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

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 second issue has 20 technical papers with a broad range of topics as follows:

The first paper "Secure satellite-terrestrial transmission over incumbent terrestrial networks via cooperative beamforming" focuses on a coexistence system of satellite-terrestrial network and cellular network in the millimeter-wave (mmWave) bands, where the physical layer security problem is analyzed. Both the cooperative and non-cooperative secure transmission beamforming schemes are considered. To achieve this goal, non-cooperative and cooperative beamforming schemes are proposed to maximize the achievable secrecy rate in the paper. In addition, an iteration based approximate genetic algorithm is designed to solve the nonconvex secrecy rate maximization problem.

The second paper "Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications" considers hybrid MIMO phased-array time-modulated directional modulation scheme. The key is to divide the transmit array into multiple subarrays, where each subarray can be used to form a directional beam. On top of this, directional modulation scheme, in which on/off switch is incorporated to each antenna, is combined to enhance the secrecy. To find the transmit and receive aperture functions, least square algorithm is used.

The third paper "Secrecy rate analysis of UAV-enabled mmWave networks using matárn hardcore point processes" proposes the physical layer security in unmanned aerial vehicles (UAV)-enabled multi-antenna mmWave communication which is under realistic 3D environment include antenna gains and location. In addition, the authors further propose the

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).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSAC.2018.2832398

transmit jamming approach to degrade the eavesdropper's rate. Finally, the results show the optimal jamming factor of the UAV-enabled network will highly increase the average secrecy rate.

The fourth paper "Joint beamforming and jamming design for mmWave information surveillance systems" proposes the joint beamforming and jamming design in mmWave information surveillance system. A novel penalty dual decomposition algorithm has been proposed to jointly optimize the analog transmit and receive beamforming vector of the suspicious transmission link. The simulation results show that the proposed algorithm has better performance than the competing beamforming and jamming algorithm.

The fifth paper "Secure NOMA based two-way relay networks using artificial noise and full duplex" investigates the issue of secure communication in two-way relaying systems, where two users wish to exchange their NOMA signals via a trusted relay in the presence of single and multiple eavesdroppers. The artificial noise and full duplex techniques are combined to improve the secrecy performance.

The sixth paper "Secure communications in noma system: subcarrier assignment and power allocation" investigates the secure subcarrier and power allocation schemes for the NOMA two-way relay wireless networks in the presence of an eavesdropper without and with cooperative jamming. The proposed algorithms properly allocate resources to user pairs, and the performance of the secrecy energy efficiency of the system can be improved comparing to the conventional NOMA scheme.

The seventh paper "Intelligent interference exploitation for heterogeneous cellular networks against eavesdropping" studies physical layer security for a heterogeneous cellular network comprised of a macro cell and a small cell, where a passive eavesdropper is assumed to tap the confidential transmission of both the macro cell and small cell. A so-called interference-canceled underlay spectrum sharing (IC-USS) scheme is proposed to protect the macro-cell and small-cell transmissions against eavesdropping. Also, conventional overlay spectrum sharing (OSS) and interference-limited spectrum sharing (IL-USS) are considered as benchmark. The authors derive closed-form expressions of overall outage probability and intercept probability for the OSS, IL-USS, and IC-USS schemes. The secrecy diversity analysis is also conducted.

The eighth paper "Blind authentication at the physical layer under time-varying fading channels" proposes a new blind authentication scheme at the physical layer that combines the techniques of blind known interference cancellation and differential processing to implement authentication without requiring complicated processing procedure, such as channel estimation, message symbol recovery, etc.

The ninth paper "A new design paradigm for secure full-duplex multiuser systems" considers a full-duplex multiuser system where a full-duplex base station is designed to simultaneously serve both downlink and uplink users in the presence of half-duplex eavesdroppers. In particular, suboptimal resource allocation algorithms are proposed to maximize the minimum secrecy rate under different scenarios.

The tenth paper "Secrecy performance of finite-sized in-band selective relaying systems with unreliable backhaul and cooperative eavesdroppers" investigates the secrecy performance of a finite-sized in-band selective relaying system with M transmitters connected via unreliable backhaul links, N decode-and-forward relays, and K collaborative eavesdroppers. To send the source message to the destination, a transmitter-relay pair that achieves the highest end-to-end signal-to-noise ratio is selected for transmissions, while the K eavesdroppers combine all the received signals from the selected transmitter and relay using maximum ratio combining.

The eleventh paper "Physical detection of misbehavior in relay systems with unreliable channel state information" deals with the detection of misbehavior in a relay system, considering both cases that the relay may forward garbled information, and/or the relay system may provide unreliable CSI feedback. The action of the relay is classified into two categories, namely detectable and undetectable. For the detectable case, two algorithms are proposed respectively for cases with and without direct S-D link. For the undetectable case, it is proved that these kinds of attacks will not affect the system performance.

The twelfth paper "Secure transmission and self-energy recycling for wireless-powered relay systems with partial eavesdropper channel state information" studies robust secure beamforming design and relay power allocation problems in a wireless-powered full-phase relay system with self-energy recycling. A novel two-phase protocol is proposed. An alternative method is proposed to solve the challenging non-convex problem.

The thirteenth paper "Coordinated beamforming with artificial noise for secure swipt under non-linear EH model: centralized and distributed designs" proposes a power-efficient resource allocation for multicell secure simultaneous wireless information and power transfer systems. In particular, the proposed centralized and distributed algorithms take into account the non-linear energy harvesting circuit, imperfect channel state information, and the existence of potential eavesdropper.

The fourteenth paper "Hierarchical competition as equilibrium program with equilibrium constraints towards security-enhanced wireless networks" focuses on distributed resource competition in a network that constitutes security oriented and regular users. A multi-leader-follower game formulated is adopted. Furthermore, the paper formulates optimization problems with equilibrium constraints for a particular case of one security-oriented user as leader and a more general case of multiple security-oriented users. The solution to the optimization problem is given by successive convex approximation and local Nash equilibrium.

The fifteenth paper "Unified Interference Engineering for Wireless Information Secrecy" proposes a unified interference engineering strategy that combines various existing interference engineering strategies. This strategy enables an efficient and flexible utilization of the capabilities of multiple heterogeneous nodes for information secrecy protection. A theoretical framework for the feasibility analysis and algorithm design of the unified interference engineering strategy is established by exploiting tools from algebraic geometry. Based on this framework, transceivers and stream assignment have been designed in heterogeneous networks, which

achieves significant performance gain for wireless information secrecy.

The sixteenth paper "Social security aided D2D communications: performance bound and implementation mechanism" proposes a social security aware device to device (D2D) communication architecture that exploits social-domain trust for securing physical-domain communication. The system ergodic rate of social security aided communications is analyzed by using stochastic geometry, and numerical results show that the proposed social security aided D2D communication increases the system secrecy rate significantly compared to the scheme without considering social trust relation. Furthermore, in order to provide implementation mechanism, matching theory are utilized to implement efficient resource allocation among multiple users.

The seventeenth paper "Secure user-centric clustering for energy efficient ultra dense networks: design and optimization" studies user centric clustering of small cell base stations in a ultra dense small cell network, where the design objective is to achieve both throughput quality of service (QoS) and secrecy QoS with high energy efficiency. Two secure joint transmission strategies, namely dedicated jamming and embedded jamming are considered with both known and unknown eavesdropper channel state information. The optimization problems, which are shown to be NP-hard, are solved by decoupled heuristics. Through numerical studies, performance metrics are analyzed. In particular, the notion of security v.s. energy efficiency which exhibits a trade-off relationship is defined and investigated.

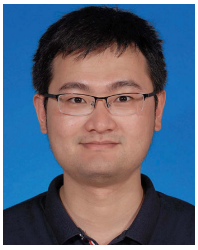
The eighteenth paper "Secure downlink transmission in the internet of things: how many antennas are needed?" studies the physical layer security in Internet of Things, where limited feedback resources are considered. The authors aim to investigate how many transmit antennas should be used for secure transmission. The closed-form expression for network secrecy throughput is derived. The formulated problem is non-convex and thus the authors develop an optimization framework involving the block coordinate descent algorithm and the one-dimensional search method.

The nineteenth paper "Tradeoff between delay and physical layer security in wireless networks" evaluates the tradeoff between the delay and the physical layer security in wireless networks. By combining the tools from stochastic geometry and queueing theory, this paper derives the close-formed results for the mean delay and the secrecy outage probability. The authors also analyze the effect of a simple transmission mechanism which splits a message into two packets.

The twentieth paper "Managing physical layer security in wireless cellular networks: a cyber insurance approach" presents a cyber insurance framework for wireless services, in which the network users pay a premium to the insurer in order to protect themselves from the loss due to cyber risk. Specifically, to assess the vulnerabilities of insured users, the service outage probability of a user is given in this paper. Meanwhile, a ruin probability of the insurer is analyzed.

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 their special issue, but we hope that these papers might appear elsewhere. They also thank all the Reviewers, who were very responsive to their repeated reminders about staying on schedule. Their critical comments and suggestions to the Authors contributed substantially to their 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 their special issue.



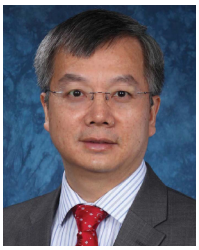
Yongpeng Wu (S'08–M'13–SM'17) received the B.S. degree in telecommunication engineering from Wuhan University, Wuhan, China, in 2007, and the Ph.D. degree in communication and signal processing from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2013.

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-N*ü*rnberg, 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.