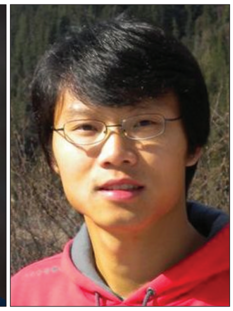
GUEST EDITORIAL

WIRELESS PHYSICAL LAYER SECURITY

Walid Saad ***Xiangyun Zhou*** ***Mérouane Debbah*** ***H. Vincent Poor***

The ongoing paradigm shift from classical centralized wireless technologies toward distributed large-scale networks such as the Internet of Things has introduced new security challenges that cannot be fully handled via traditional cryptographic means. In emerging wireless environments, devices have limited capabilities and are not controlled by a central control center; thus, the implementation of computationally expensive cryptographic techniques can be challenging. Motivated by this paradigm shift, substantial recent research has been investigating the use of the physical layer as a means to develop low-complexity and effective wireless security mechanisms. Such techniques are grouped under the umbrella of *physical layer security*. These techniques range from information-theoretic security, which exploits channel advantages to thwart eavesdropping, to physical layer fingerprinting techniques that exploit physical layer features for device identification. In this context, providing state-of-the-art tutorials on the various approaches to physical layer security is of considerable interest. This Feature Topic gathers together tutorial-style and survey articles that provide an in-depth overview of the broad spectrum of security opportunities brought forward by physical layer security.

In this second issue of the Feature Topic on wireless physical layer security, the first article by Lin *et al.* investigates the impact of channel state information (CSI) on wireless secrecy. In this regard, the authors expose how different levels of CSI may affect confidentiality in terms of information-theoretic secrecy. Then the next article, by Bash *et al.*, studies the use of covert communication techniques that can counter security threats from adversaries that use non-computational methods, such as side-channel analysis, to jeopardize wireless transmissions. Various secrecy signaling and coding schemes have been designed at the physical layer of wireless systems to guarantee confidentiality against information leakage to unauthorized receivers, among which the strategy based on the idea of node cooperation is promising and is discussed in the following three articles. In this regard, the work by Jimenez *et al.* provides a broad overview of this area while discussing one case study to quantify the benefits of relay resource allocation for improving wireless secrecy. Next, Chen *et al.* focus on scenarios in which relays are equipped with multiple antennas. For such settings, the authors discuss how one can exploit MIMO techniques to further enhance cooperation and boost the secrecy of wireless transmission. The next article provides a signal processing approach to the problem of wireless cooperation, and focuses on secrecy signal design and optimization techniques to increase secrecy performance. The privacy of a wireless user and the operation of a wireless network can be threatened by the leakage of transmission signatures, even when encryption and authentication services are employed. The Feature Topic concludes with an article by Rahbari and Krunz that describes various passive (traffic analysis) and active (jamming) attacks that are facilitated by side-channel information. The goal is to highlight the need for novel physical-layer security techniques that can be used to complement classical encryption methods.

In a nutshell, given the significant advances in physical layer security of the past decade, this Feature Topic provides an in-depth exposition of the various challenges faced, and that will continue to be faced, in the field of wireless physical layer security. We hope that these contributions will initiate future research developments in this field and contribute toward introducing physical layer security schemes in practical scenarios.

ACKNOWLEDGMENTS

The Guest Editors would like to thank the large number of people who significantly contributed to this Feature Topic, including the authors, reviewers, and *IEEE Communications Magazine* editorial staff.

BIOGRAPHIES

WALID SAAD [S'07, M'10] (walids@vt.edu) is an assistant professor and the Steven O. Lane Junior Faculty Fellow at the Bradley Department of Electrical and Computer Engineering at Virginia Tech. His research interests include wireless and social networks, game theory, cybersecurity, smart grid, network science, cognitive radio, and self-organizing networks. He is the recipient of the NSF CAREER award in 2013, the AFOSR summer faculty fellowship in 2014, and the ONR Young Investigator Award in 2015 as well as several conference best paper awards.

XIANGYUN ZHOU (xiangyun.zhou@anu.edu.au) is a senior lecturer at the Australian National University (ANU). He received his Ph.D. degree from ANU in 2010. His research interests are in the fields of communication theory and wireless networks. He has a large number of publications in the area of physical layer security, including as Editor of *Physical Layer Security in Wireless Communications* (CRC Press). He serves as an Editor for *IEEE Transactions on Wireless Communications* and *IEEE Communications Letters*.

MÉROUANE DEBBAH [F] (merouane.debbah@huawei.com) is vice-president of the Huawei France R&D center and director of the Mathematical and Algorithmic Sciences Lab . Since 2007, he is also a full professor at Centrale Supelec. His research interests lie in fundamental mathematics, algorithms, complex systems analysis and optimization, and information and communication sciences. He is a WWRF Fellow and a member of the academic senate of Paris-Saclay. He is the recipient of several awards such as the Qualcomm Innovation Prize Award.

H. VINCENT POOR [S'72, M'77, SM'82, F'87] (poor@princeton.edu) is with Princeton University, where his interests are in wireless networking and related fields. He is a member of the National Academy of Engineering and the National Academy of Sciences, and a foreign member of the Royal Society. He received the IEEE ComSoc Marconi and Armstrong Awards in 2007 and 2009, respectively, and more recently the 2014 URSI Booker Gold Medal and honorary doctorates from several universities.