# Guest Editorial Physical Layer Security for 5G Wireless Networks, Part I

Yongpeng Wu, *Senior Member, IEEE*, Ashish Khisti, *Senior Member, IEEE*, Chengshan Xiao, *Fellow, IEEE*, Giuseppe Caire, *Fellow, IEEE*, Kai-Kit Wong, *Fellow, IEEE*, and Xiqi Gao, *Fellow, IEEE*

## I. Introduction

THE unprecedented growth in the number of mobile data and connected machines ever-fast approaches limits of fourth generation technologies to address this enormous data demand. Therefore, the development of the fifth generation (5G) wireless communication technologies is a priority issue currently. The evolution towards 5G wireless communications will be a cornerstone for realizing the future human-centric and connected machine-centric networks, which achieve near-instantaneous, zero distance connectivity for people and connected machines. On the other hand, wireless networks have been widely used in civilian and military applications and become an indispensable part of our daily life. People rely heavily on wireless networks for transmission of important/private information, such as credit card information, energy pricing, e-health data, command, and control messages. Therefore, security is a critical issue for future 5G wireless networks. Physical layer security techniques can be used to either perform secure data transmission directly or generate the distribution of cryptography keys for conventional cryptography techniques in the 5G networks. With careful management and implementation, physical layer security can be used as an additional level of protection on top of the existing security schemes. As such, they will formulate a well-integrated security solution together that efficiently safeguards the confidential and privacy communication data in 5G wireless networks. The main goal of this IEEE JSAC Special Issue on “Physical Layer Security for 5G Wireless Networks” is to bring together leading researchers in both academia and industry from diversified backgrounds to advance the theory and practice of physical layer security for 5G wireless networks.

There are total 39 accepted technical papers for our special issue, which will be published in two issues. In additional to technical papers, there is another survey paper “A survey of physical layer security techniques for 5G wireless networks and challenges ahead” in the first issue. This paper provides a latest survey of the physical layer security research on various promising 5G technologies.

## II. Accepted Technical Paper

The first issue has 19 technical papers with a broad range of topics as follows:

The first paper “Securing on-body IoT devices by exploiting creeping wave propagation” provides a good application example for the unified security strategy design across the network and the physical layers for the future Internet-of-Things vision. SecureTag is proposed to defend against active attacks for on-body devices by integrating physical layer information with upper-layer protocols. Once a suspicious transmission is detected, SecureTag initiates a physical layer-based challenge-response protocol to mitigate attacks.

The second paper “The secrecy capacity of Gaussian MIMO wiretap channels under interference constraints” studies the secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel with interference constraint. In other terms, how to characterise the amount of information two users equipped with multiple antennas can share with minimum leakage to eavesdroppers whilst minimising the interference generated at an other user. The authors show that the problem of finding the secrecy capacity can be expressed as a max-min problem so that a converging algorithm can be developed to find the solution. The optimal signaling directions are then characterised with and without interference constraint. In short, the feasibility of physical layer security with multiple antennas under interference constraint is investigated.

The third paper “Secure communication over finite state multiple-access wiretap channel with delayed feedback” analyzes the secrecy capacity region of a finite-state multiple-access wiretap channel with delayed feedback of the state and the channel output. Inner and outer bounds on the capacity region are derived for two cases: delay feedback of the state only, and delay feedback of both the state and the legitimate

Y. Wu is with the Department of Electrical Engineering, Shanghai Jiao Tong University, Minhang 200240, China (e-mail: yongpeng.wu@sjtu.edu.cn; yongpeng.wu2016@gmail.com).

A. Khisti is with the Signal Multimedia and Security Laboratory, University of Toronto, Toronto, ON M5S 3H7, Canada (e-mail: akhisti@ece.utoronto.ca).

C. Xiao is with the Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA 18015 USA (e-mail: xiaoc@lehigh.edu).

G. Caire is with the Institute for Telecommunication Systems, Technical University Berlin, 10587 Berlin, Germany (e-mail: caire@tu-berlin.de).

K.-K. Wong is with the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, U.K. (e-mail: kai-kit.wong@ucl.ac.uk).

X. Gao is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: xqgao@seu.edu.cn).

Digital Object Identifier 10.1109/JSAC.2018.2832378

receiver's output. The main finding of this paper is that, delayed feedback of the channel output has two benefits: 1) allows the generation of secret keys between the transmitters and receiver; 2) allows coordination between the two transmitters. The bounds are evaluated for a degraded Gaussian fading channel.

The secure rate region of asymmetric multilevel diversity coding systems with $L$ encoders, $L+1$ sources, and security level $L2$ is investigated in the fourth paper "Fundamental limits on a class of secure asymmetric multilevel diversity coding systems". Upper bounds on the size of secrecy keys are derived. The authors prove that unlike in the symmetric multilevel diversity coding systems, superposition coding is not optimal for secure asymmetric multilevel diversity coding systems.

The fifth paper "An LDPC code based physical layer authentication scheme with prefect security" studies multiple-message authentication over noiseless main channel case and noisy main channel case, respectively. For the noiseless main channel case, a multiple-message authentication is proposed by leveraging a novel $\epsilon$-$\mathrm{AU}_2$ hash function family and the dual of large-girth LDPC codes. For the noisy main channel case, an authentication scheme is proposed by reducing the noisy main channel case to noiseless main channel case through public discussion and stochastically degraded channel technique. The proposed schemes are proved to be perfectly secure if the number of attacks by Eve is upper bounded by a polynomial times in terms of n.

A secrecy capacity achieving polar coding scheme for the cognitive interference channel with confidential messages under the strong secrecy criterion is proposed in the sixth paper "Polar coding for the cognitive interference channel with confidential messages". It is shown that the whole secrecy capacity region of the cognitive interference channel with confidential messages can be achieved by simple point-to-point polar codes, and the proposed scheme requires the minimum rate of randomness at the encoder.

The seventh paper "Robust beamforming for physical layer security in BDMA massive MIMO" proposes a robust beamforming desgin to achieve physical layer security for a multi-user beam division multiple access massive multiple-input multiple-output (MIMO) system with imperfect channel state information (CSI). The proposed design reduces the computational complexity by obtaining a closed form solution for the optimal beamforming direction and the optimal beamforming power allocation.

The eighth paper "Exploiting inter-user interference for secure massive non-orthogonal multiple access" studies the secure massive access in a single-cell multiuser downlink communication system with massive MIMO and non-orthogonal multiple access. The non-orthogonal channel estimation is performed to reduce the length of training sequence and the inter-user interference is exploited as AN signal to confuse the eavesdroppers, especially in the scenario of active eavesdropping.

The ninth paper "Secure massive MIMO with the artificial noise-aided downlink training" proposes two AN-aiding schemes to enhance the secrecy performance of massive MIMO networks in presence of a passive eavesdropper. The authors develop the analytical expressions and tight approximations for the achievable secrecy rate to investigate the performance of the two proposed AN-aiding schemes. The results reveal that deploying AN in the downlink training phase of massive MIMO networks does not affect the downlink channel estimation process at users while enabling the system to suppress the downlink channel estimation process at eavesdropper.

The tenth paper "Optimal transmit antenna selection for massive MIMO wiretap channels" investigates the secrecy performance of a massive MIMO wiretap channel when the transmitter selects a subset of antennas corresponding to the strongest channels. Confidential messages are then transmitted to a multi-antenna legitimate receiver while a multi-antenna eavesdropper overhears the channel. For this setup, an accurate large-system approximation of the instantaneous secrecy rate is derived and this approximation is used to investigate the performance under active and passive eavesdropping.

The eleventh paper "Physically securing energy-based massive MIMO MAC via joint alignment of multi-user constellations and artificial noise" considers the optimality of jointly aligning multi-user constellations and artificial noise to secure a multiple access communication in a massive MIMO setup, i.e., the base station and the eavesdropper are equipped with large antenna arrays and each user is equipped with multiple transmit antennas. The authors start by discussing a distance optimal constellation and show that its structure can be specifically used to design a PAM alignment scheme. At this stage, the secrecy constraint is taken into consideration. Then, by exploiting the power domain freedom of the used constellation, they present a stepped water-Filing power allocation scheme that utilizes the remaining power to transmit artificial noise.

The twelfth paper "Constant envelope hybrid precoding for directional millimeter-wave communications" studies physical layer security for mmWave massive MIMO systems by considering joint hybrid analog and digital precoding and constant envelope modulation to address the challenges caused by limited number of radio frequency chains and high peak to average power ratio. Considering two specific hybrid MIMO architectures, optimization problems are formulated to minimize the power leakage to eavesdroppers while ensuring the legitimate users can correctly receive the desired data symbols. To solve these problems, the authors exploit penalty method and block coordinate descent-type algorithms, which is shown to find the stationary points of the optimization problems.

The thirteenth paper "Multiple antennas secure transmission under pilot spoofing and jamming attack" provides a scheme to counteract pilot spoofing attacks and pilot jamming attacks in a base station with multiple antennas, in time division duplex mode. The idea is to let the terminal use a random channel training, in which the pilot used by the terminal is drawn randomly from a subset of all pilots. The base station can then, without a priori knowledge, detect what pilot was transmitted, and use this to estimate both the channel to the legitimate terminal and to the malicious terminal. The paper finds closed-form expressions and approximations to measure performance in terms of error decision rate and secrecy rate.

The fourteenth paper "Mapping-varied spatial modulation for physical layer security: transmission strategy and secrecy rate" proposes a physical layer secure transmission scheme based on spatial modulation, which is termed mapping-varied spatial modulation. The scheme varies the mappings of antenna indices and constellation points according to the legitimate CSI, which is unknown by Eve. In this way Eve cannot directly decode the information and the security is improved. Furthermore, the paper studies the achievable secrecy rates of the proposed scheme under both finite-alphabet and Gaussian input.

The fifteenth paper "Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array" joint utilizes random subcarrier selection based on OFDM, phase alignment/beamforming, artificial noise, and directional modulation to achieve secure precise transmission of confidential messages. In addition, the average signal-to-interference-and-noise ratio (SINR) and its upper bound are derived.

The sixteenth paper "Optimization or alignment: secure primary transmission assisted by secondary networks" proposes, analyzes, and compares two schemes, i.e., optimal transceiver design scheme and interference alignment-based scheme, to achieve secure transmission of primary user assisted by secondary users in cognitive radio networks.

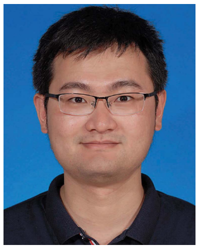
The seventeenth paper "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT" investigates the beamforming design for the artificial noise aided jamming of cognitive radio multiple-input single-output non-orthogonal multiple access with simultaneous wireless information and power transfer by using a nonlinear energy harvesting model. The beamformer is designed to minimize the transmission power for given harvested energy level and secrecy rate under perfect CSI and a bounded CSI error model.

The eighteenth paper "Robust secure beamforming for 5G cellular networks coexisting with satellite networks" studies the robust beamforming schemes for the physical layer security techniques in a scenario where a 5G cellular system uses the millimeter wave frequency and coexists with a satellite network. By developing a new physical layer security framework, and formulating a constrained optimization problem to maximize the secrecy rate at the second user while satisfying the interference level constraint at the primary user, this paper proposes two beamforming schemes, namely, heuristic beamforming scheme and iterative penalty function-based beamforming algorithm associated with the cases of coordinated and uncoordinated Eves, respectively.

The nineteenth paper "Resource management for device-to-device communication: a physical layer security perspective" studies the resource management of device-to-device (D2D) communication links underlaying cellular networks from a physical layer security perspective. Aiming to improve both security of the cellular users and spectral efficiency of D2D links, the authors have formulated the joint optimization of the power allocation and channel assignment as difficult mixed integer problem. Then, two algorithms are proposed for single-D2D and multi-D2D communications respectively. Finally, simulation results are provided to show that the win-win situation can be achieved by the proposed algorithms.

## Acknowledgment

The authors 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. Owing to the highly selective nature of JSAC, many interesting papers were not selected for our special issue, but we hope that these papers might appear elsewhere. They 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. They also thank Prof. M. Medard, JSAC Editor-in-Chief, the Executive Editor Laurel Greenidge, and the Senior Editor Prof. A. Jukan, for the effort and help they have provided for our special issue.



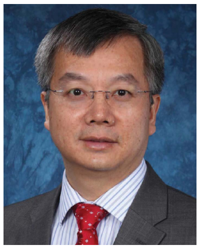
**Yongpeng Wu** (S'08–M'13–SM'17) received the B.S. degree in telecommunication engineering from Wuhan University, Wuhan, China, in 2007, and the Ph.D. degree in communication and signal processing from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2013.

During his doctoral studies, he conducted cooperative research with the Department of Electrical Engineering, Missouri University of Science and Technology, USA. He was a Senior Research Fellow with the Institute for Communications Engineering, Technical University of Munich, Germany, and a Humboldt Research Fellow and a Senior Research Fellow with the Institute for Digital Communications, University Erlangen-Nürnberg, Germany. He is currently a Tenure-Track Associate Professor with the Department of Electronic Engineering, Shanghai Jiao Tong University, China. His research interests include massive MIMO/MIMO systems, physical layer security, signal processing for wireless communications, and multivariate statistical theory.

Dr. Wu received the IEEE Student Travel Grants for the IEEE International Conference on Communications in 2010, the Alexander von Humboldt Fellowship in 2014, the Travel Grants for the IEEE Communication Theory Workshop in 2016, and the Excellent Doctoral Thesis Awards of the China Communications Society in 2016. He was an Exemplary Reviewer of the IEEE Transactions on Communications in 2015 and 2016. He is the Lead Guest Editor of the upcoming special issue Physical Layer Security for 5G Wireless Networks of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He is currently an Editor of the IEEE ACCESS and the IEEE COMMUNICATIONS LETTERS. He has been a TPC member of various conferences, including Globecom, ICC, VTC, and PIMRC.

**Ashish Khisti** received the B.A.Sc. degree in engineering sciences (electrical option) from the University of Toronto, and the S.M. and Ph.D. degrees in electrical engineering from the Massachusetts Institute of Technology. From 2009 to 2015, he was an Assistant Professor with the Electrical and Computer Engineering Department, University of Toronto, where he is currently an Associate Professor. He holds the Canada Research Chair with the University of Toronto.

Dr. Khisti was a recipient of an Ontario Early Researcher Award, the Hewlett-Packard Innovation Research Award, and the Harold H. Hazen Teaching Assistant Award from MIT. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY and is also the Guest Editor for the Proceedings of the IEEE Special Issue on Secure Communications via Physical-Layer and Information-Theoretic Techniques.



**Chengshan Xiao** (M'99–SM'02–F'10) received the B.Sc. degree in electronic engineering from the University of Electronic Science and Technology of China in 1987, the M.Sc. degree in electronic engineering from Tsinghua University in 1989, and the Ph.D. degree in electrical engineering from the University of Sydney in 1997.

He served as the Program Director with the Division of Electrical, Communications and Cyber Systems, USA National Science Foundation. He was a Senior Member of Scientific Staff with Nortel Networks, Ottawa, Canada, a Faculty Member with Tsinghua University, Beijing, China, the University of Alberta, Edmonton, Canada, the University of Missouri-Columbia, MO, USA, and the Missouri University of Science and Technology, Rolla, MO, USA. He is the Chandler Weaver Professor and the Chair of the Department of Electrical and Computer Engineering, Lehigh University. He also held visiting professor positions in Germany and Hong Kong. His research interests include wireless communications, signal processing, and underwater acoustic communications. He is the holder of several patents granted in USA, Canada, China, and Europe. His invented algorithms have been implemented into Nortel's base station radio products after successful technical field trials and network integration. He is a fellow of the Canadian Academy of Engineering.

Dr. Xiao served as an Elected Member of the Board of Governors, a member of the Fellow Evaluation Committee, the Director of Conference Publications, the Distinguished Lecturer of the IEEE Communications Society, and the Distinguished Lecturer of the IEEE Vehicular Technology. He received several distinguished awards, including 2014 Humboldt Research Award, the 2014 IEEE Communications Society Joseph LoCicero Award, the 2015 IEEE Wireless Communications Technical Committee Recognition Award, and the 2017 IEEE Communications Society Harold Sobol Award. He is the Awards Committee Chair of the IEEE Communications Society. He was the Technical Program Chair of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, the Technical Program Co-Chair of the 2017 IEEE Global Communications Conference, Singapore. He served as the founding Chair of the IEEE Wireless Communications Technical Committee. He also served as an Editor, an Area Editor, and the Editor-in-Chief for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS-I.

**Giuseppe Caire** (F'05) was born in Torino, Italy, in 1965. He received the B.Sc. degree in electrical engineering from the Politecnico di Torino, Italy, in 1990, the M.Sc. degree in electrical engineering from Princeton University in 1992, and the Ph.D. degree from the Politecnico di Torino in 1994.

He was a Post-Doctoral Research Fellow with the European Space Agency, ESTEC, Noordwijk, The Netherlands, from 1994 to 1995. He has been an Assistant Professor in telecommunications with the Politecnico di Torino, an Associate Professor with the University of Parma, Italy, and a Professor with the Department of Mobile Communications, Eurecom Institute, Sophia-Antipolis, France. He is currently a Professor of electrical engineering with the Viterbi School of Engineering, University of Southern California, Los Angeles, CA, USA, and an Alexander von Humboldt Professor with the Electrical Engineering and Computer Science Department, Technical University of Berlin, Germany.

His main research interests are in the field of communications theory, information theory, and channel and source coding. He received the Jack Neubauer Best System Paper Award from the IEEE Vehicular Technology Society in 2003, the IEEE Communications Society & Information Theory Society Joint Paper Award in 2004 and 2011, respectively, the Okawa Research Award in 2006, the Alexander von Humboldt Professorship in 2014, and the Vodafone Innovation Prize in 2015. He served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS from 1998 to 2001 and the IEEE TRANSACTIONS ON INFORMATION THEORY from 2001 to 2003. He has served on the Board of Governors of the IEEE Information Theory Society from 2004 to 2007 and as an Officer from 2008 to 2013. He was the President of the IEEE Information Theory Society in 2011.

**Kai-Kit Wong** (M'01–SM'08–F'16) received the B.Eng., M.Phil., and Ph.D. degrees from The Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively, all in electrical and electronic engineering. He took up academic and research positions with the University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group of Stanford University, and the University of Hull, U.K. He is the Chair in wireless communications with the Department of Electronic and Electrical Engineering, University College London, U.K.

His current research centers around 5G and beyond mobile communications, including topics such as massive MIMO, full-duplex communications, millimetre-wave communications, edge caching and fog networking, physical layer security, wireless power transfer and mobile computing, V2X communications, cognitive radios, fluid antenna communications systems, and remote ECG detection. He was a co-recipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2000 IEEE VTS Japan Chapter Award at the IEEE Vehicular Technology Conference in Japan in 2000, and a few other international best paper awards.

Dr. Wong is a fellow of IET. He serves on the editorial board of several international journals. He had served as an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS from 2009 to 2012 and an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2005 to 2011. He was also the Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Special Issue on virtual MIMO in 2013. He has been serving as the Senior Editor for the IEEE COMMUNICATIONS LETTERS since 2012 and also for the IEEE WIRELESS COMMUNICATIONS LETTERS since 2016. He is currently the Guest Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Special Issue on physical layer security for 5G.

**Xiqi Gao** (S'92–A'96–M'02–SM'07–F'15) received the Ph.D. degree in electrical engineering from Southeast University, Nanjing, China, in 1997.

He joined the Department of Radio Engineering, Southeast University, in 1992, where he has been a Professor of information systems and communications since 2001. From 1999 to 2000, he was a Visiting Scholar with the Massachusetts Institute of Technology, Cambridge, MA, USA, and Boston University, Boston, MA, USA. From 2007 to 2008, he visited the Darmstadt University of Technology, Darmstadt, Germany, as a Humboldt Scholar. His current research interests include broadband multicarrier communications, MIMO wireless communications, channel estimation and turbo equalization, and multirate signal processing for wireless communications. From 2007 to 2012, he served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. From 2009 to 2013, he served as an Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS.

Dr. Gao received the Science and Technology Awards of the State Education Ministry of China in 1998, 2006, and 2009, respectively, the National Technological Invention Award of China in 2011, and the 2011 IEEE Communications Society Stephen O. Rice Prize Paper Award in the Field of Communications Theory.