A Survey of Optimization Approaches for Wireless Physical Layer Security

Dong Wang, Bo Bai, *Senior Member, IEEE*, Wenbo Zhao, and Zhu Han, *Fellow, IEEE*

***Abstract*—Due to the malicious attacks in wireless networks, physical layer security has attracted increasing concerns from both academia and industry. The research on physical layer security mainly focuses either on the secrecy capacity/achievable secrecy rate/capacity-equivocation region from the perspective of information theory, or on the security designs from the viewpoints of optimization and signal processing. Because of its importance in security designs, the latter research direction is surveyed in a comprehensive way in this paper. The survey begins with typical wiretap channel models to cover common scenarios and systems. The topics on physical-layer security designs are then summarized from resource allocation, beamforming/precoding, and antenna/node selection and cooperation. Based on the aforementioned schemes, the performance metrics and fundamental optimization problems are discussed, which are generally adopted in security designs. Thereafter, the state of the art of optimization approaches on each research topic of physical layer security is reviewed from four categories of optimization problems, such as secrecy rate maximization, secrecy outrage probability minimization, power consumption minimization, and secure energy efficiency maximization. Furthermore, the impacts of channel state information on optimization and design are discussed. Finally, the survey concludes with the observations on potential future directions and open challenges.**

***Index Terms*—Physical layer security, optimization, resource allocation, beamforming, precoding, cooperative transmission.**

I. Introduction

With the rapid evolution of information and communication technologies, mobile Internet and Internet of Things (IoT) have become indispensable in daily life. As the foundation of these networks, the cellular network has been designed to support Internet connectivity and full interworking with heterogeneous wireless access networks [1]. This fact, therefore, leads to complicated network architectures, network topologies, access technologies, service requirements, and mobile equipments while bringing serious security issues in wireless information transmission. How to guarantee the security of confidential information has become the precondition to the commercial application of some emerging wireless networks and communication services. Therefore, the theories and technologies of information security have attracted increasing concerns from both academia and industry recently.

During last few decades, the information security mostly depends on the cryptographic encryption and decryption methods which are deployed at the upper layers of protocol stack. The encryption-based security technologies have been shown to be effective in many cases, but their inherent vulnerabilities are heavy computation and key management costs which may result in high complexity and resource consumption [2]. As an alternative security technology, the physical layer security, based on the information theory framework, is to utilize the inherent randomness of the physical medium and the difference between the legitimate channels and the wiretap channels to guarantee secure information transmission [3]. Compared with cryptographic approaches, as shown in Table I, the physical layer security does not rely on the computing capability of the communication equipments, and thus has the advantages of lower complexity and resource savings. It has been shown from the viewpoint of information theory that the physical layer security can achieve perfect secrecy even if the eavesdropper has very strong computing capability. Besides, the physical layer security has a performance metric for secrecy evaluation, i.e., equivocation rate which measures the uncertainty of the confidential message at eavesdroppers. Furthermore, by exploiting the physical layer features, this security technique can flexibly adjust transmission strategies and parameters to accommodate the channel changes. In summary, physical layer security presents distinctive advantages and promising prospects. Therefore, the physical layer security can be used as an effective supplementary for the cryptographic techniques to further enhance information security.

The concept of secrecy communication was first proposed in the pioneering work of Shannon in 1949 [4], in which secrecy communication was investigated from the viewpoint of information theory. It was proposed therein that the approach termed "one-time pad" could achieve the perfect secrecy. However, it was very difficult to apply this method in practice due to the intractable difficulties of key generation and management. Being different from the Shannon's model of

Manuscript received March 3, 2018; revised September 15, 2018; accepted October 28, 2018. Date of publication November 23, 2018; date of current version May 31, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61871401, in part by the Anhui Provincial Natural Science Foundation under Grant 1708085MF139 and Grant 1708085QF158, in part by the U.S. AFOSR MURI under Grant 18RT0073, and in part by NSF under Grant CNS-1717454, Grant CNS-1731424, Grant CNS-1702850, Grant CNS-1646607, and Grant ECCS-1547201. *(Corresponding author: Bo Bai.)*

D. Wang and W. Zhao are with the New Star Research Institute of Applied Technology, Hefei 230031, China (e-mail: eewgdg@yeah.net; zhao-wen-bo@139.com).

B. Bai is with the Future Network Theory Laboratory, 2012 Labs, Huawei Technologies Company Ltd., Hong Kong (e-mail: baibo8@huawei.com).

Z. Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 02447, South Korea (e-mail: zhan2@uh.edu).

Digital Object Identifier 10.1109/COMST.2018.2883144

TABLE I
COMPARISON BETWEEN CRYPTOGRAPHIC ENCRYPTION AND PHYSICAL LAYER SECURITY

	Cryptographic encryption	Physical layer security
Theoretical basis	Cryptography	Information theory
Secrecy level	Can be deciphered by brute-force computing	Achieving perfect secrecy
Computing ability requirements	Heavily relying on the computing ability	Being independent of computing ability
Encryption key management	Heavy costs resulting from key generation, management, and distribution	With no need of any key
Evaluation criterion	Being unable to accurately assess the leakage of confidential information	Evaluating secrecy precisely by equivocation rate
Adaptability to channel changes	Poor channel adaptability	Adjusting transmission strategies and parameters to well adapt the channel changes

secrecy communication, Wyner proposed the wiretap channel model in 1975 [5], in which the perfect secrecy could be achieved at the physical layer by utilizing the difference between the legitimate channel and the illegitimate channel without any key. In Wyner's wiretap channel model, the signal received by the eavesdropper was a degraded version of the signal received by the destination. The characteristic of signal degradation at the eavesdropper made it possible to achieve secrecy at the physical layer. It was also proved by Wyner that the secrecy capacity of a discrete memoryless channel was the maximum value of the difference between the mutual information of the legitimate link and the mutual information of the wiretap link. Thereafter, Csiszár and Körner generalized the degraded wiretap channel to broadcast channel with confidential messages, and analysed the secrecy capacity of a more general (non-degraded) wiretap channel [6]. Following these works, Leung-Yan-Cheong and Hellman investigated the Gaussian wiretap channel and derived the secrecy capacity which is the difference of legitimate channel capacity and wiretap channel capacity [7]. Nevertheless, the early research work cannot be applied directly, since the physical layer security needed suitable secure coding schemes to match the channel states. However, the secure coding technology was less developed in early stage, and the theories and technologies on physical layer security were thus believed to be impractical. Moreover, the fact that the encryption-based security technologies held a dominant position for a long time affected the development of physical layer security. In recent decades, the encryption-based security technologies have exposed some limitations in practical applications. Meanwhile, the coding theories and technologies have got a rapid development, which laid a solid foundation of physical layer security. Accordingly, more and more attentions have been paid on the physical layer security.

The studies on physical layer security can be roughly summarized from two main aspects: 1) the studies related to secrecy rate/capacity from the perspective of information-theoretic security, 2) and the studies related to system designs from the viewpoints of optimization and signal processing [8]–[12]. The first aspect mainly focuses on the secrecy capacity, achievable secrecy rate, and capacity-equivocation region based on the ideas of information theory. On the other hand, the second aspect mainly focuses on the secure strategy designs based on the techniques of optimization and signal processing. Because of the importance in practical security designs, our objective in this survey is to provide a comprehensive overview on the optimization and design of secure physical layer transmission. The investigations on the topic that we just mentioned are based on the framework of information-theoretic security, since all involved performance metrics, optimization problems, and security solutions in this survey are intertwined with the secrecy rate/capacity which are based on information theory.

Many excellent surveys have been published in physical layer security, which provide comprehensive overviews and insightful comments to understand the fundamental principles, technology status, and future trends in this field. In [13], the fundamentals and technologies of physical layer security are reviewed comprehensively. Specifically, in [13], the technologies, challenges, and solutions are summarized from more methodological viewpoints involving wiretap coding, multi-antenna and relay cooperation, physical-layer key generation, and physical-layer authentication. Moreover, we highlight the focused issues and the main contents of some published surveys in Table II. In contrast to existing surveys, our work tries to review the recent advances in physical layer security from the perspective of system optimization and design. First, we summarize the research topics and the secure strategies that cover extensive problems in system optimization and design, such as secure resource allocation, signal processing and cooperative diversity. Second, the performance metrics and the related optimization problem formulations are investigated to provide deep insights into secure transmission designs. Finally, we survey the state of the art of optimization and design on each research topic of physical layer security from four categories of basic optimization problems, i.e., maximization of achievable secrecy rate, minimization of secrecy outrage probability, minimization of power consumption, and maximization of secure energy efficiency (EE). In particular, some optimization approaches and secure strategies which are usually appeared in physical-layer transmission designs are summarized with detailed procedures.

In summary, this survey provides a well-rounded overview for newcomers to understand the optimization and design

TABLE II
BRIEF SUMMARIES ON EXISTING SURVEYS

Surveys	Publications	Focused issues	Main contents
[1]	IEEE Communications Surveys & Tutorials	Security for long term evolution (LTE) and LTE-advanced Networks.	Security functionalities, security vulnerabilities, and existing security solutions.
[10]	IEEE Communications Surveys & Tutorials	Physical layer security in multiuser wireless networks.	Security improvements in multi-antenna, broadcast, multiple-access, interference, and relay channels, as well as physical-layer key generation and secure coding.
[13]	IEEE Communications Surveys & Tutorials	Comprehensive overview on the fundamentals and technologies of physical layer security.	Technologies, challenges, and solutions in physical layer security are studied from the aspects of wiretap coding, multi-antenna and relay cooperation, physical-layer key generation, and physical-layer authentication.
[11]	Proceedings of the IEEE	Lessons learned from information-theoretic security with multiple wireless transmitters.	Designing secure wireless systems with unauthenticated entities by cooperative jamming/relaying and interference alignment.
[14]	Proceedings of the IEEE	Security vulnerabilities, security threats, and efficient defense mechanisms.	Discussing the security requirements and attacks at each protocol layer, investigating the existing security protocols and algorithms, while exploring the state of the art in physical layer security.
[15]	Proceedings of the IEEE	Physical layer security in the Internet of Things.	Surveying the advances and challenges in resource constrained secrecy coding and secret-key generation in the Internet of Things.
[8]	IEEE Signal Processing Magazine	Cooperative security at physical layer.	Guaranteeing information security by using cooperative techniques which consist of carefully designed coding and signaling schemes.
[9]	IEEE Signal Processing Magazine	Signal processing techniques for secrecy in multi-antenna wireless systems.	Enhancing physical layer security in multi-antenna systems by beamforming/precoding with or without artificial noise.
[12]	IEEE Communications Magazine	Recent research on enhancing secrecy via cooperation.	Signal design and optimization to increase secrecy based on cooperative relaying and jamming.
[16]	IEEE Communications Magazine	A joint framework involving both the physical layer and application layer security technologies.	Proposing a joint security scheme by exploiting the security capacity and signal processing technologies at the physical layer and the authentication and watermarking strategies at the application layer.
[17]	IEEE Communications Magazine	Physical layer security for massive MIMO.	Discussing the passive eavesdropping and active attacks in massive MIMO systems while proposing three detection schemes to identify the active attacks.
[18]	IEEE Communications Magazine	Physical layer security in cooperative relay networks.	Pure or hybrid relaying/jamming combinations for secrecy improvements with trusted/untrusted relays.
[19]	IEEE Communications Magazine	Physical layer security in the 5G network.	The opportunities and challenges offered by the disruptive technologies enabling 5G for achieving high physical layer security.
[20]	IEEE Communications Magazine	Challenges of physical layer security in practical applications.	Identifying the important issues to apply physical layer security into practice.
[21]	IEEE Wireless Communications	Several prevalent methods to enhance physical layer security.	Classifying the methods of physical layer security into five major categories while comparing their reliability, computational complexity, and secrecy capacity.
[22]	IEEE Network	Diversity techniques to improve physical layer security.	Exploiting MIMO diversity, multiuser diversity, and cooperative diversity to secure wireless communications.

in physical layer security. The contributions of this survey is based on the following work: 1) Summarizing general wiretap channel models to cover the basic scenarios in this field, followed with usually appeared optimization approaches. 2) Investigating hot topics in physical layer security from the perspective of system optimization and design. 3) Seeking deep insights into performance metrics to achieve different requirements in system designs. 4) Reviewing the state of the art of optimization and design in this field and the harmful impacts of channel state information (CSI) on designing security solutions. 5) Discussing future possible directions and open challenges.

The remainder of this paper is organized as follows. In Section II, typical wiretap channel models and optimization concepts are introduced to cover common communication scenarios and optimization approaches. In Section III, the research topics in physical layer security are investigated from the perspective of secure resource allocation, beamforming/procoding, and antenna/node selection and cooperation. In Section IV, we seek deep insights into performance metrics which can be adopted in all research topics to evaluate the proposed secure transmission strategies. The state of the art of optimization and design in physical layer security is reviewed in Section V, followed with usually appeared optimization approaches and security strategies. Section VI investigates the common assumptions of CSI and their negative impacts on secure transmission designs. Future possible directions and open challenges are discussed In Section VII to provide some lessons for newcomers. Finally, the survey is concluded in Section VIII. A diagram is illustrated in Fig. 1 to show the

TABLE III
ABBREVIATIONS AND THEIR DEFINITIONS

Abbreviation	Definition
5G	The fifth generation
AF	Amplify-and-forward
AN	Artificial noise
CSI	Channel state information
CI	Channel inversion
DC	Difference of convex functions
DF	Decode-and-forward
EE	Energy efficiency
GSVD	Generalized singular value decomposition
I/Q	In-phase and quadrature
IoT	Internet of things
LTE	Long term evolution
MIMO	Multiple-input multiple-output
MIMOME	Multi-input multi-output multi-eavesdropper
MISO	Multiple-input single-output
MISOME	Multi-input single-output multi-eavesdropper
MRC	Maximal ratio combining
MRT	Maximum ratio transmission
mm-Wave	Millimeter-wave
OFDMA	Orthogonal frequency division multiple access
QoS	Quality of service
RCI	Regularized channel inversion
SISO	Single-input single-output
SIMO	Single-input multiple-output
SDP	Semidefinite programming
SDR	Semidefinite relaxation
SE	Spectrum efficiency
SPCA	Sequential parametric convex approximation
SNR	Signal-to-noise ratio
SINR	Signal-to-interference-plus-noise ratio
S-DPC	Secret dirty-paper coding
ZF	Zero-forcing

outline and structure of this paper. In addition, abbreviations used in this paper are defined in Table III.

Notations: Throughout this paper, matrices and vectors are denoted by bold uppercase letters and bold lowercase letters, respectively. $\boldsymbol{x}$ denote the set of optimization variable without physical meaning. Mutual information, conjugate transpose, and Euclidean norm are represented by $I(\cdot;\cdot)$, $(\cdot)^H$, and $\|\cdot\|$, respectively. The trace of a matrix is denoted by Tr(). $\mathbf{W} \succeq \mathbf{0}$ means that $\mathbf{W}$ is a positive semidefinite matrix.

II. FUNDAMENTALS

In this section, we give several typical wiretap channel models to cover the common scenarios and systems considered in the survey, and introduce general concepts of optimization and optimization problems to clarify the variables and parameters in security designs.

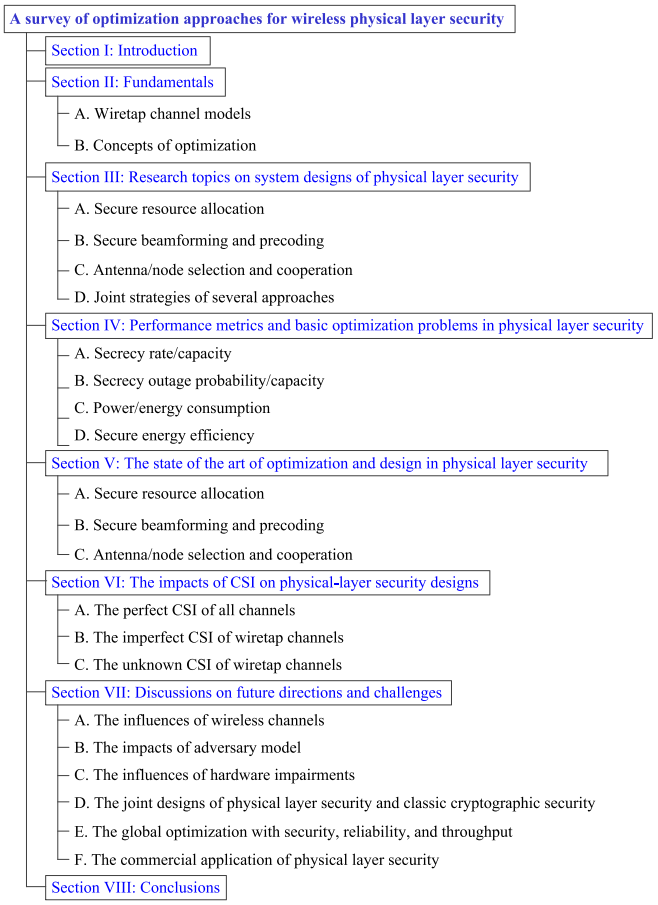


Fig. 1. The structural diagram of this survey.

A. Wiretap Channel Models

The typical wiretap channel models usually include multiple-input multiple-output (MIMO) wiretap channels, broadcast wiretap channels, multiple-access wiretap channels, interference wiretap channels, and relay wiretap channels [10], etc.

1) MIMO Wiretap Channels: The simplest network in physical layer security is composed of a transmitter, a legitimate receiver, and an unauthorized receiver (eavesdropper), in which confidential messages are exchanged between the transmitter and the legitimate receiver while protecting from the unauthorized receiver. In such a scenario, the terminals may be equipped with multiple antennas. The typical channel model for multi-antenna scenarios is the MIMO wiretap channel which can cover the special models of single-input single-output (SISO), single-input multiple-output (SIMO), and multiple-input single-output (MISO) channels. In the MIMO channel in which the transmitter, receiver, and eavesdropper are deployed with n_t, n_d, and n_e antennas, respectively, the general expressions for the received signals at the legitimate receiver and eavesdropper are, respectively,

given by [10]

$$\mathbf{y}_d = \mathbf{H}_d \mathbf{x}_s + \mathbf{z}_d, \tag{1}$$

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x}_s + \mathbf{z}_e, \tag{2}$$

where $\mathbf{x}_s$ is the $n_t \times 1$ encoded signal with a covariance matrix constraint $\mathbb{E}\{\mathbf{x}_s \mathbf{x}_s^H\} = \mathbf{Q}_x$ for $\mathbf{Q}_x \succeq \mathbf{0}$ or an average power constraint $\mathrm{Tr}\{\mathbf{Q}_x\} \leq P_{max}$ for a peak power P_{max}. The $n_d \times n_t$ matrix $\mathbf{H}_d$ and the $n_e \times n_t$ matrix $\mathbf{H}_e$ are the channel gain matrices to the legitimate receiver and the eavesdropper, respectively. $\mathbf{z}_d$ and $\mathbf{z}_e$ are white Gaussian noise vectors at the legitimate receiver and eavesdropper, respectively. This wiretap channel model is typical, and to be widely investigated in physical layer security.

2) Broadcast Wiretap Channels: The broadcast wiretap channels are raised in multi-user networks with more than two receivers where one transmitter delivers confidential information to multiple users with the presence of multiple eavesdroppers. We assume that there are one transmitter equipped with n_t antennas, *I* users each with n_{d_i} antennas, and *J* eavesdroppers each with n_{e_j} antennas. In the downlink, the transmitter transmits confidential messages to the legitimate users while preventing from overhearing of the eavesdroppers. This broadcast channel can be equivalent to a compound wiretap channel which is defined as [3], [23]

$$\mathbf{y}_{d_i} = \mathbf{H}_{d_i} \mathbf{x}_s + \mathbf{z}_{d_i}, i = 1, 2, \ldots, I, \tag{3}$$

$$\mathbf{y}_{e_j} = \mathbf{H}_{e_j} \mathbf{x}_s + \mathbf{z}_{e_j}, j = 1, 2, \ldots, J, \tag{4}$$

where $\mathbf{x}_s$ denotes the $n_t \times 1$ encoded signal for the confidential messages which is subject to a covariance matrix constraint $\mathbb{E}\{\mathbf{x}_s \mathbf{x}_s^H\} = \mathbf{Q}_x$ for $\mathbf{Q}_x \succeq \mathbf{0}$ or an average power constraint $\mathrm{Tr}\{\mathbf{Q}_x\} \leq P_{max}$ for a peak power P_{max}. $\mathbf{y}_{d_i}$ and $\mathbf{y}_{e_j}$ are the received signals at user *i* and eavesdropper *j*, respectively. $\mathbf{H}_{d_i}$ is $n_{d_i} \times n_t$ channel matrix to user *i* and $\mathbf{H}_{e_j}$ is $n_{e_j} \times n_t$ channel matrix to eavesdropper *j*. $\mathbf{z}_{d_i}$ and $\mathbf{z}_{e_j}$ are white Gaussian noise vectors at user *i* and eavesdropper *j*, respectively. The compound wiretap channel has several special cases including the parallel wiretap channel with two eavesdroppers, the fading wiretap channel with multiple eavesdroppers, and the wiretap channel with multiple receivers [3], etc. In addition, another specific broadcast channel is the broadcast channel with separate confidential messages of each user in which each downlink message must be kept secret from all other unintended users (each user is seen as an eavesdropper for messages not intended to it) [10].

3) Multiple-Access Wiretap Channels: In the multiple-access wiretap channel, multiple transmitters transmit messages to a legitimate receiver with the existence of an eavesdropper. There are *K* transmitters each with n_{t_k} antennas, one legitimate receiver with n_d antennas, and one eavesdropper with n_e antennas. Let us define $n_d \times n_{t_k}$ matrix $\mathbf{H}_{d_k}$ and $n_e \times n_{t_k}$ matrix $\mathbf{H}_{e_k}$ as the channel matrices from transmitter *k* to the receiver and the eavesdropper, respectively. Then, the received signals at the receiver and the eavesdropper are, respectively, expressed as [24]

$$\mathbf{y}_d = \sum_{k=1}^{K} \mathbf{H}_{d_k} \mathbf{x}_{s_k} + \mathbf{z}_d, \tag{5}$$

$$\mathbf{y}_e = \sum_{k=1}^{K} \mathbf{H}_{e_k} \mathbf{x}_{s_k} + \mathbf{z}_e, \tag{6}$$

where $\mathbf{x}_{s_k}$ denotes the $n_{t_k} \times 1$ encoded signal at transmitter *k* with a covariance matrix constraint or an average power constraint. $\mathbf{z}_d$ and $\mathbf{z}_e$ are the white Gaussian noise vectors at the receiver and the eavesdropper, respectively. Some special cases of multiple-access channel in physical layer security are also investigated, such as SISO multiple-access channel with an eavesdropper [25] and multiple-access channel with common and confidential messages [3].

4) Interference Wiretap Channels: The interference wiretap channel refers to the scenario where multiple links are simultaneously active in the same time and frequency slot, and hence potentially interfere with each other [26]. At the same time, the communications over the multiple links are overheard by an eavesdropper. We consider the interference wiretap channel with *K* user pairs and an eavesdropper, where the source user *k*, the destination user *k*, and the eavesdropper are deployed with n_{t_k}, n_{d_k}, and n_e antennas, respectively, $k = 1, \ldots, K$. The received signals of destination user *k* and the eavesdropper are, respectively, written as [27]

$$\mathbf{y}_{d_k} = \mathbf{H}_{d_{kk}} \mathbf{x}_{s_k} + \sum_{l \neq k}^{K} \mathbf{H}_{d_{kl}} \mathbf{x}_{s_l} + \mathbf{z}_{d_k}, \tag{7}$$

$$\mathbf{y}_e = \sum_{l=1}^{K} \mathbf{H}_{e_l} \mathbf{x}_{s_l} + \mathbf{z}_e, \tag{8}$$

where $\mathbf{x}_{s_l}$ is the $n_{t_l} \times 1$ transmitted signal of source user *l* with a covariance matrix constraint or an average power constraint. The $n_{d_k} \times n_{t_l}$ matrix $\mathbf{H}_{d_{kl}}$ denotes the channel matrix from source user *l* to destination user *k*. The $n_e \times n_{t_l}$ matrix $\mathbf{H}_{e_l}$ denotes the channel matrix from source user *l* to the eavesdropper. $\mathbf{z}_{d_k}$ and $\mathbf{z}_e$ are the white Gaussian noise vectors at destination user *k* and the eavesdropper, respectively. A further model of interest is the interference channel with separate confidential messages, in which each source message must be kept confidential from all other unintended users. A specific case of this channel model is studied in [3] where SISO interference channel is used to deliver two confidential messages.

5) Relay Wiretap Channels: A typical cooperative wireless network considering physical layer security is consist of a source, a destination, a relay, and an eavesdropper, each with n_t, n_d, n_r, and n_e antennas, respectively. The relay is operated in a decode-and-forward (DF) mode. In the first phase, the source transmits the $n_t \times 1$ signal vector $\mathbf{x}_s$ to the relay. The relay, the destination, and the eavesdropper receive the signal as [28]

$$\mathbf{y}_r = \mathbf{H}_{sr} \mathbf{x}_s + \mathbf{z}_r, \tag{9}$$

$$\mathbf{y}_d^{(1)} = \mathbf{H}_{sd} \mathbf{x}_s + \mathbf{z}_d, \tag{10}$$

$$\mathbf{y}_e^{(1)} = \mathbf{H}_{se} \mathbf{x}_s + \mathbf{z}_e, \tag{11}$$

where the $n_r \times n_t$ matrix $\mathbf{H}_{sr}$, the $n_d \times n_t$ matrix $\mathbf{H}_{sd}$, and the $n_e \times n_t$ matrix $\mathbf{H}_{se}$ are the channel matrices from the source to the relay, the destination, and the eavesdropper, respectively. $\mathbf{z}_r$, $\mathbf{z}_d$, and $\mathbf{z}_e$ are the white Gaussian noise vectors at the relay,

the destination, and the eavesdropper, respectively. The relay decodes the received signal and forwards it to the destination. Let the $n_d \times n_r$ matrix $\mathbf{H}_{rd}$ and the $n_e \times n_r$ matrix $\mathbf{H}_{re}$ denote the channel matrices from the relay to the destination and the eavesdropper, respectively. In the second phase, the $n_r \times 1$ transmitted signal vector $\mathbf{x}_r$ of the relay is a new version of $\mathbf{x}_s$ by using an encoding scheme. Then, the received signals at the destination and the eavesdropper are, respectively, obtained as

$$\mathbf{y}_d^{(2)} = \mathbf{H}_{rd}\mathbf{x}_r + \mathbf{z}_d, \tag{12}$$

$$\mathbf{y}_e^{(2)} = \mathbf{H}_{re}\mathbf{x}_r + \mathbf{z}_e. \tag{13}$$

The other typical cooperative channel model is the amplify-and-forward (AF) relay channel which is also investigated extensively in physical layer security, such as in [29] and [30].

B. Concepts of Optimization

In this subsection, the concepts of optimization and optimization problems are introduced for understanding the survey easily.

1) General Optimization Problem: A general mathematical optimization problem can be formulated as [31]

$$\min_{\boldsymbol{x}} \ f(\boldsymbol{x}) \quad \text{s.t.} \ \begin{cases} h_i(\boldsymbol{x}) \le b_i, & i = 1, 2, \ldots, m, \\ g_j(\boldsymbol{x}) = c_j, & i = 1, 2, \ldots, n, \end{cases} \tag{14}$$

where $\boldsymbol{x}$ is the set of optimization variable. The function $f(\boldsymbol{x})$ is the objective function. The constraint conditions $h_i(\boldsymbol{x}) \le b_i$ and $g_j(\boldsymbol{x}) = c_j$ are the inequality and equality constraints, respectively. If there is no constraint, we say the problem is unconstrained. The optimization problem formulated in (14) describes the problem of finding an optimal $\boldsymbol{x}^*$ that minimizes $f(\boldsymbol{x})$ among all $\boldsymbol{x}$ satisfying the constraints $h_i(\boldsymbol{x}) \le b_i$ and $g_j(\boldsymbol{x}) = c_j$. Therefore, $\boldsymbol{x}^*$ is called the optimal solution of the problem (14).

Convex optimization is an important class of optimization problem. The standard convex optimization is defined as [31]

$$\min_{\boldsymbol{x}} \ f(\boldsymbol{x}) \quad \text{s.t.} \ \begin{cases} h_i(\boldsymbol{x}) \le b_i, & i = 1, 2, \ldots, m, \\ d_j^T \boldsymbol{x} = c_j, & j = 1, 2, \ldots, n, \end{cases} \tag{15}$$

where $f(\boldsymbol{x})$ and $h_i(\boldsymbol{x})$ are convex functions. Comparing to problem (14), the convex problem has the characteristics that the objective function and inequality constraint functions must be convex while the equality constraint functions $g_j(\boldsymbol{x}) = d_j^T \boldsymbol{x} - c_j$ must be affine [31]. Convex optimization problems can be solved optimally by many efficient algorithms, such as interior-point methods. If a practical problem can be formulated as a convex optimization problem, the original problem can then be solved. Therefore, many problems can be solved via convex optimization by transforming the original problem into a convex optimization problem.

Another class of optimization problem is nonconvex optimization which covers the problems with nonconvex objective function or/and nonconvex constraint functions. The nonconvex optimization problems are usually intractable. The complexity of global optimization methods for nonconvex problems may grow exponentially with the problem sizes. However, some nonconvex problems can be transformed into or approximated by convex problems. By solving the resulting convex problems, we can get the optimal solution of the original nonconvex problems. Moreover, to overcome the difficulties of solving nonconvex problems, some heuristic algorithms can be designed based on convex optimization, such as randomized algorithms in which an approximate solution to a nonconvex problem is found by drawing some number of candidates from a probability distribution, and taking the best one found as the approximate solution [31]. In addition, for nonconvex problems, the compromise is to give up seeking the optimal solution. Instead, we seek a locally optimal solution by combining convex optimization with a local optimization method, where convex optimization can be used for initialization of local optimization.

2) Optimization in Physical Layer Security: Following the great progress in theories and algorithms of optimization, the system designs in physical layer security has greatly benefited from recent advances to the point where optimization has now emerged as a major signal processing technique.

Towards general optimization problem (14) in physical layer security, the objective function $f(\boldsymbol{x})$ may be the considered performance metrics, such as secrecy rate/capacity, secrecy outage probability/capacity, power consumption, and secure EE which will be elaborated in Section IV. The optimization variable $\boldsymbol{x}$ may be the resources in the designs of secure resource allocation, beamformer/precoder in the designs of secure beamforming/precoding, or candidates of antennas/cooperative nodes in the designs of antenna/node selection and cooperation. The secure resource allocation, beamforming/precoding, and antenna/node selection and cooperation mentioned here are the research topics in physical layer security, which will be discussed in detail in Section III.

In physical layer security, the majority of optimization problems are nonconvex due to the property of logarithmic subtraction in secrecy rate/capacity. We can roughly list several optimization problems usually appeared in this field as follows.

- Integer programming in which some or all optimization variables are constrained to be integer values. This kind of problems is usually raised in the designs of secure subcarrier allocation and antenna/node selection.
- Mixed integer programming that concerns the problems having discrete and continuous variables. In joint subcarrier and power allocation, or joint antenna/node selection and beamforming, such problems are dealt with usually.
- Difference of convex functions (DC) programming where the objective function is a subtraction of two convex functions. This feature fits with the definition of secrecy rate/capacity. Therefore, DC programming is widely used for solving the problems of secrecy rate maximization.
- Quadratic programming where the objective function has quadratic terms. This problem appears in the designs of secure power allocation and beamforming, such as the typical optimization problem of power minimization.

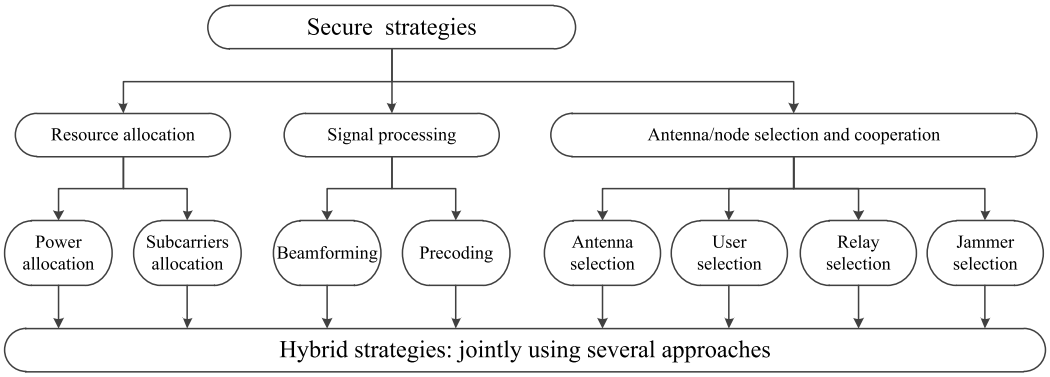


Fig. 2. Secure strategies for improving physical layer security.

- Semidefinite programming (SDP) which optimizes a linear function of the variables subject to linear equality constraints and a nonnegativity constraint on the variables. In physical layer security, some nonconvex problems are usually transformed into SDP to get an efficient algorithm that is easy to implement.
- Fractional programming which focuses on optimizing a ratio of two nonlinear functions. The typical example is EE maximization with the considerations of physical layer security.

To cope with the nonconvexity of the optimization problems in physical layer security designs, many optimization techniques have been proposed, such as dual decomposition, alternating search, penalty function method, sequential parametric convex approximation (SPCA), semidefinite relaxation (SDR), and so on, which will be discussed in Section V.

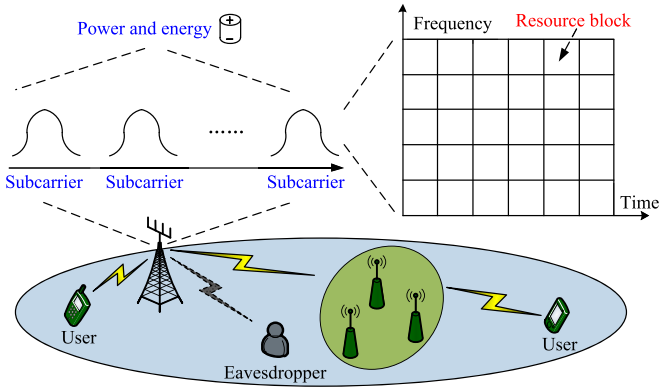


Fig. 3. An illustration of the multidimensional wireless resources in a multi-antenna multi-node OFDMA-based wireless network.

III. Research Topics on System Designs of Physical Layer Security

Many conventional physical layer technologies of wireless communications without secrecy consideration can be redesigned for confidential information transmission under the framework of physical layer security. From the perspective of system designs, the research topics on physical layer security mainly focus on secure resource allocation, secure beamforming/procoding, secure antenna/node selection[1] and cooperation, and the joint considerations based on the aforementioned strategies, as shown in Fig. 2.

A. Secure Resource Allocation

Resource allocation which has been widely used in the conventional communications without the consideration of secrecy [32], is also an effective way for enhancing physical layer security. The multidimensional wireless resources make it possible to intentionally extend the difference between the legitimate channel and the wiretap channel by secure resource allocation. The multidimensional wireless resources typically contain the frequency, timeslot, and power in orthogonal frequency division multiple access (OFDMA) networks. In multi-antenna and multi-node wireless networks, the wireless resources generally refer to the spatial degrees of freedom provided by multiple antennas and nodes, as shown in Fig. 3.

Given the limited network resources such as bandwidth and energy, the main challenge of secure resource allocation is to utilize the limited resources as efficient as possible to achieve the requirements of some performance metrics, such as secrecy rate, secrecy outage probability, power consumption, and secure EE. Hence, many works have focused on the two basic problems of secure resource allocation that are the subcarrier allocation and the power allocation in multicarrier networks.

The subcarrier allocation aims at finding the optimal subcarrier usage policy that is able to effectively improve spectral efficiency and information security. Without loss of generality, the secure subcarrier allocation is usually formulated as a binary integer programming [33]–[36]. More specifically, whether or not a subcarrier is used for communication is specified by a decision variable $\alpha \in \{0, 1\}$, with $\alpha = 1$ meaning that the subcarrier is used for transmitting and $\alpha = 0$ otherwise.

Adaptive power allocation among multiple carriers and nodes is another important method, which can be applied for a further performance improvement [37]–[48]. Accordingly,

[1]Node selection usually adopted in multi-node scenarios includes user selection, relay selection, and jammer selection.

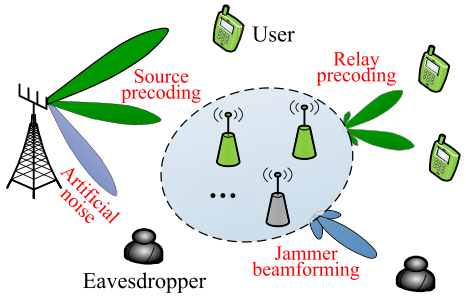


Fig. 4. An illustration of secure beamforming and precoding in a multi-antenna and multi-node cooperative network.

different strategies based on joint subcarrier and power allocation have been proposed to achieve different design requirements in physical layer security [34]–[36], [49]–[51]. The joint subcarrier and power allocation are generally modeled as mixed integer nonlinear optimization which is an NP-hard problem in most situations. In practice, a number of optimization techniques have been proposed to provide simple and suboptimal solutions for such combinatorial optimization problems [34], [35], [38], [49], [50].

B. Secure Beamforming and Precoding

Signal processing techniques, such as beamforming and precoding which are popular in multi-antenna and multi-node cooperative networks, have been demonstrated as promising ways to achieve the physical layer security [9]. The deployment of multi-antenna and multi-node cooperative networks is thought to have great potential to enhance not only transmission effectiveness and reliability but also wireless security. It has been verified that collaborative beamforming and precoding in multi-antenna and multi-node cooperative networks can bring some benefits in terms of the secrecy rate, secrecy outage probability, power/energy consumption, and secure EE.

Beamforming and precoding technologies have been exploited to achieve different performance requirements in secure transmission. Secure beamforming typically refers to one-rank transmission by which only single data stream is transmitted over multiple antennas or nodes, whereas secure precoding refers to multi-rank transmission by which more than one data streams can be transmitted at the same time [9]. Generally speaking, beamforming serves as a special case of precoding. An illustration of secure beamforming and precoding in multi-antenna and multi-node cooperative networks is shown in Fig. 4, where the source precoding is assisted by artificial noise (AN) and the intermediate nodes are used for relay precoding and jammer beamforming.

The main idea of secure beaforming is to compute the optimal beamforming vector for achieving some performance metrics of physical layer security by enhancing the signal quality at the destination node and decreasing the signal quality at the eavesdropper. Most of the secure beamforming involves solving optimization problems. Due to the special form of logarithmic subtraction in the secrecy rate, the optimization problems of secure beamforming are usually neither convex nor concave in many situations. Therefore, they can only be solved by numerical methods with high complexity, such as in [29] and [52]–[56]. To mitigate the computational cost, some low-complexity suboptimal algorithms have been proposed to simplify the beamforming designs [57], [58].

Noteworthily, several existing beamforming techniques which are simple but not optimal have been also adopted widely in different scenarios of secure communications, such as null-space beamforming (also named zero-forcing beamforming) [57]–[61] and maximum ratio transmission (MRT) beamforming [58], [62]–[64]. Null-space beamforming chooses the beamforming vector lying in the null space of the eavesdropper's channel vector. Then, the eavesdropper gets nothing in the transmission process, such that the information leakage is avoided. In optimization designs, nulling signal at the eavesdropper can be expressed as a constraint, i.e.,

$$\mathbf{h}_e \mathbf{w}^H = 0, \tag{16}$$

where $\mathbf{h}_e$ and $\mathbf{w}$ denote the eavesdropper's channel vector and the null-space beamforming vector, respectively. MRT is another attractive beamforming scheme because of its low computational complexity. MRT combined with maximal ratio combining (MRC) can maximize the signal-to-noise ratio (SNR) at the receiver and achieve a performance close to channel capacity in low-SNR scenarios [65]. In particular, the transmitter calculates its MRT beamforming vector, which only requires the knowledge of the channel from itself to the receiver. MRT beamforming can be expressed as

$$\mathbf{w} = \frac{\mathbf{h}^H}{\|\mathbf{h}\|}, \tag{17}$$

where $\mathbf{w}$ and $\mathbf{h}$ denote the MRT beamforming vector and the legitimate channel vector from the transmitter to the intended receiver, respectively.

Precoding is another important technology to achieve different design objectives in physical layer security, which is especially appropriate for multi-stream data transmission or multi-user access. When the intended transceivers are equipped with multiple antennas, the confidential messages of one or multiple users can be spatially multiplexed onto multiple independent subchannels via precoding. By optimizing the precoder, the interested performance metrics of physical layer security can be achieved while the quality of service (QoS) can be guaranteed simultaneously [66]–[71]. The secret dirty-paper coding (S-DPC) has been proposed to achieve the maximum secrecy rate in [72] and [73]. However, the complexity of S-DPC is computationally prohibitive, so that it is difficult to apply this precoding scheme in practice. The complexity of a precoding scheme may be crucial, which affects the application of precoding schemes in practice. In literature, due to the high complexity of the optimal precoding in some scenarios, as alternatives the suboptimal schemes have been developed to reduce computational complexity and facilitate their practical application [66], [67], [69], [70]. As a matter of fact, the linear precoding techniques are also attractive alternatives because of their simplicity [66], [74]. As more simple linear precoding techniques, generalized singular value

decomposition (GSVD) [26], [28], [74]–[77] and regularized channel inversion (RCI) [78]–[82] have been extensively adopted in physical-layer secure transmission. The GSVD is to simultaneously diagonalize the legitimate channels and the wiretap channels, such that a set of parallel independent subchannels is created to transmit the messages of different users [74], [83]. Channel inversion (CI) precoding, sometimes known as zero-forcing (ZF) precoding, is a popular and practical linear precoding scheme which can control inter-user interference by canceling all signals leaked to the unintended users. RCI based on CI has better performance than plain CI by using a regularization parameter. RCI can achieve a tradeoff among signal power, interference, and information leakage [78].

Using AN to deteriorate the quality of the received signals at eavesdroppers is also a good way in physical layer security, which is herein referred to as noise-assisted secure strategies. In such strategies, the transmitted signal is superimposed with AN [30], [42], [45], [62], [83]–[92]. This strategy is also termed as "masked beamforming" in the multi-input single-output multi-eavesdropper (MISOME) wiretap channel [75], "masked precoding" in the multi-input multi-output multi-eavesdropper (MIMOME) wiretap channel in [76], and "AN precoding" in [42]. In order to avoid interfering destination node, the simple but not optimal method is to let the AN lie in the null space of the signal space, i.e., satisfying

$$\mathbf{hz} = 0, \tag{18}$$

where $\mathbf{h}$ and $\mathbf{z}$ denote legitimate channel vector and AN vector, respectively [42], [87]–[89]. Furthermore, the AN can also be optimized globally to achieve the optimal secure performance [30], [62], [83].

C. Antenna/Node Selection and Cooperation

In multi-antenna and multi-node wireless networks, antenna and node selection have been exploited to strengthen transmission reliability, which also have great potential to enhance wireless security [22]. It has been verified that selecting the proper antennas or nodes from the candidate set is a simple but effective way to improve the performance of secure transmission while saving resource. As a result, antenna/node selection and cooperation have been considered and widely investigated in many works.

MIMO technologies are believed to be one of the foremost technologies pertaining to physical layer security. In a MIMO system, transmit antenna selection provides solutions to reduce the hardware complexity resulted from large antenna arrays and radio frequency chains, insertion losses attributed to radio frequency switches, and feedback overhead needed for transceiver communication [93]. In physical layer security, transmit antenna selection as a usual approach to exploit spatial degrees of freedom in multi-antenna scenarios, has been comprehensively investigated for maximizing the secrecy rate [93], improving the SNR of the legitimate channels [94], [95], and enhancing security from the viewpoint of secrecy outage performance [96]–[100].

In multi-user networks, the randomness of users' geographical locations leading to random signal attenuation independently across users, can also be used to enhance secure performance [101]. Accordingly, user selection/scheduling as a promising paradigm can be adopted to utilize the spatial diversity in multi-user networks [22], [102]. In a multi-user network, user selection determines which users should be scheduled for confidential data transmission. Typically, the user with the best channel quality is selected to improve secrecy rate or throughput [103]–[105]. This optimal selection scheme depends on both the legitimate and wiretap channels. Some suboptimal user selection schemes with considering wiretap links are also used due to their low complexity or the unavailability of wiretap CSI [22], [103], [104], [106]. In addition, user selection/scheduling can also be used for saving power with secrecy rate constraints or enabling the largest possible user set with an effective transmission power constraint [107]. In some situations, the legitimate channels to users may experience severe propagation loss and deep fading, and such users may have little chance to be scheduled. Therefore, the fairness of user selection/scheduling needs to be considered. Two competing problems should be balanced herein: achieving the optimal secure QoS while ensuring each user with certain opportunities to access networks [22], [108].

In multi-relay cooperative networks, the distributed relay nodes may provide spatial degrees of freedom which can be exploited to improve secure QoS against the eavesdropping attack. It is well-known that cooperative relaying with relay selection can bring some benefits in terms of rate, EE, and security. More specifically, cooperative relaying combined with relay selection has the potential of maximizing the secrecy capacity [109], maximizing the Shannon capacity to the destination node as well as minimizing that to the eavesdropper [109], [110], reducing the secrecy outage probability [111], [112], maximizing the SNR ratio of the destination node to the eavesdropper [110], [113], or saving the limited power of network nodes [64], [114], [115]. Generally speaking, to strengthen the network security against the eavesdropping attack, three relay selection schemes have been proposed, which are referred to as minimum selection considering only the relay-eavesdropper links, conventional selection considering only the relay-destination links, and the optimal selection taking the both links into account [110], [113]. In literature, some heuristic algorithms have also been proposed for the optimal relay selection with different purposes.

Relay nodes can be used for not only cooperative relaying but also cooperative jamming [10], [11], [116]. Cooperative jamming with jammer selection also has the ability to enhance secrecy of wireless networks. This security-enhanced strategy selects the jammers from trusted or untrusted intermediate nodes to confuse eavesdroppers by transmitting artificial interference signals [117]–[120]. With regard to the untrusted nodes which may be potential eavesdroppers, we should use them discreetly. However, it has been verified in [121] that, seeking for cooperation with the untrusted relay nodes can achieve a higher secrecy rate than just treating them as pure eavesdroppers. In other words, the untrusted relays

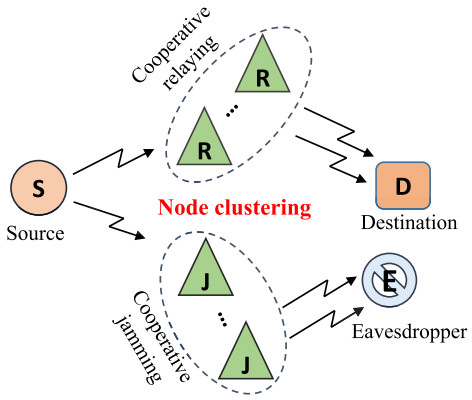


Fig. 5. An illustration of joint relay and jammer selection and cooperation.

can also be used for cooperative relaying while protecting the confidential data from them [29], [52], [122]–[129]. Therefore, no matter whether the relays are trusted or not, they can be used intelligently for cooperative relaying or jamming [129], [130]. Moreover, cooperative jamming with the destination node can also provide secrecy improvements, such as in [40], [127], and [131].

In practice, the joint relay and jammer selection is more effective for improving the secure performance of the whole network than using any single approach. As illustrated in Fig. 5, by using such a joint method, some proper intermediate nodes are selected to operate at a conventional relaying mode for assisting the confidential data transmission between the source node and the destination node. Meanwhile, another set of intermediate nodes are selected as jammers to confuse the potential eavesdropper [132]–[138].

D. Joint Strategies of Several Approaches

The secrecy improvements in physical layer can be supported by secure resource allocation, signal processing, and antenna/node selection and cooperation. Secure resource allocation mainly focuses on resource usage policies by fully using the multidimensional wireless resources involving frequency, timeslot and power. Secure beamforming and precoding belonging to signal processing are to design beamformer and precoder to well exploit the characteristics of multi-antenna and multi-node settings which may form MIMO or virtual MIMO networks. Antenna/node selection and cooperation aim at selecting the proper antennas or nodes from the candidate set to improve the performance of secure transmission. All of the foregoing strategies can be carried out to strengthen information security while achieving the requirements of performance metrics and resource savings. In other words, based on the ideas of these fundamental security strategies, we can design some different transmission schemes to achieve the specific requirements of network performance subject to secrecy and resource constraints.

In order to achieve better performance of physical layer security, any single approach mentioned above might not be sufficient. Therefore, the joint strategies based on some of the above approaches may be preferable in practical applications. As in [36], [139], and [140], joint resource allocation and user scheduling have been proposed to enhance physical layer security in OFDMA networks. Antenna selection combined with beamforming/precoding has been demonstrated to be effective in secure MIMO system designs [93], [95], [141]. Distributed beamforming with relay/jammer selection has been exploited in cooperative networks [142]–[144]. Additionally, other joint strategies have also been addressed for some specific scenarios to obtain secrecy improvements, such as cooperative beamforming and user selection in [106] and [145], jamming-aided beamforming/precoding in [63], [84], [85], [91], and [146]–[148], joint power allocation and beamforming/precoding in [77] and [149]–[151], etc.

IV. Performance Metrics and Basic Optimization Problems in Physical Layer Security

For the secure transmission designs, the choice of performance metrics is remarkably critical. In physical layer security designs, there are several problems usually being raised from different performance requirements:

1) The transmission effectiveness of secure transmission strategies, that is evaluated by the achievable secrecy rate/capacity.
2) The reliability of secure transmission strategies, which is measured by secrecy outage probability/capacity.
3) The power cost of secure transmission strategies, that is the minimum power consumption needed for ensuring the secure QoS.
4) The EE of secure transmission strategies, which focuses on the amount of secret bits transferred with unit energy or the energy consumption required for sending one secret bit.

To investigate these problems listed above, the corresponding metrics termed as secrecy rate/capacity, secrecy outage probability/capacity, power consumption, and secure EE, are usually adopted in system designs to evaluate the achievable performance of the proposed secure transmission strategies. More specifically, these performance metrics are usually taken as the optimization objectives for system designs in different application scenarios.

A. Secrecy Rate/Capacity

Being similar to the data rate in conventional communications, the secrecy rate is a fundamental metric to assess the transmission effectiveness of physical-layer secure strategies. In physical layer security, the secrecy rate is defined as the secret bits transmitted on the given channel per second, which heavily depends on channel inputs. To evaluate the secrecy more conveniently and computation affordably, the Gaussian inputs as well as the achievable secrecy rate are usually adopted in many works [12]. The achievable secrecy rate can be described as the difference between the achievable data rate of the legitimate channel and the wiretap channel with the Gaussian codebook, which is expressed as

$$R_s = [R_m - R_e]^+, \tag{19}$$

where $[x]^+ \triangleq \max\{0, x\}$. R_m denotes the data rate of the legitimate channel from the source node to the destination node. R_e denotes the data rate of the wiretap channel from the source node to the eavesdropper. Clearly, the achievable secrecy rate is a lower bound of the secrecy capacity [12]. In practical designs, by some approaches as secure beamforming or resource allocation, a non-zero secrecy rate can be obtained since the wiretap channel is intentionally degraded while improving the quality of legitimate channel.

Another metric closely related to secrecy rate is secrecy capacity, which is defined as the upper bound of the secrecy rate [3], [152]. More specifically, the secrecy capacity is the maximum secrecy rate by which the confidential messages of the source node can be securely and reliably transmitted to the destination node whereas the unauthenticated users cannot obtain any useful information in this process. In Wyner's pioneering work [5], the secrecy capacity of a degraded wiretap channel has been given by

$$C_s = \sup_{p(X)} \{I(X; Y) - I(X; Z)\}, \tag{20}$$

where *X* denotes the channel inputs at source node. *Y* and *Z* denote the channel outputs at the destination node and eavesdropper, respectively. $I(\cdot;\cdot)$ represents the mutual information. The secrecy capacity shown in (20) can be achieved by choosing the optimal input probability distribution *p*(*X*). For any distribution *p*(*X*), the corresponding *X*, *Y*, and *Z* form a Markov chain [3], [152].

Based on Wyner's results, Csiszár and Körner investigated a more general (non-degraded) wiretap channel and derived its secrecy capacity as [6]

$$C_s = \sup_{p(V,X)} \{I(V; Y) - I(V; Z)\}, \tag{21}$$

where *V* is an auxiliary input variable. By introducing appropriate random variable *V*, the maximization in (21) can be implemented over all joint probability distributions *p*(*V*, *X*) while forming a Markov chain $V \rightarrow X \rightarrow (Y, Z)$. As to the familiar Gaussian channel, the secrecy capacity has been derived in [7] as following:

$$C_s = C_m - C_e, \tag{22}$$

where C_m and C_e denote the Shannon capacities of the legitimate and wiretap channels, respectively.

The aforementioned secrecy rate and secrecy capacity have been investigated without considering the fading of wireless channels. However, fading of wireless channels is an inevitable issue in many situations, as stated in [152] in which three standard fading models as well as the corresponding ergodic secrecy rate/capacity have been well discussed, including the ergodic-fading model, block-fading model, and quasi-static fading model. When the channel fading is taken into consideration, the average capability of secure communication over fading channels should be evaluated, and the ergodic secrecy rate or secrecy capacity is then a quite suitable metric for this case [12], [153]. In practice, since achieving ergodic secrecy capacity may be computationally difficult in many situations, the achievable ergodic secrecy rate is therefore adopted to measure the secrecy performance in fading scenarios. The achievable ergodic secrecy rate is defined as the difference between the ergodic rates of the legitimate and wiretap channels with Gaussian codebooks, which is more computationally efficient in many cases. As the lower bound of ergodic secrecy capacity, the achievable ergodic secrecy rate has usually been taken as the optimization objective in secure transmission designs with the consideration of channel fading [12].

Towards secure communication system designs, the primary concern is how much the secrecy rate can be achieved for delivering the confidential data securely and reliably. This problem can be modeled as maximization of the achievable secrecy rate, that is to maximize the achievable secrecy rate as much as possible by using some physical-layer technologies such as resource allocation, beamforming/precoding, cooperative diversity, or other optimization algorithms. To maximize the achievable secrecy rate, the most important factor is the power limitation in addition to the bandwidth. Accordingly, one common formulation of achievable secrecy rate maximization on the given channels generally aims at maximizing the secrecy rate under the constraints of the maximum allowed power. For instance, the achievable secrecy rate maximization in a relay network can be modeled as

$$\begin{aligned} \max_{P_t^{(S)}, P_t^{(j)}, j\in\Omega} \quad & R_s\left(P_t^{(S)}, P_t^{(j)}\right) \\ \text{s.t.} \quad & P_t^{(S)} + \sum_{j\in\Omega} P_t^{(j)} \le P_{max}^{sum}, \\ & \text{or} \begin{cases} 0 \le P_t^{(S)} \le P_{max}^{(S)}, \\ 0 \le P_t^{(j)} \le P_{max}^{(j)}, j \in \Omega, \end{cases} \end{aligned} \tag{23}$$

where P_{sum}^{max} denotes the maximum sum transmission power of all nodes in the relay network, and $P_{max}^{(S)}$ and $P_{max}^{(j)}$ denote the maximum transmission power of the source and the *j*th relay nodes, respectively. In existing literature, there are two kinds of power constraints in the problem of secrecy rate maximization. One is the sum power constraints of all nodes specified by the constraint $P_t^{(S)} + \sum_{j\in\Omega} P_t^{(j)} \le P_{max}^{sum}$ in (23), and the other is the individual power constraint of each node specified by the constraints $0 \le P_t^{(S)} \le P_{max}^{(S)}$ and $0 \le P_t^{(j)} \le P_{max}^{(j)}, j \in \Omega$ in (23). Noteworthily, beamforming may be more effective for maximizing secrecy rate by strengthening signals on a desired direction and suppressing/eliminating signals on undesired directions. When beamforming is considered in such a relay network, the weight vector of all relays will be introduced to replace power, as investigated in [59] and [154]. The maximization of the achievable secrecy rate has been comprehensively investigated in many scenarios, for example multicarrier systems, multi-antenna systems, multi-node cooperative systems, etc.

B. Secrecy Outage Probability/Capacity

Due to the channel fading and imperfect CSI, secure transmission may be broken. Therefore, it is of particular interest to explore the secrecy outage behaviour of a secure transmission strategy [153], [155]. Then, the secrecy outage probability is an appropriate metric to characterize the probability that secure

transmission cannot be achieved. Precisely, the secrecy outage probability is defined as the probability that a secrecy outage event happens.

There are two different definitions of secrecy outage events. The more popular one is that the secrecy outage happens when the instantaneous secrecy capacity C_s drops below a target secrecy rate R_s^0, i.e., $\{C_s < R_s^0\}$ [40], [155]–[159]. In other words, the target secrecy rate is too high to be supported by the current channel state, and the information security is compromised. The secrecy outage probability of this definition is given by

$$p_{out}\Big(R_s^0\Big) = \Pr\Big\{C_s < R_s^0\Big\}. \tag{24}$$

In (24), the outage events $\{C_s < R_s^0\}$ happen whenever the intended receiver does not receive the secret messages reliably (i.e., the message cannot be decoded correctly by intended receivers) or the message transmission is not perfectly secure (i.e., some information may leak to eavesdroppers) [160], [161]. However, this definition does not distinguish between reliability and security. As a result, an outage based on this definition does not necessarily imply a failure in achieving perfect secrecy. To be specific, the outage events $\{C_m < R_s^0\}$ mean that the secrecy rate cannot be supported by the legitimate channels and the secure transmission would be certainly suspended. Clearly, these suspension events fall within the outage events $\{C_s < R_s^0\}$ due to $C_m < R_s^0$ implying $C_s < R_s^0$, but it is clearly not a failure in achieving perfect secrecy [161]. Then, the outage probability in secure transmissions can be more explicitly expressed as [33]

$$p_{out}\Big(R_m^0, R_s^0\Big) = 1 - \Pr\Big\{C_m \geq R_m^0, C_s \geq R_s^0\Big\}, \tag{25}$$

where R_m^0 is the target coding rate of the confidential message, $R_s^0 \leq R_m^0$. The outage events $\{C_m < R_m^0\}$ imply the legitimate channels cannot support the coding rate R_m^0. Consequently, at a target secrecy rate R_s^0 and a target coding rate R_m^0, the reliable and secure transmission can only be ensured at a probability $1 - p_{out}(R_m^0, R_s^0)$.

The other definition of secrecy outage is proposed in [161], which directly measures the probability that a transmitted message fails to achieve perfect secrecy. In [161], considering the Wyner's encoding scheme [5], the rate difference $R_e \triangleq R_m - R_s$ is defined to reflect the cost of securing message transmission against eavesdropping, where R_m and R_s, respectively, denote two rates chosen by secure encoder, namely, the rate of the transmitted codewords and the rate of the confidential information. The transmitted messages can be decoded correctly if $R_m < C_m$, whereas it fails to achieve perfect secrecy if $R_e < C_e$. Hence, the secrecy outage probability is defined in [161] as

$$p_{out}(C_e) = \Pr\{R_m - R_s < C_e | \text{message transmission}\}, \tag{26}$$

which is a probability conditioned upon a message actually being transmitted. If the source transmitter has no knowledge about the instantaneous CSI of the legitimate channel, the transmission may always occur, so that the secrecy outage probability in (26) then reduces to the unconditional probability $\Pr\{R_m - R_s < C_e\}$. More generally, when the instantaneous CSI of legitimate channel is available, the source transmitter can decide whether or not to transmit with possibly variable rates according to channel conditions. Therefore, it is possible to reduce the secrecy outage probability by carefully designing the rate of the transmitted codewords R_m, the rate of the confidential information R_s, and the condition for transmission [161].

Another important concept related to the secrecy outage probability is the secrecy outage capacity $C_{out}(\epsilon)$, which is defined as the largest secrecy rate that can be supported under a tolerable secrecy outage probability ϵ [12], [157], [162], [163]. In other words, the secrecy outage capacity is the maximum achievable secrecy rate such that the secrecy outage probability is less than ϵ, i.e.,

$$p_{out}(C_{out}(\epsilon)) = \Pr\{C_s < C_{out}(\epsilon)\} = \epsilon. \tag{27}$$

The practical significance of secrecy outage probability/capacity is that these definitions provide outage formulations which give a more explicit measure of the security level. From the system design perspective, it is meaningful to evaluate the secrecy outage behaviour of the proposed transmission scheme [161].

For the optimization design in physical layer security, the reliability of secure transmission which is generally measured by secrecy outage probability has also attracted increasing concerns. Ideally, the secure communication should be implemented without outage. Motivated by this observation, we expect to reduce the secrecy outage probability with the best effort. This raises the optimization problem of secrecy outage probability minimization subject to resource constraints. Taking the relay network as an example, the minimization of the secrecy outage probability can be roughly formulated as

$$\begin{aligned} \min_{P_t^{(S)}, P_t^{(j)}, j\in\Omega} \quad & p_{out}\Big(R_s^0\Big) \\ \text{s.t.} \quad & \begin{cases} 0 \leq P_t^{(S)} \leq P_{max}^{(S)}, \\ 0 \leq P_t^{(j)} \leq P_{max}^{(j)}, j \in \Omega. \end{cases} \end{aligned} \tag{28}$$

In (28), the peak power of each transmission node is taken into account to limit the excessive high power consumption resulted from the improvement of the secrecy rate in minimizing secrecy outage probability.

C. Power/Energy Consumption

Power/energy consumption is a key consideration in resource-limited scenarios such as battery-dependent networks. In general, the sustainability of secure communications in such networks is the most important concern. Therefore, to reduce energy consumption and prolong network lifetime, power/energy cost is one primary metric considered in physical layer security designs.

Before designing a secure transmission scheme with limited power and energy, we first analyse the factors of power consumption in wireless networks [163]. According to [164], the total power consumption along the signal path can be divided into two main components: the power consumption of all the power amplifiers P_a and the power consumption of all other

circuit blocks P_c. The power consumption of all power amplifiers heavily depends on the output power of power amplifiers P_t, i.e.,

$$P_a = P_t/\eta, \tag{29}$$

where η is the efficiency of power amplifier. The other circuit blocks include the basic circuits at the transmitter and receiver excluding power amplifiers, such as active filter, frequency synthesizer, mixer, intermediate frequency amplifier, analog-to-digital or digital-to-analog converter, and so on [163], [164]. Accordingly, the power consumption of all other circuit blocks P_c can be roughly expressed as [164], [165]

$$P_c = N_t P_{ct} + N_r P_{cr} + P_{c0}, \tag{30}$$

where N_t and N_r denote the numbers of transmitter antennas and receiver antennas, respectively. P_{ct} and P_{cr} denote the power consumed by the basic circuits at each transmit and receive chain, respectively. P_{c0} denotes the power consumed by baseband circuits such as digital signal processing circuits. It can be seen that P_{ct}, P_{cr}, and P_{c0} are independent of the secrecy rate. As a result, the total power consumption of a system can be given by

$$\begin{aligned} P &= P_a + P_c \\ &= P_t/\eta + N_t P_{ct} + N_r P_{cr} + P_{c0}. \end{aligned} \tag{31}$$

The power consumption of a wireless communication system can be usually formulated as (31). However, in a practical scenario, there may be some variations in the power consumption model. For example, in a cooperative relay network, the power consumption model can be expressed as

$$P = \frac{1}{2\eta}\left(P_t^{(S)} + \sum_{j\in\Omega} P_t^{(j)}\right) + P_c^{(S)} + \sum_{j\in\Omega} P_c^{(j)}, \tag{32}$$

where, Ω is the set composed of relay nodes and *j* denotes the *j*th relay node. $P_t^{(S)}$ and $P_t^{(j)}$ denote the transmission power of the source node and the *j*th relay node, respectively. $P_c^{(S)}$ and $P_c^{(j)}$, respectively, denote the power of the basic circuit blocks at the source node and the *j*th relay node, which can be obtained by (30). The factor $\frac{1}{2}$ lies in the fact that the transmission is completed in two stages due to half duplex.

The resource-limited regime motivates us to develop the power-efficient transmission strategies which aim at minimizing power consumption [114], [166], [167]. For this purpose, the power level of transmitters should be adjusted to save transmission power while satisfying the target QoS requirements. It is worth noting that, although relay cooperation has the potential of transmission effectiveness, reliability, and security, relay nodes may consume additional power, such as the basic circuit power which is inherent in relay cooperation and unrelated with secrecy rate. Therefore, from the viewpoint of transmission designs, the power adaptation and relay selection should be performed jointly to achieve the requirements of power-efficient secure transmission.

It is noteworthy that a higher transmission rate of messages can be achieved if no secrecy constraint is imposed. When secrecy is considered, the transmission rate of confidential messages will decrease due to secure coding. Hence, higher power consumption is needed to ensure a higher level of secrecy at the physical layer [168].

For secure transmission designs in power-limited scenarios, such as the transmission nodes powered by batteries or energy harvesting devices [169], we should give priority to saving power and prolonging communication durations. These observations motivate us to design secure transmission schemes focusing on the minimization problem of power cost. In general, power minimization means consuming the minimum power to achieve the fundamental demand of secure transmission such as the minimum target secrecy rate [53], [59], [114], [154], the required SNR threshold of destination node [91], [170], the given probability of secrecy [86], or other performance requirements. For example, in a relay network, the basic formulation of power minimization can be expressed as

$$\begin{aligned} \min_{P_t^{(S)}, P_t^{(j)}, j\in\Omega} \quad & P = \frac{1}{2\eta}\left(P_t^{(S)} + \sum_{j\in\Omega} P_t^{(j)}\right) + P_c^{(S)} \\ & \quad + \sum_{j\in\Omega} P_c^{(j)} \\ \text{s.t.} \quad & R_s \geq R_s^0. \end{aligned} \tag{33}$$

The formulation in (33) is only a rough model, which can be specified in practical applications. For instance, when the beamforming is performed for minimizing the power consumption, the total power is then determined by the weights of beamformer [59], [154], [171].

D. Secure EE

In the conventional communications without secrecy constraints, the utilized efficiency of system energy referred to as EE is an important metric for green transmission strategy designs. When the security threats and energy limitations are considered jointly in wireless networks, it is significant to design energy-efficient secure transmission strategies which should operate in a confidential and green manner. Therefore, from the perspective of green physical layer security, an appropriate metric for assessing the utilized efficiency of system energy is also of primary importance. In general, the utilized efficiency of system energy can be measured by different metrics from different viewpoints, such as the viewpoints from the component level, equipment level, and system/network level. Towards the EE of system/network level, it aims at measuring both the energy consumed by all communication nodes and the performance experienced at the network level (i.e., capacity, security, coverage, etc.). The EE of system/network level is popular in transmission strategy designs.

There are two main metrics which have been defined for evaluating the EE of novel techniques towards physical layer security. One metric is the secure EE [64], [115], [172], which is defined as the amount of secret bits transmitted with unit energy consumption. Designing energy-efficient secure transmission strategies with this metric, it is expected to maximize the secure EE. The resulting effect is that as much confidential

information as possible is transmitted with a given amount of energy. Hence, given the amount of energy ΔE consumed in a duration ΔT, the secure EE can be defined as

$$E_B = \frac{R_s \Delta T}{\Delta E} = \frac{R_s}{P}(\text{bits/Joule}). \tag{34}$$

The metric of secure EE is in fact the ratio of secrecy rate to total power consumption, which has been frequently used in literature for investigating the EE of physical-layer secure communications [64], [71], [115], [172], [173]. This metric is also termed as "secret bits per Joule", since its unit is bits/Joule.

Another metric proposed to assess the EE of physical-layer secure transmissions is the energy per secret bit, which is suitable for evaluating the minimum energy required to send one secret bit (i.e., minimum bit energy required for reliable communications under secrecy constraints). The precise formula of this metric is the ratio of total power consumption to secrecy rate [174], [175], i.e.,

$$E_J = \frac{P}{R_s}(\text{Joules/bit}). \tag{35}$$

Noteworthily, these two metrics of secure EE are reciprocal to each other. The resulting optimization problem by using one metric is in general the dual problem of that by using the other metric. Which metric is better in practice should fully consider the practical scenarios, for reducing the difficulties of secure transmission designs. As stated in [176], the metric of secret bits per Joule is more popular since it is convenient to capture the degree of proportionality between the energy consumption and different levels of load. This metric can reflect dynamic network conditions considering energy consumption and secrecy constraints in different situations of load. However, the metric of energy per secret bit is suitable to assess the network EE only at a nonzero secrecy rate.

In addition, it is obvious that the metrics of secure EE are closely related to the model of the power consumption. The traditional energy-efficient technologies only consider the transmission power, but which is not the only part of power consumption in a networks. A holistic and system-wide power model is imperative [177]. Therefore, the secure EE should be formulated with all power consumption including transmission power, basic circuit power, and signaling overhead in the entire network [177].

In physical layer security, more power and energy, compared with the conventional communication without secrecy requirement, may be consumed to protect confidential information against eavesdropping. This observation can be verified by the secrecy rate function shown in (19) where the information rate leaking to the eavesdropper generates extra consumption of power and energy. This fact may increase the burden of power and energy supplies, in particular in the scenarios with limited power and energy. When the limited power and energy become the main factors for securing communications, the first concern, impelled by the requirements of "green communication", is to deliver confidential information with high secure EE as much as possible. This motivation raises the maximization of the secure EE in physical layer security. Also taking the relay network as an instance, the mathematical formulation of secure EE maximization can be roughly modeled as

$$\max_{P_t^{(S)}, P_t^{(j)}, j\in\Omega} \left\{ E_B = \frac{R_s}{P} \right\}$$
$$\text{s.t.} \quad \begin{cases} 0 \le P_t^{(S)} \le P_{max}^{(S)}, \\ 0 \le P_t^{(j)} \le P_{max}^{(j)}, j \in \Omega, \\ R_s \ge R_s^0. \end{cases} \tag{36}$$

It is worth noting that the secure EE maximization should ensure the secure QoS requirement which is specified by the constraint $R_s \ge R_s^0$ in (36). Here, R_s^0 is used to avoid achieving high secure EE but with too low secrecy rate. In [51] and [178], R_s^0 can be adjusted to balance the system performance between secure EE and secrecy rate.

It is pointed out that the aforementioned metrics and optimization problems are all based on information-theoretic security, since those metrics and problems are intertwined with the secrecy rate/capacity which is based on information theory. According to [179], another type of performance metrics for secrecy is based on practical measures where the secrecy level is quantified by the metrics that can be observed in practical communication scenarios, such as secrecy gap which is usually characterized by bit error rate or packet error rate versus SNR. To be specific, secrecy gap reflects the minimum required difference between the SNR of legitimate receiver and eavesdropper for which secure communication is possible [179], [180]. This metric has also been used to make a quantitative measure for system designs, for instance in [180]–[182].

V. The State of the Art of Optimization and Design in Physical Layer Security

In the previous section, we discussed the performance metrics and fundamental optimization problems in physical layer security. Each research topic of physical-layer security designs investigated in Section III involves extending these fundamental optimization problems to practical scenarios according to specific application conditions and solving the resulting optimization problems to achieve the required performance metrics. In this section, the state of the art of optimization and design in physical layer security will be summarized from the perspectives of the aforementioned research topics in physical-layer security designs. Each research topic will be presented from four categories of fundamental optimization problems including maximization of achievable secrecy rate, minimization of secrecy outrage probability, minimization of power consumption, and maximization of secure EE.

A. Secure Resource Allocation

As a promising way for improving the performance requirements of physical layer security, secure resource allocation has been extensively investigated for different purposes. As discussed above, the designs of secure resource allocation are usually performed by solving four optimization problems which are related with the corresponding performance metrics.

1) Maximization of Achievable Secrecy Rate: Many works focus on designing secure resource allocation strategies to improve achievable secrecy rate. A conventional approach towards maximizing secrecy rate in multicarrier systems is to globally allocate the limited power and subcarriers for all transmission nodes. This goal usually leads to a mixed integral programming in many scenarios, which has been investigated in many works [34], [35], [38], [49], [50], [183]. Such as in [34], the resource allocation for a secure multicarrier AF relay communication system is investigated, in which decision variables $\mu_{si} \in \{0,1\}$ and $\mu_{ri} \in \{0,1\}$ are defined for the source and the relay, respectively, for specifying the state of communication on a carrier *i*. More specifically, if $\mu_{si} = 1$ and $\mu_{ri} = 1$ then both the source and the relay transmit in respective slots, while if $\mu_{si} = 1$ and $\mu_{ri} = 0$ then only the source transmits in its slot and it remains silent with the relay in the second slot. The case $\mu_{si} = 0$ and $\mu_{ri} = 0$ indicates no communication in both the slots and the case $\mu_{si} = 0$ and $\mu_{ri} = 1$ has no significance. Then, the resource allocation strategy for maximizing secrecy capacity in such a relay-aided multicarrier system can be derived by solving the typical mixed integral programming

$$\max_{P_{si},P_{ri},\mu_{si},\mu_{ri}} \quad \sum_i C_i(P_{si},P_{ri},\mu_{si},\mu_{ri})$$
$$\text{s.t.} \quad \begin{cases} \sum_i \mu_{si}(P_{si}+\mu_{ri}P_{ri}) \le P_{sum}^{max} \\ P_{si} \ge 0, P_{ri} \ge 0 \\ \mu_{si} \in \{0,1\}, \mu_{ri} \in \{0,1\}, \end{cases} \tag{37}$$

where P_{si}, P_{ri}, and C_i denote the source power, the relay power, and the secrecy capacity on carrier *i*, respectively.

Other specific formulations towards different scenarios have also been explored in this areas. In [35], a secure resource allocation policy is addressed for a downlink OFDMA-based network with the coexistence of secure users and normal users which have no confidential messages and do not care about security issues. In [38], the transmission modes referred to as no communication, direct communication, and relay communication are determined adaptively by subcarrier allocation while the optimal source and relay power allocation policy over all subcarriers is addressed to maximize the sum secrecy rate under a total power constraint. Jamming and AN-aided resource allocation for sum secrecy rate maximization is, respectively, studied in [49] and [183], where the former focuses on the OFDMA-based two-way relay wireless sensor networks while the latter focuses on the OFDMA systems with joint secrecy information and power transfer. For considering the fairness of resource allocation in secure multiuser OFDMA downlink works, the work presented in [50] aims to assign subchannels and allocate power to optimize the max-min fairness criterion over the users' secrecy rate. Besides, robust secure resource allocation in relay-assisted cognitive radio networks is investigated in [184] considering the uncertainty of CSI.

To solve the problems of secure resource allocation mentioned above, the approach of dual decomposition is usually adopted in many foregoing works. The basic idea of dual decomposition can be summarized as: 1) constructing a Lagrangian dual problem associated with the original problem

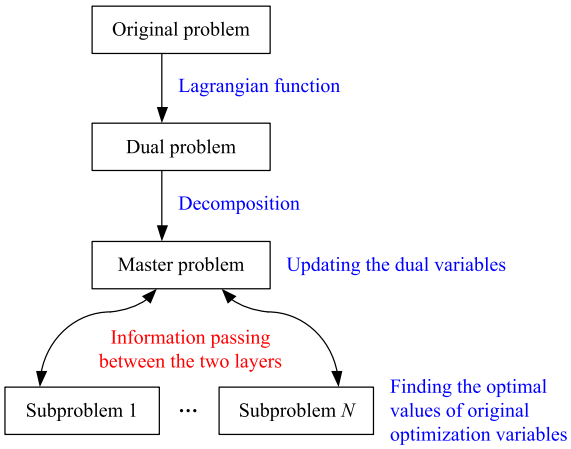


Fig. 6. Dual decomposition approach for secure resource allocation.

by transforming the constraints into the objective function in the form of a weighted sum, and 2) decomposing the Lagrangian dual problem into distributed subproblems which are then coordinated with a high-level master problem by iterative alternating optimization between the two levels [185], as illustrated in Fig. 6. Based on dual decomposition, the resource allocation in some secure scenarios can be solved by different distributed algorithms which are efficient for computing in many cases.

2) Minimization of Secrecy Outage Probability: Secure resource allocation is also an effective approach for minimizing secrecy outage probability. Considering a typical secure OFDMA downlink system in [33], the outage-optimal subcarrier allocation is addressed to minimize the secrecy outage probability p_{out}^m of each user *m* while guaranteeing that each user has the identical probability to access each subcarrier *n*. The formulation of the problem is summarized as

$$\min \quad \{p_{out}^m\}_{\forall m}$$
$$\text{s.t.} \quad \begin{cases} \sum_{\forall m} \mu_{mn} \le 1 \\ \sum_{\forall n} \mu_{mn} \le 1 \\ \mu_{mn} \in \{0,1\}, \end{cases} \tag{38}$$

where μ_{mn} are the decision variables with $\mu_{mn} = 1$ meaning that subcarrier *n* is assigned to user *m*. Otherwise, $\mu_{mn} = 0$. The constraints $\sum_{\forall m} \mu_{mn} \le 1$ and $\sum_{\forall n} \mu_{mn} \le 1$ imply that each subcarrier can only be assigned to no more than one user with identical probability. It is noted that, to deal with the difficulty of such a probabilistic integral programming, a random bipartite graph approach is proposed with a logarithm-polynomial complexity when applying parallel implementations. A more complicated formulation of probabilistic mixed integral programming is investigated in [186] to minimize the secrecy outage probability of a wireless systems with adaptive transmission rates and secrecy rates, in which a stochastic network optimization framework is introduced to overcome the difficulty of such a problem.

The outage-optimal power allocation is also explored extensively. By deriving explicit expressions of the secrecy outage probability, the closed-form solutions of the optimal power

allocation are obtained to achieve high outage performance in an AF relay network with destination-assisted jamming [40], an AN-aided secure multi-antenna transmission coexisting with randomly distributed eavesdroppers [45], [187], and a MISO system with a multi-antenna eavesdropper [90], respectively.

The minimization of the secrecy outage probability is also raised in the scenarios of secure wireless information and power transfer in [188]–[190]. In [188], the transmission power allocation and power splitting ratio for AN signal are jointly optimized to minimize the outage probability for delay-limited secrecy information transmission based on the approaches of dual decomposition and alternating optimization. In [189], the minimum secrecy outage probability is achieved by optimizing the optimal placement of energy harvesting node with physical layer security considerations. In [190], the secrecy outage probability minimization problem and the average harvested energy maximization problem in wireless information and power transfer systems are solved by an optimization framework of target secrecy rate and power allocation ratio.

It is worth noting that the minimization of the secrecy outage probability is dual to the maximization of the secrecy outage capacity which is another optimization design related to secrecy outage performance. As in [36], the packet data rate, secrecy data rate, power, and subcarrier allocation policies of an OFDMA DF relay network are designed to maximize the average secrecy outage capacity by the dual decomposition and gradient method. In [191], the solutions of the optimal relay power allocations for a massive MIMO DF relay network are derived for maximizing the secrecy outage capacity and minimizing the interception probability, respectively. The results in [191] are expanded in [48], in which to cope with the nonconvexity of the joint node power and transmission time allocation problem, the approach of alternating optimization is addressed by maximizing over some of the variables and then maximizing over the rest.

3) Minimization of Power Consumption: The power consumption of physical-layer secure communications can also be decreased by the designs of secure resource allocation strategies. To be specific, by optimal resource allocation, we can consume as less power as possible to achieve different requirements of secure QoS, as shown in Table IV. The use of AN or jamming signals can deteriorate the wiretap channel, but it also increases the total power consumption. Therefore, the optimal power allocation between the desired information and AN/jamming signals is very important for saving power. In a MISO system in [86], the optimal power allocation between transmitted information and AN is developed for minimizing the transmission power while ensuring a given probability of secrecy. In [192] where a multiuser MISO network with friendly jamming is considered, the power allocation strategy is optimized to minimize the total power allocated to the information signals and jamming signals while maintaining secure QoS requirements. A non-orthogonal multiple access system is considered in [193] where a closed-form solution is derived to minimize the transmission power. Additionally, considering the application scenario where an user communicates simultaneously with a macro base station and a small-cell access point, a joint optimization of traffic scheduling and power allocation problem is formulated in [194] with the objective of minimizing the total power consumption while meeting both the user's traffic demand and secrecy requirement.

4) Maximization of Secure EE: Secure resource allocation is also effectively used for improving the EE of physical-layer secure communications. To the best of our knowledge, the concept of secrecy capacity per unit cost is defined in [195] to study the cost-efficient wide-band secrecy communications, in which the cost of the secrecy capacity may be the number of channel use, the duration of transmission, or the amount of energy consumption. The research status of secure EE maximization by resource allocation can be summarized from the following aspects.

- Multiuser multiple-access networks: The secure EE maximization of an OFDMA downlink network is studied in [51] where the power, secrecy data rate, and subcarrier allocation policies are optimized based on fractional programming and dual decomposition. In a time-division multiple-access network considered in [196], the secure EE measured by the average energy consumption of the system per transmitted information bit is investigated by using Markov decision process and cross layer design techniques, where information flow and joint optimization of higher and physical layer is permitted. To tackle the problem in [196], the strategies of packet scheduling and transmitter buffering are designed while the heuristic algorithm of simulated annealing is used to solve the optimization problem due to its advantage to help avoiding local minima.
- Multi-antenna networks: The energy-efficient resource allocation is carried out in multi-antenna networks in [197] with different CSI scenarios involving perfect CSI, partial CSI, and statical CSI. The work is expanded in [198] by using the strategy of AN, while the fractional programming and the sequential convex optimization tool are introduced to tackle the nonconvex problem. In [199], based on the optimization framework of [197] and [198], two EE metrics are optimized, namely the metric of secret bits per Joule and the metric of secret-key EE which is defined as the ratio between the system secret-key capacity and the consumed power. In particular in [163], [173], and [200], the optimization problems of energy-efficient secure communications are formulated by using an specific secure EE metric which is therein defined as the ratio of the secrecy outage capacity to the total power consumption.
- Relay networks: In [64], [115], and [172], the energy-efficient power allocation is developed for DF, AF, and untrusted two-way relay networks, respectively. To deal with the nonconvexity of the problems, several optimization approaches are jointly applied, which involve fractional programming, penalty function method, alternating optimization, DC programming. The EE of repetition coding and parallel coding relaying under the partial secrecy regime is investigated by power allocation

TABLE IV
THE COMPARISON OF POWER-EFFICIENT RESOURCE ALLOCATION IN DIFFERENT SCENARIOS

Scenarios	Wireless resources	Assumptions of CSI	Secure QoS constraints	Solutions
MISO networks with AN [86]	The total power for secrecy information and AN	Perfect CSI of legitimate channel and unknown CSI of eavesdropper	Received SNR at destination and a given probability of secrecy	A closed-form solution
Multiuser MISO networks with jamming [192]	The total power for secrecy information and jamming signals	Perfect CSI of all channels	Target secrecy rate	Numerical analyses based on a line search method
A non-orthogonal multiple access system with multiple users [193]	Decoding order, transmission rates, and power	Instantaneous channel gains of all users and the average channel gain of the eavesdropper	Target secrecy rate and secrecy outage probability	A closed-form solution by problem simplification
Traffic offloading via a dual-connectivity in cellular networks [194]	Data rate and transmission power	Perfect CSI of legitimate channel and statistics CSI of eavesdropper	Traffic demand and secrecy outage requirement	Performing a series of equivalent transformations and proposing an efficient algorithm to compute the optimal offloading solution

in [201] based on the fractional programming and a golden section search algorithm.

- Cognitive radio networks: To implement the energy-efficient secure communications in cognitive radio networks in [202], the optimal power allocation and power splitting at the secondary transmitter are optimized under secrecy constraints, while an EE Stackelberg game between the primary and secondary transmitters is formulated for maximizing their utilities. In [203], the medium access probability and transmission power of secondary transmitters are jointly optimized to maximize the secure EE of the secondary network. In [204], a secure EE maximization problem is established under the constraints of data rate and transmission power of the cognitive transmission as well as the interference limitation to the primary user, which is solved based on the fractional programming, penalty function method, and DC programming.
- The tradeoff between energy and secrecy: The tradeoff between energy and secrecy also attracts many concerns recently [175], [205]–[207]. In [175] and [205], the tradeoff between energy and secrecy is explored from an information-theoretic perspective, while the metric of partial secrecy is proposed to characterize the secrecy level of a communication system by looking jointly at the application layer metric and physical layer secrecy metric. In [206], a framework is developed to study the spectrum efficiency (SE) and EE for secure transmission in underlaid random cognitive radio networks, and the joint secure SE and EE optimization problem is formulated therein by using an unified secure SE-EE tradeoff metric. The energy-efficient secure communication in large-scale device-to-device underlaid cellular networks is investigated in [207], in which a link adaptation scheme is proposed to strike a balance between secure EE and SE by maximizing the weighted product of secure EE and SE.

It is observed that, the most of the secure EE maximization formulations are nonconvex, so that they are very intractable in practice. Therefore, some nonconvex optimization methods are introduced to cope with the challenges, such as the fractional programming, penalty function method, alternating optimization, DC programming, etc. To be specific, the fractional programming can transform the secure EE function (which is a fractional function) into a parameterized polynomial subtractive form which can be tackled by the Dinkelbach algorithm. The penalty function method is able to eliminate the nonconvex constraint of secrecy rate by incorporating the constraint into the objective function. In some cases, the optimization problem is nonconvex or unsolvable for all variables, but it is tractable when we tackle the problem with some of the variables and then tackle it with the rest. Such characteristics are beneficial to implement alternating optimization. Towards the optimization problem in which the objective function can be reformulated as a difference of two convex functions, the DC programming is an effective method which solves the problem iteratively by solving a series of convex subproblems. The explanations of these optimization methods can be found in Table V.

B. Secure Beamforming and Precoding

The deployments of multiple antennas or nodes in wireless networks facilitate the technologies of MIMO or virtual MIMO to be applied extensively, which provide abundant opportunities to perform secure beamforming and precoding [8], [9], [12], [22]. It has been demonstrated that, by beamforming and precoding in multi-antenna and multi-node cooperative networks, we can obtain some benefits in terms of secrecy rate, secrecy outage probability, power consumption, and secure EE. Naturally, to gain these benefits, the optimization designs on beamforming and precoding can be solved with the four performance metrics in practice.

1) Maximization of Achievable Secrecy Rate: Following the extensive applications of multi-antenna technologies, secure beamforming and precoding have been paid increasing concerns for secrecy rate improvements [9]. It is verified in [216] that exploiting space-time diversity at a multi-antenna transmitter can enhance information security and information-hiding capabilities. After that, to improve the secrecy rate of multi-antenna networks, some optimal or suboptimal schemes of secure beamforming/precoding have been proposed for multifarious scenarios based on different methods.

TABLE V
THE EXPLANATIONS OF SEVERAL OPTIMIZATION METHODS USED FOR SECURE EE MAXIMIZATION

Optimization methods	Problem formulations	Problem transformations	Algorithm procedures
Fractional programming [208], [209]	$\max\left\{f(\boldsymbol{x})=\frac{h(\boldsymbol{x})}{g(\boldsymbol{x})}\right\}$ s.t. $\boldsymbol{x}\in\mathbb{D}$	Being related to the parameterized problem $\max\{h(\boldsymbol{x})-\varepsilon g(\boldsymbol{x}):\boldsymbol{x}\in\mathbb{D}\}$ with parameter ε.	1) For a given initial value $\boldsymbol{x}_0$, calculate $\varepsilon_1=\frac{h(\boldsymbol{x}_0)}{g(\boldsymbol{x}_0)}$; let iterative index $i=1$. 2) For ε_i, calculate the optimal solution $\boldsymbol{x}_i$ by solving the parameterized problem. 3) Stopping test with $\boldsymbol{x}_i$: If true, then stop; otherwise, go to step 4). 4) For obtained $\boldsymbol{x}_i$, calculate $\varepsilon_{i+1}=\frac{h(\boldsymbol{x}_i)}{g(\boldsymbol{x}_i)}$, $i:=i+1$, and return to step 2).
Penalty function method [210], [211]	$\min f(\boldsymbol{x})$ s.t. $\begin{cases} l_k(\boldsymbol{x})\le 0 \\ \boldsymbol{x}\in\mathbb{D}, \end{cases}$ where $k=1,\cdots,m$.	Defining a penalty function $L(\boldsymbol{x})\triangleq\max\{0,l_k(\boldsymbol{x})\}_k$ for the nonconvex constraints $l_k(\boldsymbol{x})\le 0$, and transforming the problem formulation into $\min\{f(\boldsymbol{x})+\tau L(\boldsymbol{x}):\boldsymbol{x}\in\mathbb{D}\}$, where $\tau>0$ is a penalty factor.	1) Choose a small penalty factor τ_0 and an increasing factor ρ for updating τ. Let iterative index $i=0$. 2) For τ_i, calculate the optimal $\boldsymbol{x}_i$ by solving the resulting penalty problem. 3) Stopping test with $\boldsymbol{x}_i$: If true, then stop; otherwise, go to step 4). 4) Update τ by $\tau_{i+1}=\rho\tau_i$, $i:=i+1$, and return to step 2).
Alternating optimization [212], [213]	$\min f(\boldsymbol{x})$ s.t. $\boldsymbol{x}\in\mathbb{D}$	By partitioning the variables $\boldsymbol{x}$ into two subsets $\boldsymbol{y}$ and $\boldsymbol{z}$, the problem can be iteratively solved by tackling the following subproblems $\min_{\boldsymbol{y}}\{f(\boldsymbol{y},\boldsymbol{z}_i):\boldsymbol{y}\in\mathbb{D}(\boldsymbol{y},\boldsymbol{z}_i)\}$ $\min_{\boldsymbol{z}}\{f(\boldsymbol{y}_{i+1},\boldsymbol{z}):\boldsymbol{z}\in\mathbb{D}(\boldsymbol{y}_{i+1},\boldsymbol{z})\}$	1) Choose a starting point $\boldsymbol{x}_0=(\boldsymbol{y}_0,\boldsymbol{z}_0)$ and let iterative index $i=0$. 2) For the given $\boldsymbol{z}_i$, find the optimal solution $\boldsymbol{y}_{i+1}$ of $\min_{\boldsymbol{y}}\{f(\boldsymbol{y},\boldsymbol{z}_i):\boldsymbol{y}\in\mathbb{D}(\boldsymbol{y},\boldsymbol{z}_i)\}$. 3) For the given $\boldsymbol{y}_{i+1}$, find the optimal solution $\boldsymbol{z}_{i+1}$ of $\min_{\boldsymbol{z}}\{f(\boldsymbol{y}_{i+1},\boldsymbol{z}):\boldsymbol{z}\in\mathbb{D}(\boldsymbol{y}_{i+1},\boldsymbol{z})\}$. 4) Stopping test with $(\boldsymbol{y}_{i+1},\boldsymbol{z}_{i+1})$: If true, then stop; otherwise, let $i:=i+1$ and go to step 2).
DC programming [214], [215]	$\min\{f(\boldsymbol{x})=f_1(\boldsymbol{x})-f_2(\boldsymbol{x})\}$ s.t. $\boldsymbol{x}\in\mathbb{D}$, where $\mathbb{D}$, $f_1(\boldsymbol{x})$, and $f_2(\boldsymbol{x})$ are convex.	Being solved iteratively by tackling $\min\{f_1(\boldsymbol{x})-f_2(\boldsymbol{x}_i)-\langle\nabla f_2(\boldsymbol{x}_i),\boldsymbol{x}-\boldsymbol{x}_i\rangle:\boldsymbol{x}\in\mathbb{D}\}$, where ∇ denotes the gradient of a function and $\langle\cdot,\cdot\rangle$ denotes dot product.	1) Choose a starting point $\boldsymbol{x}_0$ and let iterative index $i=0$. 2) For fixed $\boldsymbol{x}_i$, find the optimal solution $\boldsymbol{x}_{i+1}$ of $\min\{f_1(\boldsymbol{x})-f_2(\boldsymbol{x}_i)-\langle\nabla f_2(\boldsymbol{x}_i),\boldsymbol{x}-\boldsymbol{x}_i\rangle:\boldsymbol{x}\in\mathbb{D}\}$. 3) Stopping test with $\boldsymbol{x}_{i+1}$: If true, then stop; otherwise, go to step 4). 4) Let $i:=i+1$ and go to step 2).

a) Conventional beamforming/precoding: The conventional beamforming/precoding schemes, such as MRT, signal/AN null space, and GSVD, are applied separately or jointly for secrecy enhancements, due to the inherent simplicity and easy implementation. For achieving a better secrecy performance, power allocation is usually optimized for these schemes. The MRT beamforming controls the beam towards the intended user for strengthening its received signals. Since the MRT beamforming may lead to information leakage on the direction to the eavesdropper, the AN null-space beamforming can then be exploited to disrupt the reception at the eavesdropper by emitting AN on the null space of legitimate channels. Such a joint scheme with MRT and AN null-space beamforming is of particular interest in practice when the eavesdropper's CSI is unavailable. If the transmitter has the full CSI of the eavesdropper, the ZF beamforming can then be performed to overcome the faults of information leakage to the eavesdropper by completely suppressing the beam towards the eavesdropper. To tradeoff the intended received signal and information leakage to eavesdropper or other users, RCI precoding is proposed based on a real regularization parameter which can be designed for secrecy rate improvements. When all nodes in a network are equipped with multiple antennas while the perfect CSI of all nodes is available, the GSVD precoding can be implemented to decompose both the legitimate channels and the wiretap channels into a set of parallel independent subchannels which can be used separately to transmit different messages. The works on the conventional beamforming/precoding schemes are compared in Table **VI**. Noteworthily, these conventional beamforming/precoding schemes are suboptimal in many situations, and the optimal designs in this field have therefore attracted great interest.

b) Optimal beamforming/precoding: To achieve the optimal secrecy performance, the strategy of beamforming/precoding is carefully designed by optimization approaches. The precoding matrix design for maximizing the secrecy capacity $C_s(\mathbf{W})$ in a standard three-node (two legitimate users and an eavesdropper) MIMO wiretap network is formulated as [83]

$$\begin{aligned}\max_{\mathbf{W}}\ & C_s(\mathbf{W})\\ \text{s.t.}\ & \mathrm{Tr}(\mathbf{W})\le P^{max},\mathbf{W}\succeq\mathbf{0},\end{aligned}\tag{39}$$

where $\mathbf{W}$ is the precoding matrix with the maximum power constraint P^{max} and the positive semidefinite constraint $\mathbf{W}\succeq\mathbf{0}$. Such a nonconvex problem is solved by alternating optimization and dual decomposition, while the resulting algorithm is extended to the scenario with destination jamming. In [68], the linear precoding strategies for secrecy rate

TABLE VI
THE COMPARISONS OF THE WORKS ON THE CONVENTIONAL BEAMFORMING/PRECODING SCHEMES

Schemes	CSI conditions	Expression/Constraints	Explanations
Joint MRT and AN null-space beamforming [42], [58], [62], [63], [88]	Legitimate CSI	$\mathbf{W} = \mathbf{H}^H/\|\mathbf{H}\|$ and $\mathbf{HZ} = \mathbf{0}$	Controlling the beam towards the intended user while Emitting AN on the null space of legitimate channels. The performance can be improved by power allocation between AN and information-bearing signal.
ZF beamforming [58]–[61]	Legitimate and wiretap CSI	$\mathbf{W} = \mathbf{H}^H(\mathbf{H}\mathbf{H}^H)^{-1}$ or $\mathbf{H}_e\mathbf{W}^H = \mathbf{0}$	Eliminating information leakage to the eavesdropper. This strategy is generally obtained by $\mathbf{H}^H(\mathbf{H}\mathbf{H}^H)^{-1}$ or optimized with the constraint $\mathbf{H}_e\mathbf{W}^H = \mathbf{0}$ in system designs.
RCI precoding [78]–[82]	Legitimate CSI	$\mathbf{W} = \mathbf{H}^H(\mathbf{H}\mathbf{H}^H + \alpha\mathbf{I})^{-1}$	To balance the intended signal and information leakage by designing a regularization parameter α. The secrecy performance of this strategy can be improved by power allocation.
GSVD precoding [26], [28], [74]–[77]	Legitimate and wiretap CSI	$\mathbf{HW} = \mathbf{UA}$ and $\mathbf{H}_e\mathbf{W} = \mathbf{U}_e\mathbf{A}_e$	Performing GSVD for matrix $(\mathbf{H}, \mathbf{H}_e)$, and returning the precoding matrix $\mathbf{W}$, unitary matrices $\mathbf{U}$ and $\mathbf{U}_e$, nonnegative diagonal matrices $\mathbf{A}$ and $\mathbf{A}_e$. Power allocation can also be optimized for secrecy improvements in this strategy.

*Notations: $\mathbf{H}$, $\mathbf{H}_e$, $\mathbf{W}$, and $\mathbf{Z}$ denote the matrices of legitimate channels, wiretap channels, beamforming/precoding, and AN, respectively.

maximization in multiuser multiantenna networks are investigated in the broadcasting and multicasting scenarios, and an iterative algorithm based on second-order cone programming is proposed with low complexity and provable convergence. Focusing on the secure communications in dual-polarized MIMO systems, a scheme of dual-structured precoding is addressed in [217] in which a preprocessing matrix based on the polarized array spatial correlation and a linear precoding scheme based on different CSI are concatenated. The secure beamforming for typical three-node (two legitimate users and a relay) MIMO relay networks is explored in [29] and [52], where the untrusted relay is treated as an eavesdropper. To reduce the difficulties of the joint designs in [29] and [52], the alternating optimization is used to iteratively deal with the source and the relay beamforming in an alternate fashion. To solve the resulting subproblems from alternating optimization, the SDP is introduced in the both works to transform a fractional quadratically constrained quadratic problem into a SDP problem by the technique of SDR [218] and the rank-one matrix decomposition theorem [219]. Besides, the beamforming for maximizing the secrecy rate in simultaneous wireless information and power transfer is designed in [54], [220], and [221], where the optimal solutions are derived also based on SDR. More specifically, by relaxing the rank-one constraint, the considered optimization problems are therein constructed as SDP problems which can be solved easily by some existing optimization techniques and rank-one reduction [54], [220]–[222].

2) Minimization of Secrecy Outage Probability: In physical layer security, the potential of secure beamforming and precoding for minimizing secrecy outage probability has also been explored in recent years. Naturally, the existing beamforming/precoding schemes mentioned in the last subsection can also be used to achieve the goal of secrecy outage probability reduction. As in [159], the AN-assisted beamforming is performed for degrading the eavesdroppers' channels while the optimal power allocation between the confidential information and AN is obtained in closed form to minimize the secrecy rate outage probability. In [156], the outage probability of secure transmission is minimized by the single-stream beamforming (based on MRT and ZF beamforming) and the use of AN in the null space of the legitimate channels. When only the location information of the eavesdropper is available at the source user in [223] and [224], the location-based beamforming is optimally designed to minimize the secrecy outage probability in Rician wiretap channels, while the resulting solution is extended to examine the solution of the optimal beamformer in the presence of a multi-antenna jammer [224]. To transmit information securely in millimeter-wave (mm-Wave) MISO-OFDM systems with partial channel knowledge, a hybrid precoder is implemented in [225] by an iterative design with the objective of minimizing the secrecy outage probability.

3) Minimization of Power Consumption: In the existing literature, secure beamforming and precoding are also used to support the designs of power minimization in different scenarios. The beamforming for minimizing transmission power in relay networks is investigated in [53], [59], [91], and [154] with different constraints. The typical mathematical model for minimizing the total power of the source and relays under a target secrecy rate constraint $R_s \geq R_s^0$ is given as [59], [154]

$$\begin{aligned} \min_{P_s, \mathbf{w}} \ & \left\{ P_s + \|\mathbf{w}\|^2 \right\} \\ \text{s.t.} \ & R_s(P_s, \mathbf{w}) \geq R_s^0, \end{aligned} \tag{40}$$

where P_s and $\mathbf{w}$ are the source power and the relay weights, respectively. In particular in [91], the beamformer of the relays is optimized to minimize the power allocated for transmitting confidential information, so that as much power as possible can be used to transmit AN to confuse the eavesdropper. In [226] where a secure multiuser broadcast system is considered, the optimal precoding matrix at the base station and the jamming covariance matrix at the friendly jammer are jointly designed to minimize the total transmission power under the signal-to-interference-plus-noise ratio (SINR) constraints at the users and eavesdroppers. In [227], the transmission beamforming is performed for minimizing the power consumption of a full-duplex base station considering both self-interference mitigation and physical layer security. Additionally, the physical

layer security in satellite communication is considered in [170] where the beamforming and power allocation under the individual secrecy rate constraints are designed for minimizing the overall transmission power used by all beams. In a new cognitive radio network as described in [228], a cooperative beamforming scheme is proposed to minimize the transmission power of a secondary transmitter while providing different SINR for an eavesdropper, a primary receiver, and multiple secondary receivers.

The problems of power minimization by beamforming/precoding are also raised in simultaneous wireless information and power transfer systems considering multifarious settings.

- Multi-antenna broadcast networks: In such settings, simultaneous wireless information and power transfer is implemented by transmission beamforming which is designed to jointly or separately satisfy the constraints of secrecy rate, secrecy outage probability, energy-harvesting outage probability, and received SINR ratio [229]–[235]. In order to achieve secure transmission, the transmission beamforming is also aided with AN strategy in many works [230]–[235].
- Distributed antenna systems: In [236], the beamforming and AN vectors are jointly optimized to minimize the total transmission power while providing QoS for reliable communication and efficient power transfer in a given time slot, in which the capacity-limited backhaul links is taken into account.
- Multi-cell multigroup multicast systems: In [237], two different optimization targets are considered for a multicell multigroup MISO system, i.e., power minimization and SINR balancing. The centralized and distributed beamforming algorithms are proposed for the considered optimization problems, based on the techniques of SDR and alternating optimization.
- Cognitive radio networks: Simultaneous wireless information and power transfer are raised in cognitive radio networks in [238] and [239]. In [238], the total transmission power at the energy transmitter and the secondary transmitter is minimized by a cooperative precoding design while satisfying secrecy rate, energy harvesting, and interference temperature constraints. In [239], the total transmission power of the secondary transmitter is minimized while ensuring that the QoS requirement on secure communication is satisfied.

It is noted that, in many works, the technique of SDR is extensively adopted in the designs of transmission beamforming [229], [231]–[235], [239], such that an approximation problem can be directly obtained and solved by the method of SDP. In general, the resulting relaxed problem by SDR cannot ensure to get a rank-one solution. It always acts as an upper bound of the performance for the original problem [218]. In some cases, the solution obtained by SDR is provably optimal, or the rank of the solution can be reduced by some techniques of rank reduction. Noteworthily, solving the SDP problem may result in relatively poor performance if SDP returns a high-rank solution. To overcome the difficulty, a method termed as SPCA [240], [241] is usually employed to find a suboptimal solution [229], [231]. The SPCA method approximates the nonconvex constraints by an upper convex estimate, and then results in a problem which can be solved directly. The two methods are briefly compared in Table VII.

4) Maximization of Secure EE: The energy-efficient beamforming and precoding in physical layer security have also been given many attentions. In [71], the energy-efficient precoder design in a conventional three-node (including a transmitter, a legitimate receiver, and an eavesdropper) MIMO wiretap channel is proposed based on the fractional programming and Taylor series expansion. In [174], by providing a second-order approximation to the MIMO secrecy capacity with its first and second derivatives, the metric of minimum bit energy is examined for secure and reliable communications in the low-SNR regime while characterizing the tradeoff between EE and secrecy. A beamformer design is performed in [243] for secure and energy-efficient wireless communication over MIMO channels with multiple user pairs and an eavesdropper, where a path-following computational procedure is proposed to cope with the intractable nonconvex problem and to yield at least a locally optimal solution. In [244], the robust energy-efficient transmission design for MISOME wiretap channels is investigated by the fractional programming and tight convex relaxation, so that the primal fractional optimization problem is solved by solving a sequence of SDP problems. The energy-efficient beamforming for secure cognitive communication is raised in [245], in which the primal problem is tackled by the combined use of the fractional programming and DC programming. In addition, in a MIMOME network with simultaneous wireless information and power transfer [246], the transmission covariance matrices and power splitting ratio for decoding information and harvesting energy are designed jointly to maximize the secure EE, where the fractional programming and alternating optimization are also employed for handling the nonconvexity of the optimization problem.

C. Antenna/Node Selection and Cooperation

Antenna/node selection and cooperation in multi-antenna and multi-node wireless networks have been well exploited for achieving different performance requirements of physical layer security. Being similar to the former subsections, the state of the art of optimization designs in this research topic can also be reviewed from the four categories of optimization problems.

1) Maximization of Achievable Secrecy Rate: Great efforts have been made for the optimization designs of antenna/node selection and cooperation to increase the achievable secrecy rate. Multi-antenna diversity can provide the gain of secrecy rate by designing proper strategy of antenna selection, as investigated in [93], [95], and [247]. In multiuser scenarios, user selecting/scheduling can bring the improvement of secrecy rate by using multiuser diversity, such as the optimal and suboptimal scheduling in a multiuser MISO system [145], the maximum instantaneous SNR scheduling and approximate proportional fair scheduling in a multiuser MISO system with a multi-antenna eavesdropper [108], and the round-robin

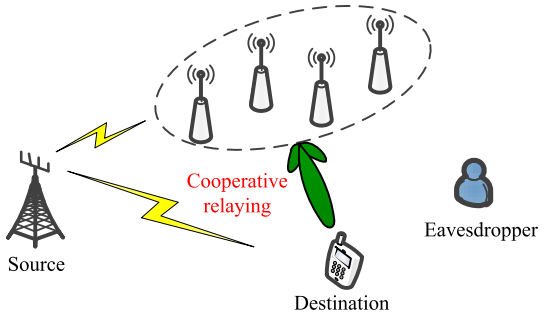
TABLE VII
THE COMPARISONS OF SDR AND SPCA

Optimization methods	Problem formulations	Problem transformations	Comments
SDR [218], [242]	$\min_{\boldsymbol{x}\in\mathbb{R}^n} \boldsymbol{x}^T\mathbf{A}_0\boldsymbol{x}$ s.t. $\boldsymbol{x}^T\mathbf{A}_i\boldsymbol{x} \geq b_i$, where $\mathbf{A}_i$ are symmetric square matrices, $i = 0, 1, 2, \cdots$.	By defining $\mathbf{X} = \boldsymbol{x}\boldsymbol{x}^T$ which is equivalent to $\mathbf{X}$ being a symmetric positive semidefinite matrix with rank one constraint $rank(\mathbf{X}) = 1$, we get that $\boldsymbol{x}^T\mathbf{A}_i\boldsymbol{x} = \text{Tr}(\mathbf{A}_i\mathbf{X})$. By ignoring $rank(\mathbf{X}) = 1$, we obtain a relaxed problem known as an SDP: $\min_{\mathbf{X}} \text{Tr}(\mathbf{A}_0\mathbf{X})$ s.t. $\begin{cases} \text{Tr}(\mathbf{A}_i\mathbf{X}) \geq b_i, i = 1, 2, \cdots \\ \mathbf{X} \succeq 0. \end{cases}$	The core idea of the method is that we drop the rank-one constraint to obtain a SDP problem. The SDP problem can be handled very conveniently by readily available software packages. However, the resulting SDP problem may lead to relatively poor performance if SDP returns a high-rank solution.
SPCA [240], [241]	$\min_{\boldsymbol{x}\in\mathbb{R}^n} f(\boldsymbol{x})$ s.t. $l_i(\boldsymbol{x}) \leq 0, i = 1, 2, \cdots$ where $f(\boldsymbol{x})$ is convex, and $l_i(\boldsymbol{x})$ is nonconvex.	By defining a function $L_i(\boldsymbol{x}, \varphi_i)$ which is a convex upper approximation of the nonconvex function $l_i(\boldsymbol{x})$, i.e., $l_i(\boldsymbol{x}) \leq L_i(\boldsymbol{x}, \varphi_i)$, the original problem can be approximated by the following convex problem: $\min_{\boldsymbol{x}\in\mathbb{R}^n} f(\boldsymbol{x})$ s.t. $L_i(\boldsymbol{x}, \varphi_i) \leq 0, i = 1, 2, \cdots,$ where φ_i is a slack variable which is updated at each iteration.	The basic idea of the method is that, at each iteration, we replace each of the nonconvex constraints by its upper convex approximation function with an appropriate φ_i. Thus, the method is required to iteratively solve a convex problem based on convex optimization. The difficulty of the method is to carefully choose the upper convex estimates and slack variables.

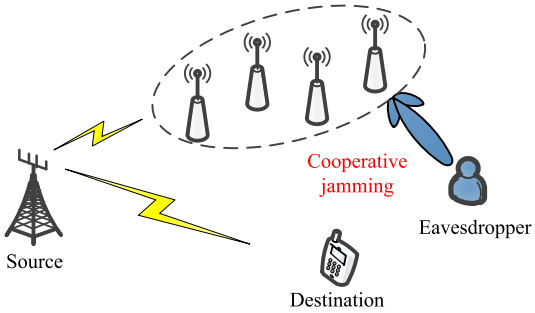
user scheduling as well as the optimal and suboptimal user scheduling in a cognitive radio network [103], [104].

In cooperative networks, the broadcast feature of wireless transmission results in two aspects, namely node cooperation and data secrecy [248]. Node cooperation means that users can help improve each other's rate by intelligently using their received signals. Data secrecy implies that the information leakage to the undesired users may cause some severe problems of information security. Accordingly, node cooperation and data secrecy have been studied jointly in multi-node cooperative scenarios in recent years. The cooperative nodes act two roles in physical layer security, including cooperative relaying and cooperative jamming [9]–[12], [18], [249]. Cooperative relaying is to enhance the legitimate channels while cooperative jamming is to degrade the wiretap channels. In practice, the cooperative nodes may be trusted or untrusted. For the trusted nodes, they can be used for relaying and jamming separately or jointly [18]. As to untrusted nodes, seeking for cooperative relaying or jamming with them may be better than treating them as pure eavesdroppers [121], [122]. According to the roles of the cooperative nodes, there are generally four kinds of node-assisted transmission designs, which involve cooperative relaying, cooperative jamming, hybird cooperative relaying and jamming, and cooperative relaying with AN [12], [30], as illustrated in Fig. 7.

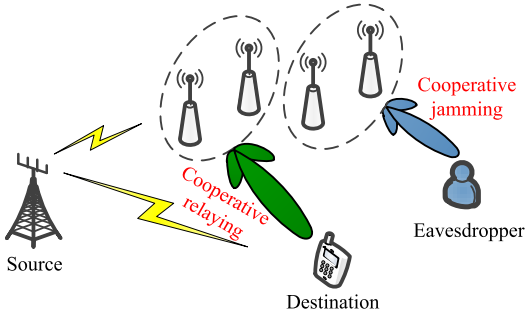
- Cooperative relaying: When the channels from the source to the destination are too poor or even nonexistent, signal retransmission by intermediate nodes is an effective way for confidential data transmissions, as shown in Fig. 7(a). Seeking for cooperative relaying with the intermediate nodes, the confidential data can be delivered securely and reliably, while some signal processing technologies can be applied into system designs to achieve both the performance requirements and resource saving. The typical cooperative relaying supported by beamforming to improve secrecy rate is investigated in [29], [52], [58]–[61], [154], and [250], where the relays are trusted [58]–[61], [154], [250], [251] or untrusted [29], [52]. The optimal power control for multi-hop relaying is raised in [44]. The optimal relay selection and relay placement for cooperative relaying are concerned in [109] and [252], respectively. In [110], three opportunistic relay selection schemes are studied for maximizing the Shannon capacity to the destination as well as for minimizing that to the eavesdroppers. According to [110] and [132], the relay selection schemes can be sorted into four categories, as listed in Table VIII.
- Cooperative jamming: When there is the direct channel from the source to the destination, the relays can be used as jammers to emit artificial interference, such that the channels to the eavesdropper are degraded and the confidential information is protected against eavesdropping, as depicted in Fig. 7(b). A simple but suboptimal jamming strategy is null-space cooperative jamming which emits artificial interference in the null space of the channels from the relays to the destination. Such a null-space jamming strategy degrades only the wiretap channels while with no influence to the legitimate channels. Trying to obtain the optimal cooperative jamming designs, the solutions of jamming signal weights are elaborated in [59], [147], and [154]. In [28], two types of cooperative jamming schemes referred to as full cooperative jamming and partial cooperative jamming are proposed depending on that whether both the transmitter and the temporary helpers (which are acted by the source and the destination) transmit jamming signals at the same time. The secure transmissions with and without cooperative jamming are compared in [39] based on the worst-case optimization. Using the intermediate nodes to relay or to jam, which is a better choice? Such a problem involving cooperative mode decision is discussed in [129], in which the performance comparison



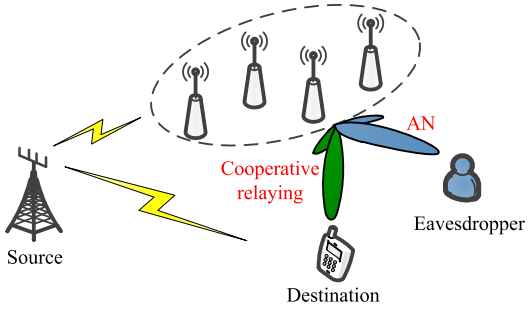
(a) Intermediate nodes used as relays for beamforming



(b) Intermediate nodes used as jammers for beamforming



(c) Intermediate nodes grouped as relays and jammers for beamforming



(d) Intermediate nodes used for joint relay beamforming and AN precoding

Fig. 7. Different strategies of intermediate node assisted transmission in cooperative networks.

TABLE VIII
RELAY SELECTION SCHEMES

Schemes	Mathematical formulations	Achievable secrecy rates	Explanations
Conventional selection	$k^* = \arg\max_{k\in\Omega}\{\gamma_{k,D}\}$	$C_s = \max_{k\in\Omega}\{C_{k,D}\} - C_{k^*,E}$	The relay which has the highest instantaneous SNR of the relay-destination links will be selected for relaying.
Minimum selection	$k^* = \arg\min_{k\in\Omega}\{\gamma_{k,E}\}$	$C_s = C_{k^*,D} - \min_{k\in\Omega}\{C_{k,E}\}$	The relay that has the lowest instantaneous SNR of the relay-eavesdropper links will be selected for relaying.
Optimal selection	$k^* = \arg\min_{k\in\Omega}\left\{\frac{1+\gamma_{k,D}}{1+\gamma_{k,E}}\right\}$	$C_s = C_{k^*,D} - C_{k^*,E}$	The optimal selection incorporates the quality of both links into the selection decision metric. The relay that has the highest achievable secrecy rate will be selected for relaying.
Suboptimal selection	$k^* = \arg\min_{k\in\Omega}\left\{\frac{\gamma_{k,D}}{\mathbb{E}\{\gamma_{k,E}\}}\right\}$	$C_s = C_{k^*,D} - \mathbb{E}\{C_{k^*,E}\}$	The suboptimal selection scheme selects the appropriate relay based on the statistical knowledge of the relay-eavesdropper links. The scheme can avoid the instantaneous estimate of the wiretap channels.

*Notations: C_s is the secrecy rate. k^* is the selected relay from the relay set Ω. $\gamma_{k,D}$ and $\gamma_{k,E}$ are the instantaneous SNR of the links from relay k to the destination and the eavesdropper, respectively. $C_{k,D}$ and $C_{k,E}$ are the channel capacity of the links from relay k to the destination and the eavesdropper, respectively. $\mathbb{E}\{\cdot\}$ denotes expectation.

between the relay transmission scheme and the direct transmission scheme with jamming is examined in the distance normalized SNR regime. Additionally, in [129], it is also concluded that, in the high distance normalized SNR regime, the direct transmission scheme provides higher secrecy rate compared with the relay transmission scheme, while in the low distance normalized SNR regime, the relay transmission scheme outperforms the direct transmission scheme.

- Hybrid cooperative relaying and jamming: A more widely-used strategy is hybrid cooperative relaying and jamming which is based on the combined application of the two methods. In such a hybrid strategy, the intermediate nodes are grouped as relays and jammers. The relays retransmit the received confidential information to improve the signal quality at the destination while the jammers continuously emit artificial interference to confuse the eavesdroppers, as illustrated in Fig 7(c). This may take the confidential information under protection in all stages of cooperative transmission. As in [132], [133], [138], and [142]–[144], the hybrid cooperative relaying and jamming are investigated in different

settings where joint relay and jammer selection are also taken into account. A multiuser relaying scheme with the intended user jamming is proposed in [102] where the optimal user selection is also considered in the sense of maximizing the secrecy rate. In [123], the untrusted two-way relaying with friendly jammers is investigated based on Stackelberg game. In [146], a hybrid relaying and jamming scheme with the optimal relay selection and power allocation is developed for maximizing the secrecy rate, in which the destination and the source are used as jammers to jam the eavesdropper in the first and second phase of cooperative transmissions, respectively.

- Cooperative relaying with AN: In this strategy, as shown in Fig. 7(d), the relays are used to forward confidential information and transmit AN simultaneously. To be specific, the confidential information retransmitted at each relay is superimposed with an AN. This strategy subsumes all the above three designs and makes better use of available degrees of freedom at relays [30]. As a result, the combined designs of cooperative relaying and AN precoding have been widely considered in physical layer security, such as in [30], [117], [253], and [254]. Noteworthily, it is generally challenging to jointly optimize AN precoding and relay beamforming [30]. Therefore, some suboptimal but effective schemes have been proposed. The joint AN-aided beamforming and power allocation are studied in [28], where a closed-form jamming beamformer and a GSVD-based secure relaying scheme with each corresponding optimal power allocation are developed for the cases of single and multiple stream data transmissions, respectively. In [255], for a single-relay MIMO wiretap channel, an interference alignment approach is addressed to obtain a simplified and suboptimal design of AN-assisted cooperative relaying.

2) Minimization of Secrecy Outage Probability: The spatial diversity provided by multiple antennas and nodes can be effectively utilized for reducing the secrecy outage probability in multi-antenna and multi-node networks. The antenna selection for enhancing the secrecy outage performance has been investigated for MIMOME networks [100], [256], MIMO relay networks [257], non-orthogonal multiple access systems [258], and cognitive radio networks [259]. The antenna selection combined with AN is proposed for decreasing the secrecy outage probability in secure two-way relaying communications in [260]. In multi-node scenarios, the relay and jammer selection in DF relay networks are studied separately or jointly for minimizing the secrecy outage probability in [112] and [136]. The best relay and user pair selection for minimizing the secrecy outage probability of a multiuser AF relay network are addressed in [113], in which the analytical expressions of the secrecy outage probability are also derived for the proposed three selection criteria. The selections of the transmission protocols are also investigated in [261] and [262]. In [261], the secure transmission protocol which switches between DF beamforming and cooperative jamming is proposed for the purpose of maximizing secrecy rate and minimizing secrecy outage probability in different communication scenarios. A secure opportunistic transmission protocol that aims at finding an optimal scheme between direct transmission and relaying transmission, is developed in [262] to achieve the lowest secrecy outage probability of cooperative wireless networks. Some works also consider designing the strategies of node selection and cooperation to reduce the secrecy outage probability of cooperative energy harvesting networks [263]–[265]. In [263], the relay and jammer selection are considered for the cooperative energy harvesting networks with a friendly jammer. In [264], the secrecy outage probability of a wireless powered communication network with an energy harvesting jammer is analyzed and minimized by optimizing the time allocation between the two phases of information transfer and energy transfer. The work presented in [264] is extended to a more general multiuser situation with an additional consideration of jamming power allocation in [265].

3) Minimization of Power Consumption: Although multiple node cooperation can support the improvements of information security, multiple nodes used for information transmission may bring additional power consumption. In particular, some cooperative nodes may consume high power but bring inconsiderably improvement of secrecy. Accordingly, node selection and cooperation for saving power while ensuring secure QoS requirements have been also studied in physical layer security. As investigated in [114], the so-called power-efficient secure communication is discussed with the objective of power minimization by optimal relay selection. In [266], a secure adaptive relay cooperation approach is developed to ensure wireless information security in an untrusted relay network with relay energy harvesting, while a greedy battery-aware relay selection scheme is proposed to minimize the power consumption in such a network.

4) Maximization of Secure EE: It has been verified that antenna/node selection and cooperation also can bring the gain of secure EE. In [267], the secure EE of a cooperative MIMO relay network is investigated, in which transmit antenna selection and MRC are deployed at the transmitter and the receivers, respectively. Considering three possible cooperation scenarios in [268], namely the jammer only, relay only, and the relay-jammer pair, the adaptive cooperation schemes are addressed for energy-efficient physical layer security. In [269], hybrid full-/half-duplex receiver deployment strategies are proposed for wireless ad hoc networks to optimize the network-wide secrecy throughput and network-wide secure EE, respectively. The potential advantages of massive MIMO technologies are also explored for improving secure EE [270], [271]. In [270], the potential benefits of massive MIMO aided heterogeneous cloud radio access networks are explored in terms of the secrecy and EE. In [271], the advantages of massive MIMO relaying are utilized to improve the secure EE which is specially defined as the ratio of the secrecy outage capacity to the total power consumption. Moreover, the energy-efficient secure communication over a large-scale wireless network is studied by the combined application of game theory and stochastic geometry in [272]. An alternating optimization scheme is proposed therein for maximizing the secure EE of the legitimate transmitters by

controlling the node activation probability, confidential message rate, redundancy rate, and the number of active antennas. In addition, an energy-efficient node activation game between the transmitters and the eavesdroppers is also studied therein, where the transmitters and the eavesdroppers control their node activation probabilities to maximize the secrecy EE and the eavesdropping EE, respectively.

VI. The Impacts of CSI on Physical-Layer Security Designs

It has been discussed that the priori knowledge of the legitimate and wiretap channels' CSI is very important for the choices of secrecy metrics and the designs of secrecy strategies [12]. To achieve the optimal performance of secure transmission, the perfect CSI of both the legitimate and wiretap channels is indispensable for system designs. For getting the CSI of the legitimate channels, some conventional methods (such as training/estimation and feedback), being similar to that in the traditional communications without secrecy constraints, can be used in physical layer security designs. However, due to the existences of estimation error and feedback delay in some cases, it may be difficult in practice to get the perfect CSI of legitimate channels. Regarding the CSI of wiretap channels, it can be obtained perfectly when the eavesdroppers are also the legitimate users of the network but have different service from that of the intended users. However, when the eavesdroppers are passive, vicious or even hostile, it may be impossible to get the perfect CSI of such eavesdroppers. According to the above discussions, the following assumptions of CSI have been considered in physical layer security, i.e., the perfect CSI of all channels, the imperfect CSI of wiretap channels, and the unknown CSI of wiretap channels.

A. The Perfect CSI of All Channels

In the literature on physical layer security, the perfect CSI of all channels has been commonly assumed for designing the optimal transmission scheme which can match the instantaneous changes of channel states, such as in [35], [38], [44], [52], [55], [59]–[61], [109], and [154]. In fact, the perfect CSI including that of eavesdroppers, can be obtained at all communication nodes in some situations. For instance, the eavesdropper is active in the network and its transmissions can be monitored. This case arises particularly in the practical applications combining multicast and unicast transmissions, in which the user plays double roles as legitimate receiver for some signals and eavesdropper for others [59]. Alternatively, the eavesdropper is also a legitimate user of the network whereas its service differs from that of the intended user [61]. In other words, instead of eavesdroppers, there can be friendly nodes in the network that are not supposed to hear certain messages. This case arises often in military communications, where lower level network users can only access to less information [154]. Because the confidential information of the source user is expected to be received only by the intended user, the other users (they are even legitimate and friendly) in the network should be treated as eavesdroppers for secure transmission designs. However, such legitimate and friendly users can feed back the perfect CSI to transmitters. Accordingly, the optimal secure transmission designs can be performed with the perfect CSI of all channels.

B. The Imperfect CSI of Wiretap Channels

In many situations, the perfect CSI of the main channel can be easily obtained by channel estimation and CSI feedback, whereas getting the perfect CSI of the wiretap channels is very difficult or even impossible. In such cases, the imperfect CSI of eavesdroppers may be obtained in practice, based on the past channel observations or a priori knowledge of the particular propagation environment [273], [274]. The uncertainties of the imperfect eavesdropper's CSI can be generally characterized by three ways. The first way is that the channel of eavesdropper follow some probability distributions [144], [251], such as the Gaussian distribution, Rayleigh distribution, Rician distribution, and so on. In this way, only the statistical information of the eavesdroppers' channels, i.e., the mean and covariance of the probability distribution, is available for the system designs, such as the assumptions in [40], [42], [51], [58], and [64]. The second way to characterize the uncertainties of eavesdroppers' channels is termed as the deterministic uncertainty model in [30], [39], [58], [170], [234], [253], and [275]. In the deterministic uncertainty model which belongs to compound channel in information theory, the unknown wiretap channels are assumed to fall in a sphere or a set. To be specific, the uncertainty region of eavesdropper's channels is modeled as a sphere $\mathbb{H}_e$ with center $\bar{\mathbf{h}}_e$ and radius $\sqrt{\epsilon}$, that is [30], [39], [58], [170], [234], [253], [275]

$$\begin{aligned}\mathbb{H}_e &= \left\{\mathbf{h}_e \middle| \|\mathbf{h}_e - \bar{\mathbf{h}}_e\|^2 \le \epsilon\right\} \\ &= \left\{\bar{\mathbf{h}}_e + \mathbf{v}_e \middle| \|\mathbf{v}_e\|^2 \le \epsilon\right\}. \end{aligned} \tag{41}$$

In (41), $\mathbf{h}_e$, $\bar{\mathbf{h}}_e$, $\mathbf{v}_e$, and $\epsilon > 0$ denote the real channel vector of eavesdropper, the estimated channel vector of eavesdropper, the estimation error vector, and the channel mismatch, respectively. By this model, we have that $\mathbf{h}_e \in \mathbb{H}_e$. The third way to model the imperfect eavesdropper's channels is based on the imperfect channel estimate $\bar{\mathbf{h}}_e$, the estimation error vector $\mathbf{v}_e$, and a scalar $\kappa \in [0, 1]$ for indicating the degree of channel knowledge. This model can be expressed as [156], [276]

$$\mathbf{h}_e = \sqrt{\kappa}\bar{\mathbf{h}}_e + \sqrt{1-\kappa}\mathbf{v}_e. \tag{42}$$

In (42), if $\kappa = 1$, it means that the eavesdropper's CSI is perfect, while if $\kappa = 0$, it implies that we fail to get any CSI of the eavesdroppers.

In some worse cases, the perfect CSI of both legitimate and wiretap channels is unavailable due to limited feedback or other reasons, such as discussed in [40], [45], and [56]. Then, the uncertainties of legitimate channels can also be characterized by the three methods mentioned above. It is worth noting that, towards the uncertainties of real channels, the robust secure designs are commonly performed to ensure achieving the security, reliability, and robustness of information transmission [30], [39], [56], [234], [253], [275].

C. The Unknown CSI of Wiretap Channels

The assumption on the perfect CSI of all channels is commonly used for calculating the instantaneous secrecy capacity and secrecy rate which are needed for instantaneous optimization designs. Using the perfect CSI, the security and reliability of information transmission can be guaranteed by secure coding and rate adaptation. However, a more practical assumption is that the CSI of wiretap channels is completely absent due to the concealment and hostility of eavesdroppers [47], [91], [256], [277]. Moreover, whether there exists any eavesdropper cannot be known in some situations. Because the eavesdroppers' CSI is unknown at the transmitters, the expression of the instantaneous secrecy rate is unavailable. Therefore, the instantaneous optimization cannot be performed. Then, a probabilistic view of security or a QoS-based optimization can be considered for secure transmission designs. Such as in [256], a strategy of transmission antenna selection to enhance the secrecy performance of MIMO wiretap channels without eavesdroppers' CSI is proposed based on three important metrics, i.e., the probability of non-zero secrecy capacity, the secrecy outage probability, and the ϵ-outage secrecy capacity. In [47], secrecy sum rate maximization considering each user's QoS constraint and unknown eavesdropper's CSI is investigated for a non-orthogonal multiple access system. In [91], a QoS-based secure strategy is addressed to enhance the security of a cooperative relay network without eavesdropper's CSI. It is worth pointing out that, exploiting AN or jamming signal to enhance secrecy has been demonstrated to be effective when the eavesdropper's CSI is unknown or imperfect [9].

VII. Discussions on Future Directions and Challenges

It has been shown in previous sections that the physical layer security has attracted increasing concerns. Some great progress has been made in the fields of information-theoretical security and optimal secure designs at physical layer. However, it has been observed that many studies in the existing works are performed with some special assumptions on CSI, eavesdropper model, and application scenarios. These assumptions may be unpractical or even contrary to real conditions. Therefore, there are still many significant problems needed to be investigated to promote the practical applicability of physical layer security. In the following, some possible future directions and open challenges are simply discussed. Since the future work in physical layer security is very extensive, only a few directions are discussed.

A. The Influences of Wireless Channels

The influences of wireless channels on secrecy must be further studied. In literature, it is often assumed that the channels to legitimate user and eavesdropper are uncorrelated. The uncorrelated property is believed to be the foundation to assume that the eavesdroppers cannot estimate the channels of legitimate transceivers. However, this assumption has its limitations considering some practical scenarios. For instance, when the transceivers as well as the eavesdroppers lie in a insufficiently rich scattering environment as discussed in [20], the assumption of uncorrelated channels is then impractical. In addition, much existing literature simply assume that the channels are quasi-static or even completely static. However, if the channels are somewhat dynamic, the resulting conclusions in those works may be in conflict with the real settings. Furthermore, the relative spatial locations between the transceivers and eavesdroppers, as well as the node mobility model, may have important impacts on wireless channels, which also need to be considered in secure transmission designs. Besides, it is already known that the secure strategy designs heavily depend on the CSI of legitimate users and eavesdroppers, whereas the perfect CSI is difficult to get in many situations due to the limited estimation and feedback or other reasons.

The challenges stemmed from the aspect of wireless channels are because of the difficulties of accurate channel estimation for wiretap channels, and the considerations of channel correlations, time varying, and node mobility. First, how to get the perfect CSI to achieve the optimal security performance is difficult to deal with, especially when the eavesdropper is inactive. Furthermore, accurate channel estimation may cause unacceptably high overhead in pilot frequency and power consumption. This is a particularly severe problem in massive MIMO networks as the overhead may grow rapidly with the antenna number. Even worse, the process of channel estimation may be attacked by pilot contamination attack which not only dramatically reduces the achievable secrecy capacity but is also difficult to detect [17]. Second, high channel correlations have been observed in [278] even when the spatial separation is much larger than half-wavelength [279]. This indicates that the spatial correlations of wireless channels may vary in different environments and the half-wavelength decorrelation assumption may not always hold [279]. Therefore, the secure transmission designs considering the channel correlations is also a challenging problem in future. Third, the time-varying characteristics of channels and the mobility of terminals are also severe issues in physical-layer secure communications since the channel qualities may vary dramatically over time and space. Therefore, how to simultaneously guarantee the security, reliability, and robustness of a secure transmission scheme with the problems mentioned above will be challenging in future work.

B. The Impacts of Adversary Model

The impacts of attack modes and adversary models are also important issues for secure transmission that has not yet been deeply explored. Much existing literature assumes that the adversaries merely passively listen to the secure communications. In other words, there are no collaboration and information exchange among the adversaries. Nevertheless, the adversaries may actively collaborate and exchange their outputs in practice to interpret the confidential messages [280]. Moreover, a slightly more sophisticated adversary may be able to predict the channels for improving the eavesdropping qualities. Some intelligent adversaries may attempt to manipulate the propagation environment for strengthening their

advantages and undermining information security [281], [282]. When these observations discussed above are taken into account, the transmission strategy designs for physical layer security will be facing great challenges.

The challenges in this direction can be discussed from the following aspects. On the one hand, the optimization and design in physical layer security will become more complicated when hybrid attacks are imposed on wireless information transmission, such as eavesdropping attack, jamming attack, denial-of-service attack, spoofing attack, message falsification/injection attack, etc. It will be of particular importance to develop new techniques to jointly defend against hybrid wireless attacks [14]. On the other hand, great difficulties result from the intelligent adversaries that not only can efficiently collaborate with each other and actively manipulate propagation environment for attacks, but also can autonomously learn the knowledge of the associated wireless network to find its weakness and then to implement adaptive attacks. Therefore, it is challenging to develop well-performing secure mechanisms to defend against the intelligent adversaries.

C. The Influences of Hardware Impairments

Hardware impairments are nonnegligible factors which should also be taken into account in physical layer security. So far, a great deal of works on the designs of security strategies assume that the transceiver hardware is perfect. However, hardware impairments truly exist in practice, due to nonlinear power amplifiers, in-phase and quadrature (I/Q) imbalance, frequency and phase offsets, quantization noise, and synchronization errors [283]. For instance, I/Q imbalance can attenuate the amplitude and rotate the phase of the desired constellation, while it can create an additional signal from the mirror subcarrier which leads to a symbol error rate. In the presence of nonlinearities of power amplifiers, the bit error rate may increases remarkably compared to linear power amplifiers [284]. Although the deleterious impacts of hardware impairments on the security performance can be mitigated by calibration and compensation algorithms, residual distortions at the transceivers are inevitable [283].

Many unknown challenges may be caused by hardware impairments in the fifth generation (5G) and beyond networks where novel physical layer technologies will be deployed, such as the technologies of massive MIMO, mm-Wave, and full duplex. In massive MIMO systems, additional challenges root in decreasing the hardware cost and increasing the power efficiency on antenna array which rise to hardware impairments. Moreover, due to the very large size of antenna array, standard algorithms for hardware impairment compensation, such as digital predistortion and phase-noise estimation and compensation may be too complex in a massive MIMO system [285]. The mm-Wave technologies utilize high frequency of mm-Wave band, ranging from $3 \sim 300$ GHz. Due to the very small wavelength, the mm-Wave networks are different from the conventional microwave networks in the following ways: large number of antennas, sensitivity to blockages, and variable propagation laws, which may deteriorate the harmful influence of hardware impairments to secure transmissions. In full duplex systems where the information is exchanged on the same frequency and time slot, the residual self-interference is still remained due to the impairments of hardware interference suppression methods, and signal processing technologies are needed to be addressed to suppress the residual self-interference thoroughly. In addition to those challenges mentioned above, in some infrastructureless networks and low-end networks (such as some specific scenarios in IoT) in which the communication equipments may be low-cost with small battery capacity, the hardware impairments may be more severe issues for implementing physical layer security.

D. The Joint Designs of Physical Layer Security and Classic Cryptographic Security

Some efforts may be needed for seeking deep insights into physical layer security and classic cryptographic security. In future, 5G network and beyond require ultra-strong security to support extremely secure service. Classic cryptographic security at the high cost of computational complexity, is usually deployed at the higher layers of protocol stack. As an alternative security technology, physical layer security has the advantages of lower complexity and resource savings. Any single security technology may not satisfy the demands of high security in future. Therefore, a natural question is how to jointly exploit the advantages of the two security technologies. Then, the cross-layer analysis and design combined with physical layer security and classic cryptographic security come naturally to mind to provide a comprehensive security solution from each layer of protocol stack.

To this end, there are many challenging problems needed to be solved in this direction, such as the secure network framework, secure coding scheme, secure network protocol, hybrid encryption algorithm, and so on. In future, the network architecture presents heterogeneous features, where the communication nodes are deployed with dissimilar characteristics such as computing capacity, energy supply capacity, radio access technologies, protocol stack architecture, etc. This requires that the joint security strategy designs can adapt to the heterogeneous architecture of networks, the variety of nodes, and the diversification of radio access technologies. This is significant but challenging work, since a joint security scheme for high level secrecy is usually followed with extremely high complexity which may limit its practical application. Moreover, the joint security scheme is expected to have a good scalability which allows the minimum amount of recomputation to update protocol parameters if some components of a network are changed. Therefore, in practice, how to design a simple but well-performing joint security scheme to tradeoff between the performance and the complexity is an urgent need to be addressed.

E. The Global Optimization With Security, Reliability, and Throughput

To achieve the optimal network performance and user experience in a wireless network, the security, reliability, and throughput should be considered jointly in system

designs [14]. However, in many existing works, these performance metrics are taken into account individually and separately to reduce the difficulty in system designs. Consequently, the proposed security mechanisms are potentially suboptimal, since the three factors interact with each other. For instance [14], the reliability and throughput of the legitimate channel can be improved by increasing the transmission power which however may improve the capacity of wiretap channel and increase the probability of successful eavesdropping. Likewise, although we can increase the coding rate at the transmitter for improving the security level while reducing the intercept probability, this leads to a decrease in transmission reliability, since higher coding rate may increase the outage probability of legitimate channel.

In order to achieve the near-perfect system performance, the global optimization with the joint considerations of security, reliability and throughput is needed to be carried out, which may be challenging and intractable. For formulating and solving such complicated multi-objective problems, some convex/nonconvex optimization techniques and game theory, as well as stochastic geometry, will be widely applied in this field [26], [138]. Furthermore, the EE of a network attracts increasing concerns at present and in future. When the requirement of EE is imposed on the global optimization discussed above, the secure transmission designs will be extremely complicated work which calls for innovative efforts to develop novel optimization theories and technologies.

F. The Commercial Application of Physical Layer Security

It is largely unexplored to apply the technologies of physical layer security into commercial wireless networks. In fact, the most research work on physical layer security still stays at the theory stage. The opportunities of applying physical layer security into real commercial networks will be quite rich while following numerous difficulties and challenges that are from not only the technical flaws of the proposed secure strategies but also the limitations of existing network architecture and technologies, such as the hurdles from the applicability of existing network framework, the expansibility of underlying air interface, and the constraints of network resources [10].

Some new technical challenges will also be raised when physical layer security are applied into the burgeoning wireless networks, such as high-speed mobile networks, device to device communications, cognitive radio networks, and IoT. For example, in high-speed mobile networks as representative Internet of Vehicles and railway communication systems, the rapid changes of wireless channels and terminal positions require to propose fast CSI evaluation schemes and dynamic authentication frameworks. In device to device communications, due to direct communications between two mobile users without the supports of base stations or core networks, it is more difficult to establish a secure and reliable connection. Cognitive radio technique, as a promising technique to alleviate spectrum scarcity, has inherent vulnerabilities in physical layer spectrum sensing, such as the harmful interference from secondary users and the impersonation attack of disguised secondary users. To detect the disguised secondary users and to mitigate secondary interference, the terminals in cognitive radio networks should have the ability of autonomous learning. Machine learning is a powerful tool that can bring inspirations to cope with the potential challenges. IoT has a lot of particular characteristics, such as a massive number of devices, low-cost hardware, limited battery capacity, weak computation ability, and distinct service scenarios, all of which bring unprecedented challenges in implementing physical layer security.

VIII. Conclusion

It is believed that physical layer security is a promising technology to strengthen the secrecy of confidential information delivery in many emerging wireless networks in which the information security has not been well solved by the conventional cryptographic methods. To understand the advantages of physical layer security, a comparison is first made between this security technology and the conventional cryptographic encryption. Then, the survey mainly focuses on providing a comprehensive overview on the optimization and design of physical-layer security transmission. The typical wiretap channel models are introduced to cover common scenarios and systems in physical layer security. The research topics in this field are summarized from secure resource allocation, beamforming/precoding, and antenna/node selection and cooperation. Towards these research topics, we then discuss the performance metrics and fundamental optimization problems raised in the system optimization and design, which involve the secrecy rate/capacity, secrecy outage probability/capacity, power/energy consumption, and secure EE. The practical significance and applied scenarios of the metrics are also investigated in the survey. Each research topic of physical-layer security designs involves using these performance metrics to formulate optimization problems according to specific application conditions. Thereafter, the state of the art of optimization and design in physical layer security is reviewed from the perspectives of the aforementioned research topics. In each research topic, the great efforts are presented from four categories of fundamental optimization problems, such as maximization of achievable secrecy rate, minimization of secrecy outrage probability, minimization of power consumption, and maximization of secure EE. Numerous optimization approaches and solution schemes are investigated in the survey to tackle different problems in security designs.

One of the major issues in the physical-layer security designs is the imperfect CSI problem. To achieve the optimal performance of system designs, the transmitters need to know the CSI of both the legitimate users and the eavesdroppers. However, in practice, getting the perfect CSI of the eavesdroppers is very difficult or even impossible. This problem exists in all research topics of physical-layer security designs. In the survey, we review the existing assumptions of CSI which have been considered in physical layer security, while we discuss three ways to characterize the uncertainties of the imperfect eavesdropper's CSI. It is observed that, to cope with the problems of the imperfect or unknown CSI of eavesdroppers, the robust security designs, probabilistic view of security, or

QoS-based optimization is usually considered in physical layer security to get a compromise solution. In addition, we discuss possible future trends and open challenges from the aspects involving the problems of imperfect CSI, eavesdropper models, and hardware impairments, as well as cross-layer security designs, global performance optimizations, and commercial application of physical layer security.

REFERENCES

[1] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*. New York, NY, USA: Pearson Educ. Inc., 2011.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends® Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, Apr. 2009.

[4] C. E. Shanon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Apr. 1949.

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

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

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

[8] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[9] 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.

[10] 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.

[11] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[12] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[13] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[14] 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.

[15] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[16] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint physical-application layer security for wireless multimedia delivery," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 66–72, Mar. 2014.

[17] 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.

[18] L. J. Rodriguez *et al.*, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[19] N. Yang *et al.*, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

[21] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[22] 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.

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

[24] H. Lee, C. Song, J. Moon, and I. Lee, "Precoder designs for MIMO Gaussian multiple access wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8563–8568, Sep. 2017.

[25] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[26] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 640–649, Sep. 2011.

[27] Z. Kong *et al.*, "Iterative distributed minimum total MSE approach for secure communications in MIMO interference channels," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 594–608, Mar. 2016.

[28] 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.

[29] 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.

[30] 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.

[31] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[32] G. Song and Y. Li, "Utility-based resource allocation and scheduling in OFDM-Based wireless broadband networks," *IEEE Commun. Mag.*, vol. 43, no. 12, pp. 127–134, Dec. 2005.

[33] B. Bai, W. Chen, and Z. Cao, "Outage optimal subcarrier allocation for downlink secure OFDMA systems," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM) Workshops*, Austin, TX, USA, Dec. 2014, pp. 1320–1325.

[34] A. Jindal and R. Bose, "Resource allocation for secure multicarrier AF relay system under total power constraint," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 231–234, Feb. 2015.

[35] 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.

[36] 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.

[37] I. Krikidis, J. S. Thompson, P. M. Grant, and S. McLaughlin, "Power allocation for cooperative-based jamming in wireless networks with secrecy constraints," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM) Workshops*, Dec. 2010, pp. 1177–1181.

[38] 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.

[39] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[40] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[41] 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.

[42] 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.

[43] 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.

[44] J.-H. Lee, "Optimal power allocation for physical layer security in multi-hop DF relay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 28–38, Jan. 2016.

[45] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.

[46] A. Benfarah, S. Tomasin, and N. Laurenti, "Power allocation in multiuser parallel Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2326–2339, Jun. 2016.

[47] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Wireless Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[48] 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.

[49] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1714–1725, Oct. 2016.

[50] S. Karachontzitis, S. Timotheou, I. Krikidis, and K. Berberidis, "Security-aware max–min resource allocation in multiuser OFDMA downlink," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 529–542, Mar. 2015.

[51] 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.

[52] 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.

[53] Z. Liu, C. Chen, L. Bai, H. Xiang, and J. Choi, "Transmit power minimization beamforming via amplify-and-forward relays in wireless networks with multiple eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 4698–4703.

[54] 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.

[55] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[56] P. Zhao, M. Zhang, H. Yu, H. Luo, and W. Chen, "Robust beamforming design for sum secrecy rate optimization in MU-MISO networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1812–1823, Sep. 2015.

[57] G. Zheng, P.-D. Arapoglou, and B. Ottersten, "Physical layer security in multibeam satellite systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 852–863, Feb. 2012.

[58] 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.

[59] 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.

[60] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[61] 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.

[62] 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.

[63] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multi-cell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 1286–1291, Sep. 2014.

[64] D. Wang, B. Bai, W. Chen, and Z. Han, "Energy efficient secure communication over decode-and-forward relay channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 892–905, Mar. 2015.

[65] C. R. Murthy, A. K. Jagannatham, and B. D. Rao, "Training-based and semiblind channel estimation for MIMO systems with maximum ratio transmission," *IEEE Trans. Signal Process.*, vol. 54, no. 7, pp. 2546–2558, Jul. 2006.

[66] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[67] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 229–238, Jan. 2013.

[68] M. F. Hanif, L. N. Tran, M. Juntti, and S. Glisic, "On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks," *IEEE Trans. Signal Process.*, vol. 62, no. 14, pp. 3536–3551, Jul. 2014.

[69] 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.

[70] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[71] 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.

[72] R. Liu and H. V. Poor, "Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.

[73] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[74] S. A. A. Fakoorian and A. L. Swindlehurst, "Dirty paper coding versus linear GSVD-based precoding in MIMO broadcast channel with confidential messages," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Houston, TX, USA, Dec. 2011, pp. 1–5.

[75] 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.

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

[77] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, USA, Jul. 2012, pp. 2321–2325.

[78] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[79] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[80] 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.

[81] N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Confidential broadcasting via linear precoding in non-homogeneous MIMO multiuser networks," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2515–2530, Jul. 2014.

[82] B. He, N. Yang, X. Zhou, and J. Yuan, "Base station cooperation for confidential broadcasting in multi-cell networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5287–5299, Oct. 2015.

[83] 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.

[84] 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.

[85] 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. 2012.

[86] N. Romero-Zurita, M. Ghogho, and D. Mclernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[87] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[88] 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.

[89] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[90] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2015.

[91] 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.

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

[93] M. F. Hanif, "Efficient algorithm for selecting secrecy rate maximizing antennas," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1818–1821, Sep. 2013.

[94] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[95] 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.

[96] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[97] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.

[98] 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.

[99] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[100] Y. Hu and X. Tao, "Secrecy outage on transmit antenna selection with weighting errors at maximal-ratio combiners," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 597–600, Apr. 2015.

[101] S. N. Diggavi, N. Al-Dhahir, A. Stamoulis, and A. R. Calderbank, "Great expectations: The value of spatial diversity in wireless networks," *Proc. IEEE*, vol. 92, no. 2, pp. 219–270, Feb. 2004.

[102] S.-I. Kim, I.-M. Kim, and J. Heo, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3724–3737, Jul. 2015.

[103] 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.

[104] 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.

[105] D. Christopoulos, S. Chatzinotas, and B. Ottersten, "Multicast multigroup precoding and user scheduling for frame-based satellite communications," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4695–4707, Sep. 2015.

[106] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5051, Dec. 2015.

[107] A. Mukherjee and A. L. Swindlehurst, "User selection in multiuser MIMO systems with secrecy considerations," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2009, pp. 1479–1482.

[108] M. Pei, A. L. Swindlehurst, D. Ma, and J. Wei, "On ergodic secrecy rate for MISO wiretap broadcast channels with opportunistic scheduling," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 50–53, Jan. 2014.

[109] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[110] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[111] 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.

[112] W. Wang, K. C. Teh, and K. H. Li, "Generalized relay selection for improved security in cooperative DF relay networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 28–31, Feb. 2015.

[113] 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.

[114] N. Nomikos *et al.*, "Relay selection for secure 5G green communications," *Telecommun. Syst.*, vol. 59, no. 1, pp. 169–187, Jan. 2015.

[115] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[116] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

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

[118] J. H. Lee and C. Wan, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure DoF and jammer scaling law," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 828–839, Feb. 2014.

[119] C. Wang, H.-M. Wang, X.-G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596–2612, May 2015.

[120] C. Wang and H.-M. Wang, "Opportunistic jamming for enhancing security: Stochastic geometry modeling and analysis," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10213–10217, Dec. 2016.

[121] 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.

[122] X. He and A. Yener, "The role of an untrusted relay in secret communication," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, Jul. 2008, pp. 2212–2216.

[123] 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.

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

[125] A. Mukherjee, "Imbalanced beamforming by a multi-antenna source for secure utilization of an untrusted relay," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1309–1312, Jul. 2013.

[126] H. Khodakarami and F. Lahouti, "Link adaptation with untrusted relay assignment: Design and performance analysis," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4874–4883, Dec. 2013.

[127] 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.

[128] J. Richter, C. Scheunert, S. Engelmann, and E. A. Jorswieck, "Weak secrecy in the multiway untrusted relay channel with compute-and-forward," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1262–1273, Jun. 2015.

[129] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[130] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, New Orleans, LO, USA, Nov. 2008, pp. 1–5.

[131] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[132] 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.

[133] 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.

[134] N.-E. Wu and H.-J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 415–418, Aug. 2013.

[135] 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.

[136] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[137] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.

[138] N. Zhang *et al.*, "Partner selection and incentive mechanism for physical layer security," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4265–4276, Aug. 2015.

[139] W. Y. Luo, L. Jin, K. Z. Huang, and Z. Zhong, "User selection and resource allocation for secure multiuser MISO-OFDMA systems," *Electron. Lett.*, vol. 47, no. 15, pp. 884–886, Jul. 2011.

[140] X. Zhu *et al.*, "Cross-layer scheduling for OFDMA-based cognitive radio systems with delay and security constraints," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5919–5934, Dec. 2015.

[141] M. Hanif, M. Juntti, and L. N. Tran, "Antenna selection with erroneous covariance matrices under secrecy constraints," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 414–420, Jan. 2016.

[142] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *J. Commun. Netw.*, vol. 14, no. 4, pp. 364–373, Aug. 2012.

[143] 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.

[144] 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.

[145] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141–144, Feb. 2013.

[146] Y. Liu and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[147] J. Yang, I.-M. Kim, and D. I. Kim, "Joint design of optimal cooperative jamming and power allocation for linear precoding," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3285–3298, Sep. 2014.

[148] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[149] H. H. Kha, H. D. Tuan, and H. H. Nguyen, "Joint optimization of source power allocation and cooperative beamforming for SC-FDMA multi-user multi-relay networks," *IEEE Trans. Commun.*, vol. 61, no. 6, pp. 2248–2259, Jun. 2013.

[150] 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.

[151] C. Wang, H.-M. Wang, D. W. K. Ng, X. G. Xia, and C. Liu, "Joint beamforming and power allocation for secrecy in peer-to-peer relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.

[152] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[153] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[154] 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.

[155] 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.

[156] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[157] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[158] S. Bashar, Z. Ding, and Y. G. 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.

[159] 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.

[160] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 762–771, Mar. 2011.

[161] X. Zhou, M. R. Mckay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[162] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.

[163] 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/CIC Int. Conf. Commun. China (ICCC)*, Shanghai, China, Oct. 2014, pp. 385–390.

[164] S. Cui, A. J. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1089–1098, Aug. 2004.

[165] C. Jiang and L. J. Cimini, "Antenna selection for energy-efficient MIMO transmission," *IEEE Commun. Lett.*, vol. 1, no. 6, pp. 577–580, Dec. 2012.

[166] A. G. Marques, G. B. Giannakis, F. F. Digham, and F. J. Ramos, "Power-efficient wireless OFDMA using limited-rate feedback," *IEEE Trans. Wireless Commun.*, vol. 7, no. 2, pp. 685–696, Feb. 2008.

[167] J. Joung and S. Sun, "Power efficient resource allocation for downlink OFDMA relay cellular networks," *IEEE Trans. Signal Process.*, vol. 60, no. 5, pp. 2447–2459, May 2012.

[168] C. Comaniciu, H. V. Poor, and R. Zhang, "An information theoretic framework for energy efficient secrecy," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Vancouver, BC, Canada, May 2013, pp. 2906–2910.

[169] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, "Transmission with energy harvesting nodes in fading wireless channels: Optimal policies," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1732–1743, Sep. 2011.

[170] J. Lei, Z. Han, M. A. Vazquez-Castro, and A. Hjorungnes, "Secure satellite communication systems design with individual secrecy rate constraints," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 661–671, Sep. 2011.

[171] J. Li, A. P. Petropulu, and S. Weber, "Transmit power minimization under secrecy capacity constraint in cooperative wireless communications," in *Proc. IEEE/SP 15th Workshop Stat. Signal Process.*, Cardiff, U.K., Aug. 2009, pp. 217–220.

[172] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861–1874, May 2016.

[173] 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.

[174] M. C. Gursoy, "Secure communication in the low-SNR regime," *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 1114–1123, Apr. 2012.

[175] C. Comaniciu and H. V. Poor, "On energy-secrecy tradeoffs for Gaussian wire-tap channels," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 314–323, Feb. 2013.

[176] R. Mahapatra, Y. Nijsure, G. Kaddoum, N. U. Hassan, and C. Yuen, "Energy efficiency tradeoff mechanism towards wireless green communication: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 686–705, 1st Quart., 2016.

[177] D. Feng *et al.*, "A survey of energy-efficient wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 167–178, 1st Quart., 2013.

[178] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation in multi-cell OFDMA systems with limited backhaul capacity," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3618–3631, Oct. 2012.

[179] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phys. Commun.*, vol. 25, pp. 14–25, Dec. 2017.

[180] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[181] J. M. Hamamreh, E. Basar, and H. Arslan, " OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.

[182] J. M. Hamamreh, H. M. Furqan, Z. Ali, and G. A. S. Sidhu, "Enhancing the security performance of OSTBC using pre-equalicodization," in *Proc. Int. Conf. Front. Inf. Technol. (FIT)*, Islamabad, Pakistan, Dec. 2017, pp. 294–298.

[183] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, Apr. 2016.

[184] N. Mokari, S. Parsaeefard, H. Saeedi, P. Azmi, and E. Hossain, "Secure robust ergodic uplink resource allocation in relay-assisted cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 63, no. 2, pp. 291–304, Jan. 2015.

[185] D. P. Palomar and M. Chiang, "A tutorial on decomposition methods for network utility maximization," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1439–1451, Aug. 2006.

[186] X. Wang, Y. Chen, L. Cai, and J. Pan, "Minimizing secrecy outage probability in multiuser wireless systems with stochastic traffic," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6449–6460, Jul. 2017.

[187] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[188] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

[189] B. He and X. Zhou, "On the placement of RF energy harvesting node in wireless networks with secrecy considerations," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM) Workshops*, Austin, TX, USA, Dec. 2014, pp. 1355–1360.

[190] H. Yu, S. Guo, and Y. Yang, "An optimization framework of target secrecy rate and power allocation for SWIPT system," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–6.

[191] J. Chen, X. Chen, and W. Gerstacker, "Optimal power allocation for a massive MIMO relay aided secure communication," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Feb. 2015, pp. 1–6.

[192] B. Akgun, O. O. Koyluoglu, and M. Krunz, "Exploiting full-duplex receivers for achieving secret communications in multiuser MISO networks," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 956–968, Feb. 2017.

[193] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct. 2017.

[194] Y. Wu, K. Guo, J. Huang, and X. S. Shen, "Secrecy-based energy-efficient data offloading via dual connectivity over unlicensed spectrums," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3252–3270, Dec. 2016.

[195] M. El-Halabi, T. Liu, and C. N. Georghiades, "Secrecy capacity per unit cost," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1909–1920, Sep. 2013.

[196] M. M. Butt, E. A. Jorswieck, and B. Ottersten, "Maximizing energy efficiency in multiple access channels by exploiting packet dropping and transmitter buffering," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4129–4141, Aug. 2015.

[197] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Energy-efficient secure communications in MISO-SE systems," in *Proc. 48th Asilomar Conf. Signals Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2014, pp. 1001–1005.

[198] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1462–1477, Dec. 2016.

[199] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Optimal energy-efficient design of confidential multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 237–252, Jan. 2018.

[200] H. Q. Ta and S. W. Kim, "Adapting rate and power for maximizing secrecy energy efficiency," *IEEE Commun. Lett.*, vol. 21, no. 9, pp. 2049–2052, Sep. 2017.

[201] J. Farhat, G. Brante, R. D. Souza, and J. L. Rebelatto, "Energy efficiency of repetition coding and parallel coding relaying under partial secrecy regime," *IEEE Access*, vol. 4, pp. 7275–7288, 2016.

[202] F. Gabry, A. Zappone, R. Thobaben, E. A. Jorswieck, and M. Skoglund, "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 437–440, Aug. 2015.

[203] X. Xu *et al.*, "Energy-efficient optimization for physical layer security in large-scale random CRNs," in *Proc. Int. Conf. Wireless Commun. Signal Process.*, Nanjing, China, Oct. 2015, pp. 1–6.

[204] J. Ouyang, W.-P. Zhu, D. Massicotte, and M. Lin, "Energy efficient optimization for physical layer security in cognitive relay networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[205] R. Zhang, C. Comaniciu, and H. V. Poor, "Outage capacity and partial secrecy for energy efficient physical layer security in Gaussian fading channels," in *Proc. 16th Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Atlantic City, NJ, USA, Jun. 2013, pp. 1–5.

[206] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706–2722, Oct. 2016.

[207] Y. Kwon, H. Suh, J. Oh, and T. Hwang, "Energy efficient communication for secure D2D underlaid cellular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9110–9123, Oct. 2017.

[208] W. Dinkelbach, "On nonlinear fractional programming," *Manag. Sci.*, vol. 13, no. 7, pp. 492–498, Mar. 1967.

[209] S. Schaible, "Fractional programming II : On Dinkelbach's algorithm," *Manag. Sci.*, vol. 22, no. 8, pp. 868–873, Apr. 1976.

[210] T. F. Coleman and A. R. Conn, "Nonlinear programming via an exact penalty function: Asymptotic analysis," *Math. Program.*, vol. 24, no. 1, pp. 137–161, 1982.

[211] M. S. Bazaraa, H. D. Sherali, and C. M. Shetty, *Nonlinear Programming: Theory and Algorithms*. Hoboken, NJ, USA: Wiley, 2013.

[212] J. Gorski, F. Pfeuffer, and K. Klamroth, "Biconvex sets and optimization with biconvex functions: A survey and extensions," *Math. Methods Oper.*, vol. 66, no. 3, pp. 373–407, Jun. 2007.

[213] U. Niesen, D. Shah, and G. W. Wornell, "Adaptive alternating minimization algorithms," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1423–1429, Mar. 2009.

[214] T. P. Dinh and H. A. L. Thi, "Recent advances in DC programming and DCA," in *Transactions on Computational Intelligence XIII* (LNCS 8342). Berlin, Germany: Springer, 2014, pp. 1–37.

[215] L. T. H. An, M. T. Belghiti, and P. D. Tao, "A new efficient algorithm based on DC programming and DCA for clustering," *J. Glob. Optim.*, vol. 37, no. 4, pp. 593–608, Aug. 2007.

[216] A. O. Hero, III, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[217] S. Gong, C. Xing, S. Chen, and Z. Fei, "Secure communications for dual-polarized MIMO systems," *IEEE Trans. Signal Process.*, vol. 65, no. 16, pp. 4177–4192, Mar. 2017.

[218] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.

[219] W. Ai, Y. Huang, and S. Zhang, "New results on Hermitian matrix rank-one decomposition," *Math. Program.*, vol. 128, nos. 1–2, pp. 253–283, 2011.

[220] 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.

[221] M. R. A. Khandaker and K.-K. Wong, "Masked beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 40–54, Jan. 2015.

[222] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, Feb. 2010.

[223] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.

[224] C. Liu and R. Malaney, "Location-based beamforming and physical layer security in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7847–7857, Nov. 2016.

[225] Y. R. Ramadan, H. Minn, and A. S. Ibrahim, "Hybrid analog–digital precoding design for secrecy mmWave MISO-OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 65, no. 11, pp. 5009–5026, Nov. 2017.

[226] J.-M. Kang, J. Yang, J. Ha, and I.-M. Kim, "Joint design of optimal precoding and cooperative jamming for multiuser secure broadcast systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10551–10556, Nov. 2017.

[227] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[228] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[229] Z. Zhu, Z. Chu, Z. Wang, and I. Lee, "Outage constrained robust beamforming for secure broadcasting systems with energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7610–7620, Nov. 2016.

[230] H. Zhang, Y. Huang, C. Li, and L. Yang, "Secure beamforming design for SWIPT in MISO broadcast channel with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7807–7819, Nov. 2016.

[231] Z. Zhu *et al.*, "Beamforming and power splitting designs for AN-aided secure multi-user MIMO SWIPT systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2861–2874, Dec. 2017.

[232] D. W. K. Ng and R. Schober, "Resource allocation for secure communication in systems with wireless information and power transfer," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM) Workshops*, Atlanta, GA, USA, Dec. 2013, pp. 1251–1257.

[233] S. Leng, D. W. K. Ng, and R. Schober, "Power efficient and secure multiuser communication systems with wireless information and power transfer," in *Proc. IEEE Int. Conf. Commun. (ICC) Workshops*, Sydney, NSW, Australia, Jun. 2014, pp. 800–806.

[234] 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.

[235] D. W. K. Ng, L. Xiang, and R. Schober, "Multi-objective beamforming for secure communication in systems with wireless information and power transfer," in *Proc. IEEE 24th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, London, U.K., Sep. 2013, pp. 7–12.

[236] 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.

[237] O. Tervo, H. Pennanen, D. Christopoulos, S. Chatzinotas, and B. Ottersten, "Distributed optimization for coordinated beamforming in multicell multigroup multicast systems: Power minimization and SINR balancing," *IEEE Trans. Signal Process.*, vol. 66, no. 1, pp. 171–185, Jun. 2018.

[238] H. Zhang, P. Sun, C. Li, Y. Huang, and L. Yang, "Cooperative precoding for wireless energy transfer and secure cognitive radio coexistence systems," *IEEE Signal Process. Lett.*, vol. 24, no. 5, pp. 540–544, May 2017.

[239] D. W. K. Ng, E. S. Lo, and R. Schober, "Multi-objective 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.

[240] A. Beck, A. Ben-Tal, and L. Tetruashvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *J. Glob. Optim.*, vol. 47, no. 1, pp. 29–51, May 2010.

[241] A. Canelas, M. Carrasco, and J. López, "Application of the sequential parametric convex approximation method to the design of robust trusses," *J. Glob. Optim.*, vol. 68, no. 1, pp. 169–187, May 2017.

[242] Y. Nesterov, "Semidefinite relaxation and nonconvex quadratic optimization," *Optim. Methods Softw.*, vol. 9, nos. 1–3, pp. 141–160, 1998.

[243] N. T. Nghia, H. D. Tuan, T. Q. Duong, and H. V. Poor, "MIMO beamforming for secure and energy-efficient wireless communication," *IEEE Signal Process. Lett.*, vol. 24, no. 2, pp. 236–239, Feb. 2017.

[244] W. Mei, Z. Chen, and J. Fang, "Robust energy-efficient transmit design for MISOME wiretap channels," in *Proc. IEEE Glob. Conf. Signal Inf. Process. (GlobalSIP)*, Washington, DC, USA, Dec. 2016, pp. 981–985.

[245] 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 Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Shanghai, China, Mar. 2016, pp. 3496–3500.

[246] W. Mei, Z. Chen, and J. Fang, "Artificial noise aided energy efficiency optimization in MIMOME system with SWIPT," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1795–1798, Aug. 2017.

[247] H. Alves, M. D. C. Tomé, P. H. J. Nardelli, C. H. M. D. Lima, and M. Latva-Aho, "Enhanced transmit antenna selection scheme for secure throughput maximization without CSI at the transmitter," *IEEE Access*, vol. 4, pp. 4861–4873, 2016.

[248] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Boston, MA, USA: Springer, 2010.

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

[250] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with finite-alphabet input," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 912–915, May 2013.

[251] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.

[252] 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.

[253] 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 2014.

[254] M. Lin, J. Ge, Y. Yang, and Y. Ji, "Joint cooperative beamforming and artificial noise design for secrecy sum rate maximization in two-way AF relay networks," *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 380–383, Feb. 2014.

[255] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[256] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[257] R. Zhao *et al.*, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 546–559, Feb. 2018.

[258] H. Lei *et al.*, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.

[259] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2015.

[260] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2189–2203, Apr. 2014.

[261] Z. Lin, Y. Cai, W. Yang, and L. Wang, "Robust secure switching transmission in multi-antenna relaying systems: Cooperative jamming or decode-and-forward beamforming," *IET Commun.*, vol. 10, no. 13, pp. 1673–1681, Sep. 2016.

[262] Q.-T. Vien, T. A. Le, and T. Q. Duong, "Opportunistic secure transmission for wireless relay networks with modify-and-forward protocol," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.

[263] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[264] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy outage minimization for wireless powered communication networks with an energy harvesting jammer," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–5.

[265] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 764–774, Feb. 2017.

[266] A. Mabrouk, A. E. Shafie, K. Tourki, and N. Al-Dhahir, "An-aided relay-selection scheme for securing untrusted RF-EH relay systems," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 4, pp. 481–493, Dec. 2017.

[267] J. Farhat, G. Brante, and R. D. Souza, "On the secure energy efficiency of TAS/MRC with relaying and jamming strategies," *IEEE Signal Process. Lett.*, vol. 24, no. 8, pp. 1228–1232, Aug. 2017.

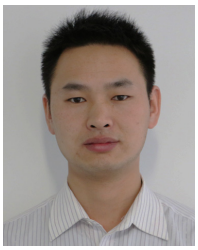
[268] L. Wang, L.-L. Yang, V. C. M. Schober, and M. Song, "Adaptive cooperation schemes for energy efficient physical layer security," in *Proc. IEEE INFOCOM Workshops*, Toronto, ON, Canada, Apr. 2014, pp. 159–160.

[269] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[270] L. Wang, K.-K. Wong, M. Elkashlan, A. Nallanathan, and S. Lambotharan, "Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1375–1389, Dec. 2016.

[271] J. Chen, X. Chen, T. Liu, and L. Lei, "Toward green and secure communications over massive MIMO relay networks: Joint source and relay power allocation," *IEEE Access*, vol. 5, pp. 869–880, 2017.

[272] Y. Kwon, X. Wang, and T. Hwang, "A game with randomly distributed eavesdroppers in wireless ad hoc networks: A secrecy EE perspective," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 9916–9930, Nov. 2017.
[273] J. Li, A. P. Petropulu, and H. V. Poor, "Cooperative transmission for relay networks based on second-order statistics of channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1280–1291, Mar. 2011.
[274] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 684–702, Jun. 2003.
[275] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage constrained robust secure transmission for MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558–5570, Oct. 2014.
[276] 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.
[277] G. Brante, H. Alves, R. D. Souza, and M. Latva-Aho, "Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1330–1342, Apr. 2015.
[278] P. Kyritsi, D. C. Cox, R. A. Valenzuela, and P. W. Wolniansky, "Correlation analysis based on MIMO channel measurements in an indoor environment," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 713–720, Jun. 2003.
[279] X. He *et al.*, "The security of link signature: A view from channel models," in *Proc. IEEE Conf. Commun. Netw. Security*, San Francisco, CA, USA, Oct. 2014, pp. 103–108.
[280] Y. Liang, H. V. Poor, and L. Ying, "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 682–692, Sep. 2011.
[281] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.
[282] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 885–899, Feb. 2017.
[283] E. Boshkovska, D. W. K. Ng, L. Dai, and R. Schober, "Power-efficient and secure WPCNs with hardware impairments and non-linear EH circuit," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2642–2657, Jun. 2018.
[284] E. Bjornson, M. Matthaiou, and M. Debbah, "A new look at dual-hop relaying: Performance limits with hardware impairments," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4512–4525, Nov. 2013.
[285] U. Gustavsson, C. Sanchéz-Perez, T. Eriksson, and F. Athley, "On the impact of hardware impairments on massive MIMO," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM) Workshops*, Austin, TX, USA, Dec. 2014, pp. 294–300.



Dong Wang received the B.S. degree from Chongqing Communication College, Chongqing, China, in 2003, the M.S. degree from the New Star Research Institute of Applied Technology, Hefei, China, in 2010, and the Ph.D. degree from the Department of Electronic Engineering from Tsinghua University, Beijing, China, in 2016. He is currently with the New Star Research Institute of Applied Technology.

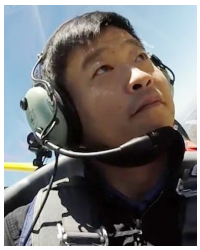
His research interests include information security and cooperative communication. He served as a Reviewer for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE ICCS 2014, and *China Communications*.

Bo Bai (S'09–M'11–SM'17) received the B.S. degree (Highest Hons.) from the School of Communication Engineering, Xidian University, Xi'an, China, in 2004 and the Ph.D. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2010. He was a Research Assistant from 2009 to 2010 and a Research Associate from 2010 to 2012 with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology. From 2012 to 2017, he was an Assistant Professor with the Department of Electronic Engineering, Tsinghua University. He has obtained the support from Backbone Talents Supporting Project of Tsinghua University. He is currently a Senior Researcher with the Future Network Theory Laboratory, 2012 Labs, Huawei Technologies Company, Ltd., Hong Kong, where he is leading a team to develop fundamental principles, algorithms, and systems for graph learning, cell-free mobile networking and edge computing, AI-enabled networking, and quantum Internet. He was a recipient of the Honor of Outstanding Graduates of Shaanxi Province and the Honor of Young Academic Talent of Electronic Engineering in Tsinghua University.

He has authored over 90 papers in major IEEE/ACM journals and conferences, two book chapters, and one textbook. He was a recipient of the Student Travel Grant at IEEE Globecom 2009 and the Best Paper Award in IEEE ICC 2016. He is one of the founded vice chairs of IEEE TCCN SIG on Social Behavior Driven Cognitive Radio Networks. He served as a Committee Member in IEEE ComSoc WTC and IEEE ComSoc SPCE. He served as the TPC Co-Chair of IEEE Infocom 2018—1st AoI Workshop, IEEE Infocom 2019—2nd AoI Workshop, and IEEE ICCC 2018, and an Industrial Forum and Exhibition Co-Chair of IEEE HotICN 2018. He also served as a TPC Member for several IEEE conferences, such as ICC, Globecom, WCNC, VTC, and ICCC. He served as a reviewer for a number of major IEEE/ACM journals and conferences. He was invited as a Young Scientist Speaker at IEEE TTM 2011. He is a USENIX Member.

Wenbo Zhao received the B.S. degree in electronic engineering and the M.S. degree in operations research from the New Star Research Institute of Applied Technology, Hefei, China, in 1994 and 1997, respectively, and the Ph.D. degree in pattern recognition and intelligent systems from the University of Science and Technology of China, Hefei, in 2003. He is currently a Professor with the New Star Research Institute of Applied Technology.

His research interests include moving target tracking, radar data processing, and statistical signal processing.



Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer of JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, ID, USA. He is currently a Professor with the Electrical and Computer Engineering Department as well as with the Computer Science Department, University of Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He was a recipient of the NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the *Journal on Advances in Signal Processing* in 2015, the IEEE Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award in IEEE JSAC) in 2016, and Several Best Paper Awards in IEEE conferences. He is currently an IEEE Communications Society Distinguished Lecturer.