

RESEARCH

Open Access



Robust transmit design for secure AF relay networks with imperfect CSI

Lingxiang Li, Yu Xu, Zhi Chen* and Jun Fang

Abstract

This paper studies robust transmit design for secure AF relay networks with imperfect channel state information (CSI). Two CSI error models, deterministically bounded error model and stochastic error model, are considered. In order to use the power at relays more efficiently, a joint cooperative relaying and jamming scheme is considered, where relays cooperate to forward the source signal and simultaneously they cooperate to send jamming signals to confuse the eavesdroppers. In this joint cooperative relaying and jamming framework, we address the robust joint optimization of the relay weights and the input covariance matrix of jamming signals for secrecy rate maximization (SRM), under both total and individual relay power constraints. Specifically, for the case of deterministically bounded error model, where the CSI error can be specified by an uncertainty set, we maximize the worst-case secrecy rate. While for the case of stochastic error model, where the probability distribution of the CSI error is Gaussian, we maximize the outage constrained secrecy rate. The challenge of these considered SRM-based optimizations lies in their non-convexity. This paper shows that such SRM-based optimization can be solved in a convex fashion and via solving a sequence of semidefinite programs (SDPs). Numerical results are presented to show the efficacy of the proposed scheme.

Keywords: Physical-layer security, Amplify-and-forward relay, Cooperative communications, Imperfect channel state information

1 Introduction

In the classical three-node wiretap channel, secrecy capacity is typically zero when the source-destination link is weaker than the source-eavesdropper link [1, 2]. One way to achieve non-zero secrecy rate in this case is to introduce multi-antenna nodes [3–11], wherein multi-antenna techniques can enable directional transmission, thus allowing secret communication even when the eavesdropper's channel has a much better quality. However, due to the cost or size limitations, multi-antenna nodes may not be available in some practical applications. In this case, node cooperation is an alternative way to enable single-antenna nodes to enjoy the benefits brought by multi-antenna nodes [12–23].

Generally, there are two kinds of cooperation schemes. One is cooperative relaying [14–16], where relays cooperate to improve the source destination channel quality.

The other is cooperative jamming (CJ) [13–15], where relays cooperate to send jamming signals to confuse the eavesdroppers.

In [13–16], cooperative relaying and cooperative jamming were considered independently. In contrast, the works of [18–26] considered a joint cooperative relaying and jamming scheme, where some of the relays cooperate to forward the source signal and simultaneously the other relays cooperate to send jamming signals to confuse the eavesdroppers. Such joint scheme is especially useful when the number of relays is large. Later, in [27, 28], a more general joint cooperative relaying and jamming scheme was proposed, where each relay forwards the source signal and transmits jamming signals simultaneously. Due to noise amplification at relays, there exists a rate performance ceiling for the source-relay-destination (SRD) link, thus spending extra power in relaying will not help increase the secrecy rate after a certain point is reached. In contrast, distributing a portion of power to transmit jamming signals to confuse the eavesdropper may be more helpful.

*Correspondence: chenzhi@uestc.edu.cn
National Key Laboratory of Science and Technology on Communications,
University of Electronic Science and Technology of China, No.2006, Xiyuan
Ave., West Hi-Tech Zone, 611731 Chengdu, China

Most of the works mentioned above assume the availability of a perfect channel state information (CSI) at relays. In practice, the CSI available at relays is usually imperfect due to different factors such as estimation error, quantization, and feedback delay. In addition, the rate performance of the relay designs obtained under the assumption of perfect CSI degrades in the presence of CSI errors. Hence, it is important to develop relay designs that are robust to CSI errors. Works along these lines include [29–35] which consider the scenario with no relays and [24–27] which consider the scenario with relays. As compared with the transmission design in the former scenario, the robust secure relay design is more difficult due to noise amplification at relays. Moreover, to the best of the authors' knowledge, existing robust designs for secure AF relay networks are few. For example, the works [24, 25] considered the stochastic CSI error model which is applicable when the imperfect CSI is mainly due to errors in channel estimation and tried to minimize the outage probability of the secrecy rate. The works [26, 27] considered the deterministically bounded CSI error model which is applicable when the CSI error is dominated by quantization errors and tried to compute the maximal achievable worst-case secrecy rate.

In this paper, we aim to give a more general framework which applies to both the deterministically bounded CSI error model and the stochastic CSI error model. For the case of deterministically bounded error model, we maximize the worst-case secrecy rate. While for the case of stochastic error model, we maximize the outage constrained secrecy rate. As in our conference paper [27], we consider a more general joint cooperative relaying and jamming scheme, where each relay forwards the source signal and transmits jamming signals simultaneously. We should note that the works [24–26] considered a different joint cooperative relaying and jamming scheme, where some of the relays cooperate to forward the source signal while the other relays cooperate to send jamming signals to confuse the eavesdroppers.

Our main contributions are summarized below.

1. Robust joint optimization of the relay weights and the input covariance matrix of jamming signals for secrecy rate maximization (SRM) is addressed, under both total and individual relay power constraints. The challenge of these SRM-based optimizations lies in their non-convexity. In this paper, we provide a unified approach for solving these SRM-based optimizations. The key insight is to recast the SRM-based problem as a two-level optimization problem: an outer problem and an inner problem. We show that the outer problem can be dealt with a one-dimensional search, while the inner problem admits a tight convex relaxation and hence can be exactly solved in an efficient manner.
2. The crux of our approach is to construct a tight convex relaxation of the inner problem. To deal with this issue, we first introduce an alternative secrecy rate constrained (SRC) power minimization problem, i.e., minimizing the total relay power, under constraints on the achievable worst-case secrecy rate or the achievable outage constrained secrecy rate. We solve the SRC power minimization problem with semidefinite relaxation (SDR) techniques, and we prove that the relaxation here is tight. We then prove that the optimal relay weights and input covariance matrix of jamming signals in the SRC power minimization problem also constitute an optimal solution to our inner problem. In this way, we provide a tight convex relaxation of our inner problem.

We should note that in the practical implementation of any coherent wireless communication systems, the issue of synchronization needs to be addressed. In this paper, the relay transmissions are assumed to be synchronized, by resorting to global positioning system (GPS) satellite signals [36] or the master-slave scheme [37]. Imperfect synchronization can also be overcome by employing carrier frequency offset (CFO) compensation [38]. Since our goal is to give the fundamental limit of the secrecy transmission rate from a theoretic perspective, and also due to the lack of space, in this paper, we do not go into the detailed analysis of the impact of imperfect synchronization.

This paper is organized as follows. In Section 2, we describe the system model. In Section 3, we consider the deterministically bounded CSI error model and compute the maximal achievable worst-case secrecy rate. In Section 4, we consider the stochastic CSI error model and compute the maximal achievable outage constrained secrecy rate. Numerical results are provided in Section 5, and conclusions are drawn in Section 6.

Notation. \mathbf{A}^H , $\text{tr}\{\mathbf{A}\}$, and $\text{rank}\{\mathbf{A}\}$ represent the hermitian transpose, trace, and rank of a matrix \mathbf{A} , respectively; $\text{diag}\{\mathbf{A}\}$ denotes a diagonal matrix with the same main diagonal elements as the matrix \mathbf{A} ; $[\mathbf{A}]_{k,k}$ denotes the k th diagonal element of the matrix \mathbf{A} ; $\text{diag}\{\mathbf{a}\}$ represents a diagonal matrix with \mathbf{a} on the main diagonal. \mathbf{I} is an identity matrix with appropriate size; $\mathbf{A} \succeq \mathbf{0}$ means \mathbf{A} is a hermitian positive semidefinite matrix; $\mathbf{A} \in \mathbb{H}^n$ means \mathbf{A} is a $n \times n$ complex hermitian matrix. $x \sim \mathcal{CN}(0, \Sigma)$ means x is a random variable following a complex circular Gaussian distribution with mean zero and covariance Σ ; $E\{\cdot\}$ is the expectation operator. $\mathbb{C}^{N \times M}$ represents a $N \times M$ complex matrix set.

2 System model

As depicted in Fig. 1, a source node aims to send confidential messages to the destination in the presence of M eavesdroppers, with the help of N relays. Each node is equipped with one antenna. Two phases including the *broadcasting phase* and the *relaying phase* are required. In the broadcasting phase, the source broadcasts its message and the received signal at relays is given by

$$\mathbf{y}_R = \mathbf{h}_{SR}s + \mathbf{n}_R, \quad (1)$$

where s , $E\{|s|^2\} = P_s$, is the data to be transmitted. $\mathbf{h}_{SR} \in \mathbb{C}^{N \times 1}$ represents the channel vector from the source to the relay. \mathbf{n}_R is the noise vector at relays, with i.i.d. entries distributed as $\mathcal{CN}(0, \sigma_R^2)$. In the relaying phase, the relay forwards a weighted version of the received signal. Simultaneously, the relay transmits jamming signals, \mathbf{n}_J , to confuse the eavesdropper. The signal transmitted by relays can thus be expressed as

$$\mathbf{x} = \text{diag}\{\mathbf{v}\}(\mathbf{h}_{SR}s + \mathbf{n}_R) + \mathbf{n}_J, \quad (2)$$

where \mathbf{v} is the relaying weight vector.

Denote $\mathbf{h}_{RD}^H \in \mathbb{C}^{1 \times N}$ and $\mathbf{g}_{RE,m}^H \in \mathbb{C}^{1 \times N}$ as the channel vector from the relays to the destination and the m th eavesdropper, respectively. The signals received at the des-

tinuation and the m th eavesdropper can be respectively expressed as

$$y_D = \mathbf{h}_{RD}^H \text{diag}\{\mathbf{v}\}(\mathbf{h}_{SR}s + \mathbf{n}_R) + \mathbf{h}_{RD}^H \mathbf{n}_J + n_D, \quad (3)$$

$$y_{E,m} = \mathbf{g}_{RE,m}^H \text{diag}\{\mathbf{v}\}(\mathbf{h}_{SR}s + \mathbf{n}_R) + \mathbf{g}_{RE,m}^H \mathbf{n}_J + n_{E,m}, \quad (4)$$

where $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ and $n_{E,m} \sim \mathcal{CN}(0, \sigma_E^2)$ are the AWGN at each receiver.

Denote $\mathbf{h} = \text{diag}\{\mathbf{h}_{SR}\}\mathbf{h}_{RD}$ and $\mathbf{g}_m = \text{diag}\{\mathbf{h}_{SR}\}\mathbf{g}_{RE,m}$ the channel from the source to the destination and the m th eavesdropper, respectively. For a given relaying weight vector \mathbf{v} and input covariance matrix of jamming signals \mathbf{Q}_J , the received signal-to-noise (SNR) at the destination and the m th eavesdropper are, respectively,

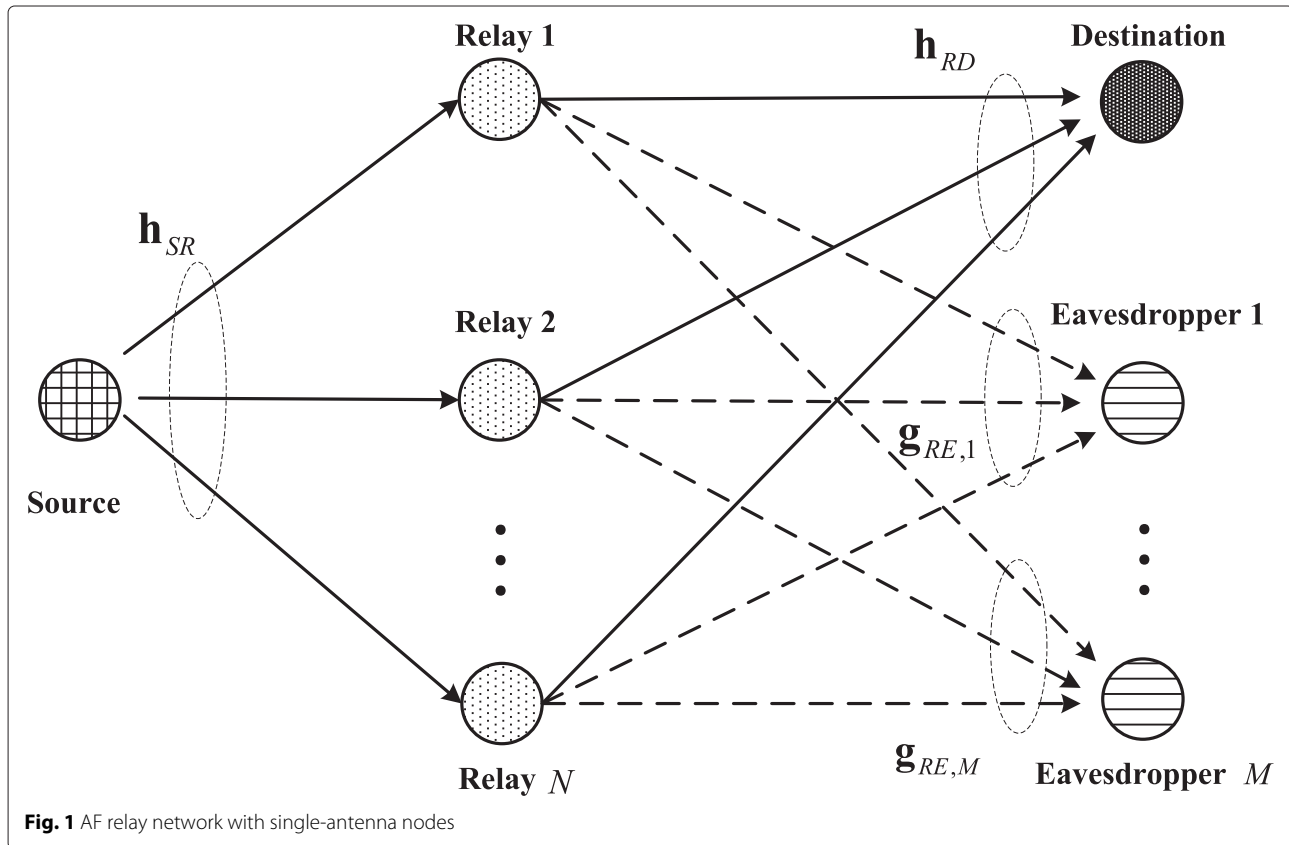
$$\gamma_D = \frac{P_s \mathbf{h}^H \mathbf{Q}_v \mathbf{h}}{\sigma_D^2 + \mathbf{h}_{RD}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_J) \mathbf{h}_{RD}}, \quad (5)$$

$$\gamma_{E,m} = \frac{P_s \mathbf{g}_m^H \mathbf{Q}_v \mathbf{g}_m}{\sigma_E^2 + \mathbf{g}_{RE,m}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_J) \mathbf{g}_{RE,m}}, \quad (6)$$

where $\mathbf{Q}_v = \mathbf{v}\mathbf{v}^H$. The transmitted power of the k th relay, $k = 1, \dots, N$, is $t_k(\mathbf{Q}_v, \mathbf{Q}_J) = \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J)$, where

$$\zeta_k(\mathbf{A}, \mathbf{B}) \triangleq [P_s \text{diag}\{\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}\mathbf{A} + \sigma_R^2 \mathbf{A} + \mathbf{B}]_{k,k}.$$

In this paper, we aim to address the robust joint optimization of the relay weights and the input covariance



matrix of jamming signals for SRM, under both total and individual relay power constraints. Two CSI error models, the deterministically bounded error model and the stochastic error model, are considered. For the case of deterministically bounded error model, we aim to maximize the worst-case secrecy rate. While for the case of stochastic error model, we aim to maximize the outage constrained secrecy rate. The challenge of these SRM-based optimizations lies in their non-convexity. In the following sections, we provide a unified approach for solving these SRM-based optimizations.

3 Robust joint relaying and jamming design with norm-bounded CSI error

In this section, we study the case where the CSI of the eavesdropping channel is partially known. The deterministically bounded error model is considered, and we aim to maximize the worst-case secrecy rate. To this end, we first solve the SRC power minimization problem. We then study the relationship between the solutions of the SRC power minimization problem and the worst-case SRM problem. By exploiting this relationship, we provide an approach for solving the worst-case SRM in a convex fashion.

3.1 Channel uncertainty

The channel vector from the relays to the eavesdroppers are modeled as [30]

$$\mathbf{g}_{\text{RE},m} = \hat{\mathbf{g}}_{\text{RE},m} + \Delta \mathbf{g}_{\text{RE},m}, m = 1, \dots, M, \quad (7)$$

where $\hat{\mathbf{g}}_{\text{RE},m}$ is the channel information known at the source node. We should note that the estimation of the eavesdropper's channel is possible in situations in which the eavesdropper is an active member of the network, and thus, its whereabouts and behavior can be monitored. $\Delta \mathbf{g}_{\text{RE},m}$ denotes the channel uncertainties. The deterministically bounded error model is considered in this section.

Thus, the actual channel coefficients $\mathbf{g}_{\text{RE},m}$ is contained in a certain sphere, i.e.,

$$\Omega_m = \{\mathbf{g}_{\text{RE},m} \mid \|\mathbf{g}_{\text{RE},m} - \hat{\mathbf{g}}_{\text{RE},m}\|_F \leq \beta_m\}, \quad (8)$$

where β_m is a known constant.

3.2 Worst-case secrecy rate constrained power minimization

In this subsection, we consider the SRC power minimization problem, i.e., minimizing the total relay power,

under the constraint on the achievable worst-case secrecy rate.

$$\begin{aligned} \min_{\{\mathbf{v}, \mathbf{Q}_J\}} \quad & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \\ \text{s.t.} \quad & \gamma_D \geq \delta_1, \\ & \gamma_{E,m} \leq \delta_2, \forall \mathbf{g}_{\text{RE},m} \in \Omega_m, m = 1, \dots, M, \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, k = 1, \dots, N, \\ & \mathbf{Q}_v = \mathbf{v}\mathbf{v}^H, \mathbf{Q}_J \succeq \mathbf{0}. \end{aligned} \quad (9)$$

where δ_1 and δ_2 denote the SNR constraints on the legitimate receiver and the eavesdropper, respectively.

By dropping the rank 1 constraint on \mathbf{Q}_v , we reformulate (9) as

$$\begin{aligned} \min_{\{\mathbf{Q}_v, \mathbf{Q}_J\}} \quad & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \\ \text{s.t.} \quad & \frac{P_s \mathbf{h}^H \mathbf{Q}_v \mathbf{h}}{\sigma_D^2 + \mathbf{h}_{\text{RD}}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_J) \mathbf{h}_{\text{RD}}} \geq \delta_1 \\ & \frac{P_s \mathbf{g}_{\text{RE},m}^H \mathbf{Q}_v \mathbf{g}_{\text{RE},m}}{\sigma_E^2 + \mathbf{g}_{\text{RE},m}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_J) \mathbf{g}_{\text{RE},m}} \leq \delta_2 \\ & \forall \mathbf{g}_{\text{RE},m} \in \Omega_m, m = 1, \dots, M \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, k = 1, \dots, N \\ & \mathbf{Q}_v \succeq \mathbf{0}, \mathbf{Q}_J \succeq \mathbf{0}. \end{aligned} \quad (10)$$

Proposition 1. The optimization (10) can be reformulated into a SDP and solved by CVX.

Proof. To handle the imperfect-CSI induced constraints in (10), we need the following lemma (please see [39] for more details). \square

Lemma 1. Let $\varphi_k(\mathbf{x}) = \mathbf{x}^H \mathbf{A}_k \mathbf{x} + 2\Re\{\mathbf{b}_k^H \mathbf{x}\} + c_k$, where $\mathbf{A}_k \in \mathbb{H}^n$, $\mathbf{b}_k \in \mathbb{C}^{n \times 1}$, $c_k \in \mathbb{R}$. Assume that there exists a point $\hat{\mathbf{x}}$ such that $\varphi_1(\hat{\mathbf{x}}) < 0$. Then, the implication $\varphi_1(\mathbf{x}) \leq 0 \Rightarrow \varphi_2(\mathbf{x}) \leq 0$ holds if and only if there exists a $\varrho \geq 0$ such that

$$\varrho \begin{bmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{bmatrix} - \begin{bmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{bmatrix} \succeq \mathbf{0},$$

For ease of exposition, we first rewrite the second constraint in (10) as

$$\mathbf{g}_{\text{RE},m}^H \Theta \mathbf{g}_{\text{RE},m} - \delta_2 \sigma_E^2 \leq 0 \quad (11)$$

where $\Theta = P_s \text{diag}\{\mathbf{h}_{\text{SR}}\}^H \mathbf{Q}_v \text{diag}\{\mathbf{h}_{\text{SR}}\} - \sigma_R^2 \delta_2 \text{diag}\{\mathbf{Q}_v\} - \delta_2 \mathbf{Q}_J$. Substituting (7) into (11) yields

$$\begin{aligned} \Delta \mathbf{g}_{\text{RE},m}^H \Theta \Delta \mathbf{g}_{\text{RE},m} + 2\Re\{\hat{\mathbf{g}}_{\text{RE},m}^H \Theta \Delta \mathbf{g}_{\text{RE},m}\} \\ + \hat{\mathbf{g}}_{\text{RE},m}^H \Theta \hat{\mathbf{g}}_{\text{RE},m} - \delta_2 \sigma_E^2 \leq 0. \end{aligned} \quad (12)$$

According to Lemma 1, $\|\Delta \mathbf{g}_{\text{RE},m}\|_F^2 \leq \beta_m^2 \Rightarrow (12)$ if and only if for some $\mu_m \geq 0$,

$$\begin{bmatrix} \mu_m \mathbf{I} - \Theta & -\Theta^H \hat{\mathbf{g}}_{\text{RE},m} \\ -\hat{\mathbf{g}}_{\text{RE},m}^H \Theta & -\beta_m^2 \mu_m - \hat{\mathbf{g}}_{\text{RE},m}^H \Theta \hat{\mathbf{g}}_{\text{RE},m} + \delta_2 \sigma_E^2 \end{bmatrix} \succeq \mathbf{0}.$$

Therefore, the optimization (10) can be re-expressed as

$$\begin{aligned} & \min_{\{\mathbf{Q}_v, \mathbf{Q}_f, \mu_1, \dots, \mu_M\}} \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \\ & \text{s.t. } P_s \text{tr}\{\mathbf{h}\mathbf{h}^H \mathbf{Q}_v\} \geq \delta_1 \sigma_D^2 + \delta_1 \bar{\xi}(\mathbf{Q}_v, \mathbf{Q}_f) \\ & \begin{bmatrix} \mu_m \mathbf{I} - \Theta & -\Theta^H \hat{\mathbf{g}}_{\text{RE},m} \\ -\hat{\mathbf{g}}_{\text{RE},m}^H \Theta & -\beta_m^2 \mu_m - \hat{\mathbf{g}}_{\text{RE},m}^H \Theta \hat{\mathbf{g}}_{\text{RE},m} + \delta_2 \sigma_E^2 \end{bmatrix} \succeq \mathbf{0} \\ & \quad m = 1, \dots, M \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \leq P_k, k = 1, \dots, N \\ & \mu_m \geq 0, \mathbf{Q}_v \succeq \mathbf{0}, \mathbf{Q}_f \succeq \mathbf{0}, \end{aligned} \quad (13)$$

where we define $\bar{\xi}(\mathbf{Q}_v, \mathbf{Q}_f) = \text{tr}\{\sigma_R^2 \text{diag}\{\mathbf{h}_{\text{RD}} \mathbf{h}_{\text{RD}}^H\} \mathbf{Q}_v + \mathbf{h}_{\text{RD}} \mathbf{h}_{\text{RD}}^H \mathbf{Q}_f\}$.

According to [39], the optimization (13) is a SDP and can be solved by CVX. This completes the proof.

Proposition 2. Denote the optimal solution to (10) as $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f\}$. Then, $\hat{\mathbf{Q}}_v$ is rank 1, provided that a positive secrecy rate is achieved.

Proof. See Appendix A. \square

By applying the matrix decomposition, we get $\hat{\mathbf{Q}}_v = \hat{\mathbf{v}} \hat{\mathbf{v}}^H$. From Proposition 2, the rank 1 constraint relaxation in (10) is tight. Therefore, $\{\hat{\mathbf{v}}, \hat{\mathbf{Q}}_f\}$ is the optimal solution to (9).

3.3 Worst-case secrecy rate maximization

In this subsection, we aim to maximize the worst-case achievable secrecy rate subject to both total and individual relay power constraints, i.e.,

$$\begin{aligned} & \max_{\{\mathbf{v}, \mathbf{Q}_f\}} \min_{\substack{m \in \{1, \dots, M\} \\ \mathbf{g}_{\text{RE},m} \in \Omega_m}} \frac{1}{2} \log(1 + \gamma_D) - \frac{1}{2} \log(1 + \gamma_{E,m}) \\ & \text{s.t. } \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \leq P_r \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \leq P_k, k = 1, \dots, N \\ & \mathbf{Q}_v = \mathbf{v} \mathbf{v}^H, \mathbf{Q}_f \succeq \mathbf{0}. \end{aligned} \quad (14)$$

In general, the optimization problem in (14) is non-convex and challenging to solve directly. To deal with this issue, the two-layer idea in [13] is adopted. The key insight is to recast the original optimization problem in (14) as a two-level optimization problem. The inner-level part is dealt with the SDR technique, and the outer-level part

is handled by a one-dimensional search. Specifically, the outer-level part is

$$\max_{\tau \in [\tau_{lb}, \tau_{ub}]} \frac{1 + \bar{f}(\tau)}{1 + \tau}, \quad (15)$$

where $\bar{f}(\tau)$ is obtained through solving the following inner-level part optimization problem for a given τ

$$\begin{aligned} \bar{f}(\tau) &= \max_{\{\mathbf{v}, \mathbf{Q}_f\}} \frac{P_s \mathbf{h}^H \mathbf{Q}_v \mathbf{h}}{\sigma_D^2 + \mathbf{h}_{\text{RD}}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_f) \mathbf{h}_{\text{RD}}} \\ & \text{s.t. } \frac{P_s \mathbf{g}_m^H \mathbf{Q}_v \mathbf{g}_m}{\sigma_E^2 + \mathbf{g}_{\text{RE},m}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_f) \mathbf{g}_{\text{RE},m}} \leq \tau \\ & \quad \forall \mathbf{g}_{\text{RE},m} \in \Omega_m, \quad m = 1, \dots, M \\ & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \leq P_r \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \leq P_k, k = 1, \dots, N \\ & \mathbf{Q}_v = \mathbf{v} \mathbf{v}^H, \mathbf{Q}_f \succeq \mathbf{0}. \end{aligned} \quad (16)$$

By dropping the rank 1 constraint on \mathbf{Q}_v , we reformulate the optimization (16) as

$$\begin{aligned} \bar{g}(\tau) &= \max_{\{\mathbf{Q}_v, \mathbf{Q}_f\}} \frac{P_s \mathbf{h}^H \mathbf{Q}_v \mathbf{h}}{\sigma_D^2 + \mathbf{h}_{\text{RD}}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_f) \mathbf{h}_{\text{RD}}} \\ & \text{s.t. } \frac{P_s \mathbf{g}_m^H \mathbf{Q}_v \mathbf{g}_m}{\sigma_E^2 + \mathbf{g}_{\text{RE},m}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_f) \mathbf{g}_{\text{RE},m}} \leq \tau \\ & \quad \forall \mathbf{g}_{\text{RE},m} \in \Omega_m, \quad m = 1, \dots, M \\ & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \leq P_r \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_f) \leq P_k, k = 1, \dots, N \\ & \mathbf{Q}_v \succeq \mathbf{0}, \mathbf{Q}_f \succeq \mathbf{0}. \end{aligned} \quad (17)$$

Proposition 3. The optimization (17) can be reformulated into a SDP and solved by CVX.

Proof. By letting $\eta = \frac{1}{\sigma_D^2 + \mathbf{h}_{\text{RD}}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_f) \mathbf{h}_{\text{RD}}}$, $\tilde{\mathbf{Q}}_v = \eta \mathbf{Q}_v$, $\tilde{\mathbf{Q}}_f = \eta \mathbf{Q}_f$, and using the Charnes-Cooper transformation, we recast the optimization (17) as

$$\begin{aligned} \bar{g}(\tau) &= \max_{\{\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f, \eta\}} P_s \text{tr}\{\mathbf{h} \mathbf{h}^H \tilde{\mathbf{Q}}_v\} \\ & \text{s.t. } \sigma_D^2 \eta + \text{tr}\{\sigma_R^2 \text{diag}\{\mathbf{h}_{\text{RD}} \mathbf{h}_{\text{RD}}^H\} \tilde{\mathbf{Q}}_v + \mathbf{h}_{\text{RD}} \mathbf{h}_{\text{RD}}^H \tilde{\mathbf{Q}}_f\} = 1 \\ & \quad \frac{P_s \mathbf{g}_m^H \tilde{\mathbf{Q}}_v \mathbf{g}_m}{\sigma_E^2 \eta + \mathbf{g}_{\text{RE},m}^H (\sigma_R^2 \text{diag}\{\tilde{\mathbf{Q}}_v\} + \tilde{\mathbf{Q}}_f) \mathbf{g}_{\text{RE},m}} \leq \tau \\ & \quad \forall \mathbf{g}_{\text{RE},m} \in \Omega_m, \quad m = 1, \dots, M \\ & \sum_{k=1}^N \zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f) \leq \eta P_r \\ & \zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f) \leq \eta P_k, k = 1, \dots, N \\ & \tilde{\mathbf{Q}}_v \succeq \mathbf{0}, \tilde{\mathbf{Q}}_f \succeq \mathbf{0}, \eta > 0. \end{aligned} \quad (18)$$

Applying the same derivation from (11) to (12) and applying Lemma 1, we re-express the optimization (18) as

$$\begin{aligned} \bar{g}(\tau) &= \max_{\{\mathbf{Q}_v, \mathbf{Q}_f, \eta, \mu_1, \dots, \mu_M\}} P_s \text{tr}\{\mathbf{h}\mathbf{h}^H \tilde{\mathbf{Q}}_v\} \\ \text{s.t. } &\sigma_D^2 \eta + \text{tr}\{\sigma_R^2 \text{diag}\{\mathbf{h}_{RD} \mathbf{h}_{RD}^H\} \tilde{\mathbf{Q}}_v + \mathbf{h}_{RD} \mathbf{h}_{RD}^H \tilde{\mathbf{Q}}_f\} = 1 \\ &\begin{bmatrix} \mu_m \mathbf{I} - \Phi & -\Phi^H \hat{\mathbf{g}}_{RE,m} \\ -\hat{\mathbf{g}}_{RE,m}^H \Phi & -\beta_m^2 \mu_m - \hat{\mathbf{g}}_{RE,m}^H \Phi \hat{\mathbf{g}}_{RE,m} + \tau \eta \sigma_E^2 \end{bmatrix} \succeq \mathbf{0} \\ &m = 1, \dots, M \\ &\sum_{k=1}^N \zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f) \leq \eta P_r \\ &\zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f) \leq \eta P_k, k = 1, \dots, N \\ &\tilde{\mathbf{Q}}_v \succeq \mathbf{0}, \tilde{\mathbf{Q}}_f \succeq \mathbf{0}, \eta > 0, \mu_m \geq 0, \end{aligned} \quad (19)$$

where $\Phi = P_s \text{diag}\{\mathbf{h}_{SR}\}^H \tilde{\mathbf{Q}}_v \text{diag}\{\mathbf{h}_{SR}\} - \sigma_R^2 \tau \text{diag}\{\tilde{\mathbf{Q}}_v\} - \tau \tilde{\mathbf{Q}}_f$.

According to [39], the optimization (19) is a SDP and can be efficiently solved by CVX. This completes the proof. \square

Proposition 4. Go back to the optimization problem (10), and let $\delta_1 = \bar{g}(\tau)$, $\delta_2 = \tau$. Then, the optimal solution to (10), $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f\}$, constitutes an optimal solution to (17).

Proof. Denote by $\{\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f\}$ the optimal solution to (17). Because $\{\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f\}$ is feasible to the optimization (17), it is also feasible to (10). In addition, $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f\}$ is the optimal solution to (10), thus

$$\sum_{k=1}^N \zeta(\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f) \leq \sum_{k=1}^N \zeta(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_f) \leq P_r,$$

which indicates the point $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f\}$ is feasible to the optimization (17).

For notional simplicity, let

$$\Psi(\mathbf{Q}_v, \mathbf{Q}_f) = \frac{P_s \mathbf{h}^H \mathbf{Q}_v \mathbf{h}}{\sigma_D^2 + \mathbf{h}_{RD}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_f) \mathbf{h}_{RD}}.$$

From the definition of $\bar{g}(\tau)$, $\Psi(\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f) \leq \bar{g}(\tau)$. Moreover, from (10), $\Psi(\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f) \geq \bar{g}(\tau)$. Thus, we have

$$\Psi(\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f) = \bar{g}(\tau),$$

which implies that the point $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f\}$ achieves the maximal value of the optimization (17). This completes the proof. \square

Remark. According to Proposition 4, $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f\}$ constitutes an optimal solution to (17). In addition, according to Proposition 2, $\text{rank}\{\hat{\mathbf{Q}}_v\} = 1$, thus, the optimization (17) is indeed a tight approximation of (16). Besides, $\{\hat{\mathbf{v}}, \hat{\mathbf{Q}}_f\}$ is the optimal solution to (16) and $\bar{f}(\tau) = \bar{g}(\tau)$.

So far, the inner-level part is solved and $\bar{f}(\tau)$ is determined for any given τ . The remaining issue now is to resolve the optimal τ^* maximizing the objective function in (15). In (15), τ_{lb} and τ_{ub} denote the lower and upper bound of $\gamma_{E,m}$, respectively. Firstly, $\gamma_{E,m}$ is no less than 0, thus, we set $\tau_{lb} = 0$. Secondly, according to the security requirement, $\gamma_{E,m}$ should be no more than γ_D . Thus, we set $\tau_{ub} = P_s P_r |\mathbf{h}|^2 / \sigma_D^2$. By performing one-dimensional search over $[\tau_{lb}, \tau_{ub}]$, the optimal τ^* which maximizes the objective function in (15) could be found. Correspondingly, the optimal solution $\{\mathbf{v}^*, \mathbf{Q}_f^*\}$ to the original optimization (14) can be obtained. In Table 1, we summarize our proposed algorithm for maximizing the worst-case secrecy rate.

4 Robust joint relaying and jamming design with stochastic CSI error

In this section, we extend our joint cooperative relaying and jamming scheme in Section 3 to the stochastic CSI error model case, and we maximize the outage constrained secrecy rate. In particular, we first solve the SRC power minimization problem. We then study the relationship between the solutions of the SRC power minimization problem and the outage constrained secrecy rate maximization problem. By exploiting this relationship, we provide an approach for solving the outage constrained secrecy rate maximization problem in a convex fashion.

4.1 Channel uncertainty

The channel vector from the relays to the eavesdroppers are modeled as [35]

$$\mathbf{g}_{RE,m} = \hat{\mathbf{g}}_{RE,m} + \Delta \mathbf{g}_{RE,m}, m = 1, \dots, M, \quad (20)$$

where $\hat{\mathbf{g}}_{RE,m}$ denotes the presume part at source node and $\Delta \mathbf{g}_{RE,m}$ is the error channel vectors. We assume that each

Table 1 An algorithm for determining the optimal solution $\{\mathbf{v}^*, \mathbf{Q}_f^*\}$ which maximizes the worst-case secrecy rate

1. Initialize $\tau_{lb} = 0$, $\tau_{ub} = P_s P_r |\mathbf{h}|^2 / \sigma_D^2$, $P_s > 0$, $P_r > 0$, $P_k \geq 0$, $\tau = 0$, $\tau_{sz} > 0$ where the step size τ_{sz} is an arbitrarily small positive quantity;
2. **while** $\tau \in [\tau_{lb}, \tau_{ub}]$ **do**
3. Calculate $\bar{g}(\tau)$ by solving (17) and let $\bar{f}(\tau) = \bar{g}(\tau)$;
4. Let $\tau = \tau + \tau_{sz}$;
5. **end while**
6. Determine τ^* which maximizes the objective function of (15);
7. Let $\tau = \tau^*$ and calculate $\bar{g}(\tau)$ by solving (17);
8. Calculate $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_f\}$ by solving (10);
8. Do the matrix decomposition $\hat{\mathbf{Q}}_v = \hat{\mathbf{v}} \hat{\mathbf{v}}^H$;
9. The optimal solution $\mathbf{v}^* = \hat{\mathbf{v}}$, $\mathbf{Q}_f^* = \hat{\mathbf{Q}}_f$.

channel error vector has a circularly symmetric complex Gaussian distribution

$$\mathbf{g}_{RE,m} \sim \mathcal{CN}(\hat{\mathbf{g}}_{RE,m}, \mathbf{C}_m) \quad m = 1, \dots, M. \quad (21)$$

4.2 Secrecy outage constrained power minimization

In this subsection, we consider the secrecy outage constrained power minimization problem, i.e., minimizing the total relay power, under the constraint on the achievable secrecy outage rate.

$$\begin{aligned} \min_{\{\mathbf{v}, \mathbf{Q}_J\}} & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \\ \text{s.t.} & \quad \gamma_D \geq \delta_1 \\ & \quad \text{Prob}\{\gamma_{E,m} \leq \delta_2\} \geq 1 - \rho, \forall m \\ & \quad \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, \forall k \\ & \quad \mathbf{Q}_v = \mathbf{v}\mathbf{v}^H, \mathbf{Q}_J \geq \mathbf{0}. \end{aligned} \quad (22)$$

By letting $\bar{\xi}(\mathbf{Q}_v, \mathbf{Q}_J) = \text{tr}\{\sigma_R^2 \text{diag}\{\mathbf{h}_{RD} \mathbf{h}_{RD}^H\} \mathbf{Q}_v + \mathbf{h}_{RD} \mathbf{h}_{RD}^H \mathbf{Q}_J\}$, and dropping the rank 1 constraint on \mathbf{Q}_v , we rewrite (22) as

$$\begin{aligned} \min_{\{\mathbf{Q}_v, \mathbf{Q}_J\}} & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \\ \text{s.t.} & \quad P_s \text{tr}\{\mathbf{h}\mathbf{h}^H \mathbf{Q}_v\} \geq \delta_1 \sigma_D^2 + \delta_1 \bar{\xi}(\mathbf{Q}_v, \mathbf{Q}_J) \\ & \quad \text{Prob}\{\gamma_{E,m} \leq \delta_2\} \geq 1 - \rho, \forall m \\ & \quad \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, \forall k \\ & \quad \mathbf{Q}_v \geq \mathbf{0}, \mathbf{Q}_J \geq \mathbf{0}, \end{aligned} \quad (23)$$

which is not known to be computationally tractable due to its rate outage probability constraints.

Proposition 5. *The optimization (23) can be safely approximated with a SDP.*

Proof. Our strategy for tackling the rate outage constraints is to find a convex set to approximate them. To this end, we first rewrite the rate outage probability constraints as

$$\text{Prob}\{-\mathbf{g}_{RE,m}^H \mathbf{\Theta} \mathbf{g}_{RE,m} + \delta_2 \sigma_E^2 \geq 0\} \geq 1 - \rho, \quad (24)$$

with $\mathbf{\Theta} = P_s \text{diag}\{\mathbf{h}_{SR}\}^H \mathbf{Q}_v \text{diag}\{\mathbf{h}_{SR}\} - \sigma_E^2 \delta_2 \text{diag}\{\mathbf{Q}_v\} - \delta_2 \mathbf{Q}_J$. Combining (20) with (21), we arrive at

$$\mathbf{g}_{RE,m} = \hat{\mathbf{g}}_{RE,m} + \mathbf{C}_m^{1/2} \mathbf{e}_m, \quad (25)$$

where $\mathbf{e}_m \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$.

Substituting (25) into (24), we then arrive at

$$\text{Prob}\{\mathbf{e}_m^H \mathbf{Q}_m \mathbf{e}_m + 2\Re\{\mathbf{e}_m^H \mathbf{r}_m\} + c_m \geq 0\} \geq 1 - \rho, \quad (26)$$

in which $\mathbf{Q}_m = -\mathbf{C}_m^{1/2} \mathbf{\Theta} \mathbf{C}_m^{1/2}$, $\mathbf{r}_m = -\mathbf{C}_m^{1/2} \mathbf{\Theta} \hat{\mathbf{g}}_{RE,m}$, and $c_m = \delta_2 \sigma_E^2 - \hat{\mathbf{g}}_{RE,m}^H \mathbf{\Theta} \hat{\mathbf{g}}_{RE,m}$.

Applying the *Sphere Bounding* method in [40], we obtain a convex restriction of (26) as follows:

$$\begin{bmatrix} \mu_m \mathbf{I} + \mathbf{Q}_m & \mathbf{r}_m \\ \mathbf{r}_m^H & c_m - \mu_m d^2 \end{bmatrix} \succeq \mathbf{0}, \forall m, \quad (27)$$

where $\mu_m \geq 0$, $d = \sqrt{\Xi_{\chi_{2N}^2}^{-1}(1 - \rho)/2}$ is the ball radius and $\Xi_{\chi_m^2}^{-1}(\cdot)$ is the inverse cumulative distribution function of the (central) chi-square random variable with m degrees of freedom.

By replacing the rate outage probability constraints in (23) with (27), we obtain

$$\begin{aligned} \min_{\{\mathbf{Q}_v, \mathbf{Q}_J, \mu_1, \dots, \mu_M\}} & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \\ \text{s.t.} & \quad P_s \text{tr}\{\mathbf{h}\mathbf{h}^H \mathbf{Q}_v\} \geq \delta_1 \sigma_D^2 + \delta_1 \bar{\xi}(\mathbf{Q}_v, \mathbf{Q}_J) \\ & \quad \begin{bmatrix} \mu_m \mathbf{I} + \mathbf{Q}_m & \mathbf{r}_m \\ \mathbf{r}_m^H & c_m - \mu_m d^2 \end{bmatrix} \succeq \mathbf{0}, \forall m \\ & \quad \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, \forall k \\ & \quad \mu_m \geq 0, \mathbf{Q}_v \geq \mathbf{0}, \mathbf{Q}_J \geq \mathbf{0}. \end{aligned} \quad (28)$$

According to [39], the optimization (28) is a SDP and can be solved by CVX. This completes the proof. \square

Proposition 6. *Denote the optimal solution to (23) as $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_J\}$. Then $\hat{\mathbf{Q}}_v$ is rank 1, provided that a positive secrecy rate is achieved.*

Proof. The KKT conditions of (28) are the same as that of (13), with the exception of $\mathbf{G}_m = [\mathbf{C}_m^{1/2}, \hat{\mathbf{g}}_{RE,m}]$. Following the proof in Appendix A, it is easy to verify $\text{rank}(\hat{\mathbf{Q}}_v) = 1$. This completes the proof. \square

By applying the matrix decomposition, we get $\hat{\mathbf{Q}}_v = \hat{\mathbf{v}}\hat{\mathbf{v}}^H$. From Proposition 5, the rank 1 constraint relaxation in (23) is tight. Therefore, $\{\hat{\mathbf{v}}, \hat{\mathbf{Q}}_J\}$ is the optimal solution to (22).

4.3 Outage constrained secrecy rate maximization

In this subsection, we aim to maximize the achievable outage constrained secrecy rate, subject to both total and individual relay power constraints, i.e.,

$$\begin{aligned} \max_{\{r, \mathbf{v}, \mathbf{Q}_J\}} & \quad r \\ \text{s.t.} & \quad \text{Prob}\{R_d - R_{e,m} \geq r\} \geq 1 - \rho, \forall m \\ & \quad \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_r \\ & \quad \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, \forall k \\ & \quad \mathbf{Q}_v = \mathbf{v}\mathbf{v}^H, \mathbf{Q}_J \geq \mathbf{0}, \end{aligned} \quad (29)$$

where $R_d = \frac{1}{2} \log(1 + \gamma_D)$, $R_{e,m} = \frac{1}{2} \log(1 + \gamma_{E,m})$. Letting $r_e = R_d - r$, we reformulate (29) as

$$\begin{aligned} \max_{\{r_e, \mathbf{v}, \mathbf{Q}_J\}} \quad & R_d - r_e \\ \text{s.t.} \quad & \text{Prob}\{R_{e,m} \leq r_e\} \geq 1 - \rho, \forall m \\ & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_r \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, \forall k \\ & \mathbf{Q}_v = \mathbf{v}\mathbf{v}^H, \mathbf{Q}_J \succeq \mathbf{0}. \end{aligned} \quad (30)$$

By applying the two-layer idea in [13], we recast (30) as a two-level optimization problem. Specifically, the outer-level problem is

$$\max_{\tau \in [\tau_{lb}, \tau_{ub}]} \frac{1}{2} \log \left(\frac{1 + \tilde{f}(\tau)}{1 + \tau} \right), \quad (31)$$

where $\tilde{f}(\tau)$ is obtained through solving the following inner-level part optimization problem for a given τ ,

$$\begin{aligned} \tilde{f}(\tau) = \max_{\{\mathbf{v}, \mathbf{Q}_J\}} \quad & \frac{P_s \mathbf{h}^H \mathbf{Q}_v \mathbf{h}}{\sigma_D^2 + \mathbf{h}_{RD}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_J) \mathbf{h}_{RD}} \\ \text{s.t.} \quad & \text{Prob}\{\gamma_{E,m} \leq \tau\} \geq 1 - \rho, \quad \forall m \\ & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_r \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, \forall k \\ & \mathbf{Q}_v = \mathbf{v}\mathbf{v}^H, \mathbf{Q}_J \succeq \mathbf{0}. \end{aligned} \quad (32)$$

By dropping the rank 1 constraint on \mathbf{Q}_v , we obtain

$$\begin{aligned} \tilde{g}(\tau) = \max_{\{\mathbf{Q}_v, \mathbf{Q}_J\}} \quad & \frac{P_s \mathbf{h}^H \mathbf{Q}_v \mathbf{h}}{\sigma_D^2 + \mathbf{h}_{RD}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_J) \mathbf{h}_{RD}} \\ \text{s.t.} \quad & \text{Prob}\{\gamma_{E,m} \leq \tau\} \geq 1 - \rho, \forall m \\ & \sum_{k=1}^N \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_r \\ & \zeta_k(\mathbf{Q}_v, \mathbf{Q}_J) \leq P_k, \forall k \\ & \mathbf{Q}_v \succeq \mathbf{0}, \mathbf{Q}_J \succeq \mathbf{0}. \end{aligned} \quad (33)$$

Proposition 7. The optimization (33) can be safely approximated with a SDP.

Proof. By letting $\eta = \frac{1}{\sigma_D^2 + \mathbf{h}_{RD}^H (\sigma_R^2 \text{diag}\{\mathbf{Q}_v\} + \mathbf{Q}_J) \mathbf{h}_{RD}}$, $\tilde{\mathbf{Q}}_v = \eta \mathbf{Q}_v$, $\tilde{\mathbf{Q}}_J = \eta \mathbf{Q}_J$, and using the Charnes-Cooper transformation, we recast the optimization (33) as

$$\begin{aligned} \tilde{g}(\tau) = \max_{\{\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_J, \eta\}} \quad & P_s \text{tr}\{\mathbf{h}\mathbf{h}^H \tilde{\mathbf{Q}}_v\} \\ \text{s.t.} \quad & \sigma_D^2 \eta + \text{tr}\{\sigma_R^2 \text{diag}\{\mathbf{h}_{RD} \mathbf{h}_{RD}^H\} \tilde{\mathbf{Q}}_v + \mathbf{h}_{RD} \mathbf{h}_{RD}^H \tilde{\mathbf{Q}}_J\} = 1 \\ & \text{Prob}\{-\mathbf{g}_{RE,m}^H \Phi \mathbf{g}_{RE,m} + \tau \eta \sigma_E^2 \geq 0\} \geq 1 - \rho, \forall m \\ & \sum_{k=1}^N \zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_J) \leq \eta P_r \\ & \zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_J) \leq \eta P_k, \forall k \\ & \tilde{\mathbf{Q}}_v \succeq \mathbf{0}, \tilde{\mathbf{Q}}_J \succeq \mathbf{0}, \eta > 0, \end{aligned} \quad (34)$$

where $\Phi = P_s \text{diag}\{\mathbf{h}_{SR}\}^H \tilde{\mathbf{Q}}_v \text{diag}\{\mathbf{h}_{SR}\} - \sigma_R^2 \tau \text{diag}\{\tilde{\mathbf{Q}}_v\} - \tau \tilde{\mathbf{Q}}_J$.

Applying the same derivation from (26) to (28), we safely approximate the rate outage constraint with LMIs, and reformulate the optimization (34) as

$$\begin{aligned} \tilde{g}(\tau) = \max_{\{\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_J, \eta, \mu_1, \dots, \mu_m\}} \quad & P_s \text{tr}\{\mathbf{h}\mathbf{h}^H \tilde{\mathbf{Q}}_v\} \\ \text{s.t.} \quad & \sigma_D^2 \eta + \text{tr}\{\sigma_R^2 \text{diag}\{\mathbf{h}_{RD} \mathbf{h}_{RD}^H\} \tilde{\mathbf{Q}}_v + \mathbf{h}_{RD} \mathbf{h}_{RD}^H \tilde{\mathbf{Q}}_J\} = 1 \\ & \begin{bmatrix} \mu_m \mathbf{I} - \mathbf{C}_m^{1/2} \Phi \mathbf{C}_m^{1/2} & -\mathbf{C}_m^{1/2} \Phi \hat{\mathbf{g}}_{RE,m} \\ -(\mathbf{C}_m^{1/2} \Phi \hat{\mathbf{g}}_{RE,m})^H & c_m - \mu_m d^2 \end{bmatrix} \succeq \mathbf{0}, \forall m \\ & \sum_{k=1}^N \zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_J) \leq \eta P_r \\ & \zeta_k(\tilde{\mathbf{Q}}_v, \tilde{\mathbf{Q}}_J) \leq \eta P_k, \forall k \\ & \tilde{\mathbf{Q}}_v \succeq \mathbf{0}, \tilde{\mathbf{Q}}_J \succeq \mathbf{0}, \eta > 0, \mu_m \geq 0, \end{aligned} \quad (35)$$

where $c_m = \tau \eta \sigma_E^2 - \hat{\mathbf{g}}_{RE,m}^H \Phi \hat{\mathbf{g}}_{RE,m}$. According to [39], the optimization (35) is a SDP and can be solved by CVX. This completes the proof. \square

Proposition 8. Go back to the optimization problem (23), and let $\delta_1 = \tilde{g}(\tau)$, $\delta_2 = \tau$. Then, the optimal solution to (23), $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_J\}$, constitutes an optimal solution to (33).

Proof. The proof is similar with that of Proposition 4 and thus omitted here. This completes the proof. \square

Remark. We should note that $\text{rank}\{\hat{\mathbf{Q}}_v\} = 1$ according to Proposition 6. Thus, the solution, $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_J\}$, is indeed a tight approximation of (32). Moreover, $\tilde{f}(\tau) = \tilde{g}(\tau)$.

So far, the inner-level part is solved and $\tilde{f}(\tau)$ is determined for any given τ . The remaining issue now is to resolve the optimal τ^* maximizing the objective function in (31). In (31), τ_{lb} and τ_{ub} denote the lower and upper bounds of $\gamma_{E,m}$, respectively. Firstly, $\gamma_{E,m}$ is no less than 0, thus we set $\tau_{lb} = 0$. Secondly, according to the security requirement, $\gamma_{E,m}$ should be no more than γ_D . Thus, we set $\tau_{ub} = P_s P_r |\mathbf{h}|^2 / \sigma_D^2$. By performing a one-dimensional search over $[\tau_{lb}, \tau_{ub}]$, the optimal τ^* which maximizes the objective function in (31) could be found. Correspondingly, the optimal solution $\{\mathbf{v}^*, \mathbf{Q}_J^*\}$ to the original optimization (29) can be obtained. In Table 2, we summarize our proposed algorithm for maximizing the outage constrained secrecy rate.

5 Numerical results

In this section, we present the numerical results to validate the secrecy rate performance of the proposed joint cooperative relaying and jamming scheme. The transmit power at the source node $P_s = 10$ dB. The covariance of noise at receivers $\sigma_D^2 = \sigma_E^2 = \sigma_R^2 = 1$. The number of relays $N = 10$. The individual relay power budget $P_k = 0.5P_r/N$ for

Table 2 An algorithm for determining the optimal solution $\{\mathbf{v}^*, \mathbf{Q}_J^*\}$ which maximizes the outage constrained secrecy rate

1. Initialize $\tau_{lb} = 0$, $\tau_{ub} = P_s P_r / |\mathbf{h}|^2 / \sigma_D^2$, $P_s > 0$, $P_r > 0$, $P_k \geq 0$, $\tau = 0$, $\tau_{sz} > 0$ where the step size τ_{sz} is an arbitrarily small positive quantity;
2. **while** $\tau \in [\tau_{lb}, \tau_{ub}]$ **do**
3. Calculate $\bar{g}(\tau)$ by solving (33) and let $\bar{f}(\tau) = \bar{g}(\tau)$;
4. Let $\tau = \tau + \tau_{sz}$;
5. **end while**
6. Determine τ^* which maximizes the objective function of (31);
7. Let $\tau = \tau^*$ and calculate $\bar{g}(\tau)$ by solving (33);
8. Calculate $\{\hat{\mathbf{Q}}_v, \hat{\mathbf{Q}}_j\}$ by solving (23);
9. Do the matrix decomposition $\hat{\mathbf{Q}}_v = \hat{\mathbf{v}}\hat{\mathbf{v}}^H$;
9. The optimal solution $\mathbf{v}^* = \hat{\mathbf{v}}$, $\mathbf{Q}_J^* = \hat{\mathbf{Q}}_j$.

$k = 1, \dots, N/2$, and $P_k = 2P_r/N$ for $k = N/2 + 1, \dots, N$. For ease of exposition, $\forall m$, we set $\beta_m/\sqrt{N} = \varepsilon$ for the case of deterministically bounded CSI error model and set $\mathbf{C}_m = \varepsilon \mathbf{I}$ for the case of stochastic CSI error model. At each trial, the entries of the channels \mathbf{h}_{SR} and \mathbf{h}_{RD} , $\hat{\mathbf{g}}_{RE,i}$ are randomly generated following an independent and identically distributed (i.i.d.) complex Gaussian distribution with zero mean and unit variance. Results are averaged over 1000 independent channel trials.

In the following figures, the lines labeled as “SRD link without Eaves” show the maximal achievable rate of the no-eavesdropper case, which provides an upper bound on the secrecy rate of all security schemes. The lines labeled as “Proposed CR and CJ” and “Relaying without jamming” illustrate the worst-case or the outage constrained secrecy rate achieved by the proposed joint cooperative relaying and jamming scheme (also referred to as the proposed scheme in the sequel) and the relaying without jamming scheme, respectively. We should note that for the relaying without jamming scheme, we set $\mathbf{Q}_J^* = 0$ and compute the relaying weights \mathbf{v}^* according to Tables 1 and 2. The lines labeled as “Jamming Power” denote the power ratio allocated to jamming signals, i.e.,

$$\delta = \text{tr}\{\mathbf{Q}_J\} / (\text{tr}\{\mathbf{Q}_v\} + \text{tr}\{\mathbf{Q}_J\}).$$

The maximal achievable secrecy rate results versus the total relay power budget are plotted in Fig. 2. Here, we set the number of eavesdroppers $M = 2$ and assume that CSI is perfectly known. That is, let $\varepsilon = 0$ or let $\mathbf{C} = \mathbf{0}$ and compute the optimal input parameter $\{\mathbf{v}^*, \mathbf{Q}_J^*\}$ according to Table 1 or Table 2. It can be observed that there exists a rate performance ceiling on the SRD link. This is because the signal received at relays contains both the signal transmitted from the source and the unavoidable additive noise. Amplifying the received signal will also amplify the additive noise. We should note that the gap between the maximal secrecy rate that can be achieved by any security

schemes and the maximal achievable rate of the SRD link is caused by the secrecy constraint. Obviously, the proposed scheme gets a smaller gap than the relaying without jamming scheme. Moreover, when the power budget at relays is large enough, the secrecy rate achieved by the proposed scheme approaches the maximal achievable rate of the SRD link.

The worst-case secrecy rate results of different schemes versus the number of eavesdroppers are plotted in Fig. 3. Here, the total relay power budget $P_r = 20$ dB and the channel mismatch $\varepsilon = 0.2$. It can be observed that both the secrecy rate achieved by the proposed scheme and that achieved by the relaying without jamming scheme decline with the increasing number of eavesdroppers. However, the secrecy rate achieved by the proposed scheme always outperforms that achieved by the relaying without jamming scheme. Moreover, the secrecy rate achieved by the proposed scheme declines gently while that achieved by the relaying without jamming scheme decreases dramatically. When the number of eavesdropper becomes larger, the power allocated to jamming signals becomes larger, and the benefits of using cooperative jamming is more obvious.

The channel mismatch impact on the worst-case secrecy rate of different schemes is plotted in Fig. 4. Here, the total relay power budget $P_r = 20$ dB and the number of eavesdroppers $M = 2$. It can be observed that both the worst-case secrecy rate achieved by the proposed scheme and that achieved by the relaying without jamming scheme decline with the increasing of channel uncertainties. However, the robustness of the proposed scheme is more obvious. In particular, the worst-case secrecy rate achieved by the proposed scheme always outperforms that achieved by the relaying without jamming scheme. Moreover, the worst-case secrecy rate achieved by the proposed scheme declines gently, while that achieved by the relaying without jamming scheme decreases dramatically. The power allocated to jamming signals increases as the channel mismatch becomes larger.

The number of eavesdroppers impact on the channel mismatch impact on the achievable outage constrained secrecy rate are plotted in Figs. 5 and 6, respectively. We set the secrecy rate outage probability $\rho = 0.1$, the total relay power budget $P_r = 20$ dB. In Fig. 5, we set the channel mismatch $\mathbf{C}_m = 0.02\mathbf{I}$ and let the number of eavesdroppers vary from 1 to 6. In Fig. 6, we set the number of eavesdroppers $M = 2$ and let the channel mismatch vary from 0 to 0.2. Similar to the behavior in Figs. 3 and 4, both the outage constrained secrecy rate achieved by the proposed scheme and that achieved by the relaying without jamming scheme decline with the increasing number of eavesdroppers or the channel uncertainties. However, the outage constrained secrecy rate achieved by the proposed scheme declines gently, while that achieved

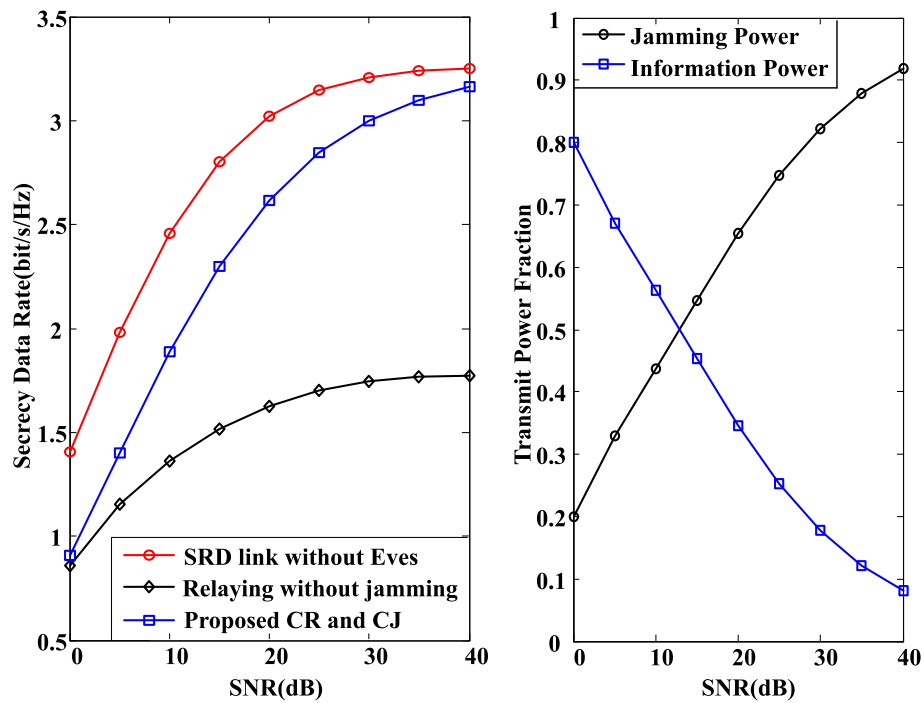


Fig. 2 Secrecy rate and transmit power fraction versus total relay power budget

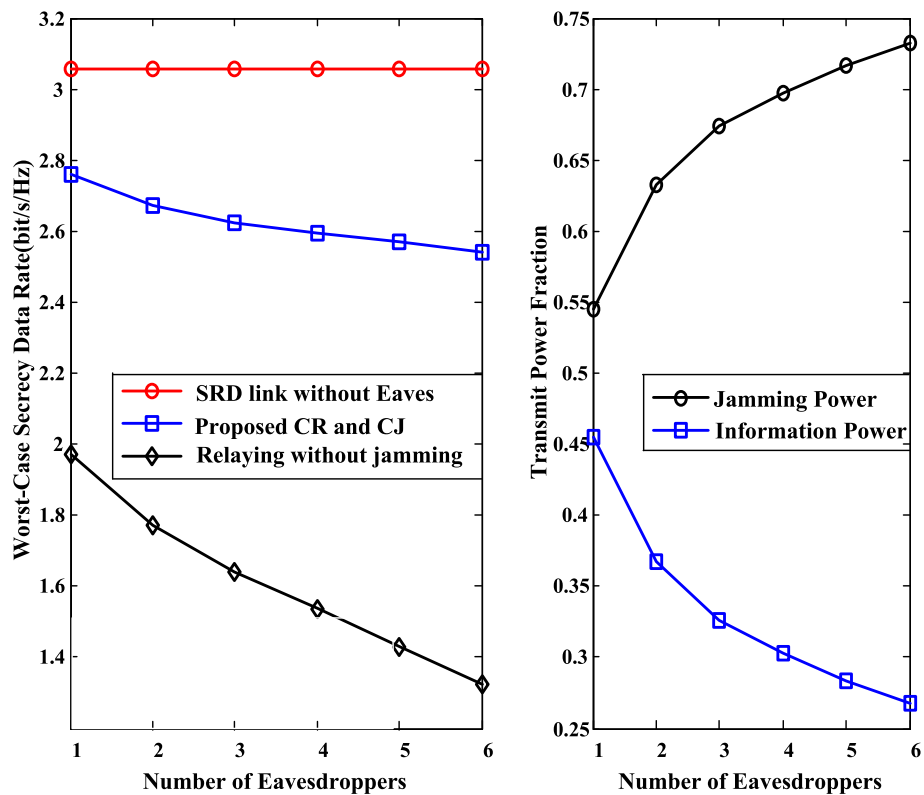


Fig. 3 Worst-case secrecy rate and transmit power fraction versus the number of eavesdroppers when $\varepsilon = 0.2$

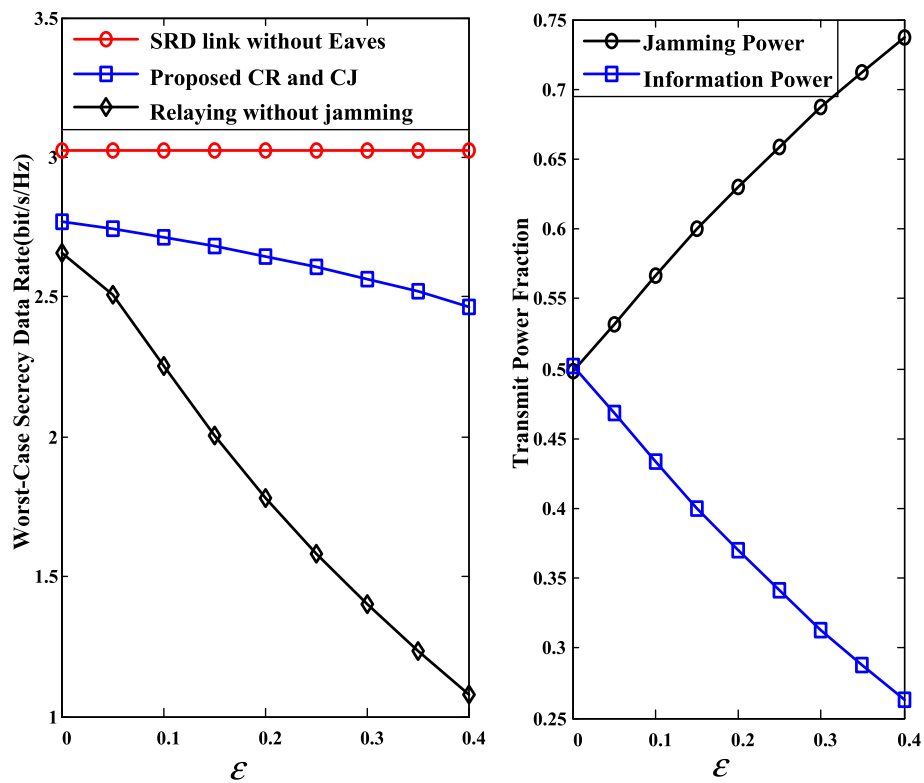


Fig. 4 Worst-case secrecy rate and transmit power fraction versus channel mismatch

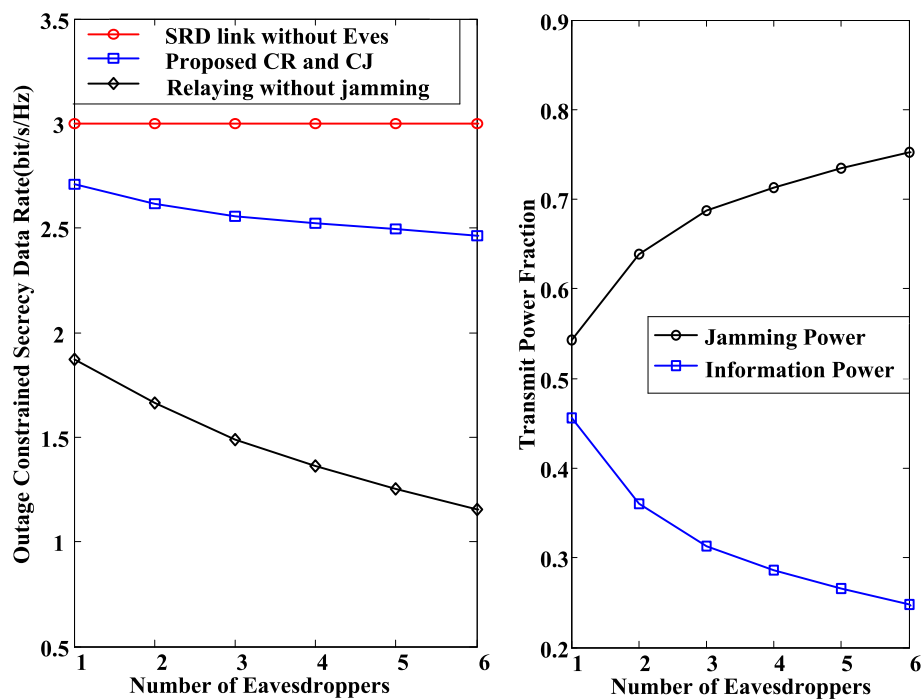


Fig. 5 Outage constrained secrecy rate and transmit power fraction versus the number of eavesdroppers

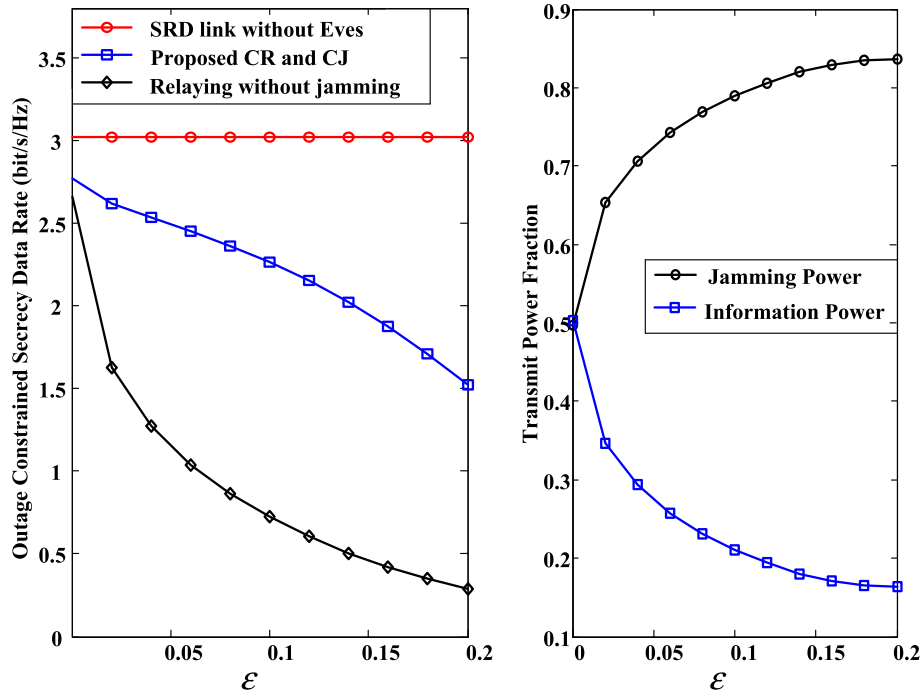


Fig. 6 Outage constrained secrecy rate and transmit power fraction versus channel mismatch

by the relaying without jamming scheme decreases dramatically. The outage constrained secrecy rate achieved by the proposed scheme always outperforms that achieved by the relaying without jamming scheme. Besides, the power ratio allocated to the jamming signals increases as the number of eavesdroppers increases or the channel mismatch becomes larger. Based on these observations, we verify the robustness of the proposed joint cooperative relaying and jamming scheme.

6 Conclusions

This paper addressed robust joint optimization of the relay weights and the input covariance matrix of jamming signals for secrecy rate maximization (SRM), under both total and individual relay power constraints. Two CSI error models, deterministically bounded error model and stochastic error model, were considered. For the case of deterministically bounded error model, we maximized the worst-case secrecy rate. While for the case of stochastic error model, we maximized the outage constrained secrecy rate. The challenge of these SRM-based optimizations lies in their non-convexity. In this paper, we provided a unified approach for solving these SRM-based optimizations. Specifically, we recast the original non-convex optimization problem into a sequence of convex optimization problems, via two-level reformulation and semidefinite relaxation techniques. Numerical results showed that the secrecy rate achieved by

the proposed joint cooperative relaying and jamming scheme outperforms that achieved by the relaying without jamming scheme. Especially, when the CSI is perfectly known and the power is large enough, the secrecy rate achieved by the proposed scheme approaches that achieved by the SRD link. Moreover, with the increasing of the total relay power budget, the number of eavesdroppers, or the channel uncertainties, distributing part of the total relay power to transmit jamming signals becomes more necessary in order to improve the secrecy rate performance.

Appendix A: Proof of Proposition 2

Proposition 2: Denote the optimal solution to (10) as $\{\hat{\mathbf{Q}}_{\mathbf{v}}, \hat{\mathbf{Q}}_{\mathbf{f}}\}$. Then $\hat{\mathbf{Q}}_{\mathbf{v}}$ is rank-one, provided that a positive secrecy rate is achieved.

Proof. According to Section III, solving the optimization (10) equals to solving the optimization (13) which is convex with part of the KKT conditions as follows

$$\begin{aligned} \mathbf{Y} = & P_s \text{diag}\{\mathbf{h}_{SR} \mathbf{h}_{SR}^H\} + \sigma_R^2 \mathbf{I} \\ & + \lambda [\sigma_R^2 f(\tau) \text{diag}\{\mathbf{h}_{RD} \mathbf{h}_{RD}^H\} - P_s \mathbf{h} \mathbf{h}^H] \\ & + \sum_{m=1}^M \text{diag}\{\mathbf{h}_{SR}\} \mathbf{G}_m \mathbf{B}_m \mathbf{G}_m^H \text{diag}\{\mathbf{h}_{SR}\}^H \\ & - \sum_{m=1}^M \sigma_R^2 \tau \text{diag}\{\mathbf{G}_m \mathbf{B}_m \mathbf{G}_m^H\} \end{aligned}$$

$$+ \sum_{k=1}^N v_k [P_s \text{diag}\{\mathbf{E}_k \mathbf{h}_{SR} \mathbf{h}_{SR}^H\} + \sigma_R^2 \mathbf{E}_k], \quad (36a)$$

$$\mathbf{X} = \mathbf{I} + \lambda f(\tau) \mathbf{h}_{RD} \mathbf{h}_{RD}^H - \sum_{m=1}^M \tau \mathbf{G}_m \mathbf{B}_m \mathbf{G}_m^H + \sum_{k=1}^N v_k \mathbf{E}_k, \quad (36b)$$

$$\mathbf{Y} \hat{\mathbf{Q}}_v = \mathbf{0}, \quad (36c)$$

$$\mathbf{Y} \succeq \mathbf{0}, \mathbf{X} \succeq \mathbf{0}, \mathbf{B}_m \succeq \mathbf{0}, \forall m, v_k \geq 0, \forall k, \lambda \geq 0, \quad (36d)$$

in which $\mathbf{G}_m = [\mathbf{I}, \hat{\mathbf{g}}_{RE,m}]$. \mathbf{Y} and \mathbf{X} are dual variables associated with $\hat{\mathbf{Q}}_v$ and $\hat{\mathbf{Q}}_j$, respectively. In addition, λ , \mathbf{B}_m and v_k are dual variables associated with corresponding inequalities in (13).

Combining (36a) and (36b), we arrive at the following equality

$$\begin{aligned} \mathbf{Y} = & P_s \text{diag}\{\mathbf{h}_{SR} \mathbf{h}_{SR}^H\} + \sigma_R^2 \text{diag}\{\mathbf{X}\} \\ & + \sum_{m=1}^M \text{diag}\{\mathbf{h}_{SR}\} \mathbf{G}_m \mathbf{B}_m \mathbf{G}_m^H \text{diag}\{\mathbf{h}_{SR}\}^H \\ & + \sum_{k=1}^N v_k [P_s \text{diag}\{\mathbf{E}_k \mathbf{h}_{SR} \mathbf{h}_{SR}^H\}] \\ & - \lambda P_s \mathbf{h} \mathbf{h}^H. \end{aligned}$$

Let

$$\begin{aligned} \tilde{\mathbf{Y}} = & P_s \text{diag}\{\mathbf{h}_{SR} \mathbf{h}_{SR}^H\} + \sigma_R^2 \text{diag}\{\mathbf{X}\} \\ & + \sum_{m=1}^M \text{diag}\{\mathbf{h}_{SR}\} \mathbf{G}_m \mathbf{B}_m \mathbf{G}_m^H \text{diag}\{\mathbf{h}_{SR}\}^H \\ & + \sum_{k=1}^N v_k [P_s \text{diag}\{\mathbf{E}_k \mathbf{h}_{SR} \mathbf{h}_{SR}^H\}]. \end{aligned}$$

Then we have

$$\mathbf{Y} = \tilde{\mathbf{Y}} - \lambda P_s \mathbf{h} \mathbf{h}^H. \quad (37)$$

Generally, $\text{diag}\{\mathbf{h}_{SR} \mathbf{h}_{SR}^H\} \succ \mathbf{0}$. And the other two terms in the sum expression of $\tilde{\mathbf{Y}}$ are non-negative hermite matrices. On the other hand, from (36d), $\mathbf{X} \succeq \mathbf{0}$, so $\text{diag}\{\mathbf{x}_d\} \succeq \mathbf{0}$. Therefore, we arrive at $\tilde{\mathbf{Y}} \succ \mathbf{0}$.

According to [41], we have $\text{rank}\{\lambda P_s \mathbf{h} \mathbf{h}^H \hat{\mathbf{Q}}_v\} \leq 1$. Substituting (37) into (36c), we arrive at $\tilde{\mathbf{Y}} \hat{\mathbf{Q}}_v = \lambda P_s \mathbf{h} \mathbf{h}^H \hat{\mathbf{Q}}_v$. Thus, $\text{rank}\{\tilde{\mathbf{Y}} \hat{\mathbf{Q}}_v\} = \text{rank}\{\lambda P_s \mathbf{h} \mathbf{h}^H \hat{\mathbf{Q}}_v\} \leq 1$. In addition, $\tilde{\mathbf{Y}} \succ \mathbf{0}$, so $\text{rank}\{\hat{\mathbf{Q}}_v\} = \text{rank}\{\tilde{\mathbf{Y}} \hat{\mathbf{Q}}_v\} \leq 1$. On the other hand, $\text{rank}\{\hat{\mathbf{Q}}_v\} = 0$ implies $\hat{\mathbf{Q}}_v = \mathbf{0}$ which contradicts with the positive secrecy rate requirement. Thus, $\text{rank}\{\hat{\mathbf{Q}}_v\} = 1$. The completes the proof. \square

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grant 61571089 and by the High-Tech Research and Development (863) Program of China under Grand 2015AA01A707.

Received: 29 December 2015 Accepted: 20 May 2016

Published online: 02 June 2016

References

- AD Wyner, The wire-tap channel. *Bell Syst. Tech. J.* **54**(8), 1355–1387 (1975)
- SK Leung-Yan-Cheong, ME Hellman, The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory.* **24**(4), 451–456 (1978)
- T Liu, S Shamai(Shitz), A note on the secrecy capacity of the multi-antenna wire-tap channel. *IEEE Trans. Inf. Theory.* **55**(6), 2547–2553 (2009)
- A Khisti, G Wornell, Secure transmission with multiple antennas I: the MISOE wiretap channel. *IEEE Trans. Inf. Theory.* **56**(7), 3088–3104 (2010)
- A Khisti, G Wornell, Secure transmission with multiple antennas II: the MIMOME wiretap channel. *IEEE Trans. Inf. Theory.* **56**(11), 5515–5532 (2010)
- J Li, AP Petropulu, in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels, (Dallas, 2010), pp. 3362–3365
- J Li, AP Petropulu, in *IEEE GLOBECOM 2011 Workshop on Physical-Layer Security*. On beamforming solution for secrecy capacity of MIMO wiretap channels, (Huston, 2011), pp. 889–892
- SAA Fakoorian, AL Swindlehurst, Solutions for the MIMO gaussian wiretap channel with a cooperative jammer. *IEEE Trans. Signal Process.* **59**(10), 5013–5022 (2011)
- SAA Fakoorian, AL Swindlehurst, in *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*. Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel, (Cambridge, 2012), pp. 2321–2325
- H-T Chiang, JS Lehnert, in *IEEE Military Communications Conference (MILCOM)*. Optimal cooperative jamming for security, (Baltimore, 2011), pp. 125–130
- J Huang, AL Swindlehurst, Cooperative jamming for secure communications MIMO relay networks. *IEEE Trans. Signal Process.* **59**(10), 4871–4884 (2011)
- L Li, Z Chen, J Fang, On secrecy capacity of Gaussian wiretap channel aided by a cooperative jammer. *IEEE Signal Process. Lett.* **21**(11), 1356–1360 (2014)
- G Zheng, L-C Choo, K-K Wong, Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Trans. Signal Process.* **59**(3), 1317–1322 (2011)
- L Dong, Z Han, AP Petropulu, HV Poor, Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **58**(3), 1875–1888 (2010)
- J Li, AP Petropulu, S Weber, On cooperative relaying schemes for wireless physical layer security. *IEEE Trans. Signal Process.* **59**(10), 4985–4997 (2011)
- Y Yang, Q Li, W-K Ma, Cooperative secure beamforming for AF relay networks with multiple eavesdroppers. *IEEE Signal Process. Lett.* **20**(1), 35–38 (2013)
- I Krikidis, JS Thompson, S McLaughlin, Relay selection for secure cooperative networks with jamming. *IEEE Trans. Wirel. Commun.* **8**(10), 5003–5011 (2009)
- S Vasudevan, S Adams, D Goeckel, Z Ding, D Towsley, KK Leung, in *2010 Annual Conference of ITA (ACITA)*. Secrecy in wireless relay channels through cooperative jamming, (Imperial College, London, 2010)
- D Goeckel, S Vasudevan, D Towsley, S Adams, Z Ding, K Leung, Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. *IEEE J. Sel. Areas Commun.* **29**(10), 2067–2076 (2011)
- G Zheng, J Li, K-K Wong, AP Petropulu, B Ottersten, in *2012 1st IEEE International Conference on Communications in China (ICCC)*. Using simple relays to improve physical-layer security, (Beijing, 2012), pp. 329–333
- H-M Wang, M Luo, Q Yin, in *IEEE Global Communications Conference (GLOBECOM)*. Hybrid cooperative relaying and jamming for secure two-way relay networks, (Anaheim, 2012), pp. 4846–4850
- J Chen, R Zhang, L Song, Z Han, B Jiao, Joint relay and jammer selection for secure two-way relay networks. *IEEE Trans. Inf. Forensics Secur.* **7**(1), 310–320 (2012)
- H-M Wang, M Luo, X-G Xia, Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI. *IEEE Signal Process. Lett.* **20**(1), 39–42 (2013)
- X Wang, K Wang, X-D Zhang, Secure relay beamforming with imperfect channel side information. *IEEE Trans. Veh. Technol.* **62**(5), 2140–2155 (2013)
- K-H Park, T Wang, M-S Alouini, On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming. *IEEE J. Sel. Areas Commun.* **31**(9), 1741–1750 (2013)

26. S Vishwakarma, A Chockalingam, in *IEEE International Conference on Communications (ICC)*. Amplify-and-forward relay beamforming for secrecy with cooperative jamming and imperfect CSI, (Budapest, 2013), pp. 1640–1645
27. L Li, Z Chen, J Fang, in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Robust transmit design for secure AF relay networks based on worst-case optimization, (Florence, 2014), pp. 2719–2723
28. Y Yang, Q Li, W-K Ma, J Ge, in *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. Optimal joint cooperative beamforming and artificial noise design for Secrecy Rate Maximization in AF Relay Networks, (Darmstadt, 2013), pp. 360–364
29. R Negi, S Goel, in *IEEE 62nd Vehicular Technology Conference (VTC-2005-Fall)*. Secret communication using artificial noise, (Texas, 2005), pp. 1906–1910
30. Q Li, W-K Ma, in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. A robust artificial noise aided transmit design for MISO secrecy (Prague Congress Center, Prague, Czech Republic, 2011), pp. 3436–3439
31. J Huang, AL Swindlehurst, Robust secure transmission in MISO channels based on worst-case optimization. *IEEE Trans. Signal Process.* **60**(4), 1696–1707 (2012)
32. S Luo, J Li, AP Petropulu, Uncoordinated cooperative jamming for secret communications. *IEEE Trans. Inf. Forensics Secur.* **8**(7), 1081–1090 (2013)
33. X Zhou, MR McKay, B Maham, A Hjørungnes, Rethinking the secrecy outage formulation: a secure transmission design perspective. *IEEE Commun. Lett.* **15**(3), 302–304 (2011)
34. X Zhang, X Zhou, MR McKay, On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels. *IEEE Trans. Veh. Technol.* **62**(5), 2170–2181 (2013)
35. Q Li, W-K Ma, AM-C So, A safe approximation approach to secrecy outage design for MIMO wiretap channels. *IEEE Signal Process. Lett.* **21**(1), 118–121 (2014)
36. V Jungnickel, MST Wirth, T Haustein, W Zirwas, in *International Symposium on Wireless Communication Systems (ISWCS)*. Synchronization of cooperative base stations, (Reykjavik, 2008), pp. 329–334
37. G Barriac, R Mudumbai, U Madhow, in *3rd International Symposium on Information Processing in Sensor Networks (IPSN)*. Distributed beamforming for information transfer in sensor networks, (Berkeley, 2004), pp. 81–88
38. B Zarikoff, J Cavers, Multiple frequency offset estimation for the downlink of coordinated MIMO systems. *IEEE J. Sel. Areas Commun.* **26**(6), 901–912 (2008)
39. S Boyd, L Vandenberghe, *Convex optimization*. (Cambridge University Press, Cambridge, 2004)
40. K-Y Wang, AM-C So, T-H Chang, W-K Ma, C-Y Chi, Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization. *IEEE Tran. Singal Process.* **62**(21), 5690–5705 (2014)
41. RA Horn, CR Johnson, *Matrix Analysis*. (Cambridge University Press, 1985)

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com