Robust Cooperative Relay Beamforming Design for Security

Xiangwu Gong[1,2], Feihong Dong[1,2], Hongjun Li[1,2] and Wei Shao[1]
[1] College of Communications Engineering, PLA University of Science and Technology, Nanjing 210000- China
[2] Institute of China Electronic System Engineering Corporation, Beijing 100141, People's Republic of China
[e-mail: xiangwugong@hotmail.com, dfh_sinlab@hotmail.com, xclhj1985@163.com, swlxssz@126.com]
*Corresponding author: Xiangwu Gong

Received July 4, 2015; revised September 1, 2015; accepted September 16, 2015; published November 30, 2015

Abstract

In this paper, we investigate a security transmission scheme at the physical layer for cooperative wireless relay networks in the presence of a passive eavesdropper. While the security scheme has been previously investigated with perfect channel state information(CSI) in the presence of a passive eavesdropper, this paper focuses on researching the robust cooperative relay beamforming mechanism for wireless relay networks which makes use of artificial noise (AN) to confuse the eavesdropper and increase its uncertainty about the source message. The transmit power used for AN is maximized to degrade the signal-to-interference-plus-noise-ratio (SINR) level at the eavesdropper, while satisfying the individual power constraint of each relay node and worst-case SINR constraint at the desired receiver under a bounded spherical region for the norm of the CSI error vector from the relays to the destination. Cooperative beamforming weight vector in the security scheme can be obtained by using S-Procedure and rank relaxation techniques. The benefit of the proposed scheme is showed in simulation results.

Keywords: Security transmission, cooperative beamforming, physical layer security, imperfect CSI, SINR

This work is supported by National Natural Science Foundation of China under Grant No. (91338106, 61231011, 61201241, 91338201 and 91438109).

http://dx.doi.org/10.3837/tiis.2015.11.013 **ISSN : 1976-7277**

1. Introduction

Due to the broadcast nature of the wireless medium, information from source could be obtained by an eavesdropper, the issues of privacy and security in wireless networks have taken on an increasingly important role, especially in civil security and military applications. Recent information-theoretic research on secure communication has focused on enhancing security at the physical layer [1]-[5]. Physical layer security exploits the physical characteristics of the wireless channel to transmit information secretly which is different from the conventional encryption techniques. This problem was first researched by Wyner [6], who introduced the wiretap channel model to achieve information-theoretic security transmission. Wyner found that when an eavesdropper obtains a degraded version of the legitimate receiver's observation, messages can be exchanged secretly at a non-zero rate between the source and the destination, while anything about the messages can not be learned by the eavesdropper.

The cooperative diversity mechanism makes use of the benefits of wireless relay network scalability in terms of cooperative resource sharing in which multiple diversity channels are created which results into higher transmission rates, increased throughout and coverage range, improvement in reliability and end-to-end performance and much more, while it can be vulnerable to eavesdropping attacks due to the additional transmission of the source message. Recently the physical layer security transmission for the cooperative relay communications has also been researched [7]-[9]. By making use of relay cooperation, wireless physical layer security can be enhanced greatly against eavesdropping attacks.

The difference between the channel capacity from source to destination (called legitimate link) and that from source to eavesdropper (called wiretap link) is defined as the achievable secrecy rate , and the maximal achievable secrecy rate is named as the secrecy capacity in [1] and [10]. At present, most work focuses on investigating the secrecy capacity at which a message can be sent secretly to intended destination while the eavesdropper cannot decode it from an information-theoretic perspective. In [11], the authors proposed the cooperative jamming and analyzed the secrecy capacity. In [12], the authors addressed secure communications of one source-destination pair with help of multiple cooperating relays in the presence of one or more eavesdroppers where the achievable secrecy rate was maximized subject to a transmit power constraint. In [13], the authors investigated the secure communication of this two-way relay scenario using physical layer security where they defined and then analyzed a source optimization problem to obtain the maximum secrecy rate. In these literatures, the CSI of the eavesdropper is known by the transmitter. Actually the eavesdropper is totally passive and even that whether there exists any eavesdropper can not be prior known in a real wiretap case. Under the condition of no eavesdropper's CSI, we can not optimize the secrecy rate directly.

Alternatively, a masked beamforming way [14] is adopted to enhance the security communication at the physical layer in this paper. It uses only the legitimate users' CSI and the artificial noise(AN) is adopted to jam the eavesdropper [15]. This way has been used to achieve security transmission for multiple-input multiple-output(MIMO) downlink wiretap channels in [16], which adopted signal-to-interference-plusnoise-ratio(SINR) as the quality-of-service(QoS) metric.

In [17], a masked beamforming way was also proposed to improve the security at the physical layer for relay communications with no eavesdropper's CSI. In [18], the authors

proposed a hybrid cooperative beamforming and jamming scheme to enhance the physical layer security of a two-way relay network in the presence of a passive eavesdropper. However, they both assumed that the available CSI was perfect. If perfect CSI is available at the transmitter, then the AN can be made invisible to the intended receiver while degrading the potential eavesdropper's channel. Obviously, it is not impossible in practice due to some factors such as quantization noise and channel mobility, etc. The inaccurate CSI for legitimate links can result in degrading to the intended user's SINR because of interference leakage to the intended user.

In [19], the authors studied the cooperative transmission for securing a decode-and-forward (DF) two-hop network under the more practical assumption that only the channel distribution information (CDI) of the eavesdropper was known. In [20], the authors investigated the physical-layer security issue of an amplify-and-forward (AF) relay network and proposed a joint cooperative beamforming and cooperative jamming design that was robust to the imperfect CSI of the multiple multi-antenna eavesdroppers. However, it is known that the secrecy rate can not be optimized directly in the presence of a passive eavesdropper. In [21], the authors studied the robust AF relay beamforming security scheme in presence of a passive eavesdropper where CSI errors were modeled as Gaussian and average mean square error(MSE) constraint was considered focusing entirely on system performance. Different from [21], this study considers a norm-bounded error model and the worst-case SINR constraint placing the highest emphasis on fairness.

In this paper, we investigate the robust beamforming scheme for security in the cooperative wireless relay networks with one source, multiple relays, one legitimate user when a passive eavesdropper is present. In this system, all nodes are equipped with single antenna. Imperfection in the CSI is modeled using a norm-bounded error model. The transmit power of the AN which lies in the null space of legitimate channels is maximized to confuse the eavesdropper, while subject to worst-case SINR constraint at the intended user. In this paper, we also consider individual power constraint of each relay node, which is more practical. A robust algorithm using S-Procedure and rank relaxation techniques is proposed to solve the minimization problem of the total transmit power of the relays for the information-bearing signals subject to worst-case SINR constraint at the intended user and the individual power constraint of each relay, which is the same as maximization of the power of the AN. In addition, an upper bound of the the transmit power of the AN can be obtained by solving multiple second-order cone-programming(SOCP) problems. Simulations show that secrecy capacity in the robust beamforming scheme is improved compared with that obtained by a naive scheme where CSI errors are not considered.

The rest of this paper is organized as follows. In Section II, the system model is described. In Section III, CSI uncertainty is described and problem formulation is proposed. In Section IV, a robust beamforming design is proposed. In Section V, the simulation results are showed. We conclude the paper in Section VI.

The notation is adopted as follows: Boldface lower (upper) case letters represent vectors (matrices); $C^{n\times m}$ and $R^{n\times m}$ stand for spaces of $n\times m$ complex and real matrices, respectively; $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$ and $(\cdot)^\dagger$ indicate transpose, conjugate, conjugate transpose and Moore Penrose inverse, respectively; $tr(\cdot)$ and $E(\cdot)$ denote the trace operator and the expectation operator; $\mathbf{A}\succ 0$ means that $\mathbf{A}$ is positive definite; $\|\mathbf{a}\|$ represents the 2-norm of the vector $\mathbf{a}$; $\mathbf{I}_M$ is the $M\times M$ identity matrix; $diag(a_1,\cdots, a_N)$ is an N sized diagonal matrix with

$a_1,\cdots, a_N$ as its diagonal elements; $log(\cdot)$ denotes the base-2 logarithm.

2. SYSTEM MODEL

We consider a cooperative relay communications system model showed in **Fig. 1**. The system consists of one source node S, n relays $\{R_i, i=1,\cdots,n\}$, one destination node D and one passive eavesdropper E. Each of nodes is equipped with single antenna and the relays use the AF protocol. The main and wiretap links are represented by the solid and dash lines, respectively. In order to focus on the effect of cooperative relay beamforming with imperfect CSI, we assume that there are no direct links from the source to the destination and eavesdropper due to the large path loss and strong shadow fading, as assumed in **[22]** and **[23]**. The passive eavesdropper E attempts to wiretap the information received by the destination node D.

The signal $\mathbf{x}_r = \left(x_{r,1},\cdots,x_{r,n}\right)^H \in C^{n\times 1}$ received by the relays is given by

$$\mathbf{x}_r = \sqrt{P}\mathbf{h}_{sr}s + \mathbf{n}_r, \tag{1}$$

where s is the signal with power P transmitted by the source and we normalize it to 1, i.e. $E\left(|s|^2\right)=1$, $\mathbf{h}_{sr} = \left(h_{sr,1},\cdots,h_{sr,1}\right)^H \in C^{n\times 1}$ is channel gain from the source to relays whose elements are independent and identically distributed (i.i.d.) complex Gaussian variables, and $\mathbf{n}_r \in C^{n\times 1}$ is noise vector whose elements are i.i.d. complex Gaussian with zero mean and variances σ_r^2.

Because the passive eavesdropper only receives signal, its channel knowledge is completely unknown for the transmitters. We also cannot optimize secrecy rate to protect the intended information. An AN scheme is a possible way to realize security transmission [23]. This scheme makes an attempt to degrade the decode ability of the eavesdropper.

The signal $\mathbf{y}_r = \left(y_{r,1},\cdots,y_{r,n}\right)^H \in C^{n\times 1}$ transmitted by the relays is given by

$$\mathbf{y}_r = \mathbf{W}\mathbf{x}_r + \mathbf{n}_{an}, \tag{2}$$

where $\mathbf{W} = diag\left(w_1,\cdots,w_n\right)$ is beamforming weight matrix in which w_i is the i th AF relay's weight, $\mathbf{n}_{an} \in C^{n\times 1}$ is the artificial noise and $P_{an} = E\left(\mathbf{n}_{an}^H\mathbf{n}_{an}\right)$ is allocated. We also assume that the transmit power of the signal transmitted by the i th relay is constrained, i.e. $E\left(\left|y_{r,i}\right|^2\right) \le P_i, i=1,\cdots,n$.

The total transmit power of the relays for the information-bearing signals can be denoted as

$$P_s = \mathbf{w}\left(P\mathbf{R}_{sr} + \sigma_r^2\mathbf{I}_n\right)\mathbf{w}, \tag{3}$$

where $\mathbf{R}_{sr} = diag\left(\left|h_{sr,1}\right|^2,\cdots,\left|h_{sr,n}\right|^2\right)$ and $\mathbf{w} = \left(w_1,\cdots,w_n\right)^H$.

The signal received by the destination is

$$y_d = \sqrt{P}\mathbf{h}_{rd}^H\mathbf{W}\mathbf{h}_{sr}s + \mathbf{h}_{rd}^H\mathbf{n}_{an} + \mathbf{h}_{rd}^H\mathbf{W}\mathbf{n}_r + n_d, \tag{4}$$

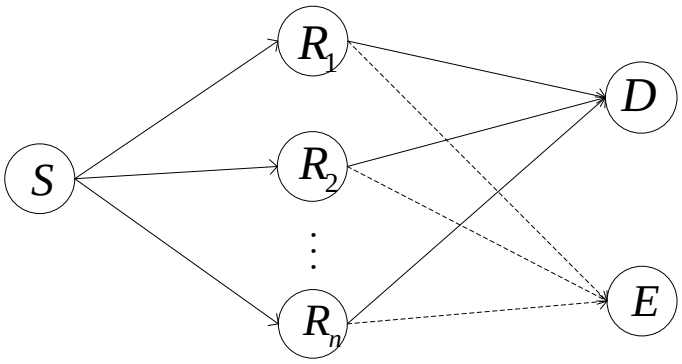


Fig. 1. System model

where $\mathbf{h}_{rd} = \left(h_{rd,1}, \cdots, h_{rd,n}\right)^H \in C^{n\times 1}$ is channel gain from the relays to destination whose elements are i.i.d. complex Gaussian variables, and n_d is additive noise that is complex Gaussian with zero mean and variance σ_d^2.

AN should not impact the legitimate links, so that it should lie in the null space of $\mathbf{h}_{rd}$, i.e. $\mathbf{h}_{rd}^H \mathbf{n}_{an} = 0$. We can obtain $\mathbf{n}_{an} = \mathbf{\Pi v}$, $\mathbf{\Pi}$ is an orthonormal basis of the null space of $\mathbf{h}_{rd}$ and $\mathbf{\Pi}^H \mathbf{\Pi} = \mathbf{I}$. Assuming that elements of $\mathbf{v}$ are i.i.d. Gaussian variables with zero mean and variances $\sigma_{a,j}^2$, $j = 1, \cdots, n-1$.

The signal received by the eavesdropper is

$$y_e = \sqrt{P}\mathbf{h}_e^H \mathbf{W}\mathbf{h}_{sr} s + \mathbf{h}_e^H \mathbf{n}_{an} + \mathbf{h}_e^H \mathbf{W}\mathbf{n}_r + n_e \ , \tag{5}$$

where $\mathbf{h}_e = \left(h_{e,1}, \cdots, h_{e,n}\right)^H \in C^{n\times 1}$ is channel gain from the relays to the eavesdropper, and n_e is additive noise that is complex Gaussian with zero mean and variance σ_e^2.

With perfect CSI, the AN can be made invisible to the intended receiver and the received SINR at the destination is expressed as

$$SINR_L = \frac{P\mathbf{w}^H \mathbf{r}_h \mathbf{r}_h^H \mathbf{w}}{\sigma_r^2 \mathbf{w}^H \mathbf{R}_{rd} \mathbf{w} + \sigma_d^2} \ , \tag{6}$$

where $\mathbf{r}_h = \left(h_{sr,1}^* h_{rd,1}, \cdots, h_{sr,n}^* h_{rd,n}\right)^H$, $\mathbf{R}_{rd} = diag\left(\left|h_{rd,1}\right|^2, \cdots, \left|h_{rd,n}\right|^2\right)$.

The potential eavesdropper is confused by AN and the received SINR at the eavesdropper is expressed as

$$SINR_E = \frac{P\mathbf{w}^H \mathbf{r}_{eh} \mathbf{r}_{eh}^H \mathbf{w}}{\sigma_r^2 \mathbf{w}^H \mathbf{R}_{re} \mathbf{w} + P_{an} \mathbf{h}_e^H \mathbf{\Pi}\mathbf{\Pi}^H \mathbf{h}_e + \sigma_e^2} \tag{7}$$

where $\mathbf{r}_{eh} = \left(h_{sr,1}^* h_{e,1}, \cdots, h_{sr,n}^* h_{e,n}\right)^H$, $\mathbf{R}_e = diag\left(\left|h_{e,1}\right|^2, \cdots, \left|h_{e,n}\right|^2\right)$.

To achieve the security transmission, the achievable maximum secrecy rate with perfect CSI can be expressed as

$$C_s = \frac{1}{2}\left\{\log\left(1+SINR_L\right)-\log\left(1+SINR_E\right)\right\}^+, \quad (8)$$

where $a^+ = \max\{0, a\}$.

3. CSI UNCERTAINTY AND PROBLEM FORMULATION

In [21], the authors considered Gaussian errors model and average MSE constraint focusing entirely on system performance. In this section, we provide a norm-bounded CSI error model and a security transmission scheme under the constraint of worst-case SINR placing the highest emphasis on fairness.

We can not obtain the eavesdropper's CSI because it is a passive node. The secrecy rate in (8) may not be optimized to obtain the secrecy capacity directly. Observing (6), (7) and (8) we can note that we hope to decrease (7) as small as possible while increasing (6). So we may achieve security transmission by jamming the eavesdropper as large as possible. We consider to maximize the transmit power of the AN subject to the received SINR constraint of the destination and individual power constraint of each relay to jam the eavesdropper. This optimization problem is the same as those of minimizing the total transmit power of the relays for the information-bearing signals with SINR and individual power constraint of each relay. With perfect CSI, the optimization problem is given by

$$\begin{aligned} &\min_{\mathbf{w}} \mathbf{w}^H \mathbf{T} \mathbf{w} \\ &s.t. SINR_L \geq \lambda \\ &\left[\mathbf{w}\mathbf{w}^H\right]_{i,i}\left[\mathbf{T}\right]_{i,i} \leq P_i, i = 1, \cdots, n \end{aligned}, \quad (9)$$

where $\mathbf{T} = P\mathbf{R}_{sr} + \sigma_r^2 \mathbf{I}_n, \lambda > 0$ is the required SINR threshold.

The problem in (9) has been solved in [17], where the authors convert this problem to an SOCP problem which can be solved optimally by interior methods. However, the authors in [17] only consider the security transmission scheme under the condition of perfect CSI.

In this paper, we focus on investigating the case where the CSI is known imperfectly at the source with its uncertainty. Different phenomena, e.g. estimation error, channel mobility, etc, can result in CSI uncertainty.

The channel gain $\mathbf{h}_{sr}$ can be directly estimated from training at the source. At high training SINRs, it is reasonable to assume that $\mathbf{h}_{sr}$ can be known nearly perfectly at the source. This is, however, not true for $\mathbf{h}_{rd}$, which, in practice, will have to be estimated by the relays and then fed back the source.

Channel uncertainty in $\mathbf{h}_{rd}$ is modeled as

$$\mathbf{h}_{rd} = \hat{\mathbf{h}}_{rd} + \mathbf{e}_{rd}, \quad (10)$$

where $\mathbf{h}_{rd}$ is the true channel gain, $\hat{\mathbf{h}}_{rd} = \left(h_{rd,1}, \cdots, h_{rd,n}\right)^H$ is the estimated channel gain, and $\mathbf{e}_{rd} = \left(e_{rd,1}, \cdots, e_{rd,n}\right)^H$ is the additive error vector. A norm-bounded CSI model is considered without any statistical knowledge, where it is assumed that

$$S=\left\{\mathbf{e}_{rd}\in C^{n\times 1}:\left\|\mathbf{e}_{rd}\right\|^2\le n\rho^2,\rho>0\right\}. \tag{11}$$

This error model has been adopted in [25] and [26] where it is called as the spherical error model. It is worth noting that the results of this paper can be easily extended to the case with an ellipsoidal error region.

With imperfect CSI, AN lies in the null space of the estimated channel $\mathbf{h}_{rd}$ and the received SINR at the destination is rewritten as

$$SINR_{LI}=\frac{P\left|\sum_{i=1}^{n}\left(\hat{h}_{rd,i}+e_{rd,i}\right)h_{sr,i}w_i\right|^2}{\sigma_r^2\sum_{i=1}^{n}\left|\hat{h}_{rd,i}+e_{rd,i}\right|^2\left|w_i\right|^2+P_{an}\left\|\mathbf{e}_{rd}\right\|^2+\sigma_d^2}, \tag{12}$$

where $P_{an}=P_{\max}-\mathbf{w}^H\left(P\mathbf{R}_{sr}+\sigma_r^2\mathbf{I}_n\right)\mathbf{w}$ and $P_{\max}=\sum_{i=1}^{n}P_i$.

Therefore, the secrecy rate with CSI uncertainty can be denoted as

$$C_s=\frac{1}{2}\left\{\log\left(1+SINR_{LI}\right)-\log\left(1+SINR_E\right)\right\}^+ \tag{13}$$

Obviously, we can note that the orthogonality between the intended signal and the AN will be lost due to the inaccurate CSI for legitimate links. We also find that the inaccurate CSI can result in degrading to the intended user's SINR because of interference leakage to the intended user by comparing (6) with (12). However, if the transmitter has partial knowledge of the CSI error, it is possible that the received SINR target at the destination is achieved by adjusting power allocation for the information-bearing signals and AN.

Considering the CSI uncertainty, our aim is to minimize the total transmit power of the relays for the information-bearing signals with worst-case SINR constraint of the destination and the individual power constraint of each relay. The remaining power is used for AN to confuse the eavesdropper. Mathematically, the problem can be written as

$$\begin{aligned}&\min_{\mathbf{w}}\ \mathbf{w}^H\mathbf{T}\mathbf{w}\\&s.t.\min_{\mathbf{e}_{rd}}SINR_L\ge\lambda\\&\left[\mathbf{w}\mathbf{w}^H\right]_{i,i}\left[\mathbf{T}\right]_{i,i}\le P_i,i=1,\cdots,n\end{aligned}, \tag{14}$$

The worst-case SINR constraint in (14) can be rewritten as $\min_{\mathbf{e}_{rd}} f\left(\mathbf{e}_{rd}\right)\ge 0$, where $f\left(\mathbf{e}_{rd}\right)$ is given by (15).

$$f\left(\mathbf{e}_{rd}\right)\overset{\Delta}{=}\sqrt{P}\left|\sum_{i=1}^{n}\left(\hat{h}_{rd,i}+e_{rd,i}\right)h_{sr,i}w_i\right|-\sqrt{\lambda\left(\sigma_r^2\sum_{i=1}^{n}\left|\hat{h}_{rd,i}+e_{rd,i}\right|^2\left|w_i\right|^2+P_{an}\left\|\mathbf{e}_{rd}\right\|^2+\sigma_d^2\right)} \tag{15}$$

We can know from [27] that the minimum of $f\left(\mathbf{e}_{rd}\right)$ is mathematically intractable due to that both the signal and self-interference contain the uncertainty. The minimum of $f\left(\mathbf{e}_{rd}\right)$ is very difficult to solve.

4. ROBUST AF RELAY BEAMFORMING SCHEME

In this section, we first provide an upper bound and a lower bound for the problem in (14). The lower bound is generally not achievable, so a scheme is also proposed to obtain the robust beamforming weight vector $\mathbf{w}$.

4.1 A Lower Bound of (14)

To obtain a lower bound for the problem in (14), a box region is considered. The box region is defined as

$$Z_R = \left\{ \mathbf{e}_{rd} \in R^{n\times 1} : \left| e_{rd,i} \right| \le \rho, \rho > 0, \forall i \right\} . \tag{16}$$

Z_R is a subset of S and the beamforming scheme based on Z_R will be a lower bound.

We define $\bar{h}_{rd,i} = \left| \hat{h}_{rd,i} \right|$ and $\bar{e}_{rd,i} = e_{rd,i} \left(\dfrac{\hat{h}^*_{rd,i}}{\left| h_{rd,i} \right|} \right)$. $\left| \hat{h}_{rd,i} + e_{rd,i} \right| = \left| \bar{h}_{rd,i} + \bar{e}_{rd,i} \right|$ can be achieved.

Lemma 1: The problem in (14) is lower bounded by solving the problem in (17) which is a convex power minimization problem.

$$\begin{aligned} &\min_{\mathbf{w}\in R^{n\times 1}, \mathbf{w}\ge 0} \mathbf{w}^H \mathbf{T} \mathbf{w} \\ &s.t. \min_{\bar{\mathbf{e}}_{rd}} SINR_{LIE} \ge \lambda, \forall \bar{\mathbf{e}}_{rd} \in Z_R \ , \\ &\left[\mathbf{w}\mathbf{w}^H \right]_{i,i} \left[\mathbf{T} \right]_{i,i} \le P_i \end{aligned} \tag{17}$$

where $\bar{\mathbf{e}}_{rd} = \left(\bar{e}_{rd,1}, \cdots, \bar{e}_{rd,1} \right)^T$, $SINR_{LIE} = \dfrac{P \left(\sum_{i=1}^{n} \left(\bar{h}_{rd,i} + \bar{e}_{rd,i} \right) h_{sr,i} w_i \right)^2}{\sigma_r^2 \sum_{i=1}^{n} \left(\bar{h}_{rd,i} + \bar{e}_{rd,i} \right) \left(w_i \right)^2 + P_{an} \sum_{i=1}^{n} \left(\bar{e}_{rd,i} \right)^2 + \sigma_d^2}$.

The proof of Lemma 1 is given in Appendix A.

4.2 An Upper Bound of (14)

Using the Csuchy-Schwarz inequality and the triangle inequality, we can obtain (18) and (19).

$$\left| \sum_{i=1}^{n} \left(\hat{h}_{rd,i} + e_{rd,i} \right) h_{sr,i} w_i \right| \ge \left| \sum_{i=1}^{n} \hat{h}_{rd,i} h_{sr,i} w_i \right| - \sqrt{n\rho^2} \left| \sum_{i=1}^{n} h_{sr,i} w_i \right| , \tag{18}$$

$$\begin{aligned} &\sigma_r^2 \sum_{i=1}^{n} \left| \hat{h}_{rd,i} + e_{rd,i} \right|^2 \left| w_i \right|^2 + P_{an} \left\| \mathbf{e}_{rd} \right\|^2 + \sigma_d^2 \le \\ &\sigma_r^2 \sum_{i=1}^{n} \left| \hat{h}_{rd,i} \right|^2 \left| w_i \right|^2 + \left(2\sqrt{n\rho^2} \left\| \hat{\mathbf{h}}_{rd} \right\| + \sigma_r^2 n\rho^2 \right) \sum_{i=1}^{n} \left| w_i \right|^2 + P_{an} n\rho^2 + \sigma_d^2 \end{aligned} . \tag{19}$$

So we can obtain a lower bound of $SINR_{LI}$, which is given by $SINR_{LI}^{l}$ in (20).

$$SINR_{LI}^{l}=\frac{\left|\sum_{i=1}^{n}\hat{h}_{rd,i}h_{sr,i}w_i\right|-\sqrt{n\rho^2}\left|\sum_{i=1}^{n}h_{sr,i}w_i\right|}{\sigma_r^2\sum_{i=1}^{n}\left|\hat{h}_{rd,i}\right|^2\left|w_i\right|^2+\left(2\sqrt{n\rho^2}\left\|\hat{\mathbf{h}}_{rd}\right\|+\sigma_r^2n\rho^2\right)\sum_{i=1}^{n}\left|w_i\right|^2+P_{an}n\rho^2+\sigma_d^2}. \quad (20)$$

An upper bound of (14) can be obtained by solving the following problem.

$$\begin{aligned}&\min_{\mathbf{w}}\ \mathbf{w}^H\mathbf{T}\mathbf{w}\\&s.t.SINR_{LI}^{l}\geq\lambda\\&\left[\mathbf{w}\mathbf{w}^H\right]_{i,i}\left[\mathbf{T}\right]_{i,i}\leq P_i\end{aligned}. \quad (21)$$

From [17], we know that the problem in (21) can be transformed into an SOCP problem which can be solved optimally. This method is straightforward but the lower bound $SINR_{LI}^{l}$ is too loose to obtain a reasonable solution.

4.3 Robust Beamforming Design

The lower bound is not available in general, so we propose a robust beamforming scheme to obtain the beamforming weight vector.

Using the fact $\left\|\mathbf{e}_{rd}\right\|^2\leq n\rho^2$, we can obtain

$$SINR_{LI}\geq SINR_l\ , \quad (22)$$

where $SINR_l=\dfrac{P\left|\sum_{i=1}^{n}\left(\hat{h}_{rd,i}+e_{rd,i}\right)h_{sr,i}w_i\right|^2}{\sigma_r^2\sum_{i=1}^{n}\left|\hat{h}_{rd,i}+\bar{e}_{rd,i}\right|^2\left|w_i\right|^2+P_{an}n\rho^2+\sigma_d^2}$.

We can reformulate the problem in (14) as

$$\begin{aligned}&\min_{\mathbf{w}}\ \mathbf{w}^H\mathbf{T}\mathbf{w}\\&s.t.\min_{\mathbf{e}_{rd}}SINR_l\geq\lambda\\&\left[\mathbf{w}\mathbf{w}^H\right]_{i,i}\left[\mathbf{T}\right]_{i,i}\leq P_i\end{aligned}. \quad (23)$$

The worst-case SINR constraint in (23) can be reformulated as

$$\left(\hat{\mathbf{h}}_{rd}+\mathbf{e}_{rd}\right)^H\mathbf{Q}\left(\hat{\mathbf{h}}_{rd}+\mathbf{e}_{rd}\right)\geq u,\forall\left\|\mathbf{e}_{rd}\right\|\leq\rho, \quad (24)$$

where $\mathbf{Q}=P\mathbf{R}_{sr}\mathbf{w}\mathbf{w}^H-\lambda\sigma_r^2\mathbf{w}\mathbf{w}^H\ u=n\lambda\rho^2\left(P_{\max}-\mathbf{w}^H\mathbf{T}\mathbf{w}\right)+\lambda\sigma_d^2$.

Using S-Procedure [27] which is given in Appendix B, the problem in (24) can be equivalently rewritten as (25).

$$\mathbf{T}\left(\mathbf{Q},\beta,u\right)=\begin{pmatrix}\beta\mathbf{I}+\mathbf{Q} & \mathbf{Q}\hat{\mathbf{h}}_{rd}\\ \hat{\mathbf{h}}_{rd}^H\mathbf{Q} & \hat{\mathbf{h}}_{rd}^H\mathbf{Q}\hat{\mathbf{h}}_{rd}-u-\beta\rho^2\end{pmatrix}\geq 0\ ,\ \exists\beta\geq 0\ , \quad (25)$$

By applying the fact $tr\left(\mathbf{AB}\right)=tr\left(\mathbf{BA}\right)$ and the problem in (23) is reformulated as

$$\begin{aligned} &\min_{\mathbf{W}_r \succeq 0, \beta \geq 0} tr\left(\mathbf{T}\mathbf{W}_r\right) \\ &s.t. \mathbf{T}\left(\mathbf{Q}, \beta, u\right) \succeq 0 \\ &\left[\mathbf{W}_r\right]_{i,i}\left[\mathbf{T}\right]_{i,i} \leq P_i \\ &rank\left(\mathbf{W}_r\right) = 1 \end{aligned}, \tag{26}$$

where $\mathbf{W}_r = \mathbf{w}\mathbf{w}^H$.

The difficult constraint in (26) is the rank constraint $rank\left(\mathbf{W}_r\right) = 1$ which is nonconvex. Thus, we may drop it to obtain the following relaxed version of (26).

$$\begin{aligned} &\min_{\mathbf{W}_r \succeq 0, \beta \geq 0} tr\left(\mathbf{T}\mathbf{W}_r\right) \\ &s.t. \mathbf{T}\left(\mathbf{Q}, \beta, u\right) \succeq 0 \\ &\left[\mathbf{W}_r\right]_{i,i}\left[\mathbf{T}\right]_{i,i} \leq P_i \end{aligned}. \tag{27}$$

The problem in (27) is a semidefinite programming (SDP) problem which is convex and can be optimally solved using interior methods. The problem in (27) has $n+1$ constraints and the dimension of $\mathbf{W}_r$ is $n \times n$, so the complexity to solve it is at least $O\left((n+1)^4 n^{\frac{1}{2}} \log\frac{1}{\varepsilon}\right)$ [27], where ε is a solution accuracy.

The important question is whether the solution to the problem in (27) is of rank one. If $\mathbf{W}_r$ is rank one, then we can obtain $\mathbf{w}^{opt}$ by using standard matrix decomposition and this solution is globally optimal. If it is not rank one, a randomization method in Table I can be applied to convert a global optimal solution $\mathbf{W}_r$ to (27) into a feasible solution $\mathbf{w}$ to (23). Different randomization methods have been researched in the literature [28]-[30]. The one we choose is Table I. If the feasible solution $\mathbf{w}$ does not subject to some constraints in (23), we can map it to a "nearby" feasible solution of (23) [28].

Table 1. Randomization Technique for Semidefinite Relaxation Approach

1) Apply the eigenvalue decomposition to $\mathbf{W}$ as $\mathbf{W}_r = \mathbf{U}\mathbf{\Sigma}\mathbf{U}^H$.
2) Choose an random vector $\mathbf{v} \in C^{n\times 1}$ where $\left[\mathbf{v}\right]_i = e^{j\theta_i}, i = 1, \cdots, n$ is achieved and θ_i is independent and uniformly distributed on $\left[0, 2\pi\right)$.
3) Choose $\mathbf{w} = \mathbf{U}\mathbf{\Sigma}^{1/2}\mathbf{v}$ which ensures that $\mathbf{w}^H\mathbf{w} = tr\left(\mathbf{W}_r\right)$.

After $\mathbf{w}$ is obtained, the transmit power of the each relay for the information-bearing signals can be given by $P_{s,i} = \left[\mathbf{w}\mathbf{w}^H\right]_{i,i}\left[\mathbf{T}\right]_{i,i}$, and AN consumes the remaining power. The transmit power of AN can be given by $P_{an} = E\left(\mathbf{n}_{an}^H\mathbf{n}_{an}\right) = \sum_{j=1}^{n-1}\sigma_{a,j}^2$.

We can get $\sigma_{a,j}^2$ by solving the following optimization problem.

$$\begin{aligned} &\max \sum_{j=1}^{n-1} \sigma_{a,j}^2 \\ &s.t. E\left|\left[n_{an}\right]_{i,1}\right|^2 \le P_i - P_{s,i}, i = 1, \cdots, n \end{aligned}, \tag{28}$$

where $E\left|\left[n_{an}\right]_{i,1}\right|^2 = \sum_{j=1}^{n-1} \left|\pi_{i,j}\right|^2 \sigma_{a,j}^2$.

We define $\theta_j = \sigma_{a,j}^2$, $j = 1, \cdots, n-1$, the problem in (28) is rewritten as

$$\begin{aligned} &\max \sum_{j=1}^{n-1} \theta_j \\ &s.t. \sum_{j=1}^{n-1} \left|\pi_{i,j}\right|^2 \theta_j \le P_i - P_{s,i}, i = 1, \cdots, n \end{aligned}, \tag{29}$$

Obviously, the problem in (29) is a linear programming problem which is convex, thus it can be easily solved to obtain the optimal solution [31].

5. SIMULATION RESULTS

In this section, we present simulation results to analyze the performance of the robust beamforming design for the cooperative wireless relay networks aiming to enhance secrecy transmission at the physical layer. We evaluate the performance of the proposed schemes in the Rayleigh flat-fading channels. In all simulations, we assume that the channel coefficients consist of complex zero-mean Gaussian random vectors with unit variance. For simplicity, we assume that all the noise power is the same for both the destination and the eavesdropper: $\sigma_r^2 = \sigma_d^2 = \sigma_e^2 = 1$. To analyze the performance, we assume that the power constraint of the each relay $P_i, i = 1, \cdots, n$ is equal. We set the number of the relays $n = 3$. We assume that the CSI errors are uniformly distributed in S. To evaluate the performance of the proposed system design, we perform 1000 independent trails to get the average results. Four schemes are provided in simulation results: a) the proposed robust beamforming design in Section IV-C, b) the lower bound in Section IV-A, c) the upper bound in Section IV-B, d) the naive scheme in which the estimated CSI is treated as the perfect channels, e) the scheme with perfect CSI proposed by [17] .

Fig. 2 provides the expected transmit power for information-bearing signals results for different desired SINRs with the CSI error bound $\rho^2 = 0.01$. In the figure, a) is labled as "Proposed design" , b) is labled as "Lower bound" and c) is labled as "Upper bound". The results show the proposed robust beamforming design achieves nearly the same expected transmit power for information-bearing signals as the lower bound. The difference between the proposed robust beamforming design and the lower is less than 1 dB. It is because that the lower is not achievable.

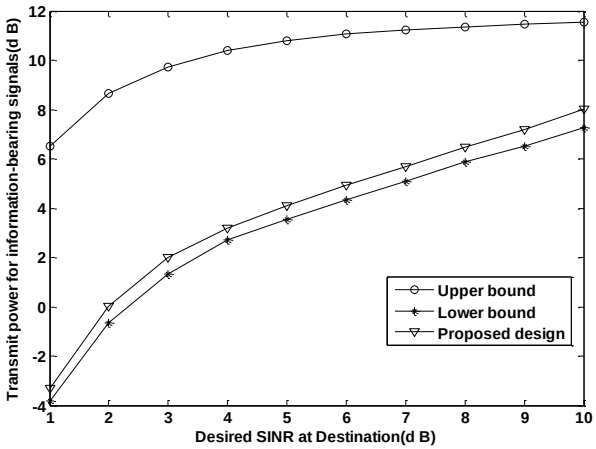


Fig. 2. Transmit power for information-bearing signals versus desired SINR at the destination

Fig. 3 shows the expected transmit power for information-bearing signals results for different number of relays with the CSI error bound $\rho^2 = 0.01$ using the methods a) b) and c). The curves show the proposed design achieves nearly the same expected transmit power for information-bearing signals as the lower bound. The results also show that the transmitted power decreases as the number of relays increases. This is because that the more relay nodes provide the power gain. Though the transmit power can be saved by increasing the number of relays, the complexity and the weight of will increase as the number of relays increases. Therefore, the optimal number of relays should be balanced by taking into account all these views.

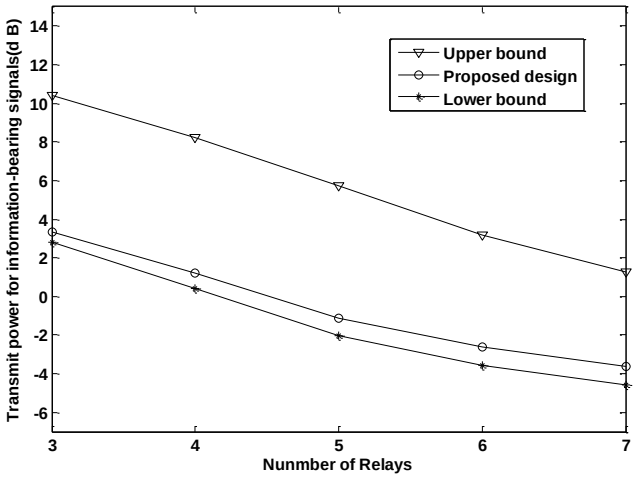


Fig. 3. Transmit power for information-bearing signals versus the number of relays

In **Fig. 4**, the curves show that the values of the received worst-case SINR in the legitimate link and in the wiretap link versus the SINR requirement on desired destination with the CSI error bound $\rho^2 = 0.01$. In the figure, the methods a), d) and e) are respectively labeled as "robust", "naive" and "perfect". The receiving destination is labled as "Destination" and the eavesdropper is labled as "Eve". In "naive" scheme, the knowledge of CSI errors is not used and the estimated CSI is treated as the perfect channels. We notice that even if the channels are perturbed small, the SINR for the legitimate user is greatly degraded in the "naive" scheme. In contrast, the legitimate user can achieve the SINR requirements and the received SINR at the eavesdropper is degraded in the "robust" scheme. We also notice that the SINR of the eavesdropper in the "robust" scheme is lower than that in the "perfect" scheme. It is because that the transmit power for information-bearing signal is increased because of interference caused by the imperfect CSI, which results in the remaining power used for the AN reducing. It is shown that the received SINR at the eavesdropper increases with desired SINR at the destination increasing. It is understanding because the transmit power used for the AN decreases.

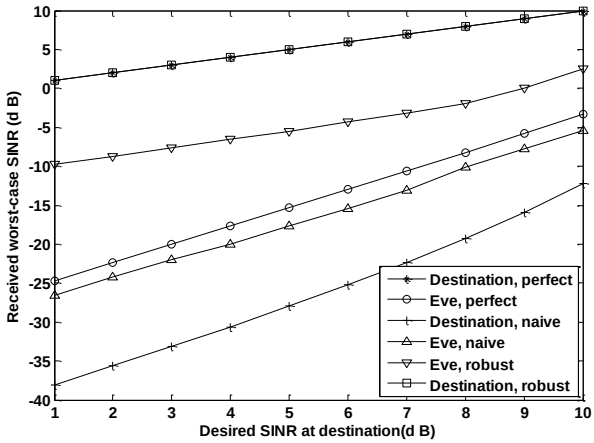


Fig. 4. Received worst-case SINR versus desired SINR at destination

Fig. 5 shows the secrecy capacity for the different received SINR targets at the destination under the condition of perfect and imperfect CSI with the CSI error bound $\rho^2 = 0.01$. In the figure, the methods a), d) and e) are respectively labeled as "robust", "naive" and "perfect". The case where CSI is perfect is shown, obviously the best secrecy capacity is obtained. When CSI is perfect, the AN can be made invisible to the desired destination while degrading the potential eavesdropper's channel. We also notice that the "robust" scheme provide nonzero secrecy capacity for all the desired SINRs. In the "naive" scheme, the secrecy capacity is reduced to zero due to that the received SINR at tha eavesdropper is always greater than that at the destination. Obviously, the robust beamforming scheme can recover a fraction of the SINR lost.

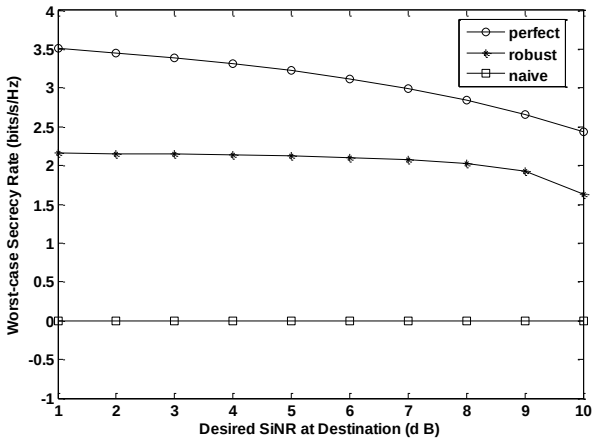


Fig. 5. Secrecy rate versus desired SINR

In **Fig. 6**, the impact of the magnitude of the CSI error bound on SINR performance in the robust beamforming scheme is illustrated. In the figure, the method a) is labeled as "robust". The receiving destination is labled as "Destination" and the eavesdropper is labled as "Eve". We notice that the destination can achieve the desired received SINR. It is also shown that the received SINR at the eavesdropper increases with the CSI error bound increasing and the gap between the destination and the eavesdropper in the robust scheme decreases.

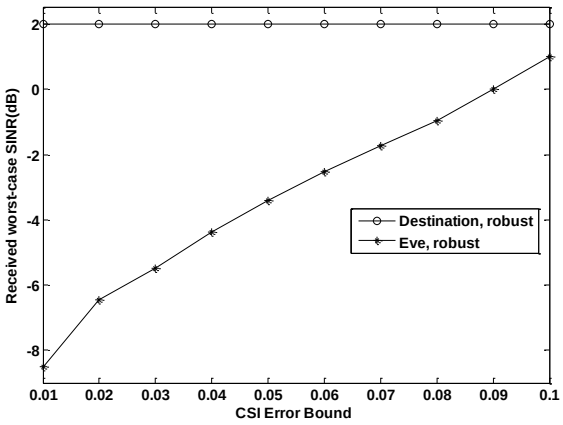


Fig. 6. Received worst-case SINR for destination and eavesdropper versus CSI error bound ρ^2

The expected transmit power for information-bearing signals results against the CSI error bound, ρ^2, are provided in **Fig. 7**. Results reveal that as expected, the transmit power for information-bearing signals increases as the error bound increases.

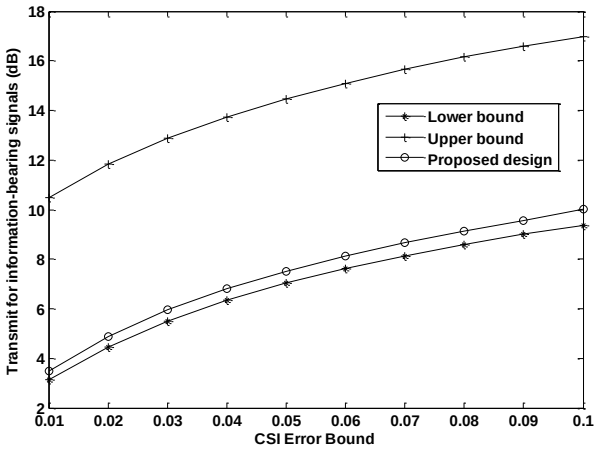


Fig. 7. Transmit power for information-bearing signals versus CSI error bound ρ^2

6. CONCLUSIONS

The security transmission scheme is presented for the cooperative wireless relay networks in the presence of a passive eavesdropper. Placing the highest emphasis on fairness, the robust cooperative relay beamforming for physical layer security is designed to maximize the transmit power of the AN to confuse the passive eavesdropper, while achieving worst-case SINR constraint at the legitimate user and the power constraint of each relay node. This problem can be solved by using S-Procedure and rank relaxation techniques. Simulation results show that the uncertainty of the CSI can greatly affect the SINR at the legitimate user. The robust beamforming scheme proposed by the paper can recover a fraction of the SINR lost in the perfect CSI.

APPENDIX A

Firstly, we proof the problem in (17) can be solved optimally. The constraint in (17) can be reformulate as

$$\min_{\bar{\mathbf{e}}_{rd}\in Z_R} \bar{f}\left(\bar{\mathbf{e}}_{rd}\right) \le 0 \tag{30}$$

where

$$f\left(\bar{\mathbf{e}}_{rd}\right) \overset{\Delta}{=} -\sqrt{P}\sum_{i=1}^{n}\left(\bar{h}_{rd,i}+\bar{e}_{rd,i}\right)h_{sr,i}w_i + \sqrt{\lambda\left(\sigma_r^2\sum_{i=1}^{n}\left(\bar{h}_{rd,i}+\bar{e}_{rd,i}\right)^2\left|w_i\right|^2 + P_{an}\sum_{i=1}^{n}\left(\bar{e}_{rd,i}\right)^2\left|w_i\right|^2+\sigma_d^2\right)}.$$

We know $f\left(\bar{\mathbf{e}}_{rd}\right)$ is convex in $\bar{\mathbf{e}}_{rd}$. Its maximum value can be obtained in the vertices [27]. When $\bar{\mathbf{e}}_{rd}$ is fixed, the problem in (17) is an SOCP problem which is convex. Therefore, we can obtain the optimum solution by solving an SOCP problem for each vertex. The region Z_R

has $2n$ vertices. Therefore, the optimum solution of (17) can be obtained by enumerating Z_R has $2n$ constraints. The complexity is at least $\mathrm{O}\left(2^n\right)$.

In the following, we proof that the solution of the problem in (17) is a lower bound of (14). $Z_R = \left\{\mathbf{e}_{rd} \in R^{n\times 1} : \left|e_{rd,i}\right| \le \rho, \rho > 0, \forall i\right\}$ is a subset of S, so the worst-case SINR in the region Z_R is better than that in the region S. Therefore, we can obtain a lower bound by solving (17).

APPENDIX B

In this appendix, we provide S-procedure for real and complex cases.[27]

Lambda 2: Let symmetric matrices $\mathbf{A}_1, \mathbf{A}_2 \in R^{n\times n}$, vectors $\mathbf{b}_1, \mathbf{b}_2 \in R^{n\times 1}$ and numbers $c_1, c_2 \in R$. For $\mathbf{x} \in R^{n\times 1}$, we define the functions

$$f_1(\mathbf{x}) = \mathbf{x}^T \mathbf{A}_1 \mathbf{x} + 2\mathbf{b}_1^T \mathbf{x} + c_1$$
$$f_2(\mathbf{x}) = \mathbf{x}^T \mathbf{A}_2 \mathbf{x} + 2\mathbf{b}_2^T \mathbf{x} + c_2$$

If there exists a vector $\mathbf{x} \in R^{n\times 1}$ such that $f_2(\mathbf{x}) > 0$, then the following two conditions are equivalent:

1) $f_1(\mathbf{x}) > 0$ for every $\mathbf{x} \in R^{n\times 1}$ such that $f_2(\mathbf{x}) > 0$;

2) there exists $\lambda \ge 0$ such that

$$\begin{pmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^T & c_1 \end{pmatrix} \succ \lambda \begin{pmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^T & c_2 \end{pmatrix}$$

Lambda 3: Let hermitian matrices $\mathbf{A}_0, \mathbf{A}_1, \mathbf{A}_2 \in C^{n\times n}$, vectors $\mathbf{b}_0, \mathbf{b}_1, \mathbf{b}_2 \in C^{n\times 1}$ and numbers $c_0, c_1, c_2 \in C$. For $\mathbf{x} \in C^{n\times 1}$, we define the functions

$$f_0(\mathbf{x}) = \mathbf{x}^h \mathbf{A}_0 \mathbf{x} + 2\mathbf{b}_0^H \mathbf{x} + c_0$$
$$f_1(\mathbf{x}) = \mathbf{x}^H \mathbf{A}_1 \mathbf{x} + 2\mathbf{b}_1^H \mathbf{x} + c_1$$
$$f_2(\mathbf{x}) = \mathbf{x}^H \mathbf{A}_2 \mathbf{x} + 2\mathbf{b}_2^H \mathbf{x} + c_2$$

If there exists a vector $\mathbf{x} \in C^{n\times 1}$ such that $f_1(\mathbf{x}), f_2(\mathbf{x}) > 0$, then the following two conditions are equivalent:

1) $f_0(\mathbf{x}) > 0$ for every $\mathbf{x} \in C^{n\times 1}$ such that $f_1(\mathbf{x}) > 0$ and $f_2(\mathbf{x}) > 0$;

2) there exists $\lambda_1, \lambda_2 \ge 0$ such that

$$\begin{pmatrix} \mathbf{A}_0 & \mathbf{b}_0 \\ \mathbf{b}_0^H & c_0 \end{pmatrix} \succ \lambda_1 \begin{pmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{pmatrix} + \lambda_2 \begin{pmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{pmatrix}$$

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, et al., "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008. Article (CrossRef Link)

[2] Y. Liang, H. V. Poor and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2491, June 2008. Article (CrossRef Link)

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

[4] T. Liu and S. Shamai, "A note on secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553, 2009. Article (CrossRef Link)

[5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, 2010. Article (CrossRef Link)

[6] A. Wyner. "The wire-tap channel," *Bell. Syst Tech. J*, vol.54, no.8, pp.1355-1387, Jan 1975. Article (CrossRef Link)

[7] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003-5011, Oct. 2009. Article (CrossRef Link)

[8] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317-1322, Mar. 2011. Article (CrossRef Link)

[9] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011. Article (CrossRef Link)

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

[11] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54 no. 6, pp. 2735-2751, June 2008. Article (CrossRef Link)

[12] L. Dong, Z. Han, A. P. Petropulu, et al. "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 50, no. 3, pp. 1875-1888, Mar. 2010. Article (CrossRef Link)

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

[14] A. Khisti, "Algorithms and architectures for multiuser, multi-terminal, and multilayer information-theoretic security," *Ph.D. dissertation*, MIT, 2008.

[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008. Article (CrossRef Link)

[16] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, Jan. 2011. Article (CrossRef Link)

[17] H. M. Wang, M. Luo and 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. Letters*, vol. 20, no. 1, pp. 39-42, Jan. 2013. Article (CrossRef Link)

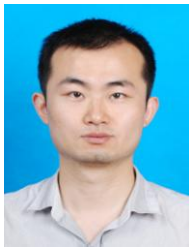
[18] H. Wang, M. Luo, Q. Yin, etc., "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Information Forensics and Security*, vol. 8, no.8, pp. 2007-2020, Oct. 2013. Article (CrossRef Link)

[19] C. Wang, H. Wang, X. Xia. "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no.2, pp. 589-605, Sep. 2014. Article (CrossRef Link)

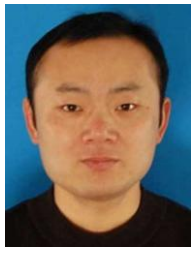
[20] C. Wang and H. Wang, "Robust Joint Beamforming and Jamming for secure AF networks: low-complexity design," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 2192-2198, May, 2015. Article (CrossRef Link)
[21] X. Gong, H. Long etc, "Robust AF Relay Beamforming for Security with MSE Constraint," accepted by *IET Commun.*.
[22] Y. Zou, X. Wang, W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks," *IEEE J. Sel. Topics Commun.*, vol. 31, no. 10, Oct. 2013. Article(CrossRef Link)
[23] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009. Article (CrossRef Link)
[24] M. Pei, J. Wei, K.-K. Wong and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3025-3029, Sep. 2012. Article (CrossRef Link)
[25] M. Shenouda and T. Davidson, "Convex conic formulations of robust downlink precoder designs with quality of service constraints," *IEEE J. Sel. Topics Signal Process*, vol. 1, no. 4, pp. 714¨C724, Dec. 2007. Article(CrossRef Link)
[26] A. Pascual-Iserte, D. Palomar, A. Perez-Neira, and M. Lagunas, "A robust maximin approach for MIMO communications with imperfect channel state information based on convex optimization," *IEEE Trans. Signal Process.*, vol. 54, no. 1, pp. 346¨C360, Jan. 2006. Article(CrossRef Link)
[27] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge University Press, 2004. Article (CrossRef Link)
[28] Z. Q. Luo, W. K. Ma, A. C. So, Y. Ye and S. Zhang, "Semidefinite relaxation of quadratic optimization problems: from its practical deployments and scope of applicability to key theoretical results," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20-34, May 2010. Article (CrossRef Link)
[29] N. D. Sidiropoulos, T. N. Davidson and Z. Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 3, pp. 2239-2251, June 2006. Article (CrossRef Link)
[30] S. Zhang, "Quadratic maximization and semidefinite relaxation," *Math. Program.*, ser. A, vol. 87, pp. 453-465, 2000. Article (CrossRef Link)
[31] D. G. Luenberger and Y. Ye, *Linear and nonlinear programming*. Springer, 2006.

Xiangwu Gong received his B.S. degree from School of Mathematics, Shandong University, China in 2009. He received his M.S. degree from School of Science, PLA University of Science and Technology, Nanjing, China in 2012. He is currently pursuing his Ph.D degree in College of Communication Engineering, PLA University of Science and Technology. His current research interests include wireless communication and physical layer security.

Feihong Dong received the B.E. degree in information system engineering from PLA University of Science and Technology, Nanjing, China in 2010. He is currently working toward the Ph.D. degree with the College of Communications Engineering, PLA University of Science and Technology. His research interests include high altitude platform communication networks, satellite communication networks and space information networks.



Hongjun Li received his B.S. degree and M.S. degree from College of Communication Engineering, PLA University of Science and Technology, Nanjing, China in 2008 and 2013 respectively. He is currently pursuing his Ph.D degree in College of Communication Engineering, PLA University of Science and Technology. His current research interests include wireless communication, satellite communication and spatial information network.



Wei Shao received the B.Sc, M.Sc and Ph.D. degrees from the College of Communication Engineering, PLAUST, Nanjing, China, in 2001, 2004, and 2007 respectively. He currently holds a position as an associate professor at the College of Communication Engineering, PLAUST. His research interests mainly include signal processing and wireless communication.