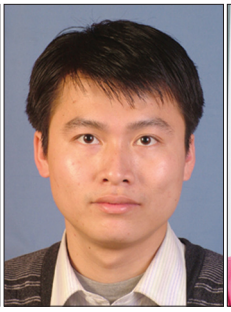
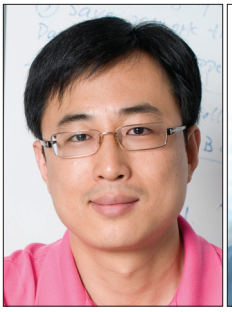
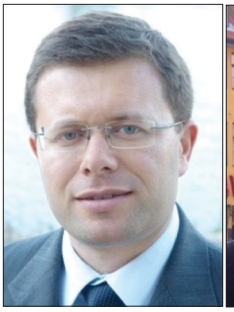
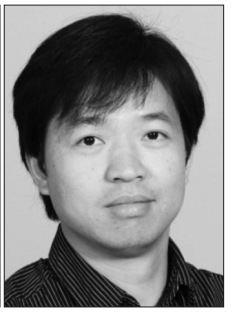
SECURITY AND PRIVACY IN EMERGING NETWORKS: PART II



Mohsen Guizani *Daojing He* *Kui Ren* *Joel J. P. Rodrigues* *Sammy Chan* *Yan Zhang*

This is the second part of the "Security and Privacy in Emerging Networks" Feature Topic. In Part I, which was published in April 2015, we selected those contributions that dealt with the theory behind the security and privacy of such networks. In Part II, we present articles that overview new security schemes for emerging networks such as vehicular, biomedical, underwater, crowdsourcing, and mobile networks. We feel that even though these emerging networks have attracted many research efforts lately, the security and privacy aspects have not been investigated well. Thus, it is important to provide ways to protect such networks from various security and privacy attacks. The aim of this FT is to promote further research interests in security and privacy in emerging networks by providing a vehicle for researchers and practitioners to discuss research challenges and open issues, and disseminate their latest research results. This can pave the way to implementing emerging networks with the necessary protection from major vulnerabilities. We received a large number of submissions but were obliged to accept only the best 13 papers. Part I was composed of six contributions that dealt with the theory of security/privacy threats, while this issue (Part II) is composed of seven articles addressing security challenges in a specific set of emerging networks.

With wireless technology available in all new vehicles, it is expected that a large amount of information will be exchanged between vehicles and/or between vehicles and roadside units (RSUs). Therefore, malicious attacks (whether intentional or not) may inject untrustworthy information into the network and cause havoc for drivers. This could lead to fatal accidents and loss of lives. Through the first article, "Toward a Trustworthy Vehicular Social Network," Q. Yang and H. Wang propose a social network approach to study trustworthy information sharing in vehicular networks. They first cover the research progress in measuring direct trust and modeling indirect trust in online social networks. They conclude with a discussion of how to apply those schemes to vehicular social networks and identify some research challenges.

As cloud-assisted wireless body sensor networks (WBSNs) are becoming increasingly popular in healthcare applications, the security and privacy threats targeting WBSNs deserve more attention. The second article, "Verifiable, Privacy-Assured, and Accurate Biomedical Signal Collection for Cloud-Assisted Wireless Body Sensor Networks," by C-M. Yu *et al.* focus on data privacy and data completeness where the authors propose a verifiable, privacy-assured, and accurate data collection scheme for cloud-assisted WBSNs. Through both simulation and prototype implementation, they show that the proposed scheme is energy-efficient and effective in protecting data privacy and completeness.

In addition, the use of underwater acoustic sensor networks (UASNs) has increased recently. However, most efforts in this area have not taken network security for UASNs seriously. Typically, UASNs are vulnerable to malicious attacks due to the unique characteristics of an underwater acoustic communication channel (e.g., low communication bandwidth, long propagation delays, and high bit error rates). In addition, the significant differences between UASNs and terrestrial wireless sensor networks (TWSNs) need special attention in the development of secure communication mechanisms for underwater sensor nodes. G. Han *et al.* address these issues in their contribution, "Secure Communication for Underwater Acoustic Sensor Networks." They present a survey of emerging topics arising from secure communications in UASNs. Then they propose a number of open research problems that, once resolved, could lead to providing secure and efficient methods for UASNs.

As we all know, mobile devices are capable of initiating sophisticated cyber-attacks, especially when they coordinate together to form what is referred to as a mobile distributed botnet (MobiBot). MobiBots leverage the absence of basic mobile operating system security mechanisms and the advantages of device-to-device (D2D) communication in masking malicious code propagation, which make them a serious security threat to any machine/network. In the next article, "From Botnets to MobiBots: A Novel Malicious Communication Paradigm for Mobile Botnets," the authors investigate the potential and impact of large-scale infection and coordination of neighboring devices. They highlight how mobile devices can leverage short-range

wireless technologies in attacks against other mobile devices that come within proximity. Later, they quantitatively measure the infection and propagation rates within MobiBots using short-range wireless technology such as Bluetooth.

On the other hand, the proliferation of mobile devices such as smartphones has enabled participatory sensing systems that collect data from users through their mobile devices and infer useful information from it. However, users have concerns regarding possible privacy leakage from their data. "Privacy-Preserving Participatory Sensing" by Q. Li and G. Cao addresses how to simultaneously protect privacy and provide incentives for participatory sensing. They review previous approaches, discuss their limitations, and propose two new types of participatory sensing systems with improved privacy protection.

A mobile crowdsourcing network (MCN) is a new promising network architecture that applies the principles of crowdsourcing to perform tasks using powerful mobile devices. However, it also raises some critical security and privacy issues that may prevent the applications and/or implementation of MCNs. The article "Security and Privacy in Mobile Crowdsourcing Networks: Challenges and Opportunities" by K. Yang *et al.* investigates some of these issues in order to achieve better understanding of these critical security and privacy challenges. They propose a general architecture for a mobile crowdsourcing network comprising of both crowdsourcing sensing and crowdsourcing computing. Then they discuss several critical security and privacy challenges that capture the essential characteristics of MCNs. They go on to formulate some research problems leading to possible research directions hoping to bring attention to further investigation into security and privacy solutions in MCNs.

The final article in this FT involves space information networks using satellites and high-altitude platform stations. Space information networks are able to enhance detection and transmission capabilities compared to current single Earth observation satellites. Although many attempts have been carried out concerning the space network architecture and protocols, the security issues have not been well investigated. C. Jiang *et al.* focus on the security problems in the space information networks from the perspectives of secure handoff, secure transmission control, secure key management, and secure routing. In their article, "Security in Space Information Networks," they review the challenges and open problems, and provide some solutions regarding the security issues on space information networks.

We are confident that these articles will add value to your research activities and give an overall direction for those researchers interested in this topic.

The Guest Editors would like to thank the previous Editor-in-Chief (Sean Moore) and the current Editor-in-Chief (Osman Gebizlioglu) for their guidance, feedback, and encouragement along the way. We are very grateful to them for allowing us to schedule two issues of the FT due to the large number of submissions received from highly qualified researchers. We also thank the IEEE Communications Magazine Publications Staff for their patience and hard work in making this issue a reality.

BIOGRAPHIES

MOHSEN GUIZANI [S'85, M'89, SM'99, F'09] (mguizani@ieee.org) is currently a professor and the associate vice president of graduate studies at Qatar University. He previously served as chair of the Computer Science Department at Western Michigan University (2002–2006)and chair of the Computer Science Department at the University of West Florida (1999–2002). He received his B.S., M.S., and Ph.D. degrees in electrical and computer engineering from Syracuse University, New York. His research interests include wireless communications and mobile computing, cloud computing, cyber security, and smart grid. He is the author of nine books and more than 400 publications in refereed journals and conferences He served as an IEEE Computer Society Distinguished Speaker from 2003 to 2005. He is a member of the IEEE Communications and IEEE Computer Societies and ASEE, and is a Senior Member of ACM.

DAOJING HE (hedaojinghit@gmail.com, djhe@sei.ecnu.edu.cn) received his B.Eng. (2007) and M. Eng. (2009) degrees from Harbin Institute of Technology, China, and his Ph.D. degree (2012) from Zhejiang University, China. He is currently a professor in the Software Engineering Institute, East China Normal University. His research interests include network and systems security. He is an Associate Editor or on the Editorial Boards of a number of international journals such as *IEEE Communications Magazine*.

KUI REN (kuiren@buffalo.edu) is an associate professor at the State University of New York at Buffalo. His research interests span cloud and outsourcing security, and wireless and wearable security. His research has been supported by NSF, DoE, AFRL, MSR, and Amazon. He was a recipient of NSF CAREER Award in 2011 and Sigma Xi/IIT Research Excellence Award in 2012. He is an Associate Editor for IEEE TMC, *TIFS*, *TSG*, and so on. He is a Distinguished Lecturer of IEEE.

JOEL J. P. C. RODRIGUES [S'01, M'06, SM'06] (joeljr@ieee.org) is a professor in the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and a researcher at the Instituto de Telecomunicações, Portugal. He is the leader of NetGNA Research Group (http://netgna.it.ubi.pt), Chair of the IEEE ComSoc TC on eHealth, Past Chair of the IEEE ComSoc TC on 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 over 400 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.

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 a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. He is an associate professor in the Department of Electronic Engineering, City University of Hong Kong.

YAN ZHANG (yanzhang@simula.no) received a Ph.D. degree from Nanyang Technological University, Singapore. Since August 2006, he has been working with Simula Research Laboratory, Norway. He is currently head of the Department of Networks at Simula Research Laboratory, and an adjunct associate professor at the Department of Informatics, University of Oslo, Norway. He is a Regional Editor, Associate Editor, on the Editorial Board, or a Guest Editor of a number of international journals. His recent research interests include wireless networks, cyber physical systems, and smart grid communications.