This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead

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*

***Abstract*—Physical layer security which safeguards data confidentiality based on the information-theoretic approaches has received significant research interest recently. The key idea behind physical layer security is to utilize the intrinsic randomness of the transmission channel to guarantee the security in physical layer. The evolution towards 5G wireless communications poses new challenges for physical layer security research. This paper provides a latest survey of the physical layer security research on various promising 5G technologies, including physical layer security coding, massive multiple-input multiple-output, millimeter wave communications, heterogeneous networks, non-orthogonal multiple access, full duplex technology, etc. Technical challenges which remain unresolved at the time of writing are summarized and the future trends of physical layer security in 5G and beyond are discussed.**

I. Introduction

Nowadays, 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 [1]. Basically, the security today relies on bit-level cryptographic techniques and associated protocols at various levels of the data processing stack. These solutions have drawbacks: standardized protections within public wireless networks are not secure enough, and many of their weaknesses are well known; even if enhanced ciphering and authentication protocols exist, they occur strong constraints and high additional costs for the users of public networks, etc. Therefore, new security approaches are issued from information theory fundamentals and focus on the secrecy capacity of the propagation channel, which is referred as physical layer security [2–10].

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

A. Khisti is with Signal Multimedia and Security Lab, University of Toronto, Bahen Building, Toronto, Canada (Email: akhisti@ece.utoronto.ca).

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

G. Caire is with Institute for Telecommunication Systems, Technical University Berlin, Einsteinufer 25, 10587 Berlin, Germany (Email: caire@tu-berlin.de).

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

X. Q. Gao is with the National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, P. R. China (Email: xqgao@seu.edu.cn).

The advantages of employing physical layer security techniques for 5G networks compared to that of cryptography techniques are on two folds. First, physical layer security techniques do not rely on computational complexity. As a result, even if the eavesdroppers (unauthorized smart devices) in the 5G networks are equipped with power computational devices, the secure and reliable communications can still be achieved. In contrast, the security of computation-based cryptography techniques will be compromised if the eavesdroppers' devices have sufficient computational capacities for hard mathematical problem. The 5G networks must simultaneously meet various different service requirements with hierarchical architectures [1], which implies that devices are always connected to the nodes with different powers and different computational capacity levels. Second, the structures of 5G networks are usually decentralized, which implies devices may randomly connect in or leave the network at any time instants. For this case, cryptographic key distribution and management become very challenging. As a result, physical layer security techniques can be used to either perform secure data transmission directly or generate the distribution of cryptography keys 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.

Considering the potential of physical layer security for 5G wireless communications, the opportunities and challenges on how the innovative 5G technologies achieve a high security level at the physical layer deserves to receive more attention from the research community. The purpose of this paper is to provide a comprehensive summarization of the latest physical layer security research results on the key technologies of 5G wireless networks. In particular, we focus on the following typical technologies:

1) Physical layer security coding: Although the first physical layer security code appears around 1970s, to design explicit security codes which can be used in practical communication systems is still challenging. We review the state of art of three important physical layer security codes, including low-density parity-check (LDPC) codes, polar codes, and lattice codes.
2) Massive MIMO: Deploying large antenna arrays significantly increases the spatial dimension of wireless

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

channels. We discuss how to exploit the extra spatial resources to effectively combat the eavesdropper and guarantee the secure communication at physical layer. Both the passive and the active eavesdropper scenarios are described.

3) Millimeter wave (mmWave) communications: Abundant spectra within the high frequency band may result in significant different propagation environments for physical layer secure communication. To understand mmWave secure transmission more clearly, research works for both point-to-point and network mmWave communication systems are introduced.
4) Heterogeneous networks: In general, a heterogeneous network is consisted of various tiers of networks which operates in the same system bandwidth. We describe in details on how to design transmission schemes to secure multi-tier communications simultaneously.
5) Non-orthogonal multiple access (NOMA): As a multiple access technology, the security of NOMA communications is an important concern which should be paid more attention. The physical layer security technology can be combined with NOMA to tackle this issue. The physical layer security of NOMA is a new and promising research frontier, where a few relevant research results so far will be summarized.
6) Full duplex technology: The full duplex technology brings both the opportunity and the challenge for the physical layer security communication. On one hand, the full duplex technology enables the receiver to generate additional AN to interferer the eavesdropper. On the other hand, the eavesdropper with full duplex technology can actively attack the communication process while eavesdropping. In general, we discuss four categorizations of full-duplex physical layer security communications, including the full duplex receiver, the full duplex transmitter and receiver, the full duplex base station, and the full duplex eavesdropper.

Moreover, we also introduce other important results for physical layer security for future wireless networks, such as the joint physical-application layer secure transmission design, the practical test bed design for physical layer security, etc. The future research challenges of physical layer security in 5G and beyond are also discussed.

It should be noted that there are already many survey and tutorial papers for physical layer security research [11–14]. However, a comprehensive study of physical layer security techniques for 5G wireless networks is still missing, which is the main contribution of this paper. The most relevant work is [12], where physical layer security for only three 5G techniques are briefly discussed in a big picture without introducing the research results in details. In contrast, our paper provides a comprehensive detailed summarization of latest research results on physical layer security for 5G wireless networks. Moreover, the corresponding research challenges at current stage are also discussed.

II. Physical Layer Security Coding

Most works on physical layer security are based on non-constructive random-coding arguments to establish the theoretic results. Such results demonstrate the existence of codes that achieve the secrecy capacity, but are of little practical usefulness. The construction of practical codes for physical layer security has received more attentions recently. In this section, we review recent works on the construction of three practical codes for physical layer security, which might be used in 5G communications.

A. LDPC Codes

In [15], A. Thangaraj *et al.* establish a connection between capacity-achieving codes and secrecy based on the metric of weak secrecy. It is proved in [15] that for an arbitrary wiretap channel, the perfect secrecy can be achieved by using codes that achieve the capacity of the eavesdropper's channel. This conclusion provides an conceptual construction for designing the secrecy transmission coding schemes over the general wiretap channel. Moreover, the authors in [15] use this idea to design LDPC codes based on nested sparse graph codes and a coset coding scheme over a wiretap channel for a noiseless channel of the desire user and a binary erasure channel (BEC) of the eavesdropper. The constructed codes are the first secrecy-capacity-achieving LDPC codes in terms of weak secrecy. Later, V. Rathi *et al.* generalizes this coding scheme to BEC of both the desire user and the eavesdropper by designing the two-edge type LDPC codes [16]. However, the proposed construction results in some degree one variable nodes in the ensemble for the desire user's channel. To circumvent this problem, numerical methods are used to optimize the degree distribution of the two edge-type LDPC ensembles. Some relatively simple ensembles are found, which achieve good secrecy performance and are close to the secrecy capacity. A. Subbramanian *et al.* construct LDPC codes with large girth block length based on Ramauja graph for a noiseless channel of the desire user and BEC of the eavesdropper [17], which achieve strong secrecy with lower rates.

LDPC codes have been designed for the Gaussian wiretap channel. The physical-layer security communication is realized in [18] by punctured LDPC codes under the criterion of bit-error rate (BER), where the secrecy information bits are hidden in the punctured bits. Therefore, these information bits are not transmitted through the channel but can be decoded at the receiver side based on the non-punctured part of the codeword. This coding scheme can yield a BER close to 0.5 at the eavesdropper's side while significantly reduces the security gap defined in [18] comparing to the non-punctured LDPC codes. However, the punctured LDPC codes result in higher power transmission comparing to the non-punctured LDPC codes. To solve this problem, M. Baldi *et al.* propose a nonsystematic coded transmission design by scrambling the information bits [19]. It is shown in [19] that this scrambling technique achieves security gap comparable to that design based on puncturing but without increasing the transmit power. This scrambling design has been extended to parallel Rayleigh distributed channels [20]. By exploiting the equivocation rate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

of eavesdropper's channel as an optimization criterion, M. Baldi *et al.* propose a code design algorithm in the finite codeword length regime [21]. Based on this algorithm, irregular LDPC codes which approach the ultimate performance limits with small codeword lengths are constructed. A brief summary of above work is given in Table I.

B. Polar Codes

For the weak secrecy criterion, H. Mahdavifar *et al.* construct a polar coding scheme to achieve the secrecy capacity for the symmetric binary-input memoryless wiretap channel under the condition that the main channel of the eavesdropper is degraded to the main channel of the desired user [22]. The main idea in [22] is to select only those bit channels which are good for both the desired user and the eavesdropper to transmit random bits. Moreover, those bit channels which are good for desired user but bad for the eavesdropper are used to transmit information bits. It is proved in [22] that this coding scheme can achieve the secrecy capacity. Furthermore, E. Hof *et al.* and M. Andersson *et al.* independently prove that this coding scheme achieves the entire *rate-equivocation region* (Defined in [23]) in [24] and [25], respectively. O. O. Koyluoglu *et al.* apply this coding scheme into a key agreement problem over the block fading wiretap channel [26]. The secure polar code is used for each fading block, from which the secrecy keys are generated based on standard privacy amplification techniques. Y.-P. Wei *et al.* develop polar codes for the general wiretap channel by relaxing the degraded and the symmetric constraints [27]. In addition, this coding scheme is extended to the multiple access wiretap channel (MA-WC), the broadcast channel with confidential message (BC-CM), and the interference channel with confidential message (IC-CM). On the other hand, S. A. A. Fakoorian *et al.* design polar codes to achieve the secrecy capacity for the arbitrary deterministic wiretap channel [28]. A polar coding scheme for bidirectional relay networks with common and confidential messages and the decode-and-forward protocol is proposed in [29].

For the strong security criterion, E. Sasoğlu *et al.* design a multi-block polar coding scheme [30] which achieves both security and reliability for the same wiretap channel model as in [22]. T. C. Gulcu *et al.* provide a simple coding scheme based on polar codes to achieve the secrecy capacity of the general wiretap channel (not necessarily degraded or symmetric) [31]. This coding scheme is also extended to achieve the capacity region of discrete memoryless BC-CM. Independently, R. A. Chou *et al.* design a more general (holds for more general conditions as given in [32, Fig. 1]) polar coding scheme for discrete memoryless BC-CM [32]. A brief summary of above work is given in Table II.

Other polar coding schemes for wiretap channels include the concatenation of two polar codes for the general wiretap channel [33], the concatenation of polar and LDPC codes to minimize the security gap [34], etc.

C. Lattice Codes

For wiretap lattice codes, J.-C. Belfiore *et al.* define a notation of secrecy gain, which reflects the eavesdropper's correct decoding probability [35, 36]. Asymptotic analysis of the secrecy gain shows that it scales exponentially with the dimension of the lattice. Also, examples of wiretap lattice codes designed based on this secrecy gain criterion for the Gaussian wiretap channel are given in [36]. A.-M. E.-Hytönen proves that the symmetry points in the secrecy function of the even extremal unimodular lattices achieve the secrecy gains [37]. In addition, a method to examine the secrecy gains for arbitrary unimodular lattices is proposed in [37]. F. Lin *et al.* calculate the symmetry points of four extremal odd unimodular lattices and 111 nonextremal unimodular lattices for dimensions $8 < n \leq 23$. It is validated that these symmetry points are actually secrecy gains via the method in [38]. Based on these secrecy gains, the best wiretap lattice codes are determined. The lattice codes which are optimal based on the secrecy gain criterion for the Rayleigh fading wiretap channels are designed in [39].

From information theory point of view, L.-C. Choo *et al.* construct a nested lattice code for the Gaussian wiretap channel based on the equivocation rate, which can meet both the reliability and the weak secrecy criterions [40]. C. Ling *et al.* further design wiretap lattice codes achieving the strong secrecy for the Gaussian wiretap channel [41]. Moreover, L.-C. Choo *et al.* propose a superposition lattice code for the Gaussian BC with confidential message with the strong secrecy [42]. A brief summary of above work is given in Table III.

Other lattice code designs for the wiretap channel includes: nested lattices code designs for cooperative jamming, interference channels, and the relay networks [10, 43, 44], the security of the continuous mod-lattice channel with feedback [45], etc.

III. Physical Layer Security in Massive MIMO Systems

Massive MIMO is a promising approach for efficient transmission of massive information and is regarded as one of "big three" 5G technologies [46]. In this section, we review the current security threats and countermeasures of massive MIMO technology based on passive and active eavesdropper scenarios, respectively.

A. Passive Eavesdropper Scenarios

Physical layer security for massive MIMO systems with passive eavesdroppers has been recently studied. J. Zhu *et al.* study secure massive MIMO transmissions for multi-cell multi-user systems over i.i.d. Rayleigh fading channel [47], where a passive eavesdropper attempts to decode the information sent to one of the users. The impact of multi-cell interference and pilot contamination on the achievable erogdic secrecy rate are analyzed and several matched filtering precoding and artificial noise (AN) generation designs are proposed to degrade the eavesdropper's channel and protect the desired user's channel. For the same system model, regularized channel inversion and AN transmission schemes are designed in [48] to further improve the secrecy rate performance. J. Wang *et al.* investigate AN-aided secure massive MIMO transmission over i.i.d. Rician fading channel [49]. For single-cell

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

TABLE I: LDPC Codes for Physical Layer Security

Paper	Main Channel	Eve Channel	Criterion	Constituent Codes
A. Thangaraj *et al.* [15]	Noiseless	BEC	Weak secrecy	Duals of LDPC
V. Rathi *et al.* [16]	BEC	BEC	Weak secrecy	Two-edge LDPC
A. Subramanian *et al.* [17]	Noiseless	BEC	Strong secrecy	Duals of LDPC
D. Klinc *et al.* [18]	Gaussian	Gaussian	BER	Punctured LDPC
M. Baldi *et al.* [19]	Gaussian	Gaussian	BER	Non-punctured LDPC
M. Baldi *et al.* [20]	Parallel Rayleigh	Parallel Rayleigh	BER	Non-punctured LDPC
M. Baldi *et al.* [21]	Gaussian	Gaussian	Equivocation rate of Eve	Irregular LDPC

TABLE II: Polar Codes for Physical Layer Security

Paper	Channel	Criterion	Main contribution
H. Mahdavifar *et al.* [22]	Symmetric binary-input memoryless degraded wiretap channel	Weak secrecy	Achieve secrecy capacity
[24, 25]	Symmetric binary-input memoryless degraded wiretap channel	Weak secrecy	Achieve rate-equivocation region
O. O. Koyluoglu *et al.* [26]	Symmetric binary-input memoryless degraded wiretap channel	Weak secrecy	Generate a key agreement
Y.-P. Wei *et al.* [27]	General wiretap channel MA-WC, BC-CM, IC-CM	Weak secrecy	Achieve secrecy capacity Achieve secrecy rate regions
S. A. A. Fakoorian *et al.* [28]	Deterministic wiretap channel	Weak secrecy	Achieve secrecy capacity
M. Andersson *et al.* [29]	Bidirectional relay networks with confidential messages	Weak secrecy	Achieve capacity-equivocation region
E. Sasoğlu *et al.* [30]	Symmetric binary-input memoryless degraded wiretap channel	Strong secrecy	Achieves both security and reliability
T. C. Gulcu *et al.* [31]	General wiretap channel	Strong secrecy	Achieve secrecy capacity
R. A. Chou *et al.* [32]	Discrete memoryless BC-CM	Strong secrecy	Achieve secrecy capacity

TABLE III: Lattice Codes for Physical Layer Security

Paper	Channel	Criterion	Main contribution
J.-C. Belfiore *et al.* [35, 36]	Gaussian wiretap channel	Secrecy gain	Define secrecy gain
A.-M. E.-Hytönen *et al.* [37]	Gaussian wiretap channel	Secrecy gain	Propose a method to examine the secrecy gain
F. Lin *et al.* [38]	Gaussian wiretap channel	Secrecy gain	Construct best lattice codes for dimensions $8 < n \leq 23$
J.-C. Belfiore *et al.* [39]	Rayleigh wiretap channel	Secrecy gain	Construct a wiretap lattice code
L.-C. Choo *et al.* [40]	Gaussian wiretap channel	Weak secrecy	Construct a nested lattice code
C. Ling *et al.* [41]	Gaussian wiretap channel	Strong secrecy	Design wiretap lattice codes
L.-C. Choo *et al.* [42]	Gaussian BC with confidential message	Strong secrecy	Propose a superposition lattice code

multiuser massive MIMO systems with distributed antennas, K. Guo *et al.* design three secure-constrained power allocation schemes [50] by maximizing the minimum user's signal-to-interference-noise ratio (SINR) subject to the eavesdropper's SINR and the sum power constraint and minimizing the sum transmit power subject to SINR constraints of users and the eavesdropper, respectively. Y. Wu *et al.* investigate secure transmission designs for large-scale MIMO systems with finite alphabet inputs [51]. Power allocation schemes for relay-aided large-scale MIMO systems are proposed in [52, 53]. A brief summary of above work is given in Table IV.

Other secure massive MIMO work with passive eavesdroppers include: secure transmission for massive MIMO systems with limited radio frequency and hardware impairments [54, 55], secure strategies in presence of a massive MIMO eavesdropper [56, 57], secrecy outage probability analysis for massive MIMO systems [58], etc.

B. *Active Eavesdropper Scenarios*

Most physical layer security research work assume that perfect channel knowledge of the legitimate user is available at the transmitter and do not consider the procedure required to obtain this channel. In time duplex division (TDD) communication systems, the users in an uplink training phase will send pilot signals to the base station (BS) to estimate the channel for the subsequent downlink transmission. From the eavesdropper's point of view, it can actively send the same pilot signals as the users to attack this uplink channel training phase and hence significantly increase its eavesdropping capability [59].

This pilot contamination attack causes a serious secrecy threat to TDD-based massive MIMO systems. On one hand, large antenna arrays beamforming leads to the hardening of the channel, which prevents the exploitation of channel fluctuations caused by fading to improve the secrecy performance. On the other hand, as illustrated in Figure 1, the pilot contamination attack enables the transmitter to beamform towards the the eavesdropper instead of the desired user. If the eavesdropper's pilot power is sufficiently large, a positive secrecy rate may not be achievable. This is significantly different from the conventional idea that massive MIMO naturally facilitates secure communication since the large antenna arrays can generate very narrow beams focusing on the desired users without spilling over the signal power in other directions. In the first time, Y. Wu *et al.* systematically analyze the secrecy threat caused by the pilot contamination attack for multi-cell multi-user massive MIMO systems over correlated fading channels [60]. Then, a matched filter precoding and AN generation design and a null space design are provided in [60] to combat the pilot contamination attack for weakly correlated channels and highly correlated channels, respectively. A unified design which combines the matched filter precoding and AN generation design and the null space design is also proposed. Simulations indicate that these designs can guarantee reliable secure communication under the pilot contamination attack, as shown in Fig. 2. At the same time, Y. O. Basciftci *et al.* study the pilot contamination attack problem for single-cell multi-user massive MIMO systems over i.i.d. fading channels [61]. It is proved in [61] that if the pilot contamination attack does not exist, the maximum secure degree of freedom (DoF) of massive MIMO systems is the same as the maximum DoF of massive MIMO systems when the eavesdropper does not exist. However, if the pilot contamination attack exists, the maximum secure DoF of massive MIMO systems could be zero. To defense the pilot contamination attack, Y. O.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

TABLE IV: Secure Massive MIMO with Passive Eavesdropper

Paper	System Model	Main Contribution
J. Zhu *et al.* [47]	Multi-cell multi-user, one desired user, one eavesdropper, i.i.d. Rayleigh	Matched filtering precoding and AN generation designs
J. Zhu *et al.* [48]	Multi-cell multi-user, one desired user, one eavesdropper, i.i.d. Rayleigh	Regularized channel inversion and AN generation designs
J. Wang *et al.* [49]	One desired user, multiple eavesdroppers, i.i.d. Rician	AN-aided secure transmission designs
K. Guo *et al.* [50]	Single-cell, multiple desired users, one eavesdropper, correlated Rayleigh	Distributed power allocation under security-constraints
Y. Wu *et al.* [51]	One desired user, one eavesdropper, perfect CSI	Secure transmission with finite alphabet inputs
X. Chen *et al.* [52, 53]	Relay-aided, one desired user, one eavesdropper, i.i.d. Rayleigh	Secrecy performance analysis and power allocation designs

Basciftci *et al.* expand cardinality of the pilot signal set and hide the pilot signal within the enlarged set. On the other hand, S. Im *et al.* employ a secret key agreement protocol for single-cell multi-user massive MIMO systems with the pilot contamination attack [62]. An estimator is designed at the BS side to evaluate the information leakage. Then, the BS and the desired user perform the reliable secure communication by adjusting the lengths of the secrecy key based on the estimated information leakage. A brief summary of above work is given in Table V.

Other secure massive transmission against active eavesdropper includes pilot retransmission strategies [63] and the secure transmission design based on game theory [64], etc.

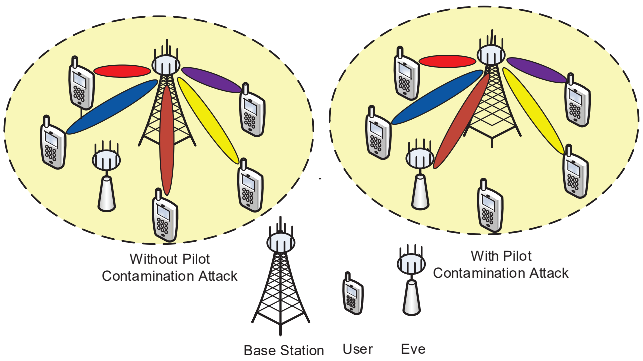


Fig. 1: Pilot contamination attack on massive MIMO systems

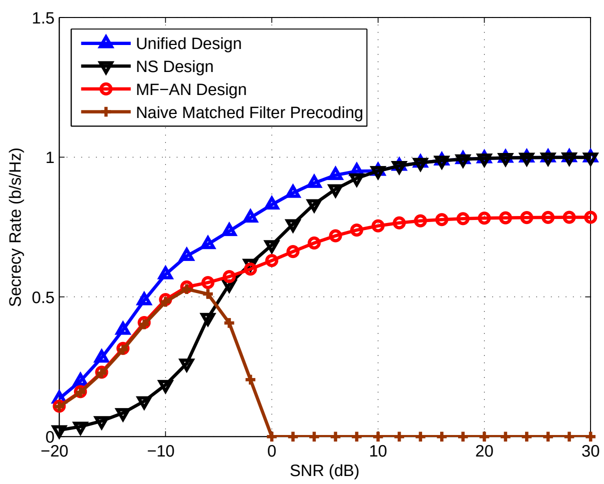


Fig. 2: Exact secrecy rate vs. the SNR for 128 antennas massive MIMO systems and different precoding designs. Experimental results extracted from [60].

IV. Physical Layer Security for mmWave Communications

One of the most promising potential 5G technologies under consideration is the use of high-frequency signals in the millimeter-wave frequency band that could allocate more bandwidth to deliver faster, higher-quality video and multimedia content [65]. Comparing to micro-Wave networks, the mmWave networks have various new characteristics such as the large number of antennas, short range and highly directional transmissions, different propagation laws, and sensitive to blockage effects, etc. Therefore, the secure mmWave communications will be different from the conventional secure micro-Wave communications.

L. Wang *et al.* first show that the high secrecy throughout can be achieved for a point-to-point mmWave communication system with multiple eavesdroppers [66]. Assuming the uniform linear array (ULA) at the transmitter, an analog beamforming with phase shift is employed based on the perfect CSI of the desired user. The ergodic secrecy rate expressions are derived for both delay-tolerant and delay-limited transmission modes. In particular, simulations show that with a large number of transmit antennas, the delay-tolerant transmission mode can achieve multi-gigabit per second secrecy rate at mmWave frequencies. Motivated by this, Y. Ju *et al.* further evaluate the secrecy performance of the mmWave communication over the multiple-input, single-output, single-antenna eavesdropper (MISOSE) wiretap channel [67]. Based on the perfect CSI of the desired user and the statistical CSI of the eavesdropper, the secrecy outage probability and secrecy throughout of the matched filter precoding and AN generation design are analyzed. The obtained results reveal that the overlap between the desired user's and the eavesdropper's spatially resolvable paths has an significantly important impact on the secrecy performance of the mmWave communication. X. Tian *et al.* investigate the hybrid precoder design for mmWave multiple-input, multiple-output, multiple-antenna eavesdropper (MIMOME) wiretap channel [68].

Based on the stochastic geometry framework, C. Wang *et al.* investigate the downlink secure communication for mmWave cellular networks as shown in Fig. 3 [69]. The BSs perform the directional beamforming with the intended users' perfect CSI and both the legitimate users and eavesdroppers in the networks are equipped with a single omnidirectional antenna. As indicated in Fig. 4, it is shown that narrowing the beam width of directional beamforming antenna with more focused array gain is beneficial for increasing the secrecy performance of mmWave networks. In addition, the effects of antenna array pattern, base station intensity, and AN generation on secrecy performance are investigated in [69]. For the same system model, S. Vuppala *et al.* further analyze the secrecy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

TABLE V: Secure Massive MIMO with Active Eavesdropper

Paper	System Model	Main Contribution
Y. Wu *et al.* [60]	Multi-cell multi-user, one desired user one eavesdropper, correlated Rayleigh	Systematically analyze the secrecy threat caused by the pilot contamination attack Propose efficient schemes to combat the pilot contamination attack
Y. O. Basciftci *et al.* [61]	Single-cell multi-user, multiple desired users one eavesdropper, i.i.d. Rayleigh	Analyze maximum secure DoF with the pilot contamination attack Propose a scheme to hide the pilot signal under the pilot contamination attack
S. Im *et al.* [62]	Single-cell multi-user, one desired user one eavesdropper, i.i.d. Rayleigh	Employ secret key agreement protocol with the pilot contamination attack Adjust the lengths of the secrecy key based on the estimated information leakage

performance for the mmWave and the micro-Wave hybrid communication [70]. It is revealed in [70] that the blockages in mmWave networks can decrease the secrecy outage probability.

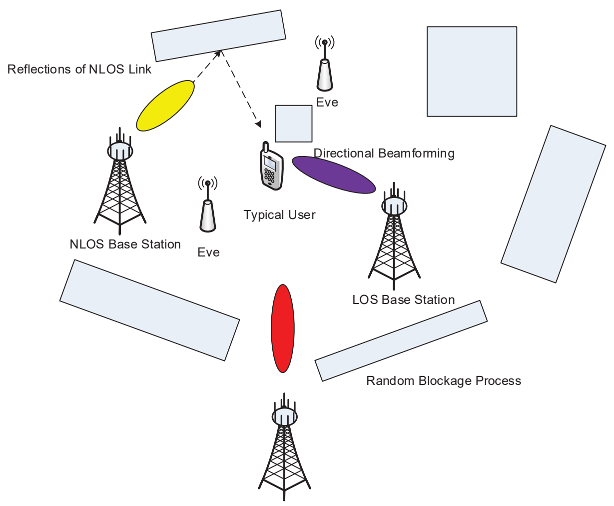


Fig. 3: Downlink secure communication for the mmWave cellular network

Y. Zhu *et al.* investigate the physical layer security for large-scale mmWave ad hoc networks, which are modeled based on stochastic geometry [71]. The directional beamforming is used between the transmitters and the desired receivers and the corresponding average secrecy rate is derived. For the special case of ULA, an explicit expression for the average secrecy rate is obtained, which reveals that using more antennas at the transmitters is beneficial for suppressing the array gains at the eavesdroppers' side. The proper power allocation between the transmit signal and AN is also discussed. S. Gong *et al.* investigate the secure precoding design for mmWave two-way amplify-and-forward (AF) MIMO relaying networks by exploiting the global perfect CSI [72]. To reduce the hardware cost and power consumption for the mmWave communication, an additional rank constraint is posed on the precoding matrix at the relay to control the number of analog-to-digital converters in the system.

The mmWave communication system is usually equipped with a large number of antennas at the transmitter with a limited number of radio frequency (RF) chains. To take advantage of this point, N. Valliappan *et al.* consider another approach by using an antenna subset modulation (ASM) technique to reach secure mmWave communication at physical layer [73]. The proposed approach utilizes a subset of antenna array to formulate a directional modulation signal intended for the desired user. By randomly choosing the antenna subset for

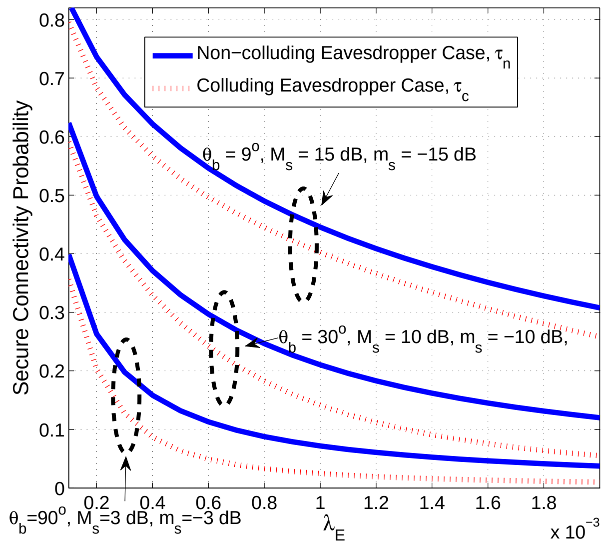


Fig. 4: Secrecy connectivity probability of mmWave cellular networks. Experimental results extracted from [69]. θ_b, M_s, m_s denote the beam width of the main lobe, the array gain of the main lob, and the array gain of the sidelobe of the directional beamforming, respectively. λ_E denote the intensity of eavesdroppers.

each symbol, the received signal for the undesired user becomes a randomized noise. Therefore, the secure transmission is achieved. M. E. Eltayeb *et al.* further extended this ASM technique to mmWave vehicular communication systems [74]. A brief summary of above work is given in Table VI.

From the eavesdropper's point of view, the work in [75] also considers the potential attack in mmWave communication. It is shown in [75] that even by using highly directional mmWaves, the reflection signals caused by small-scale physical objects will be beneficial to the eavesdropper. In some cases, the achievable secrecy rate can be decreased to zero by the attack.

V. Physical Layer Security in Heterogeneous Networks

The 5G heterogeneous networks should intelligently and seamlessly integrate multiple nodes to form a multi-tier hierarchical architecture, including the *macro cell tiers* with high-power nodes for large radio coverage areas, the *small cell tiers* with low-power nodes for small radio coverage areas, the *device tiers* which support device to device communications, etc. Fig. 5 shows a typical 4-tier macro/pico/femto/D2D heterogeneous network with users and eavesdroppers. This multi-tier architecture brings new challenges to the investi-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

TABLE VI: Secure mmWave Communications

Paper	System Model	CSI	Objective
L. Wang *et al.* [66]	Point-to-point MISO Multiple single-antenna eavesdroppers	Perfect CSI of the desired user Statistical CSI of eavesdroppers	Analyze ergodic secrecy rate
Y. Ju *et al.* [67]	MISOSE wiretap channel	Perfect CSI of desired user Statistical CSI of the eavesdropper	Analyze secrecy outage probability Analyze secrecy throughout
X. Tian *et al.* [68]	MIMOME wiretap channel	Perfect CSI of desired user Perfect CSI/No CSI of the eavesdropper	Hybrid precoders design
C. Wang *et al.* [69]	Stochastic geometry cellular networks	Perfect CSI of desired user Statistical CSI of the eavesdropper	Analyze secure connectivity probability Evaluate the effect of AN
S. Vuppala *et al.* [70]	Stochastic geometry cellular networks MmWave/micro-Wave hybrid communication	Perfect CSI of the desired user Statistical CSI of the eavesdropper	Analyze the secrecy outage probability
Y. Zhu *et al.* [71]	Stochastic geometry mmWave ad hoc networks	Perfect CSI of desired user Statistical CSI of the eavesdropper	Analyze the average secrecy rate
S. Gong *et al.* [72]	AF MIMO relay networks A multiple-antenna eavesdropper	Global perfect CSI	Secrecy precoders design
N. Valliappan *et al.* [73]	MISO, limited RF chains Single-antenna eavesdroppers	Perfect CSI of the desired user No CSI of the eavesdropper	Formulate directional modulation
M. E. Eltayeb *et al.* [74]	MISO, a single RF chain (vehicular systems) A single-antenna eavesdropper	Perfect CSI of the desired user No CSI of the eavesdropper	Formulate directional modulation

gation of physical layer security compared to the conventional single-tier topology. For example, the locations of the high/low power nodes will have a significant impact on the physical layer security design, which need to be modeled and analyzed properly. The optimal selection policy for each user among high/low power nodes under security constraints becomes difficult. The protection of confidential and privacy data between connected devices against data leakage requires sophisticated designs. Moreover, heterogeneous networks may introduce severe cross-tier interference. This should be taken into consideration when designing the reliable and secure data transmission schemes. In addition, users are accessible to an arbitrary tier, e.g., open access. Therefore, specific user association policies that coordinate both quality of service and secrecy are necessary.

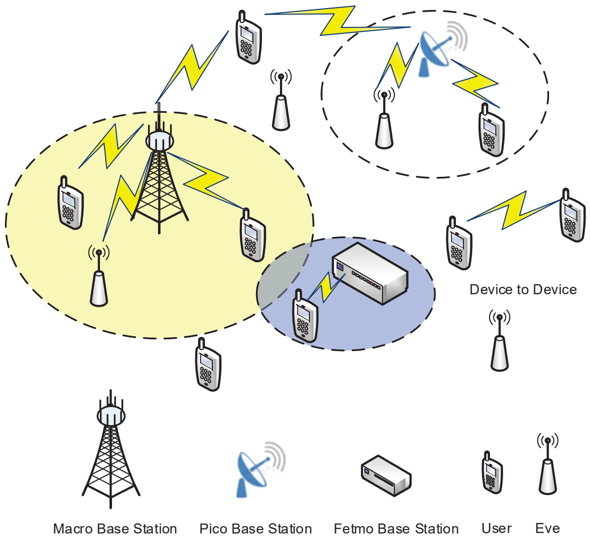


Fig. 5: A 4-tier macro/pico/femto/D2D heterogeneous network with users and eavesdroppers.

T. Lv *et al.* first study the physical layer security in a downlink two-tier heterogeneous network with multiple single-antenna users and a single-antenna eavesdropper in each cell [76]. Both the orthogonal spectrum allocation (OSA) scheme and the secrecy-oriented non-orthogonal spectrum allocation (SONOSA) scheme are considered. For OSA scheme, no interference from other cells exists and a transmit strategy to maximize the secrecy rate of one desired user under the quality of service (QoS) constraints of other users is proposed. For SONOSA, some femtocell base stations near the eavesdropper are allocated the same spectrum efficiency as the macrocell base station. Then, these femtocell base stations cooperate to generate the maximal interference at the eavesdropper side while guaranteeing the QoS requirements for the femtocell users. H. Wu *et al.* propose a user association policy by comparing the average received signal at the desired user with a given threshold [77]. Then, assuming both the inter-and intra-cell interference do not exist, closed-form expressions of secrecy outage probability are obtained for a downlink K-tier heterogeneous network with single-antenna nodes by modeling the locations of the nodes as independent Poisson Point Processes (PPPs). Furthermore, Y. J. Tolossa *et al.* derive the average secrecy rate expression under the association policy that any potential base station who provides kth largest path gain to the user can be selected as the association base station [78]. For a downlink K-tier heterogeneous network with only intra-cell interference, M. Xu *et al.* propose a dynamic coordinated multipoint transmission (CoMP) scheme to increase the secure communication coverage [79].

By considering both inter-and intra-cell interference, H.-M. Wang *et al.* obtain both secrecy and connection probabilities of a downlink K-tier heterogeneous network based on a truncated average received signal power user association policy [80]. A trade off between secrecy and connection probabilities in terms of association threshold, base station density, and power allocation between the useful signal and AN is revealed. The network-wide secrecy throughout and minimum secrecy throughput per user subject to both secrecy and connection probability constraints are further analyzed. W. Wang *et al.* derive closed expressions of secrecy and connection probabilities for a downlink small cell network [81]. The obtained results indicate that increasing the base station density is beneficial for both secrecy and connection outage probability performance. The performance of a uplink two-tier heterogeneous network is investigated in [82]. By using two-dimensional PPPs to approximate the summation of all interference in the whole space, the authors derive the exact expressions for the success-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

ful connection and secrecy outage probabilities. The secure transmission with wireless information and power transfer in a downlink two-tier heterogeneous network is studied in [83]. A brief summary of above work is given in Table VII.

VI. Physical Layer Security of NOMA

Given the scarce bandwidth resource, NOMA plays a crucial role for providing large system throughput, high reliability, improved coverage, low latency, and massive connectivity in 5G wireless networks [84]. As a result, NOMA has been recognized as an important enabling technology in 5G wireless communication systems. Because of the spectral efficiency benefit, NOMA has been recently included in 3GPP long term evolution advanced (LTE-A), which further evidences the importance of NOMA in future wireless networks. Thus, providing an unrivalled level of security for NOMA technology is one of the top priorities in the design and implementation of the 5G wireless networks. A significant effort is needed to efficiently combine physical layer security with NOMA. However, some challenges need to be resolved during the design process, such as the dissimilar transmit powers and heterogeneous security requirements of users. In addition, cooperation among users offers an interesting option to enhance the secrecy performance.

Y. Zhang *et al.* first study the secure NOMA transmission for a single-antenna, one transmitter, multiple users, and one eavesdropper system with perfect CSI of the users and no CSI of the eavesdropper [85]. Perfect successive interference cancellation (SIC) is performed at each user. The closed-formed expression of the optimal power allocation policy which maximizes the secrecy sum rate under each user's QoS constraint is derived. For the same CSI assumption, Y. Liu *et al.* further investigate the secure transmission for NOMA networks [86], as shown in Fig. 6. An eavesdropper-exclusion zone is established. To reduce the SIC complexity at the receiver, a user paring scheme is employed, where one user in the internal zone and one user in the external zone are allocated the same resource slot. When the base station only has single antenna, the secrecy outage probability is analyzed. Moreover, the secrecy diversity order is obtained, which reveals that the user with the weaker channel in the pair determines the secrecy diversity order. When the base station is equipped with multiple antennas, a matched filter precoding and AN generation design is employed to further increase the secrecy performance. Based on this design, both the exact and asymptotic (in large system limit) secrecy outage probability expressions are derived. With perfect CSI and perfect SIC assumption, Z. Ding *et al.* consider a NOMA network with both multicasting and unicasting transmissions [87]. For the unicasting transmission, it it proved that the secrecy rate for NOMA is no less than that for orthogonal multiple access in the high SNR regime. Also, the secrecy outage probability is studied. A brief summary of above work is given in Table VIII.

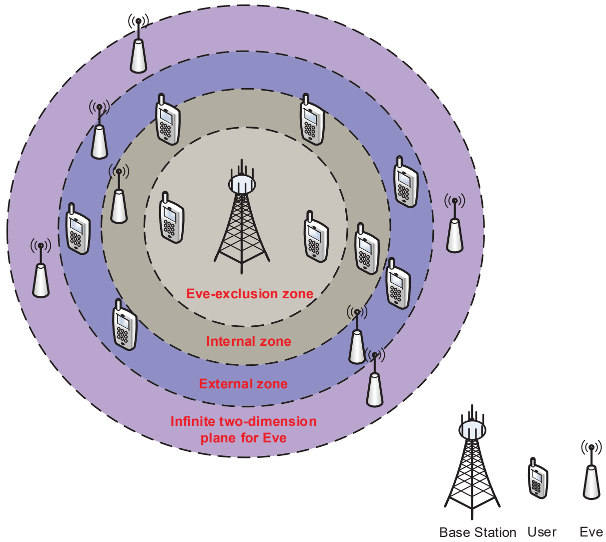


Fig. 6: Network model for the secure NOMA transmission.

VII. Physical Layer Security for Full Duplex Technology

Transmitting information by full duplex technology consists in transmitting and receiving simultaneously on the same frequency band. Theoretically, full duplex communications can double the spectral efficiency compared to the conventional half duplex communications. These last years, upstream researches have resulted in first demonstrators showing the feasibility of such systems [88]. Therefore, full duplex technology offers a promising potential for 5G. As a result, physical layer security for full duplex systems is a promising research area that has attracted much attention recently. The research on full-duplex physical layer security transmission can be mainly classified into the following four categorizations.

A. Full Duplex Receiver

W. Li *et al.* first study a single-antenna transmitter, a two-antenna full duplex receiver, and a single-antenna eavesdropper wiretap channel [89], where the full duplex receiver use one antenna to receive the signal and another antenna to send AN to the eavesdropper. The perfect self-interference cancellation (SIC) is assumed at the receiver. The closed-form expression of the secrecy outage probability for the proposed transmission scheme is derived. G. Zheng *et al.* investigate the joint transmit and receive beamforming design for a single-antenna input, multiple-antenna output, and multiple-antenna eavesdropper (SIMOME) wiretap channel with imperfect SIC [90]. The full duplex receiver transmits AN to the eavesdropper while receives data from the transmitter. For the global perfect CSI assumption, the linear receiver matrix and the AN generation matrix which maximize the achievable secrecy rate are jointly designed. It is shown that unlike the half duplex case, the secrecy rate no longer saturates at high SNR for full duplex case. The transmission design for the statistical CSI of the eavesdropper assumption is also studied in [90].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

TABLE VII: Secure transmission in heterogeneous networks

Paper	System Model	Main Contribution
T. Lv *et al.* [76]	Downlink two-tier heterogeneous network	Propose secure transmission schemes in the first time
H. Wu *et al.* [77]	Downlink K-tier heterogeneous network, no interference	Analyze secrecy outage probability
Y. J. Tolossa *et al.* [78]	Downlink K-tier heterogeneous network, no interference	Analyze average secrecy rate
M. Xu *et al.* [79]	Downlink K-tier heterogeneous network, intra-cell interference	Incorporate a dynamic CoMP scheme
H.-M. Wang [80]	Downlink K-tier heterogeneous network, inter-and intra-cell interference	Analyze secrecy and connection probabilities
W. Wang [81]	Downlink small network, inter-and intra-cell interference	Analyze secrecy and connection probabilities
H. Wu [82]	Uplink two-tier heterogeneous network, inter-and intra-cell interference	Analyze secrecy and connection probabilities
Y. Ren [83]	Downlink two-tier heterogeneous network Wireless information and power transfer	Secure transmission design

TABLE VIII: Physical Layer Security of NOMA

Paper	System Model	CSI	Objective
Y. Zhang *et al.* [85]	Single-antenna nodes A transmitter, multiple users, and a eavesdropper	Perfect CSI of users No CSI of the eavesdropper	Maximize secrecy sum-rate
Y. Liu *et al.* [86]	Downlink single-antenna networks Downlink multiple transmit antenna networks	Perfect CSI of users No CSI of the eavesdropper	Analyze secrecy outage probability
Z. Ding *et al.* [87]	Downlink MISO networks with multicasting and unicasting transmissions	Global perfect CSI	Analyze secrecy outage probability for the unicasting transmission

Moreover, a secure communication scheme for MIMOME wiretap channel with full duplex receiver and perfect SIC is designed in [91]. L. Li *et al.* further derive a closed-form expression for the maximal achievable secure degrees of freedom of the MIMOME wiretap channel with full duplex receiver under the global perfect CSI and the perfect SIC assumptions [92].

M. Masood *et al.* study a MIMOME wiretap channel with multiple full duplex receivers and multiple eavesdroppers under the global perfect CSI and the imperfect SIC assumptions [93]. Both the transmitter and the full duplex receivers will send AN to degrade the channels of the eavesdroppers. In this case, the precoding matrix and the AN generation matrix are optimized jointly to maximize the achievable secrecy rate. In the mean time, B. Akgun *et al.* consider a similar multiple-input single-output multiple-antenna eavesdropper (MISOME) wiretap channel, where the transmitter employs a zero-forcing beamforming (ZFBF) to eliminate the multiuser interference [94]. Then, the total transmit power is minimized for both instantaneous and statistical CSI of the eavesdroppers cases subject to the individual secrecy rate constraint for each user. L. Chen *et al.* investigate single antenna multi-carrier wiretap channels with full duplex receivers [95], where the power allocation among the subcarriers is designed to maximize the secrecy rate under both the total power and the legitimate links sum rate constraints. The secure communication in a single-input single-output multiple-antenna eavesdropper (SISOME) wireless ad hoc network is analyzed in [96], where a hybrid full/half duplex receiver deployment strategy is employed. The fractions of full duplex receivers which optimize the secure link number, the network-wide secrecy throughout, and the network-wide secrecy energy efficiency are derived.

For a decentralized heterogeneous network which includes a half duplex receiver tier and a full duplex receiver tier, T.-X. Zheng *et al.* derive the secrecy outage probability of a typical full duplex receiver based on the stochastic geometry framework [97]. In addition, the deployment of the full duplex receivers is optimized for the network-wide secrecy throughput maximization. T. Zhang *et al.* design the secrecy communication schemes for a cognitive wiretap channel with a multiple antenna full duplex secondary receiver [98]. A brief summary of above work is given in Table IX.

B. Full Duplex Transmitter and Receiver

O. Cepheli *et al.* investigate the bidirectional secure communication where two multiple-antenna full duplex nodes communicate with each other in presence of a multiple antenna eavesdropper [99]. The global perfect CSI and imperfect SIC assumptions are adopted. The beamforming vectors are designed to minimize the total transmit power subject to the secrecy and the QoS constraints. Assuming the global perfect CSI and perfect SIC, Y. Wan *et al.* maximize the secrecy sum rate of bidirectional full duplex communication systems in presence of a single-antenna eavesdropper under the sum transmit power constraint [100]. A null space based suboptimal design is also proposed to reduce the computational complexity. Q. Li *et al.* extend this design to the imperfect SIC and the imperfect CSI of the eavesdropper case [101]. A brief summary of above work is given in Table X.

C. Full Duplex Base Station

Considering a multiple-antenna full duplex base station which communicates with a single-antenna transmitter and a single-antenna receiver simultaneously with single-antenna eavesdropper, F. Zhu *et al.* investigate the joint precoding and AN generation design at the base station with global perfect CSI and perfect SIC to guarantee both the uplink and downlink transmission security [102]. This work is further extended to the imperfect SIC case [103]. Y. Sun *et al.* study a more general system where a multiple-antenna full duplex base station receives information from multiple single-antenna uplink users and transmit information to multiple single-antenna downlink users simultaneously in the presence of multiple potential eavesdroppers [104], as shown in Fig. 7. It is assumed that only imperfect CSIs of eavesdroppers are available at the base station. A robust resource allocation scheme is designed to minimize a total of uplink and downlink transmit power subject to the uplink and the downlink rate and security rate constraints. As illustrated in Fig. 8, the proposed design achieves significantly higher power efficiency comparing to the baseline ZFBF scheme. Y. Wang *et al.* investigate the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

TABLE IX: Secure Communications with Full Duplex Receivers

Paper	System Model	CSI	Objective
W. Li *et al.* [89]	A single-antenna transmitter, a two-antenna full duplex receiver A single-antenna eavesdropper, perfect SIC	Perfect CSI of the desired user Know the noise of eavesdropper	Analyze secrecy outage probability
G. Zheng *et al.* [90]	A single-antenna transmitter, a multiple-antenna receiver A multiple-antenna eavesdropper, imperfect SIC	Global perfect CSI Statistical CSI of the eavesdropper	Joint transmit and receive beamforming design
Y. Zhou *et al.* [91]	MIMOME wiretap channel, perfect SIC	Perfect CSI of the desired user Statistical CSI of the eavesdropper	Design a secure communication scheme
L. Li *et al.* [92]	MIMOME wiretap channel, perfect SIC	Global perfect CSI	Derive secure degrees of freedom
M. Masood *et al.* [93]	MIMOME, multiple receivers Multiple eavesdroppers, imperfect SIC	Global perfect CSI	Design precoding and AN matrices
B. Akgun *et al.* [94]	MISOME, multiple receivers Multiple eavesdroppers, imperfect SIC	Global perfect CSI Statistical CSI of the eavesdropper	Minimize total transmit power
L. Chen *et al.* [95]	Single antenna multi-carrier Wiretap channels, imperfect SIC	Global channel amplitudes	Design power allocation among the subcarriers
T.-X. Zheng *et al.* [96]	SISOME wireless ad hoc network Imperfect SIC	Global perfect CSI	Optimize full duplex receivers deployment
T.-X. Zheng *et al.* [97]	Two-tie heterogeneous network Imperfect SIC	Perfect CSI of the desired users Statistical CSI of the eavesdroppers	Analyze secrecy outage probability
T. Zhang *et al.* [98]	A cognitive wiretap channel with a multiple antenna full duplex secondary receiver, perfect SIC	Perfect CSI of the desired users No CSI of the eavesdroppers	Analyze secrecy outage probability

TABLE X: Bidirectional Secure Communications with Full Duplex Transmitters and Receivers

Paper	System Model	CSI	Objective
O. Cepheli *et al.* [99]	Multiple-antenna nodes Transmit and receive beamforming, imperfect SIC	Global perfect CSI	Minimize the total transmit power under rate constraints
Y. Wan *et al.* [100]	Multiple-antenna transmitter and receiver Single-antenna eavesdropper, perfect SIC	Global perfect CSI	Maximize the secrecy sum rate under the transmit power constraints
Q. Li *et al.* [101]	Multiple-antenna transmitter and receiver Single-antenna eavesdropper, imperfect SIC	Perfect CSI of the eavesdropper Imperfect CSI of the eavesdropper	Maximize the secrecy sum rate under the transmit power constraints

secure transmission for simultaneous wireless information and power transfer full duplex base station systems [105]. A brief summary of above work is given in Table XI.

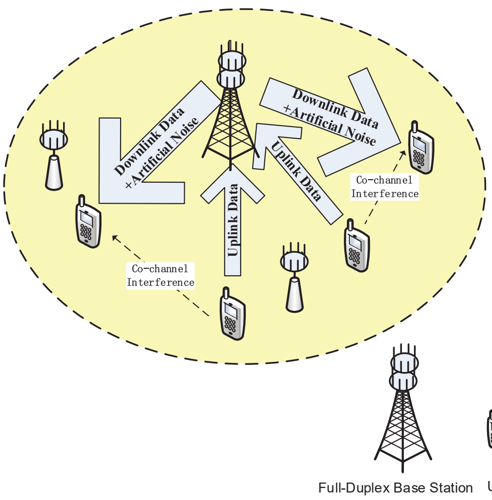


Fig. 7: Secure communication for the full-duplex base station network.

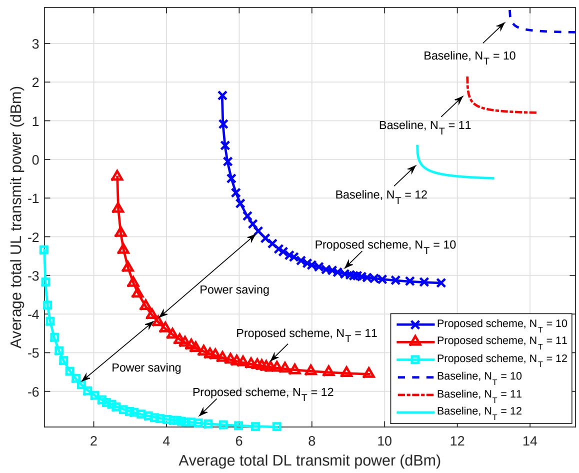


Fig. 8: Average trade off between the downlink and uplink total transmit powers. Experimental results extracted from [104].

D. Full Duplex Eavesdropper

Standing at the point of the eavesdropper, A. Mukherjee *et al.* consider a multiple antenna full duplex active eavesdropper which simultaneously eavesdrops and attacks the legitimate MIMO communication link [106]. It is assumed that the eavesdropper has the perfect knowledge of the channels among all nodes and the imperfect estimation of the self interference channel. Then, the jamming signals which minimize the secrecy rate are designed based on the Karush–Kuhn–Tucker (KKT) analysis. X. Tang *et al.* formulate the active eavesdropper problem into a hierarchical game theory problem where the eavesdropper and the legitimate user behave as a leader and a follower [107]. Then, the optimal transmission strategies at both the eavesdropper and the legitimate user's side are designed. Under the CSI uncertainty condition, M. R. Adedi *et al.* design robust transmission schemes to maximize the secrecy rate with the multiple antenna full duplex active eavesdropper and the multiple antenna full duplex receiver [108]. A brief summary of above work is given in Table XII.

There are some other works investigating full-duplex relay secure communications [109–112].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

TABLE XI: Secure Communications with Full Duplex Base Station

Paper	System Model	CSI	Objective
F. Zhu *et al.* [102]	A single-antenna transmitter, a single-antenna receiver A single-antenna eavesdropper, perfect SIC	Global perfect CSI	Maximize the secrecy transmit rate under the secrecy receive rate constraint
F. Zhu *et al.* [103]	A single-antenna transmitter, a single-antenna receiver Multiple single-antenna eavesdroppers, imperfect SIC	Global perfect CSI	Minimize the power at base station under different SINR constraints
Y. Sun *et al.* [104]	Multiple single-antenna transmitters and receivers Multiple multiple-antenna eavesdroppers, imperfect SIC	Perfect CSI of the legitimate links Imperfect CSI of eavesdroppers	Minimize the total power under secrecy rate constraints
Y. Wang *et al.* [105]	A single-antenna transmitter, a single-antenna receiver a single-antenna eavesdropper, imperfect SIC	Global perfect CSI	Maximize the secrecy rate under power and harvested energy constraints

TABLE XII: Secure Communications with Full Duplex Active Eavesdropper

Paper	System Model	CSI	Objective
A. Mukherjee *et al.* [106]	Multiple-antenna nodes Imperfect SIC	Global perfect CSI	Minimize the secrecy rate under a maximum power constraint
X. Tang *et al.* [107]	Single-antenna nodes Imperfect SIC	Perfect CSI of the eavesdropper Statistical CSI of the eavesdropper	Design optimal strategies within a hierarchical game theory framework
M. R. Adedi *et al.* [108]	Multiple-antenna nodes Imperfect SIC	Imperfect CSI between the eavesdropper and other nodes	Maximize the secrecy rate under the transmit power constraint

VIII. Other Important Research Work

Layered approaches have been traditionally applied for wireless cooperative networks, where each layer in the protocol stack is designed and operated independently. The motivation for such layered approaches is to exploit the advantage of the modularity in system design since the system dynamics caused by the interactions among the protocols at the different layers could be fairly complex. However, careful exploitation of some cross-layer protocol interactions can lead to a more efficient performance of the transmission protocol stack and hence better application level protocol performance in various wireless networking scenarios. This is particularly true for realizing network security since by exploiting the security capacity and signal processing technologies at the physical layer and the authentication and watermarking strategies at the application layer, the available network resources can be utilized more efficiently. A joint physical-application layer secure transmission scheme which includes physical layer channel coding and application layer authentication and watermarking is proposed for multimedia communication systems [113]. Simulations show that the joint scheme improves the verification probability for both static and dynamic networks. On the other hand, to limit the information leakage at bit-level, the physical layer security technique is exploited to guarantee the secure video transmission [114]. Moreover, physical layer security aware routing for multi-hop ad hoc networks are investigated [115–117]. Other researchers study the physical layer authentication [118, 119].

In addition to theoretical studies, it is also necessary to investigate the practical test bed design for physical layer security. This is important to evaluate the usefulness of the physical layer based security schemes and evaluate their performance in a practical transmission environment. Both WiFi and LTE test beds are built to examine the secrecy schemes including secrecy coding, secret key generation, and artificial noise and beamforming [120, 121]. It is revealed that in practical transmission environment, AN is still an effective approach to degrade the performance of the eavesdropper even when the desired user and the eavesdropper are very close to each other. Also, it is shown that the channel realizations have a significant impact on the secrecy coding performance. Other practical prototypes involve more on secrecy key generation, including in ultra wideband systems [122], IEEE 802.11 systems [123, 124], FM/TV systems [125], etc.

IX. Future Technical Challenges

In this section, a number of technical challenges for physical layer security in 5G and beyond are discussed.

A. Physical Layer Security Coding

As indicated in Table I, in terms of mutual information criterion, current LDPC code designs can only achieve the weak secrecy for the special BEC model. For strong secrecy, it further requires the main channel to be noiseless. How to design LDPC codes which can achieve the weak/stong secrecy for a more general channel such as the Gaussian wiretap channel is still a challenge problem. In terms of BER criterion, the LDPC codes for MIMO and massive MIMO systems can be investigated.

As indicated in Table II, most of current polar code designs require the perfect channel knowledge of the eavesdropper at the transmitter to achieve the weak/strong secrecy. How to extend the polar code designs to a more reasonable case where only channel distribution knowledge of the eavesdropper is available at the transmitter is an important research issue. This point also applies for lattice code designs.

B. Physical Layer Security in Massive MIMO Systems

The transmission designs in [60] are more effective to combat the pilot contamination attack for strong correlation channels. The defense strategy for i.i.d. fading channels in [61] requires the length of the pilot signal scales with the number of transmit antennas, which will significantly reduce the transmission efficiency for massive MIMO systems. The defense strategy in [62] is used for secret key agreement. Therefore, for massive MIMO transmission with active eavesdropper, the existing approaches are preliminary and far-from realizing secure communications theoretically and practically for massive MIMO systems. Several important issues need to be clarified for massive MIMO systems under pilot contamination attack: 1) What is the fundamental limit of secure communication? 2)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

Are there any unified transmission schemes which are effective for general massive MIMO channels? 3) How to design the secure transmission schemes in practical communication systems?

Since massive MIMO is the key technology for 5G wireless networks, another important research point for physical layer security in massive MIMO systems is the secure transmission scheme designs for the joint implementation of massive MIMO and other important 5G technologies, e.g., the secure mmWave massive MIMO communications and the secure massive communications in heterogeneous networks, etc.

C. Physical Layer Security for mmWave Communications

Normally, highly directional beamforming is used in mmWave communications to combat the path loss. This directional beamforming significantly depends on the accuracy of the CSI of the desired users. Similar as the massive MIMO case, for TDD communication systems, if an active eavesdropper jeopardizes the channel estimation phase for the desired user, this may result in a significant secure threat. However, little research has been available on how to defend the active eavesdropper in mmWave communications.

For a lower implementation cost, hybrid digital and analog precoding is often used for mmWave communications to reduce the number of RF chains. How to design secure transmission schemes based on this hybrid structure for both point-to-point and network mmWave MIMO communication systems can be studied. Secure mmWave vehicle to vehicle communications is another important research point.

D. Physical Layer Security in Heterogeneous Networks

Currently, most works for physical layer security in heterogeneous networks [77–82] focus on analyzing the secrecy performance of the networks. Since multiple tiers are available to multiple users, another possible research strategy is to investigate how to properly schedule these users access to different network ties in order to better safeguard the multi-tier communications. Based on this, precoder designs can be studied to further improve the secrecy spectrum efficiency. Moreover, the interference generated by multiple tiers may be properly exploited to degrade the performance of the eavesdropper.

E. Physical Layer Security of NOMA

The security risk is a particular concern for the multiple access techniques such as NOMA since the user is allowed to decode the transmit information for other users. As a complement of current encryption techniques, physical layer security technology is a good candidate for improving the communication security for NOMA systems.

Currently, there are only some very initial research results for physical layer security of NOMA [85–87], primary focusing on analyzing the secrecy performance of NOMA systems or providing the power allocation policy for an ideal simple NOMA model. More research work are required to design effective and efficient secure communication schemes for practical NOMA systems.

F. Physical Layer Security for Full Duplex Technology

If all the nodes in the systems are capable of full duplex communication ability, how to design the effective secure communication scheme remains unknown. In particular, the full duplex transmitter and receiver can generate AN to degrade the eavesdropper, while the full duplex eavesdropper can also generate AN to interfere the transmitter and the receiver. This may be formulated into a hierarchical game framework where some game theory methods can be exploited to solve the problem.

Another point is that for full duplex base station scenarios, current research assume both transmitter and receiver are equipped with single-antenna. The extension to multiple-antenna case can be investigated.

G. Physical Layer Security for Other 5G Scenarios and Beyond

Physical layer security technique have many other applications in 5G communications and beyond. For example, traditional security key mechanisms are mainly based on the distribution of shared keys. Due to the mobility and scalability of 5G wireless networks [1], this task is nontrivial. The physical layer secret-key generation was first investigated in [126, 127], where correlated observations of noisy phenomena can be exploited to generate secret keys by exchanging information over a public channel. As one of the few implementable physical layer security techniques, key generation can be constructed in current wireless devices. Many prototypes have been reported involving physical layer secret-key generation [122, 128–130]. However, thorough study examining the effects of environment conditions and channel parameters on the physical layer secret-key generation is still missing. In addition, in the case of key agreement, most studies consider key generation schemes with passive eavesdroppers, where the active attacks have been less studied.

The internet of thing (IoT) is the network of physical objects embedded with actuators, radio-frequency identifications, sensors, software, and connectivity to enable it to interact with manufacturers, operators, and/or other connected devices to reach common goals. 5G will be a key enabler for the IoT by providing the planform to connect a massive number of machine-type communication (MTC) devices to internet. MTC devices are usually low data rate requirements, periodic data traffic arrivals, limited hardware and signal processing complexity, limited storage memory, compact form factors, and significant energy constraints [131]. These aspects have received relatively limited attention on physical layer security in the literature. For example, a theoretically well-founded and holistic approach to precisely characterize complexity and energy constraints in physical layer security designs is still missing. Moreover, a network of massive MTC devices in IoT requires novel fundamental definitions of secrecy metrics for point-to-multipoint systems and multipoint-to-point systems with a very large number of downlink receivers and uplink transmitters, respectively. In addition, the communication channels of MTC devices may have very different propagation characteristics as opposed to the conventional Rayleigh and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

Rician multipath channel models for broadband microwave systems [132]. How to securely transmit data over these channels remains largely open.

Other interesting work includes the interplay between wireless power transfer and physical layer security [133, 134]. In particular, it is shown in [133, 134] that the jamming noise which can be used to provide security may not always be harmful and can be an energy beam as well. Therefore, it may be a good integration between wireless power transfer and physical layer security design. The physical layer security for visible light communication systems has been studied in [135].

X. Conclusion

The emerging and development of future wireless technologies such as massive MIMO technology, millimeter wave communications, machine type communication and Internet of Thing, etc have brought out new security challenges for 5G networks. To design efficient secure transmission schemes for 5G wireless communications that exploit propagation properties of radio channels in physical layer has attracted wide research interests recently. This approach is referred as physical layer security for 5G technologies. The physical layer security approaches are robust to more and more advanced passive and active eavesdroppers and are flexible for secret key generation in 5G networks. With careful management and implementation, physical layer security and conventional encryption techniques can formulate a well-integrated security solution together that efficiently safeguards the confidential and privacy communication data in 5G networks. We wish that the research results in this special issue and our survey paper will be helpful to the readers to have a better understanding of the benefits and opportunities that physical layer security techniques provide for 5G and future wireless networks.

References

[1] 5G-PPP, "5G vision," Whitepaper, Feb. 2015.

[2] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, Jun. 2008.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-Part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 3088–3104, Jul. 2010.

[5] ——, "Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4961–4972, Aug. 2011.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical-layer security via cooperating relay," *IEEE Trans. Signal Process.*, vol. 58, pp. 1875–1888, Mar. 2011.

[8] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, pp. 5013–5022, Oct. 2011.

[9] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, pp. 1317–1322, Mar. 2011.

[10] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, pp. 2121–2138, Apr. 2014.

[11] A. Mukherjee, A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tutorials*, vol. 16, pp. 1550–1573, Feb. 2014.

[12] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, pp. 20–27, Apr. 2015.

[13] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical chanllenges, recent advances, and future trends," *Proceedings of IEEE*, vol. 104, pp. 1727–1765, Sep. 2016.

[14] X. Chen, D. W. K. Ng, W. Gerstacker, and H.-H. Chen, "A survey of multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tutorials*, vol. 19, pp. 1027–1053, Jun. 2017.

[15] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Application of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2933–2945, Aug. 2007.

[16] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel," *IEEE Trans. Inf. Theory*, vol. 59, pp. 1048–1064, Feb. 2013.

[17] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using large-grith LDPC codes," *IEEE Trans. Inf. Foresics Security*, vol. 6, pp. 585–594, Sep. 2011.

[18] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Foresics Security*, vol. 6, pp. 532–540, Sep. 2011.

[19] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambing, concatenation, and HARQ for the AWGN wiretap channel: A security gap analysis," *IEEE Trans. Inf. Foresics Security*, vol. 7, pp. 883–894, Jun. 2012.

[20] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practcial codes," *IEEE Trans. Inf. Foresics Security*, vol. 9, pp. 1765–1779, Nov. 2014.

[21] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *Proc. Int. Conf. Commun. (ICC'2015)*, London, UK, Jun. 2015, pp. 435–440.

[22] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, pp. 6428–6443, Oct. 2011.

[23] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. and Trends in Commun. and Inf. Theory*, vol. 5, pp. 355–580, 2008.

[24] E. Hof and S. Shamai, "Secrecy-achieving polar-coding," in *Proc. Inf. Theory Workshop (ITW'2010)*, Cairo, Egypt, Jan. 2010, pp. 1–5.

[25] M. Andersson, V. Rathi, R. Thobahen, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, pp. 752–754, Aug. 2010.

[26] O. O. Koyluoglu and H. E. Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Inf. Foresics Security*, vol. 7, pp. 1472–1483, Oct. 2012.

[27] Y.-P. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *IEEE J. Sel. Areas Commun.*, vol. 34, pp. 278–291, Feb. 2016.

[28] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of polar codes for the deterministic wiretap channel," in *Asilomar'2013*, Pacific Grove, USA, Nov. 2013, pp. 2089–2093.

[29] M. Andersson, R. F. Schaefer, T. J. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1901–1908, Sep. 2013.

[30] E. Sasoğlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2013)*, Istanbul, Turkey, Jul. 2013, pp. 1117–1121.

[31] T. C. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," in *Proc. Inf. Theory Workshop (ITW'2015)*, Jeju Island, Korea, Oct. 2015, pp. 1–5.

[32] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, pp. 2410–2429, May 2016.

[33] J. M. Renes, R. Renner, and D. Sutter, *Efficient one-way secret key agreement and private channel coding via polarization*, in Advances in Cryptology-ASIACRYPT 2013, Ed. New York, USA: Springer, 2013, pp. 194-213.

[34] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, "Polar-LDPC concatenated coding for the AWGN wiretap channel," *IEEE Commun. Lett.*, vol. 18, pp. 1683–1686, Oct. 2014.

[35] J.-C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA'2010)*, Taichung, Taiwan, Oct. 2010, pp. 174–178.

[36] F. Oggier, P. Sole, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *IEEE Trans. Inf. Theory*, vol. 62, pp. 5690–5708, Oct. 2016.

[37] A.-M. E.-Hytönen, "On a conjecture by Belfiore and Solé on some lattices," *IEEE Trans. Inf. Theory*, vol. 58, pp. 5950–5955, Sep. 2012.

[38] F. Lin and F. Oggier, "A classification of unimodular lattice wiretap codes in small dimensions," *IEEE Trans. Inf. Theory*, vol. 59, pp. 3295–3303, Jun. 2013.

[39] J.-C. Belfiore and F. Oggier, "Lattice code design for the Rayleigh fading wiretap channel," in *Proc. Int. Conf. Commun. (ICC'2011)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[40] L.-C. Choo, C. Ling, and K.-K. Wong, "Achievable rates for lattice coded Gaussian wiretap channels," in *Proc. Int. Conf. Commun. (IC-C'2011)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[41] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, pp. 6399–6416, Oct. 2014.

[42] L.-C. Choo and C. Ling, "Superposition lattice coding for Gaussian broadcast channel with confidential message," in *Proc. Inf. Theory Workshop (ITW'2014))*, Hobart, Australia, Nov. 2014, pp. 311–315.

[43] X. He and A. Yener, "The Gaussian many-to-one inference channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 57, pp. 2730–2745, May 2011.

[44] ——, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, pp. 177–192, Jan. 2013.

[45] L. Lai, H. E. Gammal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 5059–5067, Nov. 2008.

[46] J. G. Andrews, S. Buzzi, W. Choi, S. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, pp. 1065–1082, Jun. 2014.

[47] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 4766–4781, Sep. 2014.

[48] ——, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 2245–2261, Mar. 2016.

[49] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Commun.*, vol. 64, pp. 6854–6868, Dec. 2015.

[50] K. Guo, Y. Guo, and G. Ascheid, "Security-constrained power allocation in mu-massive-MIMO with distributed antennas," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 8139–8153, Dec. 2016.

[51] Y. Wu, J.-B. Wang, J. Wang, R. Schober, and C. Xiao, "Secure transmission with large numbers of antennas and finite alphabet inputs," to appear in IEEE Trans. Commun.

[52] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, pp. 5135–5146, Sep. 2015.

[53] J. Chen, X. Chen, W. H. Gerstacker, and D. W. K. Ng, "Resource allocation for a massive MIMO relay aided secure communication," *IEEE Trans. Inf. Foresics Security*, vol. 11, pp. 1700–1711, Aug. 2016.

[54] J. Zhu, W. Xu, and N. Wang, "Secure massive MIMO systems with limited RF chains," to appear in IEEE Trans. Veh. Technol.

[55] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 2001–2016, Mar. 2017.

[56] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, Jul. 2016.

[57] B. Chen, C. Zhu, L. Shu, M. Su, J. Wei, V. C. M. Leung, and J. J. P. C. Rodrigues, "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, Sep. 2016.

[58] H. Wei, D. Wang, X. Hou, Y. Zhu, and J. Zhu, "Security analysis for massive MIMO system internal eavesdroppers," in *Proc. IEEE Veh. Tech. Conf. (VTC'2015)*, Boston, USA, Sep. 2015, pp. 1–5.

[59] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 903–907, Mar. 2012.

[60] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, pp. 3880–3900, Jul. 2016.

[61] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," [Online]. Available: http://arxiv.org/abs/1505.00396.

[62] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement with large antenna arrays under the pilot contamination attack," *IEEE Trans. Wireless Commun.*, vol. 14, pp. 6579–6594, Dec. 2015.

[63] T. T. Do, H. Q. Ngo, T. Q. Duong, T. J. Oechtering, and M. Skoglund, "Massive MIMO pilot retransmission strategies for robustification against jamming," to appear in IEEE Wireless Commun. Lett.

[64] D. B. Rawat, K. Neupane, and M. Song, "A novel algorithm for secrecy rate analysis in massive MIMO system with target SINR requirement," in *Proc. INFOCOM'2016*, San Franciso, USA, Apr. 2016, pp. 1–6.

[65] T. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[66] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath Jr., "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *Proc. IEEE SPAWC'2014*, Toronto, Canada, Jun. 2014, pp. 115–119.

[67] Y. Ju, H.-M. Wang, T.-X. Zheng, and Q. Yin, "Secure transmissions in millimeter wave systems," to appear in IEEE Trans. Commun.

[68] X. Tian, M. Li, Z. Wang, and Q. Liu, "Hybrid precoder and combinder design for secure transmission in mmWave MIMO systems," [Online]. Available: https://arxiv.org/abs/1704.08099.

[69] C. Wang and H.-M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 5569–5585, Aug. 2016.

[70] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, pp. 3507–3519, Aug. 2016.

[71] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath Jr., "Secure communication in millimeter wave Ad Hoc networks," to appear in IEEE Trans. Wireless Commun.

[72] S. Gong, C. Xing, Z. Fei, and S. Ma, "Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward MIMO relaying networks," *IEEE Trans. Veh. Technol.*, vol. 66, pp. 2059–2071, Mar. 2017.

[73] N. Valliappan, A. Lozano, and R. W. Heath Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, pp. 3231–3245, Aug. 2013.

[74] M. E. Eltayeb, J. Choi, T. Y. A.-Naffouri, and R. W. Heath Jr., "On the security of millimeter wave vehicular communication systems using random antenna subsets," [Online]. Available: https://arxiv.org/abs/1609.04499.

[75] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *Proc. IEEE Conf. Commun. and Network Security*, Florence, Italy, Sep. 2015, pp. 353–343.

[76] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, pp. 1154–1170, Jun. 2015.

[77] H. Wu, X. Tao, N. Li, and J. Xu, "Secrecy outage probability in multi-rat heterogeneous networks," *IEEE Commun. Lett.*, vol. 20, pp. 53–56, Jan. 2016.

[78] Y. J. Tolossa, S. Vuppala, and G. Abreu, "Secrecy-rate analysis in multitier heterogeneous networks under generalized fading model," *IEEE J. Int. of Things*, vol. 4, pp. 101–110, Feb. 2017.

[79] M. Xu, X. Tao, F. Yang, and H. Wu, "Enhancing secured coverage with CoMP transmission in heterogeneous celluar networks," *IEEE Commun. Lett.*, vol. 20, pp. 2272–2275, Nov. 2016.

[80] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous celluar networks," *IEEE Trans. Commun.*, vol. 64, pp. 1204–1219, Mar. 2016.

[81] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Foresics Security*, vol. 12, pp. 1470–1482, Jun. 2017.

[82] H. Wu, X. Tao, H. Chen, N. Li, and J. Xu, "Secrecy and connection performance for uplink transmission in non-uniform HetNets," in *Proc. Global Commun. Conf. (Globecom 2016)*, Washington DC, USA, Dec. 2016, pp. 1–6.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

[83] Y. Ren, T. Lv, H. Gao, and Y. Li, "Secure wireless information and power transfer in heterogeneous networks," *IEEE Access*, vol. 5, pp. 4967–4979, Apr. 2017.

[84] Huawei, "5G: A technology vision," Whitepaper, Nov. 2013.

[85] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, pp. 930–933, May 2016.

[86] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 1656–1672, Mar. 2017.

[87] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," to appear in IEEE Trans. Commun.

[88] S. Hong, J. Brand, J. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5G and beyond," *IEEE Commun. Mag.*, vol. 52, pp. 114–121, Feb. 2014.

[89] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, pp. 1628–1631, Oct. 2012.

[90] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, pp. 4962–4974, Oct. 2013.

[91] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimizaiton," *IEEE Signal Process. Lett.*, vol. 21, pp. 804–808, Jul. 2014.

[92] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex Bob in the MIMO Gaussian wiretap channel: Scheme and performance," *IEEE Signal Process. Lett.*, vol. 23, pp. 107–111, Jan. 2016.

[93] M. Masood, A. Ghrayeb, P. Babu, I. Khalil, and M. Hasna, "A minorization-maximization algorithm for maximizing the secrecy rate of the MIMOME wiretap channel," *IEEE Commun. Lett.*, vol. 21, pp. 520–523, Mar. 2017.

[94] B. Akgun, O. O. Koyluoglu, and M. Krunz, "Exploiting full-duplex receivers for achieving secret communications in multiuser MISO networks," *IEEE Trans. Commun.*, vol. 65, pp. 956–968, Feb. 2017.

[95] L. Chen, Q. Zhu, W. Meng, and Y. Hua, "Fast power allocation for secure communication with full-duplex radio," to appear in IEEE Trans. Signal Process.

[96] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless Ad Hoc networks under a hybrid full-/half-duplex receiver deployment strategy," to appear in IEEE Trans. Wireless Commun.

[97] T.-X. Zheng, H.-M. Wang, Q. Yang, and M. H. Lee, "Safeguarding decentralized wireless networks using full-duplex jamming receivers," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 278–292, Jan. 2017.

[98] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes," *IEEE Trans. Commun.*, vol. 65, pp. 335–346, Jan. 2017.

[99] Ö. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE Commun. Lett.*, vol. 18, pp. 1075–1078, Jun. 2014.

[100] Y. Wan, Q. Li, Q. Zhang, and J. Qin, "Optimal and suboptimal full-duplex secure beamforming designs for MISO two-way communications," *IEEE Commun. Lett.*, vol. 4, pp. 493–496, Oct. 2015.

[101] Q. Li, Y. Zhang, J. Lin, and S. X. Wu, "Full-duplex bidirectional secure communications under perfect and distributionally ambiguous eavesdropper's CSI," *IEEE Trans. Signal Process.*, vol. 65, pp. 4684–4697, Sep. 2017.

[102] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 64, pp. 6391–6401, Dec. 2014.

[103] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-inferference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 329–340, Jan. 2016.

[104] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 5511–5526, Aug. 2016.

[105] Y. Wang, R. Sun, and X. Wang, "Transceiver design to maximize the weighted sum secrecy rate in full-duplex SWIPT systems," *IEEE Signal Process. Lett.*, vol. 23, pp. 883–887, Jun. 2016.

[106] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Conf. Rec. 45th Asilomar Signal Syst. Comput. (ASILOMAR'2011)*, Pacific Grove, USA, Nov. 2011, pp. 265–269.

[107] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Wireless Commun.*, vol. 65, pp. 1379–1395, Mar. 2017.

[108] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 885–899, Feb. 2017.

[109] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, pp. 525–528, Apr. 2015.

[110] S. Parsaeefard and T. L.-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Foresics Security*, vol. 10, pp. 2095–2107, Oct. 2015.

[111] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Foresics Security*, vol. 10, pp. 574–583, Mar. 2015.

[112] Q. Li, W.-K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE J. Sel. Topic Signal Process.*, vol. 10, pp. 1359–1374, Dec. 2016.

[113] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physcial-application layer security for wireless multimedia delivery," *IEEE Commun. Mag.*, vol. 52, pp. 66–72, Mar. 2014.

[114] M. Hussain, Q. Du, L. Sun, and P. Ren, "Security enhancement for video transmission via noise aggregation in immersive systems," *Multimed Tools Appl*, vol. 75, pp. 5345–5357, May 2016.

[115] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, pp. 1433–1448, Jul. 2015.

[116] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 2, pp. 753–764, Feb. 2016.

[117] Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Computer Networks*, vol. 123, pp. 77–87, May 2017.

[118] K. M. Borle, B. Chen, and W. Du, "Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation," *IEEE Trans. Inf. Foresics Security*, vol. 10, pp. 2225–2235, Oct. 2015.

[119] W. Hou, X. Wang, X. Chouinard J., and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, pp. 1658–1667, May 2016.

[120] Phylaws, "WiFi test bed-WP5 conclusion and standardization aspects," Online Available: http://www.phylaws-ict.org/.

[121] ——, "LTE simulations results-Final Report," Online Available: http://www.phylaws-ict.org/.

[122] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Foresics Security*, vol. 2, pp. 364–375, Sep. 2007.

[123] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, pp. 1842–1852, Sep. 2013.

[124] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, Sep. 2016.

[125] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Washington DC, USA, Jul. 2011, pp. 211–224.

[126] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, May 1993.

[127] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, Jul. 1993.

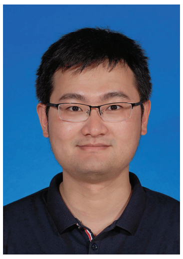
[128] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1779–1790, Sep. 2013.

[129] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 31, pp. 17–30, Jan. 2010.

[130] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *Proc. Global Commun. Conf. (Globecom'2016)*, Washington, USA, Dec. 2016, pp. 1–6.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

[131] J.-M. Liang, J.-J. Chen, H.-H. Cheng, and Y.-C. Tseng, "An energy-efficient sleep scheduling with QoS consideration in 3GPP LTE-Advanced networks for Internet of Things," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 3, pp. 13–22, Mar. 2013.
[132] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 3442–3451, Jun. 2014.
[133] H. Xing, K. K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-af relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, pp. 7971–7984, Sep. 2016.
[134] M. R. A. Khandaker, K. K. Wong, Y. Y. Zhang, and Z. Zheng, "Probabilistically robust SWIPT for secrecy MISOME systems," *IEEE Trans. Inf. Foresics Security*, vol. 12, pp. 211–226, Sep. 2016.
[135] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers," to appear in *IEEE Trans. Wireless Commun.*.



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

Dr. Wu is currently a Tenure-Track Associate Professor with the Department of Electronic Engineering, Shanghai Jiao Tong University, China. Previously, he was senior research fellow with Institute for Communications Engineering, Technical University of Munich, Germany and the Humboldt research fellow and the senior research fellow with 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, physical layer security, signal processing for wireless communications, and multivariate statistical theory.

Dr. Wu was awarded the IEEE Student Travel Grants for IEEE International Conference on Communications (ICC) 2010, the Alexander von Humboldt Fellowship in 2014, the Travel Grants for IEEE Communication Theory Workshop 2016, and the Excellent Doctoral Thesis Awards of China Communications Society 2016. He was an Exemplary Reviewer of the IEEE Transactions on Communications in 2015, 2016. He is the lead guest editor for 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 IEEE Communications Letters. He has been a TPC member of various conferences, including Globecom, ICC, VTC, and PIMRC, etc.

Ashish Khisti received his BASc Degree in Engineering Sciences (Electrical Option) from University of Toronto, and his S.M and Ph.D. Degrees in Electrical Engineering from the Massachusetts Institute of Technology. Between 2009-2015, he was an assistant professor in the Electrical and Computer Engineering department at the University of Toronto. He is presently an associate professor, and holds a Canada Research Chair in the same department.

Dr. Khisti is 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 presently serves as an associate editor for IEEE Transactions on Information Theory and is also a 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 a Bachelor of Science degree in electronic engineering from the University of Electronic Science and Technology of China in 1987, a Master of Science degree in electronic engineering from Tsinghua University in 1989, and a Ph.D. in electrical engineering from the University of Sydney in 1997.

Dr. Xiao is the Chandler Weaver Professor and Chair of the Department of Electrical and Computer Engineering at Lehigh University. He is a Fellow of the IEEE and a Fellow of the Canadian Academy of Engineering. Previously, he served as a Program Director with the Division of Electrical, Communications and Cyber Systems at the USA National Science Foundation. He was a senior member of scientific staff with Nortel Networks, Ottawa, Canada, a faculty member at Tsinghua University, Beijing, China, the University of Alberta, Edmonton, Canada, the University of Missouri - Columbia, MO, and Missouri University of Science and Technology, Rolla, MO. 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.

Dr. Xiao is the Awards Committee Chair of IEEE Communications Society. Previously, he served as an elected member of Board of Governors, a member of Fellow Evaluation Committee, Director of Conference Publications, Distinguished Lecturer of the IEEE Communications Society, and Distinguished Lecturer of the IEEE Vehicular Technology. He also served as an Editor, Area Editor and the Editor-in-Chief of the IEEE Transactions on Wireless Communications, an Associate Editor of the IEEE Transactions on Vehicular Technology, and of the IEEE Transactions on Circuits and Systems-I. He was the Technical Program Chair of the 2010 IEEE International Conference on Communications, Cape Town, South Africa, a 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 received several distinguished awards including 2014 Humboldt Research Award, 2014 IEEE Communications Society Joseph LoCicero Award, 2015 IEEE Wireless Communications Technical Committee Recognition Award, and 2017 IEEE Communications Society Harold Sobol Award.

Giuseppe Caire was born in Torino, Italy, in 1965. He received the B.Sc. in Electrical Engineering from Politecnico di Torino (Italy), in 1990, the M.Sc. in Electrical Engineering from Princeton University in 1992 and the Ph.D. from Politecnico di Torino in 1994. He has been a post-doctoral research fellow with the European Space Agency (ESTEC, Noordwijk, The Netherlands) in 1994-1995, Assistant Professor in Telecommunications at the Politecnico di Torino, Associate Professor at the University of Parma, Italy, Professor with the Department of Mobile Communications at the Eurecom Institute, Sophia-Antipolis, France, and he is currently a professor of Electrical Engineering with the Viterbi School of Engineering, University of Southern California, Los Angeles and an Alexander von Humboldt Professor with the Electrical Engineering and Computer Science Department of the Technical University of Berlin, Germany.

He served as Associate Editor for the IEEE Transactions on Communications in 1998-2001 and as Associate Editor for the IEEE Transactions on Information Theory in 2001-2003. 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 in 2011, the Okawa Research Award in 2006, the Alexander von Humboldt Professorship in 2014, and the Vodafone Innovation Prize in 2015. Giuseppe Caire is a Fellow of IEEE since 2005. He has served in the Board of Governors of the IEEE Information Theory Society from 2004 to 2007, and as officer from 2008 to 2013. He was President of the IEEE Information Theory Society in 2011. His main research interests are in the field of communications theory, information theory, channel and source coding

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825560, IEEE Journal on Selected Areas in Communications

Kai-Kit Wong (M'01-SM'08-F'16) received the BEng, the MPhil, and the PhD degrees, all in Electrical and Electronic Engineering, from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. After graduation, he took up academic and research positions at the University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group of Stanford University, and the University of Hull, UK. He is Chair in Wireless Communications at the Department of Electronic and Electrical Engineering, University College London, UK.

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, and of course cognitive radios. There are also a few other unconventional research topics that he has set his heart on, including for example, fluid antenna communications systems, remote ECG detection and etc. He is 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.

He is Fellow of IEEE and IET and is also on the editorial board of several international journals. He has served as Senior Editor for IEEE Communications Letters since 2012 and also for IEEE Wireless Communications Letters since 2016. He had also previously served as Associate Editor for IEEE Signal Processing Letters from 2009 to 2012 and Editor for IEEE Transactions on Wireless Communications from 2005 to 2011. He was also Guest Editor for IEEE JSAC SI on virtual MIMO in 2013 and currently Guest Editor for IEEE JSAC SI on physical layer security for 5G.

Xiqi Gao (S'92–AM'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 April 1992. Since May 2001, he has been a professor of information systems and communications. From September 1999 to August 2000, he was a visiting scholar at Massachusetts Institute of Technology, Cambridge, MA, USA, and Boston University, Boston, MA. From August 2007 to July 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 now 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, 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.