Rethinking Secure Precoding via Interference Exploitation: A Smart Eavesdropper Perspective

Qian Xu, *Graduate Student Member, IEEE*, Pinyi Ren, *Member, IEEE*, and A. Lee Swindlehurst, *Fellow, IEEE*

***Abstract*— Based on the concept of constructive interference (CI), multiuser interference (MUI) has recently been shown to be beneficial for communication secrecy. A few CI-based secure precoding algorithms have been proposed that use both the channel state information (CSI) and knowledge of the instantaneous transmit symbols. In this article, we examine the CI-based secure precoding problem with a focus on smart eavesdroppers that exploit statistical information gleaned from the precoded data for symbol detection. Moreover, the impact of correlation between the main and eavesdropper channels is taken into account. We first modify an existing CI-based precoding scheme to better utilize the destructive impact of the interference. Then, we point out the drawback of both the existing and the new modified CI-based precoders when faced with a smart eavesdropper. To address this deficiency, we provide a general principle for precoder design and then give two specific design examples. Finally, the scenario where the eavesdropper's CSI is unavailable is studied. Numerical results show that although our modified CI-based precoder can achieve a better energy-secrecy trade-off than the existing approach, both have a limited secrecy benefit. On the contrary, the precoders developed using the new CI-design principle can achieve a much improved tradeoff and significantly degrade the eavesdropper's performance.**

***Index Terms*— Physical layer security, constructive interference, secure precoding, symbol-level precoding.**

I. Introduction

MULTIUSER interference (MUI) is usually considered harmful for downlink multiuser communication systems. The MUI can greatly limit the achievable rate of each user especially for a dense cellular network with many users. One common approach to address MUI is multiuser precoding [1]–[4], which typically employs a linear precoder at the transmitter to suppress or completely remove the MUI at each user's receiver. Zero-forcing is a common technique to eliminate MUI [1], but it can lead to noise amplification in certain scenarios. As an alternative, signal-to-leakage-and-noise ratio can be chosen as the design metric [2], which leads to a closed-form result. For other approaches, the precoders are generally obtained by solving one or two kinds of optimization problems: maximizing the sum rate under a total power constraint (e.g., [3]) or minimizing transmit power under a quality of service (QoS) requirement at each user (e.g., [4]).

Instead of suppressing MUI, recent research [5] suggests that known interference can be exploited as a useful source for improving the received signal power. According to [5], the interference is regarded as constructive interference (CI) if it contributes to a power enhancement of the desired symbol; otherwise, it is destructive. By exploiting the information about the symbols to be transmitted and the channel state, the MUI can be designed in some cases to be constructive for the desired users. Following this idea, an increasing number of studies on CI-based precoding have been proposed [6]–[10], where [6]–[8] focused on regular multiple-input multiple-output (MIMO) systems, while [9], [10] considered massive MIMO systems with low-resolution digital-to-analog converters. These CI-based approaches can reduce the required transmit power to achieve a certain level of performance, especially when the system is heavily loaded. However, they are mainly useful for simple constellation designs like phase-shift keying (PSK), and they require symbol-level precoding, which is more complex.

In recent years, there has been a growing interest in improving the security of wireless communications systems. Physical layer security (PLS) [11] is a technique that exploits the randomness of wireless channels to achieve secure transmission. Through an appropriate design of the transmit signal, PLS techniques can be used to minimize the power of the eavesdropper's received signal while guaranteeing a certain detection performance at the desired user [12]–[16]. CI-based precoding already benefits secrecy since it can achieve the same performance for a given link with reduced transmit power, which already reduces an eavesdropper's ability to decode the sensitive data. There has been some prior work that employs a CI-based approach to improve communication secrecy [17]–[22]. In [17], [18], CI-based secure precoding algorithms were proposed to achieve energy-efficient secure message transmission and secure simultaneous wireless information and power transfer (SWIPT), respectively, assuming single-antenna eavesdroppers. Specifically, with the channel

Manuscript received July 29, 2019; revised May 5, 2020; accepted August 7, 2020. Date of publication August 14, 2020; date of current version September 3, 2020. The work of Qian Xu and Pinyi Ren was supported in part by the National Natural Science Foundation of China under Grant 61941119 and Grant 61431011 and in part by the Fundamental Research Funds for the Central Universities. The work of A. Lee Swindlehurst was supported by the U.S. National Science Foundation under Grant CCF-2008724. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Loukas Lazos. *(Corresponding author: Pinyi Ren.)*

Qian Xu and Pinyi Ren are with the School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China, and also with the Shaanxi Smart Networks and Ubiquitous Access Research Center, Xi'an 710049, China (e-mail: xq1216@stu.xjtu.edu.cn; pyren@mail.xjtu.edu.cn).

A. Lee Swindlehurst is with the Center for Pervasive Communications and Computing, University of California at Irvine, Irvine, CA 92697 USA (e-mail: swindle@uci.edu).

Digital Object Identifier 10.1109/TIFS.2020.3016836

state information (CSI) available of all users' channels, a constructive-destructive (C-D) interference-based secure precoding method[1] was proposed, which exploits the MUI to push the legitimate user's received signal into the constructive region for the desired symbol, and push the eavesdropper's noise-free received signal outside the constructive region. Similar ideas were exploited in [19], [20] to address security in distributed antenna systems with channel estimation error. To handle channel uncertainty, the work in [19] proposed a deterministic robust optimization algorithm while the work in [20] proposed a probabilistic optimization method. It was shown that distributed antenna systems with antenna selection and CI can significantly reduce power consumption, compared with centralized antenna systems. The authors in [21] extended the works in [19], [20] to the scenario where the eavesdropper's CSI is unknown. Without the eavesdropper's CSI, a requirement on the minimum power level of the artificial noise (AN) was introduced. The authors in [22] studied a related problem with a multi-antenna eavesdropper that can obtain a better estimate of the transmitted symbol. Without the eavesdropper's CSI, several power-minimizing precoding algorithms were proposed.

Similar to [17], [18], in this article we study the centralized antenna system with single-antenna legitimate users and eavesdroppers. We focus on the detection performance at the eavesdropper rather than the secrecy rate, since CI-based precoding assumes simple fixed signal constellations such as PSK or quadrature amplitude modulation (QAM), which is related to the prior work on secure transmission with finite constellations [16]. It is important to note that the eavesdropper in [17]–[22] is assumed to adopt the same detection method as the legitimate user. For that simple detector, the detection rule is simply to choose the constellation point nearest the received signal. For this simple eavesdropper, the C-D precoding method in [17], [18] can yield very good secrecy performance since the eavesdropper's received signal is designed to be far away from the real transmitted symbol. However, if the eavesdropper can exploit the statistical characteristics of the received signal, a much better detection performance can be achieved. For example, for PSK modulation, the eavesdropper can exploit knowledge of the constellation used, the QoS parameters and the channel distribution to obtain a (possibly empirical) model for the conditional distribution of the received signal phase θ_e given the transmitted symbols. This information can then in turn be used to enable the eavesdropper to implement an optimal maximum likelihood (ML) detector. In this article, an eavesdropper that can learn and implement this ML detector is referred to as a *smart* eavesdropper. When faced with a smart eavesdropper, the C-D precoding algorithm may unexpectedly reveal the transmitted symbols. This is because the restriction on the location of the eavesdropper's received signal makes the distribution of θ_e non-uniform on $[0, 2\pi]$, which helps the eavesdropper distinguish different symbols.

[1]This precoding method is referred to as C-D precoding algorithm in the following paragraphs. The details of this precoder will be given in Section III-A.

To address the above issue, in this article we restudy CI-based secure precoding from the perspective of a smart eavesdropper. Furthermore, we consider a general scenario where the eavesdropper channel is possibly correlated with the main channel, which makes it easier for the eavesdropper to observe the desired symbol. We first review the C-D precoding algorithm in [17], [18]. It is observed that although the eavesdropper's noise-free received signal is kept outside the constructive region, the scheme in [17], [18] only exploits a part of the destructive region, which significantly increases the transmit power. Inspired by this observation, we propose an improved C-D precoding algorithm, which exploits the *full* destructive region and thus can save power. Then, we point out the drawback of the above C-D precoding strategies in the presence of a smart eavesdropper. To overcome the drawback, we propose another secure precoding method, which only limits the power of the eavesdropper's received signal without any constraints on the phase. Following this, a low-complexity secure precoding algorithm is also proposed. Finally, we study a more practical scenario where the eavesdropper's CSI is unavailable. The primary contributions of the paper are enumerated below.

1) We show that the C-D approach of [17], [18] only exploits a portion of the destructive region when designing the precoder.
2) We present a modification of the C-D approach of [17], [18] that exploits the full destructive region, and that is thus able to achieve the same level of security with less transmit power.
3) We show that, for PSK signals, the C-D precoding approach is susceptible to a smart eavesdropper that can derive the conditional distribution of the phase given the transmitted signals.
4) We present a new design principle for secure CI-based precoding that addresses this deficiency, and we propose two algorithms based on this principle to generate the precoder. While these new approaches will require an increase in transmit power compared with C-D precoding, they can achieve significantly improved security that approaches the best possible performance.
5) Unlike the methods above which assume availability of the eavesdropper's CSI, we develop an alternative algorithm that uses AN for the case where the eavesdropper's CSI is unavailable. Considering the possible channel correlation, in addition to the requirement on the minimum power level of the AN [17], [21], we also require that the power of the legitimate user's received signal be equal to the minimum level for successful detection. In this way, the power of the useful signal received at the eavesdropper can be minimized.
6) Although the study of a single smart eavesdropper is sufficient to illustrate how more intelligent eavesdropping can dramatically alter secrecy performance, we generalize our proposed schemes to the scenario with multiple eavesdroppers.

The rest of this article is organized as follows. Section II gives the system model and the basic idea for constructive

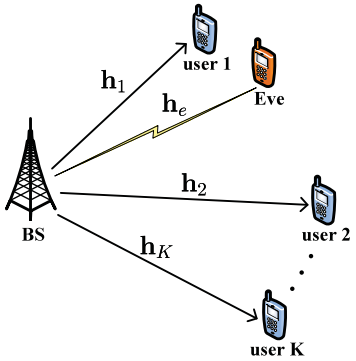


Fig. 1. System model: A downlink multiuser communication network with an eavesdropper attempting to get user 1's message.

interference. Section III first reviews the existing C-D precoding algorithm and then presents an improved version of the C-D precoding algorithm. Section IV introduces the smart eavesdropping approach and reveals the security risk of the C-D precoding methods. For mitigating smart eavesdropping, a general principle for designing a secure precoder is proposed. Then, two specific precoding algorithms are provided. Section V studies the scenario where the eavesdropper's CSI is unavailable. Section VI presents numerical results to evaluate the performance of all the precoding schemes, and finally Section VII concludes the paper.

Notations: In this article, bold upper-case letters denote matrices while bold lower-case letters denote vectors. The set of $M \times N$ complex matrices is denoted as $\mathbb{C}^{M\times N}$. For a vector $\mathbf{x}$, $\mathbf{x}^T$, $\mathbf{x}^H$, and $\|\mathbf{x}\|$ represent the transpose, Hermitian transpose, and l_2 norm of $\mathbf{x}$, respectively. For a scalar x, $|x|$ and x^* represent the l_2 norm and complex conjugate of x, respectively. $\mathbf{I}$ denotes the identity matrix while $\mathbf{1}_{N\times 1}$ represents an $N \times 1$ vector composed of all ones. Finally, $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Omega})$ denotes the complex circular Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Omega}$.

II. System Model

In this section, we first describe the system settings, including the signal constellations and channel models. Then, the basic idea of constructive interference is provided.

A. System Description

As illustrated in Fig. 1, we concentrate on downlink transmission in a single-cell multiuser system. The base station (BS), equipped with N antennas, simultaneously serves K single-antenna users using the same time-frequency resource. We consider a simple but typical scenario where a single eavesdropper (labeled as Eve), is located near one of the users (labeled as user 1) to try to wiretap the confidential message for this user. The other users are assumed to be ordinary users without a secure communication requirement.[2] Like the K users, the eavesdropper is also equipped with a single antenna.

[2]Note that our proposed schemes can be easily extended to the scenario where more than one user has secure communication requirements. However, to simplify the presentation, we only focus on achieving secure communication for user 1.

At the BS, each element of the symbol vector $\mathbf{s} = [s_1, \ldots, s_K]^T$, where s_k is the desired symbol for user k, is drawn from a normalized M-PSK constellation set $\mathcal{C}_M = \{c_m : m = 1, \cdots, M\}$ given by

$$c_m = \exp\left(j(2m-1)\Phi\right), \tag{1}$$

where $\Phi = \frac{\pi}{M}$. In addition, we assume that the BS has perfect CSI of the legitimate channel $\mathbf{H} = [\mathbf{h}_1, \cdots, \mathbf{h}_K]^T$, where $\mathbf{h}_k \in \mathbb{C}^{N\times 1}$ denotes the channel from the BS to user k. As for the eavesdropper channel $\mathbf{h}_e \in \mathbb{C}^{N\times 1}$, we first assume that full knowledge of $\mathbf{h}_e$ is available, which is a widely-adopted assumption in various studies on PLS [13]–[18]. This corresponds to the scenario where the eavesdropper is a registered user in the network but is to be prevented from intercepting sensitive messages [13], [14], [18]. The case where the information about $\mathbf{h}_e$ is unavailable will be studied in Section V. The BS designs the transmit signal vector $\mathbf{x} = \mathcal{P}(\mathbf{s}, \mathbf{H}, \mathbf{h}_e) \in \mathbb{C}^{N\times 1}$ based on the symbol vector and CSI, where the function $\mathcal{P}\{\cdot\}$ represents a general symbol-wise precoder which can be linear or non-linear.

The received signal at user k can be expressed as

$$y_k = \mathbf{h}_k^T \mathbf{x} + n_k, \tag{2}$$

where $n_k \sim \mathcal{CN}(0, 1)$ is additive white Gaussian noise at the receiver with normalized noise power; $\mathbf{h}_k \in \mathcal{CN}(\mathbf{0}, \beta_k \mathbf{I})$ is the complex channel vector with β_k modeling large-scale fading such as geometric attenuation and shadowing. Similarly, the received signal at the eavesdropper is given by

$$y_e = \mathbf{h}_e^T \mathbf{x} + n_e, \tag{3}$$

where $\mathbf{h}_e \in \mathcal{CN}(\mathbf{0}, \beta_e \mathbf{I})$ with β_e denoting the large-scale fading parameter and $n_e \sim \mathcal{CN}(0, 1)$. In this article, we focus on channels with receiver-side correlation, which is one of the biggest challenges for PLS-based security, since the similarity between the main and the eavesdropper channels makes secure transmission strategies [12]–[15] inefficient. Receiver-side correlation usually occurs for the scenario where the eavesdropper is located very close to the legitimate receiver. Moreover, we assume that the strength of the receiver-side correlation for each BS transmit antenna, which is measured by the power correlation coefficient [23], is the same. This is a reasonable assumption since the distance between the transmit antennas is much smaller than the distance to the users and eavesdropper, and thus transmitted signals from each antenna experience a similar scattering environment. It is shown in [24], [25] that the eavesdropper channel, which is correlated with the main channel with power correlation coefficient ρ, can be modeled as

$$\mathbf{h}_e = \sqrt{\beta_e}\left(\sqrt{\rho}\,\tilde{\mathbf{h}}_1 + \sqrt{1-\rho}\,\mathbf{w}\right), \tag{4}$$

where $\tilde{\mathbf{h}}_1 = \mathbf{h}_1/\sqrt{\beta_1}$ is the normalized version of $\mathbf{h}_1$ with respect to the large-scale fading parameter, and $\mathbf{w} \in \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is a random vector independent of $\tilde{\mathbf{h}}_1$. Note that since the eavesdropper is close to user 1, it will usually be true that $\beta_e = \beta_1$. The channel model in (4) is also assumed in [26], [27]. As discussed in [23], the value of ρ in practical

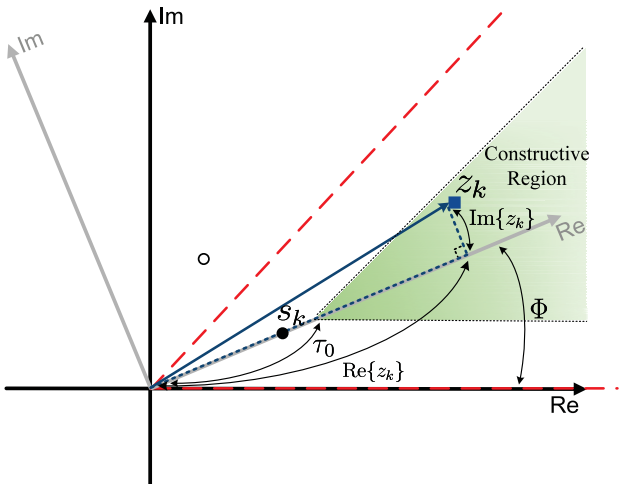


Fig. 2. Illustration of the constructive interference design for 8PSK modulation. The solid circle s_k is the symbol of interest while the hollow circle is the adjacent constellation point.

systems is determined by various factors such as the distance between user 1 and Eve as in [27], and the scattering environment. Besides using channel models [28] to measure the correlation, the value of ρ can also be obtained through field measurements [23].

The existing research in [17], [18] assumes that the eavesdropper adopts the same detection method as the legitimate users, which greatly limits the eavesdropper's capability. In this paper, we consider a smart eavesdropper that can use statistical information to improve detection performance. The details about the smart eavesdropper will be given in Section IV-A.

B. Constructive Interference

CI-based precoding transforms the undesirable MUI into useful power to push the received signal further away from the M-PSK decision boundaries, which in turn reduces the symbol error rate at the end user. To show the concept of constructive interference more clearly, we give an intuitive example in Fig. 2, where the symbol of interest s_k is assumed to be one of the constellation points of the 8PSK constellation. As illustrated in Fig. 2, the constructive region for s_k is the green sector with infinite radius and angle 2Φ, and the decision region for s_k is the sector determined by the two dashed red rays which are also referred to as decision boundaries. The distance between the constructive region and the decision boundary depends on τ_0, which is also related to the minimum signal-to-noise ratio (SNR) requirement. When the noise-free received signal $z_k = y_k - n_k$ lies in the constructive region, it is pushed deeper into the decision region and thus is more robust to additive noise perturbations. With knowledge of the CSI and the symbols to be transmitted, CI-based precoding guarantees that the noise-free signal received at each user lies in the constructive region of each user's desired symbol. In this way, the MUI is transformed into useful energy for improving the SNR.

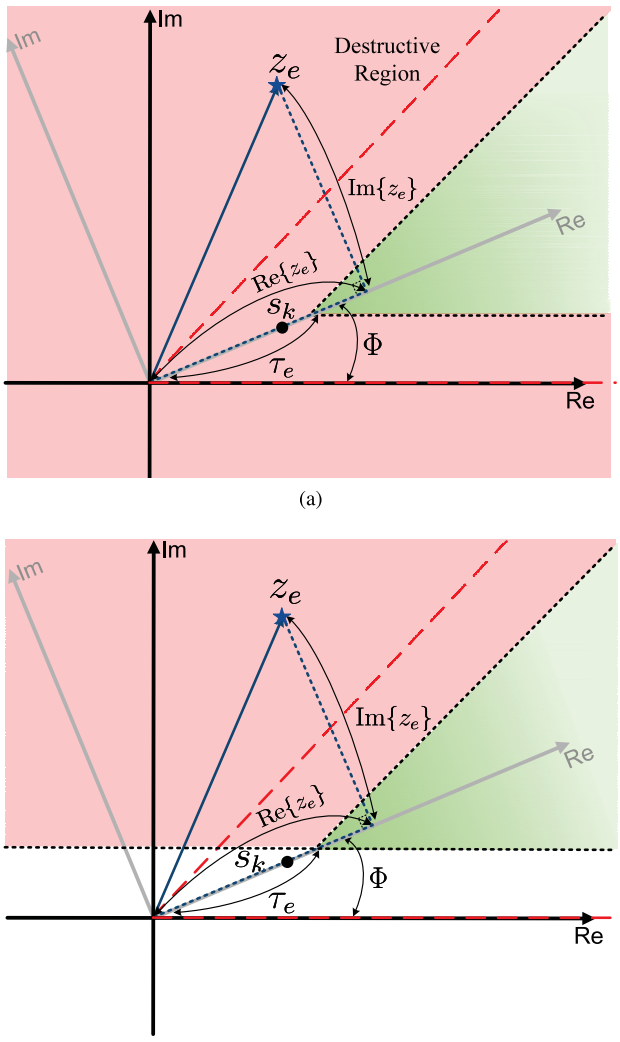


Fig. 3. The constructive-destructive interference based secure precoding for 8PSK modulation. (a) Our proposed scheme (b) The scheme in [17], [18].

III. Traditional Constructive-Destructive Interference Based Secure Precoding

In this section, we first review the existing C-D precoding algorithm in [17], [18] with eavesdropper's CSI. Then, an improved C-D precoding algorithm is proposed which can achieve a lower transmit power compared with the scheme in [17], [18]. The extension of the improved C-D precoding to the multi-eavesdropper scenario is also provided.

A. Existing C-D Precoding Algorithm

As discussed in Section II-B, it is beneficial for the legitimate users if their noise-free received signals are located in the constructive regions of the desired symbols. On the other hand, the noise-free received signal at the eavesdropper should be located outside the constructive region. Accordingly, the C-D precoding method of [17], [18] pushes the received signal at each legitimate user towards the corresponding constructive region, while guaranteeing that the noise-free received signal at the eavesdropper lies in the red area in Fig. 3(b), which is outside the constructive region. As in [17], [18], different

SNR requirements are assumed for the users and eavesdropper; in particular, it is assumed that the desired minimum SNR is γ_0 for all users, and the desired maximum SNR is γ_e for the eavesdropper. Generally, γ_e is chosen to be much smaller than γ_0 to make the eavesdropper suffer a higher symbol error rate. Since the noise power is assumed to be one, for the parameters τ_0 and τ_e in Fig. 2 and Fig. 3, we have $\tau_0 = \sqrt{\gamma_0}$ and $\tau_e = \sqrt{\gamma_e}$.

Now, we formulate the optimization problem that the C-D precoding approach of [17], [18] attempts to solve. First of all, in order to find a uniform expression for the constructive regions of different symbols in the constellation, we rotate the original coordinate system by the phase of the symbol of interest. Taking the symbol s_k as an example, the new coordinate system after rotation is shown by the gray one in both Fig. 2 and Fig. 3. Based on (2), in the new coordinate system, the real and imaginary parts of the noise-free received signal z_k can be respectively derived as

$$\mathrm{Re}\{z_k\} = \mathrm{Re}\left\{\frac{(y_k - n_k)s_k^*}{|s_k|}\right\} = \mathrm{Re}\{\mathbf{g}_k^T\mathbf{x}\} \tag{5}$$

and

$$\mathrm{Im}\{z_k\} = \mathrm{Im}\left\{\frac{(y_k - n_k)s_k^*}{|s_k|}\right\} = \mathrm{Im}\{\mathbf{g}_k^T\mathbf{x}\}, \tag{6}$$

where we adopt the new variable $\mathbf{g}_k \triangleq \mathbf{h}_k s_k^*$ and use the fact that $|s_k| = 1$. As illustrated in Fig. 2, the constructive region for s_k can be defined by the following inequality

$$|\mathrm{Im}\{z_k\}| \le (\mathrm{Re}\{z_k\} - \tau_0)\tan\Phi, \tag{7}$$

which already indicates that $\mathrm{Re}\{z_k\} \ge \tau_0$.

For convenience, we rewrite the constraint in (7) using real-valued notation. In particular, we define the following real-valued vectors

$$\mathbf{a}_k^T = \left[\mathrm{Re}\{\mathbf{g}_k^T\}, -\mathrm{Im}\{\mathbf{g}_k^T\}\right], \tag{8}$$

$$\mathbf{b}_k^T = \left[\mathrm{Im}\{\mathbf{g}_k^T\}, \mathrm{Re}\{\mathbf{g}_k^T\}\right], \tag{9}$$

$$\bar{\mathbf{x}}^T = \left[\mathrm{Re}\{\mathbf{x}^T\}, \mathrm{Im}\{\mathbf{x}^T\}\right]. \tag{10}$$

It can be easily verified that

$$\mathrm{Re}\{z_k\} = \mathbf{a}_k^T\bar{\mathbf{x}}, \quad \mathrm{Im}\{z_k\} = \mathbf{b}_k^T\bar{\mathbf{x}}. \tag{11}$$

Therefore, the real-valued reformulation of (7) can be written as

$$\left|\mathbf{b}_k^T\bar{\mathbf{x}}\right| \le \left(\mathbf{a}_k^T\bar{\mathbf{x}} - \tau_0\right)\tan\Phi, \tag{12}$$

which is equivalent to the following two constraints

$$\left(\mathbf{a}_k^T\tan\Phi - \mathbf{b}_k^T\right)\bar{\mathbf{x}} - \tau_0\tan\Phi \ge 0, \tag{13a}$$

$$\left(\mathbf{a}_k^T\tan\Phi + \mathbf{b}_k^T\right)\bar{\mathbf{x}} - \tau_0\tan\Phi \ge 0. \tag{13b}$$

According to the C-D precoding in [17], [18] (e.g., refer to problem (25) in [17]), the location of the eavesdropper's noise-free received signal in the coordinate system rotated by the phase of s_k is constrained by

$$-\mathrm{Im}\{z_e\} \le (\mathrm{Re}\{z_e\} - \tau_e)\tan\Phi, \tag{14a}$$

$$\mathrm{Im}\{z_e\} \ge (\mathrm{Re}\{z_e\} - \tau_e)\tan\Phi, \tag{14b}$$

where $z_e = \mathbf{g}_e^T\mathbf{x}$ with $\mathbf{g}_e \triangleq \mathbf{h}_e s_k^*$. Since only user 1 has the demand for secure communication, s_k is specified as s_1 when rotating the original coordinate system. $\mathrm{Re}\{z_e\}$ and $\mathrm{Im}\{z_e\}$ are the real and imaginary parts of z_e in the new coordinate system rotated by the phase of s_1. By introducing the real-valued vectors $\mathbf{a}_e^T = \left[\mathrm{Re}\{\mathbf{g}_e^T\}, -\mathrm{Im}\{\mathbf{g}_e^T\}\right]$, $\mathbf{b}_e^T = \left[\mathrm{Im}\{\mathbf{g}_e^T\}, \mathrm{Re}\{\mathbf{g}_e^T\}\right]$, and $\bar{\mathbf{x}}^T = \left[\mathrm{Re}\{\mathbf{x}^T\}, \mathrm{Im}\{\mathbf{x}^T\}\right]$, we have

$$\mathrm{Re}\{z_e\} = \mathbf{a}_e^T\bar{\mathbf{x}}, \quad \mathrm{Im}\{z_e\} = \mathbf{b}_e^T\bar{\mathbf{x}}. \tag{15}$$

Then, the inequalities in (14) can be rewritten as

$$-\mathbf{b}_e^T\bar{\mathbf{x}} \le \left(\mathbf{a}_e^T\bar{\mathbf{x}} - \tau_e\right)\tan\Phi, \tag{16a}$$

$$\mathbf{b}_e^T\bar{\mathbf{x}} \ge \left(\mathbf{a}_e^T\bar{\mathbf{x}} - \tau_e\right)\tan\Phi. \tag{16b}$$

The goal of the C-D precoding in [17] is to achieve the above constructive-destructive interference constraints for the legitimate users and the eavesdropper, while minimizing the transmit power. Thus, the optimization problem for the C-D precoding in [17] is given by

$$\min_{\bar{\mathbf{x}}} \ \|\bar{\mathbf{x}}\|^2 \tag{17a}$$

$$\text{s.t.:} \ \left(\mathbf{a}_k^T\tan\Phi - \mathbf{b}_k^T\right)\bar{\mathbf{x}} - \tau_0\tan\Phi \ge 0, \quad \forall k \tag{17b}$$

$$\left(\mathbf{a}_k^T\tan\Phi + \mathbf{b}_k^T\right)\bar{\mathbf{x}} - \tau_0\tan\Phi \ge 0, \quad \forall k \tag{17c}$$

$$-\mathbf{b}_e^T\bar{\mathbf{x}} \le \left(\mathbf{a}_e^T\bar{\mathbf{x}} - \tau_e\right)\tan\Phi, \tag{17d}$$

$$\mathbf{b}_e^T\bar{\mathbf{x}} \ge \left(\mathbf{a}_e^T\bar{\mathbf{x}} - \tau_e\right)\tan\Phi. \tag{17e}$$

Constraints (17b) and (17c) ensure that the noise-free received signal at each user lies in the constructive region of the transmitted symbol for that user. Constraints (17d) and (17e) force the noise-free received signal at the eavesdropper to be located outside the constructive region of s_1. However, it should be noticed that constraints (17d) and (17e) correspond to a fraction of the destructive interference region, as shown by the red area in Fig. 3(b). The *full* destructive region is depicted in red in Fig. 3(a). The transmit power required to solve the optimization in (17a)-(17e) will thus in general be higher than what would be required if the full destructive region were exploited in formulating the constraints in (17d) and (17e).

B. Improved C-D Precoding Algorithm

To achieve a lower transmit power, in the first algorithm we present, we derive a modification to the C-D precoding algorithm that exploits the full destructive region. As illustrated in Fig. 3(a), the entire destructive region can be described by

$$|\mathrm{Im}\{z_e\}| \ge (\mathrm{Re}\{z_e\} - \tau_e)\tan\Phi, \tag{18}$$

which is however not convex. The inequality in (18) holds when any one of the following three constraints is satisfied

$$\mathrm{Re}\{z_e\} - \tau_e \le 0, \tag{19a}$$

$$\mathrm{Im}\{z_e\} \ge (\mathrm{Re}\{z_e\} - \tau_e)\tan\Phi \quad \text{and} \quad \mathrm{Re}\{z_e\} - \tau_e > 0, \tag{19b}$$

$$-\mathrm{Im}\{z_e\} \ge (\mathrm{Re}\{z_e\} - \tau_e)\tan\Phi \quad \text{and} \quad \mathrm{Re}\{z_e\} - \tau_e > 0. \tag{19c}$$

The real-valued reformulation of (19) is given by

$$\mathbf{a}_e^T\bar{\mathbf{x}}-\tau_e\le 0, \tag{20a}$$

$$\left(\mathbf{a}_e^T\tan\Phi-\mathbf{b}_e^T\right)\bar{\mathbf{x}}-\tau_e\tan\Phi\le 0\quad\text{and}\ \mathbf{a}_e^T\bar{\mathbf{x}}-\tau_e>0, \tag{20b}$$

$$\left(\mathbf{a}_e^T\tan\Phi+\mathbf{b}_e^T\right)\bar{\mathbf{x}}-\tau_e\tan\Phi\le 0\quad\text{and}\ \mathbf{a}_e^T\bar{\mathbf{x}}-\tau_e>0. \tag{20c}$$

Based on (20), the improved C-D precoding algorithm can be formulated as

$$\min_{\bar{\mathbf{x}}}\ \|\bar{\mathbf{x}}\|^2 \tag{21a}$$

$$\text{s.t.: (17b) and (17c)}, \tag{21b}$$

$$\text{(20a) or (20b) or (20c)}. \tag{21c}$$

Note that problem (21) actually involves three different convex problems, each of which can be readily solved using standard convex optimization toolbox such as CVX [29]. After each subproblem of (21) is solved, the solution with the minimum transmit power is selected as the final C-D precoder.

C. Extension to the Case of Multiple Eavesdroppers

Although the focus of this article is not on C-D precoding, we show here how to extend our improved C-D precoding algorithm in (21) to a scenario with multiple eavesdroppers. In particular, assume that there are L eavesdroppers trying to wiretap the confidential message of user 1, and the channel between the BS and eavesdropper l, $l=1,\cdots,L$, is denoted as $\mathbf{h}_{e,l}$. Following the aforementioned real-valued expressions, we denote $\mathbf{a}_{e,l}^T=\left[\text{Re}\{\mathbf{g}_{e,l}^T\},-\text{Im}\{\mathbf{g}_{e,l}^T\}\right]$, and $\mathbf{b}_{e,l}^T=\left[\text{Im}\{\mathbf{g}_{e,l}^T\},\text{Re}\{\mathbf{g}_{e,l}^T\}\right]$, where $\mathbf{g}_{e,l}=\mathbf{h}_{e,l}s_1^*$. Based on (18) and (21), the improved C-D precoding for the multi-eavesdropper case can be formulated as

$$\min_{\bar{\mathbf{x}}}\ \|\bar{\mathbf{x}}\|^2 \tag{22a}$$

$$\text{s.t.: (17b) and (17c)}, \tag{22b}$$

$$\left|\mathbf{b}_{e,l}^T\bar{\mathbf{x}}\right|\ge\left(\mathbf{a}_{e,l}^T\bar{\mathbf{x}}-\tau_e\right)\tan\Phi,\quad\forall l. \tag{22c}$$

For each l, constraint (22c) holds when

$$\mathbf{b}_{e,l}^T\bar{\mathbf{x}}\ge\left(\mathbf{a}_{e,l}^T\bar{\mathbf{x}}-\tau_e\right)\tan\Phi,\quad\forall l \tag{23}$$

or

$$-\mathbf{b}_{e,l}^T\bar{\mathbf{x}}\ge\left(\mathbf{a}_{e,l}^T\bar{\mathbf{x}}-\tau_e\right)\tan\Phi,\quad\forall l \tag{24}$$

is satisfied. Note that the above transformation of (22c) incurs no loss of optimality for the case $\mathbf{a}_{e,l}^T\bar{\mathbf{x}}\le\tau_e$, since when $\mathbf{a}_{e,l}^T\bar{\mathbf{x}}\le\tau_e$, the union of the two regions defined by (23) and (24) is $\mathbf{b}_{e,l}^T\bar{\mathbf{x}}\in(-\infty,+\infty)$. According to the big-M method [30], we introduce binary variables $t_l\in\{0,1\}$, $l=1,\cdots,L$, and a sufficiently large constant $C>0$. Then, the either-or constraints in (23) and (24) can be transformed into the following constraints which should be satisfied simultaneously:

$$(\mathbf{a}_{e,l}^T\tan\Phi-\mathbf{b}_{e,l}^T)\bar{\mathbf{x}}-\tau_e\tan\Phi-t_lC\le 0,\quad\forall l, \tag{25a}$$

$$(\mathbf{a}_{e,l}^T\tan\Phi+\mathbf{b}_{e,l}^T)\bar{\mathbf{x}}-\tau_e\tan\Phi+(t_l-1)C\le 0,\quad\forall l. \tag{25b}$$

One can see that when $t_l=0$, constraint (25a) is activated, which corresponds to constraint (23), and constraint (25b) is always fulfilled due to the sufficiently large constant C. In contrast, when $t_l=1$, constraint (25b) is activated, which corresponds to constraint (24), and constraint (25a) is always fulfilled due to the large C. With the aid of (25), problem (22) can be transformed into the following equivalent form:

$$\min_{\bar{\mathbf{x}},t_l}\ \|\bar{\mathbf{x}}\|^2 \tag{26a}$$

$$\text{s.t.: (17b) and (17c)}, \tag{26b}$$

$$\text{(25a) and (25b)}, \tag{26c}$$

$$t_l\in\{0,1\},\quad\forall l. \tag{26d}$$

Obviously, problem (26) is a mixed integer program, which has non-polynomial-time computational complexity. To lower the complexity, we propose to use the following suboptimal algorithm for solving problem (26), which has polynomial-time computational complexity. According to [31, Theorem 2], for a sufficiently large constant $\alpha\gg 1$, an equivalent form of problem (26) is given by

$$\min_{\bar{\mathbf{x}},t_l}\ \|\bar{\mathbf{x}}\|^2+\alpha\left(\sum_{l=1}^{L}t_l-\sum_{l=1}^{L}t_l^2\right) \tag{27a}$$

$$\text{s.t.: (17b), (17c), (25a), and (25b)}, \tag{27b}$$

$$0\le t_l\le 1,\quad\forall l. \tag{27c}$$

The obstacle for solving problem (27) is the function $f(t_l)\triangleq\sum_{l=1}^{L}t_l^2$ in (27a). To tackle this issue, we use the sequential convex programming (SCP) method [32], [33] to obtain a stationary point of problem (27). Specifically, for the nth iteration, we approximate $f(t_l)$ using its first-order Taylor expansion given by

$$f(t_l,t_{l,(n)})=\sum_{l=1}^{L}t_{l,(n)}^2+2\sum_{l=1}^{L}t_{l,(n)}(t_l-t_{l,(n)}), \tag{28}$$

where $t_{l,(n)}$ is the current point in the nth iteration. Therefore, for the nth iteration, we only need to solve the following convex optimization problem

$$\min_{\bar{\mathbf{x}},t_l}\ \|\bar{\mathbf{x}}\|^2+\alpha\left(\sum_{l=1}^{L}t_l-f(t_l,t_{l,(n)})\right) \tag{29a}$$

$$\text{s.t.: (17b), (17c), (25a), and (25b)}, \tag{29b}$$

$$0\le t_l\le 1,\quad\forall l. \tag{29c}$$

The solution t_l^* to problem (29) is adopted as the current point for use in the $(n+1)$-th iteration, i.e., $t_{l,(n+1)}=t_l^*$. Given the initial points $t_{l,(0)}\in(0,1)$, $\forall l$, we solve the convex optimization problem (29) in each iteration and then update the values for $t_{l,(n)}$. This iterative algorithm will finally converge to a stationary point of problem (27) with polynomial-time complexity [32], [33].

IV. Secure Precoding Against Smart Eavesdropper

In this section, we first introduce the smart eavesdropper, who can exploit statistical information for symbol detection. The drawback of the C-D precoding when faced with a smart eavesdropper is pointed out. For mitigating smart eavesdropping, we first discuss a general principle for designing secure precoding. Then, we present a specific precoding algorithm

based on information-carrying signal suppressing (ICSS), which can overcome the drawback of the C-D precoding scheme. A fast ICSS precoding algorithm is also provided, which uses the gradient projection method for improving computational efficiency.

A. Smart Eavesdropper and Security Risk

In the discussions in Section III, the eavesdropper is assumed to adopt the same detection method as the legitimate users, namely performing symbol detection based solely on the instantaneous observed signal. However, if the eavesdropper can exploit statistical information about the received signal, the symbol detection capability can be significantly increased. One way to obtain statistical information is learning from publicly available training data used for channel estimation. On the other hand, when the eavesdropper knows the statistical distribution of all wireless channels, SNR parameters γ_0 and γ_e, and the adopted constellation, the eavesdropper can simulate the transmission by solving problem (21) for different realizations of the wireless channels and symbols, and thus empirically determine the probability distribution of the received signal conditioned on each symbol $c_m \in \mathcal{C}_M$. Note that for PSK modulation, it is sufficient to focus only on the phase of the received signal, which is denoted as θ_e. We denote the conditional PDF of θ_e given symbol c_m as $f(\theta_e|c_m)$. With empirically derived estimates of these PDFs, the eavesdropper can employ the ML criterion for symbol detection. For the ML detector, when the eavesdropper receives a new signal with phase $\theta_{e,0}$, the detection result is given by

$$c_m^* = \arg\max_{c_m} \; f(\theta_{e,0}|c_m). \tag{30}$$

Note that the ML detector in (30) not only utilizes the instantaneous information $\theta_{e,0}$ but also the statistical information about the distribution of the phase. We refer to an eavesdropper using this ML detector as a smart eavesdropper.

In the following analysis, we will focus on our improved C-D precoder to illustrate the security risk of this type of approach when faced with a smart eavesdropper. A performance comparison between the improved C-D precoder and the C-D precoder in [17] will be given in Section VI. To study the performance of C-D precoding in the presence of a smart eavesdropper, we examine empirically estimated distributions $f(\theta_e|c_1)$ for a few scenarios.[3] In Fig. 4 we show $f(\theta_e|c_1)$ for QPSK modulation in a polar coordinate system where the polar angle from 0° to 360° covers the range of values for θ_e and the radius represents probability density. The results are obtained by averaging over both the transmit symbol vector $\mathbf{s}$ where user 1's desired symbol is fixed as c_1, and all wireless channels with $\beta_k = 1$ $(k = 1, \cdots, K)$ and $\beta_e = 1$.

First, as illustrated in Fig. 4(a), when γ_e is very large which leads to nearly no constraint on the eavesdropper's received signal, there is a considerable probability that the eavesdropper's received signal lies in the decision region of c_1 (i.e., quadrant I). As such, the eavesdropper has a relatively high probability of detecting the transmitted symbol, and thus it is important to adopt security-aware precoding when channel correlation exists. As γ_e becomes smaller, we can see that the C-D algorithm produces a distribution for $f(\theta_e|c_1)$ with two narrow lobes.[4] Compared with Fig. 4(b), the lobes in Fig. 4(c) are pushed closer to the boundaries of the destructive region of c_1, i.e., the two dotted black rays in Fig. 3(a). This is because compared with pushing z_e deeper into the destructive region,

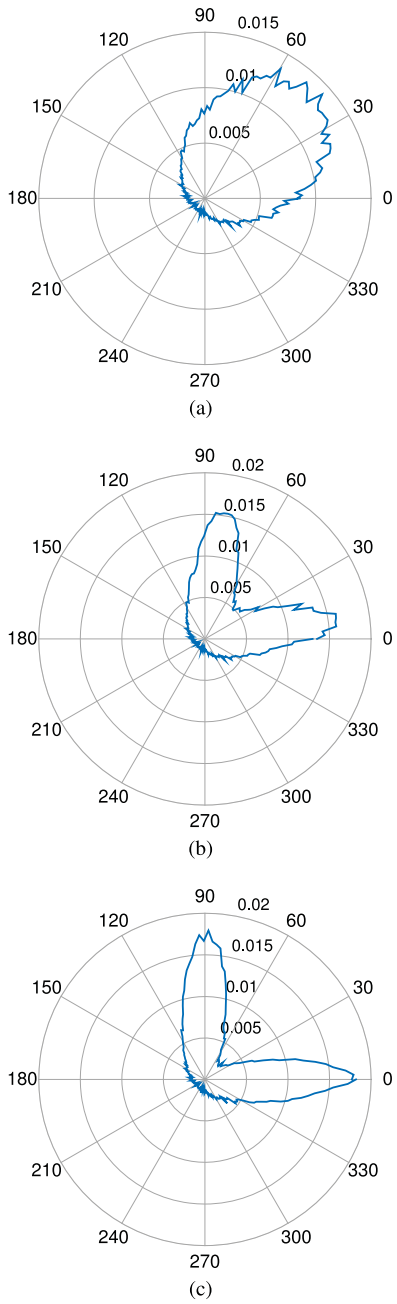


Fig. 4. QPSK modulation with channel correlation coefficient $\rho = 0.3$ and $\gamma_0 = 10$ dB: Empirical conditional PDF $f(\theta_e|c_1)$ for different SNR requirements at the eavesdropper. (a) $\gamma_e = 15$ dB (b) $\gamma_e = 0$ dB (c) $\gamma_e = -15$ dB.

[3]Considering that symbol c_m is a rotated version of c_1 by angle $(m-1)\frac{360°}{M}$, the empirical conditional PDF $f(\theta_e|c_m)$ which has been averaged over the transmitted symbols for other users and all wireless channels is also a rotated version of $f(\theta_e|c_1)$ by the same angle. Therefore, the empirical conditional PDFs for other symbols have characteristics similar to $f(\theta_e|c_1)$.

[4]As shown later in Fig. 6, if the original approach of [17] were used, the lobe would be along only one of the symbol boundaries rather than symmetrically on both of them.

pushing z_e near the boundaries can save power in most cases, which is consistent with the objective of problem (21). As a result, the probability that the eavesdropper's received signal falls in quadrant I is reduced, as illustrated in Fig. 4(b) and Fig. 4(c). This is beneficial for communication secrecy if the eavesdropper adopts the same simple detector as the legitimate user.

However, the rotational asymmetry of $f(\theta_e|c_1)$ when γ_e is small can be exploited by the eavesdropper to improve their detection probability. The distributions for different c_m will be identical to those shown in Fig. 4, except rotated by $\pm 90°$ and $180°$ for the case of QPSK. The lobes for adjacent symbols will overlap, and the correct detection probability for the eavesdropper can approach 50% for equally probable symbols, twice the minimum of 25% achieved by random guessing. Thus, whether γ_e is large or small, the security of the C-D precoding scheme is compromised. This means that the security of the system may not improve even as the transmit power increases or even if the desired user's channel is much stronger than that of the eavesdropper. Clearly, a better approach for a smart eavesdropper employing optimal ML detection would be to ensure that the distribution for different $f(\theta_e|c_m)$ are as identical and rotationally invariant as possible. This is the theme of the technique proposed in the following sections.

B. Design Principle

After revealing the security risk of the C-D precoding methods, we now provide a general design principle for secure precoding against smart eavesdropping. We know that for M-PSK modulation, the eavesdropper's minimum correct detection probability is $1/M$, which is the probability achieved by a random guess. To make random guessing the optimal strategy for a smart eavesdropper, the conditional PDFs for different symbols should be identical. Furthermore, since the conditional PDFs for other symbols are rotated versions of $f(\theta_e|c_1)$, the ideal $f(\theta_e|c_1)$ which makes the transmitted symbol totally indistinguishable from other symbols should be rotationally symmetric for every angle of $360°/M$, as mentioned in Section IV-A. Therefore, to mitigate smart eavesdropping, the focus of secure precoding is not on the instantaneous performance but on making the received symbols statistically indistinguishable.

C. ICSS Precoding

Based on the above discussion, secure precoding against a smart eavesdropper should aim at making the conditional PDFs for different symbols identical, which can be specified as making the conditional PDF rotationally symmetric in a polar coordinate system. The simplest type of rotational symmetry would be to make the conditional PDFs uniform in all directions, i,e, the phase θ_e is uniformly distributed on $[0, 2\pi]$. However, even for this special case it is still challenging to design a specific precoding algorithm that can realize the desired statistical distribution.

It is worth noting that eavesdropper's received signal consists of two parts, the information-carrying signal z_e which is also the aforementioned noise-free received signal, and the additive Gaussian noise n_e whose phase is uniformly distributed on $[0, 2\pi]$. If the information-carrying signal can be hidden in the additive noise, the ML detector at the eavesdropper will be useless. This can be achieved by simply transmitting in the null space of the eavesdropper channel. However, this will consume a lot of power especially when the eavesdropper channel is highly correlated with the main channel. To show the trade-off between consumed power and secrecy, we consider a more general and flexible approach which limits the power of the information-carrying signal, as illustrated in Fig. 5(a). Following the previous notation, for a given SNR constraint γ_e, the power of z_e is limited as

$$|z_e|^2 \leq \tau_e^2, \tag{31}$$

where $\tau_e = \sqrt{\gamma_e}$. For the complex variable z_e we have $|z_e|^2 = (\mathrm{Re}\{z_e\})^2 + (\mathrm{Im}\{z_e\})^2$. Therefore, the real-valued reformulation of (31) is given by

$$\bar{\mathbf{x}}^T \left(\mathbf{a}_e \mathbf{a}_e^T + \mathbf{b}_e \mathbf{b}_e^T \right) \bar{\mathbf{x}} \leq \tau_e^2. \tag{32}$$

Based on (32), our proposed ICSS precoding approach can be stated as

$$\min_{\bar{\mathbf{x}}} \ \|\bar{\mathbf{x}}\|^2 \tag{33a}$$

$$\text{s.t.:} \ \left(\mathbf{a}_k^T \tan\Phi - \mathbf{b}_k^T \right) \bar{\mathbf{x}} - \tau_0 \tan\Phi \geq 0, \quad \forall k \tag{33b}$$

$$\left(\mathbf{a}_k^T \tan\Phi + \mathbf{b}_k^T \right) \bar{\mathbf{x}} - \tau_0 \tan\Phi \geq 0, \quad \forall k \tag{33c}$$

$$\bar{\mathbf{x}}^T \mathbf{A} \bar{\mathbf{x}} \leq \tau_e^2, \tag{33d}$$

where $\mathbf{A} = \mathbf{a}_e \mathbf{a}_e^T + \mathbf{b}_e \mathbf{b}_e^T$. Constraints (33b) and (33c) ensure that the constructive region requirement is met at each desired user while constraint (33d) limits the maximum power of the eavesdropper's noise-free received signal. Problem (33) is convex and can be solved using convex optimization toolbox such as CVX [29].

Note that although z_e is referred to as the information-carrying signal, it can be any point on the complex plane, rather than one of the fixed constellation points. By placing a constraint on the power of z_e, we actually limit the contribution that z_e makes to the final received signal. As the power of z_e decreases, the information about the real transmitted symbol is more likely to be hidden. Therefore, the achievable secrecy level of our ICSS precoding approach will continue improving as γ_e decreases, which overcomes the drawback of C-D precoding where secrecy performance cannot be further improved as γ_e is reduced.

D. Fast ICSS Precoding

In the last subsection, we proposed an ICSS precoding algorithm that improves communication security by suppressing the power of the information-carrying signal at the eavesdropper. In this subsection, we propose another signal suppressing scheme with different constraints on the feasible region of z_e. Specifically, we change the power constraint in (33d) to the power constraint illustrated in Fig. 5(b). By requiring z_e to be located in a square with diagonal length $2\tau_e$, the maximum power of z_e is τ_e^2. The advantage of this approach is that

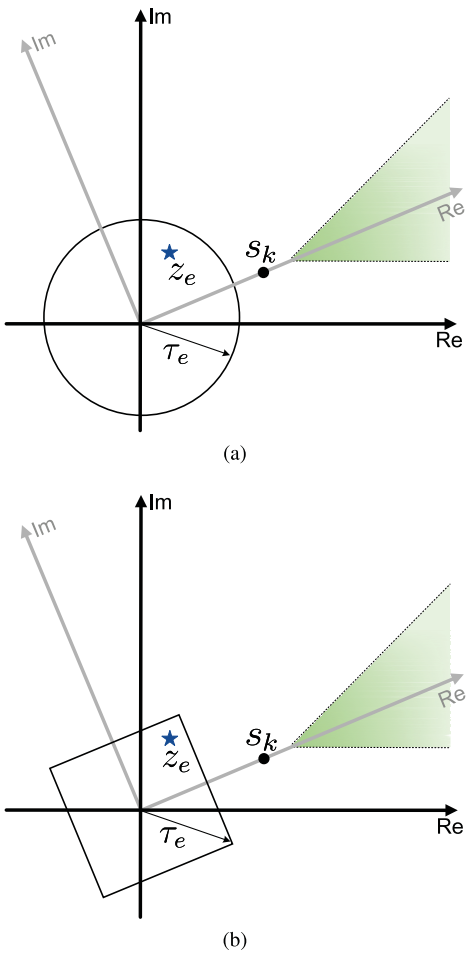


Fig. 5. Secure precoding against smart eavesdropper, where $\tau_e = \sqrt{\gamma_e}$: (a) ICSS precoding (b) Fast ICSS precoding.

the maximum power constraint can be expressed using linear rather than quadratic constraints:

$$-\sqrt{2}\tau_e/2 \le \mathrm{Re}\{z_e\} \le \sqrt{2}\tau_e/2, \tag{34a}$$
$$-\sqrt{2}\tau_e/2 \le \mathrm{Im}\{z_e\} \le \sqrt{2}\tau_e/2, \tag{34b}$$

which facilitates the development of the following fast ICSS precoding algorithm. Based on the real-valued expression (15), the fast ICSS precoding algorithm can thus be formulated as

$$\min_{\bar{\mathbf{x}}} \ \|\bar{\mathbf{x}}\|^2 \tag{35a}$$
$$\text{s.t.: } \mathbf{Q}\bar{\mathbf{x}} - \mathbf{b} \preceq \mathbf{0}, \tag{35b}$$

where

$$\mathbf{Q} = \begin{bmatrix} -\mathbf{a}_k^T \tan\Phi + \mathbf{b}_k^T \\ -\mathbf{a}_k^T \tan\Phi - \mathbf{b}_k^T \\ \mathbf{a}_e^T \\ -\mathbf{a}_e^T \\ \mathbf{b}_e^T \\ -\mathbf{b}_e^T \end{bmatrix}_{(2K+4)\times 2N},$$
$$\mathbf{b} = \begin{bmatrix} -\tau_0 \tan\Phi \mathbf{1}_{2K\times 1} \\ \frac{\sqrt{2}}{2}\tau_e \mathbf{1}_{4\times 1} \end{bmatrix}_{(2K+4)\times 1}. \tag{36}$$

The curled inequality symbol $\preceq$ in (35b) denotes component-wise inequality between vectors. According to [34], problem (35) is a standard quadratic program, which is convex. Instead of directly solving it via a convex optimization toolbox such as CVX, we propose the following efficient algorithm for solving (35). Note that problems (33) and (35) are two different convex optimization problems with different feasible regions for z_e, which are shown in Fig. 5(a) and Fig. 5(b), respectively.

To solve problem (35), we first derive the following Lagrange dual function of (35)

$$L(\bar{\mathbf{x}}, \boldsymbol{\lambda}) = \bar{\mathbf{x}}^T \bar{\mathbf{x}} + \boldsymbol{\lambda}^T (\mathbf{Q}\bar{\mathbf{x}} - \mathbf{b}), \tag{37}$$

where $\boldsymbol{\lambda} \succeq \mathbf{0}$ is the $(2K+4)\times 1$ Lagrange multiplier associated with constraint (35b). According to the Karush-Kuhn-Tucker (KKT) conditions [34], the optimal solution to problem (35) is achieved at $\frac{\partial L}{\partial \bar{\mathbf{x}}} = \mathbf{0}$. The root of $\frac{\partial L}{\partial \bar{\mathbf{x}}} = \mathbf{0}$ is given by

$$\bar{\mathbf{x}}^* = -\frac{1}{2}\mathbf{Q}^T\boldsymbol{\lambda}. \tag{38}$$

Then, we need to find the optimal $\boldsymbol{\lambda}$, which is the solution to the dual problem given by

$$\max_{\boldsymbol{\lambda}\succeq\mathbf{0}} \ g(\boldsymbol{\lambda}), \tag{39}$$

where

$$g(\boldsymbol{\lambda}) = \inf \ L(\bar{\mathbf{x}}, \boldsymbol{\lambda}) \overset{(a)}{=} -\frac{1}{4}\boldsymbol{\lambda}^T\mathbf{Q}\mathbf{Q}^T\boldsymbol{\lambda} - \boldsymbol{\lambda}^T\mathbf{b} \tag{40}$$

is the dual function, and (a) is obtained by plugging (38) into (37).

Due to the non-negative constraint $\boldsymbol{\lambda} \succeq \mathbf{0}$, it is difficult to derive a closed-form solution to (39). Therefore, we use the gradient projection method to find the solution. Since we aim at maximizing the concave function $g(\boldsymbol{\lambda})$, the current value $\boldsymbol{\lambda}_n$ is updated as

$$\boldsymbol{\lambda}_{n+1} = \max\{\boldsymbol{\lambda}_n + t_n \bigtriangledown g(\boldsymbol{\lambda}_n), \mathbf{0}\}, \tag{41}$$

where t_n is the positive step size used at the nth iteration, and $\bigtriangledown g(\boldsymbol{\lambda}) = -\frac{1}{2}\mathbf{Q}\mathbf{Q}^T\boldsymbol{\lambda} - \mathbf{b}$ is the gradient of $g(\boldsymbol{\lambda})$. The function $\max\{\boldsymbol{\lambda}, \mathbf{0}\}$ is the projection of $\boldsymbol{\lambda}$ onto the solution space $\boldsymbol{\lambda} \succeq \mathbf{0}$ in (39). For calculating the step size t_n in each iteration, we employ the backtracking line search algorithm [34], [35]. The details are shown in Algorithm 1, where the parameters t, δ, and μ are set according to [35]. With the updated step size, we can use the gradient projection method to solve problem (39) and then problem (35). The entire iterative algorithm is summarized in Algorithm 2.

Remark 1: The extension of the ICSS and the fast ICSS precoding schemes to the scenario with multiple eavesdroppers is straightforward. For ICSS precoding, we only need to impose the constraint (33d) on each eavesdropper, which does not influence the convexity of the problem. Similarly, for fast ICSS precoding, the constraint in (34) for the single eavesdropper is now applied to each eavesdropper. The new problem can be directly solved using Algorithm 2.

Algorithm 1 Backtracking Line Search Algorithm

Input: $\mathbf{Q}$, $\mathbf{QQ}^T$, $\mathbf{b}$, $\boldsymbol{\lambda}_n$, $t = 1$, $\delta = 0.1$, $\mu = 0.5$;

while 1 **do**
  $\boldsymbol{\lambda}_{n+1} = \max\{\boldsymbol{\lambda}_n + t * \bigtriangledown g(\boldsymbol{\lambda}_n), \mathbf{0}\}$;
  if $g(\boldsymbol{\lambda}_{n+1}) \geq g(\boldsymbol{\lambda}_n) + \delta \cdot \bigtriangledown g(\boldsymbol{\lambda}_n)^T(\boldsymbol{\lambda}_{n+1} - \boldsymbol{\lambda}_n)$ **then**
    Break;
  end if
  $t = \mu t$;
end while
$t_n = t$;

Output: t_n

Algorithm 2 Iterative Algorithm for Solving Problem (35)

Input: $\mathbf{Q}$, $\mathbf{QQ}^T$, $\mathbf{b}$, initial $\boldsymbol{\lambda}_0 \succeq \mathbf{0}$, $n = -1$, ϵ;

repeat
  $n = n + 1$;
  Calculate step size t_n using Algorithm 1;
  $\boldsymbol{\lambda}_{n+1} = \max\{\boldsymbol{\lambda}_n + t_n \bigtriangledown g(\boldsymbol{\lambda}_n), \mathbf{0}\}$;
until $g(\boldsymbol{\lambda}_{n+1}) - g(\boldsymbol{\lambda}_n) \leq \epsilon$ or maximum number of iterations reached
Obtain the optimal Lagrange multiplier, i.e., $\boldsymbol{\lambda}^* = \boldsymbol{\lambda}_{n+1}$;

Output: $\bar{\mathbf{x}}^* = -\frac{1}{2}\mathbf{Q}^T\boldsymbol{\lambda}^*$

E. Computational Complexity Analysis

Here, we compare the computational complexities of the ICSS and fast ICSS precoding methods. The ICSS precoding algorithm in (33) is implemented using the convex optimization toolbox CVX [29] with solver SeDuMi [36] which adopts the standard interior-point method (IPM). Thus, the computational complexity of ICSS precoding can be approximated by that of IPM. By introducing a slack variable, problem (33) can be reformulated as a conic program [37] with second-order cone constraints and linear constraints. Using the analysis in [37] applied to the ICSS optimization in (33), it is straightforward to show that the worst-case computational complexity of IPM in each iteration is on the order of $(2N+1)[2(2N+1)^2+2K(2N+1)+2K+9]$. For fast ICSS precoding, the dominant complexity of Algorithm 2 is calculating the gradient $\bigtriangledown g(\boldsymbol{\lambda})$ and the objective function $g(\boldsymbol{\lambda})$ in each iteration. Since the value of $\mathbf{QQ}^T$ is already known as an input parameter, the complexities of calculating $\bigtriangledown g(\boldsymbol{\lambda})$ and $g(\boldsymbol{\lambda})$ are both approximately on the order of $(2K+4)^2$ in each iteration. Since $N^3 \gg K^2$, the complexity of ICSS precoding in each iteration is much higher than that of fast ICSS precoding.

V. Secure Precoding Without Eavesdropper's CSI

In this section, we consider the scenario where the eavesdropper's CSI is unavailable.[5] Without the eavesdropper's CSI, we cannot control the location of z_e and thus we cannot control the distribution of the eavesdropper's received signal. On the other hand, due to the channel correlation, it is very likely that the eavesdropper's received signal is aligned with or near the symbol of interest, which makes the symbol easily detected. Recalling the channel correlation model in (4), the noise-free received signal at the eavesdropper can be decomposed as

$$z_e = \mathbf{h}_e^T\mathbf{x} = \underbrace{\sqrt{\beta_e/\beta_1}\sqrt{\rho}\mathbf{h}_1^T\mathbf{x}}_{\text{symbol of interest}} + \underbrace{\sqrt{\beta_e(1-\rho)}\mathbf{w}^T\mathbf{x}}_{\text{random term}}. \quad (42)$$

The first term in (42) represents the desired symbol for user 1, since $\mathbf{h}_1^T\mathbf{x}$ is designed to lie in the constructive region of s_1. The second term in (42) is unknown and random, changing every transmission due to different $\mathbf{x}$. Since the value of $\mathbf{w}$ is unknown, the random term $\mathbf{w}^T\mathbf{x}$ can be either constructive or destructive to the instantaneous detection of s_1. This term randomizes the statistical distribution of θ_e and thus can degrade the detection performance of the eavesdropper. Therefore, the second term in (42) acts as a type of AN as in [12], [38] which helps hide the transmitted information.

To be hidden in the AN term, the power of $\mathbf{h}_1^T\mathbf{x}$ in (42) should be as small as possible. However, the constraint in (7) requires that $z_1 = \mathbf{h}_1^T\mathbf{x}$ be located in the constructive region of s_1. It is obvious that the power-minimizing point in a constructive region is the intersection of the two constructive region boundaries. Consequently, we have $\text{Re}\{z_1\} = \tau_0$ and $\text{Im}\{z_1\} = 0$, which is equivalent to[6]

$$\mathbf{a}_1^T\bar{\mathbf{x}} = \tau_0, \quad \mathbf{b}_1^T\bar{\mathbf{x}} = 0. \quad (43)$$

In addition, the power of $\mathbf{w}^T\mathbf{x}$ should be large enough to guarantee sufficient randomization to the phase of the eavesdropper's received signal. With unknown $\mathbf{w}$, we place a constraint on the power of $\mathbf{x}$ instead, since the average power of $\mathbf{w}^T\mathbf{x}$ can be calculated as $\mathbb{E}_{\mathbf{w}}\left\{|\mathbf{w}^T\mathbf{x}|^2\right\} = \text{Tr}\left(\mathbf{x}^H\mathbb{E}_{\mathbf{w}}\left\{\mathbf{w}^*\mathbf{w}^T\right\}\mathbf{x}\right) = \|\mathbf{x}\|^2 = \|\bar{\mathbf{x}}\|^2$.

Based on the above discussion, we propose the following approach to be used when CSI for the potential eavesdropper is absent:

$$\min_{\bar{\mathbf{x}}} \ \|\bar{\mathbf{x}}\|^2 \quad (44a)$$

$$\text{s.t.: } \mathbf{a}_1^T\bar{\mathbf{x}} = \tau_0, \quad \mathbf{b}_1^T\bar{\mathbf{x}} = 0, \quad (44b)$$

$$\left(\mathbf{a}_k^T\tan\Phi - \mathbf{b}_k^T\right)\bar{\mathbf{x}} - \tau_0\tan\Phi \geq 0, \quad \forall k \neq 1 \quad (44c)$$

$$\left(\mathbf{a}_k^T\tan\Phi + \mathbf{b}_k^T\right)\bar{\mathbf{x}} - \tau_0\tan\Phi \geq 0, \quad \forall k \neq 1 \quad (44d)$$

$$\|\bar{\mathbf{x}}\|^2 \geq P_0, \quad (44e)$$

where P_0 determines the minimum average power of the AN. Without constraint (44e), problem (44) only focuses on minimizing $\|\bar{\mathbf{x}}\|^2$, which may lead to small AN values. Constraints (44c) and (44d) are the constructive region requirements for the other users.

Constraint (44e) leads to a non-convex feasible set, which makes problem (44) difficult to solve. To tackle this problem, we adopt the SCP method [32], [33], which iteratively approximates the original non-convex set by an inner convex one in

[5] The scenario without eavesdropper's CSI is also studied in [17] but only for the case of a single legitimate user. Moreover, the effect of channel correlation is not considered in [17].

[6] With this constraint, the worst-case QoS is still guaranteed for user 1.

Algorithm 3 SCP Method for Solving Problem (44)

Input: initial point $\bar{\mathbf{x}}_0$, $n = 0$, ϵ;

1: **repeat**
2: Calculate function (45) based on $\bar{\mathbf{x}}_n$;
3: Solve problem (47) and assign the optimal solution to $\bar{\mathbf{x}}_{n+1}$;
4: $n = n + 1$;
5: **until** $\|\bar{\mathbf{x}}_{n-1}\|^2 - \|\bar{\mathbf{x}}_n\|^2 \leq \epsilon$ or maximum number of iterations reached

Output: $\bar{\mathbf{x}}_n$

each iteration. Specifically, in the nth iteration we approximate function $f(\bar{\mathbf{x}}) \triangleq \|\bar{\mathbf{x}}\|^2$ using its first-order Taylor expansion $\tilde{f}(\bar{\mathbf{x}}, \bar{\mathbf{x}}_n)$ at the current point $\bar{\mathbf{x}}_n$. The expression for $\tilde{f}(\bar{\mathbf{x}}, \bar{\mathbf{x}}_n)$ is given by

$$\begin{aligned}\tilde{f}(\bar{\mathbf{x}}, \bar{\mathbf{x}}_n) &= f(\bar{\mathbf{x}}_n) + \bigtriangledown f(\bar{\mathbf{x}}_n)^T (\bar{\mathbf{x}} - \bar{\mathbf{x}}_n) \\ &= \|\bar{\mathbf{x}}_n\|^2 + 2\bar{\mathbf{x}}_n^T (\bar{\mathbf{x}} - \bar{\mathbf{x}}_n), \end{aligned} \tag{45}$$

where $\bigtriangledown f(\bar{\mathbf{x}})$ is the gradient of $f(\bar{\mathbf{x}})$ with respect to $\bar{\mathbf{x}}$. The constraint (44e) can now be replaced with

$$\tilde{f}(\bar{\mathbf{x}}, \bar{\mathbf{x}}_n) \geq P_0. \tag{46}$$

With (46), we can obtain the following convex optimization problem in the nth iteration

$$\min_{\bar{\mathbf{x}}} \ \|\bar{\mathbf{x}}\|^2 \tag{47a}$$

$$\text{s.t.: (44b)} - \text{(44d)}, \ (46). \tag{47b}$$

Problem (47) can be readily solved using standard convex optimization solvers or the gradient projection method in Section IV-D.

As shown in [33], the SCP method results in an objective function that is non-increasing at every iteration, so this approach will always converge to a local optimum of problem (44). We summarize the entire SCP method in Algorithm 3. To guarantee that the generated solution in each iteration is feasible for the original non-convex problem (44), we need to start from a point $\bar{\mathbf{x}}_0$ which belongs to the feasible set of problem (44). To find $\bar{\mathbf{x}}_0$, we use the iterative feasibility search algorithm (IFSA) proposed in [33], which iteratively minimizes the violation parameter until convergence.

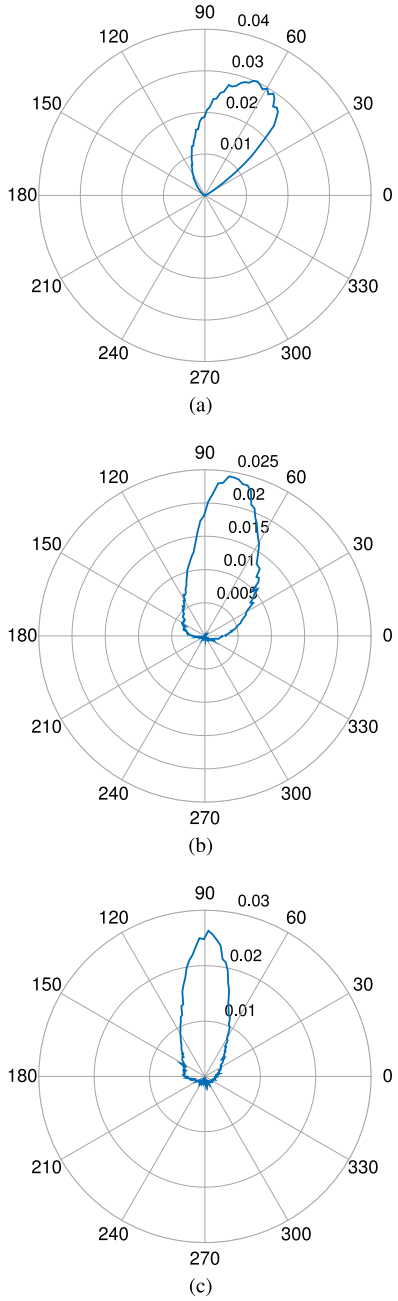


Fig. 6. The C-D precoding algorithm in [17] with QPSK modulation: Empirical conditional PDF $f(\theta_e|c_1)$ for different SNR requirements at the eavesdropper. (a) $\gamma_e = 15$ dB (b) $\gamma_e = 0$ dB (c) $\gamma_e = -15$ dB.

VI. Simulation Results

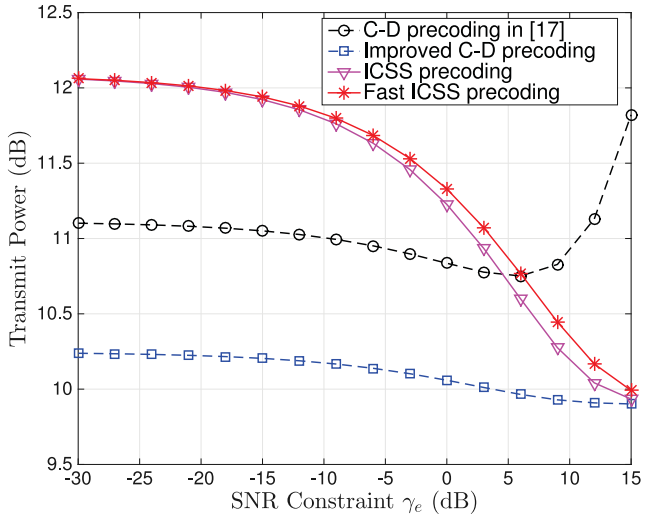
In this section, we compare the performance of the above precoding algorithms through simulation. Unless otherwise stated, we set $N = 6$, $K = 3$, $\beta_k = 1$ $(k = 1, \cdots, K)$, $\beta_e = 1$, and $\gamma_0 = 10$ dB. The eavesdropper in the simulation below adopts the detection method in (30). To simulate the performance of the eavesdropper, we first generate random transmit symbols and wireless channels to obtain the empirical conditional PDF $f(\theta_e|c_m)$. Then, the empirical decision region for each constellation point c_m can be obtained, which is the region where $f(\theta_e|c_m)$ is larger than $f(\theta_e|c_n)$ for any $n \neq m$. Based on the decision region, the detection probability for the eavesdropper can then be obtained. The transmit power in the results below is also averaged over different transmit symbols and wireless channels. In the following simulations, we first consider the scenario where the eavesdropper's CSI is available. Then, the scenario without eavesdropper's CSI is studied. Note that the case of multiple eavesdroppers is studied in Fig. 9, while all the other simulations focus on the single-eavesdropper case as described in Section II.

Similar to Fig. 4, we first depict the empirical conditional PDF $f(\theta_e|c_1)$ for the C-D precoding algorithm in [17], where QPSK modulation is adopted with channel correlation parameter $\rho = 0.3$, a desired SNR of $\gamma_0 = 10$ dB. Unlike Fig. 4, we can see that there is only one lobe in Fig. 6, since the C-D precoding in [17] actually requires $\text{Im}\{z_e\} \geq 0$, which only exploits the upper part of the entire destructive

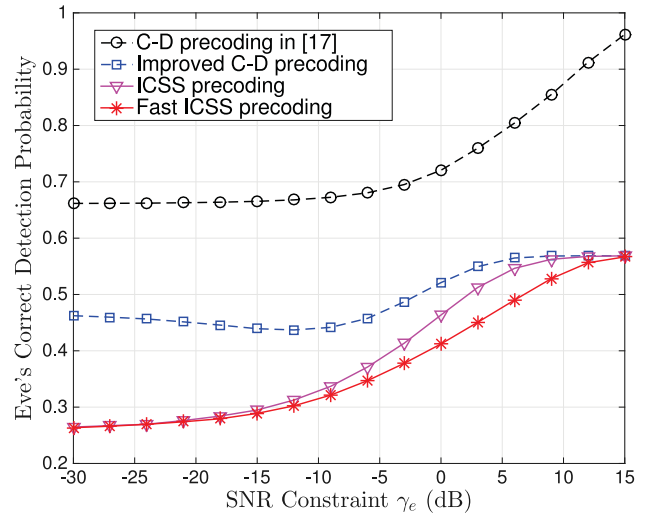
TABLE I

PERFORMANCE COMPARISON BETWEEN ICSS PRECODING ($\gamma_e = -30$ dB) AND THE TRADITIONAL ZF PRECODING

Algorithm	$N = 6,\ K = 3$			$N = 4,\ K = 3$		
	Power (dB)	$P_{\text{dec}}^{\text{Eve}}$	$\overline{\text{SER}}_k$	Power (dB)	$P_{\text{dec}}^{\text{Eve}}$	$\overline{\text{SER}}_k$
ICSS	12.06	0.26	1.4×10^{-3}	22.34	0.26	1.4×10^{-3}
ZF	12.34	0.25	1.5×10^{-3}	27.50	0.25	1.5×10^{-3}



(a)



(b)

Fig. 7. Performance comparison among different precoding algorithms for QPSK modulation with $\rho = 0.3$. (a) Transmit power versus SNR constraint (b) Eavesdropper's correct detection probability versus SNR constraint.

region. Moreover, when γ_e is larger than γ_0, e.g., $\gamma_e = 15$ dB in Fig. 6(a), there is still a significant lobe which makes the transmitted symbol easily detected. This is because the feasible region shown by the red zone in Fig. 3(b) shrinks as γ_e increases. Thus, the phase distribution of z_e is still concentrated rather than dispersed.

In Fig. 7, we compare the algorithms discussed in this article in terms of consumed power and secrecy. First, we concentrate on the comparison between the two C-D precoding strategies. From Fig. 7(a) we can see that the C-D precoding in [17] consumes more power than the improved C-D precoding algorithm. This is expected since the scheme in [17] only exploits a part of the destructive region, which leads to a stricter optimization. In addition, it is worth noting that the power consumed by the improved C-D precoding algorithm decreases as γ_e increases, while the power of the scheme in [17] first decreases and then increases. This is because the feasible set for our approach keeps getting larger as γ_e increases. However, for the algorithm in [17], too large a γ_e will unnecessarily require the imaginary part of z_e to be large, which consumes significant power.[7] For the secrecy performance in Fig. 7(b), the improved C-D precoding also outperforms the C-D precoding in [17]. This corresponds to the result in Fig. 6 that a single lobe makes the transmitted symbol more easily detected.

Next, we compare the performance of the two C-D precoding algorithms and the two ICSS algorithms. Fig. 7(b) shows that our improved C-D precoding strategy provides significantly lower detection probability than the algorithm of [17], which achieves a probability of slightly less than 0.5 for small γ_e. On the other hand, the ICSS and fast ICSS schemes can further reduce the eavesdropper's detection probability to about 0.25, which corresponds to the perfect secrecy case where the eavesdropper's optimal strategy is random guessing. However, as shown by Fig. 7(a), the consumed power of the two ICSS algorithms for $\gamma_e < 5$ dB is higher than that of the two C-D precoding schemes, particularly our improved C-D precoding algorithm. Therefore, there is a trade-off between secrecy and power, which will be discussed later in Fig. 8. Finally, from Fig. 7(b) one can see that for a given γ_e, fast ICSS precoding achieves a lower detection probability for Eve compared with ICSS precoding. This is because, as illustrated in Fig. 5, the feasible region for z_e for fast ICSS is smaller than that for ICSS precoding, which implies that fast ICSS imposes a stricter constraint on Eve's received signal power. The price paid for this improved security is that, for a given γ_e, the transmit power required for fast ICSS precoding is higher than that for ICSS precoding, as illustrated in Fig. 7(a).

Now we focus on the extreme case for the ICSS precoding algorithm where $\gamma_e = -30$ dB. In this case, the information-carrying signal z_e at the eavesdropper is nearly zero, which corresponds to the traditional zero-forcing (ZF) scheme where both the MUI and the eavesdropper's received signal are forced to be zero. Table I makes a comparison between the ICSS precoding algorithm ($\gamma_e = -30$ dB) and the traditional ZF algorithm for QPSK modulation with $\rho = 0.3$, where

[7] Typically, γ_e is chosen to be smaller than γ_0 to degrade the eavesdropper's performance. Here we consider a wider range of γ_e to thoroughly study the effect of γ_e on the performance of each precoding algorithm.

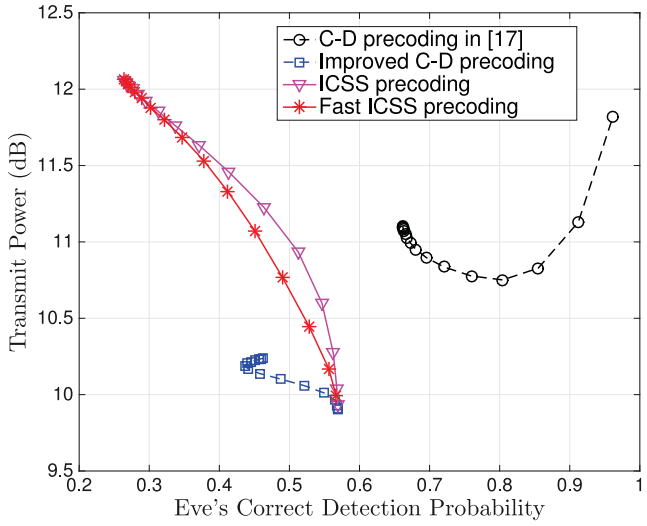


Fig. 8. Power-secrecy trade-off curve for QPSK modulation with channel correlation coefficient $\rho = 0.3$.

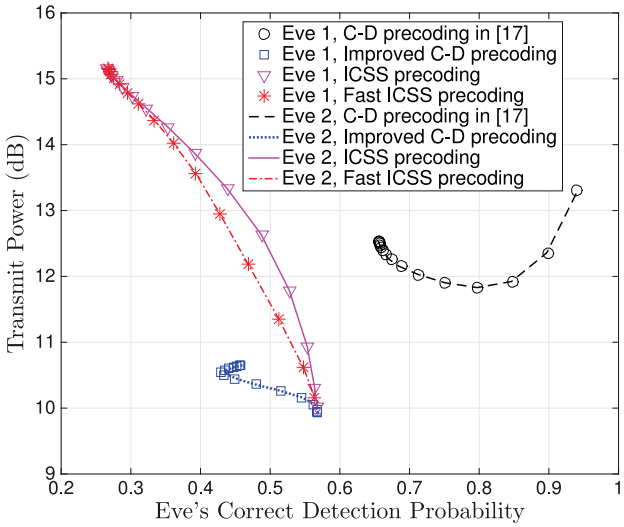


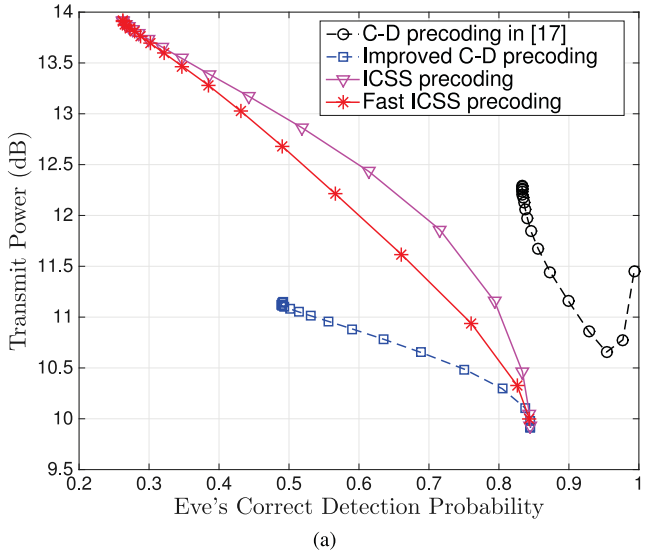
Fig. 9. The case of two eavesdroppers: Power-secrecy trade-off curve for QPSK modulation with $\rho = 0.3$ for each eavesdropper.

$\frac{P_{\text{dec}}^{\text{Eve}}}{\text{SER}_k}$ denotes the eavesdropper's detection probability, and SER_k is the symbol error rate averaged over K legitimate users. From Table I one can see that the two algorithms achieve similar detection performance at the legitimate users and the eavesdropper, but ICSS precoding requires less power especially when the system is heavily loaded (e.g., a 5dB power savings for the case of $N = 4$, $K = 3$). Unlike the ZF method whose consumed power is fixed and high, the proposed ICSS scheme, which allows one to balance the transmit power and secrecy performance, is more flexible and general. Even for the scenario with a high secrecy requirement, ICSS precoding can still benefit from the concept of CI, and thus achieves a similar secrecy performance to ZF but with a much lower transmit power, especially for heavily loaded systems.

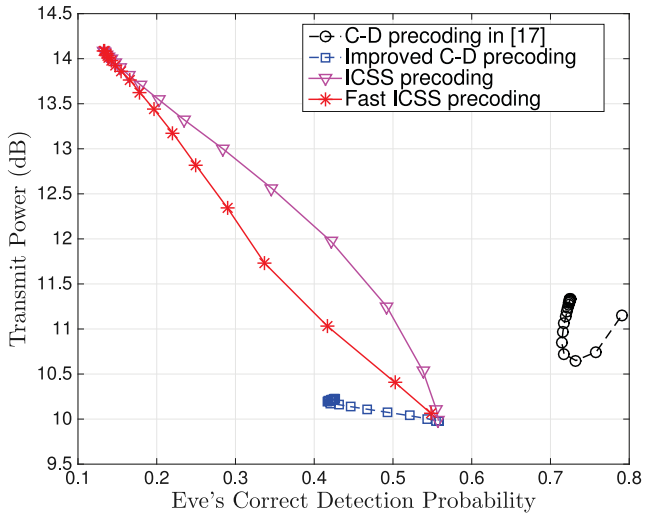
Fig. 8 depicts the power-secrecy trade-off curves for the two C-D precoding algorithms and the two ICSS algorithms, which are generated by changing the SNR constraint γ_e at the eavesdropper. First, it can be observed that the C-D precoding in [17] has the worst performance, since all the other schemes use less power but achieve a lower detection probability at the eavesdropper. In addition, the improved C-D precoding algorithm is the most energy efficient when the eavesdropper's detection probability is allowed to be higher than 0.4. However, it is worth noting that this scheme as well as the scheme in [17] cannot further degrade eavesdropper's performance, which indicates that there is a secrecy bottleneck for the C-D precoding algorithms. Further increases in the transmit power for the improved C-D precoding algorithm enhance the eavesdropper's detection probability. Therefore, the two ICSS precoding schemes are vital for eliminating the secrecy bottleneck of the C-D precoding algorithm. It is also worth noting that for the simulation scenario in Fig. 8, the fast ICSS precoding is more energy efficient than ICSS precoding. Recalling Fig. 7 which has the same simulation settings, it is observed that for a fixed γ_e, although the fast ICSS scheme consumes more power than the ICSS algorithm, it can significantly reduce the eavesdropper's detection probability. Consequently, fast ICSS precoding has a better trade-off curve than ICSS precoding. One possible reason is that compared with using a circle to limit the location of z_e, using a square which has a side perpendicular to the line on which the desired symbol is located can more effectively reduce the probability that the eavesdropper's received signal is aligned with or near the desired symbol. In addition, we remark that on top of the power-secrecy tradeoff depicted in Fig. 8, there is no obvious tradeoff between the correct detection probability of user 1 and that of Eve. This is because the power-secrecy tradeoff is based on changing γ_e, which has little impact on the detection performance of user 1 determined by the fixed γ_0.

Fig. 9 shows the results for the case of two eavesdroppers. The results for the improved C-D precoding were obtained using the low-complexity algorithm discussed in Section III-C. To compare with the single-eavesdropper results in Fig. 8, the two eavesdroppers are assumed to have the same channel correlation coefficient $\rho = 0.3$. We see in Fig. 9 that the performance for the two eavesdroppers is essentially identical, which is expected since they have the same channel correlation coefficient. Comparing Fig. 9 with Fig. 8, we see that more transmit power is required to achieve the same secrecy level when two eavesdroppers are present instead of just one. Furthermore, the relative performance of the algorithms is similar to that for the single-eavesdropper case in Fig. 8, which implies that the study of a single eavesdropper is sufficient to illustrate the impact of an intelligent eavesdropper and our proposed approaches. Therefore, in the following analysis, we focus on the single-eavesdropper scenario.

In Fig. 10, we study the trade-off between power and secrecy in an environment with higher channel correlation. Comparing Fig. 10(a) and Fig. 8, we can see that to achieve the same secrecy level, more power is needed for the scenario with $\rho = 0.7$. Moreover, when the correlation parameter rises from 0.3 to 0.7, the lowest detection probability for the eavesdropper that the two C-D precoding schemes can achieve is increased. On the contrary, the lowest probability that the two ICSS precoding algorithms can achieve remains



(a)



(b)

Fig. 10. Power-secrecy trade-off curve for a highly correlated scenario with $\rho = 0.7$. (a) QPSK modulation (b) 8PSK modulation.

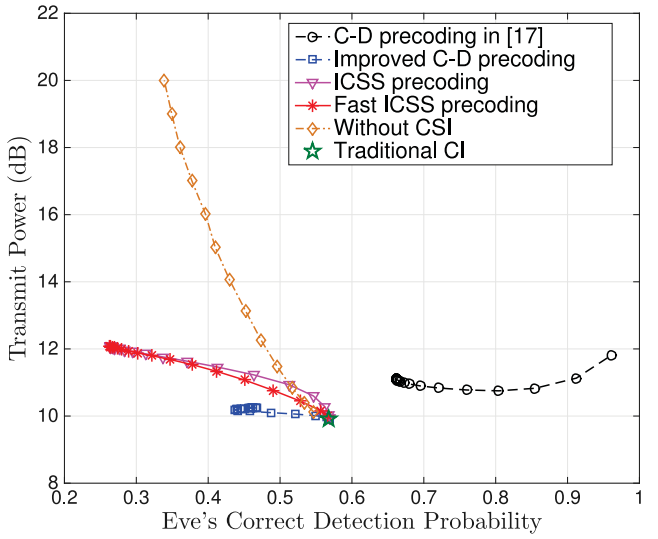


Fig. 11. Performance comparison between the schemes with and without eavesdropper's CSI for QPSK modulation, where $\rho = 0.3$.

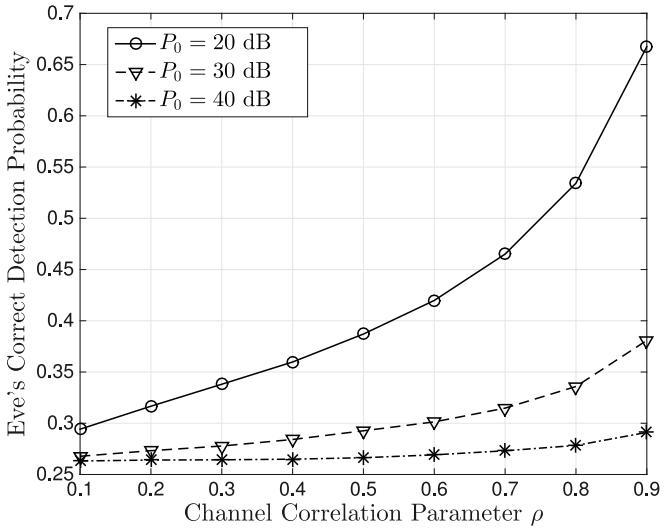


Fig. 12. Secure precoding without eavesdropper's CSI: Eavesdropper's correct detection probability versus channel correlation parameter for different P_0.

unchanged, as long as there is enough power. Therefore, the two ICSS precoding schemes are more robust to the strength of the channel correlation. We also study the case of 8PSK modulation in Fig. 10(b). It is observed that the two ICSS precoding algorithms can reduce the eavesdropper's detection probability to about 0.125, which corresponds to random guessing for 8PSK.

Finally, we investigate the scenario where the eavesdropper's CSI is unavailable. In Fig. 11, besides the scheme proposed in Section V, which is labeled "Without CSI", we also reintroduce the aforementioned CSI-dependent algorithms as baselines. Another baseline scheme, referred to as "Traditional CI", is also introduced. The Traditional CI scheme aims at solving optimization problem (17) without constraints (17d) and (17e). Thus, it only focuses on the legitimate users' communication reliability without taking secrecy into consideration. First of all, we can observe that the secrecy performance of the C-D precoding in [17] is even worse than the Traditional CI scheme, which indicates that an inappropriate design of the security-aware precoder will expose the transmitted symbol to the smart eavesdropper. Moreover, except for the C-D precoding in [17], the other three CSI-dependent methods tend to converge to the Traditional CI method as the transmit power decreases. For the algorithm that does not use eavesdropper's CSI, the minimum required power is always larger than that of the Traditional CI approach. This is because additional power is needed to satisfy constraint (44b), which in turn helps reduce the eavesdropper's detection probability. One can also observe that for the Without CSI scheme, enhancing transmit power is always beneficial for improving the secrecy. However, due to the absence of eavesdropper's CSI, more power is generally needed to achieve the same secrecy level as the two ICSS algorithms. One exception is when the eavesdropper's correct detection probability is larger than 0.5, where the Without CSI scheme is more energy-efficient than at least one of the two ICSS algorithms.

Fig. 12 shows the secrecy performance of the Without CSI approach versus the channel correlation parameter for

different P_0. From Fig. 12 we can see that the eavesdropper's detection probability increases as ρ increases, which is expected according to (42). Not only is the eavesdropper's received signal is more likely to be concentrated at the symbol of interest as ρ increases, the power of the random term in (42), which acts as noise for blocking the eavesdropper, reduces as ρ increases. Meanwhile, one can also observe that improving P_0 is beneficial for reducing the eavesdropper's detection probability, which is consistent with the result in Fig. 11 that the eavesdropper's detection probability decreases monotonically with an increase in the transmit power for the Without CSI algorithm.

VII. Conclusion

In this article, we restudied the CI-based secure precoding problem. Unlike the existing research, we considered a smart eavesdropper who can utilize statistical information for ML symbol detection. We first modified the existing CI-based precoding algorithm for a better utilization of the destructive interference. Then, we pointed out the security risk that both the original and our modified precoders have when faced with a smart eavesdropper. To combat the smart eavesdropper, a general principle for designing security-aware precoders was given. Two specific precoding algorithms were then provided. In addition, the scenario without eavesdropper's CSI was also studied. Finally, we used numerical results to show the importance of the proposed schemes for mitigating a smart eavesdropper.

References

[1] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, Feb. 2004.

[2] M. Sadek, A. Tarighat, and A. Sayed, "A leakage-based precoding scheme for downlink multi-user MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1711–1721, May 2007.

[3] S. S. Christensen, R. Agarwal, E. De Carvalho, and J. M. Cioffi, "Weighted sum-rate maximization using weighted MMSE for MIMO-BC beamforming design," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4792–4799, Dec. 2008.

[4] M. Schubert and H. Boche, "Solution of the multiuser downlink beamforming problem with individual SINR constraints," *IEEE Trans. Veh. Technol.*, vol. 53, no. 1, pp. 18–28, Jan. 2004.

[5] C. Masouros, T. Ratnarajah, M. Sellathurai, C. B. Papadias, and A. K. Shukla, "Known interference in the cellular downlink: A performance limiting factor or a source of green signal power?" *IEEE Commun. Mag.*, vol. 51, no. 10, pp. 162–171, Oct. 2013.

[6] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3628–3640, Jul. 2015.

[7] A. Li and C. Masouros, "Interference exploitation precoding made practical: Optimal closed-form solutions for PSK modulations," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7661–7676, Nov. 2018.

[8] A. Haqiqatnejad, F. Kayhan, and B. Ottersten, "Symbol-level precoding design based on distance preserving constructive interference regions," *IEEE Trans. Signal Process.*, vol. 66, no. 22, pp. 5817–5832, Nov. 2018.

[9] H. Jedda, A. Mezghani, A. L. Swindlehurst, and J. A. Nossek, "Quantized constant envelope precoding with PSK and QAM signaling," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8022–8034, Dec. 2018.

[10] A. Li, C. Masouros, F. Liu, and A. L. Swindlehurst, "Massive MIMO 1-Bit DAC transmission: A low-complexity symbol scaling approach," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7559–7575, Nov. 2018.

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

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

[13] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1417–1432, Dec. 2016.

[14] 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.

[15] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[16] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816–3825, Dec. 2012.

[17] M. R. A. Khandaker, C. Masouros, and K.-K. Wong, "Constructive interference based secure precoding: A new dimension in physical layer security," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2256–2268, Sep. 2018.

[18] M. R. A. Khandaker, C. Masouros, K.-K. Wong, and S. Timotheou, "Secure SWIPT by exploiting constructive interference and artificial noise," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1326–1340, Feb. 2019.

[19] Z. Wei, C. Masouros, and F. Liu, "Interference exploitation based secure transmission for distributed antenna systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, May 2019, pp. 1–6.

[20] Z. Wei and C. Masouros, "Robust secure precoding and antenna selection: A probabilistic optimization approach for interference exploitation," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Brighton, U.K., May 2019, pp. 2442–2446.

[21] Z. Wei and C. Masouros, "User-centric distributed antenna transmission: Secure precoding and antenna selection with interference exploitation," 2018, *arXiv:1812.05046*. [Online]. Available: http://arxiv.org/abs/1812.05046

[22] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1478–1493, Dec. 2016.

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

[24] S. Han, S. Xu, W. Meng, and L. He, "Channel-correlation-enabled transmit optimization for MISO wiretap channels," 2019, *arXiv:1907.01064*. [Online]. Available: http://arxiv.org/abs/1907.01064

[25] S. Xu, S. Han, W. Meng, S. Yan, and L. He, "Robust beamforming design for correlated MISO wiretap channels under channel uncertainty," *IEEE Wireless Commun. Lett.*, vol. 9, no. 4, pp. 553–557, Dec. 2019.

[26] D. Xu, P. Ren, and H. Lin, "Combat hybrid eavesdropping in power-domain NOMA: Joint design of timing channel and symbol transformation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 4998–5012, Jun. 2018.

[27] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

[28] W. C. Jakes, *Microwave Mobile Communications*, 2nd ed. Hoboken, NJ, USA: Wiley, 1994.

[29] M. Grant and S. Boyd. (Mar. 2014). *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. [Online]. Available: http://cvxr.com/cvx

[30] Y. Cheng, M. Pesavento, and A. Philipp, "Joint network optimization and downlink beamforming for CoMP transmissions using mixed integer conic programming," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 3972–3987, Aug. 2013.

[31] D. W. K. Ng, Y. Wu, and R. Schober, "Power efficient resource allocation for full-duplex radio distributed antenna networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2896–2911, Apr. 2016.

[32] B. R. Marks and G. P. Wright, "Technical note—A general inner approximation algorithm for nonconvex mathematical programs," *Oper. Res.*, vol. 26, no. 4, pp. 681–683, Aug. 1978.

[33] Y. Cheng and M. Pesavento, "Joint optimization of source power allocation and distributed relay beamforming in multiuser Peer-to-Peer relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 6, pp. 2962–2973, Jun. 2012.

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

[35] X. Jiang, W.-J. Zeng, A. Yasotharan, H. C. So, and T. Kirubarajan, "Quadratically constrained minimum dispersion beamforming via gradient projection," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 192–205, Jan. 2015.

[36] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optim. Methods Softw.*, vol. 11, nos. 1–4, pp. 625–653, Jan. 1999, doi: 10.1080/10556789908805766.
[37] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.
[38] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

Qian Xu (Graduate Student Member, IEEE) received the B.S. degree from Xi'an Jiaotong University, China, in 2014, where she is currently pursuing the Ph.D. degree with the School of Information and Communications Engineering. From October 2018 to October 2019, she was a Visiting Student with the Department of Electrical Engineering and Computer Science, Henry Samueli School of Engineering, University of California at Irvine, Irvine, CA, USA. Her research interests include physical-layer security, massive MIMO systems, and cooperative relaying networks.

Pinyi Ren (Member, IEEE) received the B.S. degree in information and control engineering, the M.S. degree in information and communications engineering, and the Ph.D. degree in electronic and communications system from Xi'an Jiaotong University, China, in 1994, 1997, and 2001, respectively. He is currently a Professor with the School of Information and Communications Engineering, Xi'an Jiaotong University. He has published over 100 technical papers in international journals and conferences. He is selected as a fellow of the China Institute of Communications (CIC). He is a member of the IEEE Communications Society. He received the Best Letter Award of the IEICE Communications Society in 2010. He has served as the General Chair of ICST WICON in 2011 and serves frequently as a Technical Program Committee Member of the IEEE GLOBECOM, the IEEE ICC, and the IEEE CCNC. He serves as an Editor for the *Journal of Xi'an Jiaotong University* and the *Journal of Electronics and Information Technology*. He has served as the Leading Guest Editor for the Special Issue on Distributed Wireless Networks and Services for *Mobile Networks and Applications*.

A. Lee Swindlehurst (Fellow, IEEE) received the B.S. and M.S. degrees in electrical engineering from Brigham Young University (BYU) in 1985 and 1986, respectively, and the Ph.D. degree in electrical engineering from Stanford University in 1991. He was with the Department of Electrical and Computer Engineering, BYU, from 1990 to 2007, where he was the Department Chair from 2003 to 2006. From 1996 to 1997, he held a joint appointment as a Visiting Scholar at Uppsala University and the Royal Institute of Technology, Sweden. From 2006 to 2007, he was on leave working as the Vice President of Research at ArrayComm LLC, San Jose, CA, USA. Since 2007, he has been a Professor with the Electrical Engineering and Computer Science Department, University of California at Irvine, where was the Associate Dean for Research and Graduate Studies with the Samueli School of Engineering from 2013 to 2016. From 2014 to 2017, he was a Hans Fischer Senior Fellow of the Institute for Advanced Studies, Technical University of Munich. His research interests include array signal processing for radar, wireless communications, and biomedical applications, and he has over 300 publications in these areas. In 2016, he was elected as a Foreign Member of the Royal Swedish Academy of Engineering Sciences (IVA). He received the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 IEEE Communications Society Stephen O. Rice Prize in the field of communication theory, the 2006 and 2010 IEEE Signal Processing Society's Best Paper Awards, and the 2017 IEEE Signal Processing Society Donald G. Fink Overview Paper Award. He was the inaugural Editor-in-Chief of the IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING.