third parties.

Community: This is a group of SOs and services that share common goals (e.g., accommodating guests in a smart home) and are managed by the same AS.

Capability: It is a data structure that contains a set of access rights, which is issued and signed by the AS and validated by a CO gatekeeper.

The proposed COCapBAC is built on JavaScript

Each time the subject holding a CO capability token is requesting access to SO, it will present the CO capability token to the CO gatekeeper. The CO gatekeeper acts as a PEP to execute AC policies within a CO. Such policies are managed by the AS. After validation the correctness of the token the CO gatekeeper will allow/deny access to the requested SO.

¹ SAML, <https://www.oasis-open.org/committees/security/>

² XACML, <https://www.oasis-open.org/committees/xacml/>

The proposed COCapBAC is built on JavaScript Object Notation (JSON) as a representation format for the CO capability token, as well as the use of dedicated communication protocols such as the Constrained Application Protocol (CoAP).

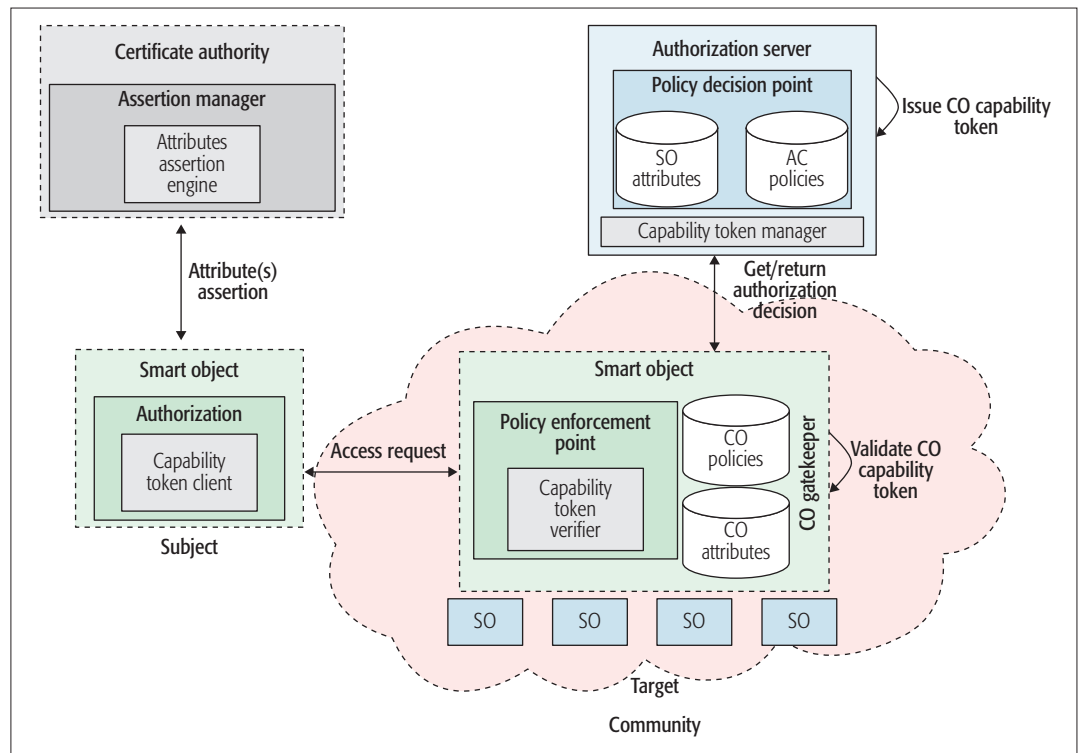


Figure 2. COCapBAC framework.

Object Notation (JSON)³ as a representation format for the CO capability token, as well as the use of dedicated communication protocols such as the Constrained Application Protocol (CoAP)⁴. The basic operation of our COCapBAC proposal is shown in Fig. 2. Below, we clarify the different steps of the process.

1. Attributes assertion: This is an initial step where a CA asserts the subject attributes (i.e., identity, location, device manufacturer, etc.)

2. Access request: Once a subject is holding asserted attributes, it can request access to a certain CO. This request is sent to either a CO gatekeeper if the address of the gatekeeper is known to the subject or to any objects in the CO, which will transfer the request to the CO gatekeeper. This request is sent along with asserted attributes.

3. Get/return authorization decision: When an access request is sent to the gatekeeper, it presents it to the AS, which checks the rights associated with the subject. The returned decision includes a CO capability token in the case that access is allowed, a request for other asserted attributes from the subject, or a message rejecting access.

4. Issue CO capability token: The CO capability token is issued by the AS upon the gatekeeper transfer of the access request from the subject to the AS (see capability components below).

5. Validate CO capability token: The validation process is undertaken by the CO gatekeeper to ensure the correctness of the CO capability token against forgery from third parties.

We extend the notations provided by the IETF Network Working Group [15] to define a CO capability token, which consists of the access rights associated with all the objects inside a given CO. This capability is verified prior to each access attempt by the gatekeeper. Components of the CO capability token are:

- Identifier (ID): This field is used to identify a capability token.
- Issuing time (II): It identifies the time at which the token was issued.
- Issuer (IS): It identifies the issuer and the signer of the token, that is, the AS.
- Subject (SU): It refers to the subject to which the capability token is granted.
- Device (DE): It is a URI used to identify the device(s) in the community to which the token applies.
- Community (CO): It references a community to which the DE belongs.
- Signature (SI): It carries the digital signature of the capability token.
- Not before (NB): The time before which the CO capability token must not be accepted.
- Not after (NA): The time after which the CO capability token must not be accepted.
- Access rights (AR): This field represents the set of rights that the issuer has granted to the subject.
 - Device (DE): It represents the smart service, device, or data for which the action is granted.
 - Action (AC): It identifies a specific granted action. Its value could be any CoAP method (i.e., GET, POST, PUT, DELETE). These methods are represented within the CoCapToken structure as read, create, modify, and delete, respectively.
 - Conditions (C): This is a set of conditions that have to be fulfilled locally on the device to grant the corresponding action; for instance, the validity time of the capability token (Fig. 3).

Figure 3 summarizes the structure of a capability token, using JSON classes, which is designed to allow access to two CO objects: a parking area gate and a temperature sensor.

³ JSON, <http://www.json.org/>

⁴ CoAP, <http://coap.tech-nology/>

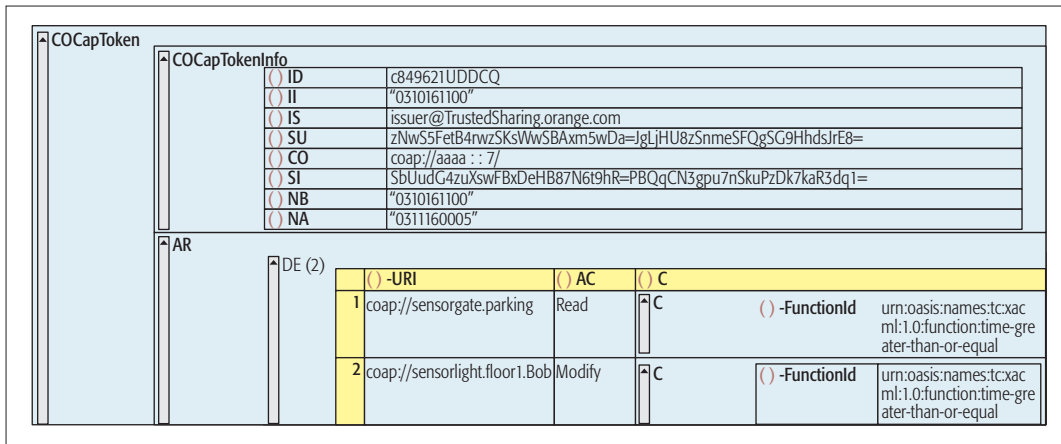


Figure 3. Structure of a COCapToken in JSON classes.

PROOF OF CONCEPT IMPLEMENTATION

One of the biggest challenges hindering the realization of AC in IoT on a wider scale is the lack of automated mechanisms for secured access to a plurality of heterogeneous objects that help people in carrying out their quotidian tasks – while paying a great deal of attention to the simplicity for the end users. Thus, the use case and implementation provided in this section is designed to demonstrate COCapBAC operation in real life. Figure 4 presents the use case, which takes place in a smart home.

1. Bob invited Alice, among other guests, to his birthday party at home. Bob stored a list of all confirmed attendees with their mobile phone numbers in his local AS server, known as Trusted Sharing, which is located inside Bob’s apartment.

2. On the party day and in order to first get into a parking space at Bob’s building, Alice uses her mobile phone number as an attribute to assert her identity at the parking gate. The parking gate sensors present Alice with an asserted attribute (i.e., telephone number) along with an access request to Bob’s home. This data is sent to the CO gatekeeper, which in this use case is the media streamer box at Bob’s home.

3. The gatekeeper presents the request and attributes to the AS to evaluate the request and the access rights associated with Alice’s phone number.

4. A CO capability token is then sent to Alice, and at the same time access to a parking space is allowed.

5. With the CO capability token now held by Alice (transferred to her smartphone), she can access other objects belonging to the same CO, as pre-specified by the AS, where each time an access request is made by Alice, the CO gatekeeper evaluates the request to make sure the capability token has not been forged before allowing or denying access to the object. Later, Bob can revoke Alice’s access to the CO: a specific policy will be sent from the AS to the gatekeeper, which can reject access to CO objects based on the revocation policy presented to it by the AS.

Steps 1 to 4 are illustrated in Fig. 4a. Step 5 is displayed in Fig. 4b.

The functionalities of the CA are outside the scope of this article. Thus, we have developed a prototype, Trusted Sharing, to demonstrate COCap generation and validation (Fig. 5). The

processing power and storage required in order to run Trusted Sharing are compatible with smartphones and/or devices capable of handling JSON code and managing the digital signatures used to secure QR codes. The goal is to demonstrate effortless deployment of our proposed COCapBAC in real-life scenarios.

Trusted Sharing is composed of sensor nodes, a router, and a smartphone application for Android operating systems. Trusted Sharing is responsible for matching an access request with its assigned access rights (using the phone number as a key for the matching). If the matching is correct, a capability token will be issued and sent to the requester smartphone via NFC technology. We assume that an attribute assertion is sent from the requester smartphone via NFC to a Trusted Sharing server, as shown in Fig. 5a1. A light sensor is used to demonstrate successful access authorized by Trusted Sharing, as shown in Fig. 5a2.

After authorized access to Bob’s parking garage, Trusted Sharing will transfer a CO capability token, as shown in Fig. 5b1. Alice chooses to transfer the CO capability token to her smartphone via NFC technology, as shown in Fig. 5b2. Finally Alice uses the CO capability token to get access to a Deezer⁵ shared playlist at Bob’s home. She can play the shared music on Bob’s media player, as shown in Fig. 5c.

For non-NFC-enabled devices, QR codes could be used to transfer a capability token, as shown in Fig. 5a1.

DISCUSSION: EMERGING REQUIREMENTS FOR AC IN FUTURE-DRIVEN DISTRIBUTED IOT ENVIRONMENTS

This article focuses on providing a particular solution to realize AC for distributed IoT environments, as deduced from challenges introduced in the literature. Behind this solution, however, there are some essential requirements we have addressed in our approach and believe should be fulfilled regardless of the solution or AC model used. Hereafter, we present these requirements to the IoT research community:

From identity-centric to attributes-centric AC approaches: Relying on a central identity management authority to assert the identities of subjects in cross-domain IoT applications seems to introduce more complexity in addition to scalability

One of the biggest challenges hindering the realization of AC in IoT on a wider scale is the lack of automated mechanisms for secured access to a plurality of heterogeneous objects that help people in carrying out their quotidian tasks – while paying a great deal of attention to the simplicity for the end users.

⁵ Deezer, <http://www.deezer.com/>

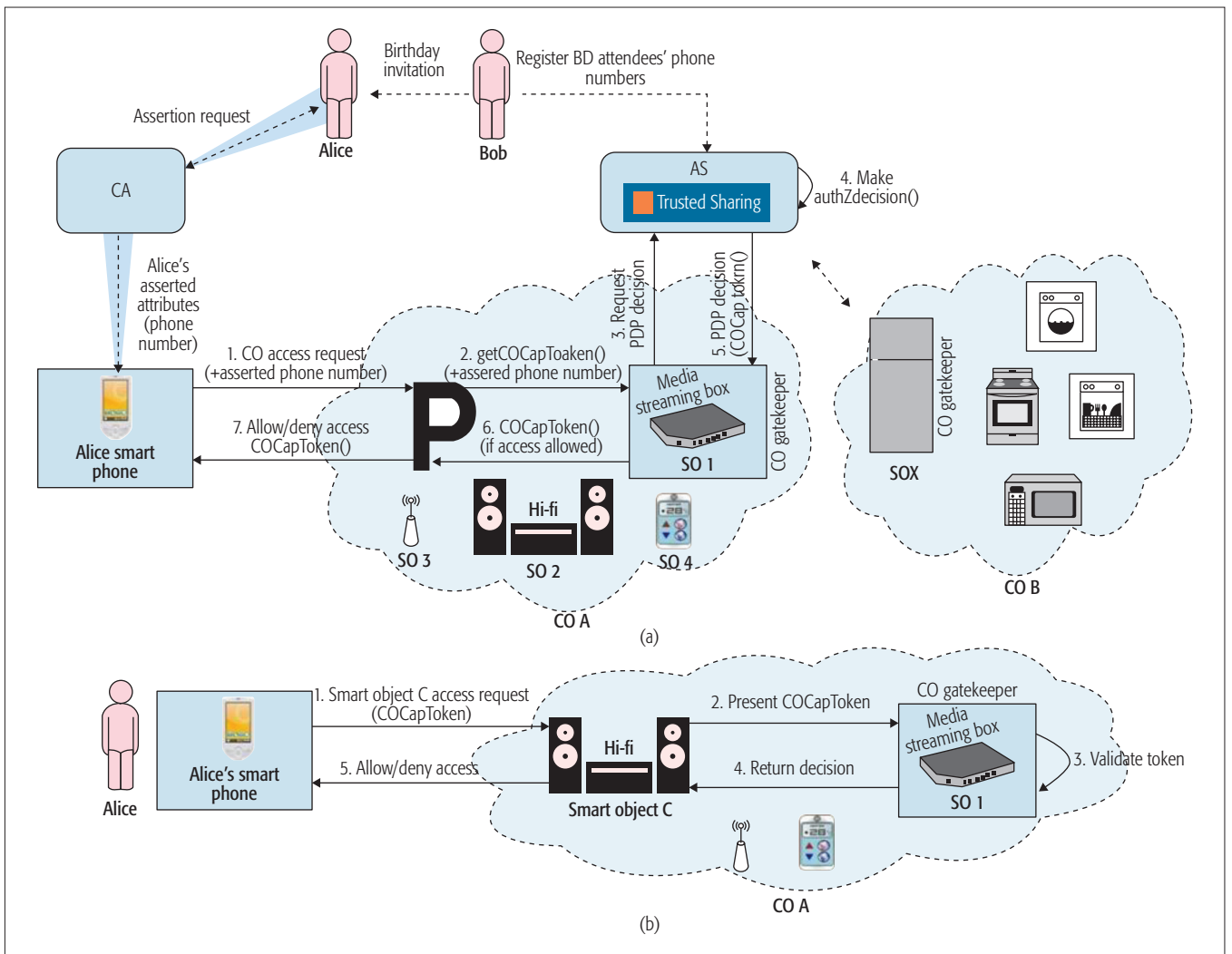


Figure 4. COCapBAC framework. a) Alice gets a CO capability token to get access to Bob's parking space and to the birthday party at Bob's apartment. b) Alice uses the same CO capability token to get access to authorized devices at Bob's apartment.

issues. It adds further complexity for IoT in particular where objects' identities are hard to maintain and assert. For instance, a laptop has its manufacturer model number, a product key of its operating system, and an IP or medium access control (MAC) address. Which identity is going to be used for granting/revoking access requests, especially when the device location might change? Instead, relying on one or more attributes for asserting the authenticity of the requester (e.g. current location, manufacturer, etc.) seems more reliable for AC in distributed environments.

From fully distributed to semi-distributed authorization: A very optimistic approach to achieve fully distributed authorization at the edge of the IoT network is sometimes suggested in the literature. This approach, however, is challenged by the number of resource limited SOs in a typical IoT scenario. To tackle this issue in future-driven AC approaches, we rather suggest allowing some designated nodes to make AC decisions on behalf of incapable SOs. Accordingly, AC rules and policies will not be stored at each individual SO, or SO controller, in the network. They will instead be managed by those designated AC decision points in a semi-distributed manner.

From user-driven to self-contained and automated AC: Finally, relying on the users' ICT skills to define AC rules and to delegate AC permissions, or capabilities, is proposed in the literature, but it might introduce great complexity issues for end users, given the number of resources to which a user might have to grant access rights. Instead, creating automated access rights delegation by relying on dynamic policies and rules defined at design time to reduce the effort at the end-user side seems necessary. Users could define general-purpose policies and let objects form communities.

CONCLUSION

This article proposes a novel framework for AC in distributed IoT: community-driven AC. From an IoT perspective, the concept of community seems well suited. This assumption is driven by the fact that IoT objects are indeed rarely fully isolated; instead, they operate in conjunction with other objects and services to fulfill a common mission. In this article we build on the concept of community to define the notion of rights. That is, an IoT entity "having an access right" means it has to play the role of the entitled party toward an obliged party in a relationship defined by the system of norms of a given community.

In fact, the importance of AC in IoT will be emphasized in the years to come, as the number of connected objects increases and IoT business models become more sophisticated. In this article we provide a set of requirements for realizing AC in IoT, independent from any particular AC mechanism. In the future, it is an important task to tailor standard AC mechanisms for applying these requirements to daily-life scenarios.

In the future, we plan to study the phases of community creation and development with AC rights associated with each phase. Additionally, we plan to extend our prototype to demonstrate access policy specification by a community manager at a bootstrapping phase. We also plan to extend our prototype to large-scale IoT systems, particularly in an enterprise.

REFERENCES

- [1] V. G. Cerf, "Access Control and the Internet of Things," *IEEE Internet Computing*, 2015, vol. 19, no. 5, p. 96.
- [2] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, 2013, vol. 57, no. 10, pp. 2266–79.
- [3] M. Archer et al., *Critical Realism: Essential Readings*, Routledge, 2013.
- [4] L. Atzori, A. Iera, and G. Morabito, 2014, "From 'Smart Objects' to 'Social Objects': The Next Evolutionary Step of the Internet of Things," *IEEE Commun. Mag.*, vol. 52, no. 1, Jan. 2014, pp. 97–105.
- [5] S. Sicari et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks*, 2015, vol. 76, pp. 146–64.
- [6] E. Vasilomanolakis et al., "On the Security and Privacy of Internet of Things Architectures and Systems," *Int'l. Wksp. Secure Internet of Things*, 2015, pp. 49–57.
- [7] J. Qian, S. Hinrichs, and K. Nahrstedt, "ACL: A Framework for Access Control List (ACL) Analysis and Optimization," *Communications and Multimedia Security Issues of the New Century*, Springer, 2001, pp. 197–211.
- [8] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*, Artech House, 2003.
- [9] C. A. Ardagna et al., "Enabling Privacy-Preserving Credential-Based Access Control with XACML and SAML," *2010 IEEE 10th Int'l. Conf. Computer and Info. Tech.*, pp. 1090–95.
- [10] L. Gong, "A Secure Identity-Based Capability System," *IEEE Symp. Proc. Security and Privacy*, 1989, pp. 56–63.
- [11] R. S. Sandhu and P. Samarati, "Access Control: Principle and Practice," *IEEE Commun. Mag.*, vol. 32, no. 9, Sept. 1994, pp. 40–48.
- [12] B. Anggorojati et al., 2012, "Capability-Based Access Control Delegation Model on the Federated IoT Network," *2012 15th Int'l. Symp. Wireless Personal Multimedia Commun.*, pp. 604–08.
- [13] J. L. Hernández-Ramos et al., "Distributed Capability-Based Access Control for the Internet of Things," *J. Internet Services and Info. Security*, 2013, vol. 3, no. 3/4, pp. 1–16.
- [14] S. Gusmeroli, S. Piccione, and D. Rotondi, "A Capability-Based Security Approach to Manage Access Control in the Internet of Things," *Mathematical and Computer Modelling*, 2013, vol. 58, no. 5, pp. 1189–1205.
- [15] A. Westerinen et al., 2001, "Terminology for Policy-Based Management, IETF RFC 3198.

BIOGRAPHIES

DINA HUSSEIN (dina.hussein@orange.com) is currently a research engineer at Orange Labs, France. She received her Ph.D. in computer science in 2015 from Pierre and Marie Curie University – Paris 6 (UPMC) in conjunction with Institut Mines-Telecom, Telecom SudParis, France, where she worked as a research engineer. Her research interests include future-driven network architecture, socially enhanced IoT services, semantic technologies, identity management, and access control in IoT.

EMMANUEL BERTIN (emmanuel.bertin@orange.com) is currently senior architect at Orange Labs, and Orange Expert on Future Networks and Communication Services. He holds a Ph.D. from Paris 6 UPMC University. He has published three books and more than 60 papers in international journals and conferences. He is involved in several Technical Program Committees and recently chaired the 19th Conference on Innovations in Clouds, Internet and Networks (ICIN).

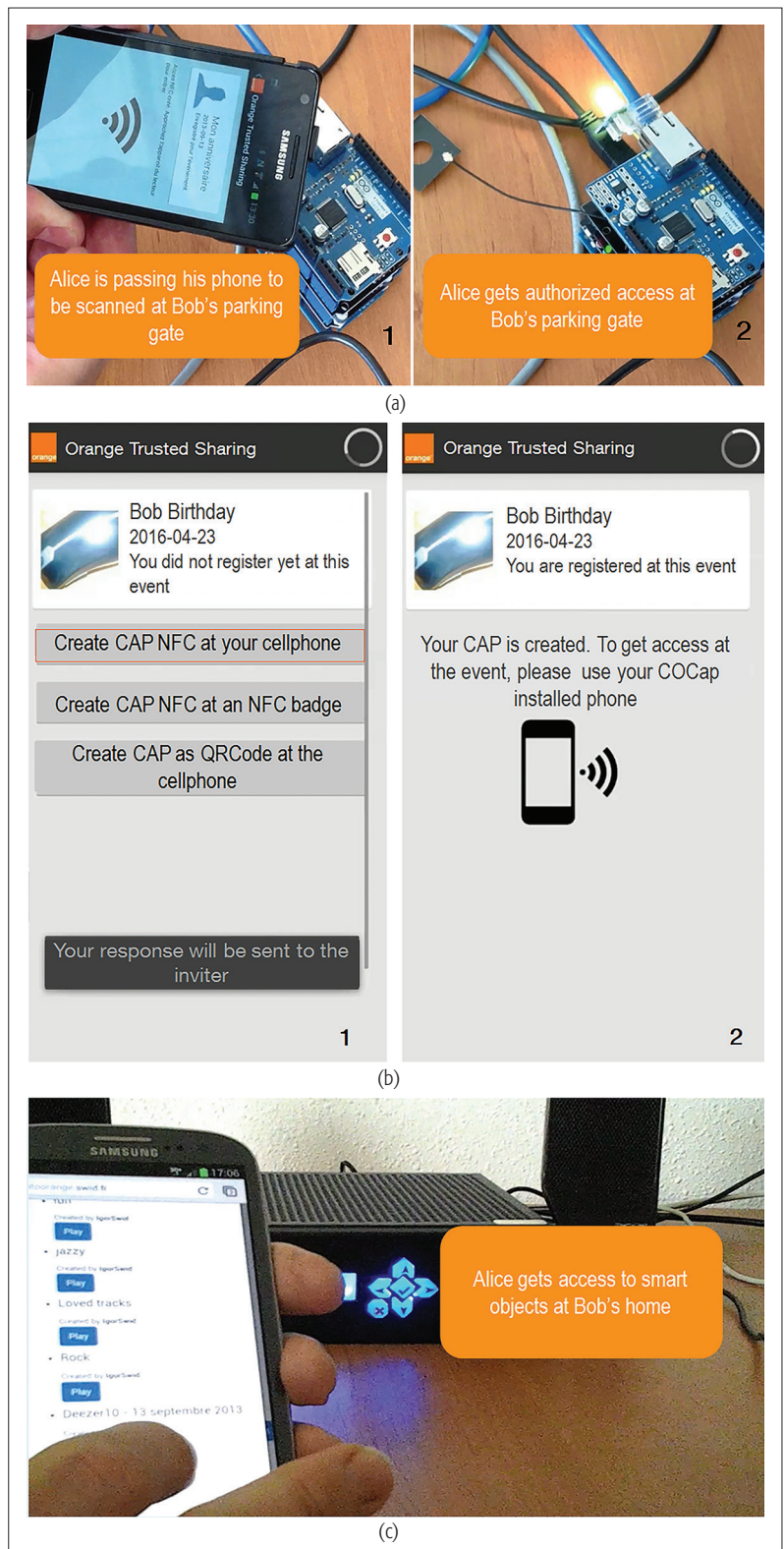


Figure 5. COCapBAC approach: A use case Implementation. a) Alice attempting to get access to Bob's building parking space. b) A CO capability token is successfully created and sent to Alice. c) Alice can use the CO capability token to get access to other objects at Bob's home.

VINCENT FREY (vincent.frey@orange.com) is currently research program manager at Orange Labs. He received an M.Sc. degree from Ecole Centrale Lyon in 1997. Since 2006, he has managed several R&D projects in the field of identity management. Beginning in 2013, he currently manages a research project entitled "Identity-Based Trusted Architecture" in Orange Labs. His expertise focuses on the topics of digital identity, from web-based to network architectures.

NETWORK TESTING AND ANALYTICS



Ying-Dar Lin



Erica Johnson



Irena Atov

Network testing could have a wide spectrum. It is not confined to lab testing with all configurations preset and all results easily reproducible. It could go to field testing with a much larger and even operational network as the testbed. This could also be hybrid testing with parts of the testbed being real and the other parts being emulated or even simulated. Although testers are usually limited to a few engineers or researchers, they could also be crowdsourced volunteers who are ordinary users. As we have expanded our series to include analytics, we are encouraging analytics-based network testing that mines more data and observations from the operational network. After all, if no interesting and useful insights can be found in the test results, network testing and its methodology are not effective enough for the developers of protocols and algorithms.

This March issue has everything mentioned above! We received 13 submissions and accepted four after two rounds of review. The first article reports 4G field testing through 19,000 km of drive test. The second article conducts hybrid testing of 4G high-speed trains where a massive number of UEs and high-speed movement are emulated, but the eNBs are real. Again, the third article resorts to field testing to profile NATs in the wild Internet, but it adopts crowdsourcing to recruit 781 users to run their client program, NATwatcher. The fourth article investigates test gears for traditional lab testing, but it pushes per-flow traffic analyzers one step further by utilizing only off-the-shelf hardware to reach the extreme of 40 Gb/s. All four articles give very good traffic analytics from their testbeds.

Identifying discrepancies between standardized performance requirements and measured results would help to diagnose bottlenecks, define next standards more realistically, and trigger better technology designs. In the first article, "From LTE to 5G for Connected Mobility," M. Lauridsen *et al.* conduct an LTE field drive test in Denmark to measure control and user plane latency, handover execution time, and coverage. Compared to the LTE standard requirements of user-plane latency (20 ms), control-plane latency (100 ms), handover execution time (49.5 ms), and supported maximum coupling loss (140 dB), the measured LTE performance shows excess user-plane latency (averaged 51–121 ms due

to long core network latency), satisfactory control-plane latency (averaged 80–120 ms) and handover execution time (averaged 40 ms), and acceptable coverage of 99 percent with respect to 140 dB. Given that the fifth generation's (5G's) target requirements could be as stringent as 1 ms, 10 ms, 0 ms, and 164 dB, respectively, the authors suggest mechanisms such as semi-persistent scheduling, mobile edge computing, network slicing, make-before-break, multi-cell connectivity, cell densification, and so on.

Packet generators and analyzers fall into the classic research area for network testing. The challenging parts are handling multi-10 Gb/s with per-flow statistics by commercial off-the-shelf (COTS) hardware. In the second article, "Traffic Analysis with Off-the-Shelf Hardware: Challenges and Lessons Learned," M. Trevisan *et al.* are able to achieve 40 Gb/s with a single COTS PC by combining the Intel Data Plane Development Kit (DPDK) and traffic analyzer Tstat into DPDKStat, using state-of-the-art techniques including receiver side scaling queues, schedule deadline, non-uniform memory access (NUMA), and hyper-threading.

Probably no environments besides high-speed trains pose more extreme conditions on 4G systems, where a massive number of onboard UEs have frequent handovers in multiple consecutive groups through a two-hop architecture with onboard mobile relay nodes (MRNs) and roadside eNBs. The in-lab testbed reported in the third article, "Load-Stress Test of Massive Handovers for LTE Two-Hop Architecture in High Speed Trains," by A. Parichehreh *et al.* has emulated UEs, high-speed handovers, and real eNBs. The result shows 70 percent handover success ratio in 600 ms, 40 percent link failure, 90 percent VoLTE call drop ratio, and throughput degradation. But with multi-cell access and directional antenna at MRNs, the performance is improved by three times to a more acceptable range.

Although Network Address Translation (NAT) extended the lifetime of IPv4, various NAT traversal techniques and their different implementations have complicated the peer-to-peer application design where peers are mostly hiding behind NAT. Applications that cannot traverse NATs well would suffer longer latency, which is unsatisfactory for real-time applications such as online gaming. The fourth article,

“NATwatcher: Profiling NATs in the Wild,” by A. Mandalari *et al.* answers what types and distributions of NAT profiles and behaviors exist on the Internet to help peer-to-peer application developers in utilizing various NAT traversal techniques. They resort to crowdsourcing to recruit 781 volunteers scattered around 65 countries and 280 ISPs with NAT products from 120 vendors. The results show that 80 percent of NATs follow standard behavior under 64 percent of tests (11 out of 17), while only 13 percent of NATs follow the standard in the other 36 percent of tests. They also identify the 11 most common NAT configurations.

BIOGRAPHIES

YING-DAR LIN [F] (ydlin@cs.nctu.edu.tw) is a Distinguished Professor at National Chiao Tung University (NCTU) in Taiwan. He received his Ph.D. in Computer Science from UCLA in 1993. He is the director of the Network Benchmarking Lab,

which reviews network products with real traffic and is an approved test lab of the Open Networking Foundation (ONF). He is an IEEE Distinguished Lecturer and ONF Research Associate. He co-authored *Computer Networks: An Open Source Approach* (McGraw-Hill, 2011).

ERICA JOHNSON (erica.johnson@iol.unh.edu) combines business acumen and an in-depth understanding of complex networking technology to direct the University of New Hampshire InterOperability Laboratory (UNH-IOL). In recognition of her ability to drive technical innovation, *Fierce Telecom* named her to the publication's 2011 Women in Wireline. She serves as an IPv6 Ready Logo Regional Officer, IPv6 Forum Fellow, and USGv6 Test Program lead. She received her Bachelor of Computer Science and M.B.A. from the University of New Hampshire in 2001 and 2011, respectively.

IRENA ATOV [SM] (i.atov@ieee.org) received her Ph.D. in electrical engineering from RMIT University, Australia, in 2003. She is currently a principal architect at Microsoft in their Skype for Business Core Engineering Group. Previously, she has worked in academia in both teaching and research roles, consulted for industry through her own company, and worked for Telstra in Melbourne, Australia, as program director of Network Analytics and Resilience. Her research has led to development of several commercial IT software products.

From LTE to 5G for Connected Mobility

Mads Lauridsen, Lucas Chavarría Giménez, Ignacio Rodríguez, Troels B. Sørensen, and Preben Mogensen

The authors measure how current LTE network implementations perform in comparison with the initial LTE requirements. The target is to identify certain key performance indicators that have suboptimal implementations, and therefore lend themselves to careful consideration when designing and standardizing next generation wireless technology. Specifically, they analyze user and control plane latency, handover execution time, and coverage, which are critical parameters for connected mobility use cases such as road vehicle safety and efficiency.

ABSTRACT

Long Term Evolution, the fourth generation of mobile communication technology, has been commercially deployed for about five years. Even though it is continuously updated through new releases, and with LTE Advanced Pro Release 13 being the latest one, the development of the fifth generation has been initiated. In this article, we measure how current LTE network implementations perform in comparison with the initial LTE requirements. The target is to identify certain key performance indicators that have suboptimal implementations and therefore lend themselves to careful consideration when designing and standardizing next generation wireless technology. Specifically, we analyze user and control plane latency, handover execution time, and coverage, which are critical parameters for connected mobility use cases such as road vehicle safety and efficiency. We study the latency, handover execution time, and coverage of four operational LTE networks based on 19,000 km of drive tests covering a mixture of rural, suburban, and urban environments. The measurements have been collected using commercial radio network scanners and measurement smartphones. Even though LTE has low air interface delays, the measurements reveal that core network delays compromise the overall round-trip time design requirement. LTE's break-before-make handover implementation causes a data interruption at each handover of 40 ms at the median level. While this is in compliance with the LTE requirements, and lower values are certainly possible, it is also clear that break-before-make will not be sufficient for connected mobility use cases such as road vehicle safety. Furthermore, the measurements reveal that LTE can provide coverage for 99 percent of the outdoor and road users, but the LTE-M or NarrowBand-IoT upgrades, as of LTE Release 13, are required in combination with other measures to allow for additional penetration losses, such as those experienced in underground parking lots. Based on the observed discrepancies between measured and standardized LTE performance, in terms of latency, handover execution time, and coverage, we conclude the article with a discussion of techniques that need careful consideration for connected mobility in fifth generation mobile communication technology.

INTRODUCTION

The third and fourth generations (3G and 4G) of mobile communication technologies are widely deployed, providing voice and mobile broad-

band as their main services. However, due to the increasing demand for higher data rates and larger system capacity [1], in addition to the emergence of new Internet of Things use cases, the fifth generation (5G) is currently being discussed. 5G is expected to be standardized and deployed in 2018 and 2020, respectively. A key scenario for 5G is connected mobility, which utilizes vehicular communication for such things as infotainment, safety, and efficiency [2]. The two latter uses impose new and challenging requirements in terms of low latency, zero handover interruption time, and ultra-high radio signal reliability [3].

While these requirements are already in the scope of 5G standardization, the ability to meet the requirements in practice is more important than ever in view of the criticality of the safety-oriented connected mobility use cases. These cases rely on vehicular communication for such capabilities as platooning, cooperative awareness, and self-driving cars [2]. In this sense, there is learning to be had from network testing on the already established 4G Long Term Evolution (LTE) infrastructure, to see if the original LTE requirements are met in practice, and if not, evaluate whether the current 5G developments are likely to minimize the gap between requirements and commercial implementation. In this article, we look at the initial design requirements of 4G LTE and the observed performance in terms of user and control plane latency and LTE handover execution time. In view of this, we discuss how 5G may be designed to address the latency and handover requirements of connected mobility use cases such as vehicular communication for safety and efficiency. Our analysis is based on an extensive measurement campaign of LTE performance in four cellular networks in Northern Jutland, Denmark. The campaign included 19,000 km of drive test with commercial radio network scanners and specialized measurement smartphones. Furthermore, we use the measurements to calibrate a radio wave propagation tool to study radio coverage, because it is a prerequisite for good latency and handover performance.

The LTE latency and handover performance has previously been studied, for example, in [4–7]. However, the scope of our measurement campaign in terms of number of studied operators, network configurations and topologies, device speeds, and scenario areas is unprecedented to the best of our knowledge. Specifically, we study four commercial operators covering both rural, urban, and suburban areas, totaling 19,000 km of drive test at speeds from 30 to 130 km/h

using specialized measurement smartphones, which provide information on not only application layer performance but also radio resource control (RRC) messages. This is a significant statistical improvement compared to [4], which is based on three days of measurements in a single, lightly loaded, urban network with line-of-sight connection, and [5], which is based on 35 km of urban drive test, and [6], which is based on field trials, where the core network (CN) was located close to the trial area to reduce the latency. The report [7] relies on data collected in the Nordic countries from 22,000 users via a smartphone application in January through March 2016, but it only provides information on data rates and user plane latency. Therefore, the statistical representation of our measurement data and the availability of network parameters ensures a solid comparison with the design requirements, enabling us to identify any discrepancies.

The article is structured as follows. First, we describe the extensive measurement campaign. Then the latency and handover performance observations are presented. Next, we present the LTE coverage and discuss how it can be extended. Then we identify discrepancies and areas for improvement by comparing the LTE requirements with the observed performance, and discuss how the 5G development can address these issues.

MEASUREMENT CAMPAIGN

The extensive measurement campaign was conducted in the region of Northern Jutland in Denmark. The region has about 585,000 inhabitants over an area of 8000 km². A large part of the region is rural area with small villages and farmland, and only few larger cities with population size in the 10–20,000 range and one major city of 130,000 inhabitants. The wireless infrastructure in the region is well developed. As was revealed in the measurement campaign, at least one operator provides all technologies over the full region. If two operators are required for 3G/4G coverage, about 60 small areas (of 0.5–4 km radius) experience limited or no coverage.

The drive test measurements were made using two cars covering about 19,000 km of city roads, rural roads, and highways within the region, and therefore includes measurements in the range of 30–130 km/h. During the drive test, samples of received signal power, data rate, round-trip time (RTT), and radio access network (RAN) specific parameters were collected simultaneously for the four main operators in Denmark. The road coverage, based on more than half a million collected data points, is illustrated in Fig. 1. The measurements were made during the daytime Monday through Friday in the period from November 2015 to May 2016. Note that the status of the four networks may have changed during the long measurement campaign, in terms of both deployed base stations and equipment, but also in terms of number of users and network load. However, this information is not publicly available; therefore, the measurement campaign reflects the performance at the specific time of measurement.

Each car, moving according to local traffic rules, was equipped with a roof box containing a Rohde & Schwarz FreeRider III system. The

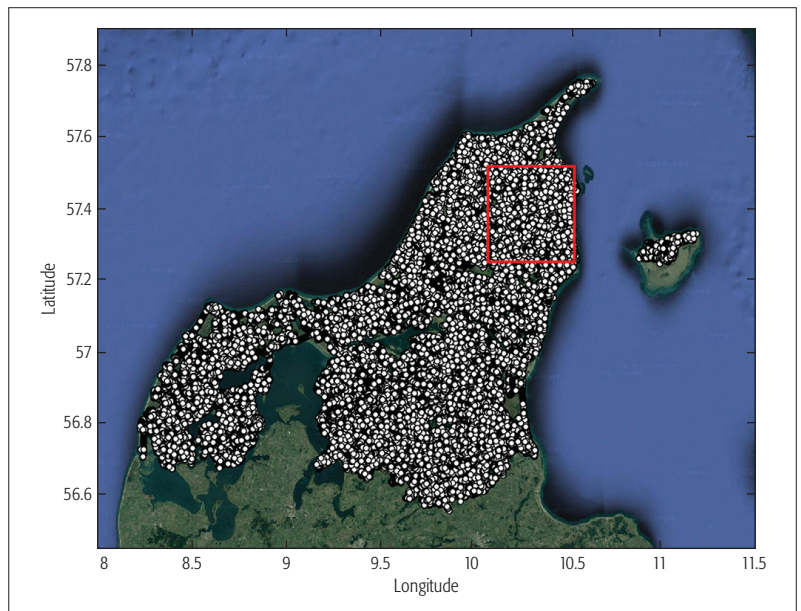


Figure 1. Overview of measurement locations in Northern Jutland. The red rectangle indicates the area that is examined in the coverage study.

system consists of four Samsung Galaxy S5 Plus smartphones, running specialized QualiPoc measurement software, and a TSME radio network scanner. The smartphones reflect the user experienced performance and, in addition, are able to record relevant network parameters such as RRC messages. Each phone was connected to one of the four main mobile network operators of Denmark using either 3G or 4G depending on the current signal levels and operator traffic steering policies, while the scanner passively monitored the allocated frequency bands for 2G, 3G, and 4G communication from 700 MHz to 2.7 GHz. We only report results for 4G in this work. The smartphones and the scanner measured the received signal power from the serving cell and all observable neighbor cells, respectively. The scanner was equipped with an external, omnidirectional Laird TRA6927M3NB-001 antenna, which was mounted in the roof box on a separate ground plane. In addition, the position was logged per measurement sample via GPS and used to generate averages of the received signal power over 50 m road segments.

Each smartphone continuously performed a series of data measurements consisting of four fixed duration FTP transfers in uplink and downlink (alternating link directions, i.e., eight transfers in total), each 20 s long, to estimate the broadband coverage. The FTP transfers were followed by a 10 s idle period and preceded by two ping measurements occurring with 1 s separation. The ping and FTP measurements were made toward a server located at Aalborg University (AAU). The server was connected via 10 Gb/s fiber to the Danish Research Network, which is connected to the Danish Internet Exchange Point via another 10 Gb/s fiber, and thus the link between the Internet and the server is expected to have minimal impact on the measurements. Ping measurements made from a computer located at AAU toward the server, passing through the Danish Research Network, result in average RTTs of 7.5 ms with a standard

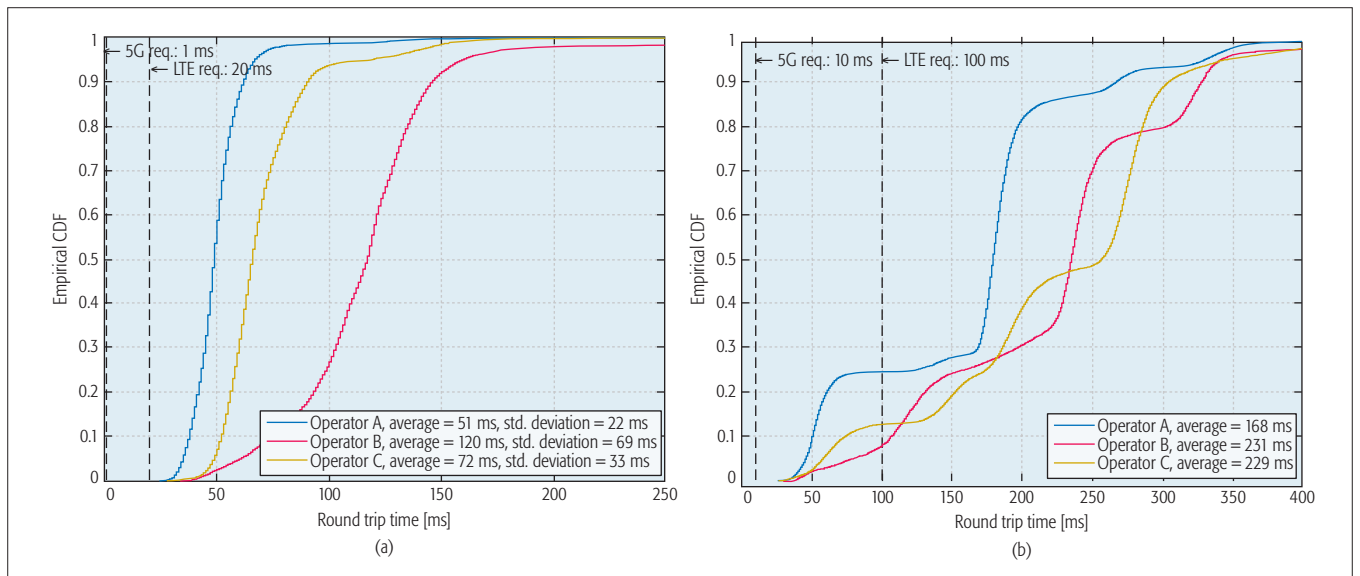


Figure 3. The LTE ping measurement results. Note the AAU server RTT is 7.5 ms, which must be added to the LTE requirement line for result interpretation: a) CDF of ping 2 – user plane latency; b) CDF of ping 1 – control plane latency.

HANDOVER EXECUTION PERFORMANCE

LTE implements break-before-make handover, where the UE breaks data exchange with the serving cell before establishing a connection toward the target cell. As a result, the UE experiences a service interruption at each handover for a short period of time. Upon reception of the handover command or the RRC Connection Reconfiguration message, which includes the mobility control information [9], the UE proceeds to reconfigure layers 2 and 3, terminating any data exchange with the network. Afterward, it performs radio frequency retuning and attempts RA toward the target cell. When completed, the UE sends the RRC Connection Reconfiguration Complete message to confirm the handover, informing the target cell that the data flow can be restored. The stage that encloses the procedures between both RRC messages is called handover execution [6]. In order to detect problems during handover execution, the UE initiates timer T_{304} after receiving the handover command. If the MAC layer successfully completes the RA procedure, the UE stops the timer. However, if timer T_{304} expires before the handover has been completed, a handover failure is declared, and the UE shall perform connection re-establishment [9].

Ideally, the time it takes to perform the handover execution is a lower-bound of the handover service interruption time. In practice, there are additional delays such as UE and eNB processing times and propagation delays that may increase the overall service interruption. Current Third Generation Partnership Project (3GPP) studies on LTE latency report a typical handover execution time of 49.5 ms [10], while the International Telecommunication Union (ITU) target is 30–60 ms [8].

The QualiPoc measurement smartphones collect the RRC signaling exchanged with the network. Therefore, the handover execution time is determined by analyzing the timestamp of the RRC messages at each handover. Figure 4 depicts the CDF of the handover execution times measured on each of the analyzed networks. The

number of registered handovers differ between networks: 161,313, 46,517, and 148,011 handovers for operator A, B, and C, respectively. However, the measured handover execution times are similar across them. As illustrated in Fig. 4, the extracted times are below 75 ms in 90 percent of the cases with a median value of approximately 40 ms, which is in line with the expected typical value of 49.5 ms reported by the 3GPP [10] and the 30–60 ms target of ITU [8]. The average handover execution time is reported to be 30 ms in [5], but the measurement only covers 35 km of urban drive test. Similarly, [6] reports average times around 25 ms, but for a field trial where the CN was located close to the trial area.

Figure 4 also illustrates handover execution times larger than 200 ms, and some are due to unsuccessful handovers (approximately 1 percent of the total number of samples). In these cases, a handover failure is declared, and the connection re-establishment increases the data interruption time up to several seconds. These extreme values show that the LTE handover execution with a break-before-make implementation may become an issue for the safety-critical connected mobility use cases with stringent latency requirements.

COVERAGE PERFORMANCE

The requested latency and handover performance cannot be achieved without sufficient radio coverage. As mentioned earlier, the 4G coverage is good in the region, but since the measurements are performed as drive tests, they only indicate road coverage. However, the connected mobility use cases focused on vehicular communication for safety and efficiency also require indoor coverage, for example, for underground parking lots and integral garages. Therefore, the extensive measurement campaign was used for calibration of a radio wave propagation tool in order to estimate the received signal power for a selected rural area of the region. The area under study is approximately 800 km² and is based on a local operator's commercial deployment of 71 eNB sectors operating in LTE band 20 (~ 800 MHz).

The area is illustrated with a red rectangle in Fig. 1. An elevation map, obtained from Kortforsyningen [11], is imported to account for terrain variations and combined with a log-normal shadow fading of 8.7 dB variance, which was estimated using the received power values from the measurement campaign. The area is divided into 50×50 m pixels, and the coupling loss is then determined between each pixel and the 71 eNB sectors. The coverage is evaluated for different user groups, which are assigned to specific pixels based on public database information. The first set is outdoor users, located in pixels that contain a house number based on Open Street Map, and road users, located in pixels that contain a road segment [11]. The other group consists of indoor users, which are also identified by house numbers. The indoor users are divided into 3 subgroups, experiencing 10, 20, and 30 dB penetration loss in addition to the observed coupling loss. The indoor groups are generated to study a

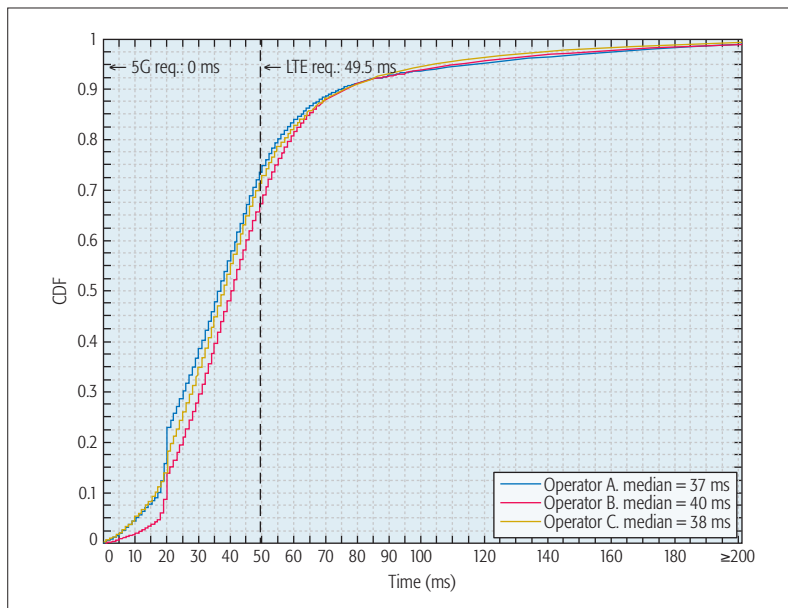


Figure 4. CDF of the handover execution time measured during the drive tests for each operator.

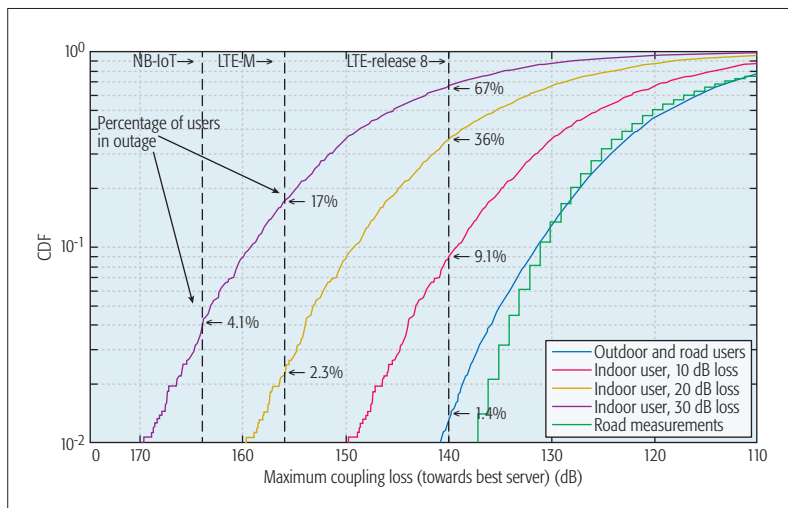


Figure 5. Coverage performance for LTE, LTE-M, and NB-IoT. Based on Fig. 3 of [11].

light indoor scenario, where, for example, a user is located close to a window and thus only experiences 10 dB additional loss, and deep indoor scenarios, where, for example, a user is located in a basement such as an underground parking lot and therefore suffers 20–30 dB additional loss [12]. For further details on the simulation setup refer to [11].

Figure 5 shows the coupling loss between the UE and the serving cell, which is selected based on the strongest received signal. The three dashed vertical lines indicate the supported maximum coupling loss (MCL) for LTE Release 8 (140 dB), LTE-M Release 13 (156 dB), and Narrowband Internet of Things (NB-IoT) Release 13 (164 dB) [13]. The two latter technologies achieve higher MCL by applying repetitions in time (at the cost of latency!) and power spectral density boosting in smaller transmission bandwidths of 1.4 MHz for LTE-M and 200 kHz for NB-IoT. Note that NB-IoT does not apply handovers, but only cell reselection. Figure 5 also contains road measurements obtained in the area indicated by the red rectangle in Fig. 1. The curve shows a good fit with the simulation of outdoor and road users, and the minor difference is attributed to remote houses in the area that are located far from the road measurements.

The results in Fig. 5 indicate that LTE Release 8 provides sufficient coverage for 99 percent of the outdoor and road users. If indoor coverage is needed LTE Release 8 provides coverage for only approximately 90 percent of light indoor users, experiencing 10 dB additional penetration loss. For deep indoor users, NB-IoT is required and can provide coverage for about 95 percent of the users. However, for most of the safety and efficiency use cases, outdoor and road users can rely on LTE Release 8, and thus also benefit from the larger bandwidth and lower latency of this technology.

ENABLING CONNECTED MOBILITY IN 5G

The connected mobility use cases, focused on road vehicle safety and efficiency, demand low latency, high reliability, and zero handover execution time [2, 3]. These parameters were also defined for LTE, but using different values since mobile broadband and voice applications were mainly targeted. In Table 1 the LTE requirements are compared to the results of the extensive measurement campaign, which represents what is achievable in commercially deployed networks. In addition, the current 5G targets are listed together with highlights of ongoing 5G research on how the mobile communication system can improve compared to LTE and address the discrepancies between standardized and measured performance. These comparisons are important in order not to experience similar performance discrepancies when 5G is deployed.

The measured LTE user plane latency (Fig. 3a) is significantly higher than the 20 ms target [8] for all operators. However, the key observation is that there is an even larger difference (51 vs. 121 ms) between two operators. Since the air interface is the same and assumed to have comparable loads, it is clear that RAN setup, routing, and CN architecture have a major impact on user

Parameter	LTE requirement	Measured LTE performance	5G target	Potential techniques
User plane latency (RTT)	20 ms	Average: A: 51 ms, B: 121 ms, C: 72 ms. Even the users in the best radio signal conditions are affected by long core network latency.	1 ms	Semi-persistent scheduling and combining of requests and data, processing time reduction, shorter TTIs, mobile edge computing, network slicing
Control plane latency (idle-to-active time)	100 ms	A and B require 120 ms, while C completes in 80 ms. Subsequent access attempts are delayed by long system information block periods.	10 ms	Optimized random access and security setup, periodicity of system information blocks, network slicing, and mobile edge computing
Handover execution time	49.5 ms	Similar median LTE values for all the operators of ~40 ms	0 ms	Make-before-break, multi-cell connectivity, UE autonomous cell management, synchronized handover
Supported maximum coupling loss	140 dB	LTE Release 8 provides coverage for 99 percent of the outdoor and road users in the rural area under study.	164 dB	Micro and macro diversity, TTI bundling, cell densification, power spectral density boosting

Table 1. Comparison of requirements, measured performance, and potential techniques for improvement.

plane latency. When designing 5G, it is therefore important to minimize the probability and impact of poor RAN and CN implementations on the envisioned new and optimized air interface. In addition, 5G research is targeting reduction of the user plane latency to 1 ms, [3] by use of shorter transmit time intervals (TTIs), bundling of scheduling request and data, decreased processing times obtained due to technology improvements, and potentially semi-persistent scheduling. Fortunately, work is also ongoing to optimize the RAN and CN. For example, the use of mobile edge computing, where processing and decision making are moved toward the eNB, is studied. Moreover, the 5G network is expected to rely on flexible slicing of the RAN and CN, and splitting of tasks between edge and central clouds to accommodate the requirements of the different use cases [14].

The control plane latency of LTE was targeted to be 100 ms or less [8], and one operator fulfills this, achieving 80 ms on average, while the two other operators require approximately 120 ms, as illustrated in Fig. 3b. However, subsequent access attempts are delayed significantly due to the 80 ms or higher periodicity of the system information blocks, which provide the information the UE needs in order to access the network. The 5G target is 10 ms, [3], and therefore the required access information must occur more frequently, at the cost of increased control overhead. Additionally, work is ongoing to develop new RA and registration methods to enable the UE to connect faster and with more consistent performance. The control plane latency will also benefit from the use of network slicing, for example, by applying faster RA schemes to time-critical applications, and using different control channel modulation and coding schemes for different applications as well as mobile edge computing, for example, by letting the eNB handle some of the tasks currently performed by the mobility management entity in LTE.

The LTE handover execution time target is 49.5 ms [10]. The measurement results in Fig. 4 show that the operators on average fulfill this target with a median of 40 ms. However, a radio link failure occurs in approximately 1 percent of the

measurements, and the subsequent connection re-establishment procedure extends the handover execution time to several seconds. The connected mobility use cases targeting safety and efficiency require 5G to provide zero service interruption time; therefore, a significant amount of work is needed in this area [3]. One proposed solution is to apply make-before-break connectivity where the UE connects to the target cell before disconnecting from the serving cell. In 5G this may be expanded to multiple connections due to the expected use of multi-cell connectivity. The cost is increased UE complexity and simultaneous utilization of resources in multiple cells. This concept is similar to the Dual Connectivity Split Bearer Architecture of LTE, which potentially can be combined with UE autonomous cell management. The latter concept allows the UE to autonomously add and release different radio links, reducing the control signaling overhead. Finally, 5G may also utilize synchronized handover, which is a random access-less procedure where the synchronized UE and cells agree on when the handover shall occur.

The supported MCL of a mobile communication system defines the radio signal availability together with the network deployment and load. The LTE Release 8 MCL is 140 dB, and the calibrated simulation in Fig. 5 of a rural area showed that a commercially deployed network would provide coverage for approximately 99 percent of the outdoor and road users. However, the connected mobility use cases focused on safety must also work in deep indoor scenarios such as underground parking lots with higher coupling loss [12]. Therefore, a certain slice of 5G must support a higher MCL, potentially similar to the 164 dB of NB-IoT. Similar to NB-IoT the 5G design can thus rely on TTI bundling, that is, repetitions of transmissions in the time domain, which, however, will harm the latency, and use of power spectral density boosting, which may harm the signal-to-interference ratio of other users. Therefore, 5G will preferably utilize the expected network of ultra-dense small cells, macrocell densification, and micro and macro diversity to improve the received signal power and reliability [15].

The LTE handover execution time requirements and observed performance are similar, but since the connected mobility use cases targeting safety and efficiency require zero service interruption time, the 5G design must utilize new mobility methods such as make-before-break, multi-cell-connectivity and synchronized handovers.

CONCLUSION

In this study we examined the performance of four LTE operators in an extensive measurement campaign of 19,000 drive test kilometers. The goal was to identify gaps between LTE requirements and achievable performance in order to avoid similar discrepancies when 5G is standardized and deployed. The 5G will be able to support connected mobility use cases focused on vehicular communication for road safety and efficiency, but improvements are needed in the areas of user and control plane latency, handover execution time, and radio signal availability.

The LTE user plane latency is observed to be twice as long as the requirement due to core network latencies, and thus diminishes the effect of an optimized air interface. For 5G it will be of key importance that the operators focus on the latency of the core architecture in order to achieve the 1 ms RTT target. The studied networks roughly achieve the LTE control plane latency requirement, but since 5G requires it to be 10 times lower the amount of random access, connection and security setup signaling must be reduced. For both latency targets the use of mobile edge computing and network slicing will be beneficial.

The LTE handover execution time requirements and observed performance are similar, but since the connected mobility use cases targeting safety and efficiency require zero service interruption time, the 5G design must utilize new mobility methods such as make-before-break, multi-cell-connectivity, and synchronized hand-overs.

The simulated LTE outdoor and road coverage is sufficient for 99 percent of the users, but in order to ensure the connected mobility operation, it is suggested that 5G target a significant cell densification and use of macro and micro diversity to improve the radio signal availability.

ACKNOWLEDGMENT

The authors would like to thank the reviewers and the Editor-in-Chief for their useful comments. Furthermore, the authors would like to thank Business Region North Denmark for providing access to the measurement data. The work was partly funded by Innovation Fund Denmark.

REFERENCES

- [1] Cisco, "Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020," white paper, 2016.
- [2] 5G Infrastructure Public Private Partnership, "5G Automotive Vision," white paper, 2015.
- [3] 3GPP, "Study on Scenarios and Requirements for Next Generation Access Technologies," TR 38.913 V0.3.0, Mar. 2016.
- [4] M. Laner et al., "A Comparison Between One-Way Delays in Operating HSPA and LTE Networks," *Proc. 2012 10th Int'l. Symposium Modeling Optimization Mobile, Ad Hoc and Wireless Networks*, May 2012, pp. 286–92.
- [5] A. Elnashar and M. A. El-Saidny, "Looking at LTE in Practice: A Performance Analysis of the LTE System Based on Field Test Results," *IEEE Vehicular Technology Mag.*, vol. 8, no. 3, Sept. 2013, pp. 81–92.
- [6] H. Holma and A. Toskala, *LTE for UMTS – Evolution to LTE-Advanced, 2nd ed.*, Wiley, 2011.

- [7] Open Signal, "State of Mobile Networks: Nordics," May 2016, report; <https://opensignal.com/reports/2016/05/nordic/state-of-the-mobile-network/>, accessed Dec. 12, 2016.
- [8] ITU-R M.2134, "Requirements Related to Technical Performance for IMT-Advanced Radio Interface(s)," Nov. 2008.
- [9] 3GPP, "Radio Resource Control Protocol Specification," TR 36.331 V13.1.0, Apr. 2016.
- [10] 3GPP, "Study on Latency Reduction Techniques for LTE," TR 36.881 V14.0.0, June 2016.
- [11] M. Lauridsen et al., "Coverage and Capacity Analysis of LTE-M and NB-IoT in a Rural Area," *Proc. IEEE VTC-Fall 2016*, Sept. 2016, pp. 1–5.
- [12] H.C. Nguyen et al., "A Simple Statistical Signal Loss Model for Deep Underground Garage," *Proc. IEEE VTC-Fall 2016*, Sept. 2016, pp. 1–5.
- [13] Nokia, "LTE-M – Optimizing LTE for the Internet of Things," white paper, 2015.
- [14] A. Colazzo, R. Ferrari, and R. Lambiasi, "Achieving Low-Latency Communication in Future Wireless Networks: The 5G NORMA Approach," *Euro. Conf. Networks and Commun.*, June 2016, pp. 1–5.
- [15] G. Pocovi et al., "Signal Quality Outage Analysis for Ultra-Reliable Communications in Cellular Networks," *Proc. IEEE GLOBECOM Wksp.*, Dec. 2015, pp. 1–6.

BIOGRAPHIES

MADS LAURIDSEN (ml@es.aau.dk) received his M.Sc. in electrical engineering and Ph.D. from Aalborg University in 2009 and 2015, respectively. He is currently an Industrial PostDoc in Nokia Bell Labs Aalborg and in the Wireless Communication Networks section of the Department of Electronic Systems at Aalborg University. His research interests include massive machine-type communication and ultra reliable low latency communication for current wireless networks and future 5G.

LUCAS CHAVARRÍA GIMÉNEZ obtained his M.Sc. degree in mobile communications from Aalborg University in 2011. From 2012 to 2014, he was employed as a research assistant at the Radio Access Technology (RATE) Section of the Department of Electronic Systems at Aalborg University. He is currently pursuing a Ph.D. degree in wireless communications within the Wireless Communication Networks (WCN) section of the Department of Electronic Systems of Aalborg University, in collaboration with Nokia-Bell Labs. His current research activities and interests include the development of mobility management solutions for the next generation of mobile networks.

IGNACIO RODRIGUEZ holds a five-year degree (B.Sc.+M.Sc) in telecommunication engineering from the University of Oviedo, Spain. He received his M.Sc. degree in mobile communications and Ph.D. degree in wireless communications from Aalborg University in 2011 and 2016, respectively. He is currently working as a postdoctoral researcher at the same institution, and his research interests are mainly related to radio propagation, channel modeling, radio network planning and optimization, M2M, ultra-reliable and low-latency communications, and industrial IoT.

TROELS B. SØRENSEN received his Ph.D. degree in wireless communications from Aalborg University in 2002. Upon completing his M.Sc. degree in electrical engineering in 1990, he worked with a Danish telecom operator developing type approval test methods. Since 1997 he has been at Aalborg University, where he is now an associate professor in the WCN section. His current research and teaching activities include cellular network performance and evolution, radio resource management, and related experimental activities.

PREBEN MOGENSEN received his M.Sc. and Ph.D. degrees from Aalborg University in 1988 and 1996, respectively. Since 2000, he has been a professor at Aalborg University and now leads the WCN section. He has co-authored more than 400 papers in various domains of wireless communication. Since 1995 he has also been associated part time with Nokia, currently as a principal engineer at Nokia-Bell Labs Aalborg. He became a Bell Labs fellow in 2016. His current research focus is on 5G, IoT, and ultra-reliable low latency communication for CPS.

Traffic Analysis with Off-the-Shelf Hardware: Challenges and Lessons Learned

Martino Trevisan, Alessandro Finamore, Marco Mellia, Maurizio Munafò, and Dario Rossi

ABSTRACT

In recent years, the progress in both hardware and software allows user-space applications to capture packets at 10 Gb/s line rate or more, with cheap COTS hardware. However, processing packets at such rates with software is still far from being trivial. In the literature, this challenge has been extensively studied for network intrusion detection systems, where per-packet operations are easy to parallelize with support of hardware acceleration. Conversely, the scalability of statistical traffic analyzers (STAs) is intrinsically complicated by the need to track per-flow state to collect statistics. This challenge has received less attention so far, and it is the focus of this work. We present and discuss design choices to enable a STA to collect hundreds of per-flow metrics at a multi-10-Gb/s line rate. We leverage a handful of hardware advancements proposed over the last years (e.g., RSS queues, NUMA architecture), and we provide insights on the trade-offs they imply when combined with state-of-the-art packet capture libraries and the multi-process paradigm. We outline the principles to design an optimized STA, and we implement them to engineer DPDKStat, a solution combining the Intel DPDK framework with the traffic analyzer Tstat. Using traces collected from real networks, we demonstrate that DPDKStat achieves 40 Gb/s of aggregated rate with a single COTS PC.

INTRODUCTION

The last years have witnessed a growing interest in solutions for Internet packet processing. The engineering of such systems is a far from trivial challenge. In fact, while Internet services are becoming more and more complex and require more processing power to monitor them, Moore's law scales at a slower pace compared to the annual bandwidth consumption rate. Traffic monitoring requires the acquisition, movement, and processing of *packets*, while maintaining their logical organization in *flows*. These are daunting tasks to tackle at 10 Gb/s line rate or more, where each packet lasts a few tens of a nanosecond. Engineering a software monitoring solution on common off-the-shelf (COTS) hardware requires a lot of ingenuity.

The advent of optimized packet acquisition libraries and ad hoc hardware solutions allevi-

ated the problem of mere packet acquisition. These solutions indeed allow the system to capture packets at 10 Gb/s line rate thanks to zero-copy, that is, moving packets via direct memory access (DMA) from the network interface controller (NIC) directly into user-space. The challenge becomes how to speed up the processing of such a deluge of data. Software developers have explored multi-core CPUs, graphical processing units (GPUs), network processing units (NPUs), and field programmable gate array (FPGA) architectures. This is testified by seminal [1] and more recent works [2–4] successfully scaling and optimizing multi-core network intrusion detection systems (NIDSs), where a large set of rules have to be checked on a per-packet base. Fewer efforts have been devoted to the area of statistical traffic analyzers (STAs), which instead aim to collect both basic statistics, for example, TCP round-trip time (RTT) or packet loss events, and more articulated indices (e.g., performance of video streaming applications). STAs normally imply keeping per-flow state; hence, they are inherently more difficult to scale than NIDSs.

In this work, we report on our experience in designing and engineering DPDKStat, a system combining the Intel DPDK framework for packet acquisition, and the traffic analyzer Tstat [5], a STA that offers a large number of per-flow metrics extracted in real time, processing IP packets, TCP segments, and application payload. We do not aim to present another fancy traffic monitoring tool. Conversely, we discuss *system bottlenecks* and *design principles* to overcome them. We evaluate DPDKStat performance using real traces collected when running on COTS PCs costing less than US\$4000. Overall, DPDKStat achieves 40 Gb/s thanks to careful engineering of the trade-offs behind packet acquisition, the multi-process paradigm, and non-uniform memory access (NUMA) architectures.

In this work we focus on the lessons learned, dissecting the most important design choices. Summarizing, our major contributions are:

- We investigate packet acquisition policies that guarantee consistent per-flow load balancing, limit timestamp errors, and avoid packet reordering and losses.
- We evaluate different design choices with traces that capture workloads representative of real scenarios.

The authors present and discuss design choices to enable a STA to collect hundreds of per-flow metrics at a multi 10Gb/s line rate. They leverage a handful of hardware advancements proposed over the last years (e.g., RSS queues, NUMA architecture), and they provide insights on the trade-offs they imply when combined with state of the art packet capture libraries and multi-process paradigm.

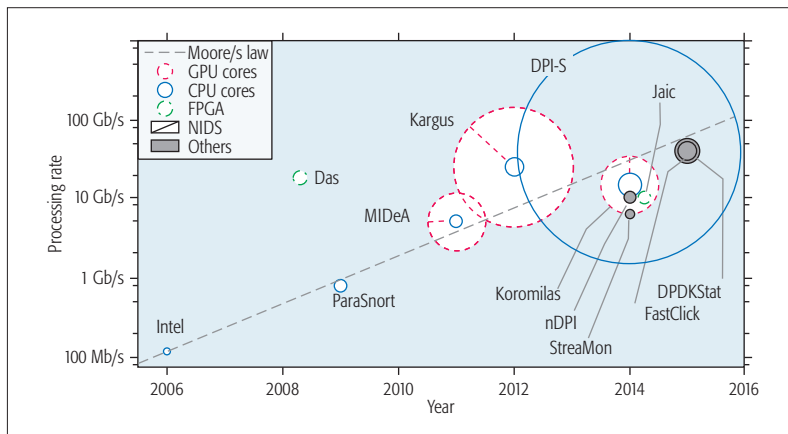


Figure 1. Synoptic of related works. Circles are centered on the year and processing rate. Radius size is a logarithmic scaling of the number of cores employed by the system.

- We quantify benefits of periodic packet acquisition via `SCHED_DEADLINE` (+85 percent), hyper-threading (+20–30 percent), and load balancing across CPUs (+10 percent).

We make available to the community both DPDKStat and the traffic generator used in our testbed (<http://tstat.polito.it/viewvc/software/tstat/branches/tstat-dpdk/README.html?view=co>, accessed 12/13/2016). The interested reader can also find more fine-grained discussions in [6].

10 YEARS OF HIGH-SPEED TRAFFIC PROCESSING

Both academia and industry have invested great effort in designing efficient high-speed Internet traffic processing systems. Since seminal work able to cope with only a few hundred megabits per second, different solutions passed the 10 Gb/s barrier. This is mostly thanks to the advanced packet capture libraries (compared and benchmarked in [7]) which solve the first engineering challenge: efficiently transfer packets from the NIC to the main memory. Some works also address the problem of efficiently storing packets on disks using COTS for later processing [8]. The challenge then becomes how to process packets in user-space, which is usually addressed using multi-threading technologies on multicore hardware.

For the sake of illustration, in Fig. 1 we represent the most important solutions as circles centered at (rate, year) with a radius proportional to the number of cores used. A straight line (in semi-log scale) represents the Moore's law exponential increase of raw processing rate, doubling every year from the initial starting point of 100 Mb/s. Comparison with old systems such as Intel or ParaSnort, is only anecdotal (<http://courses.csail.mit.edu/6.846/handouts/H11-packet-processing-white-paper.pdf>, accessed 12/13/2016). Specifically, in 2015, the processing rate speedup is close to 210 (26) with respect to the 2006 Intel system (2009 ParaSnort), well matching Moore's expectations.

Most of the works in Fig. 1 focus on NIDS (empty circles), that is, Bro or Suricata based solutions [9]. These tools are designed to trigger

alarms when packets match signatures from a predefined dictionary, and compute few statistics about the traffic itself. They work on a *per-packet* basis, using simple state machines, and are easily amenable to parallelization. However, since pattern matching is costly (e.g., a core can cope with only ~100 Mb/s), scalability is achieved with a large number of CPU or GPU cores, as in the case of MIDeA and Kargus [2], with NPUs as in Koromilas [4] and DPI-S [3], or finally, with FPGAs as in Das [10] and Jaic [11].

Figure 1 includes solutions that, despite not being STAs, are not pure NIDS either. Specifically, StreaMon [12] is a software defined network (SDN) traffic monitoring framework, FastClick [7] is an advanced software router based on Click, while nDPI [13] is a pure traffic classifier derived from OpenDPI.

To the best of our knowledge, less effort has been devoted to study scalability for STAs (filled circles in Fig. 2). These latter tools offer a smaller, yet more varied, set of functions intrinsically more difficult to parallelize than NIDS. In fact, STAs entail *per-flow* state, leading to a typically pipelined analysis workflow. To exemplify the differences between STAs and NIDSs, Fig. 2 compares processing time, maximum memory, I/O rate, and average CPU utilization when Tstat (a STA) and three NIDSs (Bro, Snort, and Suricata) process the same trace, on the same hardware, with default configurations. Tstat is faster than the other tools, but generates a lot of I/O since it logs hundreds of per-flow metrics. Notice how, despite tracking per-flow states, Tstat consumes less memory than Bro since it does not reassemble IP fragments and TCP segments.

In this simple experiment, a single CPU core is used, which is insufficient to achieve multi-10-Gb/s without parallelization. In the remainder of this work, we specifically dissect the design choices and the lessons learned to achieve this goal.

DESIGN PRINCIPLES

We assume that the STAs runs on COTS hardware which is equipped with n NICs, and c CPU cores. Notice that two NICs are required for each single full-duplex link. To cope with the load, the application needs to balance the traffic among different processing engines that are bound to different CPU cores. Figure 3 shows the different choices to be considered.

PACKET ACQUISITION AND PER-FLOW LOAD BALANCING

Goal: Several solutions have been proposed to provide efficient packet acquisition on COTS hardware. They all solve the problem of efficiently moving packets from the NICs to user-space [7, 8]. However, to compute per-flow statistics, we need to correlate packets received irrespective of the NIC where the packets are observed. Hence, the packet acquisition library needs to offer a *flow-preserving load balancing function* for correct traffic processing. This also offers the appealing opportunity to split the traffic among the c CPUs. The primary goal is to avoid costly synchronization primitives.

Proposal: The first proposal considers *load balancing in software* (Fig. 3a). This is offered by solutions such as PF_RING ZC where custom per-packet load balancing can be coded

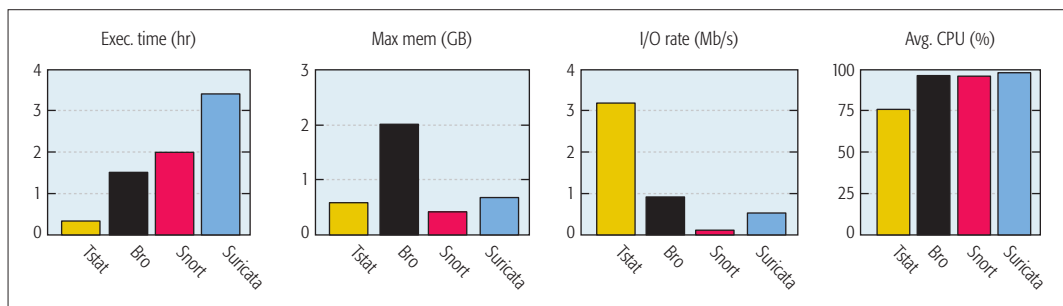


Figure 2. STA and NIDS performance comparison (1-core, all tools with default configuration).

and applied on the aggregate traffic received from the so called DNA cluster, that is, a group of NICs (<http://www.ntop.org/products/packet-capture/pfring/pfring-zc-zero-copy/>, accessed 12/13/2016). In this case, all packets received from the NICs are passed to the DNA cluster process, which timestamps and forwards them to the correct processing engine. Unfortunately, this solution does not scale as the software load balancer becomes the bottleneck, and it is non-optimal in multi-CPU scenarios where the same packet should be moved across the NUMA nodes of the system.

Modern NICs offer *load balancing in hardware*, for example, via the Intel Receiver Side Scaling (RSS) queues. Consistent per-flow load balancing is possible with specific hashing functions [14] offloaded to the NIC. This results in a system where packets are stored into different RSS queues to which the STA has direct access. In this scenario, the number of RSS queues is equal to the number of CPU cores (Fig. 3b).

Offloading function to hardware presents clear benefits, but the RSS technology suffers from some limitations. For instance, the load balancing is performed only on IP packets encapsulated directly over Ethernet, excluding other layer 2 and tunneling protocols (MPLS, GRE tunnels, etc.). RSS queues are also a scarce resource (currently, at maximum 16 for each NIC), and they require careful tuning, which we explore later.

ABSORBING TRAFFIC AND PROCESSING JITTER

Goal: Packet processing time is not constant. Traffic processing applications are engineered to minimize the average packet processing time. However, unexpected (large) processing delays typically occur, including due to slow I/O operations, periodic cleaning of data structure, critical packet composition, and so on. These delays lead eventually to packet losses in the RSS queues since they can only store up to 4096 packets, that is, few tens of microseconds at ~ 10 Gb/s. Similarly, unexpected or unbalanced traffic bursts can lead to losses too. Packet acquisition libraries already implement circular buffers to absorb such jitter. However, those are in the range of 1 MB and can only absorb less than 1 ms worth of traffic at 10 Gb/s.

Proposal: Our solution is to decouple each analysis module using a *large buffer* (Fig. 3c). For instance, 1 GB is sufficient to store approximately 1 s at 10 Gb/s. This requires two threads:

- The acquisition thread, which extracts packets from the RSS queues, and timestamps and enqueues them to the buffer tail

- The processing thread, which dequeues packets from the buffer head and processes them

Normally, such a design choice would lead to expensive process synchronization. Fortunately, lock-free shared buffer data structures using state-of-the-art zero-copy data acquisition are available. The presence of acquisition and processing threads complicates the CPU resource allocation. In fact, the RSS queues access is time-critical, so it should be operated on a dedicated core, while the processing thread runs on a separate core. In summary, the design follows a “hybrid” approach: different independent processes are attached to (a group of) RSS queues, but each process has separate threads managing acquisition and processing independently.

EFFICIENT SHARING OF CPU CORES

Goal: The adoption of threads requires particular attention in addressing how frequently they have to be executed so that resource sharing is fair and efficient among threads in each core. With a *polling* strategy, the acquisition thread fetches data from the RSS queues as soon as they are presented by the NIC. This improves timestamping accuracy, but never lets the thread sleep, wasting CPU cycles in a busy-loop when no packet is present. A complementary strategy is to enforce *periodic* execution, which allows the system to effectively *share* CPU resources between acquisition and processing threads (Fig. 3d). However, this may cause *packet reordering* if the packets of the same flow sit in different RSS queues for too long, or worse, losses in case of suboptimal tuning.

Proposal: We suggest the use of the `SCHED_DEADLINE` (SD) operating system scheduling strategy offered by the Linux kernel. SD guarantees the scheduling of a thread within a configurable deadline δ , resulting in a quasi-periodic execution.¹ With appropriate sizing, a single CPU core can be *shared* among two threads, with packet timestamping accuracy and reordering that are under control. To the best of our knowledge, we are the first to investigate the application of SD for packet processing.

FLOW MANAGEMENT AND GARBAGE COLLECTION

Goal: Stateful per-flow analysis requires garbage collection. In fact, flows may abruptly terminate; to avoid memory leakage, a timeout policy needs to be enforced in the STA: if no packets are observed for a certain amount of time T_{out} , the flow is considered terminated, and its resources are freed. It follows that every ΔT (on the order

Modern NICs offer load balancing in hardware, for example, via the Intel Receiver Side Scaling queues. Consistent per-flow load balancing is possible with specific hashing functions offloaded to the NIC. This results in a system where packets are stored into different RSS queues to which the STA has direct access.

¹ `SCHED_DEADLINE` also guarantees that the periodic thread does not consume more than a fraction of the period via the parameter `sched_runtime`. In our system, we limit CPU time to be shorter than 10 percent of the period, resulting in a stable system.

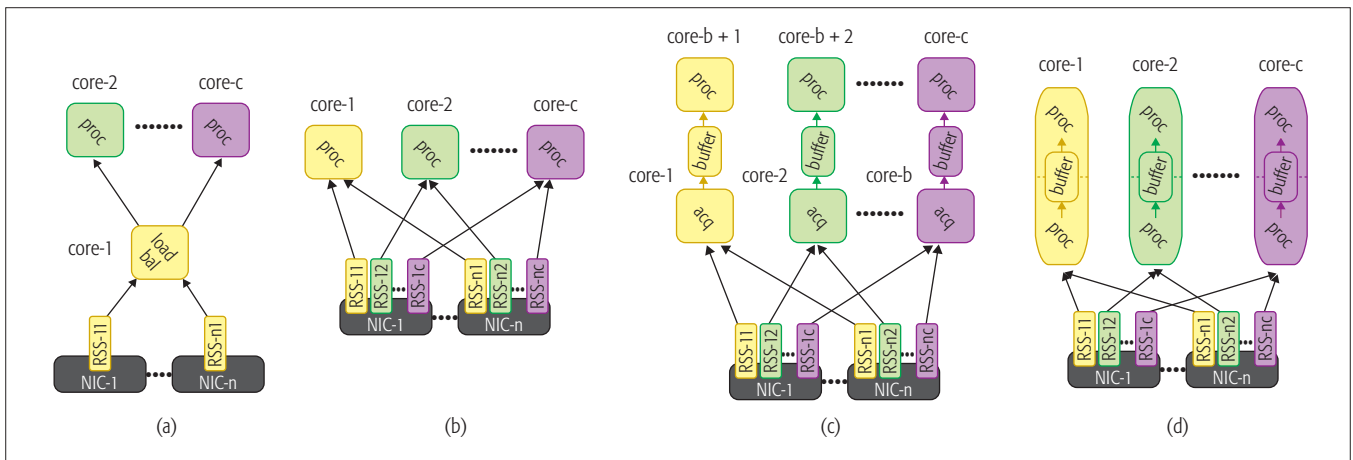


Figure 3. System architecture: the order is from the simplest one (left) to the most evolved and best performing (right): a) software load balancer; b) direct RSS queue access; c) buffered access to RSS queues with dedicated core; d) buffered access to RSS queues with shared core.

of seconds), all F flows (on the order of millions) in the STA flow table are checked to verify if they need to be purged. To avoid blocking the packet processing, a natural solution would be to implement the garbage collection in a separate thread. However, this is impractical due to the massive requirement of synchronization primitives it would entail, beside further complicating threads scheduling.

Proposal: We propose to divide the monolithic garbage collection operation in smaller parts. Assuming there are F flows to check every ΔT , we split the operation into M steps, each checking F/M flows, and invoke the garbage collection loop every $\Delta T/M$ time intervals. We report a sensitivity analysis below.

EXPERIMENTAL SETUP

In this section we provide experimental evidence of the benefits of the previous design choices. We use DPDKStat as the STA, and set up a testbed in our lab capable of achieving 40 Gb/s. A traffic generator (TG) is directly connected to a system under test (SUT), where we run DPDKStat. The TG replays packet traces at a desired speed. For every run, the *sustainable rate* R is empirically measured by looking for the maximum sending rate DPDKStat processes without observing any packet drop at the SUT. In experiments, we progressively increase the sending rate in 100 Mb/s units. We declare that the SUT achieves a rate R if in 5 separate runs at the same speed we do not observe losses.

We consider two different SUTs: *sut-SMP* (\approx US\$1500) is a single CPU architecture equipped with an Intel Xeon E3-1270 v3 @3.5 GHz, with 4 physical and 4 virtual cores, launched in 2013. It hosts 32 GB of DDR3-1333 RAM; *sut-NUMA* (\approx US\$3500) is a NUMA architecture equipped with 2 Intel Xeon E5-2660 @2.2 GHz, each with 8 physical and 8 virtual cores, launched in 2012. Each CPU is equipped with 64 GB DDR3-1333 RAM. Both SUTs are equipped with 4 Intel 82599 10 Gb/s Ethernet NICs, connected via a PCIe-3.0 with 16 lanes (64 Gb/s raw speed).

The TG has the same hardware configuration as *sut-SMP*. It has eight SSD disks in RAID-0 where packet traces can be read quickly enough

when replayed. To replay the traffic and control the sending rate, we develop our own solution based on DPDK (<https://github.com/marty90/DPDK-Replay>, accessed 12/13/2016).

We aim to benchmark our system using a workload similar to real scenarios. For this reason we rely on replaying packet traces rather than using synthetic TGs. Unfortunately, publicly available traces do not carry payload for privacy issues; hence, they do not offer a realistic benchmark for a STA. We thus consider packet traces that we collected from two live networks: Campus is a 2 h trace collected in 2015 from the Politecnico di Torino campus network (\approx 10,000 users, 7.6 M TCP and 5.4 M UDP flows, with average packet size of 811 bytes); ISP-full is a 1 h trace collected in 2014 from a European ISP PoP (\approx 20,000 residential ADSL users, 3.1 M TCP and 7.7 M UDP flows, with average packet size of 716 bytes). All traces were collected during peak time. More details are also available in [6].

Notice the different mix of TCP and UDP traffic between the two scenarios, which results in two complementary benchmarks for the STA. In fact, UDP traffic does not require a very complex state machine, but typically UDP flows are much shorter than TCP flows, resulting in a higher number of concurrent flows to track.

HARDWARE AND SOFTWARE TUNING

We now present experimental evidence of the design principles previously illustrated. We focus on two representative aspects concerning hardware and software that are of general interest: tuning packet acquisition and idle-flow management.

PACKET ACQUISITION

An RSS queue is an instrument that needs to be carefully sized. On one hand, large RSS queues are needed to avoid overflow and packet loss. Thus, we set the RSS queues to the maximum size (4096 packets). On the other hand, since packets are extracted from the RSS queues in batches, we need to control timestamp errors and avoid packet re-ordering.

We argue that it is advisable to use a `SCHED_DEADLINE` (SD) kernel policy, which unfortunately

ly induces nontrivial sampling of the RSS queue size, as the scheduling is not strictly periodic. Figure 4 reports the empirical probability density function (PDF) of the RSS queue size sampled when the packet acquisition thread is woken up by the kernel: we collect 10 million samples for deadline values of $\delta \in \{0.5, 1, 2, 4\}$ ms when processing 10 Gb/s traffic. By design, $\delta = 0.5$ ms interval should guarantee sub-millisecond time-stamp precision, which is accurate for most cases.

Now, consider an induced packet reordering effect. Suppose client requests and server responses are received at NIC- i and NIC- j , respectively. The per-flow RSS mechanism exposes them consistently to the same process. But if the packet acquisition thread visits first NIC- j and then NIC- i , an artificial out-of-sequence would be generated. To avoid this, one must guarantee that the visiting period of RSS queues is shorter than the client-server RTT so that client packets are already being removed from NIC- i when server packets are received at NIC- j . With practical Internet RTTs that are higher than 1 ms, a deadline of 0.5 ms makes this event very unlikely.

Finally, the tail of RSS occupancy distribution is important as it correlates with packet losses. With RSS queues of 4096 packets (the maximum allowed), we never recorded any loss in our (relatively short) tests. However, we can estimate the loss probability. Rather than modeling the packet arrival process at the RSS queue, we opt for a macroscopic approach, and fit the RSS queue size observations in Fig. 4 with an analytic model. We found a lognormal distribution having a good agreement with the experimental data. From the lognormal fit, we can extrapolate the RSS queue overflow probability, that is, $P(Q > 4096)$. For $\delta = 4$ ms, this happens with probability $7.2 \cdot 10^{-10}$. By reducing δ to 0.5 ms, the overflow probability becomes smaller than 10^{-20} .

BOUNDING PACKET PROCESSING TIME

Large packet processing time has a particularly severe effect since, during such time, packet loss can happen in the large buffer. In Fig. 5, we report packet processing time samples when no particular optimization is introduced (blue points, left part of the figure). Clear and periodic outliers appear with packet processing time up to 10 ms. These are due to garbage collection (GC) operations that happen periodically.

To control the occurrence of outliers, we divide the monolithic GC in smaller fractions that occur more often. Denoting by $(\Delta T, M/F)$ the GC settings, Fig. 5 shows the original setting (5 s, 1) that scans the entire flow table every 5 s, and two settings where the period and the fraction are divided by the same factor: $\times 100$ in the (50 ms, 1/100) case and 10,000 in the (0.5 ms, 1/10,000) case. The plot reports horizontal reference lines for 75th, 95th and 99th percentile statistics computed over 10^6 samples.

Comparing (5 s, 1) to (50 ms, 1/100) we see that the outliers become more numerous (by a factor of 100), but the maximum processing time is reduced (roughly by the same amount). Outliers disappear for (0.5 ms, 1/10,000), which happens since the fraction of flows to be checked by each GC event is now small enough. Observe that the 99th percentile grows, which happens since the

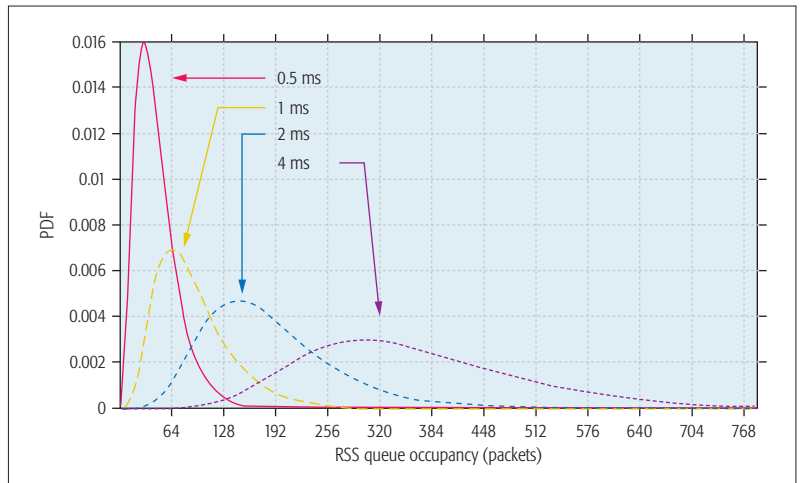


Figure 4. Distribution of the RSS queue occupancy for varying SCHED_DEADLINE packet acquisition intervals δ (sut-NUMA with ISP-full).

number of GC events is large enough to impact

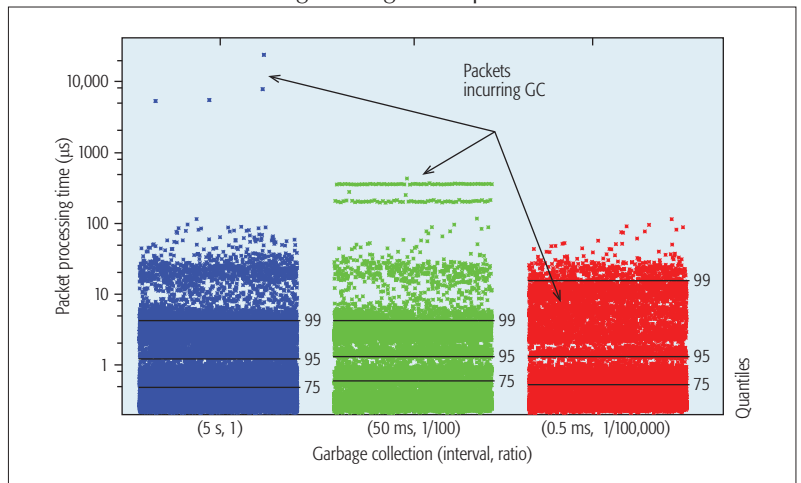


Figure 5. Per-packet processing time for various settings of the garbage collection period and size (sut-NUMA with ISP-full).

the 99th percentile. In a nutshell, the per-packet maximum processing time is now bounded, and exploiting a large buffer between acquisition and processing (Figs. 3a and 3d) allows the processing jitter to be absorbed.

EXPERIMENTAL RESULTS

We now experimentally evaluate the final DPDK-Stat design on different systems and configurations.

PERIODIC ACQUISITION AND HYPER-THREADING

Let us focus on sut-SMP first. Figure 6a shows the maximum sustainable rate (throughput for short) vs. the number of parallel processes. Results compare *polling* (dashed line) with the *SD periodic* (solid line) packet acquisition policies. Policies have a direct impact on how processes are bound to the available cores. In particular, as sketched at the top of Fig. 6a, when using polling, the best performance is obtained when packet acquisition (A) and processing (P) threads run on dedicated cores (either physical or logic), while it is counterproductive if the two threads share the same core. This does not occur when using the SD policy.

Up to two instances, both policies present

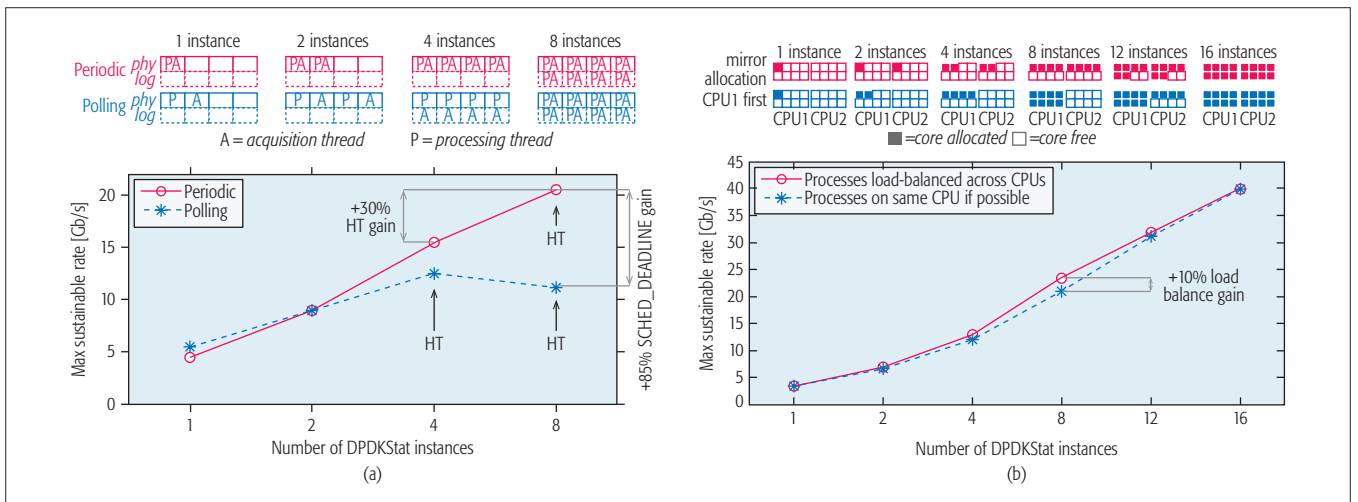


Figure 6. DDPKStat processing rates using ISP-full trace: a) sut-SMP; b) sut-NUMA (no hyper-threading).

similar performance, with a small advantage for polling in the single instance case (as two physical cores are used). When using more instances, SD presents a large performance improvement with respect to polling, a trend maintained at full capacity. Overall, the system achieves 21 Gb/s throughput without losses, about twice as much as system performance under polling. This is important to highlight since the system only has four physical cores.

Hyper-threading (HT) also yields remarkable performance speedup. Compare the 4 vs. 8 instances under periodic SD acquisition: running twice as many instances in the same amount of silicon yields +30 percent performance improvement. Conversely, HT gains are limited using polling. HT gains are completely offset in the 8 instance scenario due to increased contention. This confirms that polling is not the best strategy for packet acquisition if the SD policy is available.

COMBINING DIFFERENT CPUs

We now consider sut-NUMA where four NICs are connected via the same I/O hub and then to the same CPU (CPU1).

In this scenario, we have an additional degree of freedom in terms of core allocation policies. As schematically represented at the top of Fig. 6b, we can either use all cores of CPU1 (dashed line), which is closer to the NICs, or balance the load across CPUs (solid line). In these tests, HT is disabled, and we run all processes on the 16 physical cores.

As for the previous analysis, throughput scales linearly with the numbers of cores, and the system successfully reaches 40 Gb/s with no packet losses. Interestingly, the system is slightly faster when allocating processes on both CPUs rather than filling CPU1 first (up to +12 percent in the 4 instance scenario). Potentially, the system could be able to process even more traffic, but unfortunately we cannot test this hypothesis since our testbed is limited to 40 Gb/s, and Intel NICs offer a maximum of 16 RRS queues (thus a maximum of 16 processes). We can, however, assess HT gains to hold: in particular, when binding all 16 processes to run only on the 8+8 cores of CPU1 with HT enabled, we achieve 24 Gb/s, corresponding to

a +20 percent performance improvement with respect to the 8 instances scenario reported in Fig. 6b. This gain is lower than that obtained from sut-SMP, possibly due to the different hardware specs. Even if not possible with our hardware, it would be interesting to check different allocation policies where multiple NICs are connected to different I/O hubs and CPUs.

CONCLUSIONS

We report our experience in the design, implementation, and benchmarking of a system for statistical traffic analysis at 40 Gb/s with COTS hardware. The main lessons learned can be summarized as follows: periodic packet acquisition policies are preferable over traditional polling solutions; and the SD scheduler offered by Linux is amenable for a precise buffer control to achieve loss-free operation. Second, hyper-threading gain is sizable (20–30 percent). Third, process allocation over multiple NUMA nodes brings a non-negligible payoff (10 percent). Fourth, applications must leverage large intermediate buffers to cope with variable processing times and avoid packet losses in the buffers. This demonstrates that careful design allows one to obtain wirespeed processing at multi-10-Gb/s without the support of specialized and expensive hardware.

ACKNOWLEDGMENTS

This work was carried out at LINCS (<http://www.lincs.fr/>) and was supported by the WWTF Agency through the BigDAMA project and by NewNet@Paris, Cisco's Chair "Networks for the Future" at Telecom ParisTech (<http://newnet.telecom-paristech.fr/>).

REFERENCES

- [1] X. Chen *et al.*, "Para-Snort: A Multi-Thread Snort on Multi-Core IA Platform," *Citeseer*, 2009.
- [2] M. A. Jamshed *et al.*, "Kargus: a Highly-Scalable Software-Based Intrusion Detection System," *Proc. 2012 ACM Conf. Comp. Commun. Security*, 2012, pp. 317–28.
- [3] K. Namuk *et al.*, "A Scalable Carrier-Grade DPI System Architecture Using Synchronization of Flow Information," *IEEE JSAC*, vol. 32, no. 10, Oct 2014, pp. 1834–48.
- [4] L. Koromilas *et al.*, "Efficient Software Packet Processing on Heterogeneous and Asymmetric Hardware Architectures," *Proc. 10th ACM/IEEE Symp. Architectures Networking Commun. Systems*, 2014, pp. 207–18.

- [5] A. Finamore et al., "Experiences of Internet Traffic Monitoring with Tstat," *IEEE Network*, vol. 25, 2011, pp. 8–14.
- [6] M. Trevisan et al., "DPDKStat: 40gbps Statistical Traffic Analysis with Off-the-Shelf Hardware," tech. rep., 2016; <https://www.telecom-paristech.fr/~drossi/paper/DPDK-Stat-techrep.pdf>, accessed 12/13/2016.
- [7] T. Barbette et al., "Fast Userspace Packet Processing," *Proc. 11th ACM/IEEE Symp. Architectures Networking Commun. Systems*, 2015, pp. 5–16.
- [8] V. Moreno et al., "Testing the Capacity of Off-the-Shelf Systems to Store 10GbE Traffic," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2015, pp. 118–25.
- [9] H. Jiang et al., "Scalable High-Performance Parallel Design for Network Intrusion Detection Systems on Many-Core Processors," *Proc. 9th ACM/IEEE Symp. Architectures for Networking Commun. Systems*, 2013, pp. 137–46.
- [10] A. Das et al., "An FPGA-Based Network Intrusion Detection Architecture," *IEEE Trans. Info. Forensics Security*, vol. 3, no. 1, 2008, pp. 118–32.
- [11] K. Jaic et al., "A Practical Network Intrusion Detection System for Inline FPGAs on 10GbE Network Adapters," *Proc. 2014 IEEE 25th Int'l. Conf. Application-Specific Systems, Architectures and Processors*, 2014, pp. 180–81.
- [12] G. Bianchi et al., "Streamon: A Software-Defined Monitoring Platform," *Proc. 2014 26th IEEE Int'l. Teletraffic Congress*, 2014, pp. 1–6.
- [13] L. Deri et al., "NDPI: Open-Source High-Speed Deep Packet Inspection," *Proc. 2014 Int'l. Wireless Commun. Mobile Computing Conf.*, IEEE, 2014, pp. 617–22.
- [14] S. Woo and K. Park, "Scalable TCP Session Monitoring with Symmetric Receive-Side Scaling," KAIST, tech. rep., 2012; <https://an.kaist.ac.kr/~shinae/paper/2012-srss.pdf>, accessed 12/13/2016.

BIOGRAPHIES

MARTINO TREVISAN received his B.Sc. (2012) and M.Sc. (2015) in computer science, both from Politecnico di Torino, Italy. He is currently a Ph.D. student in electrical, electronics, and communications engineering at the same university, where he joined the Telecommunication Networks Group (TNG). He has been collaborating in both industry and European projects, and spent six months at Telecom ParisTech, France, working on high-speed traffic monitoring. His research interest areas include network measurements and traffic monitoring; he is also particularly interested in leveraging big data and machine learning techniques in such fields.

ALESSANDRO FINAMORE received his Ph.D. in electronics and communication engineering (2012) and M.Sc. (2008) from Politecnico di Torino. He has been an intern at Purdue University, Lafayette, Indiana (2010); Telefonica Research, Barcelona, Spain (2012); and Narus Inc., Sunnyvale, California (2014). He has coauthored more than 30 publications, and participated in the TPC of venues such as INFOCOM, CoNEXT, PAM, and TMA. His research interests are in the area of Internet traffic analysis, mobile systems, user quality of experience and mobility, CDN services, and big data frameworks. He is currently an associate researcher at Telefonica Research in Barcelona.

MARCO MELLIA [S'08], Ph.D., has research interests in the area of traffic monitoring and analysis, cyber monitoring, and big data analytics. He has co-authored over 250 papers published in international journals and presented in leading international conferences. He won the IRTF ANR Prize at IETF-88, and best paper awards at IEEE P2P '12, ACM CoNEXT '13, and IEEE ICDCS '15. He is on the Editorial Boards of *ACM/IEEE Transactions on Networking*, *IEEE Transactions on Network and Service Management*, and *ACM Computer Communication Review*. He holds a position as associate professor at Politecnico di Torino.

MAURIZIO MUNAFÒ is an assistant professor at the Department of Electronics and Telecommunications of Politecnico di Torino. He holds a Dr.Eng. degree in electronic engineering since 1991 and a Ph.D. in telecommunications engineering since 1994, both from Politecnico di Torino. He has co-authored about 70 journal and conference papers in the area of communication networks and systems. His current research interests are in simulation and performance analysis of communication systems and traffic modeling, measurement, and classification.

DARIO ROSSI [S'13] has research interests that include performance evaluation, Internet traffic measurement, and information-centric networking. He holds 9 patents and has coauthored over 150 papers, receiving 4 best paper awards, a Google Faculty Research Award (2015), and an IRTF Applied Network Research Prize (2016). He served on the Board of *IEEE Transactions on Green Communications and Networking* and *Elsevier Computer Networks*, and on the Program Committees of over 50 conferences including ACM ICN, ACM CoNEXT, ACM SIGCOMM, and IEEE INFOCOM (Distinguished Member 2015 and 2016). He is a professor at Telecom ParisTech and Ecole Polytechnique, and is the holder of Cisco's Chair NewNet@Paris.

NATwatcher: Profiling NATs in the Wild

Anna Maria Mandalari, Miguel Angel Diaz Bautista, Francisco Valera and Marcelo Bagnulo

The authors identify common NAT profiles in order to provide an overview of the current behavior of NATs. They develop NATwatcher, a tool to test NAT boxes using a crowdsourcing-based measurement methodology. They perform a large measurement campaign using NATwatcher recruiting over 700 users, from 65 different countries and 280 ISPs.

ABSTRACT

NATs are commonplace in the Internet nowadays. It is fair to say that most residential and mobile users are connected to the Internet through one or more NATs. As with any other technology, NAT presents upsides and downsides. Probably the most acknowledged downside of the NAT technology is that it introduces additional difficulties for some applications such as peer-to-peer applications, gaming, and others to function properly. This is partially due to the nature of the NAT technology but also due to the diversity of behaviors of the different NAT implementations deployed in the Internet. Understanding the properties of the currently deployed NAT base provides useful input for application and protocol developers regarding what to expect when deploying new applications in the Internet. The goal of this article is to identify common NAT profiles in order to provide an overview of the current behavior of NATs. We develop NATwatcher, a tool to test NAT boxes using a crowdsourcing-based measurement methodology. We perform a large measurement campaign using NATwatcher recruiting over 700 users, from 65 different countries and 280 ISPs. We present the results after testing and profiling NAT products from over 120 vendors.

INTRODUCTION

Network Address Translators (NATs) were introduced back in the early 1990s as a means to cope with the incipient address depletion crisis. Together with Classless Interdomain Routing (CIDR), they successfully extended the lifetime of IPv4 from imminent depletion until very recently, when the Internet Assigned Numbers Authority (IANA) pool of IPv4 addresses finally ran out [1]. NATs are now commonplace in the Internet and they are included by default in the Internet Access offerings for both residential and mobile customers.

NATs successfully extended the lifetime of IPv4 indeed, but at a high cost: they hardcoded the client-server paradigm in the architecture of the Internet. The basic operation of a NAT relies on the creation of a mapping state between a private address and port pair and a public address and port pair. This state is created when a client using a private address initiates communication with a server in the public Internet. Deploying applications that have an alternative paradigm, such as peer-to-peer applications, gaming, or voice-over-IP to name a few, which require hosts in the public Internet to initiate communications toward hosts

behind a NAT is challenging and requires the use of the so-called NAT traversal techniques. These techniques are usually cumbersome and increase latency, traffic, and the energy consumed by the endpoint.

While the aforementioned problem of supporting alternative application paradigms is fundamental to the nature of NAT operation, it is exacerbated by the myriad of behaviors of the different NAT implementations deployed in the Internet. Different NATs use different criteria to create, preserve, and remove their internal mapping state, and have different filtering and forwarding rules. This severely complicates the job of applications willing to manage the NAT state in order to enable alternative communication models other than the client-server one as they need to cope with all possible NAT flavors.

In order to achieve a more deterministic behavior from the NAT boxes, the Internet Engineering Task Force (IETF) produced a number of specifications defining the requirements that NATs should follow when creating, preserving, and removing their internal state as well as some recommendations in terms of the different filtering and forwarding policies that NAT should implement. In particular, the IETF released NAT behavioral requirements for handling TCP traffic [2], UDP traffic [3], and ICMP packets [4]. The goal of these requirements is to achieve more deterministic behavior of NATs and hence significantly simplify the job of deploying new application paradigms in the Internet, fostering innovation and competition. However, since these IETF standards specify the internal behavior for a NAT, it is far from trivial to assess whether NATs are following the recommendations, and to the best of our knowledge there is no information about the prevalence of NAT boxes that honor the IETF specifications.

Due to the difficulties that are inherent in performing large-scale measurements in real residential environments, to date, the few studies that are available have performed testing of different NAT devices in a lab environment. In [5] the authors study the configurations of 34 different home gateway models, analyzing the processing of various TCP and IP options and measuring the success of some network protocols when traversing NATs (i.e., STUN [6], TURN [7], and ICE [8]). In [9] the authors perform a lab study of the support of a number of features such as mapping, filtering, and hairpinning on 42 NAT device models. While these studies provide some information about the capabilities of the different NAT boxes, they provide limited information about the actual behavior

of the deployed NAT devices in the Internet. This is so because the behavior of the deployed NAT base also largely depends on the configuration of the NAT boxes and the popularity of the different NAT products.

The contribution of this article is therefore threefold. First, we design and develop NATwatcher, a tool to measure key aspects of the behavior of the deployed NAT base, along with a measurement methodology based on crowdsourcing that allows us to perform large-scale measurement using NATwatcher. Second, using the proposed methodology, we perform a large measurement campaign, and we deploy NATwatcher in over 700 measurement points, building a large dataset describing the behavior of over 700 NAT boxes from 65 different countries and 280 ISPs, testing over 120 different NAT vendors. Finally, we mine the obtained measurement results to identify common NAT profiles, providing valuable data for application developers about the ground truth of NAT behavior in the current Internet.

We find that a large majority (80 percent) of the NAT boxes we tested follow the IETF recommendations for 11 out of the 17 considered features. We also observe that about half of the NAT devices we tested exhibit the exact same behavior for all the features we tested, while the other half of the devices use a variety of configurations.

METHODOLOGY AND SETUP

This section describes our methodology to classify NATs relying on crowdsourcing platforms to perform Internet-wide measurements.

CROWDSOURCING PLATFORM

Crowdsourcing platforms are online portals that allow employers to recruit workers from around the world to perform simple tasks, normally achievable in a few minutes, called *microjobs*. Each task contains a brief description of the work to be done and how the employers will verify the completion of the task. Once these tasks are defined, a campaign is run in the platform, and every worker can apply to participate in the campaign and do the corresponding task.

When the task has been completed the number of times required by the employer, the campaign is closed. Employers must then verify that the task has been completed by each worker and pay them accordingly. Crowdsourcing platforms are traditionally focused on the human element (i.e., to test psychological profiles or to perform tests that machines cannot do). We expand the usage of these platforms to run Internet-wide measurements. Similar to the methodology used in [10], we request workers around the world that are using a NAT to connect to the Internet to run our NATwatcher tool in order to characterize the behavior of their respective NATs.

NATWATCHER: METHODOLOGY OVERVIEW

NATwatcher¹ is the tool we build to detect the characteristics of a NAT using a number of active tests. Figure 1 summarizes the operational setup of NATwatcher. In a nutshell, the worker downloads and executes the NATwatcher application. The NATwatcher application automatically executes the tests to characterize the NAT behavior by sending different combinations of packets to

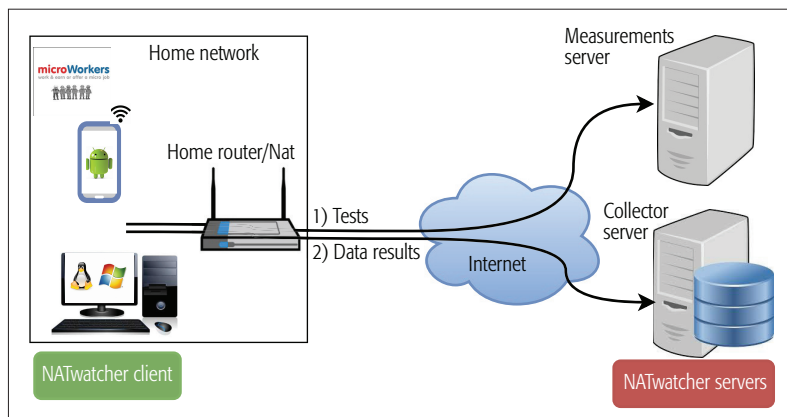


Figure 1. NATwatcher operational setup.

our Measurement server deployed in the public Internet and processes the response packets sent from the server back to the NATwatcher client (step 1 in Fig. 1). Once all the tests are completed, the application sends the compiled measurement results to a collector server where they are stored (step 2 in Fig. 1) and the code that can be used to redeem the payment.

We designed NATwatcher to be suitable for use in a crowdsourcing environment. In particular, we designed it to be as simple as possible in order to be tractable for a large number of workers. Workers are not required to have any technical background. Workers just need to download and execute the NATwatcher application, and all data are automatically collected and reported to our collector server without further worker intervention.

In order to reach a high number of workers, we developed three versions of NATwatcher: one for Android, one for Windows, and one for Linux. We therefore create two crowdsourcing campaigns, *Android-based* and *Windows/Linux-based*, which we detail next.

Android-Based Campaign: This campaign requires the worker to install our Android application (<http://www.it.uc3m.es/amandala/nat/natwatcher/natwatcher.apk>). The worker then just has to launch the application, and all the tests are then run sequentially. In order to ensure that workers' Internet access is provided through a fixed line (and not third generation [3G], 4G, etc.), the application is instrumented to run the *microjob* using the WiFi interface.

Windows and Linux-Based Campaign: This campaign requires workers to download the application (<http://www.it.uc3m.es/amandala/nat/nat.html>) and run it from a Windows or Linux machine. The application takes care of all the measurements to be performed as in the Android app. We asked workers to perform the test from their own personal computers, using a fixed line.

We also deploy a measurement server, connected to the public Internet. This server implements the server side of the tests described below including the UDP tests, the UDP STUN tests, and the TCP STUN tests.

NATWATCHER TESTS

According to our experience, a microjob offered in a crowdsourcing platform is less likely to be performed by a large number of workers if it takes more than five minutes. In order to minimize exe-

¹ The source code of NATwatcher and the anonymized datasets are available at <http://www.it.uc3m.es/amandala/nat/natwatcher/>

Crowdsourcing platforms are online portals that allow employers to recruit workers from around the world to perform simple tasks, normally achievable in a few minutes, called microjobs. Each task contains a brief description of the work to be done and how the employers will verify the completion of the task.

cution time of the microjob, we carefully selected 17 key NAT characteristics for which NATwatcher will test.

We use the tests described in [9] as a starting point. We then expand the tests set and adapt them to be run in a crowdsourcing platform. We developed all the tests in C programming language to be able to reuse the code through the different platforms (i.e., Android, Windows, and Linux). All the tests are implemented crafting UDP, ICMP, and TCP packets using Raw Sockets or Standard Sockets whenever possible.

UDP Tests:

Mapping Behavior: The test verifies if the NAT assigns the same mapping for communications between a specific internal IP address and port and any external IP address and port for UDP packets. NATs can be classified in three groups according to their mapping behavior:

- **Endpoint-Independent Mapping:** The NAT reuses the port mapping for subsequent packets sent from the same private IP address and port to any public IP address and port.
- **Address-Dependent Mapping:** The NAT reuses the port mapping for subsequent packets sent from the same private IP address and port to the same public IP address, regardless of the external port.
- **Address and Port-Dependent Mapping:** The NAT reuses the port mapping for subsequent packets sent from the same private IP address and port to the same public IP address and port while the mapping is still active.

The test is as follows: we first send two STUN binding requests² to two different public addresses of our STUN server.³ We compare the address and port returned in the two STUN responses received. If both the addresses and the ports match, we conclude that the mapping behavior of the NAT is endpoint-independent. If this is not the case, we send a third binding request to our STUN server using the primary addresses used before and a different port. If the address and port reported in the STUN response is the same as the one reported before when using the primary address and a different port, the NAT is address-dependent; otherwise, the NAT is address and port-dependent.

Filtering Behavior: The test detects the filtering behavior of the NAT. When an unsolicited packet is received from the Internet, the NAT applies filtering rules that can be classified as follows:

- **Endpoint-Independent Filtering:** The NAT forwards any packets destined to an internal host as long as a mapping exists.
- **Address-Dependent Filtering:** The NAT filters packets received from a specific external host to a specific internal host if the internal host has not previously sent any packet to that specific external host's IP address.
- **Address and Port-Dependent Filtering:** The NAT filters packets received from a specific external host to a specific internal host if the internal host has not previously sent any packet to that specific external host's IP address and port.

The test is as follows: We send a binding request to the primary address of our STUN server

with *change port* and *change address* attributes. These binding request attributes solicit the server to send the response from the alternate IP address and port. If the client receives a response, the filtering behavior of the NAT is endpoint-independent. If not, we send a third binding request to the primary address with only *change port*. If the client receives a response, the NAT is address-dependent filtering; if not, it is port-dependent filtering.

Port Preservation: This test checks if the NAT leaves the port unchanged when creating a mapping. We send a packet using a particular local source port and then compare the port number with the external bound port. If they match, the NAT is performing port preservation. If they do not match, it is possible that the NAT does not implement port preservation, but it is also possible that the specific port used as source port was already in use in another mapping (from another internal host). Because of this limitation, this test only provides a lower bound to the number of NATs that implement port preservation. It would be possible to increase the accuracy of this test by repeating the test several times. However, this would increase the time budget of the test, which we cannot afford.

Hairpinning Support: Hairpinning enables a host in the home network to access another host in the home network using the external IP address. In order to check it, we send two packets: the first one to discover our mapped address using STUN, and the second one from a different source port and toward the discovered mapped address. If we receive the response it means the NAT supports hairpinning.

Supporting the "Do Not Fragment" Flag: The NAT should properly generate the "ICMP fragmentation needed" message when a packet is received with the "do not fragment" flag set and discard that packet. Our application sends a packet with the do not fragment flag set and waits for the reception of the corresponding ICMP message.

Out-of-Order UDP Fragments: When packets are fragmented and received out of order, some NATs are required to try to reassemble and then forward the packet. In order to check this behavior, we send disordered fragments from our server and check their reception in the application.

Mapping Lifetime over Two Minutes: NATs are required to maintain UDP mappings for no less than two minutes. In order to check this, we send a first binding request to our server, and after two minutes we send another binding request using a different port but specifying that the response should be sent to the previous binding. If the answer is not filtered, it means that the previous mapping has been preserved.

Outbound Refresh Behavior: According to the UDP requirements, outgoing packets must refresh the existing binding. This test is similar to the previous one, except that an additional outgoing packet is sent one minute after the initial binding request, and the second binding request is sent after three minutes.

ICMP Tests

Reply/Request of ICMP Packets: The test verifies that the NAT supports simple ICMP Reply/Request message exchange by sending a query and waiting for the answer.

² The STUN protocol operates as follows: the client located behind the NAT sends a binding request message to a STUN server. The STUN server replies with a response message containing the IP address and port of the client in its payload, as observed from the server.

³ A STUN server has two public IP addresses: the primary one and the alternate one.

Support of ICMP Destination Unreachable: This test verifies that the NAT is capable of forwarding ICMP Destination Unreachable messages generated as a response to a previous UDP packet. We send a UDP packet to our server, and the server replies with Destination Unreachable behavior. We then verify that the ICMP error is received by the NATwatcher client.

Support of ICMP Time Exceeded: This is the same as the previous one but for ICMP Time Exceeded messages.

Support of Error Packet Hairpinning: NATs are required to support hairpinning for error messages. NATwatcher checks this by sending two packets, the first packet to discover our mapped address using STUN protocol; the second packet is an ICMP echo error message sent to the mapped address from a different port. NATwatcher verifies the reception of the error message.

TCP Tests: For the first four tests enumerated below, we use the same methodology than for UDP tests, but using TCP packets.

Mapping Behavior: The test verifies if the NAT is endpoint-independent, address-dependent, or address and port-dependent with respect to the TCP mapping behavior.

Filtering Behavior: This test verifies the filtering behavior of the NAT with respect to TCP packets (endpoint-independent, address-dependent, and address and port-dependent filtering).

Port Preservation

Hairpinning Support: The test checks the support of hairpinning for TCP packets.

Mapping and ICMP Packets: This test verifies if the mapping is maintained after an ICMP Destination Unreachable packet is received by the NAT.

We implement all the tests described before in the Linux and Windows versions of NATwatcher. However, 9 of the 17 tests need root permissions for their execution, and unfortunately, Android devices are not commonly rooted. For this reason we implement only 8 of the 17 NATwatcher tests in the case of the Android app. Specifically, we implement test numbers 1, 2, 4, 7, and 8 for UDP NAT behavior and test numbers 1, 2, and 4 for TCP behavior.

RESULTS AND DATASET

In this section, we present the collected data set, and we analyze the obtained results.

CROWDSOURCING CAMPAIGN

We defined two campaigns, one for the Windows/Linux-based application (each worker attempts 17 tests) and the other one for Android (each worker attempts 8 tests), and both were available for 28 days during June 2016. Overall, we recruited 781 workers: 170 workers participated in the Windows/Linux-based campaign, while 611 workers participated in the Android-based one.

After the campaigns, our dataset consists of 7778 unique test results.

Overall, workers are distributed among 65 countries (Fig. 2). The devices cover more than 280 Internet service providers (ISPs) for a total of 120 different operator-user interfaces (OUIs).⁴

PRIVACY CONSIDERATIONS

All the workers that we recruited through the crowdsourcing campaigns are properly informed about the details so that they are able to make a choice of whether or not to participate in the test. This information has been carefully written in a way that was understandable to the people who were approached as participants (non-technical workers). The source code we used to perform the tests is also provided to the workers so that they can check it.

Even though the goal of this article is to understand NATs' behavior, and hence we do not focus on personal human information, the information collected on our server is protected and is only shared once it has been anonymized (i.e., sensitive information replaced with indirect identifiers like numbers). Agreeing to run the test, workers give informed consent to share such data with the research community.

GENERAL RESULTS

Table 1 summarizes the results for both campaigns. For each test we show the percentage of NATs that follow a particular behavior. We color in gray the IETF recommended behaviors.

We can see that for 11 out of 17 there is wide compliance with the IETF sanctioned behavior (for these 11 tests, more than 80 percent of the analyzed NATs follow the recommended behavior). For the remaining six tests, the large majority of tests' NAT boxes do not follow the IETF recommendation.

Most of the measured NAT models implement UDP and TCP endpoint-independent mapping, and support UDP not fragment flag and receiving UDP fragments out of order; moreover, most of them follow all the ICMP requirements. All these requirements are reported as a MUST in [2–4].

For the rest of the tests the success rate decreases dramatically. In particular, it is interesting to see less than 16 percent of the devices fulfill the requirements on UDP and TCP endpoint-independent filtering, hairpinning support, and mapping lifetime over two minutes. The endpoint-independent filtering is not a mandatory requirement, but it is highly recommended if transparency is a priority. If security is the priority, NAT should follow address-dependent filtering, but as results show, the majority of NATs set address and port-dependent filtering. Applications such as online gaming, for instance, would not benefit from this kind of behavior.

Hairpinning and binding lifetime over 120 s are two mandatory requirements for UDP. Most of the NATs do not support these features as the failure rate is higher than 84 percent for these tests.

Port preservation support is recommended, particularly for outgoing TCP connections, in order to allow NAT port prediction. In our results, we find a lower bound of 78 percent of devices that use port preservation.

Results show that about 70 percent of NATs delete the TCP mapping if an ICMP error message is received affecting that specific mapping. This is strongly recommended against in [2] as it exposes the NAT to attacks relying on ICMP error messages to delete existing NAT bindings.

NATs are required to support hairpinning for error messages. NATwatcher checks this by sending two packets, the first packet to discover our mapped address using STUN protocol; the second packet is an ICMP echo error message sent to the mapped address from a different port.

⁴ We use the WHOIS database to retrieve the ISP from the public IP address of each NAT, and we use the medium access control (MAC) address of the NAT to retrieve the OUI. Since some vendors use multiple OUIs or rebrand other products, we clarify that when we refer to 120 different vendors in the article, we refer to 120 different OUIs.

All the workers that we recruited through the crowdsourcing campaigns are properly informed about the details so that they are able to make a choice of whether or not to participate in the test. This information has been carefully written in a way that was understandable to the people who have been approached as participants (non-technical workers).



Figure 2. Worldwide distribution of vantage points.

NAT CLASSIFICATION

In this subsection we identify the most common NAT configurations. For this analysis we only consider the eight tests that have been performed for all the tested NAT devices (i.e. the tests that are executed in all the campaigns). We characterize a configuration through the different combinations of the results of these tests. We identified 19 different configurations across the 781 NATs we tested. We detail in Table 2 the configurations that appear in more than 5 devices (11 out of 19).

We assign the number to each configuration based on IETF requirement compliance (i.e., we named “1” the configuration with higher RFC requirements compliance, and the one with less RFC requirements compliance is number “19”). For example, configuration number 1 in Table 2 is the configuration recommended in the different RFCs, which has UDP endpoint-independent mapping and filtering, has TCP endpoint-independent mapping, and supports hairpinning, and the UDP mapping lifetime is over 2 minutes. We consider this configuration “open,” meaning that transparency is the top priority over security.

Overall, 52.5 percent of devices implement the configuration number 9. The devices come from over 50 countries and 173 unique ISPs, for a total of 72 different vendors. The most common configuration includes endpoint-independent mapping for UDP and TCP, and the filtering as strict as possible (address and port-dependent).

There is a clear trend toward security for the rest of the configurations, as only 4 over 11 NAT configurations implement endpoint-independent filtering behavior.

Table 2 also shows that for both UDP mapping lifetime and hairpinning, the majority of analyzed devices fail to comply with the IETF recommendations.

VENDORS AND ISPs

In this section we try to figure out if the adoption of a certain common NAT configuration depends on the vendor or on the ISP.

Figure 3 shows the configuration number for each tested device.⁵ The devices (on the horizontal axis) are ordered first by vendor (Fig. 3a) and second by ISP (Fig. 3b). Each vendor/ISP is delimited by a vertical line. Devices from vendors/ISPs present in our dataset with no more than two devices are grouped after the last line on the right.

Apart from a clear trend to use configuration number 9, as mentioned earlier, we observe some “open” configurations for a few vantage points in some vendors. This can be explained considering that users can change the basic configuration that vendors impose by default to accommodate the NAT to their own needs (i.e., activating hairpinning or endpoint-independent filtering).

In Fig. 3b, we identify two ISPs (identified by arrows) where the behavior for all NATs connected to these ISPs is very uniform, exhibiting one or two configurations. These two ISPs are mobile ISPs that provide 3G and LTE Internet access services. Given that NATwatcher only runs using the WiFi interface and not the cellular one, the NATwatcher client was executed in a mobile phone connected to a hotspot, which in turn was connected to the Internet using 3G or LTE. We believe it is safe to conclude that in these cases, the NATwatcher client was behind two cascaded NATs, the one from the WiFi access point and the one from the mobile operator. This means that when the client executes NATwatcher, the results reflect the superposition of both NATs along the path, reflecting the more restrictive behavior of the two, which is likely to be the one of the NAT of the mobile operator explaining the uniform behavior observed.

⁵ The resulting configurations for each ISP/vendor are also listed and freely available at <http://www.it.uc3m.es/amandala/nat/natwatcher/>

Protocol	NATwatcher tests	NAT behavior	Number of devices(%)
UDP	Mapping behavior	Endpoint-independent mapping	80.9%
		Address-dependent mapping	0.7%
		Address and port-dependent mapping	18.4%
	Filtering behavior	Endpoint-independent filtering	14.63%
		Address-dependent filtering	1.79%
		Address and port-dependent filtering	83.56%
	Port Preservation	Yes	78.2%
		No	21.8%
	Supporting hairpinning	Yes	15.5%
		No	84.5%
	Supporting the "not fragment" flag	Yes	100%
		No	0%
	Supporting receiving UDP fragments out-of-order	Yes	100%
		No	0 %
	Mapping lifetime over 2 minute	Yes	12.5%
No		87.5%	
Outbound refresh behavior	Yes	86.03%	
	No	13.97%	
ICMP	Reply/Request of ICMP packets	Yes	84.8%
		No	15.2 %
	Supporting of ICMP Destination Unreachable	Yes	69.6%
		No	30.4%
	Supporting of ICMP Time Exceeded	Yes	91.22%
		No	8.78%
	Supporting error packet hairpinning	Yes	83.04%
		No	16.96%
TCP	Mapping behavior	Endpoint-independent mapping	78.4%
		Address-dependent mapping	0.6%
		Address and port-dependent mapping	21%
	Filtering behavior	Endpoint-independent filtering	12.5%
		Address-dependent filtering	4.85%
		Address and port-dependent filtering	82.65%
	Port Preservation	Yes	78.2%
		No	21.8%
	Supporting hairpinning	Yes	15.5%
		No	84.5%
Mapping and ICMP packets	Mapping is maintaining after receiving	29.8%	
	Mapping is not maintaining after receiving	70.2%	

Using a crowdsourcing approach, we provide insight into how vendors, ISPs, and users configure and use NATs with respect to TCP, UDP, and ICMP packets, providing useful data for designing future applications.

Table 1. IETF NAT requirements compliance results, based on the NATwatcher test.

Configuration Number	NAT tests								
	UDP mapping	UDP filtering	UDP hairpinning	TCP mapping	TCP filtering	UDP mapping over 2 min	UDP outbound refresh	TCP hairpinning	Number of devices (%)
9	E.I.	A.P.D.		E.I.	A.P.D.		✓		52.5
2	E.I.	E.I.	✓	A.P.D.	A.P.D.		✓	✓	5.5
18	A.P.D.	A.P.D.		E.I.	A.P.D.				5.2
5	E.I.	E.I.		A.P.D.	A.P.D.				2.5
1	E.I.	E.I.	✓	E.I.	E.I.		✓	✓	2
11	E.I.	A.P.D.		A.P.D.	A.P.D.				1.8
17	A.P.D.	A.P.D.		A.P.D.	A.P.D.				1.5
4	E.I.	E.I.		E.I.	E.I.				1.15
7	E.I.	A.D.		E.I.	A.D.				0.8
19	A.P.D.	A.P.D.		E.I.	A.D.		✓		0.8
8	E.I.	A.P.D.		E.I.	A.P.D.		✓		0.65

Table 2. Most common NAT configurations. For each configuration it is reported the behavior with respect to each test. An endpoint-independent behavior is reported as E.I., A.D. indicates address-dependent and A.P.D. describes an address and port-dependent behavior. For other tests RFC requirements compliance are shown with a tick.

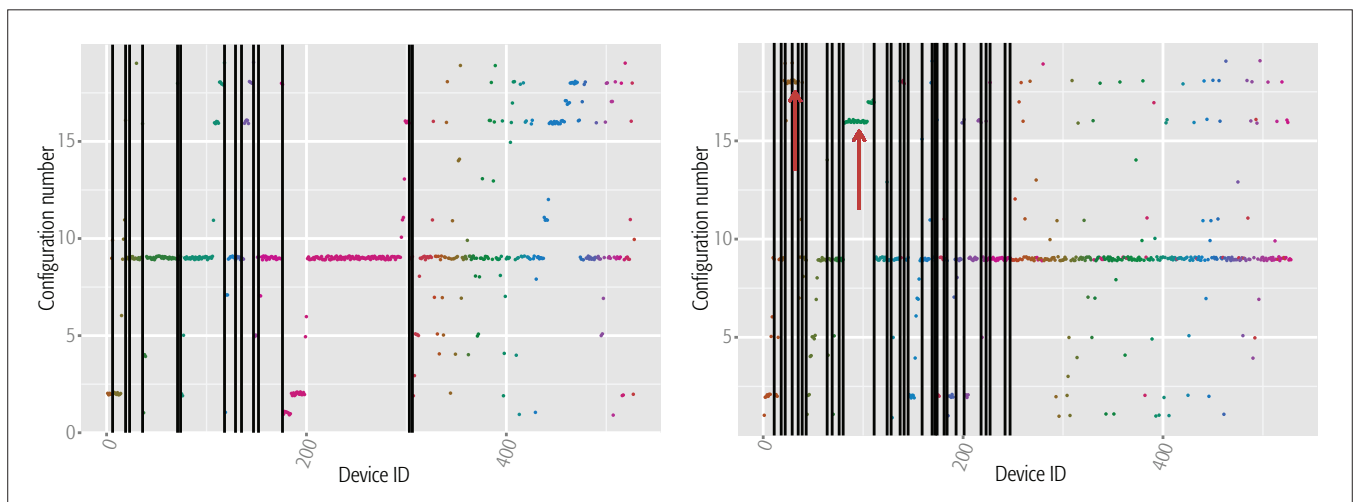


Figure 3. Configuration number vs. device ID: a) device IDs in order of vendors; b) device IDs in order of ISPs.

CONCLUSION

In this article we present NATwatcher, a tool that allows us to shed some light on the NAT behavior in the wild. Using a crowdsourcing approach, we provide insight into how vendors, ISPs, and users configure and use NATs with respect to TCP, UDP, and ICMP packets, providing useful data for designing future applications. We present the first large-scale measurement campaign of home NATs, based on data from 781 homes, from 65 countries and from 280 ISPs. The data we collected are good enough for understanding NATs' deployed behaviors, but not necessarily statistically representative of the Internet, which is composed of billions of devices.

Our study demonstrated that about 80 percent

of the tested NATs follow the IETF sanctioned behavior with respect to 11 of 17 (64 percent of tests). For the remaining 6 tests our findings show that only 13 percent of the NAT boxes follow the IETF requirements of filtering, hairpinning, and mapping lifetime over 2 minutes. Moreover, we listed the 11 most common configurations, finding that 52.5 percent of the tested NAT boxes use endpoint-independent mapping for UDP and TCP and address and port-dependent filtering, but do not support hairpinning or UDP mapping over 2 minutes. To the best of our knowledge, this is the largest dataset available describing the behavior of the deployed NAT base, and we believe it provides useful input for application and protocol designers aiming to make their applications and protocols work across NATs.

ACKNOWLEDGMENTS

The work of Anna Maria Mandalari has been funded by the EU FP7 METRICS (607728) project. The work of Marcelo Bagnulo has been partially supported by the EU FP7 Trilogy2 (317756) project and the project MASSES (TEC2012-35443) funded by MINECO. The work of Francisco Valera has been partially supported by the EU FP7 Trilogy2 (317756) project and the project DRONEXT (TEC2014-58964-C2-1-R) funded by MINECO.

REFERENCES

- [1] "Potaroo Network Tool," <http://www.potaroo.net/tools/ipv4/>, accessed Dec. 12, 2016.
- [2] S. Guha *et al.*, "NAT Behavioral Requirements for TCP," IETF RFC 5382, Oct. 2008.
- [3] F. Audet and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP," IETF RFC 4787, Jan. 2007.
- [4] P. Srisuresh *et al.*, "NAT Behavioral Requirements for ICMP," IETF RFC 5508, Apr. 2009.
- [5] S. Hätönen *et al.*, "An Experimental Study of Home Gateway Characteristics," *Proc. 10th ACM SIGCOMM Conf. Internet Measurement*, ser. IMC '10. 2010, pp. 260–66.
- [6] J. Rosenberg *et al.*, "Session Traversal Utilities for NAT (STUN)," IETF RFC 5389, Oct. 2008.
- [7] R. Mahy, P. Matthews, and J. Rosenberg, "Traversal Using Relay NAT (TURN)," IETF RFC 5766, Apr. 2010.
- [8] J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," IETF RFC 5245, Apr. 2010.
- [9] C. Jennings, "Nat Classification Test Results," IETF Internet draft, draftjennings-behave-test-results-04, July 2007, accessed Dec. 12, 2016.

- [10] A. M. Mandalari, M. Bagnulo, and A. Lutu, "Informing Protocol Design Through Crowdsourcing: The Case of Pervasive Encryption," *Proc. 2015 ACM SIGCOMM Wksp. Crowdsourcing and Crowdsourcing of Big (Internet) Data*, ser. C2B(1)D '15, 2015, pp. 3–8.

BIOGRAPHIES

ANNA MARIA MANDALARI (amandala@it.uc3m.es) completed her M.Sc. in telecommunications engineering at Mediterranean University of Reggio Calabria, Italy, in 2014 and her M.Sc. in telematics engineering at University Carlos III Madrid (UC3M), Spain, in 2015. She is a Ph.D. candidate in the Telematics Engineering Ph.D. programme at UC3M. She is doing her PhD in the context of the Marie Curie project METRICS on large-scale measurements of the effects of middleboxes in the Internet.

MIGUEL ANGEL DIAZ BAUTISTA (madiabz@indra.es) received a Bachelor's degree in computer science and engineering in 2014 from UC3M and his M.Sc. in telematics engineering in 2015. His current work is focused on Internet measurements, Android application implementation and cybersecurity.

FRANCISCO VALERA (fvalera@it.uc3m.es) received his telecommunication engineering degree in 1998 from the Technical University of Madrid (UPM), and his Ph.D. in telecommunications in 2002 from UC3M, where he is currently a tenured associate professor and head of the Telematics Engineering Department. He has published over 60 papers in the field of advanced communications in magazines and conferences.

MARCELO BAGNULO (marcelo@it.uc3m.es) received an Electrical Engineering degree in 1999 from the University of Uruguay, and a Ph.D. in telecommunications in 2005 from UC3M. In 2000 he joined the University Carlos III of Madrid, where he has been an associate professor since 2006. He has published over 60 papers in technical journals, magazines, and conferences, and he is a co-author of 18 IETF RFCs.

To the best of our knowledge, this is the largest dataset available describing the behavior of the deployed NAT base, and we believe it would provide useful input for application and protocol designers aiming to make their applications and protocols to work across NATs.

Load-Stress Test of Massive Handovers for LTE Two-Hop Architecture in High-Speed Trains

Ali Parichehreh, Umberto Spagnolini, Paolo Marini, and Alberto Fontana

The authors validate experimentally the traffic and HO latency improvements (approximately three-fold) in a multi-cell access scheme when the coverage of every single carriage is augmented by fixed directional antennas to offload UEs toward far-away eNBs along the train track.

ABSTRACT

Load-stress test is the experimental performance analysis in extreme traffic and density conditions, routinely required to validate any innovative radio access solution. This article focuses on load-stress test specifically designed for the two-hop architecture that enables the onboard connectivity in HSTs. The load-stress condition of train-to-infrastructure communication for a massive number of onboard UEs is very challenging, as it needs to account for extreme conditions and a complex testing environment. The load-stress method proposed in this article is for a ground network supporting onboard wireless connectivity in HSTs, and is validated for commercial eNBs from LTE cellular networks (Rel-11). The in-lab experimental setup is arranged by virtualizing multiple eNBs serving multiple cells, arranged sequentially along a line to simulate the HST track with a massive number of active onboard UEs. The focus of the experimental load-stress test is the analysis of the impact of Doppler shift and interruptions caused by the frequent HOs of multiple consecutive groups of UEs deployed in HST carriages at the speed of 300 km/h. The HO interruption time is characterized statistically based on the number of active UEs. The consequent impairments on the experienced QoS for high-throughput and low-latency services such as FTP and VoLTE are verified. This article validates experimentally the traffic and HO latency improvements (approximately threefold) in a multi-cell access scheme when the coverage of every single carriage is augmented by fixed directional antennas to offload UEs toward far-away eNBs along the train track.

INTRODUCTION

Seamless wireless connectivity in different mobility scenarios is one of the key requirements of fifth generation (5G) networks [1]. Recently, the Third Generation Partnership Project (3GPP) has standardized Long Term Evolution (LTE) and its advanced version, LTE-A, with a peak data rate up to 100 Mb/s in high-mobility scenarios (≥ 300 km/h), aiming at a trade-off between demanded data rate and quality of service (QoS) for high-speed train (HST) onboard passengers [2]. Despite this improvement, the hard handover (HO) nature of an LTE system, which breaks the connection before connecting to the target evolved NodeB (T-eNB), inevitably causes service interruption and degrades users' QoS.

In the HST scenario, the QoS of massive onboard UEs (say up to 1000) is highly critical, affected by different impairments such as frequent HOs, Doppler shift, and limited number of physical resource blocks (PRBs). The serving eNB (S-eNB) is highly loaded due to the large number of onboard user equipments (UEs) camped in, and when a cell change happens, the heavy HO signaling load increases both HO-induced latency and link failure rate. This situation worsens at higher speeds due to the Doppler shift and consequently the overall link quality degradation. Managing this signaling is very challenging as involves a large number of UEs, spatially concentrated in less than 200 m (i.e., the train length) moving at speeds up to 500 km/h (or equivalently, all onboard UEs cross cell-boundaries in less than 1.5 s).

Despite all the research activities on the HST onboard connectivity, due to a lack of a readily available testbed, any innovation in HST connectivity can only be validated by theoretical analyses and/or system-level simulations. Even if these validations can hardly reflect all side-challenges of actual systems [3–6], system-level simulations are crucial to highlight the importance of each individual aspect, but experimental measurements and testing with actual eNBs become mandatory to evaluate in-field benefits, possibly in realistic settings before network deployment.

The first preliminary experimental study of the LTE mobility management entity (MME), and specifically X2-based HO, was provided in [7]. A detailed analysis of the HO was investigated in [8], and a stochastic model for the HO interruption time (HIT) was extracted via a field test measurement for different urban scenarios. An experimental study analyzed the HO-induced latency in two slow and high-mobility scenarios, up to 100 km/h [9]. However, in the publicly available literature the network is loaded at most by 8 users/cell, and this load value is estimated as the experimental setup is not under complete control. This setup is not sufficient to measure the performance of the LTE network in extreme load conditions, especially in HSTs with up to 1000 UEs at speeds of 300 km/h or higher. In addition, these experiments lack control on the other active UEs' traffic and mobility profile.

Instead of conducting in-field measurements, we design a holistic laboratory experiment to evaluate the performance of MME of the LTE network with an off-the-shelf eNB, while providing high

throughput and/or low-latency Internet services for a massive number of HST onboard UEs. In these experiments, mobile UEs travel at the speed of 300 km/h, and the eNBs are frequently pushed to their load limits in a fully controlled environment. To the best of our knowledge, this is the first experimental lab study in the open literature focusing on the performance analysis of an actual LTE network along an HST railway, aiming at extracting the statistical characteristics of the frequent HOs and their impairment of the throughput, link failure, and call drop rate.

A load-stress test equipment for actual eNBs based on software defined radio is adapted to account for this critical mobility condition. The experimental setting is extended to validate different onboard relaying architectures for HSTs as specified by 3GPP [10], with conventional omnidirectional antennas and a multi-cell access scheme provided by directional antennas along the railway [4].

PRELIMINARIES

In this introductory section, we briefly detail the HST train-to-infrastructure connectivity, the HO procedure, and the multi-cell access scheme proposed to cope with massive HOs.

TWO-HOP ARCHITECTURE FOR A HIGH-SPEED TRAIN

Recently, 3GPP has standardized a two-hop architecture (Fig. 1) for HST onboard connectivity via relay nodes. Onboard relay nodes can be classified into either an layer 1 (L1)-relay or a mobile relay node (MRN) based on their functionalities.

An L1-relay is a bidirectional amplify-and-forward relay that bridges the onboard signals with the eNBs after some power equalization. An L1-relay can be considered as a low-cost solution to enable onboard connectivity, routinely deployed on HST for 2G and 3G networks, and for LTE Release 8 (Rel-8). In addition to the common disadvantages of amplify-and-forward relay, it leaves the mobility management of massive UEs to be carried out individually on each UE, and this is a remarkable drawback, as detailed later. MRNs from LTE Rel-12 are basically small cells acting as autonomous (and mobile) eNBs located in each carriage of an HST [11]. The onboard eNB acts as a compound UE that is, in turn, connected to the Donor-eNB via Un interface. Compared to L1-relay, an MRN is more complex and expensive. However, it provides one connection per carriage with a group-HO feature that performs one single HO for all the connected UEs, resulting in lower HO impairment and higher throughput per UE. The drawback of the MRN is that all the UEs will lose their connection in case of any link failure.

LTE HANDOVER ON HST

Generally, a HO procedure includes three phases: HO preparation phase (i.e., measurement report by UE and HO decision by eNB), HO execution phase (i.e., random access channel [RACH] procedure and synchronization to the T-eNB, and receiving uplink grant), and HO completion phase (i.e., path switching and bearer modification).

According to the LTE-A radio resource control (RRC) specification [12], UEs measure the reference symbol received power (RSRP) of the neighboring cells based on the configuration

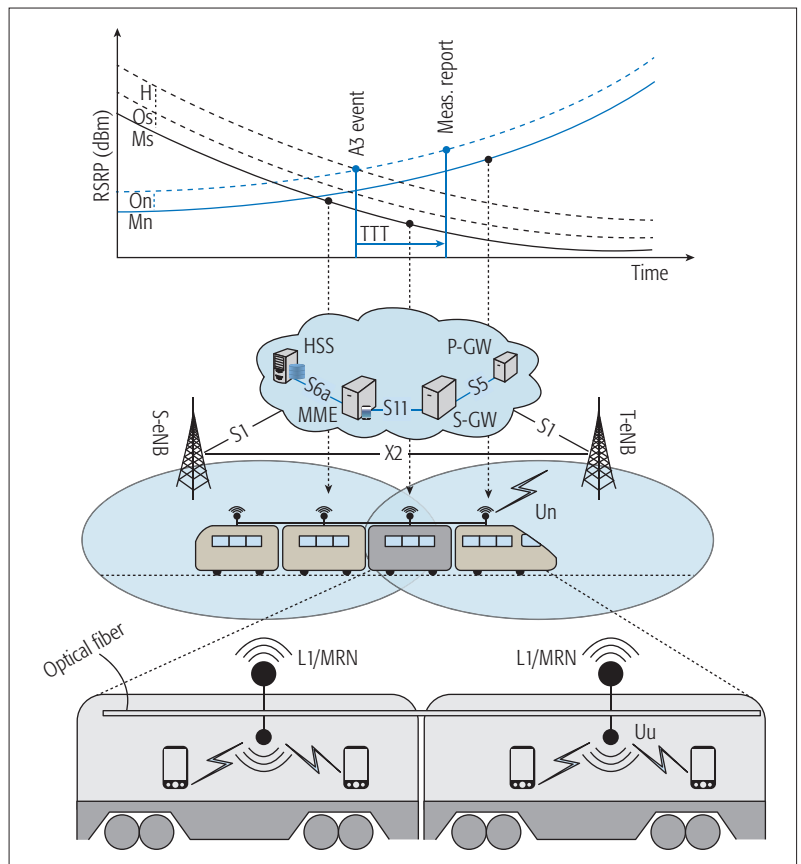


Figure 1. Two-hop architecture of an HST onboard LTE network. L1/MRN [10] on the roof of the HST. Inter-carriage communication through optical fiber, if present/necessary. A3 event for HO and related parameters (top).

in an `RRC_Connection_Reconfiguration` message received from the S-eNB. This message includes a list of neighbor eNBs to be measured and a reporting mechanism (i.e., periodic or event-based mechanism). In the periodic mechanism, UE measures the RSRP value periodically, while in the event-based mechanism, UE sends the measurement report once a certain event is triggered. Different types of events (labeled A1 to A5) can be configured in the `RRC_Connection_Reconfiguration` message to trigger a measurement report for different purposes. Among them, A2 and A3 events are commonly used for the HO procedure. An A2 event is used by UE for inter-frequency HOs to inform the eNB that the RSRP value of S-eNB is below a predefined threshold and receive the required measurement gaps necessary for inter-frequency HOs. An A3 event is used for reporting the power of received signals from serving and neighboring eNBs on the same or other configured frequencies.

As shown in Fig. 1, an A3 event happens when measured RSRP for neighbor cells (Mn) is larger than for the serving cell (Ms) up to some offset values (Os and On, for S-eNB and potential T-eNBs, respectively) and hysteresis value (H). In other words, $Mn + On > Ms + Os + H$. The S-eNB makes the HO decision according to the received measurement report, and sends information of the T-eNB to the UE through an `RRC_Connection_Reconfiguration` message to start the HO execution phase over the RACH. The HIT is

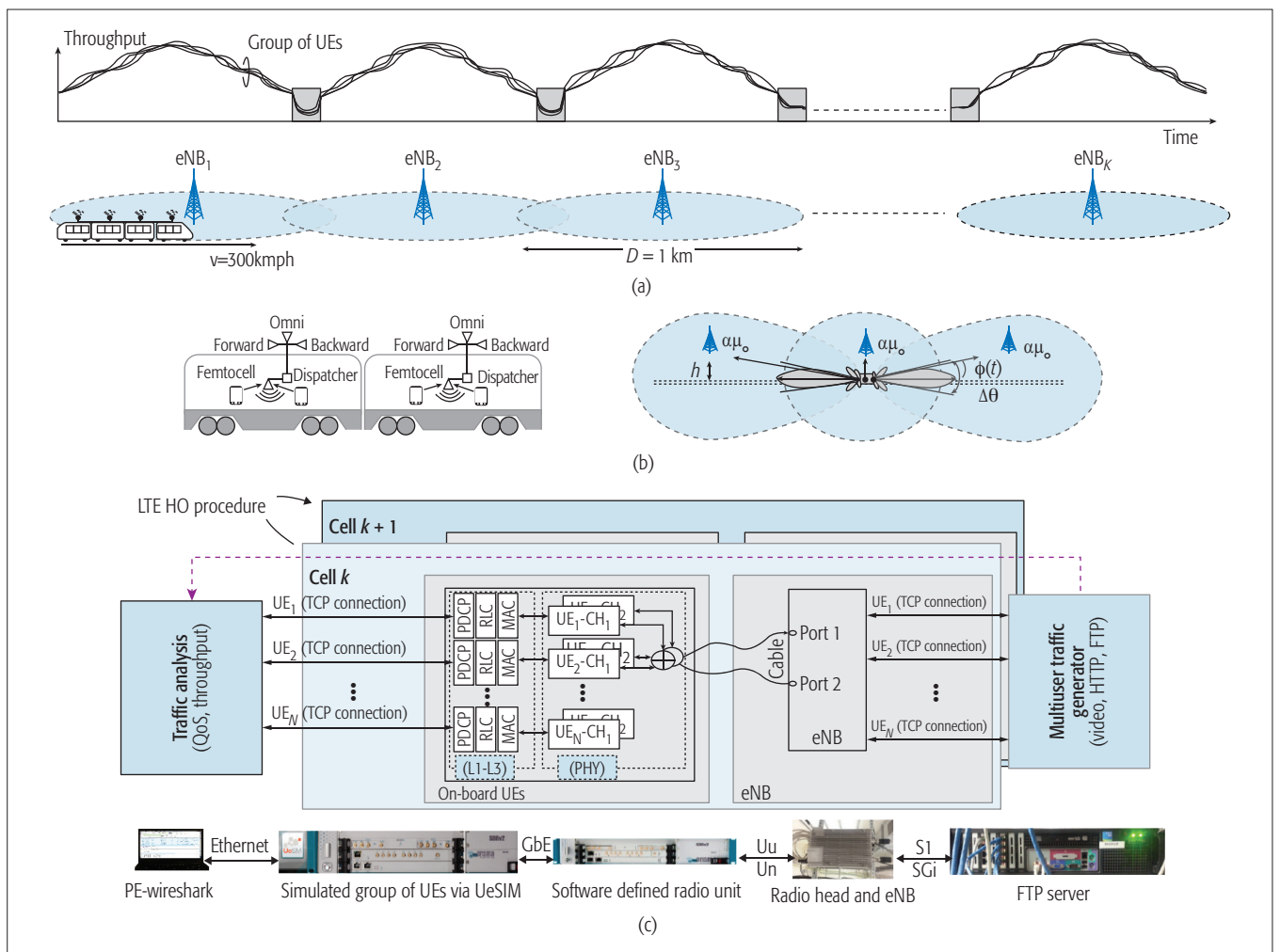


Figure 2. In-lab experimental setup overview: a) HST with $K = 200$ eNBs, cell size $D = 1$ km, $v = 300$ km/h, full-penetration loss, and instantaneous throughput of PDSCH for each UE (top), and HO (gray shaded area); b) two-hop architecture with augmented onboard relay node (L1 or MRN) with directional antennas to enable the multi-cell access scheme for two-hop architecture; c) UeSIM architecture for N UEs performing intra-frequency HO from S-eNB to T-eNB (cell k toward cell $k + 1$) with traffic generation and monitoring, and radio frequency channel emulator [14].

the interval from the time instance when the UE receives an `RRC_Connection_Reconfiguration` message to the time it sends an `RRC_Connection_Reconfiguration_Complete` message to the T-eNB after receiving an uplink grant. Finally, the HO completion phase according to the type of HO (e.g., intra-eNB, X2, or S1) will be executed.

We remark that, considering the specified two-hop architecture of HST connectivity, all the UEs inside each carriage experience the same M_s and M_n values. This is due to the fact that all the devices are served by the same wireless link provided by onboard relay (L1/MRN). Therefore, an A3 event will be triggered for all the UEs simultaneously. This potentially causes a bottleneck in the HO execution phase over the RACH.

DIRECTIONAL ANTENNAS FOR A MULTI-CELL ACCESS SCHEME

The purpose of a multi-cell access (MA) scheme on a train is to deploy multiple directional antennas on each carriage that diversifies the wireless connectivity over multiple eNBs [4]. Figure 2b shows the MA scheme that is compatible with either L1 or MRN onboard relaying. Onboard

UEs can be connected to different antennas that are either omnidirectional or directional pointing forward and backward to remote cells. These directional antennas have fixed beams that point toward lightly loaded distant eNBs, compared to the omnidirectional antenna for the local S-eNB in which the carriage is camped. A dispatcher balances the onboard UEs over the three cells (and the associated eNBs) depending on UE traffic intensity and ground eNB cell load. The MA scheme reduces the HO signaling of the local S-eNB, while distributing the carriage load among multiple eNBs and achieving higher capacity. That is, the HO decision can be manipulated by the spatial signal propagation of the directional antennas without any necessary coordination from the LTE eNB.

Compared to the current two-hop architecture [10], the directional antennas placed on each carriage that point toward less loaded neighbor cells manipulate the cell shape according to the directivity pattern (Fig. 2b). Directional antennas do not need to be adaptive as the track is mostly straight to avoid lateral passengers' accelerations at 300–500 km/h, and eNBs are cus-

tomarily deployed off-track, close to the track for maximum efficiency distance = 50 m [13]. This simple method provides an augmented number of resources (i.e., PRB and PRACH channels) for massive onboard UEs that, in turn, increases data rate and shortens the HIT for onboard UEs.

LOAD-STRESS TEST FOR HSTs: CASE STUDY AND EXPERIMENTS

Rather than having a collection of UEs onboard the HST, the lab system is based on adaptation of UeSIM, a load-stress testing equipment for the LTE radio interface and core network [14]. UeSIM is a commercial load and stress testing system able to load an eNB on the RF interface, simulating thousands of UEs, each with a different channel and traffic model, toward the same eNB (or two eNBs when in the HO region). The test evaluates the individual/aggregate QoS of massive onboard UEs in the HST scenario, using commercially available eNBs with individual UEs supporting high-throughput and/or low-latency services such as FTP and voice over LTE (VoLTE). The UeSIM system in Fig. 2 is able to load up to 8 sectors supporting all frequency bands including frequency-division duplex (FDD) and time-division duplex (TDD) frame types. Besides a customized Wireshark packet analyzer that is used to capture packets at the Uu radio interface, UeSIM provides counters at each protocol layer, aggregated at the UE, group of UEs, or eNB level to measure the network performance while simulating the mobility of the HST. The main benefit of using lab testing instead of in-field experimentation is that the number of UEs and their parameters can be individually configured from the design of the deployment scenarios to the UE behavior (from the physical layer up to the application layer parameters, radio bearer type, and mobility/traffic profiles).

The network configuration for the HST load-stress test is laid out in Table 1. The LTE air link operates at the 7th frequency band (2.6 GHz) with FDD frame structure. The bandwidth is 10 MHz, and the simulated UEs are from category 4, supporting 2×2 multiple-input multiple-output (MIMO) and up to 150 Mb/s in downlink (DL) when using a 64-quadrature amplitude modulation (QAM) and coding scheme. There are two HST scenarios of N UEs with homogeneous traffic: i) each UE downloads a 1 GB file from an external FTP server through LTE eNB over the default bearer; ii) each UE is configured to establish VoLTE over a dedicated bearer with guaranteed bit rate throughput. The UeSIM emulates the behavior of N UEs with an individual LTE protocol stack from Non Access Stratum (NAS) protocol (3GPP-TS 24.301) to the physical layer baseband processing (3GPP-TS 36.101) according to the LTE specification (Rel-11), running over a software defined radio module controlled by a multicore Linux machine. The propagation channel (e.g., path loss, fading, multipath, Doppler shift, and noise) is simulated by controlling the impairments individually for each UE at the level of baseband IQ stream, as shown in Fig. 2c. The propagation over the air link is replaced by a coaxial cable (to avoid illegal frequency radiation) toward a 2×2 MIMO eNB. In the conducted experiments, we

Network configuration				
eNB	LTE (Rel-11) band 7	Downlink 2620 MHz	Uplink 2500 MHz	Bandwidth 10 MHz
Cell size	1 km			
Off-track distance	50 m [13]			
UE category	Cat 4, 2×2 MIMO, 150 Mb/s (with 64-QAM MCS)			
Mobility scenario	300 km/h			
Number of UEs	{8,10,15,18,22,30} per carriage			
Internet service type	FTP, VoLTE			
HO configuration				
Hysteresis	0 dB			
A3-offset	2 dB			
Time to trigger	40 ms			
RACH configuration				
PRACH configuration index	3			
Total number of dedicated preambles	56			
Maximum preamble transmission	10			
RA response window size	8 ms			

Table 1. A summary of the test configuration.

consider a train with $M = 4$ carriages in a rural area and N UEs ($N = 32, 40, 60, 72, 88, 120$) moving at $v = 300$ km/h over a 200 km track (total runtime is 40 min) of K sequential eNBs (here $K = 200$) with cell size $D = 1$ km (according to the open space scenario specified in [13]). All the K eNBs are placed in the middle with omnidirectional antennas, as shown in Fig. 2a. Given these specified parameters, the train crosses cell boundaries every 12 s. Each carriage has $N/M = \{8, 10, 15, 18, 22, 30\}$ UEs on the same carrier frequency. Inter-carriage HO delay is 300 ms (i.e., time interval for two consecutive carriages for crossing the cells, assuming a carriage length of 25 m).

To carry out a holistic experimental study on the impact of massive onboard UEs on the HIT and TCP DL throughput of the LTE network, we extract a statistical model of the HIT, and verify the impact of the HIT on the FTP DL throughput for the ensemble of all N UEs by measuring the instantaneous physical downlink shared channel (PDSCH) throughput dedicated to FTP services. We first disable the Doppler shift to evaluate the HIT and the impact of HO on FTP throughput; then the effect of Doppler shift on the link and service failure is individually investigated for VoLTE service.

Each load test emulates an HST over a 200 km track by extracting the individual and aggregated statistics of UEs with sampling granularity of approximately 1 s. For every HST run, each UE performs 200 HOs, and the LTE network fulfills

$N \times 200$ HO requests. Figure 2a exemplifies the instantaneous PDSCH throughput of a subset of UEs with respect to the HST position along the track. The communication link between onboard UEs and eNBs has been designed to emulate the two-hop architecture when employing the onboard relay on top of each carriage, with either an L1 relay or an MRN. The set of eNBs to evaluate the massive HOs are configured to handle multi-sectors, and the lab setup is configured to have the train virtually move in a circle, flipping from one eNB to another.

EXPERIMENTAL RESULTS

HO LATENCY MODEL AND DISTRIBUTION

The analysis of RRC messages reveals that A3-event-based measurement of RSRP is configured for inter- and intra-frequency HOs, according to the predefined HO parameters: hysteresis and time to trigger. When HST moves across cells, the S-eNB receives the measurement report for the RSRP from UE to fulfill the HO decision procedure. Then the S-eNB

sends the required RACH resource (including a new C-RNTI, dedicated preamble index, RACH response windows size, etc.) to allow the UE to switch from the S-eNB to a T-eNB. Note that a dedicated RACH preamble is optional, and without a dedicated RACH preamble from the eNB, each UE selects any random preamble to transmit over the contention-based RACH channel. Here, eNBs are configured to send the dedicated preamble following the contention-free RACH procedure.

Even though there is a minimum deterministic delay, HO interruption time T_{off} can be modeled as a random variable depending on a complex set of parameters such as the speed of HST, cell size, and cell load [4]. For the HST travelling at $v = 300$ km/h, each UE experiences a random but periodic HIT at cell-change (every $T = 12$ s). Hence, for each carriage the off-service interval T_{off} occurs periodically and varies randomly. This causes a *cyclostationary* service model for each UE that experiences the HIT every T s. Moreover, for an HST at the speed of 300 km/h with carriage length $d = 25$ m, the HO slides backward over the consecutive carriages every 300 ms. The HO-induced latency impairs the onboard UEs' QoS gradually, and worsens over the last carriages. Thus, the QoS for onboard users depends on their carriage position, the speed of the train, and the degree of overlapping of HOs among the consecutive carriages.

The HO properties for massive UEs connected via the L1-relay node (currently deployed on the HSTs) are characterized based on the statistical analysis of the HITs vs. the number of UEs for $n \times 4$ scenarios (n UEs on each carriage and 4 carriages) in Fig. 3. HIT T_{off} can be modeled as a random variable with Nakagami distribution in accordance with the exact number of onboard UEs regardless of some minimum latency due to inherent signaling delay [12]. Distribution in Fig. 3a shows that the QoS impairment is dominated by the tails of the probability density function of T_{off} , and the spread parameter Ω of Nakagami distribution captures this impairment effectively. Note that Ω varies depending on the number of UEs, T-eNB load, and the speed of the HST, and spread $\sqrt{\Omega}$ linearly increases with N as highlighted in Fig. 3b. This is due to the limited number of PRACH resources dedicated to each eNB for HO signaling, and in our testbed we allocated 56 preambles in each eNB reserved for the RACH procedure with a 10 ms RACH period, wherein only two preambles will be detected and responded to by the eNB in each RACH channel. Therefore, the successful HO for 70 percent of the 120 UEs (in the 30×4 scenario) over the contention-free RACH channel takes at least 600 ms (without preamble misdetection). Compared to urban scenarios (low mobility) where the HIT follows a normal distribution [8], our lab experiments for the HST (high mobility) scenario with frequent and simultaneous HOs are better described by the Nakagami distribution, which accounts for heavy tails of the HITs. Similar to low mobility [8], the mean value and standard deviation of the HIT in Fig. 3b linearly increase with cell load at a higher rate compared to [8]. Results for other scenarios (e.g., 10×4 , 18×4) confirm the results so far.

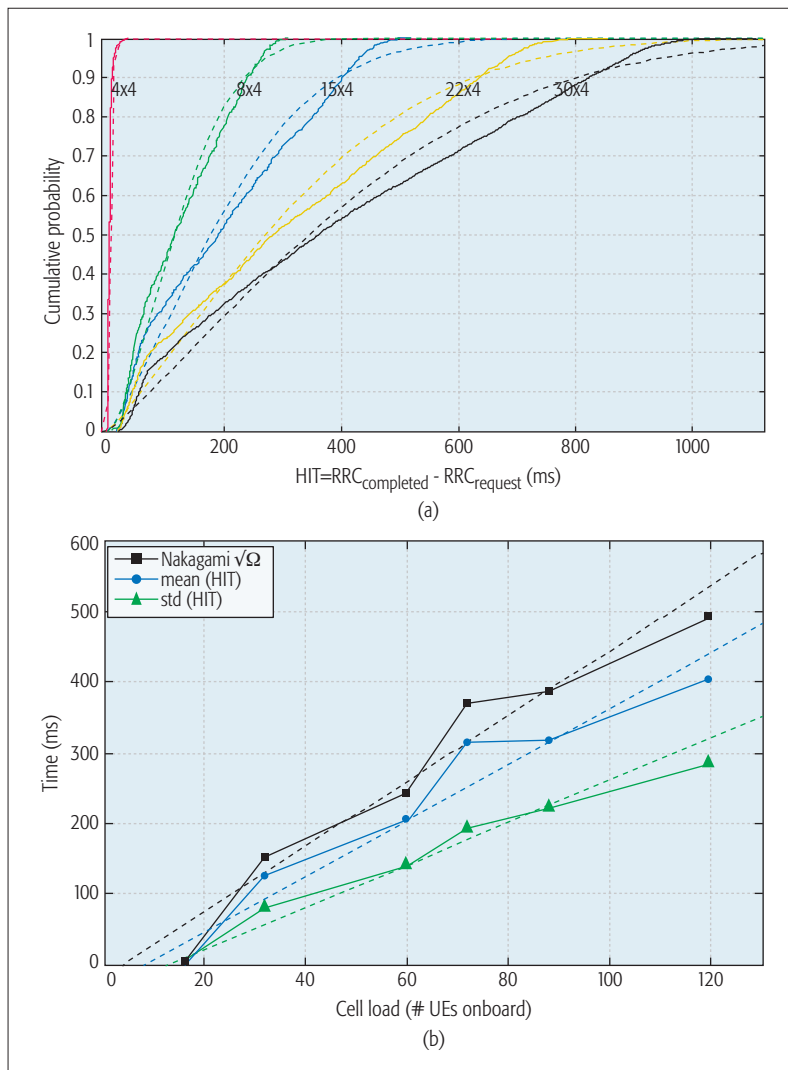


Figure 3. HO interruption time analysis vs. the number of UEs for L1 relay architecture: a) empirical CDF of HIT (solid lines) and Nakagami distribution fitting (dashed lines); b) Nakagami spread control parameter $\sqrt{\Omega}$, mean value and standard deviation of the HITs vs. the cell load, linear fitting vs. UEs (dashed line).

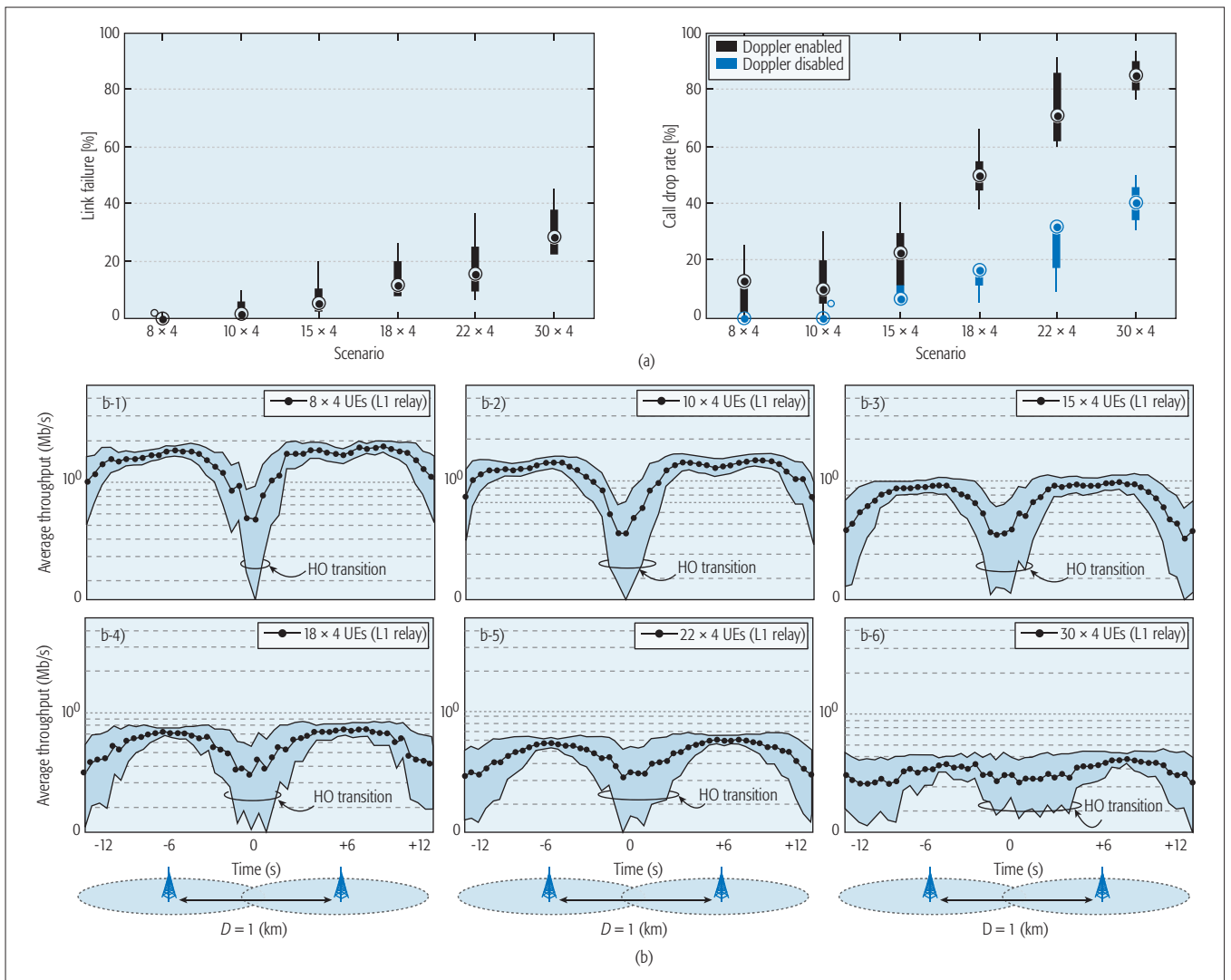


Figure 5. a) The effect of massive HOs on link failure and VoLTE call drop rate; b) the effect of massive onboard UEs on the PDSCH throughput (standard deviations in shaded area); HST with $M = 4$ carriages and $\{8, 10, 15, 18, 22, 30\}$ UEs per carriage, at speed $v = 300$ km/h. UEs are connected to the eNBs through L1-relay.

HO IMPAIRMENT ON LINK FAILURE AND VOLTE CALL DROP RATE

The effect of the HOs from a massive number of onboard UEs on the link failure rate (when Doppler shift is enabled) is shown in Fig. 4a. Link failure is the result of HO failure (due to preamble misdetection). Considering the small off-track distance, at the speed of 300 km/h, Doppler shift varies between $[-722 \text{ Hz}, +722 \text{ Hz}]$ in downlink, and $[-1444 \text{ Hz}, +1444 \text{ Hz}]$ in uplink (i.e., each UE estimates the channel comprehensive of Doppler shift in downlink, and replies with that frequency shifted synchronization in uplink, which sums to the Doppler). In order to have tractable and reproducible measurement and analysis, here we assume that the train is affected by a fixed Doppler, although in reality the speed of the train is not fixed over the track and Doppler transition when crossing the eNB imposes severe impairments on the link quality. Due to the Doppler shift and transition effects, we experienced that T-eNB fails to detect the dedicated preambles and UEs fail to accomplish the RRC reestablishment procedure. Consequently, links fail, and the link

failure rate increases significantly in high loading scenarios. This is shown in Fig. 4a; up to 40 percent of the mobile users experience link failure in the scenario with 30×4 mobile UEs.

In order to evaluate the effect of link failure on QoS, all UEs use VoLTE service with a narrow-band G.711 audio codec over RTP and dedicated bearers with QoS Class Identifier (QCI) = 1 (45 kb/s guaranteed bit rate in UL and DL directions). Open source Kamailio is the Session Initiation Protocol (SIP) server. Figure 4a illustrates the call drop without Doppler (only HO interruptions) and with Doppler enabled vs. the increasing number of mobile users, VoLTE call drop rate dramatically increases. When 120 UEs are onboard the HST, the call drop rate is 90 percent and service is useless. Again, this impairment is not only due to the link failure but also long latency induced by HO (note that the packet delay budget for QCI = 1 is 100 ms, while the HO latency lasts up to 1000 ms). At the cell boundary there is congestion on the RACH channel (besides path loss attenuation at cell boundaries), and the SIP server assumes that channel quality is not acceptable and drops the call with standard *cause-code=6*

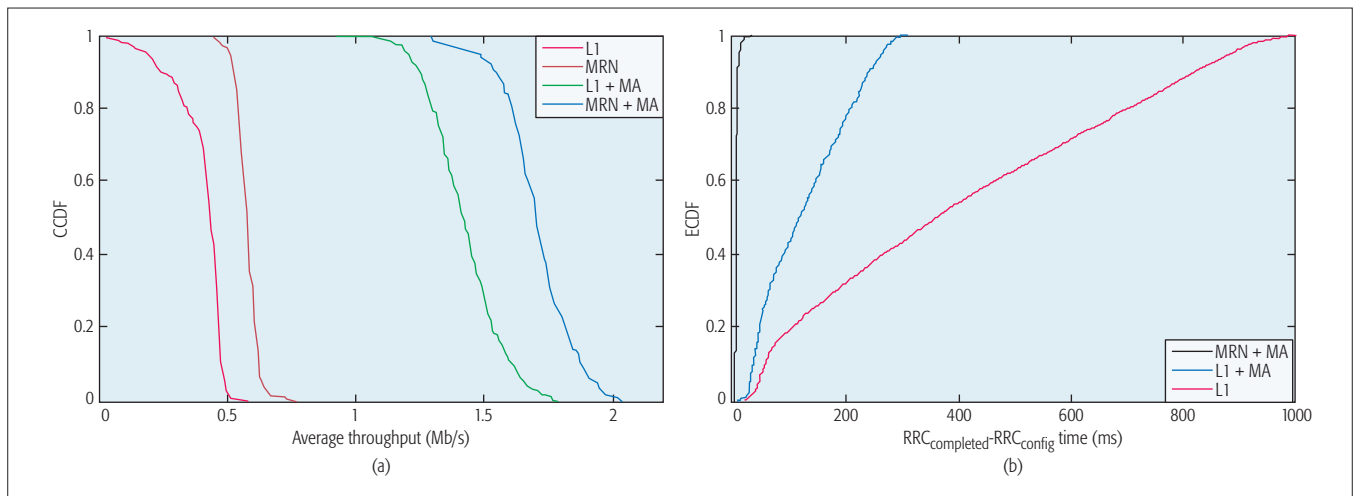


Figure 5. Cumulative distribution function (CDF) of FTP DL-throughput per UE: a) and HO time b) for different relay technologies and multi-cell access (MA) method for the heavy load case of 30 UEs per carriage (case 30×4).

(i.e., unacceptable channel according to SIP specification). This accurately reflects the nature of the internal failure over the radio interface at cell boundaries. The comparison of call drop rate with Doppler disabled shows quantitatively the compound effects of each term on the QoS.

HO IMPAIRMENT ON THE FTP DL-THROUGHPUT

The effect of the HO over the throughput of the massive onboard UEs is shown in Fig. 4b. Due to the cyclostationary behavior of the throughput, collected data are illustrated around the HO occurrence point (used for time reference: $t = 0$). Figure 4b highlights that at the cell edges the average throughput drops due to the simultaneous HOs, and UEs experience the maximum throughput inside the cell that scales by $1/N$ (70 Mb/s/ N per UE), and it decreases to 300 kb/s when increasing the number of active UEs up to 120. The 8 kb/s traffic of system information block transmission on the PDSCH is not accounted for in the per-user throughput.

When cells are heavily loaded, as for 30×4 (120 UEs over 4 carriages), the fluctuations of throughput (shaded area) increases due to the multiple HO transitions that leave the UEs in outage for long time intervals (up to 1 s for 30×4 ; Fig. 3a). More precisely, the limited number of preambles for HO signaling on one side, and the eNB's limited capability in answering the HO requests on the other side, keep the T-eNB from responding to all the HO requests in a timely manner. In fact, the S-eNB buffers the incoming measurement reports and responds to only two of them in every RACH period. Therefore, additional delay overhead on the RACH channel is inevitable (especially for the UEs located in the tail carriages of the train), which accordingly affects the congestion control procedure on the transport layer and shortens the FTP window size due to unacceptable link quality at cell boundaries.

Note that this part of the experimental result is purposely without Doppler shift to isolate the impact of the frequent HOs on the QoS of onboard users vs. the number of UEs. Since Doppler degrades overall performance considerably (with higher preamble misdetection probability and lower throughput), the results here

are the reference bound for the UE density and the specific eNB manufacturer. Note that including Doppler shift in this experiment could cause link failure, which augments the instability in the experiment and prevents the HO analysis.

LOAD TEST FOR THE MULTI-CELL ACCESS SCHEME

In L1-relay, when increasing the number of UEs, the throughput per UE decreases quite dramatically due to the mobility management for massive UEs treated independently from one another. An MRN copes with this drawback by leaving one HO per cell, thus gaining all the benefits in terms of throughput, as shown in Fig. 5a for 30×4 UE load. However, the multi-cell access (MA) scheme can reduce the massive UEs impairment, providing higher throughput and HO signaling performance, by diversifying the traffic load over three eNBs at the same time, possibly with non-overlapping HO.

The load test results for massive UEs can be extrapolated to infer the performance of the MA scheme with two additional onboard relays connected to two different eNBs located ahead of and behind the S-eNB in which that train is located. Experimental results on the same setup (only 30×4 is shown here) are in Fig. 5a, and prove that the MA scheme increases the throughput per UE up to approximately three times more compared to the conventional relay with one omnidirectional antenna per carriage. The use of three MRNs per carriage equipped with omnidirectional antennas (MRN+MA) outperforms the other schemes due to the group-HO feature that reduces the HO time for the onboard UEs. Furthermore, the L1-relay with MA scheme is a simple and effective solution for the massive UEs provided that mobility management is redesigned to account for the independent UEs to camp over far-ahead cells. As a drawback, L1+MA suffers from the cumbersome HO signaling that causes an increasing HO failure rate (around 2–6 percent for 88–120 onboard UEs for the L1-relay), while the HO failure was negligible for the MRN.

In L1-relay with omnidirectional antenna the eNB should manage 120 HOs almost simultane-

ously, and this extends the HO time up to 1 s (Fig. 5b) as a consequence of the limited number of PRACH channels dedicated to the HO procedure in each eNB. However, in the scenario with the L1-relay node with augmented coverage with the MA scheme, it can be observed that the HO time lasts no more than 300 ms. In fact, the MA scheme diversifies the HO signaling over multiple cells. In the scenario in which HST is equipped with an MRN, the HIT is less than 40 ms, which meets the IMT-Advanced HO requirements, that is, 60 ms. In the MRN the MA scheme has no practical impact on HO (same as HO time of a single UE) but rather on throughput, as shown in Fig. 5a.

CONCLUSION

In this article, we introduce a novel ad hoc load-stress testing method to analyze the performance of LTE eNBs in high-mobility scenarios when onboard connectivity is established over two-hop train-to-infrastructure architecture. We extract the statistical characteristics of the X2-based HO interruption time and its impairments on the throughput, link failure, and VoLTE call drop rate. The HO interruption time for each onboard UE is modeled by a Nakagami distribution, in which the spread control parameter depends on the cell load and number of active UEs. The lab experiment at 300 km/h (but extension of the setup to higher speed is conceptually straightforward) highlights quantitatively how the QoS at the cell edge is reduced due to the HO-induced latency. The augmentation of onboard relay nodes (L1/MRN) with fixed directional antennas can remarkably enhance by three times the QoS of massive UEs by offloading the traffic over lightly loaded cells, with faster HO responses and larger throughput.

The load-stress test highlighted some areas of improvements in HST communication:

- Adaptation of network mobility management by reducing the RA response period and/or improving the RACH processes in eNB (to manage more RACH requests at the same time)
- Offloading the traffic among the carriages during the HO interruption time
- Optimization of MA scheme via beam-width coordination of directional antennas

REFERENCES

[1] 5G Forum white paper, "5G Vision, Requirements, and Enabling Technologies," (v.2.0), 2016.
 [2] A. Ghosh *et al.*, "LTE-Advanced: Next-Generation Wireless Broadband Technology," *IEEE Wireless Commun.*, vol. 17, no. 3, June 2010, pp. 10–22.
 [3] A. Sniady *et al.*, "Ensuring Long-Term Data Integrity: ETCS Data Integrity Requirements Can Be Fulfilled Even under Unfavorable Conditions with the Proper LTE Mechanisms," *IEEE Vehic. Tech. Mag.*, vol. 11, no. 2, 2016, pp. 60–70.
 [4] A. Parichehreh *et al.*, "Seamless LTE Connectivity in High-Speed Trains," *Wireless Commun. Mobile. Comp.*, vol. 16, no. 12, 2015, pp. 1478–94.

[5] T. Han and N. Ansari, "Radio over Fiber as an Antenna Extender for High-Speed Train Communications," *IEEE Wireless Commun.*, vol. 22, no. 1, Feb. 2015, pp. 130–37.
 [6] D. Xenakis *et al.*, "Mobility Management for Femtocells in LTE-Advanced: Key Aspects and Survey of Handover Decision Algorithms," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 1, 2014, pp. 64–91.
 [7] A. Elnashar and M. A. El-Saidny, "Looking at LTE in Practice: A Performance Analysis of the LTE System Based on Field Test Results," *IEEE Vehic. Tech. Mag.*, 2013, vol. 8, no. 3, pp. 81–92.
 [8] D. Han *et al.*, "Measurement and Stochastic Modeling of Handover Delay and Interruption Time of Smartphone Real-Time Applications on LTE Networks," *IEEE Commun. Mag.*, vol. 53, no. 3, Mar. 2015, pp. 173–81.
 [9] L. C. Gimenez *et al.*, "Mobility Performance in Slow- and High-Speed LTE Real Scenarios," *IEEE VTC Spring*, Nanjing, China, 2016.
 [10] 3GPP TR 36.836, "Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Study on Mobile Relay (Release 12)," <http://www.3gpp.org/>, accessed Dec. 20, 2016.
 [11] Y. Sui *et al.*, "Moving Cells: a Promising Solution to Boost Performance for Vehicular Users," *IEEE Commun. Mag.*, vol. 51, no. 6, June 2013, pp. 62–68.
 [12] 3GPP TS 36.331, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification (Release 13)," <http://www.3gpp.org/>, accessed Dec. 20, 2016.
 [13] 3GPP TS 36.104, "Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) Radio Transmission and Reception (Release 13)," <http://www.3gpp.org/>, accessed Dec. 20, 2016.
 [14] Prisma white Paper, "UeSIM: Multi-UE Simulation over Radio Interface with a Single Device," <http://www.primatelecomtesting.com/>, accessed Dec. 20, 2016.

BIOGRAPHIES

ALI PARICHEHREH (alip@primatelecomtesting.com) received his Ph.D. degree in information technology from Politecnico di Milano, Italy, in 2015. During his Ph.D. research activity he participated in multiple national and European projects (e.g., the DIWINE EU-FP7 project). He has worked as a research engineer at Prisma Telecom Testing Company since October 2015. His current research interests include wireless networks measurement and testing, as well as resource allocation and scheduling.

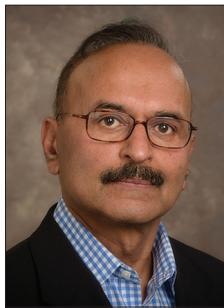
UMBERTO SPAGNOLINI (umberto.spagnolini@polimi.it) received his degree in electronic engineering (cum laude with honors) from Politecnico di Milano in 1988. He is a professor of statistical signal processing and has been a faculty member of Politecnico di Milano since 1990. He is an author of more than 300 papers and patents on methods for MIMO and cooperative communications, waveform design, and distributed synchronization. His current research interests include future broadband communication systems.

PAOLO MARINI (paolom@primatelecomtesting.com) received his M.Sc. degree in electronic engineering from Politecnico di Milano in 1987. He is one of the founders and a board member of PRISMA Telecom Testing, a T&M company focused on RAN testing, where he is VP Business Development and Marketing. His expertise covers design, testing, and management in the mobile communications area. He is also an author of several international patents. His current research interests include wireless networks validation, verification, and testing.

ALBERTO FONTANA (albertof@primatelecomtesting.com) received his M.Sc. degree in telecommunication engineering from Politecnico di Milano in 2004. From 2004 to 2007 he worked for Siemens and Nokia Siemens Network in R&D for UMTS technology and from 2008 to 2012 in LTE network technology. He has worked as a research engineer at Prisma Telecom Testing Company since 2012. His current research interests include wireless networks validation, verification, and testing.

The augmentation of onboard relay nodes (L1/MRN) with fixed directional antennas can remarkably enhance by x 3 the QoS of massive UEs by offloading the traffic over lightly loaded cells, with faster HO responses and larger throughput.

RADIO COMMUNICATIONS: COMPONENTS, SYSTEMS AND NETWORKS



Amitabh Mishra



Tom Alexander

Welcome to the March 2017 issue of the Radio Communications Series!

Wireless communications cover a wide range of fields and engage engineers from a broad array of disciplines. In keeping with this tradition, the three papers in this issue of our Series cover the gamut of wireless protocol layers – all the way from physical to the application layer.

Our first article, “Enabling Technologies toward Fully LTE-Compatible Full-Duplex Radio,” deals with a purely PHY layer topic: cancellation of self-interference between cellular transmitters and receivers. While substantial increases in efficiency of full-duplex operation are taken for granted in modern optical and copper transmission systems, wireless communications are not so lucky. Realizing practical full-duplex radios is a very complex and difficult signal processing problem (particularly in view of the space and power limitations of modern handsets). However, it is of great current interest due to the possibility of immediately doubling channel capacity in our scarce radio spectrum. The authors of the article suggest a different approach to full-duplex radio in LTE networks, where the cancellation functions are restricted to the base stations (i.e., eNodeBs). This has the benefits of simplicity, backward compatibility, and imposition of fewer constraints on the cancellation process. The article provides a broad overview of various self-interference cancellation approaches, highlights key difficulties with implementing such cancellations in actual systems, and briefly describes a testbed for exploring the proposed approach and presents some experimental results.

In contrast to the preceding article, our next article relates to the medium access control and network layers of a 5G network. The next generation of cellular networking technology is expected to support significantly higher channel bandwidths, but at the same time stringently limit end-to-end latency to support emerging applications such as telesurgery and automotive control. Millimeter wave (mmWave) bands coupled with small cell techniques can certainly provide the necessary capacity, but latency remains a critical issue. Computationally challenged radios together with large numbers of small cell communication links are not a good recipe for avoiding network delays. Titled “Achieving Ultra-Low Latency in 5G Millimeter Wave

Cellular Networks,” the article surveys some of the challenges to be faced, ranging from core network architecture down to low-level MAC functions. The authors also note that congestion control is likely to prove difficult in mmWave systems, and must be addressed if end-to-end latency is to be reduced. It closes by pointing out some directions for future work on this subject.

The final article in our issue is “Opportunities and Challenges of Trip Generation Data Collection Techniques Using Cellular Networks,” and covers session and application layer methods of localizing handsets. As we all know, cellular or Wi-Fi based tracking of personal mobile phones carried by pedestrians and automobile drivers is standard fare today, serving purposes ranging from the critical (e.g., supporting emergency services) to the mundane (e.g., indoor retail advertising). In most cases such tracking is done with the active assent and participation of the user; for example, by signing a service contract or being prompted to install an application. Passive and anonymous tracking is normally prevented by Wi-Fi and 3GPP security measures. The article reviews 3GPP security requirements protecting the privacy of mobile users, and then identifies some methods whereby these security measures can be circumvented to enable the location of handsets by third parties. In addition to tracking the location of pedestrians, the authors also show how handsets can be identified and traced back to their owners, which is essential for most tracking applications to be useful. The article focuses on locating and identifying mobile handset users without invading their privacy. In fact, the authors place particular emphasis on the security and privacy issues of methods such as those proposed to collect information about users; they note that significant societal, legal, and security concerns need to be addressed as part of the development of such systems.

We appreciate the contributions of the authors of the articles in this issue, and would also like to take this opportunity to express our gratitude to our many reviewers for helping us select and improve these articles. The support and encouragement of the Editor-in-Chief and the publication staff are much appreciated as well. And, as usual, we encourage our readership to submit articles discussing emerging trends in wireless communications.

CALL FOR PAPERS

IEEE COMMUNICATIONS MAGAZINE

EMERGING TRENDS, ISSUES, AND CHALLENGES IN BIG DATA AND ITS IMPLEMENTATION TOWARD FUTURE SMART CITIES

BACKGROUND

The world is experiencing a period of extreme urbanization. Cities in the 21st century will account for nearly 90% of the global population growth, 80% of wealth-creation and 60% of total energy consumption. The world urbanization continues to grow, and the global population is expected to double by 2050. Smart Cities are emerging as a priority for research and development across the world. In general, Smart cities integrate multiple Internet of Things (IoT) and emerging communication technologies such as fifth generation (5G) solutions in a secure fashion to manage a city's assets, such as transportation systems, hospitals, water supply networks, waste management. The goal of building a smart city is to improve the quality of life by using technology to improve the efficiency of services and meet residents' needs.

Smart cities' economic growth and large-scale urbanization drive innovation and new technologies. Technology is driving the way city officials interact with the community and the city infrastructure. The rapid progress in smart cities research is posing enormous challenge in terms of large amounts and various types of data at an unprecedented granularity, speed, and complexity are increasingly produced by the sensors of IoT via emerging communication technologies. Meanwhile, the accumulation of huge amounts of data can be used to support smart city components to reach the required level of sustainability and improve living standards. Smart cities have become data-driven, thus effective computing and utilization of big data such as distributed and parallel computing, artificial intelligence and cloud/fog computing are key factors for success in future smart cities. The use of big data can certainly help create cities where infrastructure and resources are used in a more efficient manner.

Any smart city project willing to use big data will need to capture, store, process and analyze a large amount of data generated by several sources to transform the data into useful knowledge that is applicable to a decision-making process. For example, with the help of big data and its Implementation, citizens could rapidly find available parking slots in large urban areas; big data can contribute in the city's efforts to reduce pollution through the deployment of street sensors. These sensors can measure traffic flows at different times as well as total emissions. The government can implement actions to divert traffic to less congested areas in a move to reduce carbon emissions in a particular area.

This Feature Topic (FT) is intended to encourage high-quality researchers in big data and its Implementation for future smart cities, and push the theoretical and practical research forward for a deeper understanding of future smart city constructions and operations.

In this FT, we would like to try to answer some (or all) of the following questions:

How to analyze the mass data that IOT devices produce by future smart cities? How to design the algorithm to process the mass data? How to utilize the machine learning and artificial intelligence techniques to improve the quality of life for future smart cities? How to utilize the "big data" to improve the QoS for future smart cities? How to guarantee the security and the privacy when mass data generated by IOT devices of future smart cities? How to diagnose the fault among the mass IOT devices of future smart cities? How to design the hardware to be suitable to process the mass data, among others?

Topics of interest include, but are not limited to:

- Distributed and parallel algorithms for big data in smart cities
- Big data analytics in data processing center for smart cities
- Cloud/fog computing in data processing center for smart cities
- The application of mobile cloud/fog computing for smart cities
- Fault tolerance, reliability and survivability in smart cities
- E-health and connected healthcare systems in smart cities
- Cyber-physical and social computing and networks in smart cities
- Environmental and urban monitoring in smart cities
- QoS and QoE of systems, applications, and services for smart cities
- Safety, security, privacy and trust in applications and services for smart cities
- Other topics related to big data and its implementations for smart cities

SUBMISSIONS

Articles should be tutorial in nature, with the intended audience being all members of the communications technology community. They should be written in a style comprehensible to readers outside the specialty of the article. Mathematical equations should not be used (in justified cases up to three simple equations are allowed). Articles should not exceed 4500 words (from introduction through conclusions). Figures and tables should be limited to a combined total of six. The number of references is recommended not to exceed 15. In some rare cases, more mathematical equations, figures, and tables may be allowed if well-justified. In general, however, mathematics should be avoided; instead, references to papers containing the relevant mathematics should be provided. Complete guidelines for preparation of the manuscripts are posted at <http://www.comsoc.org/commag/paper-submission-guidelines>. Please send a PDF (preferred) or MSWORD formatted paper via Manuscript Central (<http://mc.manuscriptcentral.com/commag-ieee>). Register or log in, and go to Author Center. Follow the instructions there. Select "December 2017 / Emerging Trends, Issues and Challenges in Big Data and Its Implementation towards Future Smart Cities" as the Feature Topic category for your submission.

IMPORTANT DATES

- Manuscript Submission Deadline: April 1, 2017
- Decision Notification: August 1, 2017
- Final Manuscript Due Date: September 15, 2017
- Publication Date: December 2017

GUEST EDITORS

Guangjie Han
Hohai University, China
hanguangjie@ieee.org

Jaime Lloret
Universidad Politecnica de Valencia, Spain
jlloret@dcom.upv.es

Liangtian Wan
Nanyang Technological University, Singapore
wan.liangtian.2015@ieee.org

Sammy Chan
City University of Hong Kong, Hong Kong, China
eeschan@cityu.edu.hk

Mohsen Guizani
University of Idaho, USA
mguizani@ieee.org

Wael Guibene
Intel Labs, Ireland
wael.guibene@intel.com

Enabling Technologies toward Fully LTE-Compatible Full-Duplex Radio

Gosan Noh, Hanho Wang, Changyong Shin, Seunghyeon Kim, Youngil Jeon, Hyunchol Shin, Jinup Kim, and Ilgyu Kim

The authors provide technical challenges and solutions for an LTE-compatible full-duplex cellular network, featuring wide-band and wide dynamic range support for RF self-interference cancellation and robust and efficient self-interference channel estimation for digital self-interference cancellation. Based on a realistic LTE-based cellular model, their full-duplex radio design is evaluated through system-level simulations and real-world testbed experiments.

ABSTRACT

Full-duplex radio has potential to double spectral efficiency by simultaneously transmitting and receiving signals in the same frequency band, but at the expense of additional hardware and power consumption for self-interference cancellation. Hence, the deployment of a full-duplex cellular network can be realized by employing full-duplex functionality only at an eNodeB, which is supposed to have sufficient computation and power resources, and by scheduling pairs of half-duplex UEs that are in either downlink or uplink. By doing so, fast and smooth full-duplex deployment is possible while minimally affecting the legacy UEs and the rest of the network entities. In this article, we provide technical challenges and solutions for an LTE-compatible full-duplex cellular network, featuring wideband and wide dynamic range support for RF self-interference cancellation, and robust and efficient self-interference channel estimation for digital self-interference cancellation. Based on a realistic LTE-based cellular model, our full-duplex radio design is evaluated through system-level simulations and real-world testbed experiments. Simulation results show that a significant throughput gain can be achieved by the full-duplex technique despite the existence of physical limiting factors such as path loss, fading, and other-cell interference. Testbed measurements reveal that at a bandwidth of 20 MHz, self-interference cancellation up to 37 dB is achieved in the RF domain, and most of the residual self-interference is further cancelled down to the noise floor in the subsequent digital domain.

INTRODUCTION

The explosion of wireless data traffic leads to an exponential increase in the target data rate requirements of the fifth generation (5G) wireless cellular networks. A 5G network is expected to provide 1000-fold capacity gains compared to the existing 4G networks such as 3GPP Long Term Evolution (LTE) and LTE-Advanced (LTE-A) systems [1].

The highly demanding capacity requirements of a 5G network can be met by a combination of increasing cell density, utilizing formerly unused spectrum, and improving spectral efficiency. Among them, full-duplex transmission has recently drawn much attention as a means

of potentially doubling spectral efficiency by simultaneously transmitting both the downlink and uplink signals in the same frequency band, which is a prominent advantage compared to the conventional half-duplex schemes such as frequency-division duplex (FDD) and time-division duplex (TDD).

One of the key challenging issues for full-duplex radio is the existence of strong self-interference from the transmit to receiver chains. The self-interference comes from imperfect isolation between the transmit and receive paths and reflections from nearby scatterers. It is usually much stronger than the desired received signal, sometimes even 100 dB or so stronger [2]. Thus, such self-interference should be mitigated before processing the received signals. Otherwise, any information contained in the received signal cannot be properly decoded. In this regard, there have been various attempts to suppress or cancel the self-interference in the RF and digital domains [3–5]. Kim *et al.* presented a point-to-point full-duplex scheme based on polarization-division duplexing [3]. Bharadia *et al.* implemented a full-duplex WiFi radio using analog and digital self-interference cancellation techniques [4]. Huu-sari *et al.* developed a wideband RF self-interference cancellation circuit having self-adaptive and self-healing features [5].

Different from the above prior works dealing with point-to-point and WiFi links, an attempt to apply full-duplex transmission into a cellular network was recently reported in [6], where the self-interference cancellation for full-duplex transmission is performed only at the eNodeB (i.e., base station) while the user equipments (UEs) are limited to half-duplex transmissions. Combined with an appropriate UE scheduling strategy, this scheme achieves a significant full-duplex gain. Based on this, we further improve the eNodeB-side only full-duplex scheme with the aim of ensuring compatibility with the existing LTE and LTE-A systems. Therefore, we expect a fast and smooth deployment of the full-duplex radio with minimal impact on the legacy UEs and the rest of the network entities.

Hence, in this article, we suggest system architecture and enabling technologies for the full-duplex support in an LTE-compatible cellular network, including:

- Identifying a system description with deployment scenarios and requirements

This work was supported by the Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.B0115-16-0001, 5G Communication with a Heterogeneous, Agile Mobile Network in the PyeongChang Winter Olympic Competition.

Gosan Noh, Jinup Kim, and Ilgyu Kim are with the Electronics and Telecommunications Research Institute (ETRI); Hanho Wang is with Sangmyung University; Changyong Shin is with Sun Moon University; Seunghyeon Kim is with Kwangwoon University and now is with GCT Semiconductor Inc.; Youngil Jeon, and Hyunchol Shin are with Kwangwoon University.

Digital Object Identifier:
10.1109/MCOM.2017.1600791CM

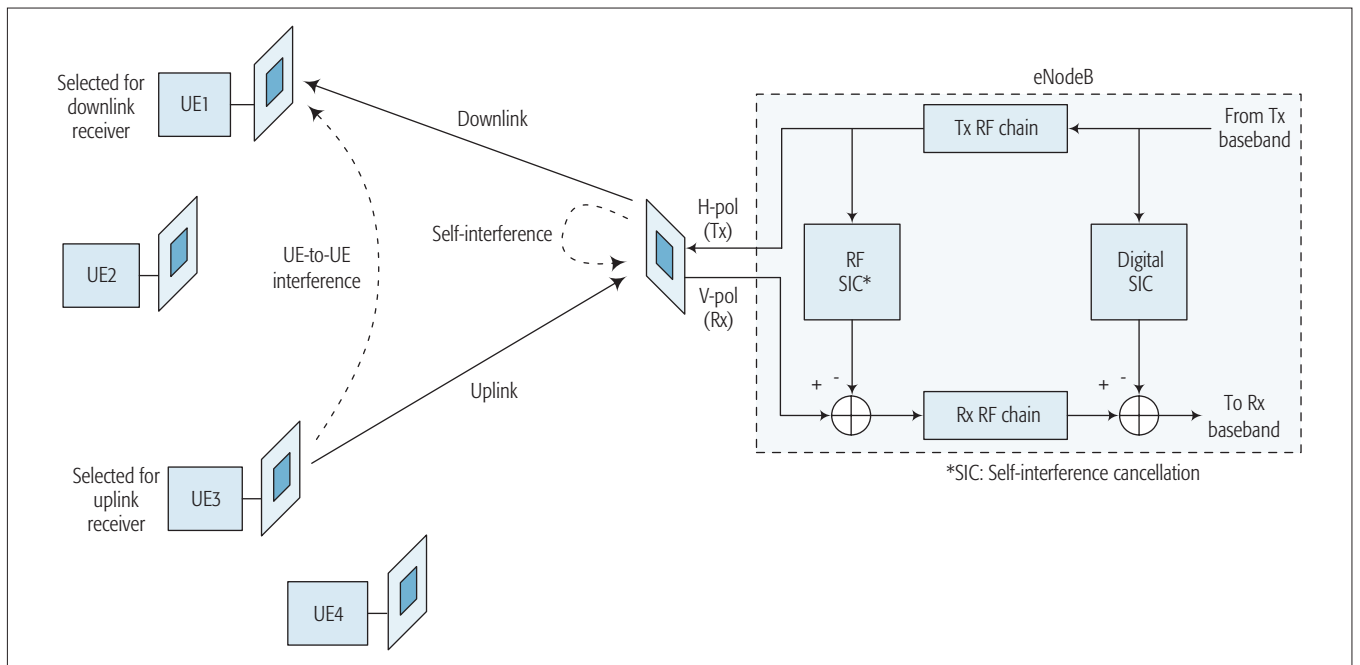


Figure 1. System overview and transceiver structure of the proposed LTE-compatible full-duplex radio.

- Providing some important implementation challenges and solutions focusing on the wideband and wide dynamic range RF self-interference cancellation and the robust and efficient digital self-interference cancellation with special consideration of the compatibility with LTE systems
- Evaluating the system-level performance under the existence of physical factors such as path loss, fading, and other-cell interference
- Describing the LTE-compatible full-duplex testbed and evaluating its real-world performance.

SYSTEM DESCRIPTION AND REQUIREMENTS

NETWORK MODEL AND DEPLOYMENT SCENARIO

We consider a full-duplex cellular system based on the LTE/LTE-A standard where each cell consists of an eNodeB and multiple UEs, as seen in Fig. 1. The full-duplex functionality is implemented only at the eNodeB, while UEs operate in the conventional half-duplex fashion, similar to [6]. The reason for employing full-duplex functionality only at the eNodeB side is twofold. First, UEs tend to have limited hardware and energy resources to support full-duplex operations (e.g., self-interference cancellation in the RF and digital domains). Second, the eNodeB-side-only full duplex facilitates backward compatibility with legacy LTE/LTE-A UEs supporting only either FDD or TDD. As a result, upgrading a half-duplex LTE system into a full-duplex one becomes possible by simply replacing the half-duplex eNodeBs with the full-duplex eNodeBs while not affecting the rest of network entities and interconnections.

Our target deployment scenario is a small cell environment with a low-power eNodeB and low-mobility UEs. With less transmit power (i.e., 20 dB or so less than the macro eNodeB [7]), the required level of self-interference power to be cancelled is considerably scaled down, thereby facilitating the self-interference cancellation with

less complexity and less residual interference. The low-mobility properties of UEs ascertain that the self-interference channel remains the same during the self-interference channel estimation and cancellation procedures, allowing reliable self-interference cancellation.

SELF-INTERFERENCE CANCELLATION

As seen from the right side of Fig. 1, the eNodeB contains several techniques to minimize the self-interference in both analog and digital domains, which include antenna separation, RF-domain cancellation, and digital-domain cancellation. Antenna separation is a technique to physically and/or electrically separate the signal paths between the transmit and receive antennas. One promising candidate is the use of a dual-polarized antenna having two orthogonal polarization components (e.g., transmission in horizontal polarization and reception in vertical polarization) [8, 9]. However, due to imperfect polarization isolation and reflections from nearby scatterers, some self-interference components still remain in the received signal, which need to be further cancelled out using analog RF circuitry and digital signal processing techniques.

RF self-interference cancellation is required to cut down the residual self-interference component in the received RF signal so that after the RF cancellation, the signal level can fall within the dynamic range of the analog-to-digital converter (ADC) in the receiver RF chain. After this, the self-interference component is further cancelled out in the digital domain without the loss due to RF receiver saturation. The RF cancellation capability can be achieved by employing an RF self-interference cancellation circuit that automatically generates a replica signal with the same magnitude but opposite phase with respect to the self-interference component and cancelling it out from the received RF signal.

After the RF cancellation, digital cancellation is performed with the baseband signal in the digital

The RF self-interference cancellation functionality is required to cover a wide channel bandwidth with a wide dynamic range. The bandwidth of the LTE signal ranges from 1.4 MHz to 20 MHz. Thus, the operational bandwidth for the RF self-interference cancellation functionality is expected to cover 20 MHz.

domain after the ADC. Using a priori information on the transmitted signal and the self-interference channel estimate, the digital cancellation can eliminate the self-interference almost to the noise floor by subtracting the generated copy of self-interference from the received baseband signal.

MULTIPLE ACCESS

In order to ensure compatibility, full-duplex operation should be supported in accordance with the existing LTE multiple access schemes, that is, orthogonal frequency-division multiple access (OFDMA) for the downlink and single-carrier frequency-division multiple access (SC-FDMA) for the uplink. Using OFDMA, the data streams intended for different UEs are transmitted on non-overlapping subcarrier sets. Thanks to the orthogonality among the subcarriers, the degradation due to multipath fading can easily be compensated using low-complexity equalization techniques, yielding inter-symbol interference (ISI)- and inter-carrier interference (ICI)-free transmission. One significant drawback of OFDMA is high peak-to-average power ratio (PAPR), degrading the power efficiency of the transmitter. The PAPR can be effectively reduced by adopting SC-FDMA in the uplink where the data symbols are discrete Fourier transform (DFT)-spread before being mapped to the subcarriers. The reason for employing the SC-FDMA only at the uplink is the limited power budget of battery-operated mobile devices. These design objectives for the multiple access are still valid for the full-duplex LTE system. Thus, the transceiver design and signal processing algorithm development for the LTE-compatible full-duplex radio should be done based on OFDMA downlink and SC-FDMA uplink.

IMPLEMENTATION

CHALLENGES AND SOLUTIONS

In order to fulfill the above requirements, some critical technical challenges need to be overcome. Specifically, one of the most challenging issues is self-interference cancellation, which needs to be implemented in both the RF and digital domains while achieving a sufficient level of compatibility with existing LTE systems. Other challenging issues to be addressed in this work are self-interference channel estimation and downlink/uplink synchronization.

RF SELF-INTERFERENCE CANCELLATION

The RF self-interference cancellation functionality is required to cover a wide channel bandwidth with a wide dynamic range. The bandwidth of the LTE signal ranges from 1.4 to 20 MHz. Thus, the operational bandwidth for the RF self-interference cancellation functionality is expected to cover 20 MHz.

Wide dynamic range capability is needed due to the large fluctuation of the self-interference signal strength. Such fluctuation originates from transmit power variation, channel path loss variation, and isolation level variation between the transmit and receive antennas [10, 11]. The measurement shows that the required dynamic range is greater than a factor of 20 dB [11]. In the following, we discuss how the wideband and wide dynamic range capabilities can be achieved.

Achieving Wideband Self-Interference Cancellation: Wideband channels tend to experience frequency selectivity, that is, the channel response varies with respect to frequency due to the delay spread in the time domain. Exploiting the multi-carrier structure of OFDMA, digital self-interference cancellation can overcome this frequency selectivity in the frequency domain by estimating the self-interference channel and cancelling the self-interference signal on a per-subcarrier basis. On the other hand, RF self-interference cancellation has limited ability to perform frequency-dependent operation. Hence, a candidate solution will be employing a multi-tap RF self-interference cancellation circuit that consists of multiple RF self-interference cancellation paths with different time delays [4, 12]. The delay for each path can be adjusted by variable delay lines.

Achieving Wide Dynamic Range Self-Interference Cancellation: Any restriction on the dynamic range of the RF self-interference cancellation circuit limits the ability to adjust the replica signal strength to a level close to the actual self-interference signal remaining at the RF receiver input terminal. If the two power levels do not match, there will remain a significant amount of uncanceled self-interference after the RF self-interference cancellation.

A promising solution to this problem is the employment of a variable-gain amplifier at the replica signal generation path before the cancellation point, as described in detail in our prior work [11]. By adjusting the gain of the variable-gain amplifier according to the fluctuating received self-interference power level, the RF self-interference canceller provides robust and improved cancellation performance.

SELF-INTERFERENCE CHANNEL ESTIMATION

The prerequisite for digital self-interference cancellation is acquiring the accurate information of the self-interference channel. In the LTE/LTE-A systems, reference signals are used for channel estimation: cell-specific reference signals (CRSSs) for the downlink and demodulation reference signals (DMRSs) for the uplink. Since we are to perform self-interference cancellation at the eNodeB, the self-interference channel estimation is involved with the CRS.

However, since the current frame structures for LTE and LTE-A were originally designed for the half-duplex modes (i.e., FDD and TDD), the CRS-based self-interference channel estimation is disturbed by the so-called pilot contamination caused by the interference from the simultaneously transmitted uplink resource elements co-located with the CRS, thereby degrading the performance of the digital self-interference cancellation.

In order to tackle the above problem, we employ an uplink nulling technique that prevents a certain portion of uplink resources from being transmitted so that the CRSSs for the self-interference channel estimation are not interfered. Although there might be uplink throughput loss due to the uplink nulling, its impact will not be significant considering the traffic asymmetry between the downlink and uplink. The peak data rate requirements of the LTE-A system are 1 Gb/s for the downlink and 500 Mb/s for the uplink, demonstrating significant asymmetry [13]. The

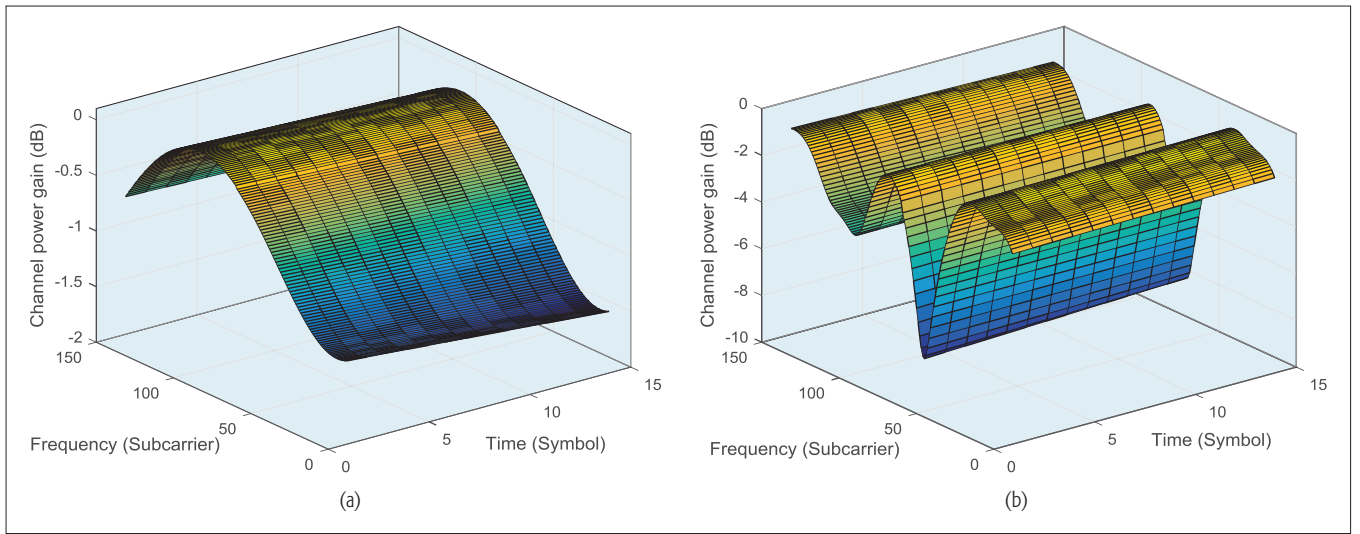


Figure 2. Time-frequency channel responses for slow fading channels: a) EPA 10 MHz; b) EVA 10 MHz.

uplink nulling can be categorized according to the amount and frequency of time-frequency resources to be nulled (i.e., per-subframe/symbol uplink nulling and per-RE uplink nulling).

Per-Subframe/Symbol Uplink Nulling: In slow fading environments with low mobility, the channel gains are supposed to be stable over a timescale that ranges from several orthogonal frequency-division multiplexing (OFDM) symbols to several radio frames. Using Clarke's model, the 50 percent coherence time at the maximum Doppler frequency of 10 Hz is about 42.3 ms [14], which is much larger than the length of a radio frame. This slow fading tendency can be observed in Fig. 2, which shows the simulated time-frequency channel responses for extended pedestrian A (EPA) and extended vehicular A (EVA) models assuming a maximum Doppler frequency of 10 MHz.

Based on the above considerations, as described in Fig. 3a, we can employ a per-subframe nulling scheme that nulls out a designated uplink subframe (i.e., the 0th uplink subframe where the physical broadcast channel (PBCH), the primary synchronization signal (PSS), and the secondary synchronization signal (SSS) are transmitted in the downlink counterpart). By doing so, the self-interference channel estimation can be done within the 0th subframe without interference from the uplink. Then, using the estimated self-interference channel knowledge, the self-interference cancellation is carried out in the rest of the subframes. If the coherence time becomes shorter than a radio frame, per-symbol uplink nulling can be employed where certain symbols (e.g., the first two of 14 symbols in a normal subframe) is nulled out, as seen in Fig. 3b.

The per-subframe/symbol uplink nulling techniques are simple and easy to implement with minimal frame structure changes to the current LTE and LTE-A standards. Only some modification on the uplink scheduler is needed. However, these per-subframe/symbol uplink nulling schemes may suffer from resource waste.

Per-RE Uplink Nulling: In order to solve the above problem, we employ the per-RE uplink nulling where only the uplink REs located at the same

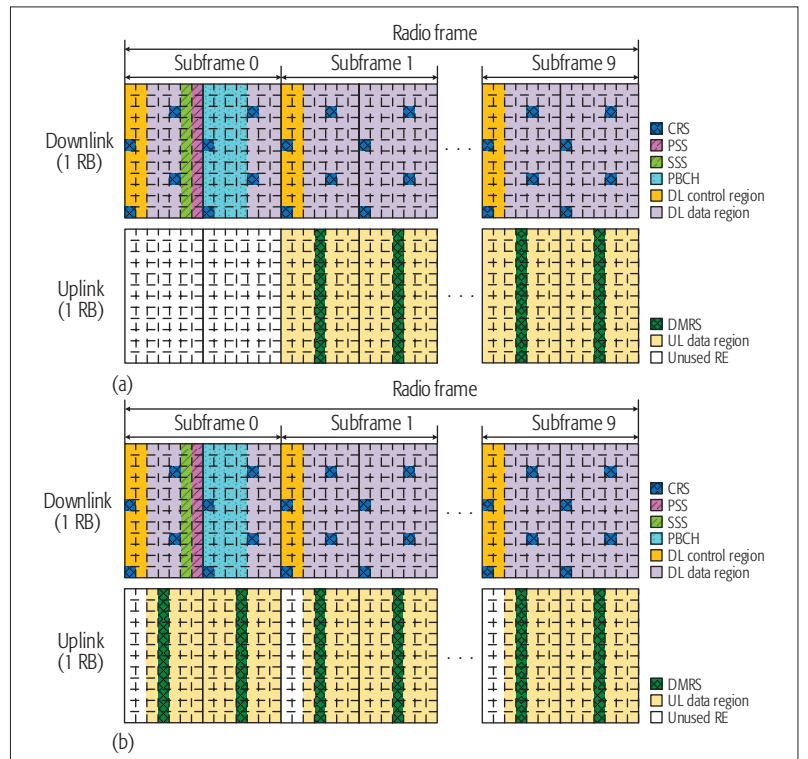


Figure 3. Time-frequency resource grids for per-subframe/symbol uplink nulling; a) per-subframe uplink nulling; b) per-symbol uplink nulling.

time-frequency positions as the downlink CRSs are nulled out. Figure 4a shows an example of per-RE uplink nulling in two consecutive resource blocks. It is clear that with per-RE uplink nulling, the downlink CRSs can be used for self-interference channel estimation without the uplink interference. The resource waste due to the per-RE uplink nulling is only 4.76 percent, which is much lower compared to the full-duplex gain.

The per-RE uplink nulling can be done by allocating the null subcarriers at the subcarrier mapping block of the SC-FDMA transmitter, which can be implemented while causing minimum impact to the LTE/LTE-A standards. At the receiv-

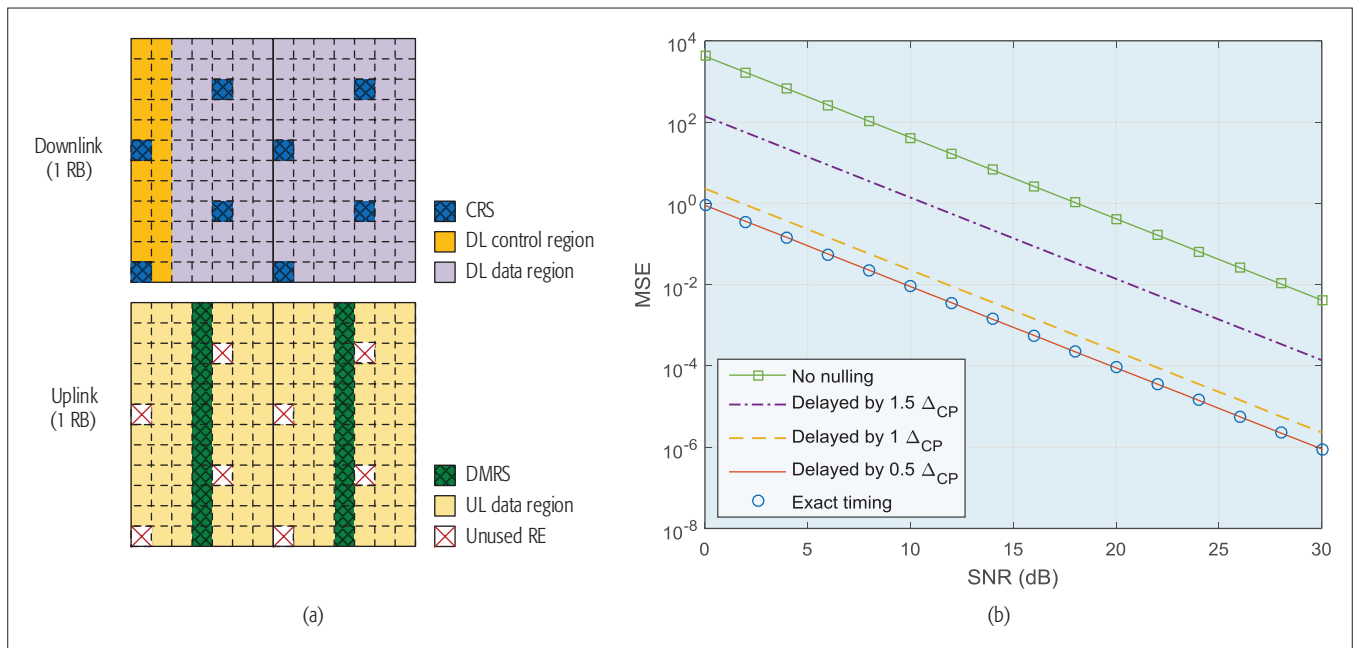


Figure 4. Per-RE uplink nulling: a) time-frequency resource grids for downlink and uplink; b) mean square error vs. interference-to-noise ratio (INR) of the self-interference link.

er, the self-interference channel estimation can be done using the downlink CRSs co-located with the uplink null subcarriers. The self-interference cancellation is then performed, followed by the null subcarrier removal and uplink channel estimation/equalization. In order to ensure backward compatibility, the eNodeB is also required to provide support for legacy UEs that do not support the per-RE uplink nulling by bypassing the null subcarrier removal and self-interference cancellation functionalities.

Frame Synchronization between Downlink and Uplink: The above self-interference channel estimation scheme requires frame synchronization between the downlink and uplink. Without the frame synchronization, the self-interference channel estimation will be disturbed by the interference from the overlapping adjacent uplink symbols. In this regard, uplink timing alignment functionality already present in LTE/LTE-A can be used to align the start time of the received uplink subframe and the transmitted downlink subframe. More specifically, using the timing advance values determined by the network based on the uplink measurement, the UEs carry out timing advance operations. By advancing or delaying the uplink signal, the amount of timing misalignment can be limited to within the cyclic prefix. Once the timing misalignment is less than the cyclic prefix, its effect can easily be overcome by phase compensation in the frequency domain.

The effect of the timing misalignment on the performance of the per-RE uplink nulling-based self-interference channel estimation is shown in Fig. 4b, which depicts the mean square error (MSE) as a function of the interference-to-noise ratio (INR) of the self-interference link. The uplink signal-to-noise ratio (SNR) is assumed to be 20 dB. The curves are plotted for different amounts of the downlink-uplink timing misalignment in terms of the ratio of the cyclic prefix length to the

OFDM symbol length Δ_{CP} . As expected, the MSE for the timing misalignment of $0.5 \Delta_{CP}$ is exactly the same as the case with the exact timing. Oppositely, we can see significant MSE degradation for the large timing misalignment case of $1.5 \Delta_{CP}$. When the timing misalignment is $1 \Delta_{CP}$, i.e., same as the cyclic prefix length, the MSE is slightly higher than the case of exact timing, which is due to the effect of the delay spread. For comparison, the MSE of the no nulling case is also plotted where the uplink interference is not avoided during the self-interference channel estimation procedure, providing the upper bound.

SYSTEM-LEVEL PERFORMANCE EVALUATION IN AN ACTUAL CELLULAR SYSTEM

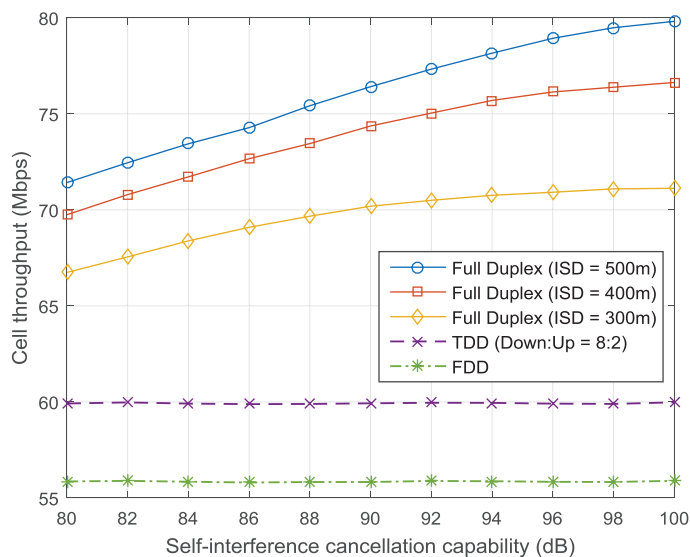
In practical cellular systems, we should consider several physical factors such as distance-dependent path loss, large- and small-scale fading, and other-cell interference in addition to the aforementioned RF and digital impairments. In this regard, we evaluate the system-level performance of the full-duplex-enabled cellular system compared to the conventional half-duplex schemes, FDD and TDD.

System-Level Evaluation Environment: We consider a heterogeneous cellular network where multiple macro and small cells are deployed in the same frequency band. The macro eNodeBs are placed on a hexagonal grid with inter-site distance (ISD) of 500 m. The small eNodeBs and UEs are randomly dropped. The UEs located within the small cell radius of 40 m are connected to the small eNodeB.

Full-duplex functionality is employed at each small eNodeB, which therefore experiences not only the intra-cell interference from itself (i.e., self-interference) but also the inter-cell interference from other macro and small cells. The specific simulation parameters are based on the 3GPP LTE-A outdoor small cell evaluation scenario with co-channel deployment of the macro and small

Parameter	Value
Carrier frequency	2.59 GHz
Bandwidth	20 MHz
Macrocell ISD	500 m
Small cell radius	40 m
eNodeB TX power	Macrocell: 46 dBm Small cell: 30 dBm
UE TX power	27 dBm
Thermal noise density	-174 dBm/Hz
eNodeB noise figure	Macrocell: 5 dB Small cell: 8 dB
UE noise figure	9 dB
Path loss	Macrocell: $128.1 + 37.6\log_{10}(R)$ Small cell: $140.7 + 36.7\log_{10}(R)$
Shadowing std	Macrocell: 8 dB Small cell: 10 dB

(a)



(b)

Figure 5. System-level evaluation results: a) simulation parameters; b) throughput vs. self-interference cancellation capability.

cells [15]. The detailed simulation parameters are described in Fig. 5a.

System-Level Evaluation Results: With the above simulation parameters, we obtained simulation results over different small eNodeB and UE drops, each with 2048 realizations. In Fig. 5b, the average throughput of a UE is plotted, which can be attained through simultaneous downlink and uplink transmissions. Comparisons with the FDD and TDD schemes are also provided. Since the system bandwidth of 20 MHz is assumed for full duplex, 10 MHz bandwidth is employed for each of the DL and UL for FDD. For TDD, DL/UL configuration 2 is employed so that the ratio between the DL and UL is about 80 and 20 percent.

Figure 5b shows that significant throughput gain through the use of full duplex is attainable despite the existence of the real-world physical factors such as path loss, fading, and other-cell interference. The amount of throughput gain is increased with the self-interference cancellation capability (i.e., the total amount of self-interference cancellation using a combination of antenna, RF, and digital cancellations), and is upper-bounded at about 95 dB, which is consistent with the existing literature [6]. The throughput gain of TDD over FDD is due to the fact that the downlink throughput is higher than the uplink throughput.

TESTBED DESCRIPTION AND PERFORMANCE EVALUATION

In this section, we describe our LTE-based full-duplex testbed in order to evaluate real-world full-duplex performance, especially on both the RF and digital self-interference cancellation capabilities.

TESTBED SETUP

The testbed for the evaluation of our full-duplex radio design represents the eNodeB side of an LTE-based full-duplex cellular system, which consists of antenna, RF cancellation circuit, and digital cancellation unit, as seen in Fig. 6a.

A dual-polarized microstrip patch antenna

is used for the separation between the transmit and receive signal paths. The center frequency is designed to be at 2.59 GHz with the -10 dB bandwidth of 140 MHz. The isolation between the horizontal and vertical ports is measured from -15 dB to -35 dB varying depending on surrounding environmental conditions [11].

The RF cancellation circuit is designed to achieve wide bandwidth and wide dynamic range cancellation capability, as described in [11]. The circuit itself has self-adaptive characteristics to automatically control the amplitude and phase of the replica signal by the use of the vector modulator and the variable-gain amplifier. In order to support wideband cancellation, a two-tap RF cancellation circuit is employed with different delay settings at the input. The delay for each tap is adjusted by using cables with different lengths in this experiment. The optimal cable length difference is found to be 152 cm, which corresponds to a time delay of 7.4 ns after extensive measurements for length difference varying from 0 cm to 200 cm. Wide dynamic range can be supported by the use of a variable-gain amplifier (Avago MGA-638P8). The RF cancellation circuit is powered by ± 10 V supply. The local oscillator inputs of the up- and down-conversion mixers are provided by a signal generator at a frequency of 2.59 GHz.

The signal processing for digital cancellation is performed using the NI USRP-2942R software-defined radio (SDR) device that has a Xilinx Kintex-7 field programmable gate array (FPGA) and two independent RF front-ends supporting frequency bands from 400 MHz to 4.4 GHz with the maximum bandwidth of 40 MHz. The SDR is controlled by a host computer using NI LabVIEW Communications Systems Design Suite 1.1 software. The baseband processing functions, including modulation, demodulation, and digital self-interference cancellation, are performed in the FPGA. The transmitter unit generates an LTE-modulated signal, followed by a high-power amplifier that can amplify the transmit signal power level to 20 dBm.

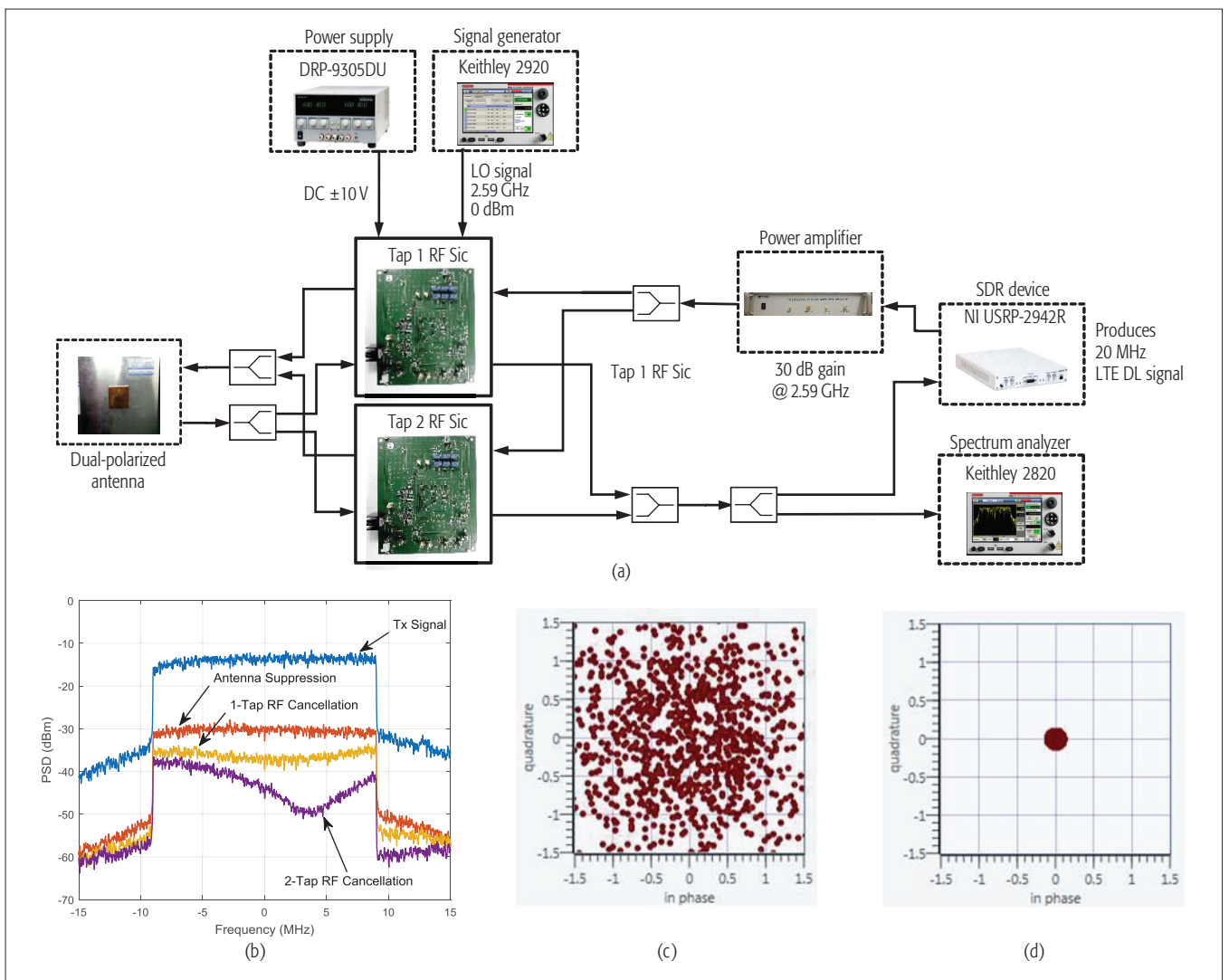


Figure 6. Testbed setup and experimental results: a) testbed setup; b) self-interference cancellation by antenna suppression and RF self-interference cancellation; c) constellation before digital cancellation; d) constellation after digital cancellation.

The implementation of the digital part is based on 3GPP LTE Release 10. The bandwidth is 20 MHz, and the fast Fourier transform (FFT) size is 2048. Each radio frame is 10 ms long and consists of 10 subframes. In addition, normal cyclic prefix is assumed. Since we employ the per-RE uplink nulling, the self-interference channel estimation is done in a similar manner of conventional downlink channel estimation.

EXPERIMENTAL RESULTS

We can see the effects of antenna separation and RF self-interference cancellation in Fig. 6b. The dual-polarized antenna can suppress the self-interference power about 17 dB. The RF self-interference cancellation circuit can further reduce the self-interference power by 6–8 dB with 1-tap RF cancellation and by 9–20 dB with 2-tap RF cancellation. We observe the frequency selectivity in the signal after RF cancellation, which can easily be handled with the per-subcarrier-based cancellation technique in a digital domain.

The effect of digital self-interference cancellation can be seen by comparing Fig. 6c (constellation before digital cancellation) and Fig. 6d (constellation after digital cancellation). The self-in-

terference component is successfully cancelled by subtracting the a priori known transmitted signal using the self-interference channel estimate.

CONCLUSION

This article introduces the essential techniques to support LTE-compatible full-duplex radio. Our approach is based on a realistic LTE/LTE-A network model assuming full-duplex eNodeB and half-duplex UE. In order to support wideband and wide dynamic range RF self-interference cancellation, we develop a multi-tap, variable-gain, and self-adaptive RF self-interference cancellation circuit. For digital self-interference cancellation, we provide a new frame structure design that can perform accurate self-interference channel estimation with the use of uplink nulling schemes. The proposed techniques for LTE-compatible full-duplex radio were evaluated through system-level simulations and real-world testbed experiments. We can see that self-interference can be efficiently cancelled with a combination of RF and digital cancellation techniques.

The various techniques discussed in this article not only enable fast deployment of the full-duplex functionality over the existing LTE/LTE-A networks

and legacy UEs, but also provide a stepping stone to better develop further enhanced full-duplex techniques along with the development of 5G wireless networks.

REFERENCES

- [1] J. G. Andrews et al., "What Will 5G Be?," *IEEE JSAC*, vol. 32, no. 6, June 2014, pp. 1065–82.
- [2] D. Kim, H. Lee, and D. Hong, "A Survey of In-Band Full-Duplex Transmission: From the Perspective of PHY and MAC Layers," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, Nov. 2015, pp. 2017–46.
- [3] K. S. Kim et al., "16-QAM OFDM-Based W-Band Polarization-Division Duplex Communication System with Multi-Gigabit Performance," *ETRI J.*, vol. 36, no. 2, Apr. 2014, pp. 206–13.
- [4] D. Bharadia, E. McMillin, and S. Katti, "Full Duplex Radios," *Proc. ACM SIGCOMM 2013*, Aug. 2013, pp. 375–86.
- [5] T. Huusari et al., "Wideband Self-Adaptive RF Cancellation Circuit for Full-Duplex Radio: Operating Principle and Measurements," *Proc. IEEE VTC-Spring 2015*, May 2015, pp. 1–7.
- [6] S. Goyal et al., "Full Duplex Cellular Systems: Will Doubling Interference Prevent Doubling Capacity," *IEEE Commun. Mag.*, vol. 53, no. 5, May 2015, pp. 121–27.
- [7] 3GPP TS 25.104, "Base Station (BS) Radio Transmission and Reception (FDD)," v. 12.7.0, Jan. 2016; <http://www.3gpp.org/DynaReport/25104.htm>, accessed Oct. 31, 2016.
- [8] M. Helno et al., "Recent Advances in Antenna Design and Interference Cancellation Algorithms for In-Band Full Duplex Relays," *IEEE Commun. Mag.*, vol. 53, no. 5, May 2015, pp. 91–101.
- [9] M. Chung et al., "Prototyping Real-Time Full Duplex Radios," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2015, pp. 56–63.
- [10] R. M. Vaghefi et al., "Cooperative Received Signal Strength-Based Sensor Localization with Unknown Transmit Powers," *IEEE Trans. Signal Processing*, vol. 61, no. 6, Mar. 2013, pp. 1389–1403.
- [11] S. Kim et al., "A 2.59-GHz RF Self-Interference Cancellation Circuit with Wide Dynamic Range for In-Band Full-Duplex Radio," *Proc. IEEE Int'l. Microwave Symp.*, May 2016.
- [12] A. Sabharwal et al., "In-Band Full-Duplex Wireless: Challenges and Opportunities," *IEEE JSAC*, vol. 32, no. 9, Sept. 2014, pp. 1637–52.
- [13] 3GPP TR 36.913, "Requirements for Further Advancements for E-UTRA (LTE-Advanced)," v. 12.0.0, Oct. 2014; <http://www.3gpp.org/DynaReport/36913.htm>, accessed Oct. 31, 2016.
- [14] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed., Prentice Hall, 2002.
- [15] 3GPP TR 36.872, "Small Cell Enhancements for E-UTRA and E-UTRAN — Physical Layer Aspects," v. 12.0.0, Dec. 2013; <http://www.3gpp.org/DynaReport/36872.htm>, accessed Oct. 31, 2016.

BIOGRAPHIES

GOSAN NOH [S'07, M'12] (gsnoh@etri.re.kr) received his B.S. and Ph.D. degrees in electrical and electronic engineering from Yonsei University, Seoul, Korea, in 2007 and 2012, respectively. From March 2012 to February 2013, he was a postdoctoral researcher at the School of Electrical and Electronic Engineering, Yonsei University. Since March 2013, he has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea, where he is a senior researcher. His research

interests include millimeter-wave transmission and high-speed train communications.

HANHO WANG joined the Information and Telecommunication Engineering Department of Sangmyung University in 2012, where he serves as an assistant professor. He received his B.S.E.E. ('04) and Ph.D. ('10) degrees from Yonsei University. He previously worked at the Korean Intellectual Property Office (KIPO) as a patent examiner in the Department of Information and Telecommunication Patent Examination.

CHANGYONG SHIN [S'04, M'07] received his B.S. ('93) and M.S. ('95) degrees from Yonsei University, Seoul, South Korea, and his Ph.D. ('06) degree from the University of Texas at Austin, all in electrical engineering. From 2007 to 2014, he was a principal research engineer with Samsung Advanced Institute of Technology, South Korea, where he worked on next-generation cellular systems. Since 2014, he has been with the School of Mechanical and ICT Convergence Engineering at Sun Moon University, South Korea.

SEUNGHYEON KIM received B.S. (2010) and Ph.D. (2016) degrees in electrical engineering from Kwangwoon University, Seoul, Korea. He is a staff engineer at GCT Semiconductor Inc., Seoul, Korea, where he is involved in wideband saw-less CMOS receiver design for LTE applications.

YOUNGIL JEON received his B.S. (2015) degree in electrical engineering from Kwangwoon University, where he is currently a Master's student. His research interests are in RF circuits and systems design for wireless communications.

HYUNCHOL SHIN [S'93, M'01, SM'10] joined the faculty of Kwangwoon University in 2003, where he is currently a professor. He received B.S. (1991), M.S. (1993), and Ph.D. (1998) degrees in electrical engineering from Korea Advanced Institute of Technology (KAIST), Daejeon, and held a postdoctoral position at the University of California Los Angeles (2003–2004). He has worked for several research companies, including Daimler-Benz Research Center, Samsung Electronics, and Qualcomm, as an RF/analog circuit designer for wireless communications. He has co-authored over 70 journal and conference papers, and holds over 30 patents. He has served on the Technical Program Committees of several IEEE conferences including ISSCC, VLSI Circuit Symposium, and A-SSCC.

JINUP KIM received his B.S. degree from Korea University, Seoul, Korea, in 1985, and M.S. and Ph.D. degrees from KAIST in 1987 and 1996, respectively. He has been with ETRI since 1987. He was a professor at the University of Science and Technology in the field of wireless communications during 2005–2010. He has researched in the field of wireless communication systems. He is currently interested in digital RF and software defined radio/cognitive radio technologies, and virtualization of the 5G access platform.

ILGYU KIM received B.S. and M.S. degree in electronic engineering from the University of Seoul, Korea, in 1993 and 1995, and his Ph.D. degree in information communications engineering from KAIST in 2009. Since 2000, he has been with ETRI, where he has been involved in the development of WCDMA, LTE, and MHN systems. Since 2012, he has been the leader of the mobile wireless backhaul research section. His main research interests include millimeter-wave communications and 5G mobile communications.

The various techniques discussed in this article not only enable fast deployment of the full-duplex functionality over the existing LTE/LTE-A networks and legacy UEs, but also provide a stepping stone to better develop further enhanced full-duplex techniques along with the development of 5G wireless networks.

Achieving Ultra-Low Latency in 5G Millimeter Wave Cellular Networks

Russell Ford, Menglei Zhang, Marco Mezzavilla, Sourjya Dutta, Sundeep Rangan, and Michele Zorzi

The authors survey some of the challenges and possible solutions for delivering end-to-end, reliable, ultra-low-latency services in mmWave cellular systems in terms of the MAC layer, congestion control, and core network architecture.

ABSTRACT

The IMT 2020 requirements of 20 Gb/s peak data rate and 1 ms latency present significant engineering challenges for the design of 5G cellular systems. Systems that make use of the mmWave bands above 10 GHz—where large regions of spectrum are available—are a promising 5G candidate that may be able to rise to the occasion. However, although the mmWave bands can support massive peak data rates, delivering these data rates for end-to-end services while maintaining reliability and ultra-low-latency performance to support emerging applications and use cases will require rethinking all layers of the protocol stack. This article surveys some of the challenges and possible solutions for delivering end-to-end, reliable, ultra-low-latency services in mmWave cellular systems in terms of the MAC layer, congestion control, and core network architecture.

INTRODUCTION

Millimeter-wave (mmWave) communication is widely considered to be a promising candidate technology for fifth generation (5G) cellular and next-generation wireless local area networks (WLANs). The wireless industry is already investing heavily in developing systems that operate in the mmWave bands, which are attractive because of the large quantities of available spectrum and the spatial degrees of freedom afforded by very high-dimensional antenna arrays (which are possible thanks to the smaller size of antenna elements at higher frequencies). Regulatory agencies are also beginning to consider defining new licensed and unlicensed bands for commercial use. Although mmWave radio links are already used in a variety of commercial applications such as satellite and point-to-point backhaul communications, until recently they were considered impractical for mobile access networks due to severe vulnerability to shadowing and poor isotropic propagation loss. Results from recent measurement campaigns have demonstrated that the limitations of the mmWave channel can indeed be overcome by high-gain smart antennas, meaning that this spectrum can now, for the first time, be exploited to provide an order of magnitude or more increase in throughput for mobile devices [1, 2].

Ultra-wideband mmWave access has now been recognized as a means of achieving the IMT

2020 requirements of 100 Mb/s cell edge and 20 Gb/s peak rate, and is expected to play a key role in future wireless networks. Prototypes have already been demonstrated that can approach such data rates [3]. However, the requirements for latency that have been proposed are perhaps even more daunting than the need for high throughput. Achieving the near instantaneous user experience required by many of the anticipated “killer apps” of the 5G *Tactile Internet*, like immersive virtual reality, augmented reality, telesurgery, and real-time cloud/fog computing, may necessitate end-to-end (E2E) latencies to be reduced below 10 ms. Other emerging use cases like mission-critical machine-type communication (MTC) and control of self-driving cars present a need for less than 1 ms of latency [4, 5].

While the mmWave bands potentially enable *ultra-low latency* and massive bandwidths at the physical (PHY) layer, realizing this level of performance for E2E services presents significant engineering challenges. Many aspects of the way cellular systems are designed must be reconsidered if the potential of the mmWave bands is to be fully realized to meet the requirements of next-generation devices and applications. In particular, achieving ultra-low latency in mobile networks calls for a reworking of the entire protocol stack from the ground up. This article surveys some of the challenges and possible solutions for delivering high-rate, ultra-low-latency E2E services in 5G cellular systems. We focus on three critical higher-layer design areas:

- Low-latency core network architecture
- A flexible medium access control (MAC) layer
- Congestion control

We discuss some key limitations of current 4G core networks for providing low-latency E2E services. We review the state-of-the-art research on mobile edge cloud (MEC) architectures, which promise to reduce delay by moving core data centers and network functions closer to the end user. However, optimizing the core network may not, by itself, be sufficient to meet the delay constraints of certain applications. We discuss how the radio stack and, in particular, the MAC layer will also need a fundamentally new design to provide sub-millisecond *over-the-air* latency. We then move up the stack and consider how optimizations may be required at the transport layer to address the high variability in the mmWave

This material is based on work supported by the National Science Foundation under Grants No. 1116589 and 1237821 as well as generous support from NYU WIRELESS affiliate memberships.

Digital Object Identifier:
10.1109/MCOM.2017.1600407CM

Russell Ford, Menglei Zhang, Marco Mezzavilla, Sourjya Dutta, and Sundeep Rangan are with New York University Polytechnic School of Engineering; Michele Zorzi is with the University of Padova.

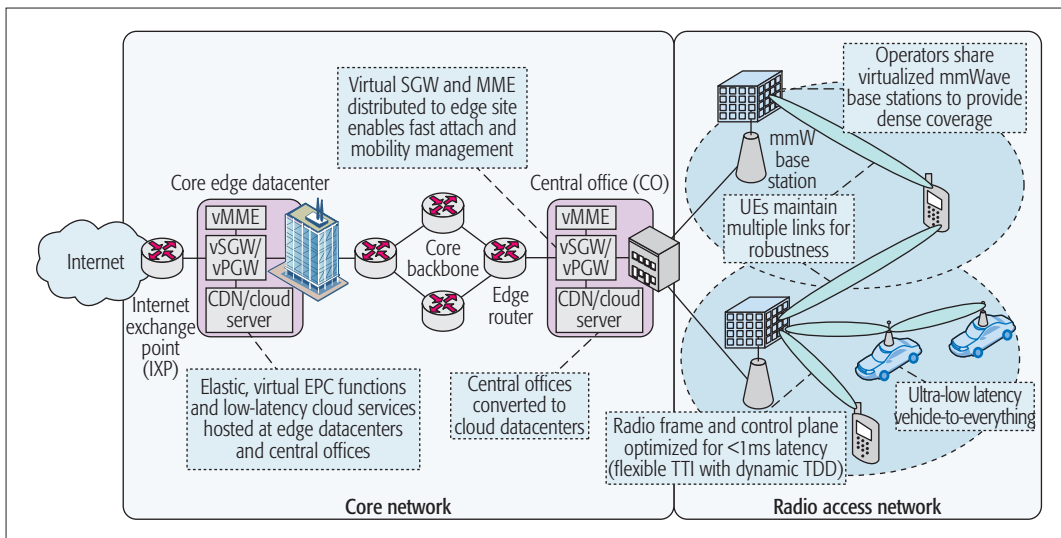


Figure 1. Realizing ultra-low latency from an end-to-end perspective will require innovations throughout the network.

channel in order to reduce round-trip times (RTTs) while maintaining high E2E reliability.

CORE NETWORK ARCHITECTURE CHALLENGES

To understand the challenges in delivering low-latency services, it is useful to begin by considering the typical cellular network architecture over which data services are delivered. Modern deployments of the 4G core network, known as the Evolved Packet Core (EPC), are characterized by a small number of high-capacity, high-reliability network elements (NEs), such as serving gateways (SGWs), packet data network gateways (PGWs), and mobility management entities (MMEs), which rely on expensive application-specific hardware. Due to the cost and complexity of managing these nodes, EPC network elements are typically located at only a small number of core data centers, making present-day mobile core networks highly centralized and geographically dispersed. The limited placement of these core NEs and Internet exchange points (IXPs), where operators peer with other networks, poses a dilemma for offering low-latency services over the top of these networks. Packets must first ingress through the IXP router and be forwarded through PGW and SGW nodes before being routed to the end user. Due to this potentially high routing delay, the target E2E latency of 10 ms for some Internet-based 5G applications cannot typically be met in the current 4G core [4–6].

To reduce latency, core functions such as gateway nodes, along with the applications and services themselves, will need to be moved closer to the network edge. Software-defined networking (SDN) and network functions virtualization (NFV) are two trends in networking being considered for future mobile network architectures, which lend themselves to more distributed topologies and offer opportunities for lower latency [7, 8]. Fundamentally, mobile SDN involves decoupling the control and data planes of routers, switches, and user-plane EPC entities. An intelligent mobile cloud controller then handles all control plane functions, and can actively monitor and control the user plane elements, which enables it to main-

tain a global view of the network state, manage traffic, and dynamically provision resources on a large scale. SDN thus provides operators greater flexibility and control in managing their networks.

To realize more flexible and scalable networks, SDN is complemented by NFV, which enables network functions to be deployed as virtual machines running on commodity servers. This removes the dependence on application-specific *Big Iron* network entities and makes it possible to deploy leaner, elastic software implementations of core network functions to edge data center sites. As shown in Fig. 1, instances of soft EPC virtual network functions (VNFs, e.g., virtual SGW and PGW instances) can be provisioned at edge data centers and central offices, or even on servers co-located with the base stations (BSs) themselves, and can be dynamically scaled to adapt to varying load. In addition to core VNFs, the application-layer services such as gaming servers and content distribution network (CDN) nodes can be hosted in the edge network. For instance, a content caching VM may be instantiated at a virtualized BS to provide real-time traffic monitoring and control data to self-driving cars. The term mobile edge cloud has been coined to refer to such a distributed, SDN and NFV-enabled mobile network, where VNFs and applications can be deployed to edge sites to better satisfy the latency requirements of 5G applications.

Moving content and application servers to the edge may also be key to improving TCP performance over unreliable mmWave links. We show how the mmWave channel can exhibit high intermittency and can rapidly fluctuate between high- and low-capacity states. Therefore, fast transport-layer feedback will be needed so that the congestion control algorithm can quickly adapt to changes in the channel capacity, and reducing the E2E latency will naturally lead to faster convergence. We continue the discussion of TCP over the mmWave channel.

Furthermore, distributing the control signaling load across many virtual MME instances placed at the edge may offer a means of reducing control-plane latency and mitigating the surge in sig-

To realize more flexible and scalable networks, SDN is complemented by NFV, which enables network functions to be deployed as virtual machines running on commodity servers. This removes the dependence on application-specific *Big Iron* network entities and makes it possible to deploy leaner, elastic software implementations of core network functions to edge data-center sites.

To achieve very low latency and react to very rapidly varying channels, control messages such as scheduling requests and channel quality indicator reports will need to have frequent opportunities for transmissions. These short control messages will thus incur significant overhead if they cannot be transmitted efficiently.

naling brought on by the anticipated 100-fold increase in connected devices, as well as the increase in handover-related signaling that may come as a result of cell densification [7]. A more distributed control plane may therefore be particularly desirable for deployments of mmWave cells, which must inherently be dense due to the limited range of the high-frequency signal.

Nevertheless, 5G networks will need to support a class of applications with more extreme latency constraints than even the MEC can meet. For instance, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)-based services, such as collision avoidance for self-driving cars, may require less than 1 ms of latency, which cannot be met by the current 4G radio stack (even before factoring in the latency of the core network and the Internet) [4, 5]. We continue in the next section with a discussion of a radio frame and MAC layer design that is suitable for meeting such stringent requirements.

MAC LAYER DESIGN ISSUES

CHALLENGES

Current 802.11 wireless LAN systems are easily able to achieve sub-millisecond airlink latencies. However, delivering very low latencies in cellular systems is significantly more challenging. Cellular systems, by their nature, must accommodate large numbers of users per cell and incur significant delay for scheduling, coordinating transmissions, and adjusting to variable channel conditions to maximally utilize the airlink resources. Indeed, the current minimum data plane latency in 4G LTE is on the order of 3 ms and can be higher than 100 ms with multiple higher-layer (i.e., radio link control layer) retransmissions. Thus, 5G mmWave MAC will need to be redesigned to reduce latency by at least an order of magnitude.

A key challenge for mmWave systems is that transmissions must be highly directional to overcome the high isotropic path loss. Most transceivers, at least in the near future, are likely to use phased arrays for directional beamforming. These arrays can achieve very high directional gains but are limited to transmitting to one user at a time, that is, via time-division multiple access (TDMA) scheduling. Unfortunately, TDMA can lead to potentially very poor resource utilization since the entire bandwidth must be allocated to a single user. This allocation can be very inefficient for short MAC-layer and higher-layer control messages since, with 1 GHz of mmWave bandwidth, even a relatively short 100 μ s TDMA slot has the capacity to transmit kilobytes of data [9]. Frequency-division multiple access (FDMA)-based systems like LTE can schedule multiple users flexibly in the frequency domain and therefore do not suffer from such poor utilization for smaller packets and control messages.

Moreover, to achieve very low latency and react to very rapidly varying channels, control messages such as scheduling requests and channel quality indicator (CQI) reports will need to have frequent opportunities for transmissions. These short control messages will thus incur significant overhead if they cannot be transmitted efficiently.

Some have contended that, due to its reliance on beamforming, mmWave access technology is

not well suited for transmission of control channels. It is argued that, since such signals must be broadcast out omnidirectionally, a split control and data channel design is required where a legacy 4G macrocell performs all control signaling and mmWave BSs simply boost the data plane capacity. However, recent works have shown that, with digital or hybrid beamforming transceivers, most of the standard control channels of 4G systems can be handled effectively in standalone mmWave systems [9, 10]. In this section, we consider such a system design where both control and data channels are transmitted in the same mmWave band. This allows for a shorter turnaround time of control feedback and faster scheduling thanks to the potential for shorter subframes when compared to LTE.¹

POTENTIAL SOLUTIONS

Following other proposed mmWave cellular designs, in this article we consider an orthogonal frequency-division multiplexing (OFDM)-based system. However, we note that many of the design considerations in this section can apply generally to other waveforms being evaluated for 5G as well.²

To deliver very low latencies at the MAC layer, there are at least three key modifications one could consider with respect to current 4G LTE OFDM systems.

Short symbol periods: Efficient TDMA transmission of short control messages requires that one can allocate control transmissions in very short time intervals. LTE uses OFDM, which enables very simple equalization. In OFDM, the minimum allocation is one symbol period, which in the current LTE system is 71.4 μ s (for a normal cyclic prefix, CP). To improve utilization, several designs have proposed using much shorter symbol periods on the order of 4 μ s. The short OFDM symbol period can be used for mmWave systems due to the wider coherence bandwidth, allowing for larger subcarrier spacing. Also, the required CP length is reduced since these systems are intended for very small cells with low root mean square (RMS) delay spreads (typically under a few hundreds of nanoseconds, even at distances of over 200 m) [1, 12].

Flexible TTI: In current LTE systems, transmissions are sent in a fixed transmission time interval (TTI) of 1 ms. With TDMA scheduling, allocating data to any reasonable-sized fixed TTI would be very inefficient for small packets that would not be able to fully utilize the TTI. Thus, variable TTI-based TDMA frame structures have been proposed in [9, 13]. Also known as flexible TTI, these schemes allow for slot sizes that can vary according to the length of the packet or transport block (TB) to be transmitted and are well suited for diverse traffic. The flexibility in resource scheduling permitted by a variable TTI system allows both intermittent and bursty traffic with small packets (characteristic of MTC) as well as high throughput flows like streaming and file transfers to be handled efficiently.

Low-power digital beamforming for control: Critical to understanding latency in multi-user environments is the choice of the RF multiple-input multiple-output (MIMO) architecture, particularly how beamforming is performed.

¹ We acknowledge that there is the possibility to reduce the subframe TTI in future LTE releases, which would reduce control plane latency. However, transmitting the control and data channel in the same mmWave band may prove to be a simpler approach than serving the control channel out of band over the legacy 4G system, as long as certain engineering challenges (discussed in the sequel) can be addressed.

² For brevity, we do not provide an assessment of new 5G waveforms. The reader is referred to Ibars *et al.* [11] for further discussion.

	Analog BF	Fully digital BF	Low-resolution digital BF
Hardware requirements	Analog processing and combining at RF with single ADC at baseband.	Dedicated baseband and RF chains for each antenna.	Dedicated baseband and RF chains for each antenna.
Power consumption	Low	High	Moderate
Spatial multiplexing	Not supported	Supported	Supported
Optimal modulation scheme	<i>M</i> -QAM	<i>M</i> -QAM	QPSK
Control overhead	High	Low	Low

Table 1. Comparison between analog and digital architectures at mmWave frequencies.

Various options are shown in Table 1. To reduce power consumption, most mmWave designs employ analog beamforming (BF) where combining is performed in analog, at either RF or intermediate frequency (IF), requiring only one digital conversion path. However, this limits the transceiver to communicate in only one direction at a time, which is particularly problematic for multiplexing short control packets over wide bandwidths. Conventional fully digital architectures can enable spatial multiplexing but come at the cost of much higher power consumption. A third option is to use a fully digital architecture, but at very low quantization resolution to reduce the power. This enables full spatial multiplexing but limits the maximum signal-to-noise ratio (SNR). In this analysis, we consider a switched architecture system where control signals are sent using low-resolution digital beamforming (to enable multiplexing small control packets) with analog beamforming in the data plane (to enable higher order modulation). As shown in [9], this approach can considerably reduce the overhead due to control signaling. Thus, more resources are available for data transmission, which in turn reduces the E2E latency.

LOW-LATENCY MMWAVE MAC

To evaluate the achievable latency with flexible TTI, we consider the frame structure in Fig. 2, similar to the designs recently proposed in [9, 13]. The design assumes that the BS transceiver is able to support both analog BF and low-resolution digital BF as previously described, and can dynamically switch between the two modes. The key components of the frame structure and MAC scheme are as follows.

Data Channel: As already noted, we consider a system where data channel transmission relies on analog BF. Therefore, transmission of data slots must be strictly TDMA-based and, as a consequence, the minimum time-domain chunk of resource allocation that can be assigned to a single user in the data period (i.e., the minimum slot length) is 1 OFDM symbol. There must be a small guard time between uplink (UL) and downlink (DL) transmissions as well as a transition time during which the BF vectors are updated at the transmitter and receiver. To reduce the number of these transitions, which are effectively wasted resources, symbols assigned to a particular user may be grouped together so that all DL and UL symbols/slots are contiguously mapped to the DL-DATA and UL-DATA regions, respectively.

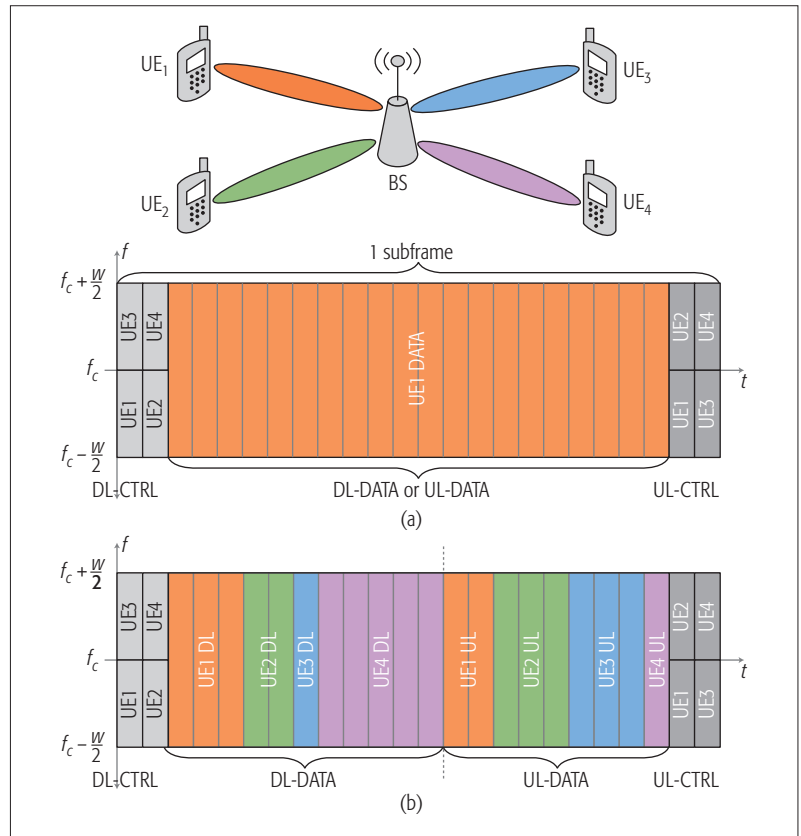


Figure 2. Variable and fixed TTI subframe formats for dynamic TDD

Thus, a slot refers to this grouping of consecutive symbols allocated to one UE.

Downlink Control Channel: The DL-CTRL period occupies the first several OFDM symbols of each subframe. We require that the location and duration of this region be fixed because the control messages it contains are periodic and must be decoded by all UEs at the beginning of the subframe. This allows a UE to decode only a small number of symbols to receive any control messages intended for itself, such as the DL control information (DCI), indicating the DL and UL assignments in the current or future subframe. If the control symbols were to be transmitted at any time during the subframe, every UE would have to continually receive and blindly decode even when they are not allocated, needlessly wasting battery power.

For BSs that do not support digital BF and must transmit the control channel in TDMA

Description	Value
Bandwidth (Hz)	1×10^9
Carrier frequency (Hz)	28×10^9
Length of one subframe (μs)	100/66.67
Number of OFDM symbols per slot	24/16
Length of one OFDM symbol (μs)	4.16
Length of CP (μs)	0.46
Subcarrier spacing (Hz)	270×10^3
Reference subcarrier spacing (Hz)	1.08×10^6
Control symbols per subframe	1 DL/1 UL
Number of HARQ processes (DL and UL)	20 DL/20 UL
Number of UEs	Case 1: {10, 20, 30, 40, 50, 60, 70, 80} Case 2: {1, 2, 3, 4, 5, 6, 7, 8}
Traffic model	Case 1: Poisson, $\lambda = 10$ Mb/s, 100 B packets Case 2: Poisson, $\lambda = 100$ Mb/s, 1000 B packets

Table 2. Parameters for variable and fixed TTI latency evaluation.

mode only, a minimum of one control symbol per allocated user would be needed. Data could, of course, be multiplexed with the control messages for better utilization of the symbol; however, the UE would still have to blindly decode a number of symbols before finding its own DCI. Therefore, there is a strong case for the BS to support digital BF capability in order to multiplex DL control signals to multiple UEs within a single DL-CTRL symbol.

Uplink Control Channel: The UL-CTRL period is used for the transmission of periodic control messages such as CQI reports, acknowledgments (ACKs), and scheduling requests (SRs) from the UEs to the BS. In the design presented here, the UL-CTRL is transmitted during the last OFDM symbol(s) of the subframe so that it is contiguous with the UL data symbols. Placement at the end of the subframe also allows ACKs to be transmitted quickly, possibly even in the same subframe as the corresponding DL transmission being ACKed (if it can be decoded in time).

HYBRID ARQ RETRANSMISSION

The severe variability and intermittency experienced by mmWave links suggest that retransmission schemes such as hybrid automatic repeat request (HARQ), which has been used successfully in 4G systems, will be relied on heavily in mmWave systems to improve reliability at the link layer.

On the other hand, retransmissions will naturally result in increased delay. In the DL case, as an example, the UE must first signal the failure of a transmission in an UL negative ACK (NACK), which must be received by the BS before it can schedule a retransmission. As we shall see in the sequel, with shorter subframes providing more frequent opportunities to transmit ACKs/NACKs and DCI messages, it is possible to achieve below 1 ms of latency for reliable link-layer delivery even after multiple retransmissions.

While the qualitative benefits of variable TTI over fixed TTI may seem self-evident, in this section we quantify the performance gains for a multi-user TDMA mmWave system with 1 GHz of bandwidth. We also demonstrate that, with the low-latency scheduling loop enabled by the proposed frame structure, LTE-style HARQ can still be employed for enhanced link-layer reliability without exceeding delay constraints excessively. Our simulations make use of the ns-3 full-stack simulation model for mmWave cellular networks presented in [14]. We model the subframe formats shown in Fig. 2 for two subframe periods: 100 μs , equivalent to 24 OFDM symbols, and 66.67 μs , equivalent to 16 OFDM symbols. Each symbol has a length of 4.16 μs , which is based on the design in [12]. Each subframe has one fixed DL-CTRL and one UL-CTRL symbol, with the remaining symbols used for DL or UL data slots. For fixed TTI mode, the entire subframe is allocated to a single user, whereas for variable TTI mode, the scheduler may allocate any number of data symbols within the subframe to match the throughput required by each user.

Additionally, reference or pilot symbols are transmitted on every fourth subcarrier for estimating the channel. This pilot spacing is chosen to be well within the coherence bandwidth [12]. We also note that there may also be some additional delay related to the beam tracking (i.e., for computing and applying the optimal TX/RX BF vectors), although the performance limitations of adaptive BF transceivers and channel tracking techniques in future implementations are still unknown. We assume that this delay can be neglected in our analysis because data is constantly being transmitted to each user equipment (UE), and channel state feedback is being transmitted by the UEs to the BS in each subframe period (which is within the coherence time), thus ensuring that the channel state information is always up-to-date at the BS [12].

UEs are uniformly distributed at distances between 10 and 150 meters from the serving BS and can have either line-of-sight (LOS) or non-LOS (NLOS) links, with path loss computed using the model from [2]. We also note that UEs are modeled as moving at 25 m/s, typical of vehicular speeds, which causes fast channel variation and frequent packet errors from small-scale fading (it is observed that between 0.5 and 3 percent of transport blocks are lost and require retransmission).

We consider a simple traffic model with Poisson arrivals where each UE sends small 100-byte packets at an average rate of 10 Mb/s, as well as a separate, higher-throughput case where 1000-byte packets are sent at a rate of 100 Mb/s. Scheduling is performed based on an Earliest Deadline First (EDF) policy where the scheduler attempts to deliver each IP packet within 1 ms from its arrival at the PDCP layer, and packets are assigned a priority based on how close they are to the deadline. Priority is therefore always given to HARQ retransmissions. We simulate the performance for between 10 and 100 UEs for the 10 Mb/s (per UE) arrival rate and between

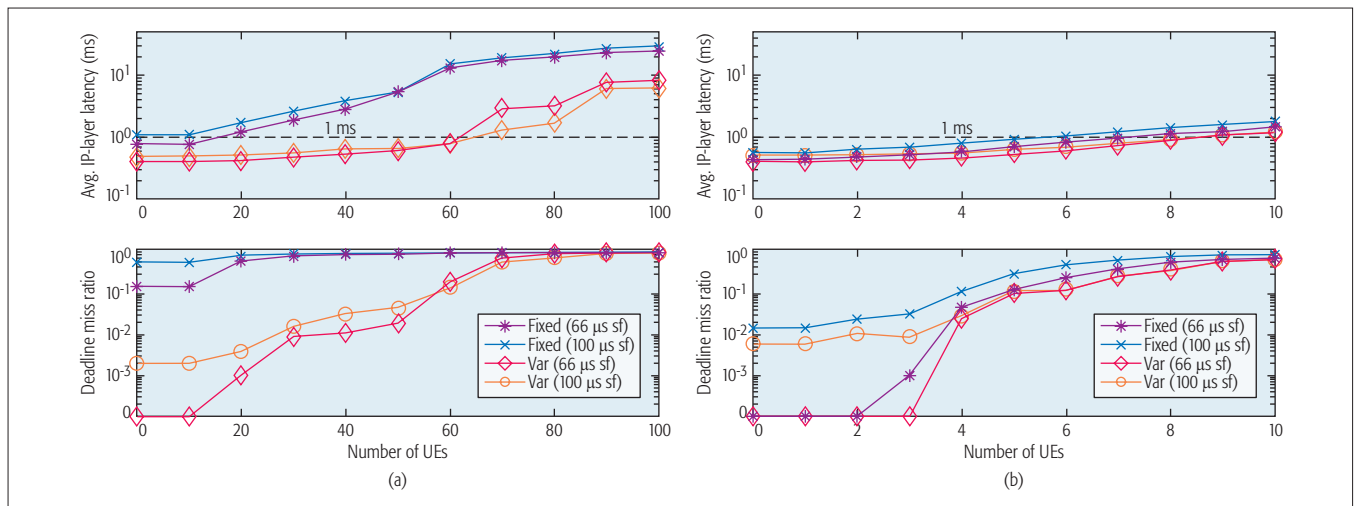


Figure 3. Latency and deadline miss ratio as a function of the downlink IP-layer arrival rate for fixed and variable TTI radio frame structures: a) 100-byte packets, 10 Mb/s per UE arrival rate; b) 1000-byte packets, 100 Mb/s per UE arrival rate. sf: subframe.

1 and 10 UEs for the 100 Mb/s case, equivalent to a total IP-layer arrival rate of between 100 and 1000 Mb/s in both cases.

Figure 3 shows the mean downlink radio link latency for the best-case 95 percent of users (i.e., the 5 percent of UEs with the highest latency are not considered). Here, latency is measured as the time between the arrival time of packets at the PDCP layer of the eNB stack and the time they are delivered to the IP layer at the UE. The deadline miss ratio (DMR), which represents the fraction of packets delivered after the 1 ms deadline, is also given for the top 95th percentile UEs. We see that for a 10 Mb/s arrival rate (Fig. 3a), variable TTI is able to achieve sub-millisecond average latency and a DMR of about 10 percent with over 60 users (corresponding to a 600 Mb/s total packet arrival rate) and consistently outperforms fixed TTI. Fixed TTI, despite the relatively short subframe compared to LTE, exceeds 1 ms average latency and has a DMR of over 60 percent even for the 20-UE case and exceeding 90 percent for 40 or more users. This result shows that variable TTI will be essential for reliable, low-latency service, particularly when considering use cases with many lower-rate devices, such as MTC.

For the higher-throughput (100 Mb/s arrival rate per UE) case in Fig. 3b, we expect the deviation between the variable and fixed TTI schemes to be less pronounced, as the bottleneck is the system throughput and not the minimum slot size. However, we do find an improvement in radio link latency of up to 500 μ s for the variable TTI scheme in some cases.

We also find that, for a smaller number of users, the shorter 66.67 μ s subframe offers some improvement over the longer 100 μ s subframe thanks to the decreased turnaround time. In particular, the DMR is consistently less for the 100 Mb/s/UE case for both variable and fixed TTI. However, this trend reverses with more users due to the lower ratio of control to data symbols in the 100 μ s subframe case. We note that the control overhead could be mitigated somewhat by multiplexing data in the DL-CTRL region. However, with low-resolution digital BF (as explained in the previous section), this data may need to be

encoded at a lower rate, leading to lower system throughput.

CONGESTION CONTROL CONSIDERATIONS

From an end-to-end point of view, mmWave communication could create networks with two features that have thus far never been seen together: links with massive peak capacity, but capacity that is highly variable. The massive peak rates arise from the tremendous amounts of spectrum available in the mmWave bands combined with large numbers of spatial degrees of freedom with high-dimensional antenna arrays. Indeed, recent prototypes have demonstrated multi-gigabits-per-second throughput in outdoor environments [3]. Simulation and analytic studies [2] have also predicted capacity gains that are orders of magnitude greater than in current cellular systems. At the same time, the mmWave channel can vary rapidly, making individual links unreliable. MmWave signals are completely blocked by many common building materials such as brick and mortar, and even the human body can cause up to 35 dB of attenuation [16]. As a result, the movement of obstacles and reflectors, or even changes in the orientation of a handset relative to the body or hand, can cause the channel to rapidly appear or disappear.

This combination of features — massive, but highly variable, bandwidth — presents particular challenges at the *transport layer*, specifically congestion control. The fundamental role of congestion control is to regulate the rate at which source packets are injected into the network to balance two competing objectives:

- To ensure sufficient packets are sent to utilize the available bandwidth
- To avoid overwhelming the network by sending too many packets, resulting in congestion and affecting other flows in the network

To illustrate these challenges, Figs. 4a and 4b show the performance of a single downlink TCP flow for a single user moving along a simulated route, where the mmWave link transitions between LoS and NLoS states due to being blocked by obstacles. The scenario is again simulated using the same model and parameters

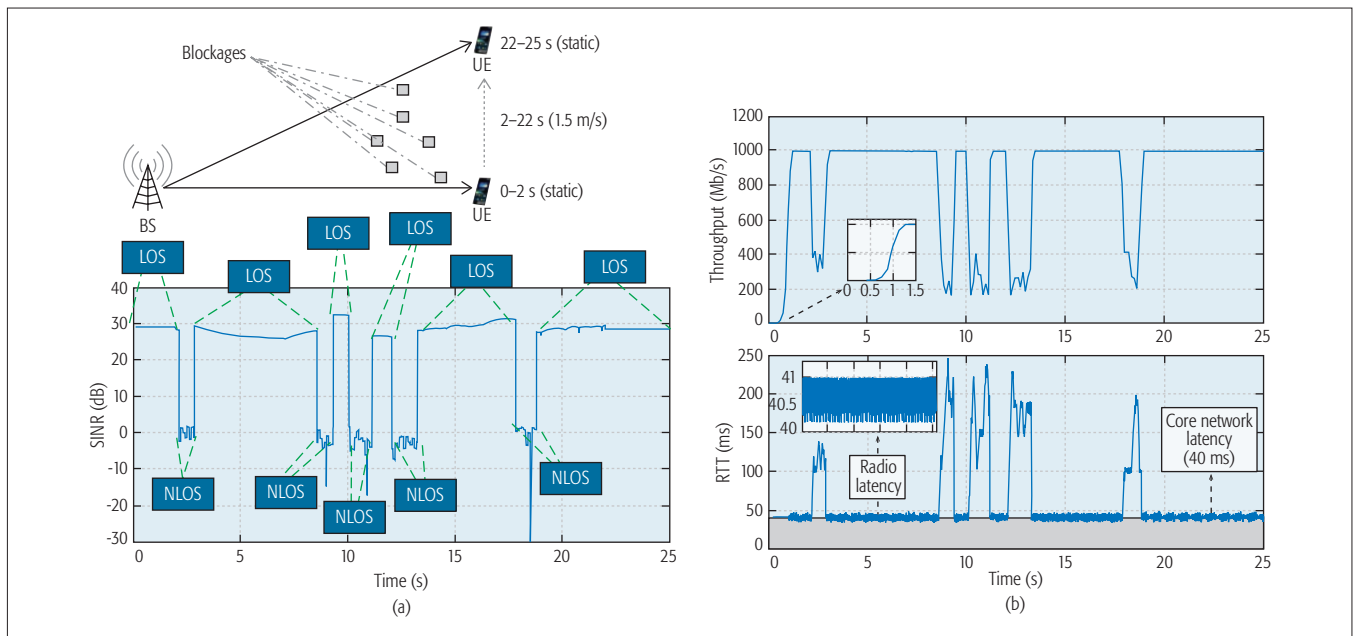


Figure 4. TCP performance degradation as a result of variability of the mmWave channel: a) plot of SINR vs. time showing the state of the mmWave link (from [15]); b) TCP performance at 1 Gb/s data rate.

introduced in the previous section. The application-layer data rate is fixed at 1 Gb/s, and a baseline one-way delay from the core and routing network is assumed to be 20 ms, or 40 ms round-trip. Under good channel conditions, the TCP server sends packets at its maximum data rate. However, following a deep fade (i.e., a sudden drop in SNR), which occurs due to the LoS path being blocked (e.g., at the 2.5 s mark in Fig. 4a), hundreds of milliseconds of additional delay are incurred, as shown in Fig. 4b. This is due to the fact that when the SINR is high, the TCP client is able to send packets at a high rate, and the BS is able to transmit packets at the rate they arrive in its DL PDCP queue. However, when the channel capacity is reduced significantly, the buffer becomes backlogged as the BS MAC/PHY-layer can no longer service it at the initial high rate. Even though the TCP NewReno congestion control algorithm is able to quickly adapt to this sharp loss in capacity, as can be seen in the figure, it is not fast enough to prevent significant spikes in latency due to the TX queue becoming backlogged. This result raises questions as to the effectiveness of current congestion control and avoidance mechanisms and indicates that a new transport-layer algorithm may be required to adapt to this high variability and more quickly converge to the channel capacity [15]. Alternatively, a split TCP scheme could be employed where the BS serves as a TCP proxy. This would enable cross-layer feedback to be facilitated by the lower BS stack to the transport layer to more directly indicate a loss in capacity and more quickly trigger congestion avoidance. Investigation of such optimizations is an interesting direction for future work.

CONCLUSIONS

The mmWave bands offer the possibility of a new generation of wide-area cellular networks with very low latencies and massive bandwidths. However, translating the exciting possibilities of the

mmWave spectrum for the physical layer to corresponding benefits for E2E services will require significant changes at multiple layers of the protocol stack. This article has identified three particular design issues that need consideration:

- Changes in the core network to bring data and services physically closer to the end user and provide greater flexibility and scalability in deploying and managing network functions
- A flexible MAC layer to enable low-latency scheduling while still allowing efficient use of the airlink resources
- Fast adaptive congestion control that handles the rapidly varying nature of the mmWave channel

For each of the three areas, we have discussed current solutions, possible directions of innovation, and some example results that show the potential of the various techniques in contributing to the reduction of the overall latency to approach the very challenging requirements set forth by the more demanding 5G applications.

We have reviewed many possible solutions and results from our own recent research as well as other state-of-the-art work, but all of these designs are still at a high-level stage, and much further effort will be needed to work out and evaluate these designs in order to make these systems a reality. However, if these technical challenges can be overcome, the potential for next-generation cellular systems is enormous.

REFERENCES

- [1] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges," *Proc. IEEE*, vol. 102, no. 3, Mar. 2014, pp. 366–85.
- [2] M. Akdeniz et al., "Millimeter Wave Channel Modeling and Cellular Capacity Evaluation," *IEEE JSAC*, vol. 32, no. 6, June 2014, pp. 1164–79.
- [3] J. Gozalvez, "5G Tests and Demonstrations [Mobile Radio]," *IEEE Vehic. Tech. Mag.*, vol. 10, no. 2, May 2015, pp. 16–25.
- [4] M. Simsek et al., "5G-Enabled Tactile Internet," *IEEE JSAC*, vol. 34, no. 3, Mar. 2016, pp. 460–73.

- [5] P. Popovski et al., "EU FP7 INFSO-ICT-317669 METIS, D1.1: Scenarios, Requirements and KPIs for 5G Mobile and Wireless System," 2013.
- [6] J. Cho et al., "SMORE: Software-Defined Networking Mobile Offloading Architecture," *Proc. 4th Wksp. All Things Cellular: Operations, Applications, & Challenges*, Aug. 2014, pp. 21–26.
- [7] P. K. Agyapong et al., "Design Considerations for a 5G Network Architecture," *IEEE Commun. Mag.*, vol. 52, no. 11, Nov. 2014, pp. 65–75.
- [8] V.-G. Nguyen, T.-X. Do, and Y. Kim, "SDN and Virtualization-Based LTE Mobile Network Architectures: A Comprehensive Survey," *J. Wireless Personal Commun.*, vol. 86, no. 3, Feb. 2016, pp. 1401–38.
- [9] S. Dutta et al., "Mac Layer Frame Design for Millimeter Wave Cellular System," *Proc. Euro. Conf. Networks and Commun.*, June 2016, pp. 117–21.
- [10] C. Barati Nt. et al., "Directional Cell Discovery in Millimeter Wave Cellular Networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, Dec. 2015, pp. 6664–78.
- [11] C. Ibars et al., "A Comparison of Waveform Candidates for 5G Millimeter Wave Systems," *Proc. 49th Asilomar Conf. Signals, Systems and Computers*, Feb. 2015, pp. 1747–51.
- [12] F. Khan, Z. Pi, and S. Rajagopal, "Millimeter-Wave Mobile Broadband with Large Scale Spatial Processing for 5G Mobile Communication," *Proc. 50th Annual Allerton Conf. Commun., Control, and Computing*, Oct. 2012, pp. 1517–23.
- [13] P. Kela et al., "A Novel Radio Frame Structure for 5G Dense Outdoor Radio Access Networks," *Proc. IEEE VTC-Spring '15*, May 2015, pp. 1–6.
- [14] R. Ford et al., "A Framework for End-to-End Evaluation of 5G MmWave Cellular Networks in ns-3," *Proc. 2016 ACM Wksp. NS-3*, June 2016, pp. 85–92.
- [15] M. Zhang et al., "Transport Layer Performance in 5G MmWave cellular," *Proc. 2016 INFOCOM Millimeter-Wave Networking Wksp.*, Mar. 2016, pp. 730–35.
- [16] J. S. Lu et al., "Modeling Human Blockers in Millimeter Wave Radio Links," *ZTE Commun.*, vol. 10, no. 4, Dec. 2012, pp. 23–28.

BIOGRAPHIES

RUSSELL FORD (russell.ford@nyu.edu) received his B.S. degree in electrical and computer engineering from Florida State University in 2010 and his M.S. degree in electrical engineering from the Polytechnic Institute of New York University (NYU) in 2012. He is currently pursuing a Ph.D. degree in computer science at NYU's Tandon School of Engineering, Brooklyn, under Prof. Sundeep Rangan. His research interests include modeling, simulation, and prototyping of 4G/5G cellular networks, algorithms for MAC- and network-layer resource allocation, and 5G mobile cloud architecture.

MENGLI ZHANG (menglei@nyu.edu) received his B.S. degree in electrical engineering from Nanjing University of Science and Technology, China in 2013 and the M.S. degree in electrical engineering in 2015 from the NYU Tandon School of Engineering, where he is currently working toward a Ph.D. degree in electrical engineering with Prof. Rangan. His research interests include wireless communications, channel modeling, transport-layer congestion control, and system-level network simulation.

MARCO MEZZAVILLA (mezzavilla@nyu.edu) is a postdoctoral researcher at the NYU Tandon School of Engineering. He received his B.Sc. (2007), M.Sc. (2010) in telecommunications engineering, and Ph.D. (2013) in information from the University of Padova, Italy, under Prof. M. Zorzi. He is serving as a reviewer for major IEEE conferences, journals, and magazines. His research interests include design and validation of communication protocols and applications of 4G/5G wireless technologies, multimedia traffic optimization, radio resource management, spectrum sharing, convex optimization, cognitive networks, and experimental analysis.

SOURIYA DUTTA (sdutta@nyu.edu) received his B.Tech degree in electronics and communications engineering from the National Institute of Technology, Durgapur, India, in 2012. He is currently working toward a Ph.D. degree in electrical and computer engineering at the NYU Tandon School of Engineering under the guidance of Prof. Rangan. His research interests include wireless communications, MAC layer design, and network simulation and prototyping.

SUNDEEP RANGAN [F'15] (srangan@nyu.edu) is an associate professor of electrical and computer engineering at NYU and the Director of NYU WIRELESS. He received his Ph.D. from the University of California, Berkeley in electrical engineering. In 2000, he co-founded (with four others) Flarion Technologies, a spinoff of Bell Labs that developed Flash OFDM, the first cellular OFDM data system. He was acquired by Qualcomm in 2006, where he was a director of engineering prior to joining NYU in 2010.

MICHELE ZORZI [F'07] (zorzi@dei.unipd.it) is with the Information Engineering Department of the University of Padova. His present research interests focus on various aspects of wireless communications. He was Editor-in-Chief of *IEEE Wireless Communications* from 2003 to 2005, *IEEE Transactions on Communications* from 2008 to 2011, and, at present, *IEEE Transactions on Cognitive Communications and Networking*. He served as a Member-at-Large of the ComSoc Board of Governors from 2009 to 2011, and as Director of Education and Training from 2014 to 2015.

Opportunities and Challenges of Trip Generation Data Collection Techniques Using Cellular Networks

Iva Bojic, Yuji Yoshimura, and Carlo Ratti

The authors discuss opportunities and limitations of tracking pedestrian activity by utilizing information provided by cellular networks. In order to track people, regardless of the underlying wireless media, two qualifications must be met: first, unique and anonymous identification, and second, geospatial visibility through time.

ABSTRACT

We are witnessing how urban areas are reclaiming road space, before devoted exclusively to cars, for pedestrians. With the increase of pedestrian activity, we need to update our existing transportation forecasting models by focusing more on people walking. The first step of extending the current models is to start with collecting information on pedestrians needed for the trip generation phase. This article discusses opportunities and limitations of tracking pedestrian activity by utilizing information provided by cellular networks. In order to track people, regardless of the underlying wireless media, two qualifications must be met: first, unique and anonymous identification, and second, geospatial visibility through time. While the latter requirement can be achieved with techniques that are similar for different wireless media, how to uniquely identify a pedestrian using a cellular network is domain-specific. We show that tracking of pedestrians using cellular networks can be done not only without their constant active participation, but also without disrupting normal cellular service. However, although this method is technically feasible, one should be very careful when wanting to implement it by keeping in mind a very important thing: how to protect people's privacy.

INTRODUCTION

Many cities across the world such as Hamburg, Madrid, and Oslo are beginning to shift their mobility solutions away from private car ownership, which leads to re-allocation of urban space from cars to people [1]. In this context, cities are forced to rethink traffic behavior in scenarios where less road space is devoted to cars and more to pedestrians. With more people on the streets, we have to extend currently used transportation forecasting models by including pedestrian activities. In this article we focus on presenting opportunities and challenges of the data collection techniques needed for the trip generation phase, which is the first step in the conventional four-step transportation forecasting process.

Data collection techniques needed for trip generation can be classified into *active* techniques where people being tracked have to actively participate in the collection process by wearing

some additional devices (e.g., wearable sensors, GPS receivers) or answering survey questions, and *passive* ones utilizing the signals from the devices that people are carrying with them at all times. The former techniques might affect people to change their behavior due to the fact that they are aware of their participation in a study and are limited in sample set, while the latter provide large-scale datasets without subjecting participants to changing their daily routines, but can also lack significant information, like how a person's socio-demographic attributes and inner thoughts can impact their flow.

This article provides insights on how to track pedestrian activity using cellular networks by presenting available techniques to uniquely identify users and localizing them. The advantage of this method, compared to other passive data collection techniques using Wi-Fi or Bluetooth, is its wide coverage and relative stability. Namely, unlike the aforementioned short-range wireless standards, the detection rate of a person's cell phone can be much higher. In addition, deployment of tracking systems based on cellular networks is easier than the deployment of a system based on image sensing devices, for example. However, although cellular networks support location inquiries, this information is not readily provided by telecommunication operators to third parties, and therefore must be retrieved independently.

The development of cellular networks began in the early 1980s and was first based on analog voice, and was known as first generation (1G). The 2G cellular network (2G) was called the Global System for Mobile Communications (GSM) and was developed by the European Telecommunications Standards Institute (ETSI) in the late 1980s, while the evolution from GSM to the 3G Universal Mobile Telecommunications System (UMTS) was developed by the Third Generation Partnership Project (3GPP). Finally, in the last few years we are witnessing successful implementations of 4G cellular networks called UMTS Long Term Evolution (LTE), also introduced by 3GPP.

Figure 1 shows the architecture of 2G, 3G, and 4G cellular networks that consist of three domains: the mobile station (MS), home network (HN), and serving network (SN). Furthermore, the HN domain consists of a home location register

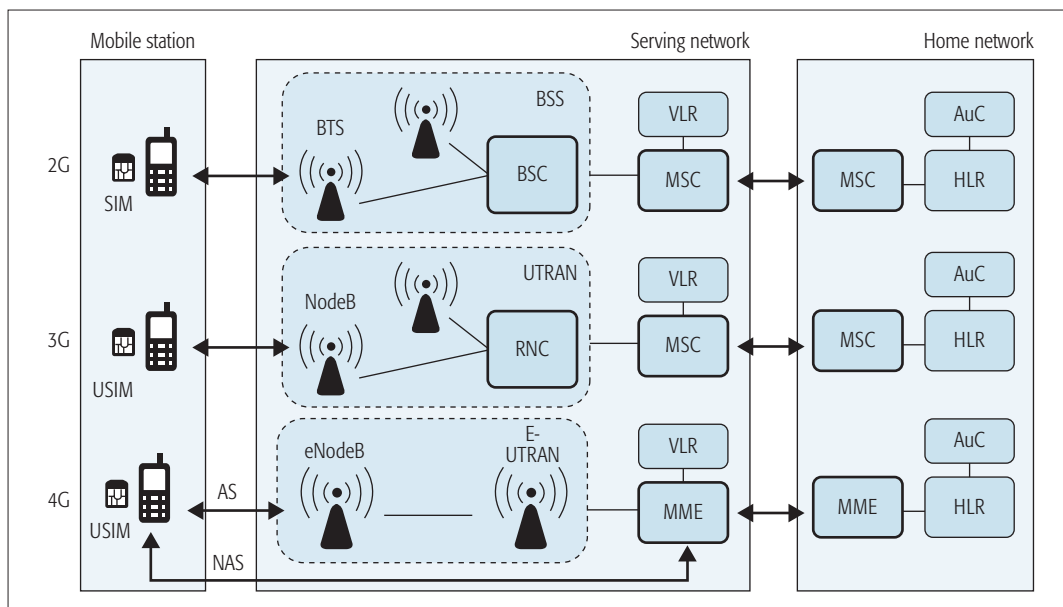


Figure 1. 2G, 3G and 4G cellular network architectures.

(HLR), which is a cellular network database with information about users' permanent identities (i.e., International Mobile Subscriber Identity [IMSI]), their telephone numbers (i.e., Mobile Station International Integrated Services Digital Network number [MSISDN]), the associated services, and general information about the location of users. The exact location of the user and his/her Temporary Mobile Station Identity (TMSI) are kept in a visitor location register (VLR), which is a part of the SN domain. Moreover, the Equipment Identity Register (EIR), which is not shown in Fig. 1 but is also connected to the mobile switching center (MSC) or mobile management entity (MME) in the HN domain, is the logical entity responsible for storing International Mobile Equipment Identities (IMEIs).

UNIQUELY IDENTIFYING PEDESTRIANS

The 3GPP published various documents related to security aspects of 2G, 3G, and 4G cellular networks (e.g., TS 42.009, Security Aspects, and TS 03.20, Security Related Network Functions for 2G; TS 33.120, Security Principles and Objectives, TS 33.102, Security Architecture, and TS 21.133, Security Threats and Requirements for 3G; and TS 33.401, Security Architecture for 4G) stating that three features should be supported:

- **User identity confidentiality:** the property that the permanent user identity (i.e., IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link
- **User location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link
- **User untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link

To achieve these goals, the user is normally identified by his/her own TMSI by which he/she is known by the visited SN rather than by the IMSI that is his/her permanent identity. To avoid user

traceability, which may lead to compromise of user identity confidentiality, the user should not be identified for a long period by means of the same temporary identity. To achieve these security features, in addition, it is required that any signaling or user data that might reveal the user identity is ciphered on the radio access link.

In order to uniquely identify users in cellular networks, one has three choices: a false base station attack (i.e., IMSI catchers) used to retrieve a user IMSI; an IMSI paging attack used for linking user IMSI and TMSI; and finally, an Authentication and Key Agreement (AKA) protocol linkability attack that does not collect any user-sensible information (i.e., IMSI or TMSI) but can be used to identify the user. Specifically, IMEI cannot be considered for the user tracking purposes because, as stated in the 3GPP standards, it should be securely stored in the MS and should not be sent to the network before the security has been activated. Moreover, an IMEI is not authenticated, so it can be changed by the user (e.g., to prevent the tracking of stolen cell phones).

A FALSE BASE STATION ATTACK

Although the 3GPP standards state that cellular networks should provide a support for user identity (i.e., IMSI) confidentiality, the user identification by a permanent identity procedure is allowed. This procedure can be invoked by the SN whenever the user cannot be identified by means of a temporary identity. The mechanism is initiated by the MSC in 2G and 3G or by the MME in 4G, and it requests the user to send his/her permanent identity. The user response contains its IMSI in a clear text. As stated in the standards themselves, this represents a breach in the provision of user identity confidentiality.

MSs always scan network frequencies and try to authenticate to the base station providing the strongest signal. A base station might accept or refuse a connection request based on the user subscription or roaming agreements. In the case of a false base station attack, an IMSI catcher is a device that acts exactly like a small base sta-

Although the 3GPP standards state that cellular networks should provide a support for user identity (i.e., IMSI) confidentiality, the user identification by a permanent identity procedure is allowed. This procedure can be invoked by the SN whenever the user cannot be identified by means of a temporary identity.

Although these security issues are improved in 3G and 4G cellular network standards, a permanent identity procedure is still done before other security procedures are started and consequently 3G and 4G networks are also prone to this kind of attacks.

tion. Being the IMSI catcher, this device offers the strongest signal to the nearby MSs (up to 100 m), forcing them to try to authenticate to the fake cellular network. The catcher can catch the IMSI of the authenticating MS before refusing the connection. Interestingly, while the 2G standard requires an MS to authenticate to an SN, it does not require the SN to authenticate to the MS. Although these security issues are improved in 3G and 4G cellular network standards, a permanent identity procedure is still done before other security procedures are started, and consequently 3G and 4G networks are also prone to this kind of attack.

The false base station threat was described by Mitchell in his technical report published in 2001 [2]. It was first believed that such attacks would be very expensive compared to other possible attacks in 2G networks, but then the cost of the base transceiver station (BTS) fell quickly; plus it also became very easy to find BTS emulators. This resulted in an increasing number of papers reporting their implementations of this kind of attacks compromising user confidentiality (e.g., [3]). It was then believed that 3G would not be vulnerable to false base station attacks. However, in 2012 Golde *et al.* showed how to use a rogue femtocell to create 3G IMSI catchers [4]. Currently, not only can different IMSI catchers be bought [5], but there are also papers reporting how to catch an IMSI catcher (i.e., IMSI catcher catchers) [6].

IMSI PAGING ATTACK

As stated in the 3GPP specifications, most control signaling messages, which are sent between an MS and an SN, are considered sensitive and must be integrity protected. However, there are signaling messages (e.g., PAGING TYPE 1) that are not required to be integrity protected, and consequently this vulnerability can be used for the IMSI paging attack. The paging procedure is usually used to locate an MS in order to deliver a service to it (e.g., phone call or SMS). Paging request messages are sent on a common control channel by an SN to all MSs in a particular area usually containing the requested TMSI. However, if an SN does not know the current MS TMSI, its IMSI can be sent instead. When an MS receives a paging message containing its IMSI or current TMSI, it sends a message containing its current TMSI.

A 2G IMSI paging attack was used to show that an MS can be localized within an area of 100 km² with multiple towers by simply wiretapping paging messages sent by an SN [7]. Moreover, using this kind of attack, it is possible to check if a particular MS is connected to a particular BTS, which can be mapped to a relatively small geographic area of approximately 1 km² or less. The IMSI paging procedure can be started sending malformed SMS messages [8] or using a method of aborted calls [7]. When using the latter, a regular phone call can be initialized with the purpose of tracking an MS and then hanging up within 5 s to avoid a ring on the MS. In that way a paging request for the particular MS is initialized without causing any user-observable side effects on the MS.

In 2012 Arapinis *et al.* also showed that it was

possible to perform IMSI paging attacks in 3G by testing their approach on T-Mobile, O2, SFR, and Vodafone victim MSs [9]. They used a commercially available femtocell that acted as a small base station with a coverage radius ranging from 10 to 50 m. By injecting a paging request in 3G, they were able to check if a particular MS was in the area covered by their device.

Finally, in [10] it was shown theoretically that 4G was also prone to the IMSI paging attacks. The authors of this article used an analogous attacker model similar to that used in [7] with the difference that their attacker was capable of causing paging request messages in 4G and listening on 4G paging channels.

AKA PROTOCOL LINKABILITY ATTACK

AKA is a mutual authentication and authenticated key establishment protocol in 3G between an SN and an MS. AKA involves the SN sending an authentication request to the MS and the MS sending its authentication response. The MS checks the validity of this request (thereby authenticating the SN), and then sends a user authentication response. Afterward, the SN checks the response and authenticates the MS, resulting in two parties having authenticated each other.

If the MS is not able to authenticate the SN, it can send either an authentication failure message or a synchronization failure message back to the SN with an indication of the problem. The authentication process consists of two phases and can fail at either the first or second stage. In the first stage the MS checks message authentication code (MAC), and in the second it verifies that the received sequence number (SQN) is in the correct range. Precisely these two messages containing a failure code can be used to distinguish between MSs, and this vulnerability can be used as a method for breaching user identity confidentiality in 3G.

The AKA protocol linkability attack exploits the error messages incorporated into AKA protocol. If an attacker is capable of sniffing the radio link and intercepts an authentication request message (i.e., RAND, AUTN pair) sent unencrypted on the radio link from an SN to a particular MS, the attacker can resend the exact message. If it does so, two possible things can happen:

- 1 If the recipient MS is the device to which the authentication request message was originally sent, it will respond with an authentication failure report containing an error code indicating a failed SQN (because this SQN has already been received).
- 2 If the recipient MS is not the device to which the authentication request message was originally sent, it will respond with an authentication failure report containing an error code indicating an incorrect MAC value.

Either way, this security leak can be used to trace the movements of a particular MS, resulting in a breach of the user untraceability.

This vulnerability in 3G was exploited in work done by Arapinis *et al.* in 2012 [9]. The 3G AKA protocol is used at the beginning of each new session in their femtocell setting making the caching of the authentication parameters very easy. However, the authors did not have the tools to test if this also happens when connecting to a typ-

ical Node B in a real 3G network, but tested their implementation in the 3G/2G interoperability scenario. They observed that in this setting the execution of the AKA protocol can be triggered by repeatedly placing a phone call for the targeted MS and hanging up within a short time window, so it cannot be detected by the user. For example, their experiments showed that the execution of AKA protocol in the U.K. Vodafone cellular network can be triggered by calling the targeted MS six times and hanging up before it even rings.

Recently, it was also shown that although in 4G networks Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol is used instead of AKA used in 3G networks, 4G is still prone to AKA protocol linkability attacks [10]. Similar to the previously described scenario, an attacker can eavesdrop an authentication request message sent from an MME on the air using femtocell techniques. As in 3G, error messages sent from different MSs in 4G are clearly different, and consequently the attacker knows whether the targeted MS is located in its observation area or not, which again results in the possibility of user traceability.

DISCUSSION

Although capturing IMEI, TMSI, and IMSI information does not directly link an MS to the user identity, it does bring different ethical issues and is illegal in many jurisdictions and countries. Moreover, when performing a false base station attack, one must trick an MS to connect to a false base station, which results in disrupting normal cell phone services, possibly having serious consequences (e.g., in case of emergencies). On the contrary, an IMSI paging attack can be performed without causing any user-observable side effects on the MS side. However, as in the previous attack, in this attack one also must collect user IMSIs. Finally, in the last attack, the user can be identified without the need to know his/her personal information (i.e., IMEI, TMSI or IMSI). The three aforementioned attacks are compared in Table 1.

LOCALIZING PEDESTRIANS

Active and passive localization techniques can be distinguished based on user involvement in them. That is, if a pedestrian or his/her MS needs to actively participate in a localization process, it is called active localization; otherwise, it is a passive one. For example, in systems based on active localization techniques, an MS is involved with different base stations and has to calculate its position. On the contrary, in passive localization systems, a user does not even have to know that he/she is being localized. While passive localization systems offer invisibility to both cellular networks providers and end users, they are harder to achieve.

Every localization technique consists of two phases: *signal measurement* and *position calculation* phases. In the first phase, certain signal parameters, such as received signal strength (RSS), time of arrival (TOA), time difference of arrival (TDoA), and angle of arrival (AoA), are extracted and then afterward used in the second phase for calculating the user position. The most popular positioning calculation methods used today are

	Can be used in			Collects user IDs		User can detect it
	2G	3G	4G	TMSI	IMSI	
IMSI catchers	✓	✓	✓	–	✓	✓
IMSI paging attack	✓	✓	✓	✓	–	–
AKA err msg attack	–	✓	✓	–	–	–

Table 1. Differences between methods used for uniquely identifying the user in cellular networks.

geometry-based methods such as triangulation, trilateration, and multilateration. The other group of methods used for the position calculation phase is called proximity-based techniques, where distances are not explicitly calculated, but locations are estimated based on connectivity and proximity constraints to known positions in indoor or outdoor environments. The latter methods are less accurate, but also have lower calculation costs than the former ones.

ACTIVE LOCALIZATION TECHNIQUES

When using active localization techniques, in the signal measurements phase an MS usually measures only RSS values, while the position calculation phase can be divided in two phases: training and localization. In the training phase, also called fingerprinting, an MS moves through the space and records RSS emanating from different base stations. Then in the localization phase, an MS estimates its location by comparing a recent RSS measurement with the previously measured values called fingerprints.

Compared to Wi-Fi fingerprinting, 2G fingerprinting has its advantages and disadvantages. The main advantage is that due to wider coverage, 2G works in more places than Wi-Fi fingerprinting. However, due to a larger range of 2G BTSs, Wi-Fi fingerprinting is more accurate than 2G fingerprinting given the same number of radio sources. Moreover, due to more stable infrastructure, Wi-Fi radio maps degrade quicker than 2G ones. Nevertheless, it was reported that the accuracy achievable for cellular network localization is comparable to that of Wi-Fi networks [11].

The two main differences among different active localization techniques for 2G presented in the literature are:

- The number of BTS signals used in the signal measurements phase
- Methods used in the localization phase

For the signal measurements phase, in [11] the six strongest BTSs were fingerprinted, and then the readings of up to 29 additional 2G channels were used, most of which were strong enough to be detected but too weak to be used for efficient communication. With that kind of fingerprinting, the median accuracy of 5 m in large multi-floor buildings together with the possibility of detecting the difference between floors for both wooden and steel-reinforced concrete structures was reported. For the localization estimation phase, in [11] only the weighted K nearest neighbors algorithm was used, while in [12], in addition to that algorithm, a support vector machine (SVM) classifier and a Gaussian process were also used. It was shown that the SVM classifier provided mean

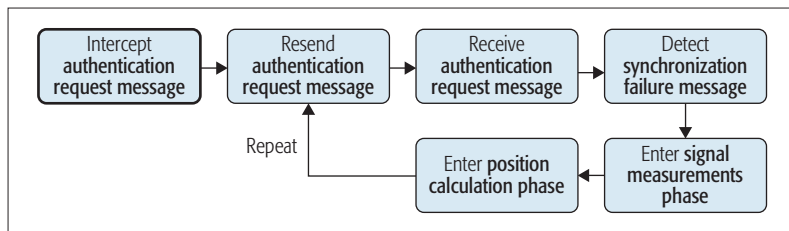


Figure 2. Tracking users passively in cellular networks.

room-level classification efficiency near 100 percent when using the full set of 2G carriers.

PASSIVE LOCALIZATION TECHNIQUES

Unlike active localization techniques, there is very little work done related to the developing passive localization techniques for cellular networks. To the best of our knowledge, only two solutions are currently available. One is a system for indoor localization of 4G signals developed in Japan [13], and the other one is a software defined radio (SDR) system that overhears 2G signals developed in Switzerland [14, 15].

The purpose of the first system was to detect students cheating on their exams [13]. The system was tested in one classroom at the Tokyo Institute of Technology Ookayama campus, where four sensors were put in every corner of the room, and one sensor with three antennas in the center of the room. Through calculating the RSS by the multiple sensors, this technique enabled the localization of the student who was cheating with an accuracy of 42 cm, which was good enough to distinguish between two seats apart for 78 cm.

In the second system, SDR was used to capture signals from 2G [14, 15]. The SDR consisted of hardware (i.e., radio front-end) and software part (i.e., signal processing modules). In this work, two things were shown:

- It was possible to capture 2G signals, convert them to messages, and parse the message content using the proposed SDR.
- It was possible to identify the signal source in order to provide the correct localization for users using 2G.

TRACKING PEDESTRIANS

The previous section showed that passive pedestrian localization using cellular networks is possible. However, in order to be able to track pedestrians as they move, one must add user identification to the localization process. In [14] it was proposed to passively track users distinguishing them based on their different TMSIs because it was observed that in the Sunrise network, a TMSI was changed every 2 h, which was enough time to run experiments, but not fine-grained enough for applications in real-world environments. Moreover, TMSI can be traced back to the user, which can be, in a sense, considered private information. We thus propose to use an AKA protocol linkability attack to test whether the pedestrian is still in the area, since it does not contain any sensible information about the pedestrian himself/herself (i.e., his/her IMSI, IMEI, or TMSI).

As discussed earlier, 3G AKA and 4G EPS-AKA protocols are used every time an MS changes its SN. In AKA or EPS-AKA protocols, authentication request messages (i.e., RAND, AUTN pair) are

sent unencrypted on the radio link, making them susceptible to interception by an attacker. This vulnerability can be used for identification of the pedestrian without learning any sensible information about him/her. Every time when a pedestrian needs to be localized, the tracking system can resend the previously intercepted authentication request message to check whether this pedestrian is still in the area. If he/she is, the authentication response message can be used to determine his/her location. Figure 2 explains the whole process in more detail.

The proposed method for tracking pedestrians using cellular networks does not invade their privacy; nor does it disrupt the existing cellular network services. The localization procedure can be repeated as many times as needed to track them with a lower or higher frequency. The only issue is how to intercept the first authentication request message, which must be investigated in more detail. However, it has been reported that the execution of the 3G AKA protocol can be triggered by repeatedly placing a phone call for the targeted MS and hanging up before the call can be detected by the user [9].

CONCLUSIONS

This article presents an unprecedented data collection technique that can be used to detect pedestrian activity in urban environments. The proposed solution allows a seamless and passive method for tracking pedestrians without invading their privacy. The advantages of tracking signals from pedestrian cell phones in the framework of other passive tracking techniques are:

- Cell phone signals can be used to track a larger number of pedestrians than other wireless communication signals such as Wi-Fi or Bluetooth, due to the widespread use of cell phones.
- Cellular networks are relatively technically stable compared to other wireless standards.
- The deployment of sensors used for tracking can be easier and cost less than other tracking techniques, including the active data collection techniques.
- Finally, since the passive detection technique is based on an unobtrusive observation method, larger-scale datasets can be created.

However, the proposed solution is not free of its own shortages and limitations. In the context of the data collection process for the trip generation purpose, very often it is not only important to know the pedestrian flow, but also their socio-demographic characteristics do matter. In that sense, what would be useful is to combine surveys with the proposed solution. In that way, the trip generation phase of the transportation forecasting process would not lack additional information about peoples' backgrounds; moreover, people would be asked to provide their cell phone numbers needed for the implementation of the AKA protocol linkability attack. However, unlike during active tracking, pedestrians would not need to carry an additional device with them all the time as a constant reminder that they are being watched, which could possibly influence them to change their behavior.

Finally, one should not disregard the security and privacy issues of building a system for seam-

less tracking. Although the proposed solution does not collect personal data about pedestrians, it has yet to be investigated how the proposed tracking system would potentially affect people's lives and habits. Moreover, before building the system it should be determined who would potentially have access to such collected data and for what purposes. The former concern falls under the domain of social studies, while the latter one should be investigated from a legal point of view. Within these limitations, the proposed solution could shed light on unknown aspects of a pedestrian activity in order to improve the quality of their lives through cities.

ACKNOWLEDGMENTS

The authors would like to thank Paolo Santi, Youjin Shin, and Alexander Amini for their useful comments and help while preparing this article. We further thank the MIT SMART Program, Center for Complex Engineering Systems (CCES) at KACST and MIT, the National Science Foundation, the MIT Portugal Program, the AT&T Foundation, Audi Volkswagen, BBVA, the Coca Cola Company, Ericsson, Expo 2015, Ferrovial, GE, and all the members of the MIT Senseable City Lab Consortium for supporting the research. Finally, the research was also partially supported by the National Research Foundation, Prime Minister's Office, Singapore, under its CREATE programme, Singapore-MIT Alliance for Research and Technology (SMART) Future Urban Mobility (FM) IRG, and by research project "Managing Trust and Coordinating Interactions in Smart Networks of People, Machines and Organizations," funded by the Croatian Science Foundation under project UIP-11-2013-8813.

REFERENCES

- [1] M. J. Nieuwenhuisen and H. Khreis, "Car Free Cities: Pathway to Healthy Urban Living," *Environment Int'l.*, vol. 94, 2016, pp. 251–62.
- [2] C. Mitchell, "The Security of the GSM Air Interface Protocol," Univ. of London, Royal Holloway, RHUL-MA-2001-3, 2001.
- [3] D. Fernandez, A. Alejos, and M. G. Sanchez, "Detection of Malicious Base Station Attacks through the Carrier Analysis," *Proc. Radio Science Meeting*, 2015, pp. 213–13.
- [4] N. Golde, K. Redon, and R. Borgaonkar, "Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications," *Proc. 19th Annual Network and Distrib. System Security Symp.*, 2012.
- [5] C. Paget, "Practical Cellphone Spying," *Def Con*, vol. 18, 2010.
- [6] A. Dabrowski et al., "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," *Proc. 30th Annual Computer Security Applications Conf.*, 2014, pp. 246–55.
- [7] D. F. Kune et al., "Location Leaks on the GSM Air Interface," *Proc. 19th Annual Network and Distrib. System Security Symp.*, 2012.
- [8] K. Nohl and S. Munaut, "Wideband GSM Sniffing," *Proc. Chaos Commun. Congress*, 2010.
- [9] M. Arapinis et al., "New Privacy Issues in Mobile Telephony: Fix and Verification," *Proc. ACM Conf. Computer and Commun. Security*, 2012, pp. 205–16.
- [10] T. Ta and J. S. Baras, "Enhancing Privacy in LTE Paging System Using Physical Layer Identification," *Data Privacy Management and Autonomous Spontaneous Security*, Springer, 2013, pp. 15–28.

- [11] A. Varshavsky et al., "GSM Indoor Localization," *Pervasive and Mobile Computing*, vol. 3, no. 6, 2007, pp. 698–720.
- [12] B. Denby et al., "High-Performance Indoor Localization with Full-Band GSM Fingerprints," *Proc. IEEE ICC Wksp.*, 2009, pp. 1–5.
- [13] System for Detecting Cheating, <http://j-net21.smrj.go.jp/develop/digital/entry/001-20120613-01.html>
- [14] I. Alyafawi, D. C. Dimitrova, and T. Braun, "SDR-Based Passive Indoor Localization System for GSM," *Proc. ACM Wksp. Software Radio Implementation Forum*, 2014, pp. 7–14.
- [15] —, "Real-Time Passive Capturing of the GSM Radio," *Proc. IEEE ICC*, 2014, pp. 4401–06.

BIOGRAPHIES

IVA BOJIC [M'08] (ivabojic@mit.edu) is a senior postdoctoral researcher at Singapore-MIT Alliance for Research and Technology, Singapore. She received her M.S. and Ph.D. degrees in computer science from the University of Zagreb Faculty of Electrical Engineering and Computing in 2009 and 2013, respectively. She also holds a second M.S. in mathematics from the University of Zagreb Faculty of Science. From 2014 to 2015 she was a Fulbright Scholar at the Massachusetts Institute of Technology and from 2009 to 2014 she was with the University of Zagreb. Her doctoral thesis was awarded the Silver Plaque Josip Loncar the Dean's award for outstanding doctoral dissertation and particularly successful scientific research. In 2012 she received the "Google Anita Borg" award from Google for strength of academic performance, leadership experience, and demonstrated passion for computer science. The same year she was also awarded the Richard E. Merwin award by IEEE for demonstrating outstanding involvement in IEEE and excellence in academic achievement. In the past, she served as an IEEE Student Ambassador for IEEE Region 8, a Chair of the IEEE Computer Society Student Chapter of Zagreb, Croatia, an IEEE Student representative, and a Chair of the IEEE Educational Activities for Croatia Section.

YUJI YOSHIMURA (yyoshi@mit.edu) is a Ph.D. candidate in computer sciences at the Universitat Pompeu Fabra and a research affiliate at the Massachusetts Institute of Technology Senseable City Laboratory. He is also a founding partner of the international technology management for innovation office, laboratory urban DECODE. He received his DEA (Diploma of Advanced Studies) and a postgraduate degree in architecture and urban studies from the Universitat Politècnica de Catalunya. Previously, he worked at the Barcelona Urban Ecology Agency and CENIT (Center for Innovation in Transport), dealing with urban mobility and environmental analysis. His recent works include the analysis of visitors' behavior in the Louvre Museum through a sensor network, and the analysis of human mobility behavior by a transaction dataset. Supported by the combination of his expertise on architecture and mobile technologies, and direct experience in mobility and environmental planning, he largely works on vehicle and pedestrian flow analysis and simulation, environmental analysis through wireless sensor technologies, and mobile technology applied to urban planning.

CARLO RATTI (ratti@mit.edu) is a professor of the practice of urban technologies at the Massachusetts Institute of Technology, where he directs the Senseable City Lab. He is also a founding partner of the international design and innovation office Carlo Ratti Associati. He graduated in engineering from the Politecnico di Torino and the École Nationale des Ponts et Chaussées in Paris, and later earned his M.Phil. and Ph.D. at the University of Cambridge, United Kingdom. He completed his Ph.D. at the Massachusetts Institute of Technology as a Fulbright Senior Scholar. He holds several patents and has co-authored over 250 publications, including the recent book *The City of Tomorrow* (Yale University Press, June 2016, with Matthew Claudel). In addition to scientific writings, he is a regular contributor to popular media including Project Syndicate, *New York Times*, *Washington Post*, *Financial Times*, and *Scientific American*. His work has been exhibited worldwide at venues such as the Venice Biennale, the Design Museum Barcelona, the Science Museum in London, MAXXI in Rome, and the Museum of Modern Art in New York City.

Although the proposed solution does not collect personal data about pedestrians, it has to be yet investigated how the proposed tracking system would potentially affect people's lives and their habits. Moreover, before building the system it should be determined who would potentially have access to such collected data and for what purposes.

A Novel SDN-Based Architecture to Provide Synchronization as a Service in 5G Scenarios

Stefano Ruffini, Paola Iovanna, Mats Forsman, and Tomas Thyni

Moving toward 5G, network synchronization is expected to play a key role in the successful deployment of the new mobile communication networks. This article presents an application of SDN (software defined networking) and NFV (network function virtualization) principles to the network synchronization area enabling to offer synchronization as a service.

ABSTRACT

Moving toward 5G, network synchronization is expected to play a key role in the successful deployment of the new mobile communication networks. This article presents an application of SDN (software defined networking) and NFV (network function virtualization) principles to the network synchronization area, making it possible to offer synchronization as a service. The approach is based on defining a harmonization layer that orchestrates radio and heterogeneous transport domains by means of a suitable subset of abstracted information exchanged among the domains, and by making use of virtualized synchronization functions.

INTRODUCTION

5G is the next step in the evolution of mobile communication. In contrast to earlier generations, 5G wireless access should not be seen as a specific radio-access technology [1]. Rather, it is the overall wireless-access solution addressing the demands and requirements of mobile communication beyond 2020. To enable connectivity for a wide range of new applications and use cases, the capabilities of 5G wireless access must extend far beyond those of previous generations. These capabilities include the possibility to provide very high data rates everywhere, support for very low latency and ultra-high reliability, and the possibility of devices with very low cost and very low energy consumption. Furthermore, 5G wireless access needs to support a massive increase in traffic in an affordable and sustainable way, implying a need for a dramatic reduction in the cost and energy consumption per delivered bit.

Synchronization is a term used in various contexts and often with different meanings. Within the scope of this article, it relates to the “*network synchronization*” concept. This concerns the distribution of common time and/or frequency references to the nodes in a network in order to align their time and frequency scales, respectively [12]. Network synchronization is traditionally important to guarantee good performance in transport and mobile operations (e.g., user equipment handover in radio networks). Frequency synchronization is generally sufficient for these purposes. However, in recent years it has become more important to deliver accurate phase/time synchronization, for instance to enable the alignment of radio frames to better use radio resources. In time divi-

sion duplexing (TDD), for example, time division allocation of uplink and downlink allows an optimized use of radio resources. This requires radio base stations to send synchronous radio signals in order to avoid interference.

As we move toward 5G, synchronization (and time synchronization in particular) is expected to become even more critical. Following are some of the aspects that are particularly relevant:

- New radio access technologies, complementing existing technologies, for which phase/time synchronization is expected to play a key role.
- New applications, such as machine type communications (MTC) and the Internet of Things (IoT), increasing the demand for accurate and/or reliable synchronization.
- New transport solutions and technologies, especially in fronthaul, will be needed to meet the challenging transmission needs of 5G in terms of capacity, reliability, latency, and robustness.
- Application of the SDN and NFV concepts, with potential impacts on the synchronization network architecture and operations. Cloud and distributed applications are additional trends that may also become relevant from a network synchronization perspective.

The control of latency is another key aspect for a successful deployment of 5G that deserves particular attention. In fact, strict latency is one of the main targets for some of the applications that need to be supported by 5G, such as automatic traffic control, remote surgery, and tactile internet. In this respect, as reported in [2], 5G systems should provide end-to-end latency of 10 ms and, in specific use cases, end-to-end latency of 1 ms. Good synchronization may become a key enabler.

In summary, 5G will impose a number of requirements that in one way or another could require accurate and reliable network synchronization and also imply a more complex handling of network synchronization operations (e.g., due to the fact that the same infrastructure shall handle different types and levels of requirements and support multiple service providers and applications). The impact on the network architecture is also particularly relevant from a synchronization perspective due to new concepts such as NFV and SDN.

On one hand this may impact how synchronization networks will be handled, but at the same

time it could provide tools that will facilitate the support of synchronization and of the latency related requirements.

This article presents how some of the aspects listed above could benefit from applying the principles of the software defined networking (SDN) and network function virtualization (NFV). The article is structured as follows. After a brief introduction of the key technologies in network synchronization and SDN/NFV, the article discusses the main network synchronization challenges expected in a 5G environment. We describe a possible approach to apply the SDN and NFV concepts to the area of network synchronization, with examples of relevant parameters and work flow. The feasibility and relevance of the solution is then demonstrated as applied to a relevant use case.

RELEVANT TECHNIQUES

DISTRIBUTING SYNCHRONIZATION IN THE NETWORK

One main technology to distribute time synchronization in a network is to generate an accurate time synchronization reference at some central location, e.g., via a GNSS (Global Navigation Satellite System) receiver, and further distribute it over the network via standard timing protocols such as IEEE 1588 [11]. GNSS may also be deployed locally (e.g., directly connected to the end user).

In the case of synchronization distribution over packet networks, the highest time synchronization accuracy can be achieved when all nodes in the network support IEEE 1588 (e.g., boundary clocks or transparent clocks). Additional architectures are being defined (e.g., partial timing support ([6])). The authors in [4] derived some basic rules to meet predefined performance objectives in different parts of the network. A proper network design would make it possible to meet 1.5 us phase accuracy on the radio interface. Frequency synchronization can also be achieved by means of synchronous Ethernet ([7, 8]). An enhanced version of synchronous Ethernet (*enhanced syncE*) is currently being defined by ITU-T.

In general, a multiplicity of approaches is possible in order to meet the relevant synchronization requirements. A combination of various techniques will in general be recommended in order to improve reliability and availability (e.g., to address GNSS vulnerability due to risk from jamming).

NFV AND SDN

Network functions virtualization (NFV) [10] proposes a new model based on the “as a service” concept by which the organization can be simplified and resources and services can be manipulated at different levels in order to create smart and fast services. The model enables a full decoupling of the network functions from the corresponding hardware infrastructure that can be shared, thus enabling a new business model where the end user (service providers) can be a client of an infrastructure provider with a clear demarcation of roles and responsibilities. According to the NFV, the network functions can be realized on one or more virtual machines running on different software and processes, avoiding the necessity of dedicated hardware for each service.

A key enabler of the NFV model is the software defined technology (software defined networking [9]) which, thanks to the separation

between the data-plane and the control plane, defines a clear demarcation between where the traffic is transmitted and the point where the decisions are taken. The main principle is based on providing a suitable abstraction of the hardware resources that can be considered as a commodity for any type of services. The combined use of SDN and NFV enables the defining and deploying of new services on demand, dynamically and very quickly, by software programming the resources, dramatically reducing the cost and time to market of new services.

SYNCHRONIZATION CHALLENGES IN 5G

Network synchronization, especially in 5G scenarios, will be relevant in several domains, with different needs and requirements. According to [2] radio and transport domains could interwork in a very tight manner, in order to provide “infrastructure as a service” (IaaS). In addition, the transport domain could evolve smoothly toward an SDN model, providing scenarios where very heterogeneous domains that differ in data-plane technology, control plane, and vendor, interwork with the radio domain to provide 5G services. In particular, some of these domains could be based on SDN, others could be based on a distributed control plane such as MPLS (Multiprotocol Label Switching)/GMPLS (Generalized Multiprotocol Label Switching), and others could be managed by a network management system. Different actors will be involved in these scenarios, both network providers and service providers.

The handling of synchronization in this framework is expected to become a challenging task, and harmonization between all involved domains will be particularly important. As an example, radio access and mobile backhaul are traditionally handled in different domains, often under different network administrators. This could make it very complex to meet some of the most stringent performance requirements, e.g., in terms of latency and network synchronization.

Network synchronization is one key example where tight cooperation between transport and radio access could provide significant benefits. Domains other than radio are also becoming of interest from a synchronization perspective. In particular, emerging synchronization needs have been reported in data centers (see as an example the “Google spanner,” where all servers must have access to a reliable and accurate time synchronization reference [14]). Other examples can be found in the financial sector, power networks, and industrial automation.

Solutions for the harmonization of different transport network domains have been proposed [13], but the case of 5G where radio and transport tightly cooperate to provide synchronization as a service is not addressed. In particular, the following synchronization related aspects still need to be fully addressed:

- Which parameters provide a suitable network model able to offer synchronization as a service?
- How to apply network virtualization principles as required by network operators?
- How to handle synchronization service level agreements (SLAs) with different levels of accuracy and with minimum operation-

Radio access and mobile backhaul are traditionally handled in different domains, often under different network administrators. This could make it very complex to meet some of the most stringent performance requirements e.g. in terms of latency and network synchronization.

The Virtual Net Sync Harmonizer, depending on the specific requirements and applicable policies, defines a suitable synchronization solution and synchronization network architecture and via the SDN controllers sets up SW defined synchronization functions and properly provisions the network.

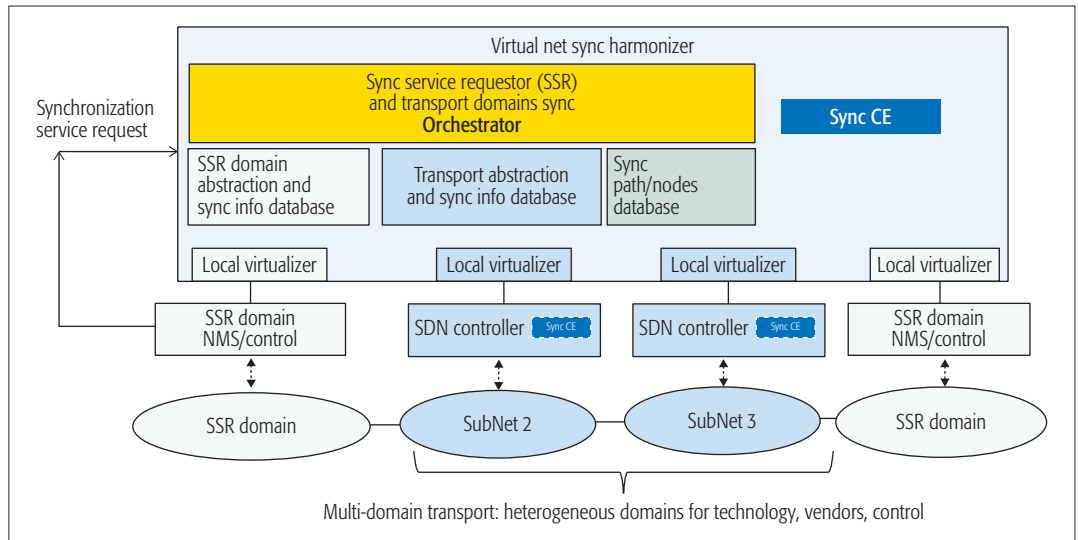


Figure 1. Virtualized Network Sync solution.

- al costs? How to differentiate the services according to the network synchronization capabilities?
 - How to handle dynamic changes in synchronization capability/requirements?
 - How to monitor related performance?
 - How to handle contexts with multiple and heterogeneous domains?
- The following sections try to answer the above questions with a potential approach based on SDN and NFV principles.

SDN-BASED SYNCHRONIZATION SERVICE

The approach described in this article and shown in Fig. 1 is specifically related to a method to deliver synchronization services. The approach assumes an abstraction modelling of the relevant parameters for a technology-agnostic service support. In this model the client could be any type of domain with any type of synchronization needs.

According to this model, in order to set up the desired end-to-end synchronization solution, the involved domains are configured by means of virtualized synchronization functions as a result of a specific synchronization service request. The concept is based on a harmonization layer on top of each domain that allows harmonizing such domains by means of processing only a subset of the information, so that the impact on each domain is minimized.

The overall architecture is based on the following key components:

- The *virtual net sync harmonizer*, which receives relevant information from each domain through standard interfaces (e.g., the Path Computation Element Protocol (PCE-P), Netconf, etc.).
- The *SDN controller/local virtualizer* pair, which collects information on a specific domain at a suitable abstraction level, and that properly sets up/configures the domain.

In order to properly support the synchronization service requirements, the virtual net sync harmonizer receives the key parameters from multiple and heterogeneous domains: information on the related IEEE1588 support (and which profile is supported, e.g., ITU-T G.8275.1 [5] vs. ITU-T

G.8275.2 [6]); information on synchronous Ethernet support; information on the link characteristic (e.g., link length, physical layer type, whether asymmetry compensation has been applied, etc.); and information on support for multi-clock domains (e.g., in the case of IEEE 1588, whether or not multiple boundary clock instances are implemented), clock-oscillator characteristics, etc.

The virtual net sync harmonizer receives the request for the synchronization service to support, that is, the “sync service requestor” (SSR) domain needs in terms of requirements and policy (e.g., absolute time accuracy vs. relative phase difference requirements; synchronization to be distributed only in isolated cluster of nodes; time synchronization vs. frequency synchronization, etc.). The relevant details of the SSR domains (e.g., topology, synchronization characteristics, etc.) are also exposed via the SSR domain NMS (network management system)/control block.

The *sync service requestor* domain could typically be a radio domain, but as mentioned earlier, other examples exist such as a network of servers implementing financial applications, power networks, industrial automation networks, etc.

The virtual net sync harmonizer, depending on the specific requirements and applicable policies, defines a suitable synchronization solution and synchronization network architecture, and via the SDN controllers, sets up SW defined synchronization functions and properly provisions the network. A specific synchronization algorithm could be involved in order to select among a set of multiple synchronization alternatives.

Looking further into the details, the virtual sync network harmonizer may be structured into the following logical functions:

- Sync service requestor (SSR) and *transport domains sync orchestrator*, which combines the relevant information.
- *Sync CE* (synchronization computation element), which selects a specific algorithm and identifies a suitable solution and synchronization network architecture.
- Relevant databases where the result of the sync CE calculation are stored, including the *SSR domain abstraction and sync info data-*

base, the *transport abstraction and sync info* database, and the *sync path nodes* database.

As an example, the nodes in the various domains could implement and support the following fundamental synchronization functions ([7, 3, 11]): oscillator of a certain quality, holdover of certain characteristics, support for synchronous Ethernet or enhanced synchronous Ethernet, and IEEE 1588 “on-path” support (e.g., boundary clock or transparent clock).

The following are software-defined functions that could be provisioned: transparent clock vs. boundary clock (e.g., in case a service requires multiple synchronization paths, a transparent clock may be more convenient); PTP (Precision Time Protocol) profile; BMCA (Best Master Clock Algorithm); PTP domains, etc.; and PTP reference priorities, synchronous Ethernet priorities, etc. This is shown with an example in Fig. 2, where the node, in addition to providing specific port capabilities, includes the concept of programmability of synchronization support (e.g., transparent clock vs. boundary clock).

EXAMPLE OF SYNCHRONIZATION NETWORK OPERATION

The operation of a synchronization network based on the architecture described in this article is presented by means of an example. The following is the sequence of the steps that could be considered in the implementation of the solution.

1. The *SDN controllers/local virtualizers* collect information on the network topology and the parameters per each node/link from all involved domains (distance in Km, characteristics of the link, such as asymmetry compensated/not compensated, type of the physical layer, e.g., microwave/fiber; node synchronization function support and clock characteristics). This information provides an abstraction of the domains.

In the case of already established synchronization flows, the related information is also collected (e.g., details of the synchronization chain from the PTP grandmaster to the border nodes per each connected node, e.g., the base station). Similar information is also collected from the SSR domain (topology, supported synchronization functions, etc.).

2. The virtual net sync-harmonizer receives the request on the specific synchronization service to offer to a specific domain (the sync service requestor-SSR domain, e.g., the radio domain), with information on the type of synchronization required, (e.g., the required accuracy, etc.) and, based on the characteristics of the network, it can decide the most appropriate solution and policy to apply.

3. The virtual net sync-harmonizer asks the *local virtualizers* (if it includes sync CE functions) to properly define the virtual synchronization functions of the nodes and sets up the synchronization flow(s) according to a specific policy and service requirements. The local virtualizer, based on the relevant parameters and the related policy, calculates the best synchronization reference and provides this information to the virtual net sync-harmonizer for proper harmonization with the other domains.

4. The virtual net sync-harmonizer sends commands to the SSR domain NMS for the proper synchronization function configuration (e.g., syn-

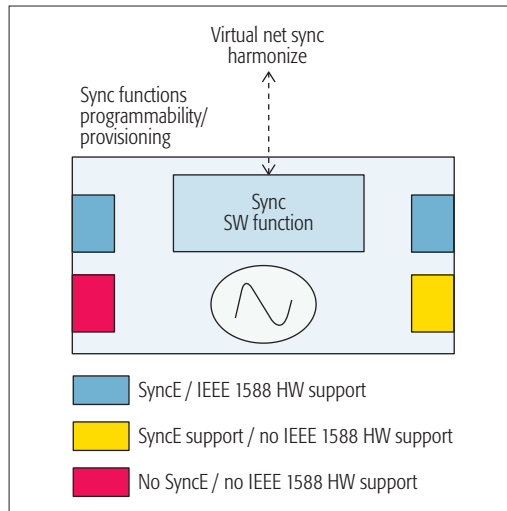


Figure 2. Sync programmability.

chronization method and reference selection) in the SSR domain. The result is to provide an end-to-end synchronization solution with certain characteristics.

5. The network is continuously monitored. Any change in the network and/or result from the performance monitoring functions, triggers a restart from step #1.

Further details on potential use cases and relevant parameters are provided later.

RELEVANT PARAMETERS FOR ABSTRACTION AND USE CASES

Examples of parameters that can be exchanged between the net sync virtual harmonizer and the sync local virtualizer are presented below. Note that for better scalability, such information could be provided per aggregated links.

Link parameters could be: the length in Km of the link, information on IEEE 1588 support (e.g., whether or not the outgoing links from the node are with IEEE 1588 support), the physical link characteristics (e.g., fiber, microwave, xDSL), and information on asymmetry compensation (e.g., indicating whether or not the asymmetry has been compensated on that link).

Node parameters could be related to information on IEEE1588 support, synchronous Ethernet support, oscillator characteristics (e.g., clock type/stratum clock hosted by the node), type of PTP clock (e.g., max constant time error the PTP clock is expected to contribute with). Additional relevant parameters can be added in a programmable approach according to the SDN principles.

Several policies can be configured, including the following as examples:

- *Frequency/time/phase*, i.e., indicating whether only frequency synchronization or both frequency and phase synchronization are required.
- *Transparent sync*, i.e., indicating whether or not the timing shall be carried transparently across the domains.
- *Physical layer-based* frequency synchronization, i.e., indicating whether frequency synchronization shall be carried via the physical layer or via timing packets;
- *Link length-based*, i.e., in a weighted-based algorithm to evaluate the best synchroniza-

The local virtualizer based on the relevant parameters and the related policy, calculates the best synchronization reference and provides this information to the Virtual Net Sync-Harmonizer for proper harmonization with the other domains.

The specific requirement from the SSR would indicate that multiple synchronization flows should be preferable available at the radio domains, so that a dynamic selection is possible depending on variable cluster combination. Moreover, it could be assumed that there can be various degrees of phase synchronization accuracy that are acceptable.

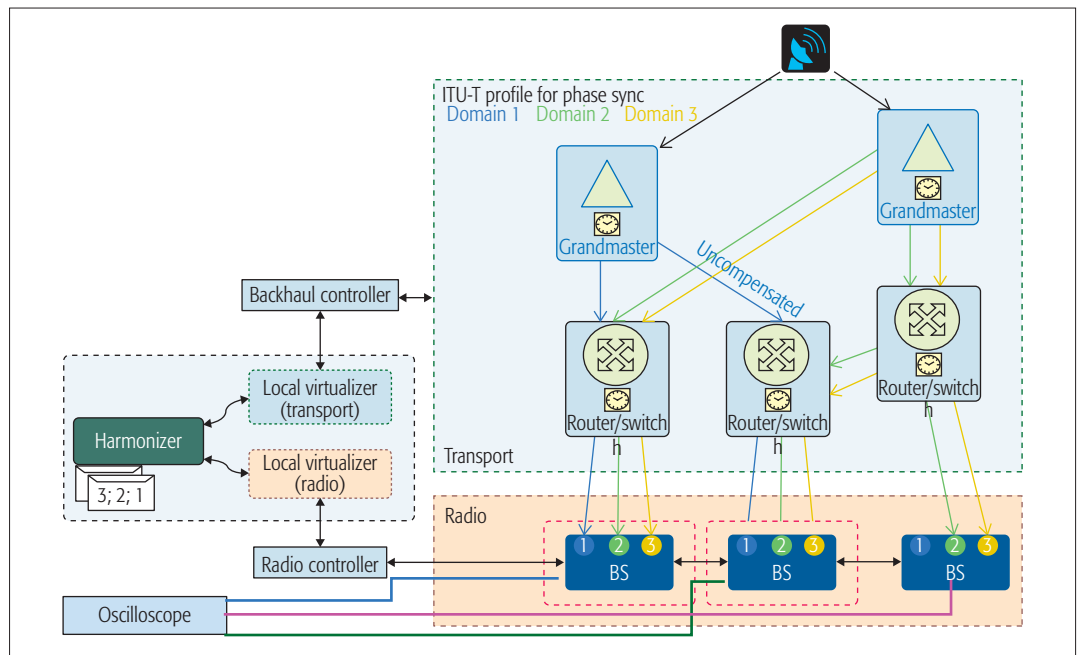


Figure 3. Synchronization for base station cluster-demo set up.

tion reference, using a multiplication factor indicating the length of the link (e.g., a multiplication factor of 2 for every 30 Km).

- *Physical layer-based*, i.e. in a weighted-based algorithm to evaluate the best synchronization reference, using a multiplication factor indicating the type of link (e.g., a multiplication factor of 1 for fibre, 2 for microwave).
- *1588 support-based*, i.e., in a weighted based algorithm to evaluate the best synchronization reference using a multiplication factor indicating whether IEEE1588 hardware on-path support is provided (e.g. 1 if all nodes support IEEE1588; 3 if the links outgoing from a node have no IEEE1588 support).
- *Asymmetry compensated-based*, i.e., in a weighted-based algorithm to evaluate the best reference, using a multiplication factor indicating whether asymmetry has been compensated in the link (e.g., a multiplication factor of 1 if compensated; 3 if not compensated).

The solution can be applied to various use cases. A few potential examples are described below.

Use Case 1–Synchronization for a Cluster of Base Stations: In this example the SSR domain is a radio domain that needs to handle various and variable clusters of base stations that require local phase synchronization (e.g., to implement coordinated multipoint (CoMP), or enhanced inter-cell interference coordination (eICIC), with different levels of phase synchronization accuracies.

The specific requirement from the SSR would indicate that multiple synchronization flows should preferably be available at the radio domains, so that a dynamic selection is possible depending on variable cluster combination. Moreover, it could be assumed that there can be various degrees of phase synchronization accuracy that are acceptable. Based on this request, the policy selected by the virtual net sync-harmonizer (by the sync CE function) is the “transparent sync” transport so

that synchronization masters owned by the SSR operator can be used and the synchronization references can be carried transparently across the domains.

The local virtualizer identifies an MPLS based network, and in order to allow for transparent transport with the highest accuracy, makes sure that the synchronization path from the master to the base stations traverses nodes with “on-path-support” (e.g., PTP transparent clocks and residence time measurement (RTM) support (see [15]). An algorithm minimizing the phase difference per each cluster of the base stations is implemented by the sync CE, selecting the best reference per base station.

Use Case 2–Request for Network Characteristics: In this example, the synchronization request concerns the performance monitoring of the packet network as a way to understand the capabilities in distributing synchronization over a partial timing support network [6]. The IEEE1588 performance monitoring tools are configured in the network nodes and the related data is collected. Moreover, asymmetry of the links is calculated by means of automatic methodologies [3].

Use Case 3–Set-up of G.8275.2 (Partial Timing Support) Network: This example can be considered as an extension of the previous example. The SSR domain requests the set-up of PTP flows (also for local GNSS assisted partial timing support), with certain characteristics (e.g., 1 us packet delay variation measured by means of an appropriate metric and 500 ns worst case asymmetry). The SSR domain also requires G.8275.2 PTP performance monitoring across the domains.

The virtual net sync-harmonizer asks the local virtualizer to set up specific performance monitoring (PM) tools and collects and assembles the performance monitoring information. Based on this information, the sync CE evaluates the suitable synchronization paths. These are defined by means of proper MPLS paths involving as much as possible RTM enabled label switching routers (LSRs). Per-

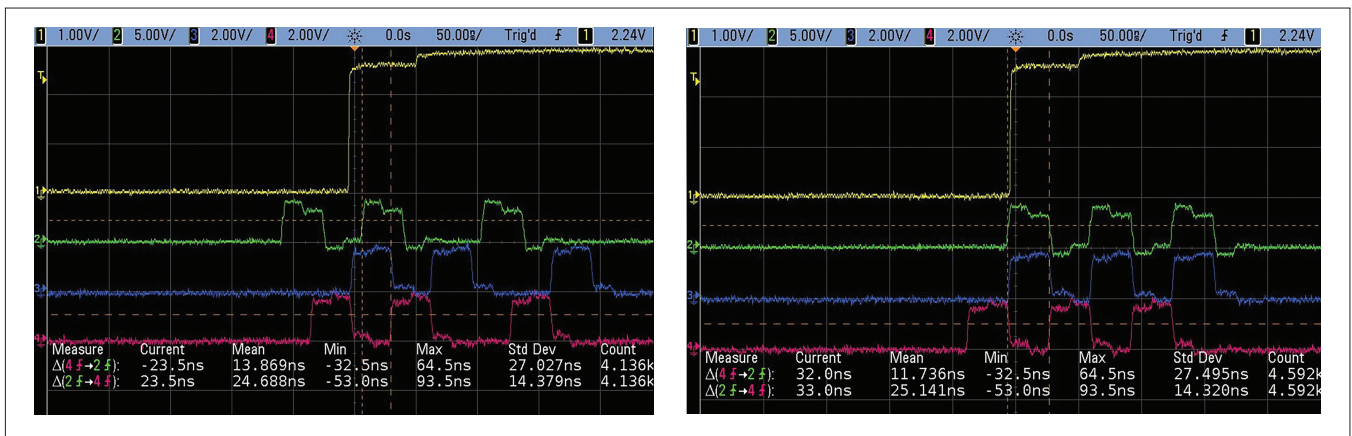


Figure 4. Phase deviation between base stations: initial status (left) and after network rearrangement (right)

formance monitoring results are continuously provided to the sync service requestor (SSR) domain.

DEMONSTRATOR

The feasibility of the solution as applicable to use case #1 described above, has been assessed via a demonstrator implemented in “opendaylight” (open source project, see <https://www.opendaylight.org/>) as shown in Fig. 3.

Two synchronization masters (PTP grandmasters), connected to a GNSS source, distribute the synchronization references (PTP flows, each of them identified by means of the PTP domain number attribute) over a packet network. The PTP flows reach the end user (base station) via different paths with different characteristics (e.g., some of the links may have been compensated for asymmetry, other have not been compensated). The characteristics of the network and of the PTP flows are made available to the (virtual net sync) harmonizer.

The radio domain sends a request to optimize the synchronization between two specific base stations (BS), highlighted with dotted red lines in the figure. Various tests have been performed. In the example shown here the relative phase deviation resulting from the initial network synchronizations setup as shown by the graph on the left in Fig. 4 (green and blue lines), in the order of 50 ns.

After the rearrangement of the synchronization network, based on the information retrieved from the transport domain (in particular by avoiding the selection of PTP references that have traversed links where the asymmetry was not compensated), it was possible to improve the phase synchronization accuracy down to a few ns, thus enabling the activation of very demanding services (e.g. multiple input multiple output (MIMO)) as shown by the right graph in Fig. 4.

Future studies are being considered to address additional use cases and to refine the network abstraction models that can be used to model the network characteristics. An optimization of the algorithms used to support the various policies could also be considered.

CONCLUSIONS

Moving toward 5G, network synchronization is expected to play a key role in the successful deployment of the new mobile communication networks. 5G will impose a number of requirements that in one way or another could require

an accurate and reliable network synchronization and also imply a more complex handling of network synchronization operations.

This article has shown how the SDN and NFV concepts could be advantageously applied in this area. The architecture that has been presented is based on a client-server model. This system works on top of the existing networks and application domains (with a hierarchical architecture) in order to limit the impact on the procedures of each domain. The hierarchical architecture and independence of the domains allow for an end-to-end interworking among domains with heterogeneous synchronization capability, and makes it possible to automatically plug-and-play network domains and nodes.

The minimum set of information relevant to set up the synchronization network is collected from each domain. This information is used to harmonize and configure each domain (both radio and transport). Examples of parameters and functions that could allow tight and efficient interworking between the various domains have been presented. The nodes in the domains support some basic hardware synchronization functions with the capability to set up specific software-based functions, which makes it possible to optimize the support for a specific request. The centralized virtual net sync harmonizer properly instructs which functions need to be implemented.

The feasibility of the solution has been assessed via a demonstrator implemented in “opendaylight” and has been applied to an important radio network use case. Future studies could include the analysis of additional use cases as well as a refinement of the network abstraction models and algorithms that can be used to model the network characteristics.

ACKNOWLEDGEMENTS

The authors would like to thank Mikael Johansson S (Ericsson), Richard Jönsson (Ericsson), Francesco Giurlanda (Coritel), and Luca Contri (Ericsson), for their valuable contribution to the implementation of the demonstrator described in this article.

REFERENCES

- [1] “5G: What is It?” Ericsson white paper, Oct. 2014, (<http://www.ericsson.com/res/docs/2014/5g-what-is-it.pdf>, accessed Oct. 2016).
- [2] “NGMN 5G White Paper,” NGMN Alliance white paper, February 17 2015 (http://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf, accessed Oct. 2016).

The feasibility of the solution has been assessed via a demonstrator implemented in “opendaylight” and has been applied to an important radio network use case. Future studies could include the analysis of additional use cases as well as a refinement of the network abstraction models and algorithms that can be used to model the network characteristics.

- [3] ITU-T Recommendation G.8271, “Time and Phase Synchronization Aspects in Packet Networks,” 2012.
- [4] ITU-T Recommendation G.8271.1, “Network Requirements for the Transport of Phase and Time,” 2013.
- [5] ITU-T Recommendation G.8275.1, “Precision Time Protocol Telecom Profile for Time/Phase Synchronization,” 2016.
- [6] ITU-T Recommendation G.8275.2, “Precision Time Protocol Telecom Profile for Time/Phase Synchronization with Partial Timing Support from the Network,” 2016.
- [7] ITU-T Recommendation G.8261, “Timing and Synchronization Aspects in Packet Networks,” 2013.
- [8] ITU-T Recommendation G.8262, “Timing Characteristics of a Synchronous Ethernet Equipment Slave Clock (EEC),” 2015.
- [9] “Software-Defined Networking: The New Norm for Networks,” ONF white paper, Apr. 13, 2013 (<https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>, accessed Oct. 2016).
- [10] “Network Functions Virtualisation, An Introduction, Benefits, Enablers, Challenges & Call for Action,” ETSI white paper, Oct. 22–24 2012 at the “SDN and OpenFlow World Congress,” Darmstadt-Germany (http://portal.etsi.org/NFV/NFV_White_Paper.pdf, accessed Oct. 2016).
- [11] IEEE Std 1588™-2008 “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” July 2008.
- [12] ITU-T Recommendation G.810, “Definitions and Terminology for Synchronization Networks,” 1996.
- [13] P. Iovanna *et al.*, “E2E Traffic Engineering Routing for Transport SDN,” *Optical Fiber Commun. Conf.*, OSA Technical Digest (online) (Optical Society of America, 2014), paper W1K.3.
- [14] J. C. Corbett *et al.*, “Spanner: Google’s Globally-Distributed Database,” *Proc. OSDI 2012*, pp. 251–64.
- [15] IETF MPLS Working Group Internet-Draft, Residence Time Measurement in MPLS Network, July 21 2016 (<https://datatracker.ietf.org/doc/draft-ietf-mpls-residence-time>, accessed Jan. 2017).

BIOGRAPHIES

STEFANO RUFFINI (stefano.ruffini@ericsson.com) graduated in telecommunication engineering from the University of Rome “La Sapienza” (Italy). He joined Ericsson in 1993 and has been working on synchronization aspects for more than 20 years. He has represented Ericsson in various standardization organizations, and is currently serving as Rapporteur of ITU-T Q13/15. He is currently involved in fronthaul and mobile backhaul studies. He has published several international journal papers and is a co-author of a book dealing with IEEE1588 and Synchronous Ethernet.

PAOLA IOVANNA (paola.iovanna@ericsson.com) graduated in electronics engineering from the University of Roma “Tor Vergata.” She joined Ericsson in 2000 and has been working on various research projects on packet and optical routing, control plane, and path computation solutions. She is currently leading a research team on transport networking and control solutions for 5G. She holds more than 50 patents and is an author of several publications in international scientific journals and conferences.

MATS FORSMAN (mats.forsman@ericsson.com) joined Ericsson in 1999 to work with intelligent networks. Since then he has worked within the IP, broadband, and optical networks areas. Today, his focus is on new concepts for transport within RAN at Ericsson Radio. One such concept area is RAN and transport interaction. He holds an M.Sc. in mathematics and natural science from Umeå University, Sweden.

TOMAS THYNI (tomas.thyni@ericsson.com) is an expert in the area of IP and transport networks. A telecommunication and network engineer, he joined Ericsson in 2000 and has worked within the IP, broadband, and optical networks areas. Currently he is working on new concepts for transport in RAN at Ericsson Radio. Prior to joining Ericsson, he worked for 15 years as an IP and transport network designer at various network operators.

An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement

Claas Lorenz, David Hock, Johann Scherer, Raphael Durner, Wolfgang Kellerer, Steffen Gebert, Nicholas Gray, Thomas Zinner, and Phuoc Tran-Gia

ABSTRACT

In recent years, the number of attacks and threat vectors against enterprise networks have been constantly increasing in numbers and variety. Despite these attacks, the main security systems, for example network firewalls, have remained rather unchanged. In addition, new challenges arise not only to the level of provided security, but also to the scalability and manageability of the deployed countermeasures such as firewalls and intrusion detection systems. Due to the tight integration into the physical network's infrastructure, a dynamic resource allocation to adapt the security measures to the current network conditions is a difficult undertaking. This article covers different architectural design patterns for the integration of SDN/NFV-based security solutions into enterprise networks.

INTRODUCTION

The security system that commonly forms the first line of defense in today's enterprise networks consists of a perimeter gateway firewall (PGF). Positioned at the edge of the network, the PGF inspects and filters all incoming and outgoing packets according to the configured security policy. Traffic spikes are often handled by over-provisioning, resulting in increased operating costs. Furthermore, this approach provides no protection against attacks conducted by malicious or previously compromised nodes inside the network. Therefore, additional security systems have to be installed at every security boundary, which results in high acquisition and maintenance expenses. Often, this leads to an abandonment of these systems and an implicit in-prizing into the enterprise's risk management.

As a relief, security systems based on the concepts of software defined networking (SDN) and network functions virtualization (NFV) have been proposed to enhance overall network security while simultaneously reducing operational costs [3]. SDN separates the control plane from the data plane and hence allows the network operator to automatically steer individual flows via a central programmable interface [8]. This allows a fine-grained security policy enforcement and thus

improves overall network security. NFV enables the migration of typical middlebox hardware such as load balancers and firewalls into software running on virtual machines [5]. These instances can be scaled up and down, depending on the actual resource requirements without over-provisioning. Hence, combining these two technologies can provide a solid foundation for the creation of an omnipresent and scalable security solution.

Following this proposition, we analyze the transformation of enterprise networks consisting of separated cloud, network, and security components to an integrated solution enabled by SDN and NFV. To illustrate the advantages and disadvantages, we examine stateful firewalling as an example of different integration approaches. Finally, we discuss the newly introduced challenges and outline possible solutions.

Due to the tight integration into the physical network's infrastructure, a dynamic resource allocation to adapt the security measures to the current network conditions is a difficult undertaking. The authors cover different architectural design patterns for the integration of SDN/NFV-based security solutions into enterprise networks.

ARCHITECTURES OF TRADITIONAL ENTERPRISE NETWORKS

We begin with a description of the status quo of traditional network architectures with special emphasis on the management systems involved, as they provide the central functionality for all operational concerns. In general, management of enterprise networks includes the topics fault, configuration, accounting, performance, and security. To address these areas, network operations mainly rely on three separated columns, as illustrated in Fig. 1 a network management system (NMS), a cloud management system (CMS), and a security management system (SMS).

At the core, the NMS is responsible for provisioning, configuring, and monitoring the available network resources. In the provisioning stage, the NMS provides the initial network connectivity to a newly deployed device and prepares all necessary prerequisites for the configuration stage. This can range from enabling network boot up to the installation of an entire operating system. Once this stage is completed, the configuration stage takes over, installing the required software and applying the appropriate settings. Finally, as soon as the device is operational, the NMS transitions to the monitoring stage and triggers alarm notifications in case of detected failures.

Claas Lorenz is with genua GmbH, Germany; David Hock and Johann Scherer are with Infosim GmbH & Co. KG, Germany; Raphael Durner and Wolfgang Kellerer are with Technical University of Munich, Germany; Steffen Gebert, Nicholas Gray, Thomas Zinner, and Phuoc Tran-Gia are with the University of Würzburg, Germany.

Although this architecture has proven to provide a functional management of the network infrastructure, it also imposes several shortcomings such as scalability issues and an increased management overhead. To mitigate these effects, we propose an enhanced enterprise network architecture based on SDN and NFV.

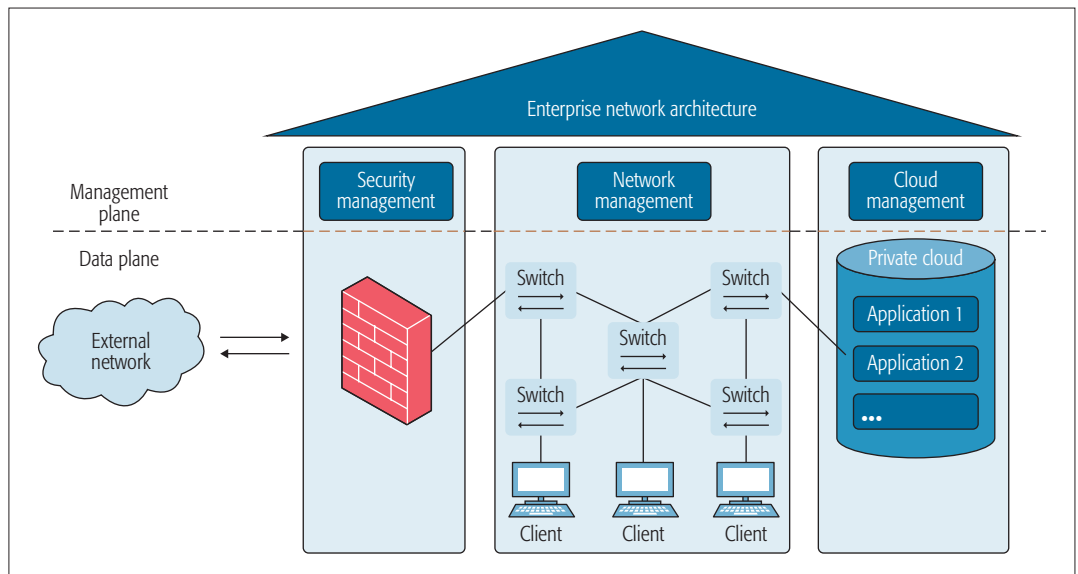


Figure 1. Traditional enterprise network architecture.

By analogy with the NMS, the CMS plays a similar role with the distinction of having its focus set on the private cloud environment of the enterprise network. Hence, the main liabilities of the CMS reside in provisioning, configuring, and monitoring of (virtual) servers and services deployed in the local cloud environment.

To address security concerns and to provide a holistic security strategy, the SMS is deployed in addition to the NMS and CMS. Its broad spectrum of tasks ranges from managing virtual private networks (VPNs) to the provisioning of public key infrastructures. Having the core task of supporting the enforcement of the enterprise's security strategy, a key feature of the SMS is the ability to define and establish these policies within the network infrastructure.

As illustrated in Fig. 1, the different management systems are loosely coupled. While the NMS and the CMS exchange runtime data and may utilize each other's services, the SMS remains rather isolated. This circumstance stems from the *need-to-know* principle that helps prevent the leakage of information useful to an attacker. The physical deployment of security middleboxes, such as the PGF located at network borders, allows the SMS to remain independent from the other management systems. A tighter integration of the SMS with these systems, for instance by providing monitoring information, could enhance the overall operation. Similar efforts have already been conducted for CMS and NMS. In order to satisfy the demands of new services and applications, network and cloud orchestration have been integrated in the evolving service-based architecture. Therefore, it is expected that the isolated operation of all management systems will no longer be possible in the near future.

Although this architecture has proven to provide functional management of the network infrastructure, it also imposes several shortcomings such as scalability issues and an increased management overhead. To mitigate these effects, we propose an enhanced enterprise network architecture based on SDN and NFV, which is described in detail within the next section.

INTEGRATION AND ADVANTAGES OF SDN/NFV-BASED SECURITY SYSTEMS

Figure 2 shows an SDN/NFV-enhanced enterprise network architecture. Whereas NFV enables the operation of network nodes such as load balancers and firewalls as virtualized entities, SDN decouples the data plane from the control plane. Packet forwarding (data plane) is handled by SDN switches, while the SDN controller implements the control plane and decides about traffic forwarding. The SDN controller runs as software on server hardware and provides a central interface to the network, thus offering enhanced monitoring capabilities in addition to the possibility of dynamic packet re-routing and manipulation.

Due to its central role, the SDN controller has to interact with all the other management systems. For instance, it interacts with the NMS and CMS when provisioning network connectivity and, vice versa, the NMS and CMS rely on vital network statistics conducted by the controller. In addition, the SMS needs to interact with the controller to enforce the security policy. Thus, the classical requirements of the SMS are widened to ensure the security of the virtualized entities initiated by the CMS and the SDN controller. Hence, the SMS must have control over all security related aspects of the intended operation, and therefore suitable interfaces to supervise the secure execution of these processes must be provided to the SMS.

Enhanced scalability. One advantage of following this approach is the possibility to easily scale the deployed security systems according to the network load. In contrast to today's security systems, which are often implemented in costly middlebox appliances and deployed in a physical stationary position, virtualized network functions run on commercial-off-the-shelf (COTS) servers and can be instantiated or migrated with relative ease. In particular, traffic spikes can be managed by dynamically deploying additional instances of the stressed system and, once the load has returned to normal thresholds, these instances can be discarded. Therefore, a more cost efficient resource allocation can be achieved, which in return results in lower operating and acquisition costs.

Finer granularity. In addition, enterprises often introduce a separation of duties to their divisions, which is also reflected in their security policy, such as access to human resource data is limited only to a specific group of people. In today's networks, this can be achieved on the network level through physical separation or coarse-grained logical separation using VLANs, as well as through access control mechanisms on the application layer. With its fine grained flow handling, SDN offers the means to dynamically define virtual networks imposed by the security policy. Each virtual network mirrors a security clearance and denies unauthenticated access. This mechanism may also be used to implement a solid policy for use cases such as bring your own device (BYOD) [6], as it makes it possible to lock a formerly unknown device into its very own virtual network with minimal access to the enterprise network. After successful authentication, its virtual network is updated to correspond to the user's security clearance and network access to further services through the means of SDN and NFV.

Flexible service chaining. Depending on the requirements imposed by the overall security policy, NFV makes it possible to chain different security measures in a service oriented manner. For instance, parts of the traffic can be dynamically routed through a firewall, then through an intrusion detection system and finally through a function performing a virus scan. With this flexibility, a solution can be created that is tailored to the needs of the enterprise, as additional services can be inserted or removed at any arbitrary position within the forwarding graph [5]. Furthermore, this decision can be made on a per-flow basis, and thus provides advantages over statically wired classical networks.

Improved firewalling. Firewalling can be regarded as one of the most challenging aspects of the security enforcement, as it involves an active intervention into the end-to-end semantics of communications. In particular, more advanced filtering techniques such as stateful firewalling typically lack hardware support, preventing security enforcement at line rate. Yet, the use of hardware for the less advanced but common stateless firewalling in appliances is quite costly, due to the complex development cycle of specialized hardware. Today, many SDN controllers have firewalling applications included, which leverage the ability of the SDN switches to drop or forward flows. This allows for mimicking the behavior of a typical stateless firewall. In this context, the integrated forwarding tables are used as a hardware accelerator and hence establish the first step to a cost effective and solid field firewall that relies on SDN principles and COTS hardware.

In the next section, we discuss multiple approaches based on the previously described SDN/NFV-enabled architecture to achieve a more advanced, scalable, and cost effective security policy enforcement in enterprise networks featuring stateful firewalls.

USE CASE: STATEFUL FIREWALLING

In this section, we propose three different approaches to implement stateful firewalls with SDN and NFV, as shown in Fig. 3. The majority of previous work regarding novice firewall imple-

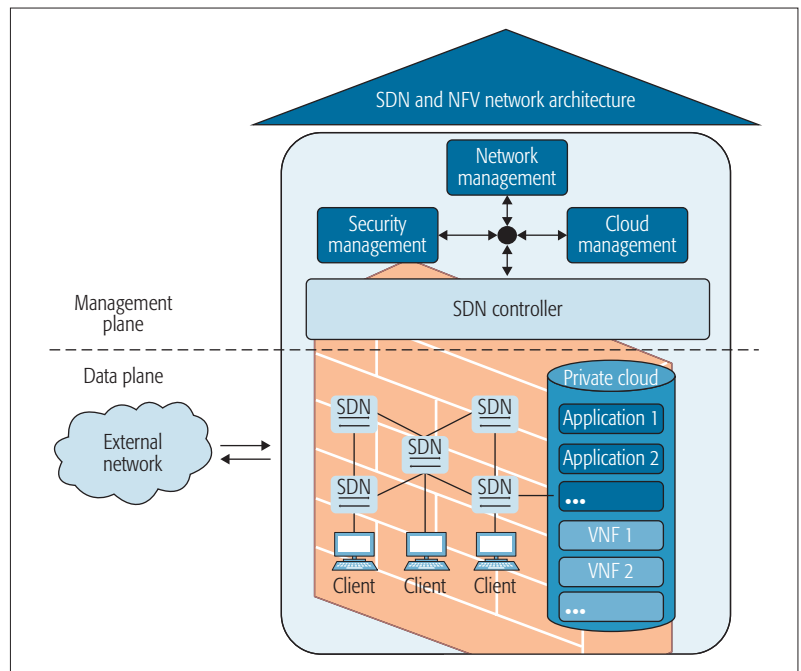


Figure 2. SDN and NFV enhanced network architecture.

mentations either completely relies on the programmability of SDN devices, or implements the firewall functionality entirely in software. Yet, most approaches are limited to stateless firewalling, meaning that a fixed set of rules allows a packet to either pass or to get dropped.

In contrast, this work proposes a hybrid approach to implement a comprehensive, stateful firewalling concept. This includes not only that a permitted egress connection results in incoming response packets being passed, but also that the state of the connection conforms to the protocol, i.e. initiated by a TCP three-way handshake. In the following sections, we detail how challenging the tracking of the connection state in regards to the protocol's state machine can be, and how this impacts the performance of different implementation approaches. Table 1 gives an overview of advantages and drawbacks of these different approaches and a comparison to classical PGF appliances. It can be seen that the hybrid approach combines the advantages of the controller-centric, SDN-based approach and the VNF-centric approach, which implements functionality in software. In contrast to a classical PGF, the proposed implementation offers better scalability and more flexibility. In general, any network function consists of parts that can be categorized as control plane functionality, e.g., the connection state, and other parts that can be grouped as data plane functionality. In the case of a firewall this is the forwarding of packets. In this context, the presented approaches differ significantly in how the data plane and control plane are constituted.

CONTROLLER-CENTRIC APPROACH

The basic idea of the controller-centric approach is to use the means of SDN switches for implementing the data plane firewall functionality. In an SDN-enabled network, packets that should not be forwarded can be dropped directly inside the switches by defining flow rules matching the cor-

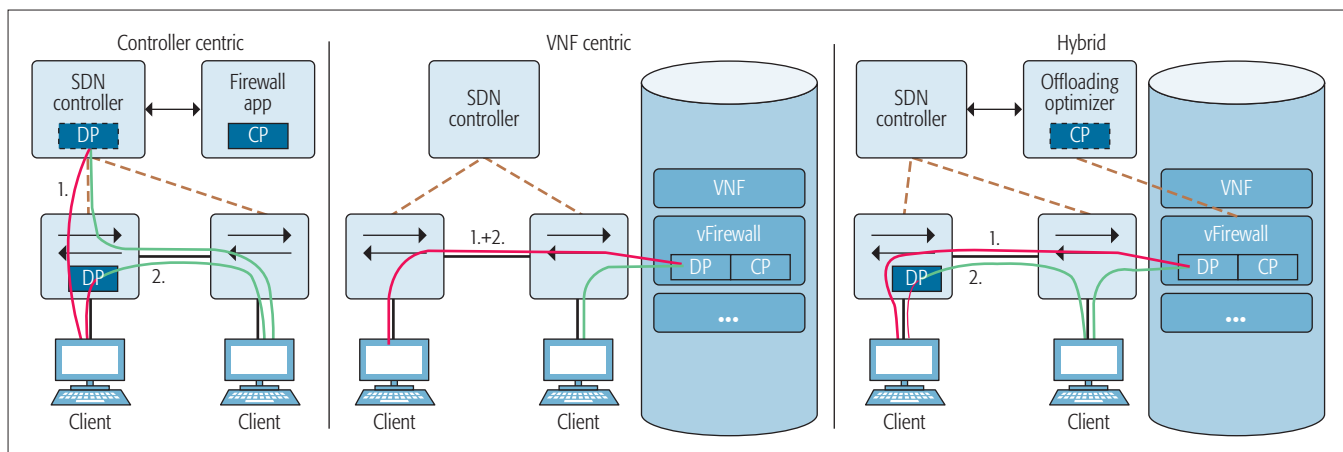


Figure 3. Three approaches implementing stateful firewalling with NFV and SDN.

responding flows. Consequently, stateless firewalls are integrated in SDN controller software such as Floodlight or FlowGuard [7]. As the actual state of the connections cannot be tracked within the switches, such control plane logic has to be implemented in the controller software. Therefore, the switches are instructed to send unknown traffic through their control channel to the controller, which also holds all security policies that should be applied. As soon as the control plane firewall function decides to forward a packet, it is sent back to the switch along with adequate information such as which interface the packet should be emitted. This detour through the controller is taken until the connection is established (Path 1 in Fig. 3). Afterward, the controller installs appropriate rules on the switch that match the relevant header fields of this specific connection, i.e. the TCP five tuple. From this point on, the forwarding is handled by the switch hardware and can happen at line rate (Path 2 in Fig. 3). Hence, there is no need for further involvement of the controller. Finally, the flow table entry will automatically be discarded, once the connection is inactive for a specified time.

The most significant drawback of this approach is the high latency during connection establishment caused by the interaction between the data plane and the control plane through the slow control channel. Further, the load on the SDN controller is increased by taking over the data plane firewall functionality during the connection setup. Even though modern controller implementations can run as a cluster and scale out with increasing load, overloading the controller with more and more network functions has to be avoided. Another problem is the very limited space within the hardware flow tables of switches, which is described later in detail.

VNF-CENTRIC APPROACH

To mitigate limited scalability and high latency, the virtualized network functions (VNFs) approach relies on virtualized firewalls that are deployed in a cloud environment. For this, all traffic is diverted to the firewall VNF, which implements tracking of the connection state as well as filtering and traffic forwarding. Therefore, the control plane (CP) and the data plane (DP) of the firewall are united in one entity, which is similar to legacy firewall

appliances. As a consequence, all traffic (1+2) is routed via the VNF as shown in Fig. 3.

Software-based firewalls already existed on the market before the introduction of the NFV concept and are available as commercial products as well as open source software, including Cisco's ASA and pfSense or IPFire. These products are not in line with the NFV concept, as they lack the ability to scale out and instead only operate in active/passive setups, where one instance handles all traffic. Firewall implementations following the VNF model [4] and utilizing mechanisms of cloud applications illustrate the benefits of NFV in terms of scalability and reliability compared to traditional deployment models. Further, the softwarization of network functions enables a scenario-tailored deployment of instances and function blocks on the available COTS hardware. For the discussed firewall use case, advanced filtering capabilities can be implemented and incorporated by intrusion-detection software and application-layer firewalls.

The downside of a VNF implementation is the limited throughput per instance, as all processing happens in software. Additionally, the virtualization overhead and resource sharing inside the physical system result in scheduling delays, which increase forwarding delays. A multitude of optimization techniques [1] are available to increase both throughput and delays of VNF running on general purpose hardware, but without reaching the performance of appliances based on application-specific integrated circuits (ASICs). The additional detour of the traffic passing through the firewall can have an even bigger influence when all communication is routed to a VNF running multiple hops away in the data center. At this point, special emphasis has to be put on the function placement [10], in order to avoid lengthening of traffic paths, which results in a service degradation. Finally, the distributed nature of multiple stateful firewall instances requires mechanisms to synchronize necessary state information, for instance all established connections.

HYBRID SDN/NFV APPROACH

To overcome the drawbacks of the previous approaches, we suggest a hybrid solution that introduces a strategy to offload bandwidth-intense connections to the SDN switching hardware. This

Approach	Description	Pro	Contra
Controller-centric	Handshake handled by the controller.	<ul style="list-style-type: none"> Follows SDN principles High throughput for established connections 	<ul style="list-style-type: none"> High latency during connection setup Does not scale well
VNF-centric	All traffic is diverted via firewall VNFs.	<ul style="list-style-type: none"> Low latency during connection setup Good scalability and reliability Possibility for application-level filtering 	<ul style="list-style-type: none"> Limited throughput per instance Higher resource usage through multiplication of traffic
Hybrid	VNF-centric for connection setup. Controller-centric for long lasting and data intensive connections.	<ul style="list-style-type: none"> Good scalability Low latency High throughput 	<ul style="list-style-type: none"> High complexity Application-layer filtering not for all connections
Classical PGF appliance	An appliance is placed between two networks and all traffic flows through it.	<ul style="list-style-type: none"> Physical placement enforces filtering of all traffic flowing between two networks High ability for self defense possible Application layer filtering for all connections 	<ul style="list-style-type: none"> Can hardly handle virtual networks due to physical placement Very high costs per instance Limited throughput per instance Does not scale well

Table 1. Advantages and drawbacks of different stateful SDN/NFV firewalling approaches and classical PGF appliances.

results in multiple data and control plane instances: the hybrid approach uses the switch hardware as the data plane, while the still existing VNF keeps both the control state and the forwarding functionality.

At first, all traffic is redirected to firewall VNFs running in the local cloud infrastructure (Path 1 in Fig. 3). Any VNF is solely responsible for connection establishment, which results in reduced initial latency compared to the controller-centric approach. The VNF will ensure the accordance of the connection with the security rules, the protocol, and optionally even with the application layer headers.

Once the connection is persistent it may be offloaded in a second step by installing forwarding rules in the switches, and thus the switch is used as firewall data plane (Path 2 in Fig. 3). This decision is undertaken by an optimizer that keeps track of all active connections held by the VNF, and therefore implements the control plane functionality. If an offloading decision for a certain flow is made, consecutive packets of this flow can be directly forwarded through the networking hardware, instead of detouring through the VNF. The advantage is a lower latency, a potentially higher throughput of the traffic flow, as well as a lower resource consumption by the VNF. Good candidates for offloading are all traffic flows that are known to be long lasting and data intensive, such as large file transfers. In contrast, short-lived flows, such as DNS requests, might never be offloaded to the hardware.

Therefore, the hybrid approach combines good scalability with low latency for initial and consecutive packets and a high throughput. On the one hand, resources are preserved both in the flow tables of switching hardware, as well as in the computing infrastructure. On the other hand, the hybrid approach is clearly more complex to implement and to monitor, as the combination of two distinct systems complicates development and operation. This is exacerbated by the necessity to implement state synchronization mechanisms similar to the ones discussed for the VNF-based approach.

To summarize, Table 2 compares the three approaches regarding where the particular functionality resides. It shows that the beneficial performance behavior of the VNF-centric approach

Approach	State tracking	Connection setup	Filtering decision
Controller-centric	Controller	CP (software)	DP (hardware)
VNF-centric	VNF	DP (software)	DP (software)
Hybrid	VNF and optimizer	DP (software)	DP (software/hardware)

Table 2. Placement patterns for different parts of the firewalling functionality.

and the hybrid approach stem from keeping state tracking and connection setup in the data plane and thus, locally. When offloading connections, the hybrid approach propagates the filtering decision to the switching hardware, which reduces the overall workload drastically. This helps keep the amount of required VNF instances to handle the overall traffic low and therefore helps to increase resource efficiency.

CHALLENGES FOR SDN/NFV-BASED FIREWALLING

Despite these advantages, a novel network security architecture also imposes new challenges that need to be taken into account before deployment. As no perimeter firewall is deployed in the presented approach, network security mainly relies on the SDN infrastructure. Due to its central role, the control plane is key to the security of the complete network. On the other hand, the fine granularity introduced with this concept leads to more traffic being filtered by the firewall and thus additional load. In the following, we will discuss the implications on both security and performance and summarize potential solutions.

CONTROL PLANE SECURITY

With the introduction of the SDN controller as a new critical component, as well as the APIs offered by switches, new threat vectors are imposed. Hence, if an attacker gains access to the controller the entire network is compromised. Further, controller software projects are based on a large code basis, and as with every feature-rich software, vulnerabilities in the control framework itself are probable. This can be mitigated by proper quality assurance mechanisms as incorporated in most larger software projects.

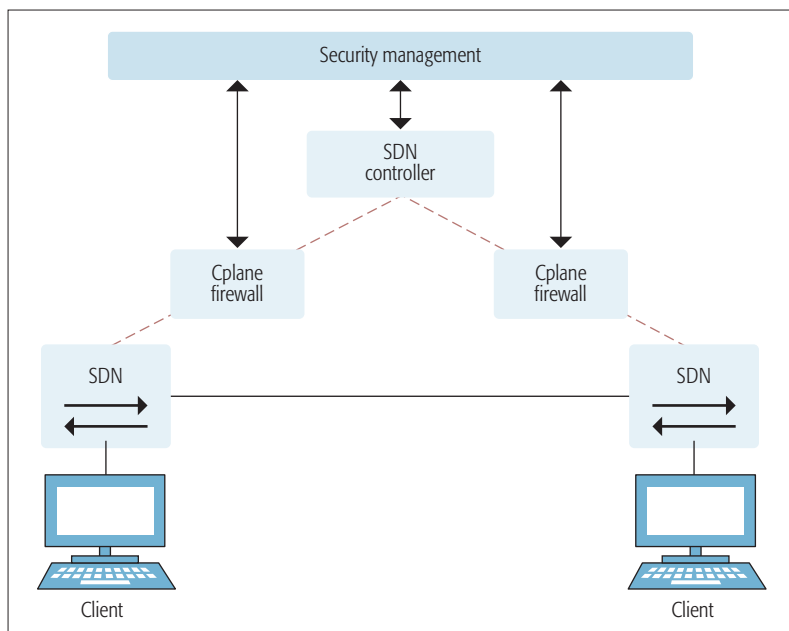


Figure 4. Control plane firewall implemented as southbound connection proxy.

Vulnerabilities residing in SDN applications that influence the controller behavior and either run as a controller plug-in or communicate with the SDN controller impose a threat to the network, as these APIs usually allow the controller to alter the state of the network. Hence, a proper authentication and authorization management for such SDN applications is mandatory. Current controller software lacks access restrictions allowing the limitation of access to the controller's API.

Furthermore, conventional firewall access rules that either deny or grant access for certain flows based on their packet headers are no longer sufficient. Whereas these rules are sufficient in classical networks, they can be circumvented if SDN-enabled devices dynamically rewrite packet headers to cross security boundaries. FortNox [12] is the first publication describing this problem and offers a possible solution: an SDN controller kernel validates all requests coming from SDN applications against defined security policies and keeps track of all existing rules in the SDN switches. However, this solution requires massive changes to existing control plane software frameworks and continuous work to keep track of their ongoing development.

The communication between switches and controllers opens another vector to a potential attacker. Related work [2] reports eavesdropping or denial of service attacks. As these kinds of attacks cannot be sensed at the control plane level, security improvements to the controllers fail to detect them. To mitigate this threat, a crucial security measure is the activation of encryption mechanisms for the controller switch connections including mutual authentication.

Another possible solution for detecting malicious rules is a control plane firewall placed between the controller and the switches. Figure 4 shows the logical placement of such a firewall.

This lightweight proxy instance can be positioned within the southbound communication of the controller and the switches, and therefore provides direct access to the network state as

well as the forwarding hardware to the SMS. The intermediate placement requires a change of the end-to-end semantics of the controller to switch relation. The control plane firewall can be regarded as a secure endpoint of the control plane connections.

The placement in the control connection enables the firewall to detect and prevent the circumvention of security restrictions by rogue controllers or hostile switches. In addition, this control plane firewall can protect from dangers originating from the data plane, and also check the instructions that the controller forwarded initiated by calls to the controller's northbound API. Together with the SMS as a centralized entity, a security cage is established around the SDN controller and therefore provides the necessary network-wide flow validation.

PERFORMANCE LIMITATIONS

Adjacent to the described security considerations, the proposed architecture also imposes performance challenges. Briefly approached earlier, these challenges are described in this section in more detail. In general, SDN is assumed to improve network performance and utilization, as packet processing is done in hardware by the switches that can offer further features, such as load-balancing and network virtualization based on the controller's instructions. Yet the amount of space in the flow tables is limited and differs from model to model. This diversity in SDN hardware also causes other problems, including differing forwarding delays as shown in [11]. In particular, a firewall relying on 5-tuple rules to be installed in the switches can therefore restrict the scalability of such implementations. To overcome this issue, a careful aggregation or a clever use of these resources is necessary. A related issue are delays originating from the control plane to data plane interaction. The authors in [9] show that the flow setup rate in an SDN environment is limited to less than one rule per ms. In particular, the hybrid approach presented earlier can be a relief, as only a limited number of flows is installed in the hardware forwarding table. Thus, the offloading decision is a major challenge with this approach. A simple solution could be to offload flows after a fixed duration or based on implicit knowledge of the applications in the enterprise environment. Nevertheless, limited resources in switches and for the VNF must be kept in mind, and therefore load balancing between the VNF and the switch may be a viable solution. As of this writing, no research results have been presented regarding this problem.

Another challenge that can be identified is the limited support for higher layers in SDN hardware. In contrast with most network functions such as load balancers, a modern application-layer firewall examines different flows very carefully and even filters content, such as HTTP traffic. As these functionalities are implemented in software, this requires large multi-purpose computing capabilities that are not provided by current network hardware (switches and routers), and thus the implementation of an advanced stateful firewall supporting application-layer filtering based solely on SDN is a difficult undertaking. On the other hand, in combination with NFV, which can be used for stateful

and application-layer filtering, an increase in flexibility and cost efficiency is expected.

CONCLUSION

Facing a constant increase of threat vectors, deploying and maintaining secure enterprise networks is becoming increasingly challenging and costly. As today's security mechanisms are often tightly integrated into the physical network infrastructure, the implementation of a dynamic resource allocation based on current network characteristics such as the load is a difficult undertaking. To provide greater flexibility and reduce operational costs, security mechanisms based on SDN and NFV have been proposed by the research community.

In this work, we summarize how a traditional enterprise network architecture can be extended to incorporate the concepts of SDN and NFV. Furthermore, we outline the main benefits of this approach. Taking stateful firewalling as example, we illustrate three potential design patterns for the implementation: controller-centric, VNF-centric, and hybrid approach. By discussing the pros and cons of each design pattern, we provide an overview, which can be used as a guideline for the development and possible integration of SDN and NFV appliances into current enterprise networks.

Despite the improved scalability and flexibility provided by an SDN and NFV enabled network, new challenges are imposed that need to be taken into account. In this context, we see the additional security considerations, which are introduced by the new SDN components and their possible performance limitations, as the most pressing concerns. Yet we are convinced that the advantages provided by SDN and NFV outweigh the disadvantages, and that the additional challenges can be tackled by further research in the following years.

ACKNOWLEDGMENTS

This work has been performed in the framework of the SarDiNe project, and is partly funded by the German Federal Ministry of Education and Research (BMBF). The authors alone are responsible for the content of the article.

REFERENCES

- [1] T. Barbette, C. Soldani, and L. Mathy, "Fast Userspace Packet Processing," *Proc. 11th ACM/IEEE Symp. Architectures for Networking and Communications Systems, ANCS '15*, Washington, DC, USA, 2015, pp. 5–16.
- [2] K. Benton, L. J. Camp, and C. Small, "OpenFlow Vulnerability Assessment Categories and Subject Descriptors," 2013, pp. 151–52.
- [3] M. Casado et al., "Ethane: Taking Control of the Enterprise," *ACM SIGCOMM Comp. Commun. Rev.*, vol. 37, ACM, 2007, pp. 1–12.
- [4] J. Deng et al., "VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Routers," *2015 IEEE Conf. Network Function Virtualization and Software Defined Network (NFV-SDN)*, 2015, pp. 107–114.
- [5] ETSI ISG NFV. Network Functions Virtualisation (NFV): Architectural Framework, RGS/NFV-002, V1.2.1, 2014.
- [6] S. Gebert et al., "Demonstrating a Personalized Secure-By-Default Bring Your Own Device Solution Based on Software Dened Networking," *28th Int'l. Teletrac Congress (ITC)*, Würzburg, Germany, Sept. 2016.
- [7] H. Hu et al., "FlowGuard: Building Robust Firewalls for Software-Dened Networks," *Proc. 3rd Wksp. Hot Topics in Software Dened Networking – HotSDN '14*, 2014, pp. 97–102.
- [8] M. Jarschel et al., "Interfaces, Attributes, and Use Cases: A Compass for SDN," *IEEE Commun. Mag.*, vol. 52, no. 6, June 2014, pp. 210–17.

- [9] M. Kuzniar, P. Peresni, and D. Kostic, "What You Need to Know About SDN Flow Tables," *Passive and Active Measurement*, Springer, 2015, pp. 347–59.
- [10] S. Lange et al., "Heuristic Approaches to the Controller Placement Problem in Large Scale SDN Networks," *IEEE Trans. Network and Service Management*, vol. 12, no. 1, Mar. 2015, pp. 4–17.
- [11] A. Lazaris et al., "Tango: Simplifying SDN Control with Automatic Switch Property Inference, Abstraction, and Optimization," *Proc. 10th ACM Int'l. Conf. Emerging Networking Experiments and Technologies*, ACM, 2014, pp. 199–212.
- [12] P. Porras et al., "A Security Enforcement Kernel for Open-Flow Networks," *Proc. 1st Wksp. Hot topics in Software Dened Networks – HotSDN '12*, 2012, pp. 121–26.

BIOGRAPHIES

CLAAS LORENZ (claas.lorenz@genua.de) is a security researcher at genua GmbH in Kirchheim, Germany. He received his master's degree in computer science from the University of Potsdam, where he is working on his Ph.D. thesis. His research interests include firewalling, SDN/NFV, and formal security verification. Since 2015 he has worked for the German network security specialist genua GmbH in the SarDiNe project, which is funded by the German Ministry of Education and Research (BMBF).

DAVID HOCK (hock@infosim.net) is a senior consultant for research and development at Infosim GmbH & Co. KG, and is coordinating Infosim's research activities. Previously he worked as a research assistant at the Chair of Communication Networks at the Institute of Computer Science Würzburg, where he finished his Dr. rer. nat. degree in 2014. His current main research interests are in the unified network and services management of mixed SDN/NFV, IoT, and legacy infrastructures.

JOHANN SCHERER (scherer@infosim.net) is a senior developer at Infosim GmbH & Co. KG in Würzburg, Germany. Prior to his work at Infosim, he studied at the University of Würzburg, where he received his master degree in 2014. His current research interests include network management and SDN/NFV integration.

RAPHAEL DURNER (r.durner@tum.de) is Ph.D. student at Technical University of Munich, Germany, where he also received his master's degree in 2014. His research interests include hybrid SDN/NFV approaches and security in SDN.

WOLFGANG KELLERER [M'96, SM'11] (wolfgang.kellerer@tum.de) is a full professor with the Technical University of Munich, heading the Chair of Communication Networks with the Department of Electrical and Computer Engineering. Previously, for more than ten years he was with NTT DOCOMO's European Research Laboratories. He currently serves as an associate editor for *IEEE Transactions on Network and Service Management* and on the editorial board of *IEEE Communications Surveys and Tutorials*.

STEFFEN GEBERT (stefen.gebert@informatik.uni-wuerzburg.de) is working toward his Ph.D. at the University of Würzburg, Germany, where he also received his diploma degree in 2011. His research interests include software-defined networks and agile network operations.

NICHOLAS GRAY (nicholas.gray@informatik.uni-wuerzburg.de) is a Ph.D. student at the University of Würzburg, Germany, where he also completed his master's thesis in 2015. His research interests include SDN/NFV architectures and their impact on network security.

THOMAS ZINNER (zinner@informatik.uni-wuerzburg.de) received his diploma and Ph.D. degrees in computer science from the University of Würzburg, Germany, in 2007 and 2012, respectively. He is heading the research group on "Next Generation Networks" at the Chair of Communication Networks, University of Würzburg. His main research interests are video streaming techniques, implementation of QoE awareness within networks, software defined networking (SDN), and network function virtualization, as well as the performance assessment of these technologies and architectures.

PHUOC TRAN-GIA (trangia@informatik.uni-wuerzburg.de) is a professor and director of the Chair of Communication Networks, University of Würzburg, Germany. He is also a member of the Advisory Board of Infosim (Germany), specializing in IP network management products and services. He has published more than 100 research papers in major conferences and journals. He was a recipient of the Fred W. Ellersick Prize in 2013 from the IEEE Communications Society.

We see the additional security considerations, which are introduced by the new SDN components and their possible performance limitations, as the most pressing concerns. Yet we are convinced that the advantages provided by SDN and NFV outweigh the disadvantages, and that the additional challenges can be tackled by further research in the following years.

ADVERTISING SALES OFFICES

Closing date for space reservation: 15th of the month prior to date of issue

NATIONAL SALES OFFICE

Mark David
Sr. Manager Advertising & Business Development
EMAIL: m.david@ieee.org

NORTHERN CALIFORNIA

George Roman
TEL: (702) 515-7247
FAX: (702) 515-7248
EMAIL: George@George.RomanMedia.com

SOUTHERN CALIFORNIA

Marshall Rubin
TEL: (818) 888 2407
FAX: (818) 888-4907
EMAIL: mr.ieeemediamedia@ieee.org

MID-ATLANTIC

Dawn Becker
TEL: (732) 772-0160
FAX: (732) 772-0164
EMAIL: db.ieeemediamedia@ieee.org

NORTHEAST

Merrie Lynch
TEL: (617) 357-8190
FAX: (617) 357-8194
EMAIL: Merrie.Lynch@celsociates2.com

Jody Estabrook

TEL: (77) 283-4528
FAX: (774) 283-4527
EMAIL: je.ieeemediamedia@ieee.org

SOUTHEAST

Scott Rickles
TEL: (770) 664-4567
FAX: (770) 740-1399
EMAIL: srickles@aol.com

MIDWEST/CENTRAL CANADA

Dave Jones
TEL: (708) 442-5633
FAX: (708) 442-7620
EMAIL: dj.ieeemediamedia@ieee.org

MIDWEST/ONTARIO, CANADA

Will Hamilton
TEL: (269) 381-2156
FAX: (269) 381-2556
EMAIL: wh.ieeemediamedia@ieee.org

TEXAS

Ben Skidmore
TEL: (972) 587-9064
FAX: (972) 692-8138
EMAIL: ben@partnerspr.com

EUROPE

Christian Hoelscher
TEL: +49 (0) 89 95002778
FAX: +49 (0) 89 95002779
EMAIL: Christian.Hoelscher@husonmedia.com

COMPANY	PAGE
IEEE ComSoc Membership.....	29
IEEE GLOBECOM.....	75
IEEE Sales and Marketing.....	Cover 3
IEEE WCET	145
IEEE Xplore	Cover 2
National Instruments	Cover 4
SoftCOM	11
Spectrum Enterprise.....	3
Tetcos.....	6

CURRENTLY SCHEDULED TOPICS

TOPIC	ISSUE DATE	MANUSCRIPT DUE DATE
HUMAN-DRIVEN EDGE COMPUTING AND COMMUNICATION	NOVEMBER 2017	APRIL 1, 2017
EDUCATION & TRAINING: SCHOLARSHIP OF TEACHING AND SUPERVISION	NOVEMBER 2017	MAY 1, 2017
EMERGING TRENDS, ISSUES AND CHALLENGES IN BIG DATA AND ITS IMPLEMENTATION TOWARDS FUTURE SMART CITIES	DECEMBER 2017	APRIL 1, 2017
HETEROGENEOUS ULTRA DENSE NETWORKS	DECEMBER 2017	MAY 15, 2017
AMATEUR DRONE SURVEILLANCE: APPLICATIONS, ARCHITECTURES, ENABLING TECHNOLOGIES, AND PUBLIC SAFETY ISSUES	JANUARY 2018	MAY 1, 2017

www.comsoc.org/commag/call-for-papers

TOPICS PLANNED FOR THE APRIL ISSUE

- FOG COMPUTING AND NETWORKING
- DESIGN AND IMPLEMENTATION
- INTEGRATED CIRCUITS FOR COMMUNICATIONS
- SDN USE CASES FOR SERVICE PROVIDER NETWORKS



Instant Access to IEEE Publications

Enhance your IEEE print subscription with online access to the IEEE Xplore® digital library.

- Download papers the day they are published
- Discover related content in IEEE Xplore
- Significant savings over print with an online institutional subscription

Start today to maximize your research potential.

Contact: onlinesupport@ieee.org
www.ieee.org/digitalsubscriptions

"IEEE is the umbrella that allows us all to stay current with technology trends."

Dr. Mathukumalli Vidyasagar
Head, Bioengineering Dept.
University of Texas, Dallas



 **IEEE**
Advancing Technology
for Humanity

INNOVATE FASTER

WITH FIELD-DEPLOYED 5G PROOF-OF-CONCEPT SYSTEMS

In the race to design next-generation wireless technologies, research teams must rely on platforms and tools that accelerate their productivity. Using the NI software defined radio platform and LabVIEW Communications, leading researchers are innovating faster and building 5G proof-of-concept systems to demonstrate new technologies first.

Accelerate your innovation at ni.com/5g



LabVIEW Communications System Design Software, USRP-2943R SDR Hardware

