Beyond Secrecy Rate in MISO Wiretap Channels: An Information Jamming Approach

Haiyang Zhang, *Member, IEEE* and Lingjie Duan, *Senior Member, IEEE*

Abstract

Cooperative jamming is a widely used approach for improving the security of wireless networks. In this approach, a friendly jammer sends jamming signals to disrupt the reception of the eavesdropper, which inevitably interferes with the legitimate receiver. In this paper, we propose a novel approach, namely, information jamming, to exceed the secrecy rate achieved by the traditional cooperative jamming approach in a multiple-input single-output (MISO) wiretap channel. We propose that multiple multi-antenna information jammers (iJammers) transmit the source signals of the legitimate transmitter rather than independent noise signals for simultaneously enhancing the signal strength at the legitimate receiver and canceling the received signal at the eavesdropper. Specifically, we aim at maximizing the achievable secrecy rate by jointly optimizing the beamforming vectors at Alice and iJammers, subject to the individual transmit power constraints. We first propose a semi-definite relaxation based approach to solve the original non-convex problem optimally. For ease of implementation, we then provide a suboptimal distributed information beamforming scheme, whose optimal solution is obtained in closed-form. Finally, we extend our study to the imperfect channel state information case. Simulation results show that our proposed information jamming approach significantly outperforms the traditional cooperative jamming approach in terms of achievable secrecy rate.

Index Terms

Physical-layer security, information jamming, secrecy rate, beamforming design.

This paper has been presented in part at IEEE Global Communications Conference (Globecom), Abu Dhabi, UAE, 2018 [1].

H. Zhang and L. Duan are with the Engineering Systems and Design Pillar, Singapore University of Technology and Design, Singapore (e-mail: {haiyang_zhang, lingjie_duan}@sutd.edu.sg).

I. Introduction

The broadcast characteristic of wireless channels makes the transmitted signals susceptible to eavesdropping by unintended receivers (eavesdroppers), and how to achieve secret communication over wireless networks is a critical and challenging issue. Physical layer security, as a promising technology to guarantee communication security by utilizing the physical properties of wireless channels (e.g., channel fading and interference), has been an active research topic in the past decade (see, e.g., [2]-[4] and references therein). In particular, the idea of physical layer security was first pioneered by Wyner [5], in which the classic wiretap channel model was introduced in a discrete memoryless channel. This work was then extended to a Gaussian wiretap channel [6], where an important performance metric in physical layer security, referred to as secrecy rate, was developed and characterized by the channel capacity difference between the main channel (from the transmitter to the legitimate receiver) and the eavesdropper channel (from the transmitter to the eavesdropper). Since then various techniques have been proposed to enlarge this difference, among which cooperative jamming is regarded as one efficient approach and has been extensively investigated in the existing literature

The fundamental principle of cooperative jamming approach is to jam the eavesdropper by using artificial noise introduced by friendly nodes. This approach was first proposed in [7], in which the Gaussian noise signal is transmitted by a friendly jammer to weaken the reception of the eavesdropper, under a single-antenna multiple access wiretap channel setup. The cooperative jamming approach was later generalized to the multi-antenna case, where the friendly jammer equipped with multiple antennas exploits the available spatial degrees of freedom to increase the secrecy rate [8]-[11]. The authors in [8] studied the optimal jamming beamforming design for maximizing the secrecy rate in multiple-input single-output (MISO) wiretap channels, and showed the asymptotic optimality of zero-forcing (ZF) beamforming strategy. In [9], the closed-form expression of the jamming transmit covariance matrix was derived in a multiple-input multiple-output (MIMO) wiretap channel, which guaranteeing the achievable secrecy rate is larger than the secrecy rate of the case without the friendly jammer. In [10], the covariance matrices at the legitimate transmitter and the friendly jammer are jointly designed so as to maximize the achievable secrecy rate or minimize the total transmit power separately. The secure degrees of freedom of MIMO wiretap channel with a multi-antenna cooperative jammer was characterized in [11]. For the wireless networks with multiple eavesdroppers, [12] studied a cooperative jamming

scheme to maximize the secrecy rate subject to the secrecy outage probability constraint. In addition, the cooperative jamming approach has also been applied to improve the achievable secrecy rate of various other system setups, such as relay system [13], wireless information and power transfer system [14], and unmanned aerial vehicle (UAV)-aided communication system [15]. More recently, [16] considered a correlated MISO wiretap channel and proposed a multiple jammers-aided cooperative jamming scheme to reduce the secrecy loss due to correlation. In [17], the authors studied robust cooperative jamming beamforming design for a two-tier 5G heterogeneous network with different security requirements.

Though efficient, the cooperative jamming approach has an inherent drawback which limits its performance. Specifically, the jamming signal is independent of the source message, and thus it can not only disrupt the reception of the eavesdropper but also interfere with the legitimate receiver, let alone enhancing the desired signal power at the legitimate receiver. Note that in addition to broadcast, superposition is another fundamental characteristic of wireless channels. The superposition characteristic leads to the overlapping of multiple signals at one receiver, which provides an opportunity to exceed the secrecy rate of wireless networks. Accordingly, we propose a novel information jamming approach to go beyond the secrecy rate achieved by the conventional cooperative jamming approach. In particular, we consider a MISO wiretap channel, where a friendly multi-antenna jammer sends the source message rather than independent noise signal to assist the legitimate transmitter.

The main contributions of this paper can be summarized as follows.

- We propose a novel information jamming approach for improving the achievable secrecy rate. Unlike the traditional cooperative jamming approach (e.g., [7]-[8]), our friendly iJammers send the source message rather than the Gaussian noise for simultaneously improving the received signal strength at the legitimate receiver and reducing that at the eavesdropper. Specifically, we aim at maximizing the achievable secrecy rate by jointly optimizing the beamforming vectors at the Alice and iJammers, subject to their individual power constraints. The formulated beamforming problem is non-convex and thus difficult to handle. Nevertheless, we propose a semi-definite relaxation (SDR) based approach to solve the original non-convex beamforming design problem optimally.
- We present a suboptimal distributed information beamforming scheme, namely, separate zero-forcing, to reduce the implementation complexity. For this scheme, each transmitter designs its beamforming vectors independently using only local CSI, so as to maximize the

received signal strength at the legitimate receiver while avoiding information leakage to the eavesdropper. We derive the corresponding optimal beamforming solution in closed-form.

- We extend our study to the imperfect CSI case. Considering the stochastic CSI errors model, we propose a robust secure beamforming design to maximize the ϵ-outage secrecy rate. In order to solve this non-convex optimization problem, we first transform it into a tractable form by appying the SDR and the Bernstein-type inequality, and then solve the resulting problem by solving a sequence of SDP feasibility problem. Based on that, an efficient bisection method-based iterative algorithm is proposed to solve the original problem.

It is worth pointing out that a related idea to our proposed information jamming approach has been used in military communications without considering the secrecy rate objective [18]-[20]. In particular, the authors in [18] derived the capacity of an AWGN channel where a disruptive jammer tries to disrupt the legitimate receiver via sending a processed version of the transmitter's signal. The results in [18] was further extended to a single-user MIMO system setup in [19], and a multiuser system in [20]. Furthermore, it is worth noting that the cooperative relaying approach also uses the source signal to improve the secrecy performance of wireless networks [21]-[22]. Several relay protocols, such as amplify-and-forward (AF) [23] and decode-and-forward (DF) [24], have been studied to facilitate secure communications. The basic principle of cooperative relaying is that the external relay node first amplifies or decodes the received signal, and then transmits the amplified signal or re-encoded signal to the legitimate receiver. Although the cooperative relaying approach could enhance the received signal quality at the legitimate receiver by forwarding the processed version of the source signal, it also increases the risk of information leakage to the eavesdropper. Differently, our proposed information jamming approach is capable of not only improving the received signal strength at the legitimate receiver but also reducing that at the eavesdropper. In addition, it is noted that different from the secure coordinated multiple point transmission systems considered in [25]-[26] where each base station only knows its own transmit data, our model assumes that the transmit data is shared among all transmitters for achieving secure information jamming.

The rest of this paper is organized as follows. Section II introduces the system model and formulates the achievable secrecy rate maximization problem. Sections III and IV respectively present the optimal and suboptimal distributed designs of information jamming. Section V considers the imperfect CSI case and provides the robust information jamming beamforming design. In section VI, numerical results are presented to verify the performances of the proposed

approaches. Finally, we conclude the paper in Section VII.

Notation: For a Hermitian matrix $\mathbf{A}$, $\mathbf{A}^H$, $|\mathbf{A}|$ and $\mathrm{Tr}\,(\mathbf{A})$ denote its conjugate transpose, determinant and trace, respectively, while $\mathbf{A} \succeq 0$ means that $\mathbf{A}$ is a positive semidefinite matrix. $\mathbf{I}_M$ and $\mathbf{0}_{M\times N}$ denote the $M \times M$ identity matrix and the $M \times N$ zero matrix, respectively. $x \sim \mathcal{CN}\,(\mu, \sigma^2)$ means that x is a circularly symmetric complex Gaussian random variable with mean μ and variance σ^2. $\|\mathbf{q}\|$ computes the Euclidean norm of a complex vector $\mathbf{q}$. For a complex number z, $\angle z$ denotes its phase. $[x]^+$ is the calculation of $\max\,(0, x)$. $\lambda_{\max}\,(\mathbf{A}, \mathbf{B})$ and $\mathbf{e}_{\max}\,(\mathbf{A}, \mathbf{B})$ respectively denote the largest generalized eigenvalue and its corresponding unit-norm generalized eigenvector of matrix pencil $(\mathbf{A}, \mathbf{B})$.

II. System Model and Problem Formulation

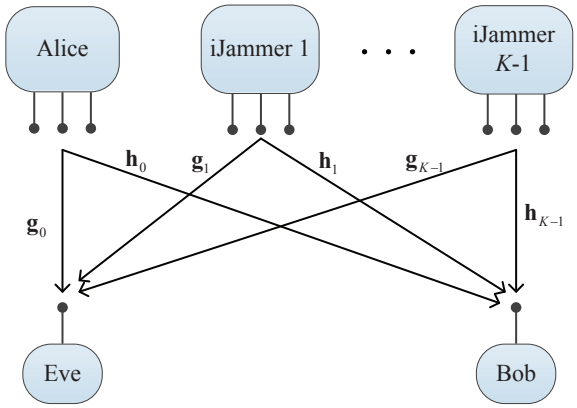

Fig. 1. System model for the MISO wiretap channel with multiple multi-antenna information jammers.

We consider a MISO wiretap channel scenario with $K-1$ friendly information jammers (iJammers) as shown in Fig. 1, where the legitimate transmitter (Alice) sends confidential messages to the legitimate receiver (Bob) in the presence of an illegal eavesdropper (Eve), who attempts to decode the confidential messages. Meanwhile, iJammers sends the same source message to strengthen the received signal at Bob and cancel the received signal at Eve. In this novel information jamming approach, iJammers exploit the source signal of Alice for designing its jamming strategy. Alice and iJammers are linked by high-capacity backhual links as in [27], they can share Alice's data signals and individual channel state information. In particular, we assume that Alice performs the optimization of beamforming vectors based on the channel state information reported from iJammers and then transfers the optimization result to them. We

consider a time-division duplexing (TDD) system, where Alice and iJammers can estimate their individual local channel state information via uplink training. Without loss of generality, we assume that Alice and iJammers are equipped with the same number of antennas, denoted by N, and Bob and Eve have a single antenna each.

For convenience, we denote the set of Alice and iJammers as $\mathcal{K} = \{0, 1, \ldots, K-1\}$, and let 0 indicate Alice and other numbers indicate iJammers. Let $\mathbf{h}_0 \in \mathbb{C}^{N\times 1}$ and $\mathbf{g}_0 \in \mathbb{C}^{N\times 1}$ denote the channel vectors from Alice to Bob and Eve, respectively, and let $\mathbf{h}_i \in \mathbb{C}^{N\times 1}$ and $\mathbf{g}_i \in \mathbb{C}^{N\times 1}$ denote the channel vectors from the ith iJammer, $i = 1, 2, \cdots, K-1$, to Bob and Eve, respectively. It is assumed that $\mathbf{h}_i$ and $\mathbf{g}_i$ are linearly independent, $\forall i \in \mathcal{K}$. Consider all channels are quasi-static flat-fading, the received complex baseband signals at Bob and Eve are respectively modeled as

$$y_b = \mathbf{h}_0^H \mathbf{x}_0 + \sum_{i=1}^{K-1} \mathbf{h}_i^H \mathbf{x}_i + z_b, \tag{1}$$

$$y_e = \mathbf{g}_0^H \mathbf{x}_0 + \sum_{i=1}^{K-1} \mathbf{g}_i^H \mathbf{x}_i + z_e, \tag{2}$$

where $\mathbf{x}_0 \in \mathbb{C}^{N\times 1}$ and $\mathbf{x}_i \in \mathbb{C}^{N\times 1}$ denote the transmitted signal vectors by Alice and the ith iJammer, respectively. $z_b \sim \mathcal{CN}(0, \sigma_b^2)$ and $z_e \sim \mathcal{CN}(0, \sigma_e^2)$ are the additive noises at Bob and Eve, respectively. Without loss of generality, we assume that $\sigma_b^2 = \sigma_e^2 = \sigma^2$.

We assume that Alice uses a beamforming vector $\mathbf{w}_0 \in \mathbb{C}^{N\times 1}$ to send confidential messages, and thus the transmitted signal vector from Alice can be given by $\mathbf{x}_0 = \mathbf{w}_0 s_a$, where $s_a \sim \mathcal{CN}(0, 1)$ is the confidential information-bearing signal. For the proposed information jamming approach, iJammers transmit the same confidential information-bearing signal shared by Alice beforehand via the secure backhaul link. Then, the transmitted signal vector $\mathbf{x}_i$ is given by $\mathbf{x}_i = \mathbf{w}_i s_a,\ \forall i = 1, \ldots, K-1$, where $\mathbf{w}_i \in \mathbb{C}^{N\times 1}$ is the beamforming vector designed by the ith iJammer.

The achievable secrecy rate of Bob can be expressed as

$$R(\{\mathbf{w}_i\}) = \Bigg[\underbrace{\log\left(1 + \frac{1}{\sigma^2}\left|\sum_{i=0}^{K-1} \mathbf{h}_i^H \mathbf{w}_i\right|^2\right)}_{R_b} - \underbrace{\log\left(1 + \frac{1}{\sigma^2}\left|\sum_{i=0}^{K-1} \mathbf{g}_i^H \mathbf{w}_i\right|^2\right)}_{R_e} \Bigg]^+, \tag{3}$$

where R_b and R_e denote the achievable rate at Bob and Eve, respectively.

Note that each term $\mathbf{h}_i^H \mathbf{w}_i, \forall i \in \mathcal{K}$ in R_b are complex numbers, if they add constructively, the received signal at Bob is strengthened and thus the achievable rate R_b is improved. Similarly,

if the terms $\mathbf{g}_i^H\mathbf{w}_i, \forall i \in \mathcal{K}$ in R_e add destructively, the received signal at Eve is weakened and hence the achievable rate $R_e\left(\mathbf{w}_i\right)$ is reduced.

In this paper, we focus on the joint beamforming design between Alice and iJammers for maximizing the achievable secrecy rate. The optimal beamforming vectors design problem is formulated as

$$\begin{aligned} \max_{\{\mathbf{w}_i\}} \quad & \log\left(1+\frac{1}{\sigma^2}\left|\sum_{i=0}^{K-1}\mathbf{h}_i^H\mathbf{w}_i\right|^2\right)-\log\left(1+\frac{1}{\sigma^2}\left|\sum_{i=0}^{K-1}\mathbf{g}_i^H\mathbf{w}_i\right|^2\right) \\ \text{s.t.} \quad & \left\|\mathbf{w}_i\right\|^2 \le P_i, \forall i \in \mathcal{K}, \end{aligned} \tag{4}$$

where P_i denotes the individual transmit power budget at ith transmitter, $\forall i \in \mathcal{K}$.

Note that the optimization method developed in [28] cannot be applied to solve problem (4) due to the individual transmit power constraints. Only under the strong assumption that the individual transmit power constraints in (4) are replaced by the single sum-power constraint $\sum_{i=0}^{K-1}\left\|\mathbf{w}_i\right\|^2 \le \sum_{i=0}^{K-1} P_i$, problem (4) can be simplified to the secrecy rate maximization problem in the conventional three-node MISO wiretap channel and then its optimal solution can be obtained in closed-form [28].

Notice that problem (4) itself is non-convex due to the non-concave objective functions, thus it is difficult to solve in general. In the next two sections, we focus on solving problem (4) by developing both optimal and suboptimal solutions.

III. Optimal Information Jamming Beamforming Design

In this section, we propose a SDR-based approach to solve the non-convex optimization problem (4) optimally.

In order to make problem (4) more tractable to solve, we first re-express the quadratic expression $\left|\sum_{i=0}^{K-1}\mathbf{h}_i^H\mathbf{w}_i\right|^2$ inside (3) as

$$\left|\sum_{i=0}^{K-1}\mathbf{h}_i^H\mathbf{w}_i\right|^2 = \left|\mathbf{a}_b^H\mathbf{v}\right|^2, \tag{5}$$

where $\mathbf{v} = \left[\mathbf{w}_0^H, \ldots, \mathbf{w}_{K-1}^H\right]^H$ is the extended vector of $\{\mathbf{w}_i\}$ and $\mathbf{a}_b = \left[\mathbf{h}_0^H, \ldots, \mathbf{h}_{K-1}^H\right]^H$.

Similarly, by defining $\mathbf{a}_e = \left[\mathbf{g}_0^H, \ldots, \mathbf{g}_{K-1}^H\right]^H$, we have

$$\left|\sum_{i=0}^{K-1}\mathbf{g}_i^H\mathbf{w}_i\right|^2 = \left|\mathbf{a}_e^H\mathbf{v}\right|^2 \tag{6}$$

By substituting (5)-(6) into problem (4) and omitting the logarithmic function due to its monotonicity, we can equivalently rewrite problem (4) as

$$\begin{aligned} \max_{\mathbf{v}} \quad & \frac{\left|\mathbf{a}_b^H\mathbf{v}\right|^2+\sigma^2}{\left|\mathbf{a}_e^H\mathbf{v}\right|^2+\sigma^2} \\ \text{s.t.} \quad & \left\|\mathbf{\Psi}_i\mathbf{v}\right\|^2 \le P_i, \forall i \in \mathcal{K}, \end{aligned} \tag{7}$$

where $\mathbf{\Psi}_i \triangleq \mathrm{Diag}\big(\underbrace{0,\ldots,0}_{iN},\underbrace{1,\ldots,1}_{N},\underbrace{0,\ldots,0}_{(K-i-1)N}\big)$ is a $KN\times KN$ square matrix. Specifically, $\mathbf{\Psi}_i$ is idempotent, i.e., $\mathbf{\Psi}_i\mathbf{\Psi}_i=\mathbf{\Psi}_i$.

Notice that although problem (7) is more tractable than problem (4), it is still non-convex. In what follows, we shall apply the technique of SDR to solve problem (7) optimally. For this purpose, we define a new optimization variable $\mathbf{V}=\mathbf{v}\mathbf{v}^H$, which follows that $\mathbf{V}\succeq 0$ and $\mathrm{Rank}\,(\mathbf{V})\le 1$. Then, we can equivalently transform problem (7) into

$$\begin{aligned} \max_{\mathbf{V}} \quad & \frac{\mathrm{Tr}\left(\mathbf{a}_b\mathbf{a}_b^H\mathbf{V}\right)+\sigma^2}{\mathrm{Tr}\left(\mathbf{a}_e\mathbf{a}_e^H\mathbf{V}\right)+\sigma^2} \\ \text{s.t.} \quad & \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{V}\right)\le P_i, \forall i\in\mathcal{K}, \\ & \mathrm{Rank}\,(\mathbf{V})=1,\ \mathbf{V}\succeq 0, \end{aligned} \tag{8}$$

where the first constraint in problem (8) comes from the fact that $\left\|\mathbf{\Psi}_i\mathbf{v}\right\|^2=\mathbf{v}^H\mathbf{\Psi}_i^H\mathbf{\Psi}_i\mathbf{v}=\mathbf{v}^H\mathbf{\Psi}_i\mathbf{v}=\mathrm{Tr}\left(\mathbf{v}^H\mathbf{\Psi}_i\mathbf{v}\right)=\mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{v}\mathbf{v}^H\right)$.

Following the SDR approach and dropping the non-convex rank-one constraint, the relaxed version of problem (8) then becomes

$$\begin{aligned} \max_{\mathbf{V}} \quad & \frac{\mathrm{Tr}\left(\mathbf{a}_b\mathbf{a}_b^H\mathbf{V}\right)+\sigma^2}{\mathrm{Tr}\left(\mathbf{a}_e\mathbf{a}_e^H\mathbf{V}\right)+\sigma^2} \\ \text{s.t.} \quad & \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{V}\right)\le P_i, \forall i\in\mathcal{K},\ \mathbf{V}\succeq 0. \end{aligned} \tag{9}$$

Let $\mathbf{V}^*$ denote the optimal solution to problem (9). If $\mathrm{Rank}\,(\mathbf{V}^*)\le 1$ finally, the relaxation is tight and there is no loss of optimality due to dropping the rank-one constraint. Then the optimal beamforming solution $\mathbf{v}^*$ to problem (7) can be obtained from the eigenvalue decomposition (EVD) of $\mathbf{V}^*$. Otherwise, if $\mathrm{Rank}\,(\mathbf{V}^*)>1$, the optimal value of problem (9) only serves as an upper bound on that of problem (8). Next, we first solve problem (9) and then check the rank of its optimal solution.

Note that problem (9) now is a quasi-convex rather than convex optimization problem due to the fractional form of objective function. We next apply the Charnes-Cooper transformation

[29] approach to further transform problem (9) into an equivalent convex optimization problem. Specifically, by introducing two new variables

$$\eta = \frac{1}{\mathrm{Tr}\left(\mathbf{a}_e\mathbf{a}_e^H\mathbf{V}\right)+\sigma^2} > 0,\ \mathbf{Q} = \eta\mathbf{V}, \tag{10}$$

we can then recast problem (9) as

$$\begin{aligned} \max_{\mathbf{Q},\eta}\quad & \mathrm{Tr}\left(\mathbf{a}_b\mathbf{a}_b^H\mathbf{Q}\right)+\eta\sigma^2 \\ \text{s.t.}\quad & \mathrm{Tr}\left(\mathbf{a}_e\mathbf{a}_e^H\mathbf{Q}\right)+\eta\sigma^2 = 1, \\ & \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{Q}\right) \le \eta P_i, \forall i \in \mathcal{K} \\ & \mathbf{Q} \succeq 0, \eta > 0. \end{aligned} \tag{11}$$

Proposition 1: Problems (9) and (11) are equivalent.

Proof: First, if $\mathbf{V}$ is any feasible solution to problem (11), then $(\mathbf{Q},\eta)$ defined in (10) is naturally feasible to problem (11) and achieves the same objective function value as that of problem (9). Second, it is easy to verify that if $(\mathbf{Q},\eta)$ is any feasible solution to problem (11), then $\mathbf{V} = \frac{\mathbf{Q}}{\eta}$ is also feasible to problem (9) and achieves the same objective function value as that of problem (11). Thus, problems (9) and (11) are equivalent in the sense that they have the same optimal objective function value. ■

From Proposition 1, the optimal solution of problem (9) can be obtained by solving problem (11) instead. Note that problem (11) is a convex SDP problem, which can be efficiently solved by using the interior-point method based convex optimization toolboxes, e.g., CVX. Also, problem (11) has one semi-definite matrix variable of size KN, and $K+1$ linear constraints. Thus, according to [31], the computational complexity of the interior-point method for solving the problem (11) is $\mathcal{O}\left(K^{4.5}N^{3.5}\log\left(1/\delta_1\right)\right)$, where δ_1 is the accuracy of solving problem (11).

Proposition 2: Let $(\mathbf{Q}^*,\eta^*)$ denote the optimal solution to problem (11), then they must satisfy that $\mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{Q}^*\right) = \eta^* P_i, \forall i \in \mathcal{K}$.

Proof: We prove Proposition 2 by contradiction. Suppose that there exists at least one $\forall i \in \mathcal{K}$ such that $\mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{Q}^*\right) < \eta^* P_i$. In this case, we can construct a new solution

$$\mathbf{Q}^\dagger = \mathbf{Q}^* + \left(\eta^* P_i - \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{Q}^*\right)\right)\mathbf{q}\mathbf{q}^H, \tag{12}$$

where $\mathbf{q} \triangleq \big[\underbrace{0,\ldots,0}_{iN},\underbrace{\tilde{\mathbf{q}}^H}_{N},\underbrace{0,\ldots,0}_{(K-i-1)N}\big]^H$ is a $NK\times 1$ complex vector, with $\tilde{\mathbf{q}} \in \mathbb{C}^{N\times 1}$ being a normalized basis vector of the null space of $\mathbf{g}_i^H$, i.e., $\mathbf{g}_i^H\tilde{\mathbf{q}} = 0$ and $\|\tilde{\mathbf{q}}\| = 1$, and satisfying $\mathbf{h}_i^H\tilde{\mathbf{q}} \neq 0$. Note that we can always find a feasible $\tilde{\mathbf{q}}$ because $\mathbf{h}_i$ and $\mathbf{g}_i$ are linearly independent as

we have assumed. Then, it is easy to check that $\left(\mathbf{Q}^{\dagger}, \eta^{*}\right)$ satisfies all the constraints of problem (11) and achieves a larger objective function value than that by $(\mathbf{Q}^{*}, \eta^{*})$, which contradicts the pre-assumption that $(\mathbf{Q}^{*}, \eta^{*})$ is optimal to problem (11). Hence, the proof Proposition 2 is completed. ■

Proposition 2 indicates that Alice and iJammers should transmit with their maximum power for maximizing the secrecy rate.

Next, we further provide the following theorem, which studies the rank property of $\mathbf{Q}^{*}$.

Theorem 1: The optimal $\mathbf{V}^{*}$ to problem (9) is of rank one, i.e., $\mathrm{Rank}\left(\mathbf{V}^{*}\right) = 1$.

Proof: The Lagrangian of problem (11) is expressed as

$$\mathcal{L}\left(\mathbf{Q}, \eta, \alpha, \{\beta_i\}\right) = \mathrm{Tr}\left(\mathbf{\Phi}\mathbf{Q}\right) + \xi\eta + \alpha \tag{13}$$

where $\mathbf{\Phi} = \left(\mathbf{a}_b\mathbf{a}_b^H - \alpha\mathbf{a}_e\mathbf{a}_e^H - \sum_{i=0}^{K-1}\beta_i\mathbf{\Psi}_i\right)$, $\xi = (1-\alpha)\,\sigma^2 + \sum_{i=0}^{K-1}\beta_i P_i$, with α and $\beta_i \geq 0, \forall i \in \mathcal{K}$ being the dual variables associated with the first two constraints in problem (11).

The Lagrangian dual function is then given by

$$\begin{aligned} g\left(\alpha, \{\beta_i\}\right) &= \max_{\mathbf{Q},\eta} \quad \mathcal{L}\left(\mathbf{Q}, \eta, \alpha, \{\beta_i\}\right) \\ &= \begin{cases} \alpha, & \text{if } \mathbf{\Phi} \preceq 0, \xi \leq 0 \\ +\infty, & \text{otherwise} \end{cases} \end{aligned} \tag{14}$$

To ensure that the Lagrangian in (13) is bounded from above, its dual problem is thus expressed as

$$\begin{aligned} \min_{\alpha,\{\beta_i\}} \quad & \alpha \\ \text{s.t.} \quad & \mathbf{\Phi} \preceq 0,\ \xi \leq 0,\ \beta_i \geq 0,\ \forall i \in \mathcal{K} \end{aligned} \tag{15}$$

Let α^{*} and $\{\beta_i^{*}\}$ denote the optimal solution to problem (15). The resulting values of $\mathbf{\Phi}$ and ξ are $\mathbf{\Phi}^{*}$ and ξ^{*}, respectively. Then, the optimal solution to problem (11), denoted by $\mathbf{Q}^{*}$ and η^{*}, should satisfy the following complementary slackness conditions

$$\mathrm{Tr}\left(\mathbf{\Phi}^{*}\mathbf{Q}^{*}\right) = 0,\ \xi^{*}\eta^{*} = 0, \tag{16}$$

$$\beta_i^{*}\left(\mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{Q}^{*}\right) - \eta^{*}P_i\right) = 0, \forall i \in \mathcal{K}, \tag{17}$$

The condition $\mathrm{Tr}\left(\mathbf{\Phi}^{*}\mathbf{Q}^{*}\right) = 0$ is equivalent to $\mathbf{\Phi}^{*}\mathbf{Q}^{*} = 0$, which means that $\mathbf{Q}^{*}$ lies in the null space of $\mathbf{\Phi}^{*}$. According to Proposition 2 and (17), we know that $\beta_i^{*} > 0, \forall i \in \mathcal{K}$. Moreover, we have

$$\mathrm{Rank}\left(\mathbf{\Phi}^{*}\right) = \mathrm{Rank}\left(-\mathbf{\Phi}^{*}\right) \geq \mathrm{Rank}\left(\sum_{i=0}^{K-1}\beta_i^{*}\mathbf{\Psi}_i^{*} + \alpha^{*}\mathbf{a}_e\mathbf{a}_e^H\right) - \mathrm{Rank}\left(\mathbf{a}_b\mathbf{a}_b^H\right) \tag{18}$$

Note that since problem (11) is convex and satisfies the Slater's condition [30], the duality gap is zero. Hence, α^* is equal to the optimal value of (11), which is obvious larger than 0. Thus, we have $\alpha^* > 0$. Therefore, we obtain that $\mathrm{Rank}\left(\sum_{i=0}^{K-1}\beta_i^*\mathbf{\Psi}_i^* + \alpha^*\mathbf{a}_e\mathbf{a}_e^H\right) = NK$ since $\sum_{i=0}^{K-1}\beta_i^*\mathbf{\Psi}_i^* + \alpha^*\mathbf{a}_e\mathbf{a}_e^H$ is a positive definite matrix. Thus, we have

$$\mathrm{Rank}\,(\mathbf{\Phi}^*) \geq NK - 1. \tag{19}$$

As a result, it follows that

$$\mathrm{Rank}\,(\mathbf{Q}^*) = NK - \mathrm{Rank}\,(\mathbf{\Phi}^*) \leq 1. \tag{20}$$

Moreover, it is obvious that $\mathbf{Q} = 0$ cannot be the optimal solution. Thus, we have $\mathrm{Rank}\,(\mathbf{Q}^*) = 1$, which completes the proof of Theorem 1. ■

According to Eq. (10) and Theorem 1, we know that the optimal solution to problem (9) is $\mathbf{V}^* = \frac{\mathbf{Q}^*}{\eta^*}$, satisfying $\mathrm{Rank}\,(\mathbf{V}) \leq 1$. Thus, the rank relaxation on $\mathbf{V}$ from problem (8) to problem (9) results in no loss of optimality.

To summarize, the original beamforming design problem (4) can be optimally solved by the following steps. First, we obtain the optimal solution $(\mathbf{Q}^*, \eta^*)$ of problem (11) via CVX, then $\mathbf{V}^* = \frac{\mathbf{Q}^*}{\eta^*}$ will be the optimal solution to problem (9). Since $\mathrm{Rank}\,(\mathbf{V}^*) = 1$, the optimal solution $\mathbf{v}^*$ to problem (8) can be obtained by the EVD of $\mathbf{V}^*$. Finally, the optimal solution $\{\mathbf{w}_i^*\}$ to the original problem (4) can be recovered from $\mathbf{v}^*$ accordingly.

IV. Suboptimal Distributed Information Jamming Beamforming Design

In the previous section, we have solved the problem (4) optimally based on the numerical optimization approach. Note that the optimal solution requires centralized optimization and a certain amount of information exchange between Alice and iJammers. For example, iJammers needs to report their CSI to Alice first, and then Alice feeds the optimization results back to iJammers. To reduce the computation complexity and the information exchange overhead, in this section, we propose a suboptimal but distributed information jamming beamforming design scheme, called separate zero-forcing (SZF). The optimal solution of the SZF scheme is obtained in closed-form.

For the SZF scheme, each transmitter designs its beamforming vectors independently using only local CSI. The design objective is to maximize the received signal strength at the legiti-

mate receiver while avoiding information leakage to the eavesdropper. As a result, the desired beamforming vectors are the optimal solution of the following optimization problem.

$$\begin{aligned} \max_{\{\mathbf{w}_i\}} \quad & \left| \sum_{i=0}^{K-1} \mathbf{h}_i^H \mathbf{w}_i \right|^2 \\ \text{s.t.} \quad & \mathbf{g}_i^H \mathbf{w}_i = 0, \ \ \|\mathbf{w}_i\|^2 \leq P_i, \ \forall i \in \mathcal{K}. \end{aligned} \tag{21}$$

We then have the following Proposition, which provides the optimal solution to problem (21).

Proposition 3: The closed-form optimal beamforming solution to problem (21) is given by

$$\hat{\mathbf{w}}_i^* = \sqrt{P_i} \frac{\left(\mathbf{I} - \hat{\mathbf{g}}_i \hat{\mathbf{g}}_i^H\right) \mathbf{h}_i e^{j\theta_i^*}}{\left\|\left(\mathbf{I} - \hat{\mathbf{g}}_i \hat{\mathbf{g}}_i^H\right) \mathbf{h}_i\right\|}, \ \forall i \in \mathcal{K}, \tag{22}$$

where $\hat{\mathbf{g}}_i = \frac{\mathbf{g}_i}{\|\mathbf{g}_i\|}$, $\theta_i^* = -\angle \mathbf{h}_i^H \mathbf{w}_i^*$, and $\mathbf{w}_i^* = \sqrt{P_i} \frac{\left(\mathbf{I} - \hat{\mathbf{g}}_i \hat{\mathbf{g}}_i^H\right) \mathbf{h}_i}{\left\|\left(\mathbf{I} - \hat{\mathbf{g}}_i \hat{\mathbf{g}}_i^H\right) \mathbf{h}_i\right\|}$.

Proof: By applying the triangle inequality to the objective function of problem (21), we have

$$\left| \sum_{i=0}^{K-1} \mathbf{h}_i^H \mathbf{w}_i \right|^2 \leq \left(\sum_{i=0}^{K-1} \left| \mathbf{h}_i^H \mathbf{w}_i \right| \right)^2. \tag{23}$$

The equality of the above inequality holds when each term of the form $\mathbf{h}_i^H \mathbf{w}_i$, $\forall i \in \mathcal{K}$, has the same phase angle, i.e., $\angle \mathbf{h}_0^H \mathbf{w}_0 = \ldots = \angle \mathbf{h}_{K-1}^H \mathbf{w}_{K-1}$. Note that any phase rotation of $\mathbf{w}_i, \forall i \in \mathcal{K}$ does not change the feasibility of the constraints in problem (21), i.e., if $\mathbf{g}_i^H \mathbf{w}_i = 0$ and $\|\mathbf{w}_i\|^2 \leq P_i$, then $\mathbf{g}_i^H \mathbf{w}_i e^{j\theta_i} = 0$ and $\left\|\mathbf{w}_i e^{j\theta_i}\right\|^2 \leq P_i$ are satisfied for any θ_i. Therefore, we can always find a set of feasible $\{\mathbf{w}_i\}$ such that $\angle \mathbf{h}_0^H \mathbf{w}_0 = \ldots = \angle \mathbf{h}_{K-1}^H \mathbf{w}_{K-1}$. Thus, the equality in (23) must hold for maximizing the objective function of (21) when the optimal solution is achieved. Moreover, notice that maximizing the right hand side of (23) is equivalent to maximize each term of the form $\left|\mathbf{h}_i^H \mathbf{w}_i\right|, \forall i \in \mathcal{K}$ since they are separable over $\mathbf{w}_i$. As a result, problem (21) can be decomposed into the following K independent subproblems:

$$\begin{aligned} \max_{\mathbf{w}_i} \quad & \left|\mathbf{h}_i^H \mathbf{w}_i\right|^2 \\ \text{s.t.} \quad & \mathbf{g}_i^H \mathbf{w}_i = 0, \|\mathbf{w}_i\|^2 \leq P_i, \ \forall i \in \mathcal{K}. \end{aligned} \tag{24}$$

Following the similar proof of Lemma 2 in [33], we can obtain that the optimal solution to problem (24) is

$$\mathbf{w}_i^* = \sqrt{P_i} \frac{\left(\mathbf{I} - \hat{\mathbf{g}}_i \hat{\mathbf{g}}_i^H\right) \mathbf{h}_i}{\left\|\left(\mathbf{I} - \hat{\mathbf{g}}_i \hat{\mathbf{g}}_i^H\right) \mathbf{h}_i\right\|}, \ \forall i \in \mathcal{K}. \tag{25}$$

where $\hat{\mathbf{g}}_i = \frac{\mathbf{g}_i}{\|\mathbf{g}_i\|}$.

Finally, the optimal solution to problem (21) has the following form:

$$\hat{\mathbf{w}}^* = \mathbf{w}_i^* e^{j\theta_i^*},\ \forall i \in \mathcal{K}. \tag{26}$$

where $\{\theta_i^*\}$ is chosen to make $\angle \mathbf{h}_0^H \mathbf{w}_0^* = \cdots = \angle \mathbf{h}_{K-1}^H \mathbf{w}_{K-1}^* = \theta$. Without loss of generality, we set $\theta = 0$ and thus $\theta_i^* = -\angle \mathbf{h}_i^H \mathbf{w}_i^*, \forall i \in \mathcal{K}$.

The proof is thus completed.

■

From Proposition 3, we can see that the $\hat{\mathbf{w}}^*$ only depends on the ith transmitter's local CSI of $\mathbf{h}_i$ and $\mathbf{g}_i$. Hence, the optimal beamforming solution of the SZF scheme can be implemented in a distributed manner, which significantly reduces the information exchange overhead and is thus easy to implement in practice.

According to Proposition 3, the achievable secrecy rate of the SZF scheme is thus given by $R^{\mathrm{SZF}} = \log\left(1 + \frac{1}{\sigma^2}\left|\sum_{i=0}^{K-1} \mathbf{h}_i^H \hat{\mathbf{w}}_i^*\right|^2\right)$.

V. Robust Information Jamming Beamforming Design

In the previous sections, we have studied the secure beamforming design under the assumption that transmitters have the perfect CSI of all the relevant channels. In this section, we extend our study to the case where only the imperfect CSI is available at each transmitter. Specifically, we aim at maximizing the ϵ-outage secrecy rate by optimizing the beamforming vectors under the stochastic CSI errors model. The corresponding outage secrecy rate maximization problem is formulated as

$$\begin{aligned} \max_{\{\mathbf{w}_i\}, R} \quad & R \\ \text{s.t.} \quad & \Pr\left(\log\left(1 + \frac{1}{\sigma^2}\left|\sum_{i=0}^{K-1} \mathbf{h}_i^H \mathbf{w}_i\right|^2\right) - \log\left(1 + \frac{1}{\sigma^2}\left|\sum_{i=0}^{K-1} \mathbf{g}_i^H \mathbf{w}_i\right|^2\right) \le R\right) \le \epsilon \\ & \|\mathbf{w}_i\|^2 \le P_i, \forall i \in \mathcal{K}, \end{aligned} \tag{27}$$

where ϵ denotes the secrecy outage probability, which specifies the maximum tolerable probability that the achievable secrecy rate is smaller than R. Following the stochastic CSI errors model [34]-[35], $\mathbf{h}_i$ and $\mathbf{g}_i$ in (27) are given by

$$\mathbf{h}_i = \hat{\mathbf{h}}_i + \Delta\mathbf{h}_i,\ \mathbf{g}_i = \hat{\mathbf{g}}_i + \Delta\mathbf{g}_i, \forall i \in \mathcal{K}, \tag{28}$$

where $\hat{\mathbf{h}}_i$ and $\hat{\mathbf{g}}_i$ are the estimate of the actual channel $\mathbf{h}_i$ and $\mathbf{g}_i$, respectively, $\Delta\mathbf{h}_i$ and $\Delta\mathbf{g}_i$ are the corresponding stochastic CSI errors, which, respectively, follows the distribution $\Delta\mathbf{h}_i \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{E}_i^h\right)$ and $\Delta\mathbf{g}_i \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{E}_i^g\right)$, with $\mathbf{E}_{h_i} \succ 0$ and $\mathbf{E}_{g_i} \succ 0$.

By defining $\Delta\mathbf{a}_b = \left[\Delta\mathbf{h}_0^H, \Delta\mathbf{h}_1^H, \ldots, \Delta\mathbf{h}_{K-1}^H\right]^H \in \mathbb{C}^{KN\times 1}$, we have

$$\begin{aligned}\left|\sum_{i=0}^{K-1}\mathbf{h}_i^H\mathbf{w}_i\right|^2 &= \left|\left(\mathbf{a}_b+\Delta\mathbf{a}_b\right)^H\mathbf{v}\right|^2 \\ &= \Delta\mathbf{a}_b^H\mathbf{V}\Delta\mathbf{a}_b + 2\mathrm{Re}\left\{\Delta\mathbf{a}_b^H\mathbf{V}\mathbf{a}_b\right\} + \mathbf{a}_b^H\mathbf{V}\mathbf{a}_b.\end{aligned} \tag{29}$$

Similarly, by defining $\Delta\mathbf{a}_e = \left[\Delta\mathbf{g}_0^H, \Delta\mathbf{g}_1^H, \ldots, \Delta\mathbf{g}_{K-1}^H\right]^H \in \mathbb{C}^{KN\times 1}$, we have

$$\left|\sum_{i=0}^{K-1}\mathbf{g}_i^H\mathbf{w}_i\right|^2 = \Delta\mathbf{a}_e^H\mathbf{V}\Delta\mathbf{a}_e + 2\mathrm{Re}\left\{\Delta\mathbf{a}_e^H\mathbf{V}\mathbf{a}_e\right\} + \mathbf{a}_e^H\mathbf{V}\mathbf{a}_e, \tag{30}$$

By substituting (29) and (30) into the first constraint of (27), yields

$$\Pr\left(\frac{\Delta\mathbf{a}_b^H\mathbf{V}\Delta\mathbf{a}_b + 2\mathrm{Re}\left\{\Delta\mathbf{a}_b^H\mathbf{V}\mathbf{a}_b\right\} + \mathbf{a}_b^H\mathbf{V}\mathbf{a}_b + \sigma^2}{\Delta\mathbf{a}_e^H\mathbf{V}\Delta\mathbf{a}_e + 2\mathrm{Re}\left\{\Delta\mathbf{a}_e^H\mathbf{V}\mathbf{a}_e\right\} + \mathbf{a}_e^H\mathbf{V}\mathbf{a}_e + \sigma^2} \le 2^R\right) \le \epsilon, \tag{31}$$

which can be further reformulated as

$$\Pr\left(\Delta\mathbf{a}^H\tilde{\mathbf{V}}\Delta\mathbf{a} + 2\mathrm{Re}\left\{\Delta\mathbf{a}^H\tilde{\mathbf{V}}\mathbf{a}\right\} + \mathbf{a}^H\tilde{\mathbf{V}}\mathbf{a} \le \left(2^R-1\right)\sigma^2\right) \le \epsilon, \tag{32}$$

where $\Delta\mathbf{a} = \begin{bmatrix}\Delta\mathbf{a}_b \\ \Delta\mathbf{a}_e\end{bmatrix} \in \mathbb{C}^{2KN\times 1}$, $\tilde{\mathbf{V}} = \begin{bmatrix}\mathbf{V} & \mathbf{0} \\ \mathbf{0} & -2^R\mathbf{V}\end{bmatrix} \in \mathbb{C}^{2KN\times 2KN}$, and $\mathbf{a} = \begin{bmatrix}\mathbf{a}_b \\ \mathbf{a}_e\end{bmatrix} \in \mathbb{C}^{2KN\times 1}$.

By substituting (32) into (27), we can rewrite it as

$$\begin{aligned}&\max_{\mathbf{V},R} \quad R \\ &\text{s.t.} \quad (32),\ \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{V}\right) \le P_i, \forall i \in \mathcal{K},\ \mathrm{Rank}\left(\mathbf{V}\right) = 1,\ \mathbf{V} \succeq 0.\end{aligned} \tag{33}$$

Notice that the first constraint in problem (33) is a chance constraint, which leads to problem (33) difficult to solve. To deal with this circumstance, we will transform this chance constraint into a deterministic form by applying the Bernstein-type inequality. To this end, we rewrite the CSI error vectors as $\Delta\mathbf{h}_i = \mathbf{E}_{h_i}^{1/2}\bar{\mathbf{h}}_i$ and $\Delta\mathbf{g}_i = \mathbf{E}_{g_i}^{1/2}\bar{\mathbf{g}}_i$, with $\bar{\mathbf{h}}_i \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_N\right)$ and $\bar{\mathbf{g}}_i \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_N\right),\ \forall i \in \mathcal{K}$. For notation simplicity, we define $\bar{\mathbf{h}} = \left[\bar{\mathbf{h}}_0^H, \bar{\mathbf{h}}_1^H, \cdots, \bar{\mathbf{h}}_{K-1}^H\right]^H \in \mathbb{C}^{KN\times 1}$, $\bar{\mathbf{g}} = \left[\bar{\mathbf{g}}_0^H, \bar{\mathbf{g}}_1^H, \cdots, \bar{\mathbf{g}}_{K-1}^H\right]^H \in \mathbb{C}^{KN\times 1}$, $\mathbf{E}_h = \mathrm{diag}\left\{\mathbf{E}_{h_0}^{1/2}, \mathbf{E}_{h_1}^{1/2}, \cdots, \mathbf{E}_{h_{K-1}}^{1/2}\right\} \in \mathbb{C}^{KN\times KN}$ and $\mathbf{E}_g = \mathrm{diag}\left\{\mathbf{E}_{g_0}^{1/2}, \mathbf{E}_{g_1}^{1/2}, \cdots, \mathbf{E}_{g_{K-1}}^{1/2}\right\} \in \mathbb{C}^{KN\times KN}$. Then, we have

$$\Delta\mathbf{a} = \mathbf{E}\mathbf{x}, \tag{34}$$

where $\mathbf{E}=\begin{bmatrix}\mathbf{E}_h & \mathbf{0}\\ \mathbf{0} & \mathbf{E}_g\end{bmatrix}\in\mathbb{C}^{2KN\times 2KN}$ and $\mathbf{x}=\begin{bmatrix}\bar{\mathbf{h}}\\ \bar{\mathbf{g}}\end{bmatrix}\in\mathbb{C}^{2KN\times 1}$.

Then, by substituting (34) into (32), it follows that

$$\Pr\Big(\mathbf{x}^H\underbrace{\mathbf{E}^H\tilde{\mathbf{V}}\mathbf{E}}_{\triangleq\,\boldsymbol{\Xi}}\mathbf{x}+2\mathrm{Re}\big\{\mathbf{x}^H\underbrace{\mathbf{E}^H\tilde{\mathbf{V}}\mathbf{a}}_{\triangleq\,\bar{\mathbf{a}}}\big\}\le\underbrace{\left(2^R-1\right)\sigma^2-\mathbf{a}\tilde{\mathbf{V}}\mathbf{a}^H}_{\triangleq\,c}\Big)\le\epsilon. \tag{35}$$

To transform the chance constraint (35) into a deterministic form, we need the following lemma.

Lemma 1: [36] Let $\mathbf{G}=\mathbf{y}^H\mathbf{A}\mathbf{y}+2\mathrm{Re}\left\{\mathbf{y}^H\mathbf{z}\right\}$, where $\mathbf{A}\in\mathrm{H}^N$ denotes a complex hermitian matrix, $\mathbf{z}\in\mathbb{C}^N$, and $\mathbf{y}\sim\mathcal{CN}\left(\mathbf{0},\mathbf{I}\right)$. Then, for any $\varsigma\ge 0$, we have

$$\Pr\left\{\mathbf{G}\le\mathrm{Tr}\left(\mathbf{A}\right)-\sqrt{2\varsigma}\sqrt{\left\|\mathrm{vec}\left(\mathbf{A}\right)\right\|^2+2\left\|\mathbf{z}\right\|^2}-\varsigma s^-\left(\mathbf{A}\right)\right\}\le\exp\left(-\varsigma\right), \tag{36}$$

where $s^-\left(\mathbf{A}\right)=\max\left\{\lambda_{\max}\left(-\mathbf{A}\right),0\right\}$, with $\lambda_{\max}\left(\mathbf{A}\right)$ being the maximum eigenvalue of $\mathbf{A}$.

According to Lemma 1, (35) can be transformed into the following deterministic form.

$$\mathrm{Tr}\left(\boldsymbol{\Xi}\right)-\sqrt{2\sigma_\epsilon}\sqrt{\left\|\mathrm{vec}\left(\boldsymbol{\Xi}\right)\right\|^2+2\left\|\bar{\mathbf{a}}\right\|^2}-\sigma_\epsilon s^-\left(\boldsymbol{\Xi}\right)\ge c \tag{37}$$

where $\sigma_\epsilon=-\ln\left(\epsilon\right)$.

By substituting (37) into (33) and dropping the non-convex rank-one constraint, we obtain

$$\begin{aligned}\max_{\mathbf{V},R}\quad & R\\ \text{s.t.}\quad & (37),\quad \mathrm{Tr}\left(\boldsymbol{\Psi}_i\mathbf{V}\right)\le P_i,\forall i\in\mathcal{K},\ \mathbf{V}\succeq 0,\end{aligned} \tag{38}$$

which is equivalent to

$$\begin{aligned}\max_{\mathbf{V},R,\mu,\nu}\quad & R\\ \text{s.t.}\quad & \mathrm{Tr}\left(\boldsymbol{\Xi}\right)-\sqrt{2\sigma_\epsilon}\mu-\sigma_\epsilon\nu\ge c,\\ & \left|\begin{array}{c}\mathrm{vec}\left(\boldsymbol{\Xi}\right)\\ \sqrt{2}\bar{\mathbf{a}}\end{array}\right|\le\mu,\\ & \nu\mathbf{I}+\boldsymbol{\Xi}\succeq\mathbf{0},\ \mathrm{Tr}\left(\boldsymbol{\Psi}_i\mathbf{V}\right)\le P_i,\forall i\in\mathcal{K},\\ & \mu\ge 0,\ \nu\ge 0,\ \mathbf{V}\succeq 0.\end{aligned} \tag{39}$$

By applying the theory of Schur complement [30], the second constraint in (39) can be equivalently transformed into the following linear matrix inequality (LMI) constraint.

$$\mathbf{F}=\begin{bmatrix}\mu\mathbf{I}_{4K^2N^2+2KN} & \begin{bmatrix}\mathrm{vec}\left(\boldsymbol{\Xi}\right)\\ \sqrt{2}\bar{\mathbf{a}}\end{bmatrix}\\ \left[\mathrm{vec}\left(\boldsymbol{\Xi}\right)^H,\sqrt{2}\bar{\mathbf{a}}^H\right] & \mu\end{bmatrix}\succeq\mathbf{0}, \tag{40}$$

By substituting (40) into problem (39), we finally arrive at

$$\begin{aligned} \max_{\mathbf{V},R,\mu,\nu} \quad & R \\ \text{s.t.} \quad & \mathrm{Tr}\left(\mathbf{\Xi}\right) - \sqrt{2\sigma_\epsilon}\mu - \sigma_\epsilon\nu \geq c, \ (40), \\ & \nu\mathbf{I} + \mathbf{\Xi} \succeq \mathbf{0}, \ \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{V}\right) \leq P_i, \forall i \in \mathcal{K}, \\ & \mu \geq 0, \ \nu \geq 0, \ \mathbf{V} \succeq 0. \end{aligned} \tag{41}$$

Notice that problem (41) is non-convex with respect to all the optimization variables. However, it is a convex SDP feasibility problem when R is fixed. Therefore, we can solve problem (41) by solving a sequence of SDP feasibility problems. For each fixed R, the feasibility problem is given by

$$\begin{aligned} \text{Find} \quad & \{\mathbf{V}, \mu, \nu\} \\ \text{s.t.} \quad & \mathrm{Tr}\left(\mathbf{\Xi}\right) - \sqrt{2\sigma_\epsilon}\mu - \sigma_\epsilon\nu \geq c, \ (40), \\ & \nu\mathbf{I} + \mathbf{\Xi} \succeq \mathbf{0}, \ \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{V}\right) \leq P_i, \forall i \in \mathcal{K}, \\ & \mu \geq 0, \ \nu \geq 0, \ \mathbf{V} \succeq 0. \end{aligned} \tag{42}$$

If problem (42) is feasible for a fixed R, then the optimal solution to problem (41) for R, denoted by R^*, must satisfy $R^* \geq R$; otherwise, $R^* < R$. Therefore, we can apply the bisection method to find the optimal R^*. Moreover, to check the feasibility of problem (42) for a fixed R, we turn to solve the following convex SDP problem.

$$\begin{aligned} \min_{\mathbf{V},\mu,\nu} \quad & \mathrm{Tr}\left(\mathbf{\Psi}_0\mathbf{V}\right) \\ \text{s.t.} \quad & \mathrm{Tr}\left(\mathbf{\Xi}\right) - \sqrt{2\sigma_\epsilon}\mu - \sigma_\epsilon\nu \geq c, \ (40), \\ & \nu\mathbf{I} + \mathbf{\Xi} \succeq \mathbf{0}, \ \mathrm{Tr}\left(\mathbf{\Psi}_i\mathbf{V}\right) \leq P_i, \forall i = 1, \ldots, K-1, \\ & \mathbf{V} \succeq 0, \ \mu \geq 0, \ \nu \geq 0 \end{aligned} \tag{43}$$

Let $\mathbf{V}^*$ and $p_0^* = \mathrm{Tr}\left(\mathbf{\Psi}_0\mathbf{V}^*\right)$ denote the optimal solution and optimal value of problem (43), respectively. It is easy to verify that if $p_0^* \leq P_0$, then (39) is feasible; otherwise, if $p_0^* \geq P_0$, (39) is infeasible.

To summarize, the bisection method-based approach for solving problem (27) is given in Algorithm 1. Its computational complexity is analyzed as follows. The number of iterations required for the bisection method is $N_{\text{iter}} = \left\lceil \log\left(\frac{R_{\max}-R_{\min}}{\delta_2}\right)\right\rceil$, where $\lceil z \rceil$ represents the smallest integer not less than z, and δ_2 denotes the desired accuracy of bisection method.

Algorithm 1: Bisection method-based algorithm for solving problem (27).

1: **Initialize:** $R_{\min}=0$, $R_{\max}=\hat{R}$.

2: **Repeat**

(a). Set $R \leftarrow 1/2\,(R_{\min}+R_{\max})$.

(b). Solve the feasibility problem (43) with a fixed R.

(c). If $p_0^* \le P_0$, set $R_{\min} \leftarrow R$ and $\mathbf{V}_{\rm opt} \leftarrow \mathbf{V}^*$; otherwise, set $R_{\max}=R$.

3: **Until** $R_{\max}-R_{\min} \le \delta_2$

4: Obtain $\mathbf{v}^*$ by EVD of $\mathbf{V}_{\rm opt}$.

5: Recover $\{\mathbf{w}_i^*\}$ to problem (27) from $\mathbf{v}^*$.

In each iteration, the SDP problem (43) is solved to help check the feasibility of problem (42) for a fixed R. Note that problem (43) has one semi-definite matrix variable of size KN and $K+2$ linear constraints. Thus, it has the same computational complexity order as that of problem (11) [31], given by $\mathcal{O}\left(K^{4.5}N^{3.5}\log\left(1/\delta_1\right)\right)$. Hence, the total complexity of Algorithm 1 is $\mathcal{O}\left(N_{\rm iter}K^{4.5}N^{3.5}\log\left(1/\delta_1\right)\right)$.

Proposition 4: The optimal solution to problem (43) satisfies $\mathrm{Rank}\left(\mathbf{V}^*\right)=1$.

Proof: The proof is similar to that of Theorem 2 in [35], and is thus omitted for brevity. ■

Proposition 4 indicates that if problem (42) is feasible for a fixed R, then we can always find a rank-one feasible solution by solving problem (43). As a result, the optimal $\mathbf{V}^*$ to problem (38) is also rank-one matrix. Hence, the rank-one relaxation on $\mathbf{V}$ results in no loss of optimality to problem (33).

VI. Numerical Results

In this section, we numerically evaluate the performances of our proposed information jamming approaches. We assume that there is only one iJammer, i.e., $K=2$. The numbers of transmit antennas at Alice and iJammer are set to $N=2$. We consider the Cartesian coordinate system with X and Y axes, where Alice, Bob and Eve are respectively located at ground points $(0,0)$, $(100\ \mathrm{m}, -50\ \mathrm{m})$ and $(100\ \mathrm{m}, 50\ \mathrm{m})$, and (x_j, y_j) denote the ground location of iJammer. Unless otherwise specified, $(x_j, y_j)=(50\ \mathrm{m}, -50\ \mathrm{m})$. For the channel models, we consider both small-scale Rayleigh fading and large-scale path loss. As such, we have

$$\mathbf{h}_i = \begin{cases} \tilde{\mathbf{h}}_i\sqrt{A_0\left(\frac{d_i}{d_0}\right)^{-\alpha}}, & d_i > d_0 \\ \tilde{\mathbf{h}}_i\sqrt{A_0}, & \text{otherwise} \end{cases}, \forall i=0,1, \tag{44}$$

where $\tilde{\mathbf{h}}_i$ denotes the Rayleigh fading component with each element being an independent and identically distributed (i.i.d.) circular complex Gaussian random variable with zero mean and unit variance; A_0 is the constant path-loss corresponding to the reference distance $d_0 = 1$ m; d_i denotes the distance between the transmitter and the receiver; α is the path loss exponent. We set $A_0 = 10^{-3}$ and $\alpha = 2.5$. The channel vectors $\{\mathbf{g}_i\}, \forall i = 0, 1$, are generated following the same principle as for $\{\mathbf{h}_i\}$. In addition, we set the maximum transmit power at Alice as $P_0 = 10$ dBm, and the noise power at Bob and Eve as $\sigma^2 = -70$ dBm. All the results also obtained by averaging over 1000 independent channel realizations.

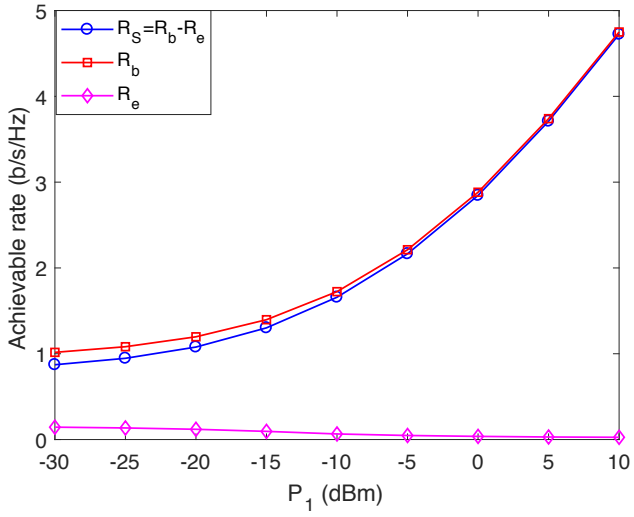

Fig. 2. Illustration of the principle of the proposed information jamming approach for the perfect CSI case.

A. Performance Evaluation Under Perfect CSI

First, we consider the perfect CSI case. Fig. 2 illustrates the fundamental principle of the proposed information jamming approach. R_b and R_e denote the achievable rates at the legitimate receiver Bob and the eavesdropper Eve, respectively. R_s denotes the achievable secrecy rate, which is the difference between R_b and R_e, i.e., $R_s = R_b - R_e$. From Fig. 2, we can see that as the iJammer's transmit power P_1 increases, the achievable rate at Bob monotonically increases, while the achievable rate at Eve monotonically decreases until it becomes equal to zero. This result is expected since our proposed information jamming approach is capable of simultaneously improving the received signal strength at Bob and reducing that at Eve for jointly maximizing the achievable secrecy rate.

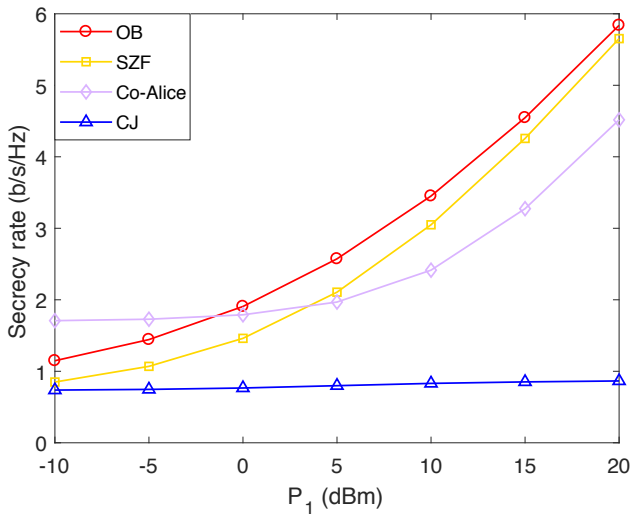

Fig. 3. Comparison of the secrecy rates of our proposed schemes, the traditional cooperative jamming scheme, and the Co-Alice scheme, under different transmit power budgets of iJammer.

Fig. 3 shows the secrecy rates achieved by our proposed solutions including the optimal beamforming solution (labeled as "OB") in Section III and the suboptimal distributed beamforming solution "SZF" in Section IV, and it also compares with the secrecy rate achieved by the co-located Alice scheme (labeled as "Co-Alice") and the traditional cooperative jamming scheme (labeled as "CJ"). For the Co-Alice scheme, iJammer is located at the position of Alice and they share the total transmit power and transmit antenna. This scheme corresponds to the conventional three-node MISO wiretap channel with the legitimate transmitter having more transmit resources. Hence, the achievable secrecy rate of Co-Alice scheme can be obtained from [28]. On the other hand, for the conventional cooperative jamming scheme, the helper node sends noise signals and the corresponding achievable secrecy rate can be calculated by using an iterative algorithm [38].

From Fig. 3, we can see that our proposed information jamming approach with the optimal solution outperforms the Co-Alice scheme when $P_1 \geq 0$ dBm. This is because the position of iJammer is closer to Bob and Eve, thus it can obviously improve the achievable secrecy rate by enhancing the signal strength at Bob and canceling the signal strength at Eve simultaneously when P_1 is large enough. However, when $P_1 < 0$ dBm, we notice that the Co-Alice scheme outperforms our proposed information jamming approach with the optimal solution. The reason is that in this case, the impact of iJammer on the achievable secrecy rate is already very small,

and therefore the achievable secrecy rate depends mainly on the number of antennas and the available transmit power at Alice. Moreover, we observe that the achievable secrecy rate of our proposed information jamming approach with the optimal solution is always greater than that of the cooperative jamming scheme, which demonstrates the advantage of our proposed information jamming approach. In addition, we also observe that with the increase of P_1, the performance gap between our proposed information jamming approach with the optimal solution and the suboptimal scheme gradually decreases. This is because as P_1 increases, iJammer has more capability and tends to cancel out the received signal at Bob to maximize the achievable eavesdropping secrecy rate. As such, the performance of the suboptimal SZF scheme gradually approaches that of the optimal solution.

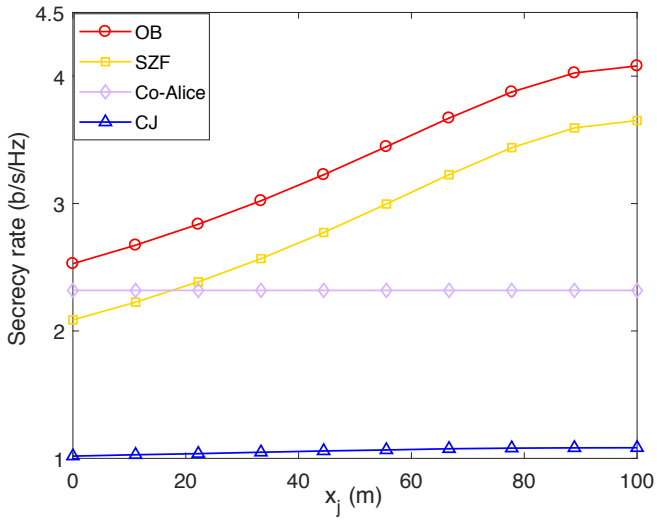

Fig. 4. Comparison of the secrecy rates of our proposed schemes, the traditional cooperative jamming scheme, and the Co-Alice scheme, under different locations of iJammer.

Next, we study the effect of the iJammer's location on the achievable secrecy rate with different cooperative schemes. We set the transmit power budget of iJmmaer as $P_1 = 10$ dBm. We investigate the case that iJammer moves along the x-axis from $x_j = 1$ m to $x_j = 100$ m, with $y_j = 0$. From Fig. 4, we can see that the our proposed information jamming approach with the optimal solution outperforms the Co-Alice scheme in terms of achievable secrecy rate. Specifically, the performance gap between them gradually enlarges as x_j increases. This is due to the fact that as x_j increases, the distance between iJammer and Bob and Eve is reduced, and thus iJammer can achieve better secrecy performance. Moreover, we observe that our proposed

information jamming approach always achieves higher secrecy rate than the cooperative jamming scheme as expected.

B. Performance Evaluation Under Imperfect CSI

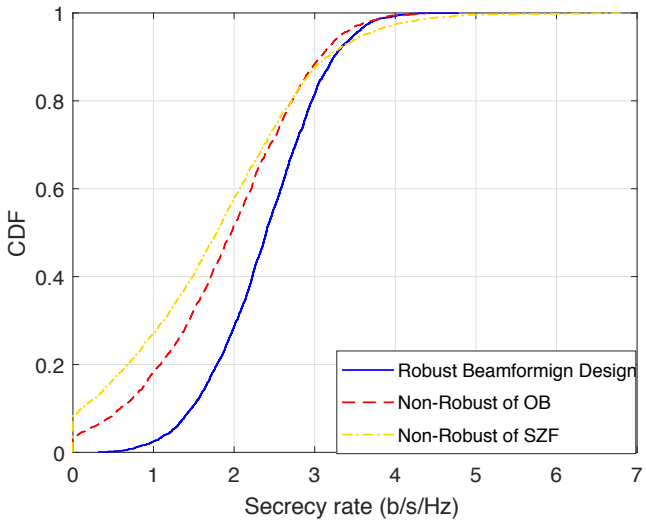

Fig. 5. The empirical CDF of the secrecy rate achieved by different schemes.

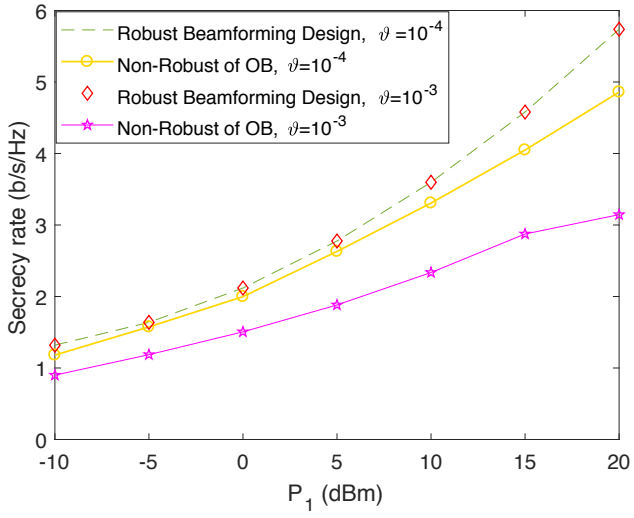

Fig. 6. Comparison of the secrecy rates of the robust optimal beamforming design and non-robust optimal beamforming design.

Next, we consider the imperfect CSI case. Fig. 5 shows the empirical cumulative distribution function (CDF) of the achieved secrecy rate for the proposed robust beamforming design in

Section IV and non-robust beamforming designs in Section II and Section III. The "non-robust" means that the beamforming vector is designed only according to the estimated CSI (neglecting the CSI errors). We label the non-robust optimal beamforming solution and non-robust SZF scheme as "Non-Robust of OB" and "Non-Robust of SZF", respectively. We set the channel error covariance matrix as $\mathbf{E}_i^h = \mathbf{E}_i^g = \vartheta \times \mathbf{I}, \forall i \in \mathcal{K}$. We set the target secrecy rate as $R = 1$ b/s/Hz, the outage probability as $\epsilon = 5\%$. We set $\vartheta = 5 \times 10^{-4}$. Fig. 5 demonstrates the robustness of our proposed robust beamforming design. Specifically, from Fig. 5, we can observe that the non-robust beamforming designs cannot satisfy the outage constraint, i.e., about 18% of the resulting secrecy rates of the "Non-Robust of OB" design fall below the target secrecy rate $R = 1$ b/s/Hz; whereas the achieved secrecy rates of the robust beamforming design can satisfy the outage constraint, thanks to taking the channel errors into account in the design.

Finally, we show in Fig. 6 the achievable secrecy rate achieved by the robust beamforming design and non-robust optimal beamforming design over P_1 with fixed $\vartheta = 10^{-4}$ and $\vartheta = 10^{-3}$. From Fig. 6, we can see that for both the cases of $\vartheta = 10^{-4}$ and $\vartheta = 10^{-3}$, the proposed robust beamforming solution achieves the higher secrecy rate for all values of P_1. Also, when ϑ increases from $\vartheta = 10^{-4}$ to $\vartheta = 10^{-3}$, the achievable secrecy rate of robust beamforming design nearly no change, while the achievable secrecy rate of non-robust optimal beamforming decreases significantly. This is because the non-robust beamforming design does not take the channel errors into its design, and hence it is sensitive to the CSI errors.

VII. Conclusion and Future Work

This paper proposed a new information jamming approach to go beyond the secrecy rate achieved by the existing cooperative jamming approach in a MISO wiretap channel. With the proposed approach, friendly multi-antenna iJammers send the source message rather than Gaussian noise to enhance the received signal strength at Bob and reduce that at Eve concurrently. Specifically, we formulated the joint beamforming design as an optimization problem to maximize the achievable secrecy rate. Despite the non-convexity of the formulated problem, we successfully obtained the optimal beamforming solution via using a SDR based optimization approach. In order to reduce the implementation complexity, we also provided a suboptimal distributed information beamforming scheme and obtained the optimal beamforming vector in closed-form. Considering the imperfect CSI case, we also studied the robust secure beamforming design to maximize the ϵ-outage secrecy rate. Numerically results showed that the proposed

information jamming approach could significantly go beyond the secrecy rate achieved by the traditional cooperative jamming approach.

There are some research directions worth pursuing in future work. First, it would be interesting to extend this work to MIMO wiretap channels with multi-antenna legitimate receiver and eavesdropper. Moreover, if there exists more than one legitimate receiver, how to characterize the achievable secrecy rate region via iJammers is an interesting problem.

REFERENCES

[1] H. Zhang and L. Duan, "Going beyond secrecy rate via information jamming,"in *Proc. IEEE Global Communications Conference (Globecom)*, Abu Dhabi, UAE, 2018.

[2] A. Mukherjee, S. 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, Aug. 2014.

[3] X. Chen, D. W. K. Ng, W. Gerstacker, and H-H. Chen, "A survey of multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 2, pp. 1027-1053, Jun. 2017.

[4] 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, June 2013.

[5] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journ.*, vol. 54, pp. 1355-1387, 1975.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451-456, Jul. 1978.

[7] 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.

[8] A. Wolf and E. A. Jorswieck, "On the zero forcing optimality for friendly jamming in MISO wiretap channels," in Proc. *IEEE 11th IEEE Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2010, pp. 1-5.

[9] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013-5022, Oct. 2011.

[10] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833-1847, May 2015.

[11] M. Nafea and A. Yener, "Secure degrees of freedom for the MIMO wiretap channel with a multi-antenna cooperative jammer," *IEEE Trans. Infor. Theory*, vol. 63, no. 11, pp. 7420-7441, Nov. 2017.

[12] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R.-F. Liao, "Cooperative jamming aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108-2117, March 2018.

[13] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2537-2551, Apr. 2016

[14] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 906-915, Mar. 2015

[15] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9385-9392, Oct. 2018

[16] S. Xu, S. Han, W. Meng, Y. Du, and L. He, "Multiple-jammer-aided secure transmission with receiver-side correlation," *IEEE Trans. Wireless Commu.*, vol. 18, no. 6, pp. 3093-3103, Jun. 2019.

[17] Y. Huo, X. Fan, L. Ma, X. Cheng, Z. Tian, and D. Chen, "Secure communications in tiered 5G wireless networks with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3265-3280, June 2019.

[18] M. Medard, "Capacity of correlated jamming channels," in *Proc. 35th Allerton Conf.*, 1997, pp. 1043-1052.

[19] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119-2123, Sep. 2004.

[20] S. Shafiee and S. Ulukus, "Mutual information games in multiuser channels with correlated jamming," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4598-4607, Oct. 2009.

[21] 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.

[22] 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.

[23] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct. 2016.

[24] D. Ng, E. 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.

[25] M. Zhang, R. Xue, H. Yu, H. Luo, and W. Chen, "Secrecy capacity optimization in coordinated multi-point processing," in *Proc. IEEE Int. Conf. Communications (ICC)*, June 2013.

[26] V. Satyanarayana, S. Chatzinotas, and B. Ottersten. "Secrecy analysis of random wireless networks with multiple eavesdroppers," in *Proc. IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct. 2017.

[27] J. Xu, L. Duan, and R. Zhang, "Transmit optimization for symbol-level spoofing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 41-55, Jan. 2018.

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

[29] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Res. Logist. Quarter.*, vol. 9, pp. 181-186, Dec. 1962.

[30] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[31] I. Pólik and T. Terlaky, "Interior point methods for nonlinear optimization," in *Nonlinear Optimization*. Springer, 2010, pp. 215-276.

[32] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," IEEE Trans. Signal Process., vol. 62, pp. 1850-1863, Apr. 2014.

[33] R. Zhang and Y.-C. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 88-102, Feb. 2008.

[34] S. Ma and D. Sun, "Chance constrained robust beamforming in cognitive radio networks," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 67-70, Jan. 2013.

[35] T. A. Le, Q.-T. Vien, H. X. Nguyen, D. W. K. Ng, and R. Schober, "Robust chance-constrained optimization for power-efficient and secure SWIPT systems," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 3, pp. 333-346, Sep. 2017.

[36] I. Bechar, "A Bernstein-type inequality for stochastic processes of quadratic forms of Gaussian variables." Avaliable: http://arxiv.org/abs/0909.3595.

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

[38] E. A. Jorswieck,"Secrecy capacity of single- and multi-antenna channels with simple helpers," in *Proc. 7th Int. ITG Conf. Source Channel Coding (SCC)*, Jan. 2010, pp. 1-6.