WIRELESS PHYSICAL LAYER SECURITY: PART 1




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 cryptgraphic means. In such 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 these considerations, 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 such tutorial-style and overview articles that provide an in-depth overview of the broad spectrum of security opportunities brought forward by physical layer security.

This Feature Topic is composed of two parts; the second part is expected to appear in the December issue of this magazine. Part 1 begins with an opening editorial by Trappe that exposes the current and future potential of wireless physical layer security. Then, Kapetanovic *et al.* present a novel application of physical layer security: massive multiple-input multiple-output (MIMO) systems. In this article, the authors focus on the robustness of massive MIMO against eavesdropping while also outlining other important related challenges. The next article by Win *et al.* also focuses on secrecy with a particular emphasis on the role of interference. In particular, it discusses how one can engineer interference to ensure confidentiality. Next, the work by Zeng tackles the problem of using the physical layer for key generation. Apart from the passive eavesdropping attack commonly considered in the literature, the author also discusses three types of active attacks and proposes a new key generation scheme to defend against them. The next article by Kailkhura *et al.* describes the security of a distributed inference framework comprising a group of spatially distributed nodes that acquire observations about a phenomenon of interest and transmit computed summary statistics to a fusion center. The authors propose efficient schemes to mitigate the impact of eavesdropping on distributed inference, and survey the currently available approaches along with avenues for future research. This first issue concludes with an article by Yu *et al.* that exposes the importance of physical layer features as a means to fingerprint and authenticate wireless devices.

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 with 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 an edited book, *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 [S'01, M'04, SM'08, F'15] (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 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.