IEEE NETWORK®
THE MAGAZINE OF GLOBAL INTERNETWORKING

Director of Magazines
Raouf Boutaba, University of Waterloo, Canada

Editor-in-Chief
Nei Kato, Tohoku University, Japan

Associate Editor-in-Chief
David Soldani, Huawei Technologies, Germany

Senior Technical Editors
Sherman Shen, University of Waterloo, Canada

Technical Editors
Nirwan Ansari, New Jersey Institute of Tech, USA
Igor Bisio, Univ. of Genoa, Italy
Lin Cai, Huawei Technologies, USA
Jiannong Cao, Poly. Univ., HK
Shanzhi Chen, Datang Telecom Technology & Industry Group, China
Yingying Chen, Stevens Institute of Tech., USA
Mianxiong Dong, Muroran Institute of Tech., Japan
Zubair Md. Fadlullah, Tohoku University, Japan
Yuguang Fang, Univ. of Florida, USA
Mohsen Guizani, Qatar Univ., Qatar
Phone Lin, National Taiwan University, Taiwan
Xiaodong Lin, OUIT, Canada
Ying-Dar Lin, National Chiao Tung Univ., Taiwan
Jiajia Liu, Xidian University, China
Pascal Lorenz, University of Haute Alsace, France
Jelena Misic, Ryerson Univ., Canada
Zhiguo Shi, Zhejiang Univ., China
Ness Shroff, OSU, USA
Anwar Walid, Bell Labs Research, Alcatel-Lucent, USA
Murtaza Zafer, IBM T. J. Watson Research Center, USA
Junshan Zhang, Arizona State Univ., USA

Feature Editors
"New Books and Multimedia"
Yu Cheng, IIT, USA

IEEE Production Staff
Joseph Milizzo, Assistant Publisher
Susan Lange, Online Production Manager
Jennifer Porcello, Production Specialist
Catherine Kemelmacher, Associate Editor

2016 IEEE Communications Society Officers
Harvey A. Freeman, *President*
Luigi Fratta, *VP–Technical Activities*
Guoliang Xue, *VP–Conferences*
Stefano Bregni, *VP–Member Relations*
Nelson Fonseca, *VP–Publications*
Rob Fish, *VP-Standards Activities*
Sergio Benedetto, *Past President*

Board of Governors
The officers above plus Members-at-Large:
Class of 2016
Sonia Aissa, Hsiao Hwa Chen
Nei Kato, Xuemin Shen
Class of 2017
Gerhard Fettweis, Araceli Garciá Gómez
Steve Gorshe, James Hong
Class of 2018
Leonard J. Cimini, Tom Hou
Robert Schober, Qian Zhang

2016 IEEE Officers
Barry L. Shoop, *President*
Karen Bartleson, *President-Elect*
Parviz Famouri, *Secretary*
Jerry L. Hudgins, *Treasurer*
Howard E. Michel, *Past-President*
E. James Prendergast, *Executive Director*
Celia Desmond, *Director, Division III*

IEEE ComSoc
IEEE Communications Society

EDITOR'S NOTE

On 5G Wireless Systems

Nei Kato

I would like to extend my warmest wishes to you all. The year 2016 will bring about more changes to beyond 4G wireless systems and expedite the 5G vision. Therefore, the first Editor's Note of the year is dedicated to 5G mobile communication, which is a highly promising research area in terms of both theory and practice. Although its initial commercialization is anticipated to be some time in 2020, the race for 5G is intensifying, and it is essential to discuss the trends, challenges, and barriers influencing the 5G evolution.

As with its predecessor, 5G is likely to emerge not all at once but in a series of incremental enhancements. A plethora of promising techniques have already been proposed to meet the 5G standard and its key requirements that include a peak rate of 20 Gb/s, an actual end-user rate of 100 to 1000 Mb/s, a 100-fold improvement in network-wide energy efficiency, a 3-fold improvement in spectrum efficiency, and so forth. While the capabilities of these future mobile networks are indeed exciting, it is important to identify the technical challenges that could impede the achievement of the actual capabilities.

5G is supposed to meet the diverse and stringent requirements of future mobile broadband users. In this vein, massive multiple-input multiple-output (MIMO) and 3D MIMO to allow high-resolution beamforming at higher frequencies are interesting techniques currently considered for the upcoming 5G systems. New channel models, channel estimation/feedback, fast processing algorithms, and pilot contamination workaround are required for these large-scale MIMO technologies to deliver their expected high performance.

By following the current roadmaps to the 5G vision, I feel that 5G is evolving into a system solution that combines several radio access technologies. As existing mobile broadband technologies like high-speed packet access (HSPA) and Long Term Evolution (LTE) continue to evolve, they will form the backbone of the overall radio access solution beyond 2020. At the same time, it is important to consider how new complementary radio access technologies for specific scenarios may develop. For instance, the space diversity strategy involving heterogeneous networks (HetNets) is now an anticipated evolution for increasing wireless capability, while the cloud radio access network (C-RAN) paradigm deals with increased complexity and interference issues. Therefore, improving the radio access technologies for 5G could be a worthy research topic, including issues such as inter-cell interference alignment, distributed interference coordination, efficient medium access control, device discovery and link setup, and so on.

One of the specific scenarios of 5G is ultra-dense deployments through which the distance between network access nodes will be significantly small (perhaps a few meters) to meet extreme capacity requirements. In such a case, direct device-to-device (D2D) communication holds great promise. If the network can manage or control the D2D traffic in licensed spectrum, it is possible to provide reliable communication services. This area requires a lot more research effort in order to make the most of its enormous potential.

Network energy efficiency will be an important challenge in 5G. Reduced link distances in ultra-dense network deployments, smart functionalities for node sleep, and minimization of signaling for network detection and synchronization are critical aspects that need to be thoroughly considered to facilitate energy-efficient 5G networks.

In contrast to single-purpose wireless systems, 5G is anticipated to provide a myriad of services for an ever growing number of heterogeneous networked devices (or so called machines) capable of communicating with one another. In other words, the Internet of Things (IoT) and large-scale machine-to-machine (M2M) communication will exploit 5G wireless systems. This will surely put many diverse requirements on the network in terms of energy consumption, device cost, latency, reliability, and so forth.

Big data is another area that can lead to both challenges and opportunities of 5G wireless systems. The above-mentioned IoT and M2M applications will generate a huge volume of data, posing a major technical challenge to the radio access networks. Software defined networking (SDN) and network function virtualization (NFV) are emerging from the necessity of running big data applications, and they have a close synergy with cloud computing. These technologies will, at some point, converge to form a highly robust 5G platform for big data. Therefore, adequate techniques to efficiently collect and analyze big data from such a huge 5G platform have to be designed very carefully.

Last but not least, security has been widely discussed in various 5G standardization bodies. To enable wide deployment of 5G services and particularly enhance customer acceptance, security, focused on authenticity, authority, integrity, and confidentiality, must be considered. The challenge lies in the fact that different 5G components have different security requirements, and they all need to be considered right from the initial phase of system design.

The topics I have considered thus far by no means constitute an exhaustive list. There are plenty more interesting issues involving 5G wireless systems. We cordially ask researchers and practitioners to join the 5G race by contributing original and creative ideas in the context of our magazine.

Call for Papers
IEEE Network Magazine
Network Forensics and Surveillance for Emerging Networks

Background

Information and communication technologies (ICT) are becoming more intertwined in our lives, and inter-connected world. The networked world has revolutionized our lives in many ways and led to a closer and much more accessible world. For example, we can reach out to anyone, anywhere and anytime, regardless of geographical distance. Our increased dependence on ICT, and the pervasive interconnectivity of systems used in our networked world are, however, vectors that can potentially be exploited for nefarious or criminal purposes (e.g. hacking, theft of intellectual property and trade secrets, and online child exploitation). Recent incidents include the compromise of millions of Sony's PlayStation Network user accounts (resulting in significant reputation and financial damages to Sony), and Stuxnet (allegedly state-sponsored). The increasing number of high profile cyberattacks, and their impacts highlighted the importance of ensuring the security of our connected world.

In a cyberattack, every action leaves an evidence trail — in routers, firewalls, web proxies, and within the network traffic. Consequently, there is a growing need for investigators to analyze network events, including network traffic, netflow, security device (or appliance) log, in order to ascertain how an attack was carried out or how an event occurred on a network. Such activities can assist in the reconstruction of a crime and, potentially, the identification of the perpetrator(s). To reduce the risk of digital evidence being called into question in judicial proceedings, it is important to have a rigorous methodology and set of procedures for conducting digital or network forensics. However, the increasing use of Internet and networked technologies, such as wearable devices and cyber physical systems in critical infrastructures, fast-advancing networking technologies, and the need to deal with volatile and dynamic data, complicate efforts to collect and preserve evidential data in a timely fashion. To keep pace with the growth and changing face of criminal activity as well as fast advancing network technologies such as SDN or wireless SDN, 4G/LTE and 5G, it is important for the forensic research and practitioner communities to have an up-to-date and in-depth understanding of the types of terrestrial artefacts that are likely to remain on the network and on networked devices, as well as the capability to undertake data collection and acquisition in a timely and forensically sound manner.

This feature topic aims to foster the dissemination of the state-of-the-art advances in network forensics and surveillance for emerging networks. Only technical papers describing previously unpublished, original, state-of-the-art research, and not currently under review by a conference or a journal will be considered. Specifically, this issue welcomes two categories of papers: 1) invited articles from qualified experts; and 2) contributed papers from open call with list of addressed topics.

Submission Guidelines

Submitted papers should not be under consideration elsewhere for publication and the authors must follow the IEEE Network guidelines regarding manuscript content and format for preparation of the manuscripts. For details, please refer to the "Author Guidelines" at the IEEE Network Web site at http://www.comsoc.org/netmag/author-guidelines. Authors must submit their manuscripts via the IEEE Network manuscript submission system at http://mc.manuscriptcentral.com/network-ieee. All papers will be reviewed by at least three (3) reviewers for their technical merit, scope, and relevance to the CFP.

Schedule for Submissions

Manuscript submission: April 15, 2016
First Revison/Reject Notification: June 15, 2016
Notification of acceptance: August 15, 2016
Final manuscript due date: September 15, 2016
Publication date: November, 2016

Guest Editors

Dr. Xiaodong Lin (corresponding guest editor)
University of Ontario Institute of Technology (UOIT), Canada
Xiaodong.lin@uoit.ca

Dr. Kim-Kwang Raymond Choo
University of South Australia, Australia
Raymond.Choo@unisa.edu.au

Dr. Ying-Dar Lin
National Chiao Tung University, Taiwan
ydlin@cs.nctu.edu.tw

Dr. Peter Mueller
IBM, Switzerland
pmu@zurich.ibm.com