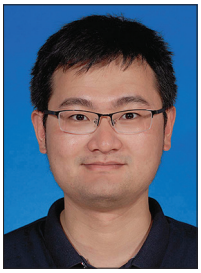
Safeguarding 5G-and-Beyond Networks with Physical Layer Security



Yongpeng Wu Trung Q. Duong A. Lee Swindlehurst

The number of mobile-connected wireless devices is quickly growing and will reach 11 billion by 2020, exceeding the world's projected population at that time (7.8 billion). Meanwhile, the demand for wireless data transmission in futuristic wireless networks is growing exponentially. For example, a mobile user is expected to download approximately 1 terabyte of data on average annually by 2020. Cutting-edge wireless-enabled applications, such as e-healthcare, augmented reality, Tactile Internet, and the Internet of Vehicles (IoV), are becoming a reality, which is triggering an explosion of mobile data traffic, a rapid increase in the number of end-devices, massive instantaneous end-to-end connections, and high-reliability low-latency services. It will be an extremely daunting task for fourth generation (4G) networks to meet the ever-increasing communication needs, and the aforementioned features have been recognized as essential requirements for the fifth generation (5G) era and beyond.

As a fundamental enabler of the future intelligent society, 5G will include the evolution of all parts of communication networks, ranging from radio to applications. As a result, security is potentially affected everywhere, and providing high-quality security services is one of the top priorities in the design and development of 5G networks. Looking back about 25 years, when 2G systems were developed and standardized, built-in security functions were introduced to combat emerging threats. In 3G, further security improvements were made, such as using mutual authentication to mitigate the threats of rogue radio base stations. For the 4G LTE standard, the main additional security mechanism was to transfer the user data encryption to the base station. Although the security designs in 2G, 3G, and 4G networks have provided a platform for undisputed socioeconomic success, against a diversified range of services, 5G will introduce new and open security challenges, such as a flexible and scalable security architecture, lightweight security, and energy-efficient security.

Physical layer security has recently been recognized as a promising mechanism to achieve confidentiality by exploiting the inherent randomness of wireless channels at the physical layer. In particular, physical layer security can enable secure communication over the wireless medium without the aid of an encryption key. This advantage makes physical layer security particularly suitable for implementation in 5G and beyond networks with massive devices and heterogeneous subsystems. As per the requirements of physical layer security, no limitations are imposed on the eavesdroppers in terms of their computational capabilities. This indicates that secure communications can still be achieved even if the eavesdroppers in futuristic networks are powerful and computational devices. Therefore, physical layer security, operating essentially independently of higher layers, is now commonly expected to augment the existing security mechanisms for safeguarding wireless communications in the 5G era and beyond networks.

Our Special Issue aims to bring together leading researchers in both academia and industry from diverse backgrounds to advance the physical layer security techniques of wireless networks in the 5G era and beyond networks. There are a total of eight papers accepted for our special issue. These papers provide a latest survey of physical layer security research on various promising techniques for 5G era and beyond networks.

The first article, "Physical Layer Security for Ultra-Reliable and Low-Latency Communications" by Riqing Chen, Chunhui Li, Shihao Yan, Robert Malaney, and Jinhong Yuan, investigates physical layer security for ultra-reliable and low-latency communication (URLLC). The trade-off between latency, reliability, and security are discussed and performance metrics for evaluating physical layer security in URLLC are provided.

In the second article, "Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective" by Qingqing Wu, Weidong Mei, and Rui Zhang, new issues from a physical layer security viewpoint of unmanned aerial vehicles (UAVs) are discussed and novel solutions to tackle these issues efficiently are provided. Two particular aspects for UAVs are studied:

1. Compared to terrestrial wireless channels that in general suffer from severe path loss, shadowing, and multi-path fading, the high altitude of UAVs generally leads to more dominant line of sight channels with the ground nodes.
2. UAVs potentially might be a new security threat to the terrestrial cellular network if they are misused by unauthorized parties for malicious purposes.

In the third article, "Low Probability of Detection Communication: Opportunities and Challenges" by Shihao Yan, Xiangyun Zhou, Jinsong Hu, and Stephen V. Hanly, the key features of low probability communication are identified and various important design considerations are studied. Research on low probability communication will enhance national security by foreseeing any future fortunate or devastating impact of this technology on our national cybersecurity and understand how to regulate the use of this new technology in future wireless communications.

In the fourth article, "Physical Layer Security by Exploiting Interference and Heterogeneous Signaling" by Ali A. Nasir,

Hoang D. Tuan, Ha H. Nguyen, and Nghia M. Nguyen, the interference channels are exploited to simultaneously reduce the interference for the users' received signals and amplify the interference at the eavesdroppers' received signal. A constructive assumption on channel state information for eavesdroppers' channels is considered, and there is no restriction that the eavesdroppers must be in worse channel conditions than the legitimate users.

The fifth article, "UAV-Involved Wireless Physical Layer Secure Communications: Overview and Research Directions" by Hui-Ming Wang, Xu Zhang, and Jia-Cheng Jiang, provides an overview of the recent research efforts on UAV-involved secure communications at the physical layer. According to different roles of UAVs in secure communications, UAV-enabled secure communications and UAV-aided secure cooperation are discussed.

The sixth article, "Physical Layer Security in UAV Systems: Challenges and Opportunities" by Xiaofang Sun, Derrick Wing Kwan Ng, Zhiguo Ding, Yanqing Xu, and Zhangdui Zhong, examines the physical layer security issues in UAV systems. The authors present an overview of emerging techniques, such as trajectory design, resource allocation, and cooperative UAVs, to fight against both passive and active eavesdropping in UAV wireless communication systems.

In the seventh article, "Physical Layer Key Generation in 5G Wireless Networks" by Long Jiao, Ning Wang, Pu Wang, Amir Alipour-Fanid, Jie Tang, and Kai Zeng, the existing key generation methods for physical layer security and possible solutions for the existing issues are provided. New insights into physical key generation in 5G wireless networks are revealed, which is expected to advance and stimulate the corresponding research under the context of 5G and beyond communication systems.

The eighth article, "Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks" by He Fang, Xianbin Wang, and Stefano Tomasin, discusses new authentication approaches based on machine learning techniques by opportunistically leveraging physical layer attributes. The authors introduce intelligent authentication approaches with the help of machine learning to address the challenges for security enhancement and more efficient management in 5G and beyond networks.

Finally, we want to thank all the authors who submitted their works to this Special Issue as well as their technical merits. They provided both the reviewers and editors with a fascinating snapshot of the range of ongoing research in the area. Due to the highly selective nature of *IEEE Wireless Communications*, many interesting papers were not selected for our Special Issue, but we hope that these papers might appear elsewhere. We also thank all the reviewers, who were very responsive to our repeated reminders about staying on schedule. Their critical comments and suggestions to the authors contributed substantially to our special issue. We also thank Prof. Yi Qian, *IEEE Wireless Communications* Editor-in-Chief, Cathy Kemelmacher, Joseph Milizzo, Jennifer Porcello, and other people for the effort and help they have provided for our special issue.

Biographies

Yongpeng Wu [S'08, M'13, SM'17] (yongpeng.wu@sjtu.edu.cn) received the B.S. degree in telecommunication engineering from Wuhan University, Wuhan, China, in July 2007, and the Ph.D. degree in communication and signal processing from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in November 2013. He is currently a tenure-track associate professor with the Department of Electronic Engineering, Shanghai Jiao Tong University, China. Previously, he was a senior research fellow with the Institute for Communications Engineering, Technical University of Munich, Germany and the Humboldt research fellow and the senior research fellow with the Institute for Digital Communications, University Erlangen-Nürnberg, Germany. During his doctoral studies, he conducted cooperative research at the Department of Electrical Engineering, Missouri University of Science and Technology, USA. His research interests include massive MIMO/MIMO systems, massive access, physical layer security, and power line communication. He was awarded an IEEE Student Travel Grant for the IEEE International Conference on Communications (ICC) in 2010, the Alexander von Humboldt Fellowship in 2014, a Travel Grant for the IEEE Communication Theory Workshop in 2016, an Excellent Doctoral Thesis Awards from the China Communications Society in 2016, the Exemplary Editor Award from *IEEE Communication Letters* in 2017, and the Young Elite Scientist Sponsorship Program by CAST in 2017. He was an Exemplary Reviewer of *IEEE Transactions on Communications* in 2015, 2016, and 2018. He was the lead guest editor for the special issue "Physical Layer Security for 5G Wireless Networks" in *IEEE Journal on Selected Areas in Communications* and the guest editor for the special issue "Safeguarding 5G-and-Beyond Networks with Physical Layer Security" in *IEEE Wireless Communications Magazine*. He is currently an editor of *IEEE Transactions on Communications* and *IEEE Communications Letters*. He has been a TPC member of various conferences including Globecom, ICC, VTC, and PIMRC.

Trung Q. Duong [S'05, M'12, SM'13] received his Ph.D. degree in telecommunications systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Currently, he is with Queen's University Belfast (UK), where he was a lecturer (assistant professor) from 2013 to 2017 and a reader (associate professor) from 2018. His current research interests include Internet of Things (IoT), wireless communications, molecular communications, and signal processing. He is the author or co-author of over 340 technical papers published in scientific journals (200+ articles) and presented at international conferences (140+ papers). He currently serves as an Editor of *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Communications*, *IET Communications*, and a lead senior editor of *IEEE Communications Letters*. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, the IEEE International Conference on Communications (ICC) in 2014, the IEEE Global Communications Conference (GLOBECOM) in 2016, the IEEE Digital Signal Processing Conference (DSP) in 2017, and the International Wireless Communications & Mobile Computing Conference (IWCMC) in 2019. He is the recipient of the prestigious Royal Academy of Engineering Research Fellowship (2016–2021) and won a prestigious Newton Prize in 2017.

A. Lee Swindlehurst received the B.S. (1985) and M.S. (1986) degrees in electrical engineering from Brigham Young University (BYU), and the Ph.D. (1991) degree in electrical engineering from Stanford University. He was with the Department of Electrical and Computer Engineering at BYU from 1990 to 2007, where he served as Department Chair from 2003 to 2006. During 1996 to 1997, he held a joint appointment as a visiting scholar at Uppsala University and the Royal Institute of Technology in Sweden. From 2006 to 2007, he was on leave working as Vice President of Research for ArrayComm LLC in San Jose, California. Since 2007 he has been a professor in the Electrical Engineering and Computer Science Department at the University of California Irvine, where he served as Associate Dean for Research and Graduate Studies in the Samueli School of Engineering from 2013 to 2016. During 2014 to 2017 he was also a Hans Fischer Senior Fellow at the Institute for Advanced Studies at the Technical University of Munich. In 2016, he was elected a Foreign Member of the Royal Swedish Academy of Engineering Sciences (IVA). His research focuses on array signal processing for radar, wireless communications, and biomedical applications, and he has over 300 publications in these areas. He is a Fellow of the IEEE and was the inaugural Editor-in-Chief of the *IEEE Journal of Selected Topics in Signal Processing*. He received the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, the 2006 and 2010 IEEE Signal Processing Society's Best Paper Awards, and the 2017 IEEE Signal Processing Society Donald G. Fink Overview Paper Award.