DECODE-AND-FORWARD RELAY BEAMFORMING FOR SECRECY WITH IMPERFECT CSI AND MULTIPLE EAVESDROPPERS

Sanjay Vishwakarma and A. Chockalingam

Department of ECE, Indian Institute of Science, Bangalore 560012, India

ABSTRACT

In this paper, we evaluate secrecy rates in cooperative relay beamforming in the presence of imperfect channel state information (CSI) and multiple eavesdroppers. A source-destination pair aided by k out of M relays, $1 \leq k \leq M$, using decode-and-forward relay beamforming is considered. We compute the worst case secrecy rate with imperfect CSI in the presence of multiple eavesdroppers, where the number of eavesdroppers can be more than the number of relays. We solve the optimization problem for all possible relay combinations to find the secrecy rate and optimum source and relay weights subject to a total power constraint. We relax the rank-1 constraint on the complex semi-definite relay weight matrix and use S-procedure to reformulate the optimization problem that can be solved using convex semi-definite programming.

1. INTRODUCTION

Wireless transmissions, by their very nature, are vulnerable to eavesdropping. There has been considerable interest in the use of physical layer mechanisms to provide secure communications, whereby the eavesdropper gets no information while the intended receiver gets the information reliably. Wyner's work on secrecy capacity of discrete memoryless wiretap channels [1] and subsequent works [2], [3] have created interest in the information-theoretic aspects of physical layer security. Secrecy capacity results for point-to-point fading channels have been widely reported [4]- [12], with several works assuming perfect knowledge of channel state information (CSI); SISO [4], [5], SIMO [6], MISO [7]- [9], and MIMO [10]- [12]. Imperfect knowledge of CSI affects the secrecy capacity, and some recent works have reported secrecy capacity results for point-to-point fading channels with imperfect CSI [13]- [16]. In a related context, wireless communication through cooperation has received much attention, and, quite naturally, secure wireless communications via cooperation has been a topic of interest in recent research [17]- [21]. Cooperative secure communication between a sender and an intended receiver aided by a set of trusted relays in the presence of eavesdropper(s) has been a widely considered scenario. Cooperation based on decode-and-forward (DF) and amplify-and-forward (AF) relaying protocols for secure communication has been investigated in [17] and [18], respectively. Collaborative relay beamforming, studied in [22] without any eavesdropper and secrecy constraint, has been studied with secrecy constraints in the presence of eavesdropper in [20] and [21] for DF and AF protocols, respectively, assuming perfect CSI. Some studies have considered secrecy capacity with cooperation under imperfect CSI assumption as well [17], [21]. In [17], only the relays-eavesdropper CSI is assumed to have estimation errors (stochastically modeled as a zero-mean random variables), whereas the relays-destination CSI is assumed to be perfect. Under these assumptions, a lower bound on the ergodic secrecy capacity is maximized under total relay transmit power constraint. The work in [21] also includes a treatment of secrecy capacity for DF protocol in the presence of imperfect CSI where the errors in $\hat{\mathbf{H}} = \hat{\mathbf{h}}\hat{\mathbf{h}}^{\dagger}$ and $\hat{\mathbf{Z}} = \hat{\mathbf{z}}\hat{\mathbf{z}}^{\dagger}$ are bounded in their Frobenius norm, where $\hat{\mathbf{h}}$ and $\hat{\mathbf{z}}$ are the estimates of the relays-destination and relays-eavesdropper channel vectors. Compared to previously reported works, two new contributions are made in this paper. First, we compute the secrecy rate in the presence of multiple eavesdroppers in decode-and-forward relay beamforming, where the number of eavesdroppers can be more than the number of relays. Second, we compute the worst case secrecy rate when there are imperfections in the CSI (modeled using a norm-bounded CSI error model) on all the links; i.e., considering imperfections in the channel knowledge of source to relays links, relays to destination links, and relays to eavesdroppers links. We also consider the existence of direct links from source to destination and source to eavesdroppers. We solve the optimization problem by relaxing the rank-1 constraint on the complex semi-definite relay weight matrix and using S-procedure to reformulate the problem that is solved using convex semi-definite programming.

2. SYSTEM MODEL

We consider the cooperative relay beamforming system model shown in Fig. 1, which consists of a source node S, M relay nodes $\{R_1, R_2, \cdots, R_M\}$, an intended destination node D, and J eavesdropper nodes $\{E_1, E_2, \cdots, E_J\}$. k relays out of M relays, $1 \leq k \leq M$, are selected to aid the communication from S to D. In addition to the links from relays to destination node and relays to eavesdropper nodes, we assume direct

* THIS WORK WAS SUPPORTED IN PART BY A GIFT FROM THE CISCO UNIVERSITY RESEARCH PROGRAM, A CORPORATE ADVISED FUND OF SILICON VALLEY COMMUNITY FOUNDATION.

978-1-4673-0971-4/12/$31.00 © 2012 IEEE

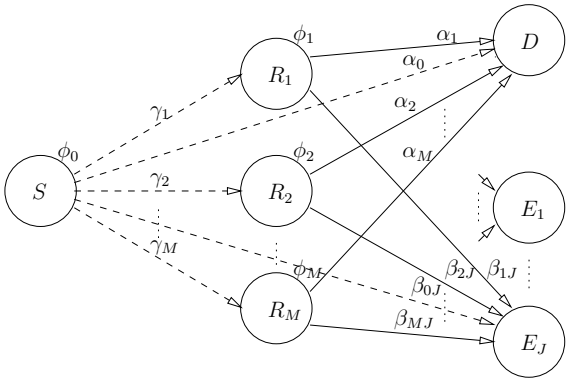


Fig. 1. System model of relay beamforming in the presence of multiple eavesdroppers.

links from source to destination node and source to eavesdropper nodes. The complex fading channel gains between source to k relays are denoted by $\{\gamma_1, \gamma_2, \cdots, \gamma_k\}$. Likewise, the channel gains between k relays to destination and k relays to the jth eavesdropper are denoted by $\{\alpha_1, \alpha_2, \cdots, \alpha_k\}$ and $\{\beta_{1j}, \beta_{2j}, \cdots, \beta_{kj}\}$, respectively, where $j = 1, 2, \cdots, J$. The channel gains on the direct links from source to destination and source to jth eavesdropper are denoted by α_0 and β_{0j}, respectively. The channel gains are assumed to be i.i.d. complex Gaussian with zero mean and variances $\sigma_{\gamma_i}^2$, $\sigma_{\alpha_0}^2$, $\sigma_{\alpha_i}^2$, $\sigma_{\beta_{0j}}^2$, and $\sigma_{\beta_{ij}}^2$.

Let ϕ_0 denote the complex weight applied on the transmitted signal by the source in the first hop of transmission, and let $\{\phi_1, \phi_2, \cdots, \phi_k\}$ denote the complex weights applied on the transmitted signals from the k relays in the second hop of transmission. Let x be the source symbol transmitted from the source in the first hop of transmission with $\mathbb{E}\{|x|^2\} = 1$. In the second hop of transmission, relays which decode this symbol successfully retransmit it to the destination.

Let $\boldsymbol{y}_R$, y_{D_1} and $y_{E_{1j}}$ denote the received signals at the k relays, destination D and jth eavesdropper E_j, respectively, in the first hop of transmission. In the second hop of transmission, the received signals at the destination and jth eavesdropper are denoted by y_{D_2} and $y_{E_{2j}}$, respectively. We have

$$\boldsymbol{y}_R = x\phi_0\boldsymbol{\gamma}^k + \boldsymbol{\eta}_R, \tag{1}$$

$$y_{D_1} = x\phi_0\alpha_0 + \eta_{D_1}, \tag{2}$$

$$y_{E_{1j}} = x\phi_0\beta_{0j} + \eta_{E_{1j}}, \quad j = 1, 2, \cdots, J, \tag{3}$$

$$y_{D_2} = x\boldsymbol{\phi}^{k\dagger}\boldsymbol{\alpha}^k + \eta_{D_2}, \tag{4}$$

$$y_{E_{2j}} = x\boldsymbol{\phi}^{k\dagger}\boldsymbol{\beta}_j^k + \eta_{E_{2j}}, \quad j = 1, 2, \cdots, J, \tag{5}$$

where $\boldsymbol{\gamma}^k = [\gamma_1, \gamma_2, \cdots, \gamma_k]^T$, $\boldsymbol{\eta}_R = [\eta_{R_1}, \cdots, \eta_{R_k}]^T$, $\boldsymbol{\phi}^k = [\phi_1^*, \phi_2^*, \cdots, \phi_k^*]^T$, $\boldsymbol{\alpha}^k = [\alpha_1, \cdots, \alpha_k]^T$, $\boldsymbol{\beta}_j^k = [\beta_{1j}, \cdots, \beta_{kj}]^T$, $j = 1, 2, \cdots, J$. $[.]^T$, $(.)^*$, and $[.]^\dagger$ denote transpose, conjugate, and conjugate transpose operations, respectively.

Let P_0 denote the total transmit power budget (i.e., source power plus relay power), and $P_s^k = \phi_0\phi_0^*$ denote the power transmitted by the source. Defining $\boldsymbol{\Phi}^k \triangleq \boldsymbol{\phi}^k\boldsymbol{\phi}^{k\dagger}$, the mth relay's transmit power is given by the mth diagonal element of $\boldsymbol{\Phi}^k$. The noise components, η's, are assumed to be i.i.d. $\mathcal{CN}(0, N_0)$.

3. SECRECY RATE WITH IMPERFECT CSI

We consider imperfect CSI, modeled as $\gamma_i = \widehat{\gamma}_i + e_{\gamma_i}, i = 1, 2, \cdots, k, \alpha_0 = \widehat{\alpha}_0 + e_{\alpha_0}, \beta_{0j} = \widehat{\beta}_{0j} + e_{\beta_{0j}}, j = 1, 2, \cdots, J$, $\boldsymbol{\alpha}^k = \widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k}, \boldsymbol{\beta}_j^k = \widehat{\boldsymbol{\beta}}_j^k + \boldsymbol{e}_{\boldsymbol{\beta}_j^k}, j = 1, 2, \cdots, J$, where γ_i's, α_0, β_{0j}'s, $\boldsymbol{\alpha}^k$, $\boldsymbol{\beta}_j^k$'s are the true CSI, $\widehat{\gamma}_i$'s, $\widehat{\alpha}_0, \widehat{\beta}_{0j}$'s, $\widehat{\boldsymbol{\alpha}}^k$, $\widehat{\boldsymbol{\beta}}_j^k$'s are the corresponding imperfect CSI, and e_{γ_i}'s, e_{α_0}, $e_{\beta_{0j}}$'s, $\boldsymbol{e}_{\boldsymbol{\alpha}^k}$, $\boldsymbol{e}_{\boldsymbol{\beta}_j^k}$ are the additive errors in the CSI. We consider a norm-bounded CSI error model, where it is assumed that

$$|e_{\gamma_i}| \le \epsilon_{\gamma_i}, \quad |e_{\alpha_0}| \le \epsilon_{\alpha_0}, \quad |e_{\beta_{0j}}| \le \epsilon_{\beta_{0j}}, \\ \|\boldsymbol{e}_{\boldsymbol{\alpha}^k}\| \le \epsilon_{\boldsymbol{\alpha}^k}, \quad \|\boldsymbol{e}_{\boldsymbol{\beta}_j^k}\| \le \epsilon_{\boldsymbol{\beta}_j^k}. \tag{6}$$

With the above uncertainties in CSI, the worst case secrecy rate for this relay link model with $1 \le k \le M$ selected relays is obtained by solving the following optimization problem:

$$C_s = \frac{1}{2}\log_2 \max_{P_s^k,\, \boldsymbol{\Phi}^k} \min_{j:1,2,\cdots,J} \min_{e_{\alpha_0},\, e_{\beta_{0j}},\, \boldsymbol{e}_{\boldsymbol{\alpha}^k},\, \boldsymbol{e}_{\boldsymbol{\beta}_j^k}} z \tag{7}$$

where

$$z = \frac{N_0 + P_s^k(\widehat{\alpha}_0 + e_{\alpha_0})(\widehat{\alpha}_0 + e_{\alpha_0})^* + (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})}{N_0 + P_s^k(\widehat{\beta}_{0j} + e_{\beta_{0j}})(\widehat{\beta}_{0j} + e_{\beta_{0j}})^* + (\widehat{\boldsymbol{\beta}}_j^k + \boldsymbol{e}_{\boldsymbol{\beta}_j^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\beta}}_j^k + \boldsymbol{e}_{\boldsymbol{\beta}_j^k})}$$

subject to power constraints

$$P_s^k \ge 0, \quad P_s^k + trace(\boldsymbol{\phi}^k\boldsymbol{\phi}^{k\dagger}) \le P_0, \tag{8}$$

which can be written in the following equivalent form:

$$\boldsymbol{\Phi}^k \succeq 0,\ rank(\boldsymbol{\Phi}^k) = 1,\ P_s^k \ge 0,\ P_s^k + trace(\boldsymbol{\Phi}^k) \le P_0,$$

and subject to CSI error constraints and information rate constraints to enable relays to correctly decode the source information. Relaxing the rank constraint [20], [23], [24] on $\boldsymbol{\Phi}^k$ and dropping the logarithm, the equivalent optimization problem is as follows:

$$\max_{P_s^k,\, \boldsymbol{\Phi}^k} \min_{j:1,2,\cdots,J} \min_{e_{\alpha_0},\, e_{\beta_{0j}},\, \boldsymbol{e}_{\boldsymbol{\alpha}^k},\, \boldsymbol{e}_{\boldsymbol{\beta}_j^k}} z \tag{9}$$

subject to

$$\boldsymbol{\Phi}^k \succeq 0, \quad P_s^k \ge 0, \quad P_s^k + trace(\boldsymbol{\Phi}^k) \le P_0, \\ |e_{\alpha_0}| \le \epsilon_{\alpha_0}, \quad |e_{\beta_{0j}}| \le \epsilon_{\beta_{0j}}, \\ \|\boldsymbol{e}_{\boldsymbol{\alpha}^k}\| \le \epsilon_{\boldsymbol{\alpha}^k}, \quad \|\boldsymbol{e}_{\boldsymbol{\beta}_j^k}\| \le \epsilon_{\boldsymbol{\beta}_j^k}, \\ \min_{e_{\gamma_i}} (N_0 + P_s^k(\widehat{\gamma}_i + e_{\gamma_i})(\widehat{\gamma}_i + e_{\gamma_i})^*) \ge \\ \min_{e_{\alpha_0},\, \boldsymbol{e}_{\boldsymbol{\alpha}^k}} (N_0 + P_s^k(\widehat{\alpha}_0 + e_{\alpha_0})(\widehat{\alpha}_0 + e_{\alpha_0})^* + \\ (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})),\ \forall i : 1, 2, \cdots, k, \\ |e_{\gamma_i}| \le \epsilon_{\gamma_i}. \tag{10}$$

The inner most minimization in (9), namely,

$$\min_{e_{\alpha_0},\, e_{\beta_{0j}},\, \boldsymbol{e}_{\boldsymbol{\alpha}^k},\, \boldsymbol{e}_{\boldsymbol{\beta}_j^k}} \; z \tag{11}$$

subject to

$$\begin{aligned}
|e_{\alpha_0}| \;\leq\; \epsilon_{\alpha_0}, \quad |e_{\beta_{0j}}| \;\leq\; \epsilon_{\beta_{0j}}, \\
\|\boldsymbol{e}_{\boldsymbol{\alpha}^k}\| \;\leq\; \epsilon_{\boldsymbol{\alpha}^k}, \quad \|\boldsymbol{e}_{\boldsymbol{\beta}_j^k}\| \;\leq\; \epsilon_{\boldsymbol{\beta}_j^k}, \\
\min_{e_{\gamma_i}} (N_0 + P_s^k(\widehat{\gamma}_i + e_{\gamma_i})(\widehat{\gamma}_i + e_{\gamma_i})^*) \;\geq \\
\min_{e_{\alpha_0},\, \boldsymbol{e}_{\boldsymbol{\alpha}^k}} (N_0 + P_s^k(\widehat{\alpha}_0 + e_{\alpha_0})(\widehat{\alpha}_0 + e_{\alpha_0})^* + \\
(\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})), \;\forall i : 1, 2, \cdots, k, \\
|e_{\gamma_i}| \leq \epsilon_{\gamma_i}.
\end{aligned} \tag{12}$$

can be written in the following maximization form:

$$\max_{\boldsymbol{e}_{\boldsymbol{\alpha}^k},\, \boldsymbol{e}_{\boldsymbol{\beta}_j^k},\, t_1^k,\, t_2^k,\, r_j^k} \; \frac{t_1^k}{r_j^k} \tag{13}$$

subject to

$$\begin{aligned}
&\forall\, \boldsymbol{e}_{\boldsymbol{\alpha}^k} \text{ s.t. } \|\boldsymbol{e}_{\boldsymbol{\alpha}^k}\| \leq \epsilon_{\boldsymbol{\alpha}^k} \\
&\implies t_1^k \leq\; N_0 + P_s^k a + (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k}),
\end{aligned}$$

$$\begin{aligned}
&\forall\, \boldsymbol{e}_{\boldsymbol{\alpha}^k} \text{ s.t. } \|\boldsymbol{e}_{\boldsymbol{\alpha}^k}\| \leq \epsilon_{\boldsymbol{\alpha}^k} \\
&\implies t_2^k \geq\; N_0 + P_s^k a + (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k}),
\end{aligned}$$

$$t_1^k \geq 0, \quad N_0 + P_s^k v_i^k \geq t_2^k, \;\; \forall i : 1, 2, \cdots, k,$$

$$\begin{aligned}
&\forall\, \boldsymbol{e}_{\boldsymbol{\beta}_j^k} \text{ s.t. } \|\boldsymbol{e}_{\boldsymbol{\beta}_j^k}\| \leq \epsilon_{\boldsymbol{\beta}_j^k} \\
&\implies r_j^k \geq N_0 + P_s^k b_j + (\widehat{\boldsymbol{\beta}}_j^k + \boldsymbol{e}_{\boldsymbol{\beta}_j^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\beta}}_j^k + \boldsymbol{e}_{\boldsymbol{\beta}_j^k}),
\end{aligned} \tag{14}$$

where

$$a = \min_{e_{\alpha_0}} (\widehat{\alpha}_0 + e_{\alpha_0})(\widehat{\alpha}_0 + e_{\alpha_0})^* \text{ subject to } |e_{\alpha_0}| \;\leq\; \epsilon_{\alpha_0}, \tag{15}$$

$$b_j = \max_{e_{\beta_{0j}}} (\widehat{\beta}_{0j} + e_{\beta_{0j}})(\widehat{\beta}_{0j} + e_{\beta_{0j}})^* \tag{16}$$

$$\text{subject to } |e_{\beta_{0j}}| \;\leq\; \epsilon_{\beta_{0j}}, \tag{17}$$

and $\forall i : 1, 2, \cdots, k,$

$$v_i^k = \min_{e_{\gamma_i}} \; (\widehat{\gamma}_i + e_{\gamma_i})(\widehat{\gamma}_i + e_{\gamma_i})^*, \text{ subject to } |e_{\gamma_i}| \leq \epsilon_{\gamma_i}. \tag{18}$$

Using Lagrangian, the values of a, b_j and v_i^k are obtained by solving the following SDP optimization problems [25]:

$$a = \max_{\lambda,\, \nu} \; \nu \tag{19}$$

$$\text{subject to } \; \lambda \geq 0, \; \begin{bmatrix} 1+\lambda & \widehat{\alpha}_0 \\ \widehat{\alpha}_0^* & \widehat{\alpha}_0^* \widehat{\alpha}_0 - \lambda \epsilon_{\alpha_0}^2 - \nu \end{bmatrix} \succeq 0, \tag{20}$$

and

$$b_j = -\max_{\lambda,\, \nu} \; \nu \tag{21}$$

$$\text{subject to } \lambda \geq 0, \begin{bmatrix} -1+\lambda & -\widehat{\beta}_{0j} \\ -\widehat{\beta}_{0j}^* & -\widehat{\beta}_{0j}^* \widehat{\beta}_{0j} - \lambda \epsilon_{\beta_{0j}}^2 - \nu \end{bmatrix} \succeq 0, \tag{22}$$

and

$$v_i^k = \max_{\lambda,\, \nu} \; \nu, \;\; \forall i : 1, 2, \cdots, k \tag{23}$$

$$\text{subject to } \; \lambda \geq 0, \; \begin{bmatrix} 1+\lambda & \widehat{\gamma}_i \\ \widehat{\gamma}_i^* & \widehat{\gamma}_i^* \widehat{\gamma}_i - \lambda \epsilon_{\gamma_i}^2 - \nu \end{bmatrix} \succeq 0. \tag{24}$$

Using S-procedure, the constraints in the optimization problem in (13), i.e., constraints (14), are transformed to equivalent LMIs (Linear Matrix Inequalities) [25]:

$$\begin{aligned}
&\forall\, \boldsymbol{e}_{\boldsymbol{\alpha}^k} \text{ s.t. } \|\boldsymbol{e}_{\boldsymbol{\alpha}^k}\| \leq \epsilon_{\boldsymbol{\alpha}^k} \implies \\
&t_1^k \leq\; N_0 + P_s^k a + (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k}) \iff \\
&\lambda_1^k \geq 0, \quad \boldsymbol{A}_1^k \triangleq \\
&\begin{bmatrix} \Phi^k + \lambda_1^k \boldsymbol{I} & \Phi^{k\dagger} \widehat{\boldsymbol{\alpha}}^k \\ \widehat{\boldsymbol{\alpha}}^{k\dagger} \Phi^k & \widehat{\boldsymbol{\alpha}}^{k\dagger} \boldsymbol{\Phi}^k \widehat{\boldsymbol{\alpha}}^k + N_0 + P_s^k a - t_1^k - \lambda_1^k \epsilon_{\boldsymbol{\alpha}^k}^2 \end{bmatrix} \succeq 0,
\end{aligned} \tag{25}$$

$$\begin{aligned}
&\forall\, \boldsymbol{e}_{\boldsymbol{\alpha}^k} \text{ s.t. } \|\boldsymbol{e}_{\boldsymbol{\alpha}^k}\| \leq \epsilon_{\boldsymbol{\alpha}^k} \implies \\
&t_2^k \geq\; N_0 + P_s^k a + (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\alpha}}^k + \boldsymbol{e}_{\boldsymbol{\alpha}^k}) \iff \\
&\lambda_2^k \geq 0, \quad \boldsymbol{A}_2^k \triangleq \\
&\begin{bmatrix} -\Phi^k + \lambda_2^k \boldsymbol{I} & -\Phi^{k\dagger} \widehat{\boldsymbol{\alpha}}^k \\ -\widehat{\boldsymbol{\alpha}}^{k\dagger} \Phi^k & -\widehat{\boldsymbol{\alpha}}^{k\dagger} \boldsymbol{\Phi}^k \widehat{\boldsymbol{\alpha}}^k - N_0 - P_s^k a + t_2^k - \lambda_2^k \epsilon_{\boldsymbol{\alpha}^k}^2 \end{bmatrix} \succeq 0,
\end{aligned} \tag{26}$$

$$\begin{aligned}
&\forall\, \boldsymbol{e}_{\boldsymbol{\beta}_j^k} \text{ s.t. } \|\boldsymbol{e}_{\boldsymbol{\beta}_j^k}\| \leq \epsilon_{\boldsymbol{\beta}_j^k} \implies \\
&r_j^k \geq N_0 + P_s^k b_j + (\widehat{\boldsymbol{\beta}}_j^k + \boldsymbol{e}_{\boldsymbol{\beta}_j^k})^\dagger \boldsymbol{\Phi}^k (\widehat{\boldsymbol{\beta}}_j^k + \boldsymbol{e}_{\boldsymbol{\beta}_j^k}) \iff \\
&\mu_j^k \geq 0, \quad \boldsymbol{B}_j^k \triangleq \\
&\begin{bmatrix} -\Phi^k + \mu_j^k \boldsymbol{I} & -\Phi^{k\dagger} \widehat{\boldsymbol{\beta}}_j^k \\ -\widehat{\boldsymbol{\beta}}_j^{k\dagger} \Phi^k & -\widehat{\boldsymbol{\beta}}_j^{k\dagger} \boldsymbol{\Phi}^k \widehat{\boldsymbol{\beta}}_j^k - N_0 - P_s^k b_j + r_j^k - \mu_j^k \epsilon_{\boldsymbol{\beta}_j^k}^2 \end{bmatrix} \succeq 0,
\end{aligned} \tag{27}$$

$$\forall i : 1, 2, \cdots, k, \; N_0 + P_s^k v_i^k \geq t_2^k, \;\; t_1^k \geq 0. \tag{28}$$

Using (25), (26), (27) and (28) the maximization problem in (13) can be written as:

$$\max_{t_1^k,\, t_2^k,\, r_j^k,\, \lambda_1^k,\, \lambda_2^k,\, \mu_j^k} \; \frac{t_1^k}{r_j^k} \tag{29}$$

subject to

$$\begin{aligned}
t_1^k \geq 0, \quad \lambda_1^k \geq 0, \quad \lambda_2^k \geq 0, \quad \mu_j^k \geq 0, \\
N_0 + P_s^k v_i^k \geq t_2^k, \quad \forall i : 1, 2, \cdots, k, \\
\boldsymbol{A}_1^k \succeq 0, \quad \boldsymbol{A}_2^k \succeq 0, \quad \boldsymbol{B}_j^k \succeq 0,
\end{aligned} \tag{30}$$

Using the above, the original optimization problem can be written as:

$$\max_{P_s^k,\, \boldsymbol{\Phi}^k} \; \min_{j:1,2,\cdots,J} \; \max_{t_1^k, t_2^k, r_j^k, \lambda_1^k, \lambda_2^k, \mu_j^k} \; \frac{t_1^k}{r_j^k} \tag{31}$$

subject to

$$\begin{aligned} \boldsymbol{\Phi}^k \succeq 0, \quad P_s^k \geq 0, \quad P_s^k + trace(\boldsymbol{\Phi}^k) \leq P_0, \\ t_1^k \geq 0, \quad \lambda_1^k \geq 0, \quad \lambda_2^k \geq 0, \quad \mu_j^k \geq 0, \\ \forall i : 1, 2, \cdots, k, \quad N_0 + P_s^k v_i^k \geq t_2^k, \\ \boldsymbol{A}_1^k \succeq 0, \quad \boldsymbol{A}_2^k \succeq 0, \quad \boldsymbol{B}_j^k \succeq 0. \end{aligned} \tag{32}$$

Further, using the fact that $(\max\ \min) \leq (\min\ \max)$, the results of the above optimization problem is lower bounded by the results of the following optimization problem:

$$\max_{P_s^k,\ \boldsymbol{\Phi}^k} \ \max_{t_1^k, t_2^k, r_j^k, \lambda_1^k, \lambda_2^k, \mu_j^k} \ \min_{j:1,2,\cdots,J} \ \frac{t_1^k}{r_j^k}, \tag{33}$$

which can be rewritten in an equivalent form as:

$$\max_{P_s^k, \boldsymbol{\Phi}^k, t_1^k, t_2^k, r_j^k, \lambda_1^k, \lambda_2^k, \mu_j^k,\ j:1,2,\cdots,J,\ s^k} \ s^k, \tag{34}$$

subject to

$$\begin{aligned} \boldsymbol{\Phi}^k \succeq 0, \quad P_s^k \geq 0, \quad P_s^k + trace(\boldsymbol{\Phi}^k) \leq P_0, \\ t_1^k \geq 0, \quad \lambda_1^k \geq 0, \quad \lambda_2^k \geq 0, \\ \forall i : 1, 2, \cdots, k, \quad N_0 + P_s^k v_i^k \geq t_2^k, \\ \boldsymbol{A}_1^k \succeq 0, \quad \boldsymbol{A}_2^k \succeq 0, \\ \forall j : 1, 2, \cdots, J, \quad t_1^k \geq s^k r_j^k, \quad \mu_j^k \geq 0, \quad \boldsymbol{B}_j^k \succeq 0. \end{aligned} \tag{35}$$

For a given s^k, the above optimization problem is formulated as the following semi-definite feasibility problem:

$$\text{find} \quad P_s^k,\ \boldsymbol{\Phi}^k,\ t_1^k,\ t_2^k,\ r_j^k,\ \lambda_1^k,\ \lambda_2^k,\ \mu_j^k,\ j : 1, 2, \cdots, J \tag{36}$$

subject to the constraints in (34). The maximum value of s^k can be obtained using bisection method as follows. Let s_{max}^k lie in the interval $[s_{ll}^k,\ s_{lu}^k]$. Check the feasibility of (36) at $s^k = (s_{ll}^k + s_{lu}^k)/2$. If feasible, then $s_{ll}^k = s^k$, else $s_{lu}^k = s^k$. Repeat this until $s_{ll}^k = s_{lu}^k$ or the desired accuracy is achieved. Secrecy rate for the k selected relays is then given by

$$C_s^k = \frac{1}{2} \log_2 s_{max}^k, \tag{37}$$

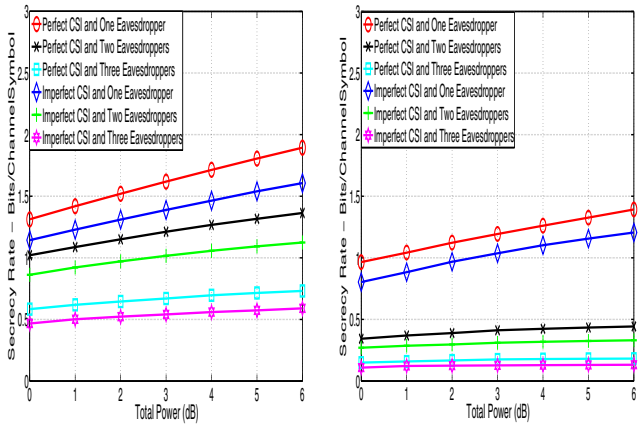
and the maximum secrecy rate is

$$C_s^{max} = \max_{\text{all relay combinations}} C_s^k. \tag{38}$$

Maximization in (38) is performed over all 2^M possible relay combinations.

4. SIMULATION RESULTS

We evaluated the secrecy rates for different system scenarios through simulations [26], [27]. The results are generated for $M = 2$, $J = 1, 2, 3$, and $N_0 = 1$. We take the norm of the CSI error vectors on all links to be equal, and we denote it by ϵ. We evaluate the secrecy rates for different number of eavesdroppers with perfect as well as imperfect CSI.



(a) Destination channels stronger.(b) Eaves' channels stronger.

Fig. 2. Secrecy rate versus total transmit power.

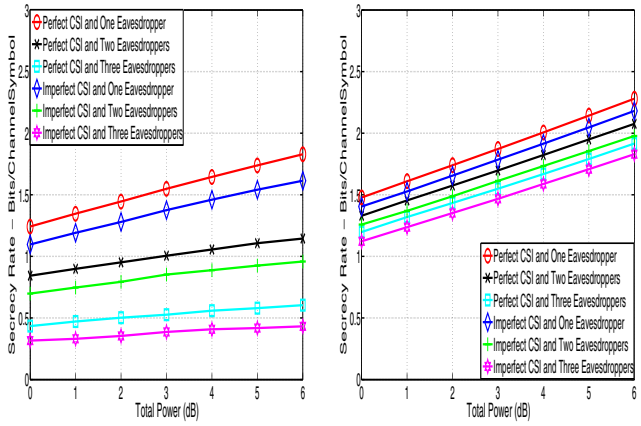
In Fig. 2(a), we plot the secrecy rate as a function of total transmit power, P_0, for the case when the source to destination channel is stronger than source to eavesdroppers channels, and the relays to destination channels are stronger than relays to eavesdroppers channels. The following system parameters are used: $\sigma_{\gamma_1} = \sigma_{\gamma_2} = 4.0$, $\sigma_{\alpha_0} = 2.0$, $\sigma_{\alpha_1} = \sigma_{\alpha_2} = 4.0$, $\sigma_{\beta_{01}} = 0.5$, $\sigma_{\beta_{02}} = 1.0$, $\sigma_{\beta_{03}} = 1.5$, $\sigma_{\beta_{11}} = \sigma_{\beta_{21}} = 1.0$, $\sigma_{\beta_{12}} = \sigma_{\beta_{22}} = 2.0$, $\sigma_{\beta_{13}} = \sigma_{\beta_{23}} = 3.0$, and $\epsilon = 0.1$. It is seen that imperfect CSI degrades secrecy rates compared to those with perfect CSI, and that increased number of eavesdroppers results in reduced secrecy rates.

Next, in Fig. 2(b), we present the secrecy rate for the case when the source to destination channel is weaker than the source to eavesdroppers channels and the relays to destination channels are weaker than the relays to eavesdroppers channels. The following parameters are used in Fig. 2(b): $\sigma_{\gamma_1} = \sigma_{\gamma_2} = 5.0$, $\sigma_{\alpha_0} = 0.5$, $\sigma_{\alpha_1} = \sigma_{\alpha_2} = 5.0$, $\sigma_{\beta_{01}} = 1.0$, $\sigma_{\beta_{02}} = 1.5$, $\sigma_{\beta_{03}} = 2.0$, $\sigma_{\beta_{11}} = \sigma_{\beta_{21}} = 5.5$, $\sigma_{\beta_{12}} = \sigma_{\beta_{22}} = 6.0$, $\sigma_{\beta_{13}} = \sigma_{\beta_{23}} = 6.5$, and $\epsilon = 0.1$. We observe similar behaviour as in Fig. 2(a).

In Fig. 3(a), we show the effect of having direct links from source to eavesdroppers and not having a direct link from source to destination, when the relays to destination channels are stronger than the relays to eavesdroppers channels. $\sigma_{\gamma_1} = \sigma_{\gamma_2} = 4.0$, $\sigma_{\alpha_0} = 0.0$, $\sigma_{\alpha_1} = \sigma_{\alpha_2} = 4.0$, $\sigma_{\beta_{01}} = 0.5$, $\sigma_{\beta_{02}} = 1.0$, $\sigma_{\beta_{03}} = 1.5$, $\sigma_{\beta_{11}} = \sigma_{\beta_{21}} = 1.0$, $\sigma_{\beta_{12}} = \sigma_{\beta_{22}} = 2.0$, $\sigma_{\beta_{13}} = \sigma_{\beta_{23}} = 3.0$, and $\epsilon = 0.1$. In Fig. 3(b), we show the effect of not having a direct link from source to any eavesdropper and having direct links from source to destination, when the relays to destination channel is stronger than the relays to eavesdroppers channels. $\sigma_{\gamma_1} = \sigma_{\gamma_2} = 4.0$, $\sigma_{\alpha_0} = 2.0, \sigma_{\alpha_1} = \sigma_{\alpha_2} = 4.0$, $\sigma_{\beta_{01}} = 0.0$, $\sigma_{\beta_{02}} = 0.0$, $\sigma_{\beta_{03}} = 0.0$, $\sigma_{\beta_{11}} = \sigma_{\beta_{21}} = 1.0$, $\sigma_{\beta_{12}} = \sigma_{\beta_{22}} = 2.0$, $\sigma_{\beta_{13}} = \sigma_{\beta_{23}} = 3.0$ and $\epsilon = 0.1$. From Figs. 3(a) and (b), we see that the availability of direct links to eavesdroppers can significantly

degrade the secrecy rate.

In Fig. 4, we plot the secrecy rate as a function of CSI error (ϵ) with $P_0 = 6$ dB and remaining system parameters are same as in Fig. 2(a). It is seen that secrecy rate degrades with increase in CSI error (ϵ) and the number of eavesdroppers.



(a) No direct link to destination. (b) No direct link to eaves.

Fig. 3. Secrecy rate versus total transmit power.

5. CONCLUSIONS

We evaluated secrecy rates in decode-and-forward cooperative relay beamforming in the presence of imperfect CSI (using a norm-bounded CSI error model) and multiple eavesdroppers, where the number of eavesdroppers can be more than the number of relays. We solved the optimization problem for all possible relay combinations to find the secrecy rate and optimum source and relay weights subject to a total power constraint. We relaxed the rank-1 constraint on the complex semi-definite relay weight matrix and used S-procedure to reformulate the optimization problem that was solved using convex semi-definite programming.

6. REFERENCES

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

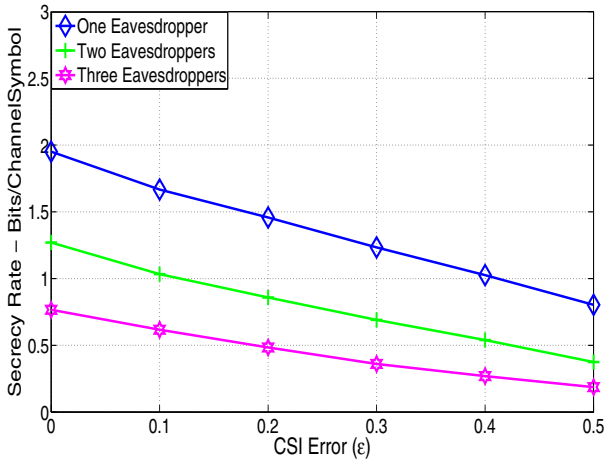


Fig. 4. Secrecy rate versus CSI error (ϵ) – Destination channel stronger.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel,"*IEEE Trans. Inf. Theory*, vol. IT-24, pp. 451- 456, July 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages,"*IEEE Trans. Inf. Theory*, vol. IT-24, pp. 339-348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, June 2008.

[5] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, October 2008.

[6] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," *Proc. IEEE ISIT'2005*, pp. 2152-2155, September 2005.

[7] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraint," *Proc. IEEE ISIT'2007*, June 2007.

[8] R. Liu and H. V. Poor, "Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans.Inf. Theory*, vol. 55, no. 3, pp. 1235-1249, March 2009.

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

[10] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "The Gaussian MIMO wiretap channel," *Proc. IEEE ISIT'2007*, June 2007.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Proc. IEEE ISIT'2008*, July 2008.

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

[13] M. Bloch and J. Laneman, "Information-spectrum methods for information-theoretic security," *Proc. ITA'2009*, pp. 23-28, Feb. 2009.

[14] Y. Y. Pei, Y. C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information,"*IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683-1693, April 2011.

[15] Q. Li and W-K. ma, "Optimal and robust transmit designs for MISO channel secrecy via semi-definite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799-3812, August 2011.

[16] J. H. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," April 2011. arXiv:1104.3161v1 [cs.IT] 15 Apr 2011.

[17] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," *Proc. 46th Annual Allerton Conf. Commun., Control, and Computing*, September 2008.

[18] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," *Proc. IEEE ICASSP'2008*, Taipei, April 2009.

[19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, March 2010.

[20] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," *Proc. IEEE ICC'2010*, Cape Town, May 2010.

[21] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," *Proc. CISS'2010*, March 2010.

[22] G. Zheng, K-K. Wong, A. Paulraj, and B. Ottersten, "Robust collaborative-relay beamforming," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3130-3143, August 2009.

[23] Z. Q. Luo and W. Yu,"An introduction to convex optimization for communications and signal processing," *IEEE Jl. Sel. Areas in Communications*, vol. 24, no. 8, pp. 1426 - 1438, August 2006.

[24] M. Bengtsson and B. Ottersten, Optimal and Suboptimal Transmit Beamforming, in Handbook of Antennas inWireless Communications, L. C. Godara, Ed. Boca Raton, FL: CRC, 2002.

[25] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge Univ. Press, 2004.

[26] J. Sturm, "Using SeDuMi 1.03: A MATLAB toolbox for optimization over symmetric ones," *Opt. Methods and Software*, vol. 11-12, pp. 625-653, 1999. Special issue on Interior Point Methods (CD supplement with software).

[27] J. Lofberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," *Proc. CACSD Conf.*, Taipei, 2004. [Online] Available: http://control.ee.ethz.ch/ joloef/yalmip.php.