JOINT TRANSCEIVER DESIGNS FOR SECURE COMMUNICATIONS OVER MIMO RELAY

Yuan Gao *1, Yunlong Cai *2, Qingjiang Shi †3, Benoit Champagne ‡4, and Minjian Zhao *5

* Department of ISEE, Zhejiang University, Hangzhou, China

† School of Information and Science Technology, Zhejiang Sci-Tech University, Hangzhou, China

‡ Department of Electrical and Computer Engineering, McGill University, Montreal, Quebec, Canada

1 gaoyuan19930415@zju.edu.cn, 2 ylcai@zju.edu.cn, 3 qing.j.shi@gmail.com, 4 benoit.champagne@mcgill.ca, 5 mjzhao@zju.edu.cn

ABSTRACT

This paper addresses the transceiver design problem for secure downlink communications over a multiple-input multiple-output (MIMO) relay system in the presence of multiple eavesdroppers. A new algorithm based on alternating optimization (AO) is first proposed to maximize the signal-to-noise ratio (SNR) of a legitimate receiver under power constraints at the base station (BS) and the relay station (RS) and a set of secrecy constraints, by using the semidefinite relaxation (SDR) technique. To reduce complexity, a simplified design algorithm based on switched relaying (SR) is also proposed, in which both the BS and the RS are equipped with a codebook of permutation matrices. Based on this codebook, we construct a number of latent transceivers, each consisting of a BS beamforming vector and an optimally scaled RS permutation matrix. We use the bisection search and second-order cone programming (SOCP) techniques to design each latent transceiver and choose the optimal one with the largest SNR. We also develop an efficient approach to construct the codebook of permutation matrices. Our results show that the SR based algorithm significantly reduces the computational complexity while maintaining a similar performance to the AO based algorithm.[1]

Index Terms— Beamforming, switched relaying, physical layer security.

1. INTRODUCTION

As a complement to traditional encryption, physical layer security [1] - [5], which exploits signal processing techniques to ensure secure communication has become an active research area. In recent years, especially, physical layer security techniques that can enhance security in communications over MIMO relay systems have attracted considerable interest [6] - [11]. Hong *et al.* [6] mentioned two different secrecy applications of the MIMO relays, namely: i) secrecy beamforming and precoding with trusted and untrusted relays, and ii) a secure communication system with relays as cooperative jammers. Mukherjee *et al.* [7] enriched Hong's theory and divided security issues in relay networks into two broad categories. For specific problems of secure communications over a MIMO relay, Ding *et al.* combined interference alignment with cooperative jamming in order to ensure secure transmission to the legitimate receiver in the presence of an eavesdropper in [8]. A generalized singular value decomposition (GSVD) method is used by Huang *et al.* in [9] to propose a cooperative jamming (CJ) scheme for secure communications with MIMO relays. Both works [8] and [9] considered only one eavesdropper in the communication network, which is overly restrictive. By considering the case of multiple eavesdroppers, Zhang *et al.* exploited the beamforming and jamming technique to maximize the worst-case secrecy rate in [10] while Yang *et al.* optimized the relay matrix to maximize the received SNR at the destination under a set of secrecy constraints in [11]. All the mentioned studies optimize the beamforming vector and the relay matrix separately without considering the possibility of joint design.

In this paper, we jointly optimize the BS beamforming vector and the RS AF transformation matrix in order to maximize the SNR of a legitimate receiver in the presence of multiple eavesdroppers, under power constraints at the BS and the RS and a set of secrecy constraints. We firstly propose a new algorithm based on alternating optimization (AO) and using the celebrated SDR [15] technique to solve this physical layer security problem. To reduce complexity as well as the signaling overhead, a simplified algorithm based on switched relaying [16] is also proposed to solve this problem. In the SR scheme, we assume that the proposed joint design algorithm is implemented at the BS[2]. The BS and the RS are both equipped with a finite codebook of permutation matrices. The BS creates a number of latent transceivers based on all the elements within the codebook and determines the optimal latent transceiver as the one with the largest SNR before data transmission. An efficient approach to construct the codebook of permutation matrices is also developed in the paper. Finally, the simulation results show that the SR based algorithm significantly reduces the computational complexity while maintaining a similar performance when compared to the AO based design.

2. SYSTEM MODEL AND PROBLEM STATEMENT

Let us consider a MIMO relay system as depicted in Fig. 1 which consists of one BS, one RS, and one legitimate receiver denoted as node D, which is overheard by K eavesdroppers. Each eavesdropper is assigned a unique index $k \in \mathcal{K} \triangleq \{1, 2, \cdots, K\}$ and denoted as E_k. D and $E_k, \forall k \in \mathcal{K}$ are equipped with single antenna, while the BS and the RS are equipped with N_t and N_r antennas, respectively. We assume that no direct link between the BS and the node D is available due to severe attenuation.

In the first phase, the received vector at the RS is given by

$$\mathbf{r}_R = \mathbf{H}_1 \mathbf{p} b + \mathbf{n}_1, \qquad (1)$$

[1]This work was supported in part by the National Natural Science Foundation of China under Grants 61471319 and 61302076, Zhejiang Provincial Natural Science Foundation of China under Grant LY14F010013, and the National High Technology Research and Development Program (863 Program) of China under Grant 2014AA01A707.

[2]In cellular systems, it is preferable to implement most of the signal processing operations at the BS rather than the RS, due to the fact that the BS is more powerful while the RS is expected to have a simple structure and low energy consumption [12] - [14].

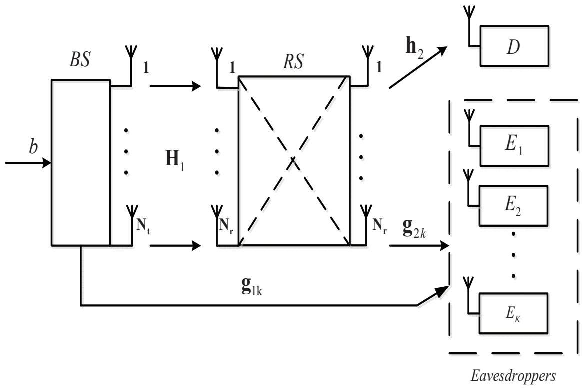

Fig. 1. MIMO relay systems in the presence of multiple eavesdroppers

where b denotes the transmit information symbol at a given time instant, modeled as a zero-mean Gaussian random variable with variance $E\{|b|^2\} = 1$. $\mathbf{p}\in\mathbb{C}^{N_t\times 1}$ denotes the BS beamforming vector and $\mathbf{H}_1\in\mathbb{C}^{N_r\times N_t}$ is the channel matrix between the BS and the RS, whose elements are independent and identically distributed (i.i.d.) complex circular Gaussian variables with zero mean and unit variance, which we indicate by the standard notation $\mathcal{CN}(0,1)$, and $\mathbf{n}_1\in\mathbb{C}^{N_r\times 1}$ is the additive zero-mean complex Gaussian noise with covariance matrix $E[\mathbf{n}_1\mathbf{n}_1^H] = \sigma_1^2\mathbf{I}$, where σ_1^2 denotes the noise variance in the first phase (from BS to RS).

In the second phase (from RS to D), the vector $\mathbf{r}_R\in\mathbb{C}^{N_r\times 1}$ is operated by the RS AF transformation matrix $\mathbf{W}\in\mathbb{C}^{N_r\times N_r}$. The forwarded signal vector from the RS is given by
-3mm
$$\mathbf{x}_R = \mathbf{W}(\mathbf{H}_1\mathbf{p}b + \mathbf{n}_1). \tag{2}$$

For the second phase, the received signal at the legitimate receiver is given by
$$y_D = \mathbf{h}_2^H\mathbf{x}_R + n_2 = \mathbf{h}_2^H\mathbf{W}(\mathbf{H}_1\mathbf{p}b + \mathbf{n}_1) + n_2, \tag{3}$$
where $\mathbf{h}_2\in\mathbb{C}^{N_r\times 1}$ is the channel vector between the RS and the legitimate receiver, whose entries are i.i.d. zero mean complex circular Gaussian variables with unit variance, and n_2 denotes the additive zero mean complex Gaussian noise in the second phase, where $E[|n_2|^2] = \sigma_2^2$ denotes the second phase noise variance.

The transmit power of the BS in the first phase and that of the RS in the second phase are given by $P_B = E[\|\mathbf{p}b\|^2] = \mathrm{Tr}\{\mathbf{p}\mathbf{p}^H\}$ and
$$P_R = E[\|\mathbf{x}_R\|^2] = E[\mathrm{Tr}\{\mathbf{W}\mathbf{H}_1\mathbf{p}\mathbf{p}^H\mathbf{H}_1^H\mathbf{W}^2 + \sigma_1^2\mathbf{W}\mathbf{W}^H\}], \tag{4}$$
respectively.

We adopt, as a metric of transmission reliability, the received signal-to-noise ratio (SNR) at the legitimate receiver, which is given by
$$\mathrm{SNR}_D = \frac{|\mathbf{h}_2^H\mathbf{W}\mathbf{H}_1\mathbf{p}|^2}{\sigma_1^2\|\mathbf{h}_2^H\mathbf{W}\|^2 + \sigma_2^2}. \tag{5}$$

During the transmission, $E_k, \forall k\in\mathcal{K}$ can overhear signals from both the BS and the RS. Let $\mathbf{g}_{1k}\in\mathbb{C}^{N_t\times 1}$ and $\mathbf{g}_{2k}\in\mathbb{C}^{N_r\times 1}$, respectively denote the complex conjugate BS-E_k and RS-E_k channels. The signals overheard by E_k, respectively from the BS and the RS are given by
$$\begin{aligned} y_{1k} &= \mathbf{g}_{1k}^H\mathbf{p}b + n_{1k}, \\ y_{2k} &= \mathbf{g}_{2k}^H\mathbf{x}_R + n_{2k} = \mathbf{g}_{2k}^H\mathbf{W}(\mathbf{H}_1\mathbf{p}b + \mathbf{n}_1) + n_{2k}, \end{aligned} \tag{6}$$
where n_{1k} and n_{2k} denote complex circular Gaussian additive noise terms with zero mean and variances σ_{1k}^2 and σ_{2k}^2, respectively. It is assumed that for each transmission phase, each E_k adopts the selection diversity combining scheme[3].

We aim to design the BS beamforming vector $\mathbf{p}$ and the RS AF transformation matrix $\mathbf{W}$ jointly, in order to maximize the SNR achieved by the legitimate receiver under the BS and the RS power constraints, while keeping the SNR of eavesdroppers below a certain threshold γ. The optimization problem is given by
$$\begin{aligned} \max_{\mathbf{p},\mathbf{W}} \quad & \mathrm{SNR}_D \\ \text{s.t.} \quad & P_B \le P_t,\ P_R \le P_r, \\ & \frac{|\mathbf{g}_{1k}^H\mathbf{p}|^2}{\sigma_{1k}^2} \le \gamma,\ \frac{|\mathbf{g}_{2k}^H\mathbf{W}\mathbf{H}_1\mathbf{p}|^2}{\sigma_1^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2 + \sigma_{2k}^2} \le \gamma,\ \forall k\in\mathcal{K}. \end{aligned} \tag{7}$$

3. PROPOSED AO BASED TRANSCEIVER DESIGN

We first present the AO based transceiver design algorithm for the joint optimization of the BS beamforming vector and the RS AF transformation matrix. Let us consider the optimization of $\mathbf{p}$ while the RS AF transformation matrix $\mathbf{W}$ is fixed. We can see that the celebrated SDR technique can be applied to solve the resulting optimization problem by introducing a new variable $\mathbf{P} = \mathbf{p}\mathbf{p}^H$. Thus, problem (7) can be reformulated as the following problem by ignoring the rank-one constraints for $\mathbf{P}$:
$$\begin{aligned} \max_{\mathbf{P}} \quad & \frac{\mathbf{h}_2^H\mathbf{W}\mathbf{H}_1\mathbf{P}\mathbf{H}_1^H\mathbf{W}^H\mathbf{h}_2}{\sigma_1^2\|\mathbf{h}_2^H\mathbf{W}\|^2 + \sigma_2^2} \\ \text{s.t.} \quad & \mathrm{Tr}\{\mathbf{P}\} \le P_t, \\ & E[\mathrm{Tr}\{(\mathbf{W}\mathbf{H}_1\mathbf{P}\mathbf{H}_1^H\mathbf{W}^H) + \sigma_1^2(\mathbf{W}\mathbf{W}^H)\}] \le P_r, \\ & \frac{\mathbf{g}_{1k}^H\mathbf{P}\mathbf{g}_{1k}}{\sigma_{1k}^2} \le \gamma,\ \frac{\mathbf{g}_{2k}^H\mathbf{W}\mathbf{H}_1\mathbf{P}\mathbf{H}_1^H\mathbf{W}^H\mathbf{g}_{2k}}{\sigma_1^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2 + \sigma_{2k}^2} \le \gamma, \\ & \mathbf{P}\succeq\mathbf{0},\ \forall k\in\mathcal{K}. \end{aligned} \tag{8}$$
In this way, problem (7) is relaxed to a convex semidefinite program (SDP) [17], which can be efficiently solved by available software packages, e.g., SeDuMi [17].

Next, we consider the optimization of the RS AF transformation matrix $\mathbf{W}$ while assuming that $\mathbf{p}$ is fixed. Noting that $\mathbf{x}^T\mathbf{Y}\mathbf{z} = \mathrm{vec}(\mathbf{x}\mathbf{z}^T)^T\mathrm{vec}(\mathbf{Y})$, the numerator in (5) can be rewritten as
$$|\mathbf{h}_2^H\mathbf{W}\mathbf{H}_1\mathbf{p}|^2 = |\mathbf{u}^T\mathrm{vec}(\mathbf{W})|^2 = \mathbf{u}^T\tilde{\mathbf{W}}\mathrm{conj}(\mathbf{u}), \tag{9}$$
where $\mathbf{u} = \mathrm{vec}(\mathrm{conj}(\mathbf{h}_2)\mathbf{p}^T\mathbf{H}_1^T)$ and $\tilde{\mathbf{W}} = \mathrm{vec}(\mathbf{W})\mathrm{vec}(\mathbf{W})^H$. The operator $\mathrm{vec}(\cdot)$ stacks the elements of a matrix in one long column vector while $\mathrm{conj}(\cdot)$ denotes the conjugate of a certain matrix. Thus, the optimization objective can be reformulated as
$$\mathrm{SNR}_D = \frac{\mathbf{u}^T\tilde{\mathbf{W}}\mathrm{conj}(\mathbf{u})}{\sigma_1^2\sum_{j=1}^{N_t}\mathbf{h}_2^H\mathbf{E}_j\tilde{\mathbf{W}}\mathbf{E}_j^H\mathbf{h}_2 + \sigma_2^2}, \tag{10}$$
where $\mathbf{E}_k \in \{0,1\}^{N_r^2\times N_r^2}$ is a linear mapping matrix such that $\mathbf{h}_2^H\mathbf{E}_j\mathrm{vec}(\mathbf{W}) = \mathbf{h}_2^H\mathbf{W}(:,j)$, and $\mathbf{W}(:,j)$ denotes the jth column of $\mathbf{W}$. Similarly, the SNR constraints of the RS-E_k link can be reformulated as
$$\frac{\mathbf{v}_k^T\tilde{\mathbf{W}}\mathrm{conj}(\mathbf{v}_k)}{\sigma_1^2\sum_{j=1}^{N_t}\mathbf{g}_{2k}^H\mathbf{E}_j\tilde{\mathbf{W}}\mathbf{E}_j^H\mathbf{g}_{2k} + \sigma_{2k}^2} \le \gamma, \tag{11}$$

[3]In this paper, selection diversity combining is assumed at each E_k due to its operational simplicity. However, the proposed algorithm can be extended to other types of combiners, such as the optimal maximum ratio combiner.

Table 1. AO based transceiver design algorithm

1. Initialize $\mathbf{W}$ and define the tolerance of accuracy δ.
2. **Repeat**
   - Solve problem (8) with fixed $\mathbf{W}$ to obtain the updated $\mathbf{p}$. Employ the rank-one recovery method if higher-rank solutions are returned by solving problem (8).
   - Solve problem (13) with fixed $\mathbf{p}$ to obtain the updated $\mathbf{W}$. Employ the rank-one recovery method to obtain $\mathbf{W}$ if higher-rank solutions of $\tilde{\mathbf{W}}$ are returned by solving problem (13). If the SNR_D of the recovery solution is larger than that of the previous step, then continue; else terminate the algorithm.
3. **Until** the SNR_D between two adjacent iterations is less than δ.

where $\mathbf{v}_k = \text{vec}(\text{conj}(\mathbf{g}_{2k})\mathbf{p}^T\mathbf{H}_1^T)$. Using the identity $\text{vec}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\text{vec}(\mathbf{B})$ [18], the RS power constraint can be reformulated as

$$\text{Tr}\{(\mathbf{p}^T\mathbf{H}_1^T \otimes \mathbf{I}_{N_t})\tilde{\mathbf{W}}(\mathbf{p}^T\mathbf{H}_1^T \otimes \mathbf{I}_{N_t})^H\} + \sigma_1^2\text{Tr}(\tilde{\mathbf{W}}) \le P_r. \quad (12)$$

Hence, the optimization problem can be reformulated as the following SDP problem:

$$\begin{aligned} \max_{\tilde{\mathbf{W}}\succeq \mathbf{0}} \quad & \text{SNR}_D \\ \text{s.t.} \quad & (11),\ (12),\ \forall k \in \mathcal{K} \end{aligned} \quad (13)$$

Problem (13) can now be solved with any accuracy $\epsilon > 0$ by using the bisection method to obtain $\tilde{\mathbf{W}}$. A rank-one recovery method inspired by the randomization procedure [15] will be adopted when the optimal solutions to (8) and (13) are not rank-one. The AO based iterative algorithm to solve problem (7) is summarized in Table 1, which can keep the objective nondecreasing as the iterations proceed.

4. PROPOSED SR BASED TRANSCEIVER DESIGN

In this section, we describe a more efficient and simpler transceiver design algorithm, namely the SR based algorithm. We equip the B-S and the RS with a finite codebook of permutation matrices[4], i.e., $\mathcal{T} = \{\mathbf{T}_1, \mathbf{T}_2, \ldots, \mathbf{T}_B\}$, where B is the codebook size which satisfies $B \ll N_r!$[5]. The RS AF transformation matrix is constructed by multiplying the appropriate permutation matrix from the codebook with a power scaling factor. That is to say, the optimization of $\mathbf{W}$ is replaced by that of $\beta_l\mathbf{T}_l$, where $\mathbf{T}_l$ and β_l denote the lth permutation matrix in $\mathcal{T}$ and the corresponding power scaling factor, respectively, $l \in \{1, \ldots, B\}$. Thus, the lth permutation matrix gives rise to a permuted channel matrix, and creates a latent transceiver, which for each index l requires the determination of the BS beamforming vector $\mathbf{p}_l$ and the RS power scaling factor β_l. We can design B such latent transceivers, that is, one for each permutation matrix in $\mathcal{T}$, and choose the optimal transceiver with the largest SNR_D. The proposed SR scheme works as follows:

- The BS designs the B latent transceivers based on available permutation matrices within the codebook; it then determines the optimal latent transceiver with the largest SNR_D.

[4]A permutation matrix is a square binary matrix that has exactly one entry equal to 1 in each row and each column, while all the other entries are equal to 0.

[5]The total number of permutation matrices at the RS is $N_r!$. It is not realistic to use all the permutation matrices as the codebook when N_r is large.

Table 2. The design algorithm for latent transceivers

1. Initialize $t_{min} = \text{SNR}_{D_{min}}$ and $t_{max} = \text{SNR}_{D_{max}}$, where $\text{SNR}_{D_{min}}$ and $\text{SNR}_{D_{max}}$ define the range of relevant SNR_D. Let $\epsilon > 0$ be the desired accuracy.
2. Set $t = (t_{min} + t_{max})/2$.
3. Solve the SOCP feasibility problem. If the problem is feasible, then set $t_{min} = t$. Otherwise, set $t_{max} = t$.

$$\begin{aligned} \text{find} \quad & \mathbf{p}_l, \rho_l \\ \text{s.t.} \quad & \sqrt{t}\|[\sigma_1\|\mathbf{h}_2^H\mathbf{T}_l\|,\ \rho_l\sigma_2]\| \le \mathbf{h}_2^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l, \\ & \|\mathbf{p}_l\| \le \sqrt{P_t},\ \Im(\mathbf{h}_2^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l) = 0, \\ & \|[(\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l)^T,\ \sigma_1\sqrt{N_r}]\| \le \sqrt{P_r}\rho_l, \\ & |\mathbf{g}_{1k}^H\mathbf{p}_l| \le \sqrt{\gamma}\sigma_{1k}, \\ & |\mathbf{g}_{2k}^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l| \le \sqrt{\gamma}\sigma_1\|\mathbf{g}_{2k}^H\mathbf{T}_l\|,\ \forall k \in \mathcal{K}. \end{aligned}$$

4. If $(t_{max} - t_{min}) > \epsilon$ then go to Step 2. Otherwise, return $\rho_l^\star = \rho_l$ and $\mathbf{p}_l^\star = \mathbf{p}_l$, where ρ_l and $\mathbf{p}_l$ represent the last feasible solution of the upper problem and STOP.

- The BS sends the index of the optimal latent transceiver, say l^o, and the corresponding power scaling factor β_{l^o} to the RS through signaling channels.
- Based on the signaling bits forwarded from the BS, the RS determines the corresponding AF transformation matrix $\mathbf{W} = \beta_{l^o}\mathbf{T}_{l^o}$.

In the following, we firstly describe the design algorithm for the construction of the latent transceivers. The design method for the codebook of permutation matrices is also described in this section.

4.1. The design algorithm for latent transceivers

In this part, we develop a new design algorithm to construct the latent transceivers. For each permutation matrix, problem (7) now can be reformulated as

$$\begin{aligned} \max_{\mathbf{p}_l,\beta_l} \quad & \frac{\beta_l^2|\mathbf{h}_2^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l|^2}{\sigma_1^2\beta_l^2\|\mathbf{h}_2^H\mathbf{T}_l\|^2 + \sigma_2^2} \\ \text{s.t.} \quad & \|\mathbf{p}_l\|^2 \le P_t,\ \beta_l^2(\|\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l\|^2 + \sigma_1^2 N_r) \le P_r, \\ & \frac{|\mathbf{g}_{1k}^H\mathbf{p}_l|^2}{\sigma_{1k}^2} \le \gamma,\ \frac{\beta_l^2|\mathbf{g}_{2k}^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l|^2}{\sigma_1^2\beta_l^2\|\mathbf{g}_{2k}^H\mathbf{T}_l\|^2 + \sigma_{2k}^2} \le \gamma,\ \forall k \in \mathcal{K}. \end{aligned} \quad (14)$$

Firstly, we define $\rho_l = \frac{1}{\beta_l}$. Since the noise term could be very insignificant as compared to the other terms, we can ignore the effect of σ_{2k}^2 to make the problem more tractable. The following form will be obtained after introducing a variable t:

$$\begin{aligned} \max_{\mathbf{p}_l,\rho_l,t} \quad & t \\ \text{s.t.} \quad & t(\sigma_1^2\|\mathbf{h}_2^H\mathbf{T}_l\|^2 + \rho_l^2\sigma_2^2) \le |\mathbf{h}_2^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l|^2, \\ & \|\mathbf{p}_l\|^2 \le P_t,\ t \ge 0, \\ & \|[(\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l)^T,\ \sigma_1\sqrt{N_r}]\|^2 \le P_r\rho_l^2, \\ & |\mathbf{g}_{1k}^H\mathbf{p}_l|^2 \le \gamma\sigma_{1k}^2, \\ & |\mathbf{g}_{2k}^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l|^2 \le \gamma\sigma_1^2\|\mathbf{g}_{2k}^H\mathbf{T}_l\|^2,\ \forall k \in \mathcal{K}. \end{aligned} \quad (15)$$

Since phase rotation will not change our optimization results, we can rotate the phase of $\mathbf{h}_2^H\mathbf{T}_l\mathbf{H}_1\mathbf{p}_l$ and then extract the root of both sides to transform the original constraints into second order cone (SOC) constraints. Thus, problem (15) can be solved with any accuracy $\epsilon > 0$ by using the bisection method presented in Table 2.

Table 3. Complexity analysis of the proposed algorithms

Algorithms	Complexity
AO-based	$I_1(\mathcal{O}(m_1\sqrt{N_t}(N_t^3+m_1N_t^2+m_1^2))+$ $\mathcal{O}(m_2N_r(N_r^6+m_2N_r^4+m_2^2)))$
SR-based	$BI_2(\mathcal{O}(m\sqrt{6}(9+(N_t+1)^2+(N_r+2)^2+m^2)))$

4.2. Codebook Design

We now propose a heuristic scheme to construct the codebook of permutation matrices. We seek to choose the permutation matrices which are more likely to result in higher power received by the legitimate receiver. Interestingly, through exhaustive simulation experiments, we observed that if the singular values of the permuted matrices $\mathbf{h}_l = \mathbf{h}_2^H\mathbf{T}_l\mathbf{H}_1$ are smaller, the total received power is usually larger, where $\mathbf{h}_l$ represents the $1\times N_r$ equivalent channel matrix between the BS and the legitimate receiver.

Let ξ^l denote the singular value of $\mathbf{h}_l$. We construct the codebook of permutation matrices by choosing the ones which correspond to the smallest B singular values, i.e.,

$$\{\mathbf{T}_1,\ldots,\mathbf{T}_B\} = \arg\min_{\mathbf{T}_l} B(\xi^l), \tag{16}$$

where $\min B(\cdot)$ returns the permutation matrices corresponding to the smallest B singular values. The performance of the above codebook design approach will be presented along with the simulation results in Section 6.

5. COMPUTATIONAL COMPLEXITY

In this section, we compare the computational complexity of the proposed AO based and SR based algorithms. The complexity of the AO based algorithm is dominated by the solution of (8) and (13) I_1 times, where I_1 denotes the iteration number. Problem (8) involves 1 linear matrix inequality (LMI) limits of size N_t and $m_1 = \mathcal{O}(N_t^2)$ decision variables. Thus, the complexity of a generic interior-point method for solving problem (8) is given by $\mathcal{O}(m_1\sqrt{N_t}(N_t^3+m_1N_t^2+m_1^2))$. Similarly, the complexity of solving problem (13) can be written as $\mathcal{O}(m_2N_r(N_r^6+m_2N_r^4+m_2^2))$, where $m_2 = \mathcal{O}(N_r^4)$.

The complexity of the SR based algorithm is dominated by the solution of problem (15) I_2 times, where I_2 is the iteration number. Problem (15) involves 3 SOC constraints, including 1 SOC of dimension 3, 1 SOC of dimension N_t+1 and 1 SOC of dimension N_r+2. The number of variables is $m = \mathcal{O}(N_t+1)$.

We summarize the computational complexity of the two algorithms in Table 3 for comparison. It is of interest to investigate the asymptotic complexity of the proposed algorithms when N_t, N_r and K are large, i.e., when we let $N_r = N_t = K \longrightarrow \infty$. We further assume that $I_1 = I_2 = I$ for simplicity. Under these conditions, one can verify that the complexities of the proposed AO based and SR based algorithms in Table 3 are $2IN_t^{13}$ and $3\sqrt{6}BIN_t^3$, respectively. Since the value of codebook size B is usually small, the SR based algorithm has lower complexity compared with the AO based algorithm.

6. SIMULATIONS

In this section, we evaluate the performance of the proposed SR based and AO based algorithms. In all experiments, the number of antennas is $N_t = N_r = 4$. The maximum transmit power is normalized as $P_t = P_r = 1$, and the noise variances of the legitimate links are adjusted so that the input SNR$\triangleq \frac{P_t}{\sigma_1^2} = \frac{P_r}{\sigma_2^2}$. The noise variances of all the eavesdroppers through the BS-E_k and the RS-E_k links are set to $\sigma_{1k}^2 = \sigma_{2k}^2 = 0.01$ while the threshold γ is set as $0\ dB$. All the results are obtained by averaging 1000 independent Monte Carlo runs.

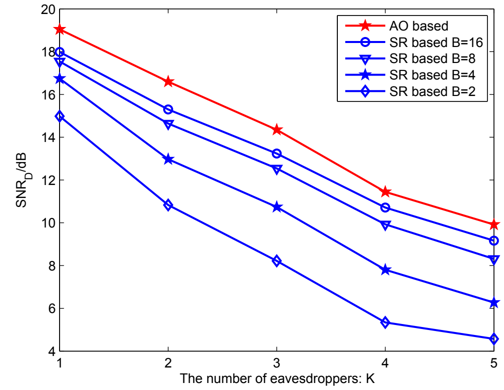

Fig. 2. The SNR$_D$ achieved at the legitimate receiver versus the number of eavesdroppers (SNR= 20dB).

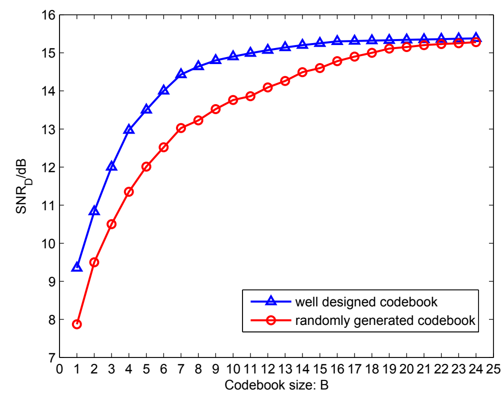

Fig. 3. The SNR$_D$ achieved at the legitimate receiver versus the codebook size (SNR= 20dB, $K=2$).

Fig. 2 shows that the performance of the SR based algorithm can be very close to that of the AO based algorithm in terms of the achieved SNR$_D$. The number of signaling bits for the SR based algorithm is much less than that for the AO based algorithm since only the index of the optimal transceiver and the power scaling factor have to be sent to the RS, instead of the whole RS AF transformation matrix. Fig. 3 presents the SNR$_D$ achieved at the legitimate receiver as a function of codebook size B, which shows that the SR based algorithm equipped with the well designed codebook works better than the SR based algorithm equipped with a randomly generated codebook.

7. CONCLUSION

In this paper, we have considered the joint transceiver design problem for secure communication over a MIMO relay with multi-eavesdroppers. We have proposed AO based and SR based algorithms for the joint optimization of the BS beamforming vector and the RS AF transformation matrix. Specifically, the SR based algorithm can achieve similar performance compared with the AO based algorithm with reduced complexity and overhead. We have also developed an efficient approach for the permutation matrix codebook design. The simulation results have shown satisfactory performance of the proposed algorithms. Robust design algorithms against channel state information (CSI) errors will be considered in the future.

8. REFERENCES

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

[2] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer.* Springer, Norwell, MA, USA, 2009.

[3] A. Khisti and G. Wornell, "Secure transmission with multiple antennas—I: The MISOME wiretap channel," in *IEEE Trans. Inform. Theory,* vol. 56, no. 7, pp. 3088- 3104, July. 2010.

[4] A. Khisti and G. Wornell, "Secure transmission with multiple antennas—II: The MIMOME wiretap channel," in *IEEE Trans. Inform. Theory,* vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge University Press, 2011.

[6] Y.-W. Hong, P. Lan, P.-C. Kuo and C.-C. Jay, "Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches," in *IEEE Signal Process. Mag.,* vol. 30, no. 5, pp. 29-40, 2013.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," in *IEEE Commun. Surv. Tut.,* vol. 16, no. 3, pp.1550-1573, 2014.

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

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

[10] C. Zhang, H. Gao, H.-J. Liu and T.-J. Lv, "Robust beamforming and jamming for secure AF relay networks with multiple eavesdroppers," in *IEEE Military Communications Comference (MILCOM),* pp. 495-500, Oct. 2014.

[11] J.-X. Yang, B. Champagne and Y.-L. Zou, "MIMO AF relaying security: robust transceiver design in the presence of multiple eavesdroppers," in *IEEE International Conference on Communications (ICC),* Jun. 2015.

[12] D. Feng, C. Jiang, G. Lim, L. J. Cimini, Jr., G. Feng, and G. Y. Li, "A survey of energy-efficient wireless communications," in *IEEE Commun. Surveys Tutorials,* vol. 15, no. 1, pp. 167-178, First Quarter 2013.

[13] G. Y. Li, Z. Xu, C. Xiong, C. Yang, S. Zhang, Y. Chen, and S. Xu, "Energy-efficient wireless communications: tutorial, survey, and open issues," in *IEEE Wireless Commun.,* pp. 28-35, Dec. 2011.

[14] N. Banerjee, M. D. Corner, D. Towsley, and B. N. Levine, "Relays, base stations, and meshes: enhancing mobile networks with infrastructure," in *Proc. MOBICOM, San Francisco, USA.,* pp. 81-91, Sep. 2008.

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

[16] Y. Cai, R. de Lamare, L. Yang and M. Zhao, "Robust MMSE precoding based on switched relaying and side information for multiuser MIMO relay systems," in *IEEE Trans. Veh. Technol.,* vol. pp, no. 99, pp. 1, Dec. 2014.

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

[18] R. A. Horn and C. R. Johnson, *Matrix analysis.* Cambridge, U.K.: Cambridge Univ. Press, 2012.