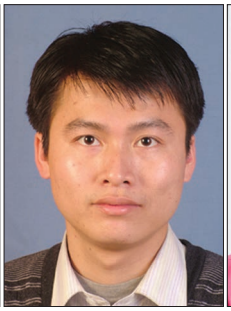
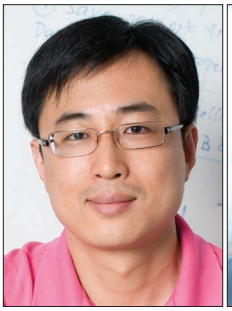
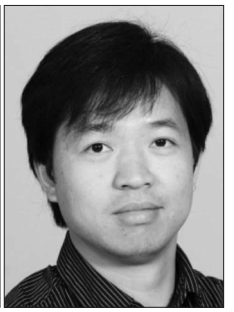
SECURITY AND PRIVACY IN EMERGING NETWORKS: PART 1

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

With the recent advancements in networking technologies, some new emerging networks are being implemented that have the potential to be deployed broadly and on a large scale in the near future. In the wired domain, these emerging networks include, for example, networks based on software-defined networking (SDN) and named data networking (NDN). In the wireless domain, they include mobile and wireless networks involving handheld computing devices, sensors and RFID devices, body area sensor networks, and participatory sensing networks, to name a few.

Although these kinds of networks have attracted much research effort, the security and privacy issues have not been studied well so far. Thus, there is an urgent need to protect these networks from various security and privacy threats. This could pave the way to implement these networks without major security obstacles. This Feature Topic aims to promote further research interest 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. We received an overwhelmingly large number of high-quality submissions (40 papers) out of which we accepted only the top 13 articles. We are lucky to get the permission of the Editor-in-Chief of *IEEE Communications Magazine* to divide the accepted papers into two parts. Part 1 will be composed of six manuscripts that deal with the theory of security and privacy threats of emerging networks, and the second part is composed of seven papers addressing the same issues with more specific applications of security and privacy. Part 2 is scheduled to appear in June 2015. We invite you to stay tuned and check that issue as it will complement the topics discussed in this first part.

The first article, by Yang *et al.*, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," attempts to shed some light on the physical layer security related to fifth generation (5G) mobile and wireless networks. The authors examine some inherent vulnerabilities in 5G wireless networks and focus on three main technologies: heterogeneous networks, massive multiple-input multiple-output, and millimeter-wave. They identify possible opportunities and challenges in these technologies and warn security designers of the possible problems that could exist and must be tackled.

On the other hand, 5G mobile networks use densified small cell deployment with overlay coverage through coexisting heterogeneous networks (HetNets). This type of multi-tier architecture along with stringent latency requirements in 5G bring new challenges in security provisioning due to the potential frequent handovers and authentications. In the second article, the authors overview related studies and introduce SDN into 5G as a platform to enable efficient authentication handover and privacy protection. Thus, "Authentication Handover and Privacy Protection in 5G HetNet Using Software-Defined Networking" by X. Suan and X. Wang attempts to simplify authentication handover by sharing the user-dependent security context information among related access points. They demonstrate that SDN-enabled security solutions are highly efficient when using a centralized controlling capability.

The growth of software defined networks (SDNs) promises to dramatically simplify network management and enable innovation through network programmability. However, security is expected to remain the main impediment to SDNs' growth. This is due in part to the fact that security is not considered as part of the initial SDN design. The third article, "Securing the Software Defined Networks: Taxonomy, Requirements, and Open Issues" by A. Akhunzada *et al.*, discusses the state-of-the-art security solutions in order to overcome those challenges. The authors classify the existing security solutions based on SDN layers/interfaces, security measures, simulation environments, and security objectives. They then point out possible attacks and threats targeting SDNs with potential key security requirements. Finally, open issues and challenges of SDN security are presented that may be deemed appropriate for researchers to address in order to help SDNs achieve their potential goals.

Along the same line, Zhou *et al.* conceived a novel conceptual network security mechanism called the evolving defense

mechanism (EDM). In their contribution, "Evolving Defense Mechanism for Future Network Security," they show that EDM is an inspiration of a network configuration originating from a biological gene. They provide an overview of EDM and argue that it is able to avoid deficiencies of conventional network security approaches. They first discuss dynamic network configuration for preventing attacks and then sketch a way to implement EDM as an ideal framework based on SDN serving as an ecosystem and coexisting environments.

The next article, "Distributed Denial of Service Attacks in SDN with Cloud Computing," may help us make full use of SDN's advantages to defeat DDoS attacks in cloud computing environments. The authors, Q. Yan and R. Yu, first discuss the new trends and characteristics of DDoS attacks in cloud computing environments. Then they show that SDN brings new opportunities and special features in defeating DDoS attacks. They finally present a number of challenges that need to be addressed to mitigate DDoS attacks when SDN is combined with cloud computing.

In the final article of Part 1 of this Feature Topic, "De-Anonymizing and Countermeasures in Anonymous Communication Networks," M. Yang *et al.* classify and provide an overview of existing de-anonymizing techniques and propose countermeasures to mitigate those risks.

We are confident that this selection of high-quality articles will provide some research directions in the field. While most of the above articles discuss SDN security, there are plenty of issues that have been presented that will need more focus and attention to be developed for emerging networks. We strongly believe that all of us (from multiple disciplines) have to join our efforts, and must come together and strive hard to overcome technical roadblocks in order to bring the vision of emerging network security to reality.

The Guest Editors would like to thank the outgoing Editor-in-Chief (Sean Moore) and the incoming 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 Feature Topic 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 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 all 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 Computer Societies and ASEE, and a Senior Member of ACM.

DAOJING HE (hedaojinghit@gmail.com) 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 at 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. Hiss research interest spans 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 an NSF CAREER Award in 2011 and a Sigma Xi/IIT Research Excellence Award in 2012. He is an Associate Editor for IEEE TMC, TIFS, TSG, and others. He is a Distinguished Lecturer of IEEE.

JOEL 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 the 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 of over 400 papers, two books, and three patents. He is the recipient of several Outstanding Leadership and Outstanding Service Awards from the 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 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 Guest Editor of a number of international journals. His recent research interests include wireless networks, cyber physical systems, and smart grid communications.