Guest Editorial: Wireless Physical Layer Security

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

► To cite this version:

Walid Saad, Xiangyun Zhou, Mérouane Debbah, H. Vincent Poor. Guest Editorial: Wireless Physical Layer Security. IEEE Communications Magazine, 2015, 53 (12), pp.18. 10.1109/mcom.2015.7355560 . hal-01341108

HAL Id: hal-01341108

<https://hal.science/hal-01341108>

Submitted on 4 Jul 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Guest Editorial: Special Issue on Wireless Physical Layer Security

Walid Saad¹, Xiangyun Zhou², Mrouane Debbah³, and H. Vincent Poor⁴

¹ Wireless@VT, Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA, Email: walids@vt.edu

² Research School of Engineering, Australian National University, Canberra, Australia, Email: xiangyun.zhou@anu.edu.au

³ Mathematical and Algorithmic Sciences Lab, Huawei France R & D, Paris, France, Email: merouane.debbah@huawei.com

⁴ Electrical Engineering Department, Princeton University, Princeton, NJ, USA, Email: poor@princeton.edu

The ongoing paradigm shift from classical, centralized wireless technologies towards 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 are of limited capabilities and are not controlled by a central control center; and, 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 exploit 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 magazine feature topic is composed of two issues. The first issue begins by 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 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 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 and optimize secrecy. Next, the work by Zeng tackles the problem of using the physical layer for key generation. Apart from the passive eavesdropping attack that is 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 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 mitigation schemes to mitigate the impact of eavesdropping on distributed inference and they survey the currently available approaches along with avenues for future research. This first issue concludes with an article that exposes the importance of physical layer features as a means to

fingerprint and authenticate wireless devices.

In the second issue to be published in December 2015, the first article 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 on 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 the wireless transmission. The next article provides a signal processing approach to the problem of wireless cooperation, and it 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 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 that faced and will continue to face the field of wireless physical layer security. We hope that these contributions will initiate future research developments in this field and will contribute towards introducing physical layer security schemes in practical scenarios.

Acknowledgements. The guest editors would like to thank the large number of people who significantly contributed to this special issue, including the authors, reviewers, and *Communications Magazine* editorial staff.

Walid Saad (S'07, M'10) is an Assistant Professor 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. Dr. Saad is the recipient of the NSF CAREER award in 2013 and of the AFOSR summer faculty fellowship in 2014 as well as of several conference best paper awards.

Xiangyun Zhou 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*.

Mrouane Debbah is the 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 & communication sciences. He is an IEEE Fellow, 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 (S72, M77, SM82, F87) 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.