A Survey on Multiple-Antenna Techniques for Physical Layer Security

Xiaoming Chen, *Senior Member, IEEE*, Derrick Wing Kwan Ng, *Member, IEEE*, Wolfgang H. Gerstacker, *Senior Member, IEEE*, and Hsiao-Hwa Chen, *Fellow, IEEE*

***Abstract*—As a complement to high-layer encryption techniques, physical layer security has been widely recognized as a promising way to enhance wireless security by exploiting the characteristics of wireless channels, including fading, noise, and interference. In order to enhance the received signal power at legitimate receivers and impair the received signal quality at eavesdroppers simultaneously, multiple-antenna techniques have been proposed for physical layer security to improve secrecy performance via exploiting spatial degrees of freedom. This paper provides a comprehensive survey on various multiple-antenna techniques in physical layer security, with an emphasis on transmit beamforming designs for multiple-antenna nodes. Specifically, we provide a detailed investigation on multiple-antenna techniques for guaranteeing secure communications in point-to-point systems, dual-hop relaying systems, multiuser systems, and heterogeneous networks. Finally, future research directions and challenges are identified.**

***Index Terms*—Physical layer security, multiple-antenna technique, secrecy performance, beamforming design.**

ABBREVIATIONS

AF	Amplify-and-Forward
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BC	BroadCasting
BD	Block Decomposition
BF	BeamForming
BS	Base Station
CF	Compute-and-Forward
CR	Cognitive Radio
CSI	Channel State Information
D2D	Device-to-Device
DF	Decode-and-Forward
DoF	Degree of Freedom
DPC	Dirty Paper Coding
EE	Energy Efficiency
Eve	Eavesdropper
EVD	EigenValue Decomposition
FD	Full Duplex
FDD	Frequency Division Duplex
GSVD	Generalized Singular Value Decomposition
HD	Half Duplex
HetNet	Heterogeneous Network
LDPC	Low-Density Parity-Check
MIMO	Multiple-Input Multiple-Output
MIMOME	MIMO Multiple-Eavesdropper
MISO	Multiple-Input Single-Ouput
MMSE	Minimum Mean Squared Error
MRC	Maximum Ratio Combination
MRT	Maximum Ratio Transmission
MUD	Multiple-User Detection
OFDM	Orthogonal Frequency Division Multiple
PHY-security	PHYsical layer security
QoS	Quality of Service
SC	Secrecy Capacity
SDP	Semi-Definite Programming
SIC	Successive Interference Cancellation
SINR	Signal-Interference-plus-Noise Ratio
SNR	Signal-Noise Ratio
STC	Space Time Coding
TDD	Time Division Duplex
THP	Tomlison-Harashima Precoding
UE	User Equipment
WIPT	Wireless Information and Power Transfer
WPC	Wireless Powered Communication
ZF	Zero Forcing.

Manuscript received January 20, 2016; revised June 29, 2016 and October 6, 2016; accepted November 20, 2016. Date of publication November 29, 2016; date of current version May 31, 2017. This work was supported in part by the Natural Science Foundation of China under Grant 61301102, in part by the Australian Research Council's Discovery Early Career Researcher Award (DECRA) under Grant DE170100137, and in part by the National Science Council of Taiwan under Grant NSC102-2221-E-006-008-MY3.

X. Chen is with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310016, China (e-mail: chen_xiaoming@zju.edu.cn).

D. W. K. Ng is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2033, Australia (e-mail: wingn@ece.ubc.ca).

W. H. Gerstacker is with the Institute for Digital Communications, University of Erlangen-Nürnberg, Erlangen 91058, Germany (e-mail: wolfgang.gerstacker@fau.de).

H.-H. Chen is with the Department of Engineering Science, National Cheng Kung University, Tainan 70101, Taiwan (e-mail: hshwchen@ieee.org).

Digital Object Identifier 10.1109/COMST.2016.2633387

I. INTRODUCTION

INFORMATION security has been always a critical issue for wireless communications due to the broadcast nature of wireless medium. In fact, communication security is a quite old topic, which can be traced back to the birth of wireless communications. As a simple example, soldiers in ancient times used flags to deliver messages between each others over a long distance in a battlefield. In this way, however,

TABLE I
PERFORMANCE METRICS OF PHY-SECURITY

Type	Definition	CSI requirement
Instantaneous performance metrics	Secrecy rate [9]: the rate difference of the legitimate channel and the eavesdropper channel	Full instantaneous CSI, deterministic imperfect CSI
	Secrecy capacity [62]: the maximum secrecy rate	
Statistical peformance metrics	Ergodic secrecy rate [49]: the statistical average of secrecy rate over channel distributions	Indeterministic imperfect CSI, statistical CSI
	Secrecy outage probability [51]: the probability that the real transmission rate is greater than secrecy rate	
	Interception probability [53]: the probability that eavesdropper channel rate is greater than legitimate channel rate	
Asymptotic performance metrics	Secrcy diversity order [55]: the high-SNR slop of secrecy outage probability	
	Secrecy degrees of freedom [57]: the number of independent symbols transmitted in parallel at a high SNR	

the enemy might also have got the information. To circumvent this problem, an unique flag signalling, as a primary technique of anti-interception, was used to prevent information leakage. Nowadays, high-layer encryption techniques have been widely adopted to guarantee information security, such as the works done in [1]. However, with the development of mobile Internet, traditional cryptographic techniques may be insufficient or even not suitable, since an additional secure channel is required for private key exchanges [2]. Fortunately, physical layer security (PHY-security) enables the secure communications by only exploiting the characteristics of wireless channels, e.g., fading, noise, and interferences, so as to avoid the use of extra spectral resources and to reduce signalling overhead [3]–[6]. Specifically, there exist channel codes, e.g., Wyner codes [4], polar codes [7], and low-density parity-check (LDPC) codes [8], to guarantee communication security and reliability simultaneously at physical layer based on the randomness of wireless channels.

Although PHY-security can be measured by instantaneous, statistical, or asymptotical performance metrics, as shown in Table I, the performance of PHY-security is determined in essence by the performance gap of a legitimate channel and an eavesdropper channel [9]–[12]. This is intuitive since PHY-security aims to make the transmission rate higher than the eavesdropper channel capacity, but lower than the legitimate channel capacity. In this context, one should simultaneously improve the received signal power at the legitimate receiver and impair the received signal quality at the eavesdropper in order to provide a fast, secure, and reliable communication. However, in single-antenna systems, there are only limited effective means to improve communication security, wherein power allocation may be a possible means to enhance wireless security. It is worth pointing out that power allocation in PHY-security is a nontrivial task, because transmit power will affect the quality of both legitimate and eavesdropped signals. In general, the associated optimization problem in power allocation is nonconvex and there is no well-known systematic approach for obtaining a globally optimal solution. In [13], a suboptimal power allocation scheme was proposed to minimize signal-to-interference-plus-noise-ratio (SINR) at an eavesdropper, instead of maximizing the secrecy rate directly. Nevertheless, minimizing the SINR at an eavesdropper is only an indirect performance metric to improve communication security, and the result cannot guarantee a nonnegative secrecy rate. Furthermore, an asymptotically optimal power and subcarrier allocation strategy was presented in [14] for maximization of ergodic secrecy rate in orthogonal frequency division multiple access (OFDMA) based broadband wireless networks. However, the performance gain in improved secrecy due to power allocation is limited, and thus it is difficult to guarantee any quality-of-service (QoS) for secure communications. For instance, it was shown in [15] that if interception distances between the source and the eavesdroppers are shorter than that between the source and the legitimate receiver, the secrecy performance is generally unsatisfactory in single-antenna systems. As a result, cooperative jamming was proposed by introducing an interference source, which can cripple the interception capabilities of an eavesdropper [16]. However, as shown in [17], a single-antenna jammer can also severely interfere with the legitimate receiver, and thus the secrecy performance may be even worse than that without cooperative jamming. Only if the jammer is close to the eavesdropper, the secrecy performance may be enhanced by cooperative jamming. However, this case seldom happens in practice.

Intuitively, if legitimate and eavesdropper channels are nearly orthogonal, it is easy to enhance the strength of legitimate signal and to impair the intercepted signal simultaneously by some means. However, since the legitimate and the eavesdropped signals are generated from the same source and pass through the same channel concurrently in general, it is impossible to separate them in time and frequency domains. A feasible method is to exploit the spatial degrees of freedom offered by multiple antennas. For example, if a source is equipped with multiple antennas, the information signal may be transmitted in the null space of the eavesdropper channel. Then, the eavesdropper will not able to receive any information, even if the interception distance is short. Similarly, if a jammer deploys multiple antennas, it can avoid interference leakage to a legitimate receiver, and hence improves the secrecy performance effectively. Naturally, multiple-antenna techniques for providing PHY-security are effective and powerful, and thus have drawn considerable attentions, as shown in [18]–[22] and the references given therein. It was shown in [23] that even with inter-antenna correlation, multiple-antenna techniques still might enhance wireless security. Nowadays, secure communication based on various multiple-antenna techniques has become a prevailing research topic. In particular, multiple-antenna relaying [24], [25], multiple-antenna jamming [26], [27], multiuser downlink or multiple access [28], [29], massive MIMO [30], [31], and multiple-antenna directional modulation [32]–[35], are exploited to improve the secrecy performance. In Fig. 1, we show a block diagram to classify multiple-antenna techniques for providing PHY-security in several different categories, which will be discussed in detail next.

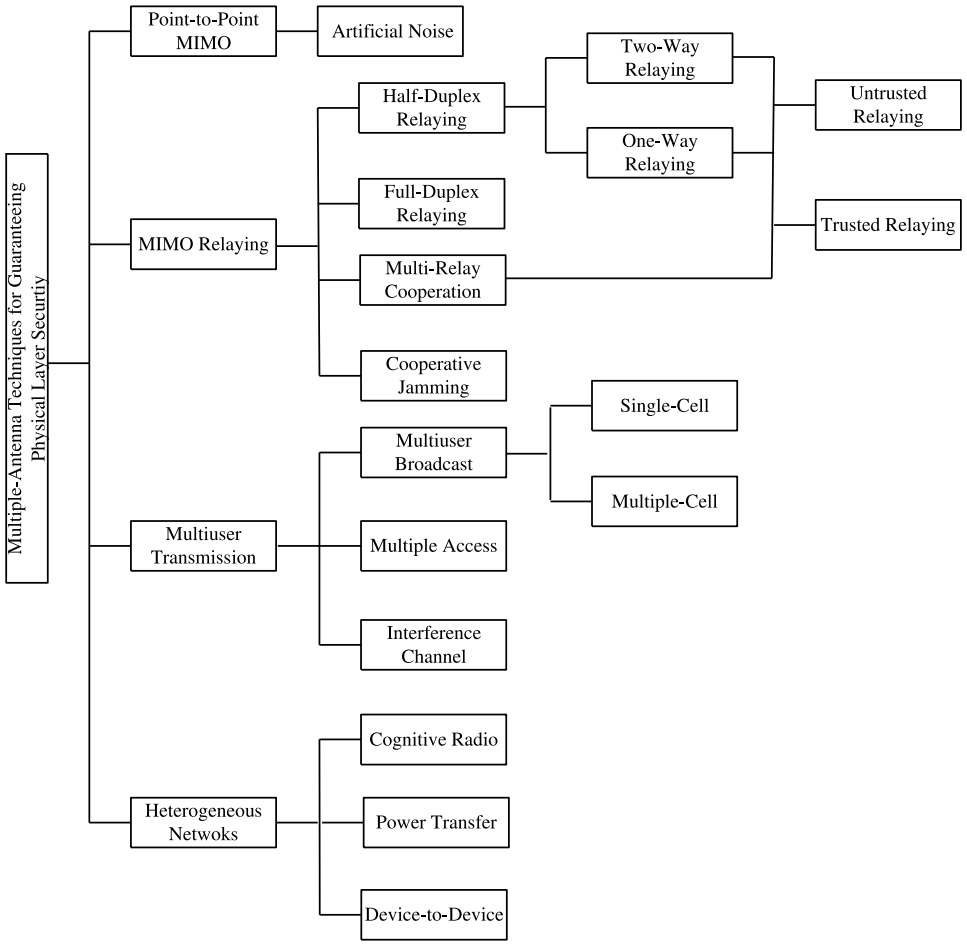


Fig. 1. An illustration of multiple-antenna techniques for guaranteeing PHY-security.

TABLE II
MULTIPLE-ANTENNA BF FOR PHY-SECURITY

Type	Name	Principle	Charateristics
Linear	ZF [36]	Transmit the signal in the null space of the eavesdropper channel	Simple but poor secrecy performance
	MMSE [37]	Minimize the MSE of the legitimate signal	Balance between performance and complexity
	GSVD [38]	Leverage the general SVD of the legitimate and eavesdropper channel matrices	Tradeoff between performance and complexity
Nonlinear	THP [39]	Employ a transmit feedback filter and a modulo operation on the transmitting signal	Good performance but high computational complexity
	DPC [40]	Successively cancel interference and reduce information leakage	Achieve the capacity region with unbearable complexity

A promising approach in multiple-antenna enabled PHY-security is to use various linear or nonlinear beamforming (BF) techniques, as listed in Table II. Although the design of BF can be done according to different criteria, a common goal is to direct the signal towards the legitimate destination, while reducing the signal strength at the eavesdropper direction by making use of spatial degrees of freedom [41]–[43]. For instance, in multiple-relay aided secure communications, cooperative secure beamforming is designed to maximize the information rate at a legitimated receiver, while completely eliminating information leakage to the eavesdroppers [44]. Besides, cooperative jamming plays an important role for guaranteeing communication security in two-hop relay systems. In particular, a legitimate receiver and a transmitter act as jammers in the first and second hops, respectively [45]. It is generally known that beamformer and jamming signal designs in multiple-antenna systems depend on the availability of channel state information (CSI) at the transmitter [46], [47]. Compared to traditional systems without considering PHY-security, enabling communication security via multiple antennas requires more complete CSI knowledge. Specifically, not only the CSI of legitimate channel, but also the CSI of eavesdropper channel is needed to facilitate the design of an efficient beamformer, since secrecy rate is determined by the legitimate and the eavesdropper channels jointly. In other words, the amount of CSI available at the transmitter determines the secrecy performance. For example, in cooperative jamming aided secure communications, if a jammer has full CSI of its own channel to a legitimate receiver, then interference to the legitimate receiver can be avoided completely by transmitting the jamming signal in the null space spanned by the channel of the legitimate receiver. However, if the jammer has only partial CSI, then there will be interference leakage to the legitimate receiver.

TABLE III
CSI COMBINATIONS IN POINT-TO-POINT SECURE COMMUNICATIONS

	Full ECSI	Deterministic imperfect ECSI	Indeterministic imperfect ECSI	Statistical ECSI
Full LCSI	Case 1	Case 2	Case 3	Case 4
Deterministic imperfect LCSI	Case 5	Case 6	Case 7	Case 8
Indeterministic imperfect LCSI	Case 9	Case 10	Case 11	Case 12
Statistical LCSI	Case 13	Case 14	Case 15	Case 16

Also, if the jammer has no CSI, the legitimate receiver may suffer from severer interference than the eavesdropper. In order to design an effective beamformer, the transmitter is required to know the CSI at least to a certain extent. The amount of CSI at the transmitter is commonly classified into four categories, including full instantaneous CSI, deterministic imperfect instantaneous CSI, indeterministic imperfect instantaneous CSI, and statistical CSI [48]. Note that CSI accuracy not only determines the secrecy performance, but also affects the performance metric. As shown in Table I, when full CSI is available, it is likely to achieve the secrecy rate. In general, it is difficult for a transmitter to obtain full eavesdropper CSI (ECSI), since the eavesdroppers are usually silent to hide their existence. Moreover, a transmitter also seldom obtains perfect full legitimate CSI (LCSI) due to feedback delay or channel estimation errors. Hence, it seems impractical to have global and perfect CSI at a transmitter. If CSI uncertainty is deterministic, a minimum secrecy rate in the worst case can be guaranteed. Otherwise, it is not possible to maintain a steady secrecy rate over all fading channel realizations. As a result, several other compromised secrecy performance metrics were proposed to quantify communication security statistically, such as ergodic secrecy rate [49], [50], secrecy outage probability [51], [52], and interception probability [53], [54]. In other words, perfectly secure communications can be guaranteed with a high probability. Moreover, the asymptotic characteristics of secrecy performance at a hight SNR, i.e., secrecy diversity order [55], [56] and secrecy degrees of freedom [57], [58], can also be obtained in a statistical sense. In Table III, we list sixteen CSI acquisition scenarios in point-to-point secure communication systems, where only cases 1, 2, 5, and 6 can provide perfectly secure communications. In addition, in multiple-antenna scenarios, the required amount of CSI increases significantly and CSI acquisition is expected to be more complicated. For example, in a MIMO relaying scenario [59], [60], a relay may have full CSI of the first hop and imperfect CSI of the second hop due to asymmetric characteristics of propagation channels.

As aforementioned, there are a large number of multiple-antenna techniques for enabling PHY-security with different CSI availabilities. Although people have studied this topic extensively, numerous theoretical and technical issues still remain open. Besides, we have not seen a complete survey to reveal multiple-antenna techniques in PHY-security in terms of fundamental results, recent advances, and future trends. For example, Mukherjee *et al*. [61] gave a primary investigation on multi-antenna techniques in multiuser wireless secrecy networks, but it did not take CSI accuracy into consideration. In fact, as discussed earlier, the CSI accuracy has a great impact on the secrecy performance of multi-antenna techniques.

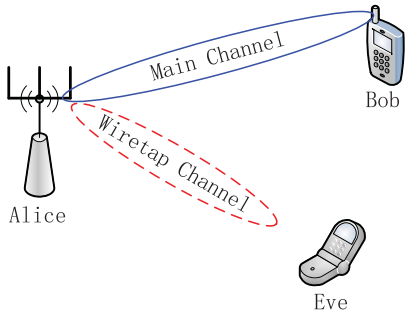


Fig. 2. A three-node point-to-point secure communication model.

In this article, we investigate state-of-the-art research results from the perspective of CSI accuracy and point out potential directions and challenges for future works.

The rest of this article can be outlined as follows. We first discuss secrecy beamforming in point-to-point multiple-antenna systems in Section II. Then, the cases of secure dual-hop MIMO relaying systems are investigated in Section III. In Section IV, we study PHY-security in multiuser systems. Section V focuses on the secrecy issues in heterogeneous networks, followed by the conclusions and future research directions in Section VI.

II. POINT-TO-POINT MULTI-ANTENNA TECHNIQUES

A three-node point-to-point secure communication model is a typical research model, which includes a transmitter (also known as Alice), a legitimate receiver (also known as Bob), and an eavesdropper (also known as Eve), as shown in Fig. 2. The transmitter sends a confidential message to the legitimate receiver, while the eavesdropper receives the signal and intends to decode it. Intuitively, this model serves as the smallest but fundamental component of all sophisticated secure communication systems. Thus, we start the analysis and the design of multiple-antenna secure communications from this three-node point-to-point model.

A. Secrecy Capacity

The crux of PHY-security is to deliver confidential messages with a maximum transmission rate, at which the eavesdropper is unable to decode any information. In analogy to general communications, the maximum achievable secrecy transmission rate is called secrecy capacity, which is a principal metric to measure wireless communication security. Generally speaking, secrecy capacity is determined by both the qualities of main channel, i.e., the channel between Alice and Bob, and the wiretap channel, i.e., the channel between Alice and Eve.

It is proved that in additive white Gaussian noise (AWGN) channels, the secrecy capacity is equal to the difference between the two channel capacities [62]. Mathematically, it can be expressed as

$$C_s = C_m - C_w, \tag{1}$$

where $C_m = \log_2(1 + \frac{P}{N_m})$ is the Shannon capacity of the main channel from Alice to Bob and $C_w = \log_2(1 + \frac{P}{N_w})$ is the Shannon capacity of the wiretap channel from Alice to Eve. Variables P, N_m, and N_w denote transmit power, noise power of the main channel, and noise power of the wiretap channel, respectively. In this case, it is possible to achieve secure communications only if the main channel has a better signal-to-noise ratio (SNR) than the wiretap channel, i.e., $\frac{P}{N_m} > \frac{P}{N_w}$. Furthermore, in a quasi-static flat fading scenario, the channel gains for the main and wiretap channels change randomly over different time slots but remain constant in each slot. Thus, a quasi-static fading channel in each time slot can be viewed as a complex AWGN channel. The secrecy capacity for a channel realization in the quasi-static fading scenario is given by [63]

$$C_s = \left[\log_2\left(1 + |h_m|^2 \frac{P}{N_m}\right) - \log_2\left(1 + |h_w|^2 \frac{P}{N_w}\right)\right]^+, \tag{2}$$

where h_m and h_w are the channel coefficients of the main and wiretap channels, respectively, and $[x]^+$ denotes the calculation of $\max(x, 0)$. However, the instantaneous secrecy capacity is different for different channel fading realizations. In order to evaluate the security in a long-term sense, i.e., across multiple coherent time slots, average secrecy capacity was proposed in [64] as a performance metric. To be more specific, the average secrecy capacity is equal to the maximum average instantaneous secrecy capacity over fading channels. In general, the average secrecy capacity is maximized through power allocation according to CSI at the transmitter. Thus, the average secrecy capacity may be different if a transmitter has different CSI combinations, as mentioned in Table III. For example, if a transmitter has the CSI of the main channel only, without CSI of the wiretap channel, power allocation is performed based only on the CSI of the main channel. Thus, the secrecy capacity in this case is in general lower than that with full CSI.

In summary, the secrecy capacity of the point-to-point systems is determined mainly by the capacity difference of the main and wiretap channels and CSI availability at the transmitter.

B. Beamformer Design

Among various physical layer techniques reported in the literature, multiple-antenna techniques can most effectively improve the secrecy capacity via simultaneously increasing the quality of the main channel and impairing that of the wiretap channel by spatial beamforming. In order to effectively exploit the benefits of multiple-antenna techniques for guaranteeing PHY-security, a proper design of transmit beamformer is necessary. As a simple example, if a transmitter has global and perfect CSI, it is possible to send a secret message in the null space of the wiretap channel, such that the eavesdropper cannot overhear any information. Nevertheless, it is clear that this orthogonal beamforming scheme is not optimal from the viewpoint of maximizing the secrecy capacity, since it may partially sacrifice spatial degrees of freedom for improving the received strength at a legitimate receiver. Hence, it is imperative to strike a balance between enhancing the quality of legitimate channel and degrading the quality of wiretap channel.

Unfortunately, it is a challenging task to design an optimal beamformer to enable secure communications under general system settings, since the objective function of the secrecy capacity is unlikely to be a convex function of the transmit beamformer. Thus, Khisti and Wornell [65] considered a special case, where a transmitter and an eavesdropper are equipped with multiple antennas and the intended receiver is a single-antenna device. If the channel matrices are fixed and known to all the terminals, it was proved that the capacity-achieving beamformer has a direction along the generalized eigenvector corresponding to the maximum generalized eigenvalue of the main and wiretap channels. Then, through asymptotic analysis, it was also found that a simple masked beamforming scheme that radiates the signal power isotropically in all directions can attain near-optimal performance in a high SNR region. On the other hand, the authors also studied the case of a multiple-antenna legitimate receiver in [66]. Compared to the case of a single-antenna legitimate receiver, the case with a multiple-antenna legitimate receiver is much more complicated. It was shown that in order to achieve the secrecy capacity, the transmit signal should be coded based on Gaussian wiretap codebooks. To get more insights, Fakoorian and Swindlehurst [67] calculated the rank of the optimal input covariance matrix. In particular, the authors revealed the relationship between the rank and the channel matrices for the legitimate receiver and the eavesdropper. Furthermore, the authors determined the necessary and sufficient conditions that an optimal input covariance matrix is full rank and presented a method for characterizing the resulting covariance matrix.

1) Beamforming With Full CSI: Even if full CSI is available, it is in general difficult to design an optimal transmit beamformer. In order to obtain a tractable solution, alternative optimization schemes were proposed accordingly. In [68], the objective function was divided into two components, namely the main channel capacity and the wiretap channel capacity. Through maximizing the main channel capacity subject to a constraint on the wiretap channel capacity, a suboptimal beamforming scheme was presented. Moreover, Cumanan *et al.* [69] approximated the secrecy capacity based on a Taylor series expansion, and thus transformed the original problem into a tractable convex optimization problem. By considering practical finite-alphabet input, Wu *et al.* [70] developed an iterative algorithm for finding an optimal precoding matrix based on a gradient descent method with a backtracking line search. The main difficulty in designing the optimal beamformer lies in the non-convexity of the secrecy capacity. Another possible way to design a suboptimal beamformer is to replace the nonconvex objective function with other relevant convex performance metrics. For example, the mean-squared

TABLE IV
BEAMFORMER DESIGN IN POINT-TO-POINT MULTIPLE-ANTENNA SYSTEMS WITH FULL CSI

Author	System model	Contributions
A. Khisti *et al.* [65]	Multi-antenna transmitter, eavesdropper, and single-antenna receiver	Design capacity achieving beam along the direction of generalized eigenvector corresponding to the maximum generalized eigenvalue of the main and wiretap channels
A. Khisti *et al.* [66]	Multi-antenna transmitter, eavesdropper, and receiver	Suggest that capacity achieving transmit signal should be coded based on Gaussian wiretap codebooks
S. Fakoorian *et al.* [67]	Multi-antenna transmitter, eavesdropper, and receiver	Derive an expression of optimal input variance when the optimal solution is full-rank
Q. Li *et al.* [68]	Multi-antenna transmitter, eavesdropper, and receiver	Propose an alternative optimization water-filling algorithm based on iterations
K. Cumanan *et al.* [69]	Multi-antenna transmitter, eavesdropper, and receiver	Propose an iterative algorithm to maximize approximated secrecy rate based on Taylor series expansion
Y. Wu *et al.* [70]	Multi-antenna transmitter, eavesdropper, and receiver	Develop an iterative algorithm for finding an optimal linear precoding matrix with finite-alphabet input
H. Reboredo *et al.* [71]	Multi-antenna transmitter, eavesdropper, and receiver	Design transmit and receive filters, which minimize MSE between legitimate parties; whilst assuring that eavesdropper MSE remains above a certain threshold
H. Zhang, *et al.* [72]	Multi-antenna transmitter, eavesdropper, and receiver	Propose an iterative algorithm to maximize approximated energy efficiency based on Taylor series expansion
Z. Rezki, *et al.* [73]	Multi-antenna transmitter, eavesdropper, and receiver	Achieve finite-SNR diversity-multiplexing trade-off with zero-forcing transmit scheme

error (MSE) is a commonly used performance metric in conventional wireless communications. Reboredo *et al.* [71] formulated a beamforming design problem as an optimization problem for minimizing the MSE at a legitimate receiver, while assuring that the MSE at the eavesdropper remains to be above a given threshold. Taking green communications into consideration, Zhang *et al.* [72] derived an iterative algorithm to design a beamformer to maximize energy efficiency (EE) of the system subject to secrecy rate and transmit power constraints. Additionally, the concept of diversity-multiplexing trade-off was also introduced into multiple-antenna secure communications [73]. A brief summary of beamformer design in point-to-point multiple-antenna systems with full CSI is given in Table IV.

2) Robust Beamforming: In the aforementioned works [65]–[73], the beamformer design was done based on the assumption of full CSI at the transmitter. However, in practice, the transmitter in multiple-antenna systems usually obtain only partial CSI through information feedback from the receiver(s) [74]–[76] in frequency division duplex (FDD) systems or directly using channel reciprocity [77]–[79] in time division duplex (TDD) systems. Indeed, the accuracy of CSI has a great impact on the performance of multiple-antenna systems. Especially in multiple-antenna secure communication systems, if a transmitter has imperfect CSI, there is a high probability in information leakage to the eavesdropper, resulting in secrecy performance degradation [80]. Thus, it is imperative to design robust beamforming schemes to reduce the performance degradation. Lin *et al.* [22] considered the case of partial CSI of the main channel at the transmitter. A modified Lloyd algorithm was proposed to construct codebooks for conveying a quantized precoder from a legitimate receiver to the transmitter. Moreover, a low-complexity post-processing algorithm was proposed to compensate for SNR loss due to partial CSI. Note that in secure communications, the eavesdropper is usually passive and keeps silent, and thus the transmitter may have a little or even no eavesdropper CSI. Assuming the availability of partial eavesdropper CSI, Chu *et al.* [81] proposed a robust beamforming scheme to maximize the secrecy rate, subject to maximum secrecy outage probability and maximum transmit power constraints. Furthermore, a semi-definite programming (SDP) approach was used in [82] to solve a robust beamforming optimization problem in a scenario that both the legitimate and the eavesdropper CSI are imperfect. If there is no eavesdropper CSI, the optimal beamformer should be designed to align with the legitimate channel. In this case, Bashar *et al.* [83] exploited a predetermined codebook to convey the quantized legitimate CSI, and analyzed the effect of limited feedback on the secrecy outage probability. A special beamforming scheme, namely transmit antenna selection, was adopted to enhance wireless security by taking into account of outdated legitimate CSI without eavesdropper CSI in [84]. It was shown that the expected diversity gain due to the antenna selection process cannot be realized when CSI is outdated. On the other hand, in fast fading channels, the channel coefficients may change in every symbol. The cost for CSI feedback or estimation in tracking the variation of channels may be prohibitive for practical systems. Thus, utilizing statistical CSI is a better option for beamforming design since the channel statistic change slowly over time. Interestingly, it was found that using Gaussian distributed input with equal power allocation is optimal when the number of antennas at the receiver is larger than that at the eavesdropper [85]. In the worst-case scenario with no CSI at any node, it was proven that a constant norm channel input can achieve maximum secure degrees of freedom over MIMO Rayleigh block fading wiretap channels [86]. We provide a summary of robust beamforming schemes in Table V for point-to-point secure communications.

C. Power Allocation

In secure communications, secrecy capacity is not necessarily an increasing function of transmit power, since both the capacities of the main and wiretap channels improve with increased transmit power. Therefore, it makes sense to allocate transmit power according to the states of the main and wiretap channels for optimizing secrecy performance. Similarly, the design of power allocation depends heavily on the available CSI at the transmitter. Under a practical assumption of full legitimate CSI and partial eavesdropper CSI in terms of

TABLE V
ROBUST BEAMFORMING SCHEMES FOR POINT-TO-POINT SECURE COMMUNICATIONS

Authors	System model	CSI accuracy	Contributions
C-H. Lin *et al.* [81]	Multi-antenna transmitter, eavesdropper, and receiver	Partial legitimate CSI, no eavesdropper CSI	Propose a precoding and post-coding system to achieve data secrecy
Z. Chu *et al.* [82]	Multi-antenna transmitter, eavesdropper, and receiver	Perfect legitimate CSI, imperfect eavesdropper CSI	Propose a robust beamforming scheme to maximize secrecy rate
Q. Li *et al.* [83]	Multi-antenna transmitter, single-antenna receiver, and multiple multi-antenna eavesdroppers	Imperfect legitimate CSI, imperfect eavesdropper CSI	Develop an optimal robust beamforming scheme via SDP
S. Bashar *et al.* [84]	Multi-antenna transmitter, eavesdropper, and single-antenna receiver	Partial legitimate CSI, no eavesdropper CSI	Analyze the effect of codebook design on secrecy outage probability
N. Ferdinand *et al.* [85]	Multi-antenna transmitter, single-antenna eavesdropper, and receiver	Outdated legitimate CSI, no eavesdropper CSI	Provide an antenna selection scheme to maximize SNR at receiver
S-C. Lin *et al.* [86]	Multi-antenna transmitter, eavesdropper, and receiver	Statistical legitimate CSI, statistical eavesdropper CSI	Show that using Gaussian distributed input with equal power allocation is optimal
T-Y. Liu *et al.* [87]	Multi-antenna transmitter, eavesdropper, and receiver	No legitimate CSI, no eavesdropper CSI	Prove that a constant norm channel input can achieve maximum secure degrees of freedom

average received SNR, it was found that the optimal power allocation is regulated in an on-off manner defined by a threshold depending only on the numbers of transmit antennas and the average SNRs of both main and wiretap channels [87]. If there is no legitimate CSI at a transmitter, the Alamouti space-time code can be used to enhance the wireless security by combining antenna selection and power allocation. Specifically, in each fading block over two time slots, two antennas at a transmitter with the highest channel gains are selected based on the feedback from the legitimate receiver. The transmitter uses the two antennas to send Alamouti coded symbols for secure information transmission. During the transmissions, the transmitter optimizes the transmit power from the two antennas, so as to minimize the secrecy outage probability [88].

Considering the requirement of green communications, energy efficiency, defined as the ratio of secrecy rate and total power consumption, has become an important performance metric for secure communications. Thus, power allocation from the perspective of maximizing the energy efficiency is receiving more and more attention [89]. However, even with full CSI, energy-efficient power allocation for PHY-security is nontrivial, because energy efficiency is in general nonconvex with respect to transmit power. In this context, several alternative optimization schemes have been proposed to solve this challenge to some extent. Zhang *et al.* [72] applied a Taylor series expansion to the expression of secrecy rate, and thus the approximated secrecy rate is quasi-convex. Then, by using classical fractional programming, an energy-efficient power allocation strategy was derived. Furthermore, Zappone *et al.* [90] proposed to perform eigenvalue decomposition and selection to the expression of the secrecy rate before Taylor series expansion, which may reduce the complexity of power allocation. Also, efforts have been made to achieve energy-efficient power allocation under a practical assumption that eavesdropper CSI is unavailable at the transmitter. In this case, energy efficiency is usually defined as a ratio of secrecy outage capacity and total power consumption. The special case with a high SINR was considered in [91], in order to make the energy-efficient optimization problem tractable. Differently, Chen *et al.* [92] made use of the property of channel hardening to design an energy-efficient power allocation scheme for a massive MIMO based secure communication system. Table VI gives a summary of the above reviewed power allocation schemes.

D. Artificial Noise

According to the definition of secrecy capacity, as shown in Eqn. (2), the secrecy capacity is a decreasing function of the interception distance between a transmitter and an eavesdropper. A challenging issue in guaranteeing PHY-security arises if the eavesdropper is usually located closer to the transmitter than the legitimate receiver, namely short-distance interception. In this context, even if spatial beamforming is used, the secrecy performance may not be satisfactory. To further improve communication security, artificial noise (AN) is inserted into the transmit signal intentionally to confuse the eavesdropper [93], [94], as shown in Fig. 3(a). The key of AN design is to avoid interference leakage to the legitimate receiver, while impairing the intercepted signal at the eavesdropper. To this end, AN is adopted in conjunction with multiple-antenna techniques. Specifically, by exploiting spatial degrees of freedom offered by multiple transmit antennas, it is possible to adjust the directions of AN and the transmit signal jointly through spatial beamforming, so as to optimize the secrecy performance [95]–[98]. Intuitively, the performance of AN is determined by the accuracy of CSI at the transmitter. If the transmitter has full CSI, there are maximum spatial degrees of freedom available to design the beamformer. However, in practice, the eavesdropper CSI is usually imperfect or even unavailable. To deal with imperfect CSI in both the main and wiretap channels, Tang *et al.* [99] proposed a robust beamforming scheme to maximize the worst-case secrecy rate via SDP. To further relax the assumptions of imperfect eavesdropper CSI, Wang *et al.* [100] considered a case of perfect legitimate CSI and statistical distribution of the wiretap channel for MISO secure communications. Aiming to maximize the achievable secrecy rate, they suggested a beamforming scheme and the corresponding optimal power allocation between the transmit signal and AN. Then, the scheme was extended to the case of MIMO systems in [101], where a lower bound on

TABLE VI
POWER ALLOCATION SCHEMES FOR POINT-TO-POINT SECURE COMMUNICATIONS

Authors	System model	CSI accuracy	Contributions
T. Nguyen *et al.* [88]	Multi-antenna transmitter, eavesdropper, and single-antenna receiver	Full legitimate CSI, partial eavesdropper CSI	Optimal power control is regulated in an on-off fashion with the threshold depending only on the number of antennas and the average SNRs
S. Yan *et al.* [89]	Multi-antenna transmitter, eavesdropper, and receiver	No legitimate CSI, No eavesdropper CSI	Propose a joint antenna selection and power allocation scheme based on Alamouti coding
H. Zhang *et al.* [91]	Multi-antenna transmitter, eavesdropper, and receiver	Full legitimate CSI, Full eavesdropper CSI	Propose a suboptimal energy-efficient power allocation scheme using Taylor series expansion
A. Zappone *et al.* [92]	Multi-antenna transmitter, eavesdropper, and receiver	Full legitimate CSI, Full eavesdropper CSI	Propose a suboptimal energy-efficient power allocation scheme using eigenvalue selection and Taylor series expansion
D. W. K. Ng *et al.* [93]	Multi-antenna transmitter, eavesdropper, and single-antenna receiver	Full legitimate CSI, No eavesdropper CSI	Propose an energy-efficient power allocation scheme at a high SINR
X. Chen *et al.* [94]	Large-scale antenna transmitter, single-antenna receiver, and eavesdroppers	Imperfect legitimate CSI, no eavesdropper CSI	Propose an energy-efficient power allocation scheme using channel hardening

TABLE VII
ARTIFICIAL NOISE JAMMING IN POINT-TO-POINT MULTI-ANTENNA SYSTEMS

Authors	CSI accuracy	Contributions
Y. Tang *et al.* [101]	Imperfect legitimate CSI, imperfect eavesdropper CSI	Solve the worst-case secrecy rate maximization problem via SDP
B. Wang *et al.* [102]	Perfect legitimate CSI, statistical eavesdropper CSI	Provide optimal beamforming and the corresponding power allocation scheme
S-H. Tsai *et al.* [103]	Full legitimate CSI, statistical eavesdropper CSI	Propose a water-filling power allocation scheme to maximize the lower bound on secrecy rate
X. Zhou *et al.* [104]	Perfect legitimate CSI, perfect eavesdropper CSI	Obtain an expression of achievable secrecy rate and give the corresponding power allocation scheme
X. Zhang *et al.* [105]	Perfect legitimate CSI, perfect eavesdropper CSI	Provide power allocation and rate parameter of wiretap code for achieving maximal throughput
S-C. Lin *et al.* [106]	Quantized legitimate CSI, no eavesdropper CSI	Propose an optimal power allocation scheme to maximize secrecy rate under AN leakage
X. Zhang *et al.* [107]	Quantized legitimate CSI, no eavesdropper CSI	Present a joint wiretap coding rate, transmit power, and feedback amount optimization scheme to maximize throughput
Y. Yang, *et al.* [108]	Outdated legitimate CSI, no eavesdropper CSI	Propose a power allocation scheme to minimize the upper bound on secrecy rate loss due to delayed feedback

the secrecy rate was derived and a water-filling power allocation scheme was presented to maximize the lower bound. In the situation without eavesdropper CSI at the transmitter, it is optimal to transmit the desired signal in the direction of the legitimate receiver and send AN in the orthogonal space of the main channel in order to maximize the received SNR and avoid the interference to the legitimate receiver simultaneously. Zhou and McKay [102] and Zhang *et al.* [103] analyzed the secrecy performance and designed the corresponding power allocation scheme over fast and slow fading channels, respectively. In slow fading channels, the channel coherence time is usually longer than the length of a codeword, and in such a scenario, secrecy outage probability is adopted as the performance metric. In contrast, in fast fading channels, the channel coherence time is much shorter than the length of a codeword, and the ergodic secrecy rate becomes a more appropriate performance metric. In a more practical scenario where the transmitter has only partial CSI through limited feedback from the legitimate receiver, the AN that was originally intended to jam the eavesdropper may now strongly interfere the main channel, causing a significant secrecy rate loss. In [104], the impact of quantized channel feedback was investigated in detail, and a power allocation scheme for information signal power and the AN power was proposed to maximize the secrecy rate. Moreover, the authors also revealed the relationship between the amount of feedback and the power allocation. It was found that when the amount of feedback is sufficiently large, one should allocate power evenly among the desired and AN signals; whereas when the amount of feedback is small, one should be more conservative in allocating power to the AN signal. The secrecy performance with limited CSI feedback is further improved by optimizing the amount of feedbacks and transmit power jointly [105]. It was shown that a good strategy is to use approximately 20% of feedback bits to quantize the channel gain information, with the remainder to quantize the channel direction information. During CSI feedback from the legitimate receivers, the feedback delay may lead to CSI mismatch. In [106], the effect of feedback delay was studied and an optimal power allocation scheme was given to minimize the performance loss. A summary of artificial noise jamming schemes is shown in Table VII.

It is worth pointing out that AN does not have to be necessarily sent by an information transmitter. In practice, AN can also be transmitted by a legitimate receiver [107], as shown in Fig. 3(b). In this scenario, the CSI feedback for the design of AN is not required, which significantly reduces the overhead. A problem of this scheme is the self-interference caused at a legitimate receiver, which impairs the information signal reception performance. Fortunately, since the receiver knows the AN signal in prior, it may cancel the interference in the received signal via successive interference cancellation. Furthermore, it is possible to send the AN from both information transmitter and legitimate receiver, as shown in Fig. 3(c), so as to enhance the communication security. In [108], a full-duplex wireless technique was applied

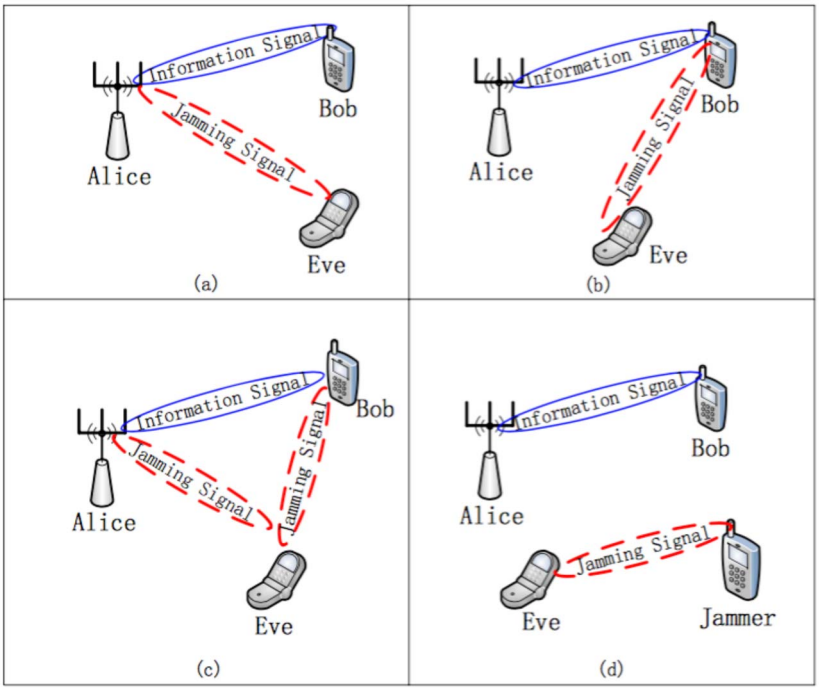


Fig. 3. Four cooperative jamming models of point-to-point secure communications.

to suppress the self-interference at the receiver for mitigating the effect of self-interference on the received signal. A more general case was considered in [109], where two nodes exchange information in the presence of an eavesdropper. To ensure communication security, AN is inserted into the transmitted signals from both nodes, and a full-duplex wireless technique was employed to cancel the interference at the two nodes. On the other hand, AN can also be sent by an external helper, which is also known as cooperative jammer, as shown in Fig. 3(d). Yet, the jamming signal will simultaneously cause interference to a legitimate receiver and an eavesdropper. Fakoorian and Swindlehurst [110] revealed a structure of the AN covariance matrix that guarantees a secrecy rate, which is at least equal to the secrecy capacity of the wiretap channel without jamming signal. Intuitively, it is optimal to send AN in the null space between the helper and the legitimate receiver [111]. However, this scheme requires additional coordination and synchronization between the helpers, which consumes extra overhead. To relax this requirement, an uncoordinated cooperative jamming scheme was proposed in [112]. In this scheme, although the helpers require only local CSI, it has been shown that the secrecy rate performance is close to the optimal one. A more general case was studied in [113], where a cooperative jammer got partial local CSI from the legitimate receiver for designing the AN signal. Especially, the relation between the secrecy performance and the amount of CSI feedback was exactly revealed.

E. Multiple-Eavesdropper Case

The worst case for point-to-point secure communications is that there are multiple eavesdroppers concurrently overhearing the message sent from a transmitter to the legitimate receiver. Compared to a single-eavesdropper case, the multiple-eavesdropper case has a poor secrecy performance. This is because, on one hand, the eavesdropping capability is enhanced. On the other hand, more spatial degrees of freedom should be used to despair the eavesdropper, and thus the quality of the legitimate signal is decreased accordingly. In [114], the impact of the number of eavesdroppers on the secrecy outage probability was investigated. It was shown that once the number of eavesdroppers is large enough, the interception probability approaches to one. In general, there are two typical scenarios for multiple-eavesdropper interception [102], [115]. The first one is referred to as colluding eavesdropping, where multiple eavesdroppers eavesdrop the message cooperatively. It is clear that this scenario is equivalent to that of a multiple-antenna eavesdropper with spatially distributed antennas. Multiple-eavesdropper colluding eavesdropping is in general a worse case, since the eavesdroppers have the strongest capability. In this case, even with full channel state information (CSI) about the eavesdropper channel, the legitimate transmitter should be equipped with more antennas for guaranteeing security. However, due to the size limitation, it is difficult for a general wireless node to be equipped with a large number of antennas. More importantly, eavesdroppers are usually passive and well hidden, and thus eavesdropper CSI is imperfect or even unavailable. In other words, it is impossible to transmit the signal in the null space of the eavesdropper channels. Even with the aid of AN, multiple AN signals are required to simultaneously confuse these eavesdroppers, resulting in a high power consumption. If eavesdropper CSI is imperfect, the efficiency of AN would be further decreased. Even worse, if legitimate CSI is not perfect at the transmitter either, the AN aided secure schemes might be unavailable,

since the AN would interfere with the legitimate receiver. The second scenario is non-colluding eavesdropping, where each eavesdropper independently overhears the message. In this scenario, the secrecy rate is limited by the eavesdropper with the strongest eavesdropping capability. Therefore, the multiple-antenna techniques are commonly designed by optimizing the minimum secrecy rate. Li *et al.* [68] used an alternating optimization method to design transmit beamforming for maximizing the secrecy rate in the ideal case of full CSI. To avoid the challenge that the secrecy rate is nonconvex, the transmit beamforming was designed by minimizing the transmit power, while satisfying a minimum secrecy rate constraint in [116]. Especially, robust beamforming was also studied by considering deterministic imperfect eavesdropper CSI. Moreover, AN is usually adopted to confuse the eavesdroppers together with adaptive beamforming. Similarly, the maximization of secrecy rate and the minimization of transmit power were regarded as the optimization objectives for jointly designing transmit beamforming and AN in [97] and [117], respectively. As shown in these previous works, with the goal of providing a secure communication with quality of service (QoS) guarantee in the case of multiple eavesdroppers, more resources, i.e., antennas, power, and spectrum, are needed. In order to achieve a balance between secrecy performance and resource consumption, it makes sense to design the multiple-antenna secure schemes from the perspective of maximizing the resource utilization efficiency. However, resource-efficient design is an open issue even in the scenario of a single eavesdropper, since resource efficiency is not or cannot be simply approximated by a convex function.

Remarks: Although point-to-point communication is the simplest secure communication model, extensive studies have already been done on it, which provides some useful guidelines for designing the multiple-antenna techniques. First, CSI accuracy influences the performance metric. If full CSI is available, secrecy rate can be used to measure wireless security. If CSI is imperfect but channel uncertainty is bounded, it is possible to obtain a secrecy rate in the worst case. For this, robust optimization is usually adopted though maximizing the minimum rate. If channel uncertainty is unbounded or even only statistical CSI is available, the secrecy performance can be evaluated and optimized only in a statistical sense. Usually, some heuristic methods are utilized to design the multiple-antenna techniques. For example, assuming that eavesdropper CSI is unavailable, we know that maximum ratio transmission (MRT) might be a good choice to maximize the SNR at the legitimate receiver. Second, it is difficult to optimize the secrecy rate directly even in a point-to-point model, since the difference of two logarithmic functions is nonconvex. So far, there are two methods to partially solve this challenge. The first method is based on sightly revision on a secrecy rate expression, such as adopting a Taylor series expansion. The second method is to replace the secrecy rate with bounded SINRs at the legitimate receiver and the eavesdropper, respectively. Clearly, these design principles are also applicable in more complicated multiple-antenna scenarios, such as dual-hop relaying systems as discussed in the next section.

III. Dual-Hop Multi-Antenna Relay Techniques

According to the definition of secrecy capacity in Section II-A, interception distance has a great impact on wireless security. Especially, if an eavesdropper is closer to the transmitter than the legitimate receiver, the secrecy performance may not be satisfactory. In point-to-point systems, it is impossible to shorten the access distance to enhance communication security. Several pioneer works revealed that the utilization of cooperative relay may facilitate security in wireless communications due to short access distance through relay forwarding [118]–[120]. In particular, a multiple-antenna relay or multiple cooperative relays can effectively enhance wireless security [121]. On one hand, a relay helps the transmitter by enhancing received signal quality at the legitimate receiver through cooperative diversity. On the other hand, it can weaken the interception capability of an eavesdropper by deteriorating the channel quality through spatial beamforming or jamming. Compared to traditional point-to-point secure communication systems, even though dual-hop secure relay systems introduce only an additional relay node, its design and optimization become more complicated [122]. First, it involves more system parameters, such as transmit beamformers, transmit powers, relay transmit durations, and relaying protocols. Second, the transmission schemes adopted in the source and the relay are naturally coupled. Thus, a joint design of the transmission scheme may be required, and this may lead to a high computational complexity. Third, to fully exploit the benefits of multiple-antenna relay techniques for guaranteeing PHY-security, the transmitters (the source and the relay) require full or at least partial CSI. In other words, the CSI between multiple nodes should be collected, yielding more system overheads for exchanging CSI. In the sequel, we provide a survey on multi-antenna relay techniques for guaranteeing PHY-security from the perspectives of relay protocols, schemes, and roles, respectively.

A. Relay Protocols

In secure relaying communications, a source wishes to send confidential messages to a destination, while leveraging the help from a relay node to hide the messages from the eavesdropper(s). Thus, relaying protocol has a great impact on the secrecy performance. For example, amplify-and-forward (AF) [123]–[125] and decode-and-forward (DF) [126]–[128] are two commonly adopted relay protocols. An AF relay amplifies and forwards the noise polluted signal, while a DF relay forwards the original signal after decoding the received signal at the relay. From the perspective of PHY-security, it is not easy to judge which protocol is better, especially in multiple-antenna relaying systems. In practice, relay protocol can be combined with various transmit precoding and receive detection techniques [129], [130] at the source and the relay, leading to a complicated design of relaying protocol. In the following, we discuss the PHY-security issues in AF and DF relays.

1) AF Protocol: Based on AF relay protocol, a multiple-antenna relay forwards a weighted version of the received

TABLE VIII
BEAMFORMING FOR AF SECURE RELAY COMMUNICATIONS

Authors	CSI accuracy	Contributions
H-M. Wang *et al.* [135]	Global CSI	Propose a joint GSVD precoding at source and ZF-SVD precoding at relay and a power allocation scheme
M. Mirzaee *et al.* [136]	Global CSI	Provide a joint design method of transmit and receiver beamforming at relay
X. Wang *et al.* [137]	Full legitimate CSI, imperfect eavesdropper CSI	Design a robust relay beamformer, including optimal rank-one, MF, and ZF beamformer
Y. Yang *et al.* [138]	Global CSI	Present secrecy rate maximization beamforming and null space beamforming for cooperative relays

TABLE IX
BEAMFORMING FOR DF SECURE RELAY COMMUNICATIONS

Authors	CSI accuracy	Contributions
M. Jilani *et al.* [139]	Full legitimate CSI, no eavesdropper CSI	Propose a joint GSVD precoding at source and ZF-SVD precoding at relay and power allocation scheme
D. W. K. Ng *et al.* [140]	Imperfect legitimate CSI, no eavesdropper CSI	Provide a robust resource allocation and scheduling scheme
J. Li *et al.* [141]	Global CSI	Design an optimal relay beamformer to maximize secrecy rate and minimize transmit power, respectively
X. Chen *et al.* [142]	Imperfect legitimate CSI, no eavesdropper CSI	Compare secrecy outage capacity of AF and DF protocols

noisy signal that it heard. In dual-hop AF secure MIMO relaying networks, even with full CSI, the optimal scheme to achieve the secrecy capacity involves solving a nonconvex optimization problem that is still widely open. Aiming to find an efficient way to enhance the secrecy rate with a tractable resource allocation algorithm, Wang *et al.* [131] proposed a suboptimal joint source and relay linear precoding and power allocation scheme based on AF relaying protocol. In this scheme, a source node adopts a generalized singular value decomposition (SVD) based precoding to transmit the signal in the first phase, and a multiple-antenna relay node forwards the received signal based on the SVD precoding in the null space of the wiretap channel in the second phase. Power allocations in both phases were optimized to maximize the secrecy rate by an iterative alternating optimization algorithm. Mirzaee and Akhlaghi [132] focused on a joint design of transmit and receive beamforming at a relay, so as to maximize the achievable secrecy rate subject to a maximum relay transmit power constraint. Considering imperfect CSI of an eavesdropper, Wang *et al.* [133] studied the problem of designing a robust relay beamformer, including optimal rank-1, match-and-forward (MF), and zero-forcing (ZF) beamformers. It was found that in a deterministic CSI uncertainty model, the optimal rank-1 beamformer is equivalent to an MF beamformer. Additionally, multi-relay cooperative secure beamforming for relay networks was developed in [134]. Superficially, a secrecy rate maximization (SRM) beamforming scheme was proposed under both total and individual relay power constraints. Then, in order to reduce the computational complexity, a null space beamforming scheme was presented through maximizing the information rate at the destination, while completely eliminating the information leakage to the eavesdropper. A brief summary of beamforming schemes for AF secure relay communications is given in Table VIII.

2) DF Protocol: Based on DF relay protocol, a multiple-antenna relay forwards a weighted version of the signal that it heard. Since the received noise at the relay is removed during decoding, the relay has more degrees of freedom for improving the system performance compared to the AF relay protocol. In [135], under an assumption that the eavesdropped CSI is unavailable, joint SVD and generalized SVD (GSVD) precoding were applied to enhance wireless security. Specifically, at the information source, the GSVD was performed to simultaneously diagonalize the channel matrices of the relay and the legitimate destination. Then, at the relay, the SVD was performed to beamform the signal towards the destination. In [119], the problem of resource allocation and scheduling in MIMO-OFDMA relaying systems with imperfect CSI was addressed. The packet data rate, secrecy data rate, power and subcarrier allocation policies were optimized jointly to maximize the average secrecy outage capacity. Similarly, multiple-relay cooperative beamforming scheme can be combined with DF relay protocol. In [136], the optimal relay beamformers were designed with the goals of maximization of achievable secrecy rate and minimization of the total transmit power, respectively. The secrecy performance of AF and DF relay protocols was analyzed and compared to the scenario that the relay is equipped with a large number of antennas in [137]. It was shown that with high transmit powers, AF relay protocol is always better than DF relay protocol from the perspectives of both secrecy performance and implementation complexity. A brief summary of beamforming schemes for DF secure relay communications is given in Table IX.

In addition to commonly used AF and DF, several other relaying protocols also exhibit a good performance under some special conditions. In [138], randomize-and-forward (RF) relay protocol was studied in four-node relaying networks. It was shown that RF is always better than DF from the perspective of secure connection. Compute-and-forward (CF) relaying protocol was adopted in a bidirectional relaying network in [139]. In particular, a relay computes a function of two messages using naturally occurring sum of symbols simultaneously transmitted by user nodes in a Gaussian multiple access channel, and the computed function value is forwarded to the user nodes in an ensuing broadcast phase. A modify-and forward (MF) relaying proposal was proposed in [140], where the relay first modifies the message received from the source and then

TABLE X
RELAY PROTOCOLS IN SECURE RELAY COMMUNICATIONS

Protocols	Definition	Characteristics
AF [127]	Left-multiply the received signal by a transforming matrix, and then forward it	Simple but amplify noise
DF [130]	Decode the received signal, and then forward it	Suffer high complexity but without noise amplification
RF [143]	Use independent randomization for the forwarding signal	Need extra randomly coding
CF [144]	Compute a function of the superposed messages, and then forward the function value	Increase the complexity of the destination
MF [145]	Modify the received message, and then forward it	Need extra information exchange for the modification
NF [146]	Send an independent noise signal	Fail to enhance the legitimate signal

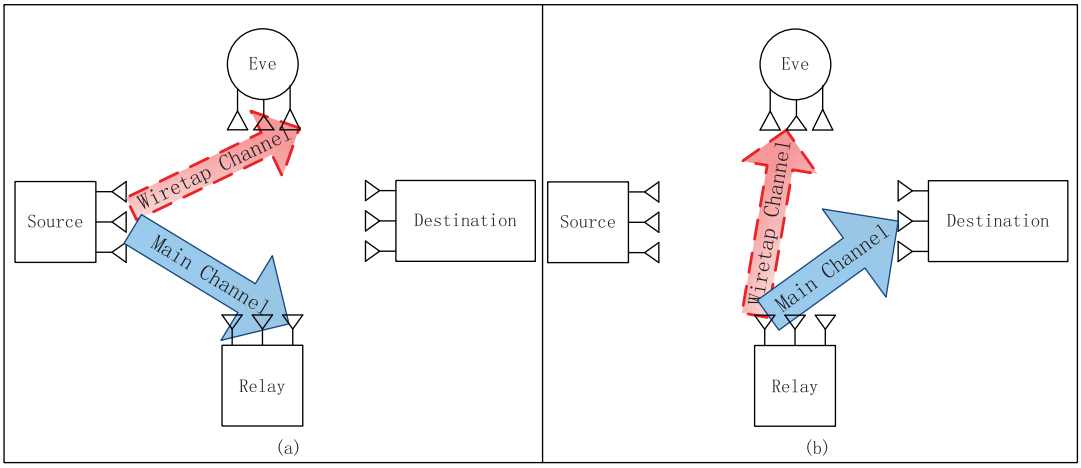


Fig. 4. A one-way relay model. (a) Transmission in the first time slot; (b) Transmission in the second time slot.

forwards the modified message to the destination. If the modification operation at the relay was inherently shared between legitimate users, only the destination can recover the original message and thus an improved secrecy performance is achieved in comparison with the counterparts. However, over the wireless media in practice, the channel dedicated for sharing knowledge between the relay and the destination also suffers from fading and background noise, which may cause a performance degradation of the MF scheme. Traditionally, the relay is utilized to forward the signal from the source. Lai and Gamal [118] proposed a noise-forwarding (NF) relaying protocol, where the relay sends signals independent of the source message. Interestingly, it was proved that NF can enhance the secrecy performance over direct transmission. In fact, the relay based on NF can be regarded as a friendly jammer, which sends artificial noise to confuse the eavesdropper. A comparison of various secure relaying protocols is presented in Table X.

B. Relay Schemes

In general, a multiple-antenna relay is possible to adopt different relay schemes to facilitate secure transmission from the source to the destination by making use of spatial degrees of freedom. For example, by exploiting the spatial degrees of freedom offered by a multiple-antenna relay, AN can be transmitted concurrently with the forwarded signal from a relay to confuse the eavesdropper(s). However, it can also forward multiple sources' signals simultaneously, and thus achieve a higher spectral efficiency. It is clear that the relay scheme plays an important role in secure communications. In this subsection, we give a review on four typical relay schemes, including one-way half-duplex relaying, two-way half-duplex relaying, full-duplex relaying, and cooperative relaying schemes.

1) One-Way Half-Duplex Relaying: One-way half-duplex relay technique is the most popular relay scheme [141]–[143]. In this case, two time slots are required to accomplish a transmission cycle. During the first time slot, a source sends a message to a relay, as shown in Fig 4(a). Then, the relay forwards the post-processed signal to a legitimate destination within the second time slot, as shown in Fig. 4(b). Meanwhile, an eavesdropper (or Eve in Fig. 4) also receives the signals and tries to decode them. With multiple antennas equipped at the relay, various receive detection and transmit precoding schemes can be adopted during the first and second slots, respectively. In [141], multiple data streams transmission was considered in two-hop relaying networks, where an eavesdropper can wiretap the relay channels in both hops. GSVD-based secure relay schemes were proposed to facilitate the transmission of multiple secure data streams, and the optimal power allocation was found for the GSVD relay scheme via geometric programming. In [142], the number of achievable secure degrees of freedom for one-way MIMO relay networks was quantified and had been shown to match to a performance upper bound when the number of antennas at the destination is sufficiently large. A so-called group-sparse penalty was exploited in [143] to design beamformers in AF MIMO one-way relaying networks to maximize the secrecy rate. The main disadvantage of one-way half duplex relaying is a loss

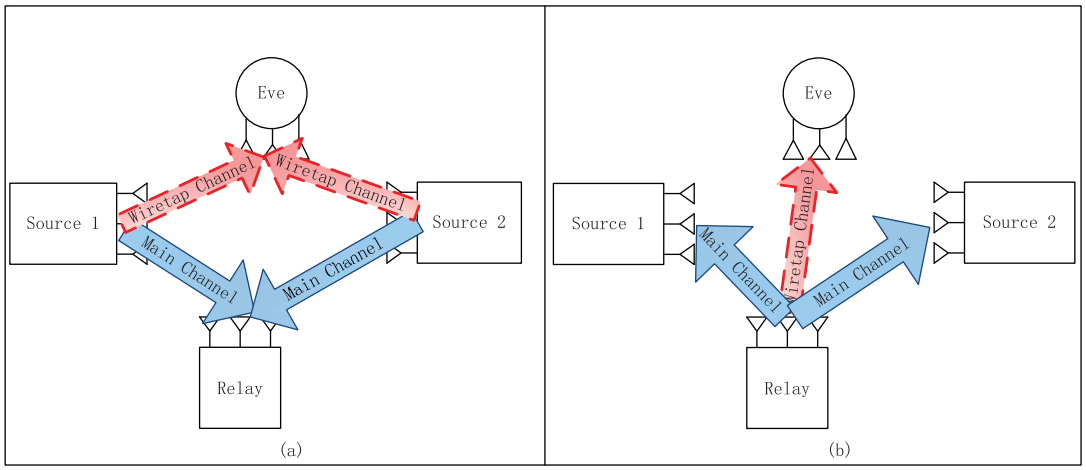


Fig. 5. A two-way relay model. (a) Transmission in the first time slot; (b) Transmission in the second time slot.

in throughput compared to full duplex relaying. Fortunately, this throughput loss can be partially recovered by two-way half-duplex relaying, which will be discussed in the next section.

2) Two-Way Half-Duplex Relaying: In a two-way half-duplex relaying scenario, a source and a destination exchange messages with the aid of a relay in two time slots, as seen in Fig. 5. Specifically, the source and the destination send their signals simultaneously to a relay during the first time slot. Then, the relay broadcasts the post-processed and mixed signals in the second time slot. After that, both the source and the destination subtract their own transmitted signals from the received signal, and then recover the desired information transmitted from the other node. Compared to one-way relay, two-way relay has two advantages from the perspective of wireless security. First, two-way half-duplex relaying has the potential in doubling system spectral efficiency of the legitimate signal transmission. Second, concurrent transmission of two signals may degrade the quality of intercepted signal at the eavesdropper when the eavesdropper cannot perform interference cancelation. Hence, secure transmission based on two-way relay protocol has received considerable interests [144]–[146]. To effectively exploit the benefits of two-way half-duplex relaying, a common method is to adopt network coding [147], [148]. Cai and Yeung [149] first proved the effectiveness of network coding in a wiretap network and presented a method in constructing secure linear network codes. In [150], physical layer network coding (PNC) was applied to enhance wireless security in MIMO two-way half-duplex relaying networks. In particular, the authors proposed a joint beamforming and power allocation scheme to maximize a lower bound on the secrecy sum rate. Considering imperfect eavesdropper CSI at the source and the destination in PNC-based MIMO two-way relaying networks [151], Jayasinghe *et al.* [151] designed a robust beamforming scheme to minimize the MSE at a relay, while guaranteeing communication security. In [152], the secrecy performance of another network coding scheme, namely analog network coding (ANC), was evaluated in MIMO two-way half-duplex relaying channels. The corresponding secure beamforming schemes were presented in the cases with and without eavesdropped CSI, respectively.

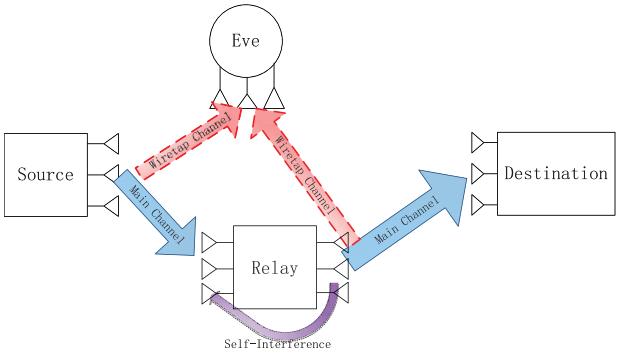


Fig. 6. A full-duplex relay communication model.

3) Full-Duplex Relaying: Both of the aforementioned one-way and two-way relaying protocols adopt a half duplex scheme, which separates the transmitting and receiving processes in orthogonal time slots or frequency bands. However, if a relay can simultaneously transmit and receive signals, namely full-duplex relay [153]–[155], as shown in Fig. 6, the spectral efficiency can be potentially doubled with respect to half-duplex one-way relay. More importantly, a full-duplex scheme can enable secure and effective wireless transmission. Thus, secure communication based on full-duplex relay becomes a research hotspot recently [156]–[158]. In [159], the secure degrees of freedom were analyzed for full-duplex relaying networks over MIMO quasi-static fading channels, and then the achievable diversity versus secure multiplexing gain trade-off was derived. Full-duplex communication technology can also be combined with multiple relays to perform cooperative secure communications [160]. In this cooperative scheme, all the relays decode the message sent by the source and at the same time perform zero-forcing beamforming by transmitting scaled versions of the same signal to the destination. It was shown in [160] that all the relayed signals can be eliminated from the eavesdropper's observation. In addition, full-duplex relaying may be adopted together with other PHY-security techniques, in

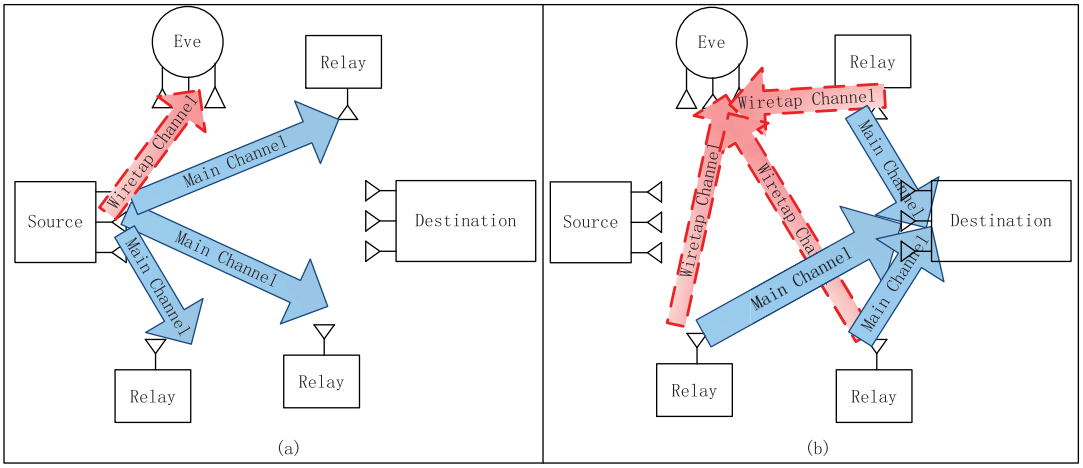


Fig. 7. A cooperative relay model. (a) Transmission in the first time slot; (b) Transmission in the second time slot.

order to enhance wireless security significantly. For example, in [161] a jointly cooperative relay and jamming protocol based on full-duplex capable relay was proposed. This protocol divides the transmission into two time slots. In the first time slot, the full-duplex relay receives data and sends jamming signal to the eavesdropper simultaneously. Then, in the second time slot, the relay forwards the data to the destination, while the source jams the eavesdropper. Note that the proposed full-duplex relaying in [161] is different from traditional ones, since the relay sends the jamming signal while receiving the legitimate signal. Thus, a complete transmission cycle still requires two orthogonal time slots.

4) Cooperative Relay: If there is a strict space limitation at a relay, it may be impossible to deploy multiple antennas. In this case, multiple single-antenna relays can cooperatively assist secure communications [162]–[164], as seen in Fig. 7. The advantages of cooperative relaying for enabling PHY-security are two-fold. First, these relays are geographically distributed, then the communication distance between the source and the destination may be shortened, and thus the secrecy performance is improved. Second, these relays can play different roles according to channel conditions. For example, the relays close to an eavesdropper may act as cooperative jammers to generate strong interference to the eavesdropper. Meanwhile, the remaining relays forward the previously received signal to the legitimate receiver cooperatively. Compared to the jamming schemes with a co-located multiple-antenna relay, the one with cooperative relaying has a lower hardware complexity in each relay. To exploit the benefits of cooperative relaying, the key is to design cooperative beamforming for these distributed relays. In [165], the optimal design of beamforming/precoding at the relays was investigated in detail, and the corresponding explicit expressions of achievable outage probability and diversity-multiplexing tradeoff were developed. It was shown that by introducing cooperative relaying, secrecy outage probability approaching to zero can be achieved. In practice, it is a challenging issue to guarantee wireless security under the condition of no eavesdropper CSI, especially for cooperative relaying. Yet, a corresponding viable solution was proposed in [166]. In particular, joint cooperative beamforming and jamming were adopted to enhance the security, where some of intermediate nodes adopt distributed beamforming, while the remaining nodes jam the eavesdropper simultaneously. The beamforming weights and power allocation were obtained through minimizing the transmit power, while satisfying individual power and minimum received SNR constraints. In addition to wireless security, transmission reliability is also an important performance metric. In [167], the concept of security-reliability trade-off was presented. Furthermore, opportunistic relay selection in cooperative relay networks was proposed to improve the trade-off performance.

C. Relay Roles

Originally, relaying was used to forward the legitimate signal, so as to enhance the received SNR and to reduce the information leakage. However, if a relay is equipped with multiple antennas or multiple relays work cooperatively, the roles of the relay can be extended by making use of spatial degrees of freedom. For example, a relay may also act as a cooperative jammer to confuse the eavesdropper. Note that other than a helper, the relay may be pretended by an eavesdropper. In this case, the information is intercepted with a high probability. In what follows, we give an introduction of the two different roles of the relay.

1) Helper: The relay can play the roles as an information forwarder and a jammer based on multiple-antenna techniques. Intuitively, the information and jamming signals should be separated to avoid the interference to the legitimate receiver. Generally, the interference avoidance is realized through spatial beamforming [168]–[170]. In multiple relays cooperative transmission, there are two operation modes for a relay to perform forwarding and jamming. In the first mode, all relays conduct forwarding and jamming simultaneously. For example, Wang and Wang [171] proposed a low-complexity robust joint beamforming and jamming scheme for an AF relay network in the presence of imperfect eavesdropper CSI. A more general case was considered in [172], where there are several

multiple-antenna relays and multiple-antenna eavesdroppers. In the second mode, information delivering and cooperative jamming are performed by different relays. In [173], an optimal partition for data relays and jamming relays was solved in the case of imperfect CSI. A special case was considered in [174], where the best relay in terms of channel condition was selected among all the relays to forward confidential signal and the remaining relays send jamming signals to cripple the interception capabilities of eavesdropper. Besides, Wang *et al.* [174] studied the optimal power allocation issues for confidential signal and jamming signals to maximize the ergodic secrecy rate. To simplify the system design, the use of two relay nodes to increase security against eavesdroppers was proposed in [163]. The first relay operates in conventional mode, which assists the source to deliver its data to the destination via a DF relaying strategy. The second relay is used as a jammer to create interference intentionally to the eavesdroppers. Different selection schemes were derived based on instantaneous and statistical knowledge of eavesdropper channels, respectively.

2) Eavesdropper: A key feature in relaying systems described above is that they all assumed that the relay can be trusted. In other words, the relays will assist secure transmissions in the best way they can. However, from recent research works, several papers have considered the use of untrusted relays [175]–[178]. In modelling an untrusted relay, although the relay is a cooperative node, information intended for the destination must be kept secret from the relay, since it may be an eavesdropper indeed. Even with an untrusted relay, it is possible to improve the security with respect to the case without a relay as shown in [41]. The untrusted relaying has a great impact on the secrecy performance. The achievable secrecy rate of the DF protocol is zero, while the AF protocol can achieve a nonzero secrecy rate. Thus, it is necessary to enhance wireless security in the presence of an untrusted relay by some means. A promising solution to handle the security problems caused by the untrusted relaying is the use of cooperative jamming by treating a relay as a potential eavesdropper. Wang *et al.* [179] suggested the destination to act as a jammer to confuse the untrusted relay. Specifically, during the first phase, while the source transmits the information signal to the relay, the destination transmits the jamming signal to jam the relay (a potential eavesdropper). During the second phase, the relay forwards the signal to the destination. Furthermore, assuming the total transmit power at the source and the destination is given, Huang and Swindlehurst [180] presented an optimal power allocation scheme for the source and the relay to maximize the ergodic secrecy capacity. This idea was then extended to the case with multiple untrusted relays [181], [182]. In [181], relay selection combining with cooperative jamming at the destination and transmit beamforming at the source was proposed, so as to maximize the achievable secrecy rate. However, cooperative jamming consumes extra power, resulting in a low energy efficiency. In fact, if the destination replaces the jamming signal with useful signal, the effect of jamming still holds true. This is because the relay intercepts one data stream, while being confused by the other data streams. Inspired by this idea, the problem of PHY-security in MIMO two-way untrusted relay networks was studied in [181]. The beamformers at two sources and the relay were optimized to maximize the sum secrecy rate. Furthermore, cooperative jamming was combined with two-way relaying in [182] with a goal of enhancing wireless security in the presence of an untrusted relay. Different from the jamming schemes in [179] and [180], Zhang *et al.* [182] considered the case that jamming signals come from external friendly jammers. In order to optimize the jamming power, the authors formulated a Stackelberg game between the sources and the friendly jammers as a power control scheme to achieve optimized secrecy rate of the sources, in which the sources and the friendly jammers are treated as the sole buyer and the sellers, respectively.

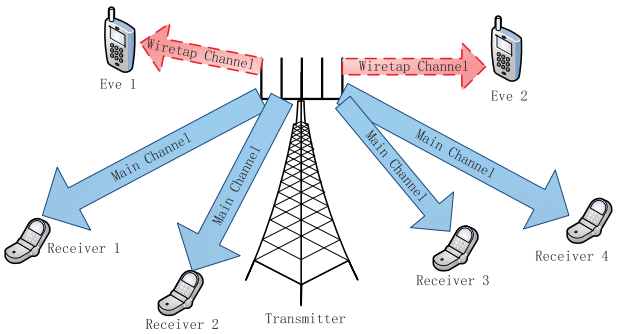


Fig. 8. A secure communication model of a broadcast channel.

Remarks: The secrecy performance of relay networks depends heavily on the coordination between the source, the relay, and the destination. In previous works, multi-antenna techniques for these nodes have been individually designed, which may result in a performance loss. As a simple example, in the two-way relaying schemes, the signals from two transmitters are superimposed. The coordination is helpful for interference mitigation at the receivers. In the following, we consider a more complicated secure communication model, namely multiuser transmission.

IV. Multiuser Transmission Techniques

Multiple-antenna systems can support multiuser transmission concurrently, e.g., multiuser broadcast and multiple access, which improve the spectral efficiency significantly [183]–[185]. Unfortunately, each user may suffer from strong multiple access interference, resulting in a low received signal quality. In this context, multiuser transmission may face severe secrecy problems [186]–[188]. In this section, we focus on the security issues in multiple-antenna multiuser communications over broadcast channel, multiple access channel, and interference channel, respectively.

A. Broadcast Channel

In a broadcast channel, a common transmitter sends confidential messages to multiple receivers concurrently in the presence of one or multiple legitimate eavesdroppers, as illustrated in Fig. 8. A typical scenario for a broadcast channel is cellular systems, where a base station communicates with

multiple mobile users in the downlink. Since each user receives mixed signals for all users, the desired signal is interfered by the other users' signals. Besides, it may also increase the susceptibility to eavesdropping as there are more opportunities for information leakage. In fact, the secrecy capacity is affected not only by the signals of desired user and the eavesdropper, but also by those of the other users. In [189], the characterization of the secrecy capacity region for an MIMO Gaussian broadcast channel with two receivers was analyzed via a channel enhancement argument. Then, the problem of secrecy capacity for a more general case with a group of legitimate users and a group of eavesdroppers was studied in [190]. Several insightful upper and lower bounds on the secrecy capacity were derived. However, the secrecy capacity for a general broadcast channel is still an open issue.

Compared to traditional point-to-point and relaying secure communications, the design and optimization of secure communications over broadcast channels are more sophisticated. This is because both inter-user interference and information leakage to eavesdroppers should be mitigated simultaneously. In [191], the interference alignment with wiretap code constructions was applied to multiple-antenna secure broadcast channels for reducing interference leakage to the legitimate receivers. Besides, secrecy performance was analyzed and new lower and upper bounds on the secure degrees of freedom were derived. In order to solve the challenging issue of no eavesdropper CSI at the transmitter, AN was introduced to secure broadcast communications in [192]. The AN selectively degrades the passive eavesdropper's channel, while remaining to be orthogonal to the desired legitimate receivers. Furthermore, the authors presented power allocation schemes between information signal and AN signal based on zero-forcing and MMSE beamformers, respectively. A more adverse case, in which the transmitter has no eavesdropped CSI and partial legitimate CSI, was studied in [193]. Yet, the AN strategy may not always be an efficient solution since the AN signal also interferes with the information signals received at the legitimate receivers. To this end, opportunistic user scheduling based on partial eavesdropper CSI was adopted to improve the performance of wireless security. In this opportunistic user scheduling scheme, it was shown that the number of accessing users, i.e., their transmission modes, has a great impact on the secrecy performance. Thus, Chen and Zhang [193] further proposed a scheme to select an optimal transmission mode according to channel conditions and system parameters. Recently, massive MIMO technique was applied to guarantee secure communications, by exploiting its large array gain and high spatial resolution. It was proved that if the number of antennas is large enough, the information leakage is negligible even if the CSI of eavesdropper channel is unavailable. Thus, massive MIMO is expected to be an effective way to improve secrecy performance when the transmitter has only imperfect legitimate CSI and no eavesdropper CSI. Interestingly, even with simple regularized channel inversion precoding, massive MIMO may achieve a high secrecy performance [194]. The optimal regularization parameter and the optimal network load were derived by applying deterministic approximation for the secrecy sum-rate. Furthermore, the broadcast channel with spatial correlation and line-of-sight component was considered in [195] and the results provided a reliable performance prediction.

In modern wireless communication systems such as multi-cellular systems, interference is a critical system performance limiting factor [197], [198]. In particular, the users at the cell edge suffer from multiple-cell interferences, and thus face a severe security issue. In [196], the secrecy performance in terms of ergodic secrecy rate, secrecy outage probability, and interception probability were analyzed in an environment of multiple cells. It was found that the secrecy performance will be saturated at a high SNR region for the case of no eavesdropped CSI. To avoid or mitigate inter-cell interferences, multiple-cell cooperation or network MIMO techniques were proposed in [199] and [200], which coordinate the transmit beamformers of multiple base stations. The proposed multiple-cell cooperation requires CSI sharing between multiple cells. However, due to limited backhaul capacity, it is only possible to convey partial CSI between multi-cellular base stations. Moreover, the CSI of eavesdropper is usually unavailable in practice. In such a situation, massive MIMO techniques combined with multiple-cell cooperation were naturally proposed to enhance wireless security. In [201], massive MIMO and AN techniques were applied to address the security issues in multi-cellular downlink communications without eavesdropper CSI. It was shown that even with random AN shaping matrices, it is possible to achieve a favourable performance in an adverse environment of pilot contamination. Furthermore, power allocation between the legitimate signal and the AN signal was studied with different linear precoding schemes for data and AN in [202]. The active attacks from the eavesdroppers were considered in [203]. Specifically, the attack occurs in the uplink pilots estimation for the transmitter to estimate the downlink channel of legitimate receiver. This results in a legitimate CSI uncertainty at the transmitter and thus the eavesdropper can overhear more information. The effect of active attacking was analyzed under the massive MIMO setting and the AN was proposed to degrade the channel quality of eavesdropper. Interestingly, it was found that if the transmitter has statistical CSI of the eavesdropper, the information leakage can be completely avoided by transmitting the information in the null space of correlation matrix of the eavesdropper channel. Thus, the AN generation is not required in massive MIMO systems in this scenario.

B. Multiple Access Channel

In multiple access channels, multiple legitimate transmitters send confidential messages to a common receiver simultaneously, while one or more eavesdroppers may try to decode the information, as shown in Fig. 9. In order to guarantee secure multiple access, the cooperation of transmitters is required. However, due to geographical separation, such cooperation should be carried out distributively. So far, secure multiple access was studied mainly from an information-theoretic viewpoint. In [204], the secrecy capacity region of a special class of multiple access channels was studied, where there is one eavesdropper in a multiple access system and

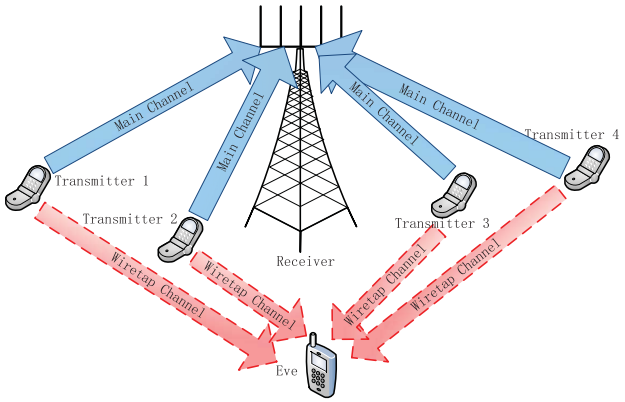


Fig. 9. A secure communication model of a multiple access channel.

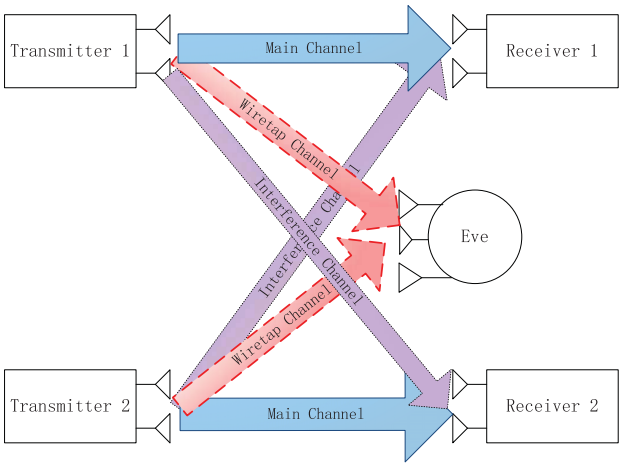


Fig. 10. A secure communication model of an interference channel.

the eavesdropper can only overhear the transmit signal of one of the transmitters. The capacity regions of this special class of multiple access channels with and without secrecy requirements were compared to illustrate the price to be paid for secrecy communications. Furthermore, the performance of secure communications over multiple access wiretap channels with channel uncertainty was evaluated in [205], and a multi-letter description of a strong secrecy capacity region was established. Additionally, from the perspective of secure degrees of freedom, it was proved in [206] that through interference alignment and structured cooperative jamming, the sum secure degrees of freedom of a K-user Gaussian multiple access wiretap channel is $\frac{K(K-1)}{K(K-1)+1}$.

C. Interference Channel

Interference channel is a more general channel model, where multiple transmitter-receiver pairs communicate with each other over the same channel, as shown in Fig. 10. Each receiver not only receives the desired signal from its corresponding transmitter, but also encounters interferences from the other transmitters. Thus, there is a high probability of information leakage since all the receivers are in the range of service coverage. In order to reduce the interferences and to improve the performance, several interference cancellation and mitigation techniques were proposed in the literature, such as interference alignment [207], [208]. Naturally, interference alignment can also be used to enhance wireless PHY-security, and its secrecy performance was extensively evaluated under various conditions. In [209], the secrecy performance in terms of secure degrees of freedom was analyzed for interference alignment over the interference channel with confidential messages and for the case with an external eavesdropper, respectively. It was shown that interference alignment with confidential messages can achieve more secure degrees of freedom than the one with an external eavesdropper, since the latter case is lack of CSI of the eavesdropper. A more general performance evaluation for Gaussian interference channels with interference alignment was carried out in [210], which considered three different secrecy scenarios: (1) K-user interference channel with an external eavesdropper; (2) K-user interference channel with confidential messages; (3) K-user interference channel with confidential message and an external eavesdropper. It was shown that the three proposed interference alignment schemes converge asymptotically to the same sum secure degrees of freedom in all three scenarios. In [211], the integration of interference alignment and AN was studied for two-user MIMO Gaussian interference channels in the presence of an external eavesdropper. The authors considered a practical case, where the eavesdropper channel is completely unknown to the legitimate communication parities, and can be varying in an arbitrary fashion from one channel usage to the others. This interference alignment scheme combined with AN may possess a large secure degrees of freedom, which are connected closely to the rank of the effective channel matrix, over which the eavesdropper experiences the AN. Other than interference alignment, coordinated beamforming is also an effective way to enhance secrecy over interference channels. In [212], imperfect CSI with bounded ellipsoidal uncertainty was assumed at the transmitters, and thus a robust coordinated beamforming scheme was proposed for minimizing the total transmit power subject to the worst-case individual SINR and equivocation rates constraints.

Remarks: The inter-user interference in traditional multiuser networks is an adverse factor limiting the performance, but it also can be exploited as an extra AN in secure communications to confuse the eavesdropper(s). Thus, in multiuser secure communications, it is necessary to strike a balance between reducing the interference to the legitimate users and enhancing the interference to the eavesdroppers. In this case, the design of multiple-antenna techniques requires more accurate CSI and cooperation between the users, which is challenging in practical systems indeed. Therefore, it makes sense to design distributed secure schemes. In fact, these issues not only arise in the case of multiuser transmission, but also appear in the multiple-network cases, namely heterogeneous networks as discussed in the following.

V. Heterogeneous Networks

With the advancement of wireless communications, nowadays there are multiple communication systems operating over the same spectrum band simultaneously due to

spectrum scarcity. The coexistence of multiple heterogeneous networks is prone to information leakage to unintended users or nodes. As a result, the secrecy in heterogeneous networks receives considerable interests in the last decade, and various PHY-security techniques were developed according to the characteristics of these networks. In this section, we discuss the issues on PHY-security in various heterogeneous networks.

A. Cognitive Radio Networks

Cognitive radio (CR) has been proposed to realize spectrum sharing as a means to solve spectrum scarcity problem. Specifically, a CR secondary network is allowed to access the licensed spectrum, if the spectrum is idle or the interference originating from a CR network does not degrade the QoS of primary network [213]–[215]. Security issues in CR networks have been attracting continuously growing attention due to the open and dynamic nature of CR architecture, where various unknown wireless devices are allowed to opportunistically access the licensed spectrum. This specific feature makes CR systems vulnerable to eavesdropping [216]–[218]. Thus, extensive studies have been carried out for protecting CR network against eavesdropping through PHY-security [219]–[221].

For providing secure communications in CR networks, on one hand, CR networks should avoid or decrease the interferences to primary networks, so as to satisfy the precondition for allowing to access the licensed spectrum. On the other hand, CR networks should try to improve the secrecy performance. Therefore, multiple-antenna techniques are naturally applied to secure CR communications to achieve two goals by making use of its spatial degrees of freedom [222]–[225]. A basic four-node secure CR communication model was studied in [226], where a multiple-antenna CR transmitter sends secret information to a legitimate CR receiver in the presence of an eavesdropper and a primary user on the licensed band. The transmit beamformer was designed in order to maximize the secrecy capacity under maximum transmit power and maximum interference power leakage constraints. Due to the non-convexity of the optimization problem, three suboptimal schemes were presented to strike a balance between optimality and computational complexity, namely secret beamforming, projected secret beamforming, and projected cognitive beamforming. Furthermore, Pei *et al.* [227] considered the case of imperfect CSI of the cognitive, primary, and eavesdropper channels. Specifically, robust secure cognitive beamforming was proposed to maximize the secrecy rate in the worst case, and two approaches were provided to solve the problem of beamformer design. In [228], an interesting multiple-objective joint optimization problem for secure communications in multiuser CR networks with wireless information and power transfer was studied. A multiple-antenna cognitive transmitter transfers information and power simultaneously to cognitive receivers, while the energy receivers may intercept the information and should be treated as potential eavesdroppers. Through optimizing transmit beamformers for the signal and AN, a set of Pareto optimal resource allocation policies were designed to provide security communications and achieve three important system design objectives: i.e., total transmit power minimization, energy harvesting efficiency maximization, and interference power leakage-to-transmit power ratio minimization. Different from the above works, a scenario with multiple-antenna cognitive receiver and eavesdropper was considered in [229]. Closed-form expressions for the exact and asymptotic secrecy outage probability were derived. Based on these results, the impacts of maximum transmit power at CR networks and the peak interference power leakage to the primary network on the secrecy performance were revealed. Energy-efficient beamforming for secure communication in cognitive radio networks was studied in [230]. As aforementioned, a Taylor series expansion was applied to transform the secrecy rate to a convex function.

Moreover, cooperative relay is also an effective way to enhance transmission security in CR networks. Similar to traditional secure relay transmission, cooperative beamforming and cooperative jamming are usually optimized jointly. In [231], relays were divided into two portions, one for information relaying, and the other for cooperative jamming. The beamformers were designed for maximizing the secrecy rate, subject to a constraint that the attenuation of SNR at a primary receiver is guaranteed below a threshold. To simplify the cooperative scheme, a pair of cognitive relays are opportunistically selected for security protection against eavesdropping in [232]. The first relay transmits secret information to the destination, and the second relay, acting as a friendly jammer, transmits a jamming signal to confuse the eavesdropper. Four relay selection policies, namely random relay and random jammer, random jammer and best relay, best relay and best jammer, and best relay and no jammer, were analyzed and compared. It was shown that the absence of the jammer gives rise to a phenomenon of secrecy rate outage saturation. To solve this problem in the case without jammer, multiple relays selection was proposed in [233]. Besides, the security-reliability trade-off performance was analyzed for the multiple relays selection scheme. It was found that as the number of relays increases, the trade-off between security and reliability improves significantly via proper relay selection.

B. Wireless Information and Power Transfer Networks

Recently, simultaneous wireless information and power transfer (SWIPT) receives considerable interests from academia and industry [234]–[237]. In fact, wireless power transfer can prolong the lifetime of a wireless network via convenient ways. Besides, both information and power are transferred concurrently over the same carrier, which extends the function of traditional wireless communications. Conceptually, a source transmits information and power signals simultaneously to one or multiple receivers. Generally speaking, a power receiver is usually closer to the source than the information receiver, since the energy harvesting circuitry is less sensitive than the information decoding circuitry [238], [239]. Thus, if a power receiver is malicious, it may successfully decode the information, resulting in information leakage. Moreover, there may be an external eavesdropper, who pretends to be a legitimate information or power receiver. The security issues in wireless information and power transfer have

drawn a great deal of attention, and a lot of works proposed various effective solutions [240]–[242]. Therein, multiple-antenna technique exhibits a strong capability to enhance security, since it can support efficient power transfer and secure information transmission by making use of spatial degrees of freedom [243]–[247]. A basic three-node model of secure wireless information and power transfer was considered in [248], where the messages sent to an information receiver may be eavesdropped by energy receivers, which are presumed to harvest energy only from the received signal. To achieve communication security, the transmit beamformer is optimized to maximize the achievable secrecy rate, subject to a total maximum transmit power constraint and a minimum requirement of harvested energy. Furthermore, a joint beamforming and artificial noise design problem was addressed to improve the secrecy performance. Then, the secrecy problem in a four-node model was analyzed in [249], where an external eavesdropper overhears the information. With the consideration of channel uncertainties, a robust secure transmission scheme was designed, which maximizes the worst-case secrecy rate under transmit power constraint and energy harvesting constraint. The authors further extended the scheme to the case of multiple eavesdroppers, and a robust AN-aided secure transmission scheme was proposed to significantly improve the secrecy performance in [250]. The case with multiple power receivers, also treated as potential eavesdroppers, was studied in [251]. In particular, two typical problems were investigated with different practical objectives: the first problem maximizes the secrecy rate for an information receiver subject to individual harvested energy constraints, while the second problem maximizes the weighted sum-energy transferred to energy receivers subject to a secrecy rate constraint.

Note that it is possible to enhance information security and energy efficiency in wireless information and power transfer by introducing an extra helper. In [252], a cooperative jammer was deployed to introduce jamming interference and assist the source to supply wireless power. Transmit beamforming at the source and cooperative jamming by the jammer were optimized jointly by maximizing the worst-case secrecy rate under transmit power constraint and worst-case energy harvesting constraint. In addition, cooperative relaying is also an effective way to enhance secrecy wireless information and power transfer. In [253], a multiple-antenna relay was used to cooperatively forward information and power, and to decrease information leakage. The problem of secure relay beamforming was studied to maximize the secrecy rate under the constraints of minimum relay transmit power and maximum harvested energy. The benefits of a massive MIMO relay were exploited in [254] for providing communication security in SWIPT networks. It was shown in [254] that the power transfer efficiency is improved significantly by exploiting a large array gain of massive MIMO. Also, the information leakage is decreased sharply due to the use of high-resolution spatial beamformer. Furthermore, an energy-efficient power allocation scheme was proposed for such a wireless powered massive MIMO secure relaying system in [255], which partially solved the problem of energy efficiency for SWIPT.

C. Device-to-Device Communication Networks

An exponentially increasing demand on wireless communications pushes up the density of devices in local areas. Consequently, device-to-device (D2D) communications, which enable direct communications between user equipments (UEs) in proximity, have been proposed as a competitive technology for next generation cellular networks [256], [257]. Thus, both spectrum efficiency and energy efficiency can be improved significantly with so-called proximity gain and hop gain. Due to spectrum sharing within the cellular networks, the D2D communications could generate a large interference to cellular users, resulting in performance degradation. Extensive research has been undertaken on the management of interferences, in order to guarantee reliable communications in D2D-enabled cellular networks [258], [259]. In fact, the originally harmful interferences from D2D communications can be exploited to enhance transmission security of cellular networks [260]–[262]. Specifically, a D2D user, which plays a role as a cooperative jammer, can be exploited to confuse the eavesdropper, and thus it also gets more chances to transmit its own message. In [263], transmit power and access control of the D2D link were optimized jointly to maximize the achievable data rate of D2D communications, subject to a secrecy outage probability constraint for cellular users. Then, the authors extended their study to the case of a large-scale D2D-enabled cellular network in [264]. A similar D2D link scheduling strategy was proposed to enhance PHY-security of cellular communications, and at the same time to create extra transmission opportunities for D2D users. A case with multiple eavesdroppers and multiple D2D links in a MISO downlink was considered in [265]. The robust beamforming at a multiple-antenna legitimate transmitter was designed to minimize transmit power and to maximize secrecy rate, respectively, subject to a D2D transmission rate constraint. It was shown that D2D communications can potentially improve the secrecy performance.

Remarks: The key for security enhancement in heterogeneous networks is inter-network cooperation. However, due to relative independence of different networks, it is difficult to exchange all necessary information. Thus, it is imperative to design some low-complexity secure schemes by exploiting the characteristics of these networks. For instance, it is possible to extend the sensing capability of cognitive radio networks for obtaining the knowledge of eavesdropper(s) [220]. In SWIPT networks, the energy signal can be reused as the AN signal.

VI. Future Research Directions and Challenges

Despite many fruitful research efforts in studying PHY-security with multiple-antenna techniques, there are many challenging issues remained to be tackled. In the following, we list some initial ideas and research directions.

A. CSI Acquisition

CSI has a great impact on the secrecy performance, especially in multiple-antenna secure communications. However, the acquisition of CSI at a transmitter is a nontrivial task.

On one hand, eavesdropper CSI is difficult to obtain due to the hidden nature of eavesdroppers. On the other hand, legitimate CSI may be imperfect and even unavailable. For instance, the legitimate CSI is usually obtained through limited feedback in FDD systems. If channel varies too fast, the amount of feedbacks required to keep tracking the channel will be increased sharply. More importantly, the obtained CSI may be outdated, leading to resource allocation mismatch. Moreover, in the process of CSI feedbacks, an eavesdropper may also get the same CSI. Based on this information, the eavesdropper can design and adopt the corresponding interception strategy, so as to eavesdrop more legitimate information data. Hence, it is necessary to design a secure and reliable CSI feedback mechanism.

B. Active Eavesdropping

In some cases, the eavesdropper may actively interfere with secure transmission for obtaining more information [266]. For example, in the stage of channel estimation of legitimate receivers, an eavesdropper may send the same pilots as the legitimate receivers, which is known as a type of active eavesdropping. Then, the accuracy of CSI of the legitimate receivers is compromised and more information may potentially be leaked. Also, in the stage of information transmission, the eavesdropper may transmit a jamming signal to the legitimate receiver, and thus to decrease the quality of the signal received at the legitimate receiver. To guarantee secure communications, not only it is imperative to overcome the impact of active attacking, but also it is necessary to track the behaviour of an eavesdropper using the received attacking signal.

C. Green and Secure Communications

In secure communications, energy consumption is becoming a major concern due to the requirement of green communications. In general, energy saving and wireless security are not aligned with each other. Thus, secrecy energy efficiency, defined as the ratio of secrecy rate and energy consumption, is regarded as a proper quantity to leverage a tradeoff between energy saving and security guarantee. However, achieving green and secure communications by maximizing the secrecy energy efficiency is not a trivial task. First, the objective, namely secrecy energy efficiency, is usually nonconvex. Fractional programming that has been successful applied to conventional communications without secrecy requirement cannot directly solve this problem, since secrecy rate in terms of the difference of two logarithmic functions is not convex or quasi-convex. Second, eavesdropper CSI may be unavailable and legitimate CSI is usually imperfect at a transmitter, which makes the optimization problem for maximizing the secrecy energy efficiency more complicated and unsolvable.

D. Mobile Relay

The positions of relays significantly affect the secrecy performance. Previous works usually used the position information of relays to perform relay selection and role arrangement. For example, some relays close to an eavesdropper can be adopted for cooperative jamming, and the others are used to deliver information. In practice, both legitimate users and eavesdroppers are not static. Thus, a fixed relay assignment is expected not to work well in providing secure communications. One possible solution to this problem is to deploy vehicular relays [267]. In particular, the mobile relays can flexibly move their positions and select different secrecy schemes. However, it is still an open issue to design mobile relays to facilitate secure communications. The research challenges are two-folds. First, the mobile relays require the knowledge of the eavesdropper(s) to adjust their positions. Second, more signalling overheads are required for multiple relays cooperation.

E. Combination of Encryption and PHY-Security

Physical layer security focuses mainly on pure signal processing techniques and its performance is subject to channel conditions; whereas high-layer cryptographic techniques work well independently of channel conditions. In secure communications, the CSI required for enabling PHY-security may be imperfect or even unavailable. Thus, we can integrate cryptographic techniques in transceiver designs. Combining cryptographic techniques with PHY-security offers another way to improve the secrecy performance significantly. For example, PHY-security can provide a secure channel for the exchange of private keys, while cryptographic techniques provide reliable CSI feedbacks for PHY-security. As pointed out in [268], the design of security mechanisms in future wireless networks must consider encryption and PHY-security techniques jointly according to security requirements of wireless networks, security attacks encountered in wireless networks, and the characteristics of wireless networks, such as Bluetooth, Wi-Fi, WiMAX, and the long-term evolution (LTE) systems. So far, such a joint framework design for secure communications has not been studied extensively.

VII. Conclusion

This article has provided a review on multiple-antenna techniques in physical layer secure communications from both theoretical and technical perspectives. First, we presented an investigation on point-to-point multiple-antenna secure systems, focusing on beamforming designs with various types of CSI. Then, we surveyed the issues on multiple-antenna relay techniques for secrecy enhancement from the perspectives of relaying protocols, schemes, and roles, respectively. Afterwards, we presented an overview on secure transmission in multiuser scenarios, and introduced the state-of-the-art interference mitigation techniques for enabling PHY-security. Then, we went ahead to provide a survey identifying the secrecy issues in various heterogeneous networks. Finally, we discussed the potential challenges for PHY-security based on multiple-antenna techniques and pointed out some possible future research directions.

References

[1] W. Stallings, *Cryptography and Network Security Principles and Practices*. Upper Saddle River, NJ, USA: Prentice-Hall PTR, 2006.
[2] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[7] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[8] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[9] Y. O. Basciftci, O. Gungor, C. E. Koksal, and F. Ozguner, "On the secrecy capacity of block fading channels with a hybrid adversary," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1325–1343, Mar. 2015.

[10] 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, no. 6, pp. 3442–3451, Jun. 2014.

[11] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[12] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

[13] S. Bashar and Z. Ding, "Optimum power allocation against information leakage in wireless network," in *Proc. IEEE GLOBECOM*, Honolulu, HI, USA, Dec. 2009, pp. 1–6.

[14] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, Sep. 2011.

[15] X. Chen, L. Lei, H. Zhang, and C. Yuen, "On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI," in *Proc. IEEE ICC*, Sydney, NSW, Australia, Jun. 2014, pp. 2052–2057.

[16] X. Zhou, M. Tao, and R. A. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *Proc. IEEE ICC*, Ottawa, ON, Canada, Jun. 2012, pp. 2339–2344.

[17] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative jamming using compromised secrecy region minimization," in *Proc. CWIT*, Toronto, ON, Canada, Jun. 2013, pp. 214–218.

[18] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[19] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[20] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[21] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[22] C.-H. Lin, S.-H. Tsai, and Y.-P. Lin, "Secure transmission using MIMO precoding," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 801–813, May 2014.

[23] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[24] J. Huang and A. L. Swindlehurst, "Cooperation strategies for secrecy in MIMO relay networks with unknown eavesdropper CSI," in *Proc. IEEE ICASSP*, Prague, Czech Republic, May 2011, pp. 3424–3427.

[25] J. Chen, X. Chen, T. Liu, and L. Lei, "Energy-efficient power allocation for secure communications in large-scale MIMO relaying systems," in *Proc. IEEE ICCC*, Shanghai, China, Oct. 2014, pp. 385–390.

[26] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE SSP*, Aug./Sep. 2009, pp. 417–420.

[27] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Jun. 2013.

[28] X. Chen and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 503–506, Oct. 2013.

[29] P. Xu, Z. Ding, and X. Dai, "Rate regions for multiple access channel with conference and secrecy constraints," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1961–1974, Dec. 2013.

[30] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015

[31] 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. Forensics Security*, vol. 11, no. 8, pp. 1700–1711, Aug. 2016.

[32] N. Valliappan, A. Lozano, and R. W. Heath, Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[33] T. Hong, M.-Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 1417–1420, 2011.

[34] M. Hafez and H. Arslan, "On directional modulation: An analysis of transmission scheme with multiple direction," in *Proc. IEEE ICCW*, London, U.K., Jun. 2015, pp. 459–463.

[35] M. Yusuf and H. Arslan, "Secure multi-user transmission using CoMP directional modulation," in *Proc. IEEE VTC Fall*, Boston, MA, USA, Sep. 2015, pp. 1–2.

[36] Z. Rezki and M.-S. Alouini, "On the finite-SNR diversity-multiplexing tradeoff of zero-forcing transmit scheme under secrecy constraint," in *Proc. IEEE ICC*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[37] M. Pei, L. Wang, and D. Ma, "Linear MMSE transceiver optimization for general MIMO wiretap channels with QoS constraints," in *Proc. IEEE/CIC ICCC*, Xi'an, China, Aug. 2013, pp. 259–263.

[38] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007, pp. 2471–2475.

[39] L. Zhang, Y. Cai, B. Champagne, and M. Zhao, "Tomlinson–Harashima precoding design in MIMO wiretap channels based on the MMSE criterion," in *Proc. IEEE ICCW*, London U.K., Jun. 2015, pp. 470–474.

[40] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *Proc. IEEE ISIT*, Austin, TX, USA, Jun. 2010, pp. 2578–2582.

[41] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[42] S.-H. Lai, P.-H. Lin, S.-C. Lin, and H.-J. Su, "On optimal artificial-noise assisted secure beamforming for the multiple-input multiple-output fading eavesdropper channel," in *Proc. IEEE WCNC*, Paris, France, Apr. 2012, pp. 513–517.

[43] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, "Secure beamforming for MIMO two-way transmission with an untrusted relay," in *Proc. IEEE WCNC*, Shanghai, China, Apr. 2013, pp. 4180–4185.

[44] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[45] J. Huang and A. L. Swindlehurst, "Secure communications via cooperative jamming in two-hop relay systems," in *Proc. IEEE GLOBECOM*, Miami, FL, USA, Dec. 2010, pp. 1–5.

[46] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 506–522, Feb. 2005.

[47] X. Chen, Z. Zhang, and H.-H. Chen, "On distributed antenna systems with limited feedback precoding: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 17, no. 2, pp. 80–88, Apr. 2010.

[48] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, Sep. 2013.

[49] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[50] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.

[51] Z. Li, P. Mu, B. Wang, and X. Hu, "Practical transmission scheme with fixed communication rate under constraints of transmit power and secrecy outage probability," *IEEE Commun. Lett.*, vol. 19, no. 6, pp. 1057–1060, Jun. 2015.

[52] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

[53] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *Proc. IEEE ICC*, Budapest, Hungary, Jun. 2013, pp. 2183–2187.

[54] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan./Feb. 2015.

[55] T. V. Nguyen, T. Q. S. Quek, Y. H. Kim, and H. Shin, "Secrecy diversity in MISOME wiretap channel," in *Proc. IEEE GLOBECOM*, Anaheim, CA, USA, Dec. 2012, pp. 4840–4845.

[56] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[57] X. He, A. Khisti, and A. Yener, "MIMO multiple access channel with an arbitrarily varying eavesdropper: Secrecy degrees of freedom," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 4733–4745, Aug. 2013.

[58] M. Kobayashi, P. Piantanida, S. Yang, and S. Shamai, "On the secrecy degrees of freedom of the multiantenna block fading wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 703–711, Sep. 2011.

[59] J. Chen, X. Chen, X. Wang, and L. Lei, "Optimal power allocation for secure communications in large-scale MIMO relaying systems," in *Proc. IEEE ICC*, London U.K., Jun. 2015, pp. 1801–1806.

[60] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[61] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[62] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[63] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[64] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[65] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[66] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[67] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May 2013.

[68] Q. Li *et al.*, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[69] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[70] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.

[71] H. Reboredo, J. Xavier, and M. R. D. Rodrigues, "Filter design with secrecy constraints: The MIMO Gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[72] H. Zhang, Y. Huang, S. Li, and L. Yang, "Energy-efficient precoder design for MIMO wiretap channels," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1559–1562, Sep. 2014.

[73] Z. Rezki and M.-S. Alouini, "Secure diversity-multiplexing tradeoff of zero-forcing transmit scheme at finite-SNR," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 1138–1147, Apr. 2012.

[74] D. J. Love *et al.*, "An overview of limited feedback in wireless communication systems," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 8, pp. 1341–1365, Oct. 2008.

[75] X. Chen, Z. Zhang, and S. Chen, "Finite-signal-to-noise ratio diversity-multiplexing-rate trade-off in limited feedback beamforming systems with imperfect channel state information," *IET Commun.*, vol. 6, no. 7, pp. 751–758, May 2012.

[76] P. Xia and G. B. Giannakis, "Design and analysis of transmit-beamforming based on limited-rate feedback," *IEEE Trans. Signal Process.*, vol. 54, no. 5, pp. 1853–1863, May 2006.

[77] T. L. Marzetta and B. M. Hochwald, "Fast transfer of channel state information in wireless systems," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1268–1278, Apr. 2006.

[78] M. Kobayashi, N. Jindal, and G. Caire, "Training and feedback optimization for multiuser MIMO downlink," *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2228–2240, Aug. 2011.

[79] U. Salim and D. Slock, "How much feedback is required for TDD multi-antenna broadcast channels with user selection?" *EURASIP J. Adv. Signal Process.*, vol. 2010, pp. 1–14, 2010.

[80] T. T. Kim and H. V. Poor, "Secure communications with insecure feedback: Breaking the high-SNR ceiling," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3700–3711, Aug. 2010.

[81] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, "Robust outage secrecy rate optimizations for a MIMO secrecy channel," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, Feb. 2015.

[82] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[83] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[84] N. S. Ferdinand, D. B. Da Costa, and M. Latva-Aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, May 2013.

[85] S.-C. Lin and C.-L. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3293–3306, Jun. 2014.

[86] T.-Y. Liu, P. Mukherjee, S. Ulukus, S.-C. Lin, and Y.-W. P. Hong, "Secure degrees of freedom of MIMO Rayleigh block fading wiretap channels with no CSI anywhere," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2655–2669, May 2015.

[87] T. V. Nguyen and H. Shin, "Power allocation and achievable secrecy rates in MISOME wiretap channels," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1196–1198, Nov. 2011.

[88] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[89] X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Commun. Lett.*, vol. 17, no. 4, pp. 637–640, Apr. 2013.

[90] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Secrecy and energy efficiency in MIMO-ME systems," in *Proc. IEEE SPAWC*, Stockholm, Sweden, Jun./Jul. 2015, pp. 380–384.

[91] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.

[92] X. Chen, C. Yuen, and Z. Zhang, "Exploiting large-scale MIMO techniques for physical layer security with imperfect channel state information," in *Proc. IEEE GLOBECOM*, Austin, TX, USA, Dec. 2014, pp. 1648–1653.

[93] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[94] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.

[95] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[96] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.

[97] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[98] N. Yang *et al.*, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[99] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2096–2099, Nov. 2013.

[100] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with artificial-noise-aided beamforming for MISO wiretap channels under secrecy outage constraint," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 18–21, Jan. 2015.

[101] S.-H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.

[102] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[103] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[104] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[105] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, Jr., "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May 2015.

[106] Y. Yang, W. Wang, H. Zhao, and L. Zhao, "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation," *J. Commun. Netw.*, vol. 14, no. 4, pp. 374–384, Aug. 2012.

[107] 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, no. 10, pp. 1628–1631, Oct. 2012.

[108] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.

[109] 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, no. 6, pp. 1075–1078, Jun. 2014.

[110] 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, no. 10, pp. 5013–5022, Oct. 2011.

[111] P. Xu, Z. Ding, X. Dai, and K. K. Leung, "A general framework of wiretap channel with helping interference and state information," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 182–195, Feb. 2014.

[112] S. Luo, J. Li, and A. P. Petropulu, "Uncoordinated cooperative jamming for secret communications," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1081–1090, Jul. 2013.

[113] X. Chen, J. Chen, H. Zhang, Y. Zhang, and C. Yuen, "On secrecy performance of multiantenna-jammer-aided secure communications with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8014–8024, Oct. 2016.

[114] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007, pp. 1301–1305.

[115] T. V. Nguyen, Y. Jeong, J. S. Kwak, and H. Shin, "Secure multiple-input single-output communication—Part II: δ-secrecy symbol error probability and secrecy diversity," *IET Commun.*, vol. 8, no. 8, pp. 1227–1238, May 2014.

[116] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[117] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[118] L. Lai and H. E. Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[119] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[120] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[121] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40–46, Dec. 2015.

[122] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[123] C. Zhong, M. Matthaiou, G. Karagiannidis, A. Huang, and Z. Zhang, "Capacity bounds for AF dual-hop relaying in G fading channel," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1730–1740, May 2012.

[124] S. Yang and J.-C. Belfiore, "Towards the optimal amplify-and-forward cooperative diversity scheme," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3114–3126, Sep. 2007.

[125] S. Berger, M. Kuhn, A. Wittneben, T. Unger, and A. Klein, "Recent advances in amplify-and-forward two-hop relaying," *IEEE Commun. Mag.*, vol. 47, no. 7, pp. 50–56, Jul. 2009.

[126] T. Wang, A. Cano, G. B. Giannakis, and J. N. Laneman, "High-performance cooperative demodulation with decode-and-forward relays," *IEEE Trans. Commun.*, vol. 55, no. 7, pp. 1427–1438, Jul. 2007.

[127] C. S. Patel and G. L. Stuber, "Channel estimation for amplify and forward relay based cooperation diversity systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2348–2356, Jun. 2007.

[128] Z. Yi and I.-M. Kim, "Diversity order analysis of the decode-and-forward cooperative networks with relay selection," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1792–1799, May 2008.

[129] S. Jin, M. R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop system," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

[130] G. Zhu *et al.*, "Ergodic capacity comparison of different relay precoding schemes in dual-hop AF systems with co-channel interference," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2314–2328, Jul. 2014.

[131] H.-M. Wang, F. Liu, and X.-G. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1240–1250, Aug. 2014.

[132] M. Mirzaee and S. Akhlaghi, "The achievable secrecy rate of multi-antenna AF relaying using joint transmit and receive beamforming," in *Proc. IST*, Sep. 2014, pp. 1122–1127.

[133] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[134] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdropper," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[135] M. Jilani and T. Ohtsuki, "Joint SVD-GSVD precoding technique and secrecy capacity lower bound for the MIMO relay wire-tap channel," in *Proc. IEEE VTC Spring*, Yokohama, Japan, May 2012, pp. 1–5.

[136] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[137] 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, no. 9, pp. 5135–5146, Sep. 2015.

[138] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[139] S. Vatedka, N. Kashyap, and A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2531–2556, May 2015.

[140] S. W. Kim, "Modify-and-forward for securing cooperative relay communications," in *Proc. Int. Zurich Seminar Commun.*, Zürich, Switzerland, Feb. 2014, pp. 136–139.

[141] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[142] T. T. Kim and H. V. Poor, "On the secure degrees of freedom of relaying with half-duplex feedback," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 291–302, Jan. 2011.

[143] M. Zhao, S. Feng, Y. Liu, and X. Wang, "Secure beamforming based on sparsity in multiple amplify-and-forward MIMO relay networks," in *Proc. IEEE WCSP*, Hefei, China, Oct. 2014, pp. 1–6.

[144] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[145] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[146] J. Zhao, W. Zheng, X. Wen, and L. Zhang, "Joint resource allocation in secure two-way relay networks with QoS guarantee and fairness," in *Proc. IEEE WCNC*, Istanbul, Turkey, Apr. 2014, pp. 1985–1989.

[147] R. Zhang, Y.-C. Liang, C. C. Chai, and S. Cui, "Optimal beamforming for two-way multi-antenna relay channel with analogue network coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 699–712, Jun. 2009.

[148] Y. Zhang, Z. Zhang, R. Yin, G. Yu, and W. Wang, "Joint network-channel coding with rateless code in two-way relay systems," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3158–3169, Jul. 2013.

[149] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

[150] C. Zhang, H. Gao, T. Lv, Y. Lu, and X. Su, "Beamforming for secure two-way relay networks with physical layer network coding," in *Proc. IEEE GLOBECOM*, Austin, TX, USA, Dec. 2014, pp. 1734–1739.

[151] K. Jayasinghe, P. Jayasinghe, N. Rajatheva, and M. Latva-Aho, "Secure beamforming design for physical layer network coding based MIMO two-way relaying," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1270–1273, Jul. 2014.

[152] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. IEEE SPAWC*, Marrakesh, Morocco, Jun. 2010, pp. 1–5.

[153] I. Krikidis, H. A. Suraweera, P. J. Smith, and C. Yuen, "Full-duplex relay selection for amplify-and-forward cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4381–4393, Dec. 2012.

[154] D. W. K. Ng, E. S. Lo, and R. Schober, "Dynamic resource allocation in MIMO-OFDMA systems with full-duplex and hybrid relaying," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1291–1304, May 2012.

[155] R. H. Gohary and H. Yanikomeroglu, "Grassmannian signalling achieves tight bounds on the ergodic high-SNR capacity of the non-coherent MIMO full-duplex relay channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2480–2494, May 2014.

[156] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[157] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[158] H. Alves, G. Brante, R. D. Souza, D. B. da Costa, and M. Latva-Aho, "On the performance of secure full-duplex relaying under composite fading channels," *IEEE Signal Process. Lett.*, vol. 22, no. 7, pp. 867–870, Jul. 2015.

[159] K. T. Gowda, T. Q. S. Quek, and H. Shin, "Secure diversity-multiplexing tradeoffs in MIMO relay channels," in *Proc. IEEE ISIT*, Seoul, South Korea, Jul. 2009, pp. 1433–1437.

[160] R. Bassily and S. Ulukus, "Secure communication in multiple relay networks through decode-and-forward strategies," *J. Commun. Netw.*, vol. 14, no. 4, pp. 352–363, Aug. 2012.

[161] S. Parsaeefard and T. Le-Ngoc, "Full-duplex relay with jamming protocol for improving physical-layer security," in *Proc. IEEE PIMRC*, Washington, DC, USA, Sep. 2014, pp. 129–133.

[162] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[163] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[164] M. Lin, J. Ge, and Y. Yang, "An effective secure transmission scheme for AF relay networks with two-hop information leakage," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1676–1679, Aug. 2013.

[165] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[166] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[167] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[168] G. Zheng, L.-C. Choo, and K.-K. Wang, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[169] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[170] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.

[171] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: Low-complexity design," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 2192–2198, May 2015.

[172] Q. Li *et al.*, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[173] S. Vishwakarma and A. Chockalingam, "Amplify-and-forward relay beamforming for secrecy with cooperative jamming and imperfect CSI," in *Proc. IEEE ICC*, Budapest, Hungary, Jun. 2013, pp. 3047–3052.

[174] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[175] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[176] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Başar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *Proc. MILCOM*, Baltimore, MD, USA, Nov. 2011, pp. 119–124.

[177] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 463–466, Mar. 2015.

[178] W. Wang, K. C. Teh, and K. H. Li, "Relay selection for secure successive AF relaying networks with untrusted nodes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2466–2476, Nov. 2016.

[179] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.

[180] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Proc. Asilomar SSC*, Pacific Grove, CA, USA, Nov. 2013, pp. 1555–1559.

[181] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.

[182] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[183] D. Gesbert, M. Kountouris, R. W. Heath, Jr., C. B. Chae, and T. Salzer, "From single user to multiuser communications: Shifting the MIMO paradigm," *IEEE Signal Process. Mag.*, vol. 24, no. 5, pp. 36–46, Oct. 2007.

[184] K. Kurve, "Multi-user MIMO systems: The future in the making," *IEEE Potentials*, vol. 28, no. 6, pp. 37–42, Nov./Dec. 2009.

[185] X. Chen, Z. Zhang, S. Chen, and C. Wang, "Adaptive mode selection for multiuser MIMO downlink employing rateless codes with QoS provisioning," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 790–799, Feb. 2012.

[186] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[187] H. Jeon, D. Hwang, J. Choi, H. Lee, and J. Ha, "Secure type-based multiple access," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 763–774, Sep. 2011.

[188] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sep. 2014.

[189] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[190] E. Ekrem and S. Ulukus, "Secure broadcasting using multiple antennas," *J. Commun. Netw.*, vol. 12, no. 5, pp. 411–432, Oct. 2010.

[191] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[192] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. Allerton CCC*, Monticello, IL, USA, Sep./Oct. 2009, pp. 1134–1141.

[193] X. Chen and Y. Zhang, "Mode selection in MU-MIMO downlink networks: A physical-layer security perspective," *IEEE Syst. J.*, to be published, doi: 10.1109/JSYST.2015.2413843.

[194] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[195] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, and X. Gao, "Ergodic secrecy sum-rate for multiuser downlink transmission via regularized channel inversion: Large system analysis," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1627–1630, Sep. 2014.

[196] X. Chen and H.-H. Chen, "Physical layer security in multi-cell MISO downlinks with incomplete CSI—A unified secrecy performance analysis," *IEEE Trans. Signal Process.*, vol. 62, no. 23, pp. 6286–6297, Dec. 2014.

[197] X. Ge, K. Huang, C.-X. Wang, X. Hong, and X. Yang, "Capacity analysis of a multi-cell multi-antenna cooperative cellular network with co-channel interference," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3298–3309, Oct. 2011.

[198] T. Ren and R. J. La, "Downlink beamforming algorithms with inter-cell interference in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 10, pp. 2814–2823, Oct. 2006.

[199] D. Gesbert *et al.*, "Multi-cell MIMO cooperative networks: A new look at interference," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 9, pp. 1380–1408, Dec. 2010.

[200] J. Zhang, R. Chen, J. G. Andrews, A. Ghosh, and R. W. Heath, "Networked MIMO with clustered linear precoding," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1910–1921, Apr. 2009.

[201] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[202] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[203] 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, no. 7, pp. 3880–3900, Jul. 2016.

[204] N. Liu and W. Kang, "The secrecy capacity region of a special class of multiple access channels," in *Proc. IEEE ISIT*, St. Petersburg, Russia, Jul./Aug. 2011, pp. 623–627.

[205] R. F. Schaefer and H. V. Poor, "On secure communication over multiple access wiretap channels under channel uncertainty," in *Proc. IEEE CNS*, San Francisco, CA, USA, Oct. 2014, pp. 109–114.

[206] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," in *Proc. IEEE ISIT*, Istanbul, Turkey, Jul. 2013, pp. 1337–1341.

[207] X. Chen and C. Yuen, "Performance analysis and optimization for interference alignment over MIMO interference channels with limited feedback," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1785–1795, Apr. 2014.

[208] H. Ning, C. Ling, and K. K. Leung, "Feasibility condition for interference alignment with diversity," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2902–2912, May 2011.

[209] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[210] J. Xie and S. Ulukus, "Secure degrees of freedom of K-user Gaussian interference channels: A unified view," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2647–2661, May 2015.

[211] X. He and A. Yener, "The interference wiretap channel with an arbitrarily varying eavesdropper: Aligning interference with artificial noise," in *Proc. Allerton Conf.*, Monticello, IL, USA, Oct. 2012, pp. 204–211.

[212] J. Ni *et al.*, "Robust coordinated beamforming for secure MISO interference channels with bounded ellipsoidal uncertainties," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 407–410, Aug. 2013.

[213] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[214] Q. Zhao and B. M. Sadler, "A Survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, May 2007.

[215] X. Chen, H.-H. Chen, and W. Meng, "Cooperative communications for cognitive radio networks—From theory to application," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1180–1193, 3rd Quart., 2014.

[216] T. Jiang, T. Li, and J. Ren, "Toward secure cognitive communications in wireless networks," *IEEE Wireless Commun.*, vol. 19, no. 4, pp. 82–88, Aug. 2012.

[217] Y. Wu and X. Chen, "Robust beamforming and power splitting for secrecy wireless information and power transfer in cognitive relay networks," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1152–1155, Jun. 2016.

[218] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[219] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Commun.*, vol. 12, no. 3, pp. 132–150, Mar. 2015.

[220] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart., 2013.

[221] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

[222] H. Mu and J. K. Tugnait, "Secure degrees of freedom in MIMO cognitive radio systems," in *Proc. IEEE GLOBECOM*, Austin, TX, USA, Dec. 2014, pp. 1011–1016.

[223] O. Cepheli and G. K. Kurt, "Physical layer security in cognitive radio networks: A beamforming approach," in *Proc. BlackSeaCom*, Batumi, Georgia, Jul. 2013, pp. 233–237.

[224] T. Kwon, V. W. S. Wong, and R. Schober, "Secure MISO cognitive radio system with perfect and imperfect CSI," in *Proc. IEEE GLOBECOM*, Anaheim, CA, USA, Dec. 2012, pp. 1236–1241.

[225] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Achieving cognitive and secure transmissions using multiple antennas," in *Proc. IEEE PIMRC*, Tokyo, Japan, Sep. 2009, pp. 1–5.

[226] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[227] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[228] D. W. K. Ng, E. S. Lo, and R. Schober, "Multiobjective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3166–3184, May 2016.

[229] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[230] J. Ouyang, M. Lin, W.-P. Zhu, D. Massicotte, and A. L. Swindlehurst, "Energy efficient beamforming for secure communication in cognitive radio networks," in *Proc. IEEE ICASSP*, Shanghai, China, Mar. 2016, pp. 3496–3500.

[231] W. Li, M. Xin, M. Yue, T. Yinglei, and Z. Yong, "Security-oriented transmission based on cooperative relays in cognitive radio," *China Commun.*, vol. 10, no. 8, pp. 27–35, Aug. 2013.

[232] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[233] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.

[234] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[235] K. Huang and E. Larsson, "Simultaneous information and power transfer for broadband wireless systems," *IEEE Trans. Signal Process.*, vol. 61, no. 23, pp. 5972–5986, Dec. 2013.

[236] X. Chen, C. Yuen, and Z. Zhang, "Wireless energy and information transfer tradeoff for limited-feedback multiantenna systems with energy beamforming," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 407–412, Jan. 2014.

[237] D. W. K. Ng, E. S. Lo, and R. Schober, "Wireless information and power transfer: Energy efficiency optimization in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6352–6370, Dec. 2013.

[238] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

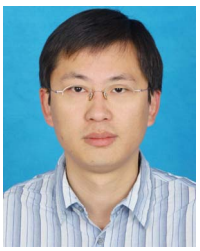
[239] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 117–125, Apr. 2015.

[240] X. Chen, D. W. K. Ng, and H.-H. Chen, "Secrecy wireless information and power transfer: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 54–61, Apr. 2016.

[241] Y. Wu, X. Chen, C. Yuen, and C. Zhong, "Robust resource allocation for secrecy wireless powered communication networks," *IEEE Commun. Lett.*, to be published, doi: 10.1109/LCOMM.2016.2598327.

[242] X. Jiang *et al.*, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3858–3871, Sep. 2016.

[243] X. Chen, Z. Zhang, H.-H. Chen, and H. Zhang, "Enhancing wireless information and power transfer by exploiting multi-antenna techniques," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 133–141, Apr. 2015.
[244] Z. Ding *et al.*, "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 86–93, Apr. 2015.
[245] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
[246] J. Zhang *et al.*, "Achievable ergodic secrecy rate for MIMO SWIPT wiretap channels," in *Proc. IEEE ICC*, London, U.K., Jun. 2015, pp. 453–458.
[247] D. W. K. Ng and R. Schober, "Secure and green SWIPT in distributed antenna networks with limited backhaul capacity," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5082–5097, Sep. 2015.
[248] Q. Shi, W. Xu, J. Wu, E. Song, and Y, Wang, "Secure beamforming for MIMO broadcasting with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2841–2853, May 2015.
[249] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure transmission in MISO simultaneous wireless information and power transfer system," *IEEE Trans. Veh. Technol.*, vol. 64, no. 1, pp. 400–405, Jan. 2015.
[250] M. Tian, X. Huang, Q. Zhang, and J. Qin, "Robust AN-aided secure transmission scheme in MISO channels with simultaneous wireless information and power transfer," *IEEE Signal Process. Lett.*, vol. 22, no. 6, pp. 723–727, Jun. 2015.
[251] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.
[252] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 906–915, Mar. 2015.
[253] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2462–2467, Jun. 2014.
[254] X. Chen, J. Chen, and T. Liu, "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8025–8035, Oct. 2016.
[255] C. Du, X. Chen, and L. Lei, "Energy-efficient power allocation for secure communications in wireless powered massive MIMO relaying systems," in *Proc. WCSP*, Nanjing, China, Oct. 2015, pp. 1–6.
[256] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.
[257] R. Yin *et al.*, "Joint spectrum and power allocation for D2D communications underlaying cellular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2182–2195, Apr. 2016.
[258] R. Tanbourgi, H. Jäkel, and F. K. Jondral, "Cooperative interference cancellation using device-to-device communications," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 118–124, Jun. 2014.
[259] R. Yin, G. Yu, H. Zhang, Z. Zhang, and G. Y. Li, "Pricing-based interference coordination for D2D communications in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1519–1532, Mar. 2015.
[260] M. Alam, D. Yang, J. Rodriguez, and R. A. Abd-Alhameed, "Secure device-to-device communication in LTE-A," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 66–73, Apr. 2014.
[261] S. A. M. Ghanem and M. Ara, "Secure communications with D2D cooperation," in *Proc. IEEE ICCSPA*, Sharjah, UAE, Feb. 2015, pp. 1–6.
[262] K. Zhang, M. Peng, P. Zhang, and X. Li, "Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2016.2566298.
[263] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.
[264] C. Ma *et al.*, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.
[265] Z. Chu, K. Cumanan, M. Xu, and Z. Ding, "Robust secrecy rate optimisations for multiuser multiple-input–single-output channel with device-to-device communications," *IET Commun.*, vol. 9, no. 3, pp. 396–403, Feb. 2015.
[266] C. Shahriar *et al.*, "PHY-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292–314, 1st Quart., 2015.
[267] L. Wang, T. Ke, M. Song, Y. Wei, and Y. Teng, "Research on secrecy capacity oriented relay selection for mobile cooperative networks," in *Proc. IEEE CCIS*, Beijing, China, Sep. 2011, pp. 443–447.
[268] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.



Xiaoming Chen (M'10–SM'14) received the B.Sc. degree from Hohai University in 2005, the M.Sc. degree from the Nanjing University of Science and Technology in 2007, and the Ph.D. degree from Zhejiang University, China, in 2011, all in electronic engineering. He is currently a Research Professor with the College of Information Science and Electronic Engineering, Zhejiang University. He was an Associate Professor with the Nanjing University of Aeronautics and Astronautics, China, and a Humboldt Research Fellow with Friedrich-Alexander-University Erlangen-Nürnberg, Germany. His research interests mainly focus on multiple-antenna techniques, wireless security, wireless power transfer, and mobile computing. He serves as an Associate Editor for the IEEE ACCESS and an Editor for the IEEE COMMUNICATIONS LETTERS. He was honoured as an Exemplary Reviewer of the IEEE COMMUNICATIONS LETTERS in 2014 and the IEEE TRANSACTIONS ON COMMUNICATIONS in 2015.

Derrick Wing Kwan Ng (S'06–M'12) received the bachelor's (First Class Hons.) degree and the M.Phil. degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST) in 2006 and 2008, respectively, and the Ph.D. degree from the University of British Columbia (UBC) in 2012. In the Summer of 2011 and Spring of 2012, he was a Visiting Scholar with the Centre Tecnològic de Telecomunicacions de Catalunya-Hong Kong. He was a Senior Post-Doctoral Fellow with the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg, Germany. He is currently a Lecturer with the University of New South Wales, Sydney, Australia. His research interests include convex and nonconvex optimization, physical layer security, wireless information and power transfer, and green (energy-efficient) wireless communications. He was a recipient of the Australian Research Council's Discovery Early Career Researcher Award in 2017, the Best Paper Awards at the IEEE International Conference on Computing, Networking and Communications 2016, the IEEE Wireless Communications and Networking Conference (WCNC) 2012, the IEEE Global Telecommunication Conference (Globecom) 2011, and the IEEE Third International Conference on Communications and Networking in China 2008, the IEEE Student Travel Grants for attending the IEEE WCNC 2010, the IEEE International Conference on Communications (ICC) 2011, and the IEEE Globecom 2011, the 2009 Four Year Doctoral Fellowship from the UBC, Sumida & Ichiro Yawata Foundation Scholarship in 2008, and the Research and Development Excellence Scholarship from the Center for Wireless Information Technology, HKUST, in 2006. He has been serving as an Editorial Assistant to the Editor-in-Chief for the IEEE TRANSACTIONS ON COMMUNICATIONS since 2012. He is currently an Editor of the IEEE COMMUNICATIONS LETTERS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING. He was the Co-Chair of the Wireless Access Track of the 2014 IEEE 80th Vehicular Technology Conference. He has been a TPC member of various conferences, including the Globecom, WCNC, ICC, VTC, and PIMRC. He was honoured as an Exemplary Reviewer of the IEEE TRANSACTIONS ON COMMUNICATIONS in 2015, the Top Reviewer of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2014, and an Exemplary Reviewer of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2012, 2014, and 2015.

Wolfgang H. Gerstacker (S'93–M'98–SM'11) received the Dipl.-Ing. degree in electrical engineering, the Dr.-Ing. degree, and the Habilitation degree from Friedrich-Alexander-University Erlangen-Nürnberg, Germany, in 1991, 1998, and 2004, respectively. Since 2002, he has been with the Chair of Mobile Communications (currently, the Institute for Digital Communications), University of Erlangen-Nürnberg, where he is currently a Professor. He has conducted various projects with partners from industry. His research interests are in the broad area of digital communications and statistical signal processing. He was a recipient of several awards, including the Research Award of the German Society for Information Technology in 2001, the EEEfCOM Innovation Award in 2003, the Vodafone Innovation Award in 2004, the Best Paper Award of EURASIP Signal Processing in 2006, and the "Mobile Satellite & Positioning" Track Paper Award of VTC2011-Spring. He is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He is an Area Editor of *Physical Communication* (Elsevier). He was an Editorial Board Member of the *EURASIP Journal on Wireless Communications and Networking* from 2004 to 2012 and served as a Guest Editor for several Special Issues of Journals. He has served as a Technical Program Committee Member of various conferences. He has been the Technical Program Co-Chair of the IEEE International Black Sea Conference on Communications and Networking 2014, the Co-Chair of the Cooperative Communications, Distributed MIMO and Relaying Track of VTC2013-Fall, and serves as the General Chair for ACM NanoCom 2016.

Hsiao-Hwa Chen (S'89–M'91–SM'00–F'10) received the B.Sc. and M.Sc. degrees from Zhejiang University, China, in 1982 and 1985, respectively, and the Ph.D. degree from the University of Oulu, Finland, in 1991. He is currently a Distinguished Professor with the Department of Engineering Science, National Cheng Kung University, Taiwan. He has authored or co-authored over 400 technical papers in major international journals and conferences, six books, and over ten book chapters in the areas of communications. He was a recipient of the Best Paper Award in IEEE WCNC 2008 and the IEEE 2016 Jack Neubauer Memorial Award. He served or is serving as an Editor or/and Guest Editor for numerous technical journals. He served as the General Chair, the TPC Chair, and the Symposium Chair for many international conferences. He is the Founding Editor-in-Chief of *Security and Communication Networks Journal* (Wiley). He served as the Editor-in-Chief for the IEEE WIRELESS COMMUNICATIONS from 2012 to 2015. He is a fellow of IET, and an elected Member at Large of IEEE ComSoc.