MIMO Decode-and-Forward Relay Beamforming for Secrecy with Cooperative Jamming

Sanjay Vishwakarma and A. Chockalingam
Department of ECE, Indian Institute of Science, Bangalore 560012

***Abstract*—In this paper, we consider decode-and-forward (DF) relay beamforming for secrecy with cooperative jamming (CJ) in the presence of multiple eavesdroppers. The communication between a source-destination pair is aided by a multiple-input multiple-output (MIMO) relay. The source has one transmit antenna and the destination and eavesdroppers have one receive antenna each. The source and the MIMO relay are constrained with powers P_S and P_R, respectively. We relax the rank-1 constraint on the signal beamforming matrix and transform the secrecy rate max-min optimization problem to a single maximization problem, which is solved by semidefinite programming techniques. We obtain the optimum source power, signal relay weights, and jamming covariance matrix. We show that the solution of the rank-relaxed optimization problem has rank-1. Numerical results show that CJ can improve the secrecy rate.**

keywords: Relay beamforming, decode-and-forward, physical layer security, secrecy rate, cooperative jamming, multiple eavesdroppers, semidefinite programming.

I. Introduction

The early studies on providing security using physical layer techniques started with the innovative works in [1]–[3]. Wireless transmissions, being broadcast in nature, require special attention to protect them from getting eavesdropped [4]. Investigation of the secrecy capacity/rate of various channels has been a topic of research interest. For example, the secrecy capacity results for point-to-point single-antenna and multi-antenna wireless channels have been reported in the literature [5]–[8]. Also, artificial noise injection (also referred to as cooperative jamming) is known to improve secrecy rates [9]. This is achieved by adding artificially generated noise (jamming signal) to the information bearing signal such that it degrades the channel towards the eavesdropper(s) but does not degrade the intended receiver's channel.

Recently, there has been a lot of interest in cooperative relay communication with secrecy constraints [10]–[15]. Cooperative relays act as distributed antennas and they can help improving the secrecy rates. The relays can operate under amplify-and-forward (AF) and decode-and-forward (DF) protocols. In this paper, we consider DF relay beamforming for secrecy with cooperative jamming (CJ) in the presence of multiple eavesdroppers. DF relay beamforming using single-antenna relays has been considered in [15]. It did not consider CJ. Our present work, on the other hand, considers secrecy rate in the presence of CJ injected by a multi-antenna relay (MIMO relay). In the considered system, the MIMO relay aids the communication between source and destination. The source, destination, and eavesdroppers are single-antenna nodes. The source and MIMO relay are power constrained. In addition to forwarding the decoded signal, the MIMO relay aids secrecy by injecting artificial noise (jamming signal) to degrade the eavesdroppers' channels. For this system, we obtain the optimum source power, signal relay weights, and jamming covariance matrix. We do this by relaxing the rank-1 constraint on the signal beamforming matrix and transforming the secrecy rate max-min optimization problem to a single maximization problem, which is then solved by semidefinite programming techniques. We show that the solution of the rank-relaxed optimization problem has rank-1, and that the CJ signal transmitted by the MIMO relay improves the secrecy rate.

Notations : $\boldsymbol{A} \in \mathbb{C}^{N_1 \times N_2}$ implies that $\boldsymbol{A}$ is a complex matrix of dimension $N_1 \times N_2$. $\boldsymbol{A} \succeq \boldsymbol{0}$ and $\boldsymbol{A} \succ \boldsymbol{0}$ denote that $\boldsymbol{A}$ is a positive semidefinite matrix and positive definite matrix, respectively. $\boldsymbol{I}$ denotes the identity matrix. Transpose and complex conjugate transpose operations are denoted by $[.]^T$ and $[.]^*$, respectively. $\| . \|$ denotes 2-norm operation. $\mathbb{E}[.]$ denotes expectation operation.

II. System Model

Consider a DF cooperative relaying scheme which consists of a source node S having single transmit antenna, a MIMO relay node R having N receive and transmit antennas, an intended destination node D having single receive antenna, and J eavesdropper nodes $\{E_1, E_2, \cdots, E_J\}$ having single receive antenna each. The system model is shown in Fig. 1.

In addition to the links from relay to destination node and relay to eavesdropper nodes, we assume direct links from source to destination node and source to eavesdropper nodes. The complex fading channel gain vector between the source and relay is denoted by $\boldsymbol{g} \in \mathbb{C}^{N \times 1}$. Likewise, the channel vector between the relay and destination is denoted by $\boldsymbol{h} \in \mathbb{C}^{1 \times N}$, and the channel vector between the relay and the jth eavesdropper is denoted by $\boldsymbol{z}_j \in \mathbb{C}^{1 \times N}$, $j = 1, 2, \cdots, J$. The channel gains on the direct links from the source to destination and the source to jth eavesdropper are denoted by h_0 and z_{0j}, respectively. We also assume that channel gains on all the links are known and that they remain static over the transmission of a codeword. This assumption is reasonable when the eavesdroppers are also legitimate users in the network.

Let P_S and P_R denote the available transmit powers for the source and relay, respectively. The source transmits an i.i.d. symbol $x \sim \mathcal{CN}(0, 1)$ in the first hop of transmission. In the second hop, the relay transmits the successfully

This work was supported in part by a gift from the Cisco University Research Program, a corporate advised fund of Silicon Valley Community Foundation.

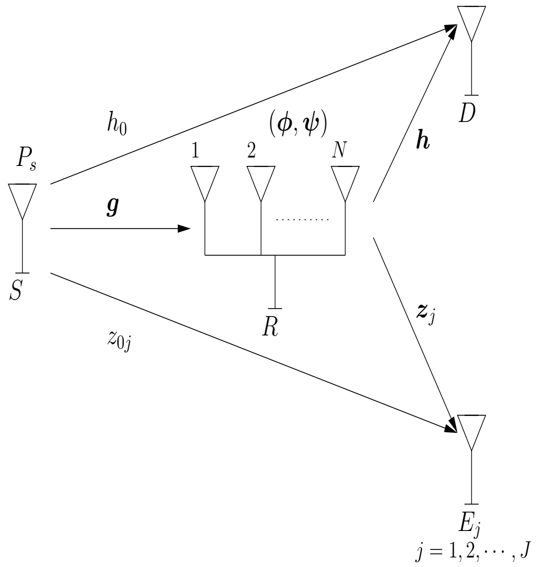

Fig. 1. System model – DF relay beamforming with cooperative jamming using MIMO relay.

decoded symbol to the destination. Let $\{\phi_1, \phi_2, \cdots, \phi_N\}$ denote the complex weights applied on the decoded symbol x transmitted by the relay in the second hop. Define $\boldsymbol{\phi} = [\phi_1, \phi_2, \cdots, \phi_N]^T \in \mathbb{C}^{N\times 1}$. In addition to the decoded symbol x, the relay also transmits an i.i.d. jamming signal $\boldsymbol{\psi} \in \mathbb{C}^{N\times 1}$ where $\boldsymbol{\psi} \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Psi})$ and $\boldsymbol{\Psi} = \mathbb{E}[\boldsymbol{\psi}\boldsymbol{\psi}^*]$, with an intention to degrade the links towards the eavesdroppers.

Let $P_s(\leq P_S)$ denote the power transmitted by the source S in the first hop. Let $\boldsymbol{y}_R \in \mathbb{C}^{N\times 1}$, y_{D_1}, and $y_{E_{1j}}$ denote the received signals at the relay R, destination D, and jth eavesdropper E_j, respectively, in the first hop. In the second hop, the received signals at the destination and jth eavesdropper are denoted by y_{D_2} and $y_{E_{2j}}$, respectively. We have

$$\boldsymbol{y}_R = \sqrt{P_s}\boldsymbol{g}x + \boldsymbol{\eta}_R, \quad (1)$$

$$y_{D_1} = \sqrt{P_s}h_0 x + \eta_{D_1}, \quad (2)$$

$$y_{E_{1j}} = \sqrt{P_s}z_{0j}x + \eta_{E_{1j}}, \quad \forall j = 1, 2, \cdots, J, \quad (3)$$

$$y_{D_2} = \boldsymbol{h}\boldsymbol{\phi}x + \boldsymbol{h}\boldsymbol{\psi} + \eta_{D_2}, \quad (4)$$

$$y_{E_{2j}} = \boldsymbol{z}_j\boldsymbol{\phi}x + \boldsymbol{z}_j\boldsymbol{\psi} + \eta_{E_{2j}}, \quad \forall j = 1, 2, \cdots, J. \quad (5)$$

The noise components, η's, are assumed to be i.i.d. $\mathcal{CN}(0, N_0)$.

III. MIMO DF Relay Beamforming with CJ

Using (1), the information rate at the relay R is

$$\frac{1}{2}I(x;\ \boldsymbol{y}_R) = \frac{1}{2}\log_2\left(1 + \frac{P_s \parallel \boldsymbol{g} \parallel^2}{N_0}\right), \quad (6)$$

where the factor $1/2$ appears because of two hops. Using (2) and (4), the information rate at the destination D is

$$\frac{1}{2}I(x;\ y_{D_1},\ y_{D_2}) = \frac{1}{2}\log_2\left(1 + \frac{P_s \mid h_0 \mid^2}{N_0} + \frac{\boldsymbol{h}\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{h}^*}{N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*}\right). \quad (7)$$

Similarly, using (3) and (5), the information rate at the eavesdropper E_j is

$$\frac{1}{2}I(x;\ y_{E_{1j}},\ y_{E_{2j}}) = \frac{1}{2}\log_2\left(1 + \frac{P_s \mid z_{0j} \mid^2}{N_0} + \frac{\boldsymbol{z}_j\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j\boldsymbol{\Psi}\boldsymbol{z}_j^*}\right). \quad (8)$$

Further, the relay will be able to correctly decode the symbol x if [11,15]

$$\frac{1}{2}I(x;\ \boldsymbol{y}_R) \geq \frac{1}{2}I(x;\ y_{D_1},\ y_{D_2}),$$

$$\text{i.e.,} \quad \frac{1}{2}\log_2\left(1 + \frac{P_s \parallel \boldsymbol{g} \parallel^2}{N_0}\right) \geq \frac{1}{2}\log_2\left(1 + \frac{P_s \mid h_0 \mid^2}{N_0} + \frac{\boldsymbol{h}\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{h}^*}{N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*}\right). \quad (9)$$

The total power (signal power plus jamming signal power) transmitted by the relay is given by

$$\boldsymbol{\phi}^*\boldsymbol{\phi} + trace(\boldsymbol{\Psi}) \leq P_R. \quad (10)$$

Using (7), (8), and subject to the constraints in (9), (10), the achievable secrecy rate is obtained by solving the following optimization problem:

$$R_s = \max_{P_s,\ \boldsymbol{\phi},\ \boldsymbol{\Psi}} \min_{j:1,2,\cdots,J} \frac{1}{2}\left\{ \log_2\left(1 + \frac{P_s \mid h_0 \mid^2}{N_0} + \frac{\boldsymbol{h}\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{h}^*}{N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*}\right) - \log_2\left(1 + \frac{P_s \mid z_{0j} \mid^2}{N_0} + \frac{\boldsymbol{z}_j\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j\boldsymbol{\Psi}\boldsymbol{z}_j^*}\right)\right\}$$

$$= \frac{1}{2}\log_2 \max_{P_s,\ \boldsymbol{\phi},\ \boldsymbol{\Psi}} \min_{j:1,2,\cdots,J} \left(\frac{a + \frac{\boldsymbol{h}\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{h}^*}{N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*}}{b_j + \frac{\boldsymbol{z}_j\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j\boldsymbol{\Psi}\boldsymbol{z}_j^*}}\right) \quad (11)$$

$$\text{s.t.} \quad 0 \leq P_s \leq P_S, \quad \boldsymbol{\Psi} \succeq \mathbf{0}, \quad \boldsymbol{\phi}^*\boldsymbol{\phi} + trace(\boldsymbol{\Psi}) \leq P_R, \quad \frac{1}{2}\log_2(c) \geq \frac{1}{2}\log_2\left(a + \frac{\boldsymbol{h}\boldsymbol{\phi}\boldsymbol{\phi}^*\boldsymbol{h}^*}{N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*}\right), \quad (12)$$

where

$$a = \left(1 + \frac{P_s \mid h_0 \mid^2}{N_0}\right), \quad b_j = \left(1 + \frac{P_s \mid z_{0j} \mid^2}{N_0}\right), \quad \text{and} \quad c = \left(1 + \frac{P_s \parallel \boldsymbol{g} \parallel^2}{N_0}\right).$$

We solve the above problem for a fixed $P_s = m\triangle$, where $\triangle = P_S/M$, M is a large positive integer, and $1 \leq m \leq M$. We denote the secrecy rate for a given $P_s = m\triangle$ by $R_s(m\triangle)$.

Defining $\boldsymbol{\Phi} = \boldsymbol{\phi}\boldsymbol{\phi}^*$ and dropping the logarithm in (11), (12), we write the optimization problem (11) in the following equivalent form:

$$\max_{\boldsymbol{\Phi},\ \boldsymbol{\Psi}} \min_{j:1,2,\cdots,J} \left(\frac{a + \frac{\boldsymbol{h}\boldsymbol{\Phi}\boldsymbol{h}^*}{N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*}}{b_j + \frac{\boldsymbol{z}_j\boldsymbol{\Phi}\boldsymbol{z}_j^*}{N_0 + \boldsymbol{z}_j\boldsymbol{\Psi}\boldsymbol{z}_j^*}}\right) \quad (13)$$

$$\text{s.t.}\quad \mathbf{\Phi}\succeq\mathbf{0},\quad rank(\mathbf{\Phi})=1,\quad \mathbf{\Psi}\succeq\mathbf{0},$$
$$trace(\mathbf{\Phi})+trace(\mathbf{\Psi})\ \le\ P_R,$$
$$c\ \ge\ \Big(a+\frac{\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*}{N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*}\Big). \tag{14}$$

Further, we relax the $rank(\mathbf{\Phi})=1$ in (14) and transform the inner most minimization in (13), i.e.,

$$\min_{j:1,2,\cdots,J}\left(\frac{a+\frac{\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*}{N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*}}{b_j+\frac{\boldsymbol{z}_j\mathbf{\Phi}\boldsymbol{z}_j^*}{N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*}},\right)$$

to an equivalent maximization form:

$$\max_{r,\ s}\ rs \tag{15}$$

$$\text{s.t.}\quad \Big(a+\frac{\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*}{N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*}\Big)\ \ge\ r,$$
$$\left(\frac{1}{b_j+\frac{\boldsymbol{z}_j\mathbf{\Phi}\boldsymbol{z}_j^*}{N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*}}\right)\ \ge\ s,\quad \forall j=1,2,\cdots,J. \tag{16}$$

With this, we write the optimization problem (13) in the following single maximization form:

$$\max_{\mathbf{\Phi},\ \mathbf{\Psi},\ r,\ s}\ rs \tag{17}$$

s.t.

$$r\ge 0,\ s\ge 0,\ \mathbf{\Phi}\succeq\mathbf{0},\ \mathbf{\Psi}\succeq\mathbf{0}, \tag{18.1}$$
$$trace(\mathbf{\Phi})+\ trace(\mathbf{\Psi})\ \le\ P_R, \tag{18.2}$$
$$c\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)\ \ge\ a\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)+\big(\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*\big), \tag{18.3}$$
$$a\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)+\big(\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*\big)\ \ge\ r\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big), \tag{18.4}$$
$$\forall j=1,2,\cdots,J,\quad \big(N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*\big)\ \ge$$
$$s\Big(b_j\big(N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*\big)+\big(\boldsymbol{z}_j\mathbf{\Phi}\boldsymbol{z}_j^*\big)\Big). \tag{18.5}$$
$$\tag{18}$$

In the appendix, we show that the solution $\mathbf{\Phi}$ of the above optimization problem has rank-1. We also numerically confirm that the solution $\mathbf{\Phi}$ of the above optimization problem has rank-1. This implies that the optimization problems (17) and (13) are equivalent. We solve the above optimization problem as follows.

Step 1: We split the optimization problem (17) into the following two optimization problems, and solve for r_{max} and s_{max}, respectively:

$$r_{max}\ =\ \max_{\mathbf{\Phi},\ \mathbf{\Psi},\ r}\ r \tag{19}$$

$$\text{s.t.}\quad r\ge 0,\quad \mathbf{\Phi}\succeq\mathbf{0},\quad \mathbf{\Psi}\succeq\mathbf{0},$$
$$trace(\mathbf{\Phi})+\ trace(\mathbf{\Psi})\ \le\ P_R,$$
$$c\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)\ \ge\ a\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)+\big(\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*\big),$$
$$a\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)+\big(\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*\big)\ \ge\ r\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big), \tag{20}$$

and

$$s_{max}\ =\ \max_{\mathbf{\Phi},\ \mathbf{\Psi},\ s}\ s \tag{21}$$

$$\text{s.t.}\quad s\ge 0,\quad \mathbf{\Phi}\succeq\mathbf{0},\quad \mathbf{\Psi}\succeq\mathbf{0},$$
$$trace(\mathbf{\Phi})+\ trace(\mathbf{\Psi})\ \le\ P_R,$$
$$c\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)\ \ge\ a\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)+\big(\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*\big),$$
$$\forall j=1,2,\cdots,J,\quad \big(N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*\big)\ \ge$$
$$s\Big(b_j\big(N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*\big)+\big(\boldsymbol{z}_j\mathbf{\Phi}\boldsymbol{z}_j^*\big)\Big). \tag{22}$$

For a given r and s, the optimization problems (19) and (21) can be written, respectively, as the following two semidefinite feasibility problems [16]:

$$\text{find}\ \mathbf{\Phi},\ \mathbf{\Psi}, \tag{23}$$

s.t. all the constraints in (20) are satisfied, and

$$\text{find}\ \mathbf{\Phi},\ \mathbf{\Psi}, \tag{24}$$

s.t. all the constraints in (22) are satisfied.

The optimization problems (19) and (21) can be solved using bisection method. We describe the bisection method in short to solve (19) as follows. Let r_{max} lie in the interval $[r_{ll},\ r_{ul}]$. Check the feasibility of (23) at $r=(r_{ll}+r_{ul})/2$. If (23) is feasible then $r_{ll}=r$ else $r_{ul}=r$. Repeat this until $r_{ul}-r_{ll}\le\delta$, where δ is a small positive number. The intervals $[r_{ll},\ r_{ul}]$ and $[s_{ll},\ s_{ul}]$ to compute r_{max} and s_{max} can be taken as $[1,\ c]$ and $[0,\ 1]$, respectively. The maximum values of r and s obtained in the above two independent optimization problems will be larger than the values that would be obtained in the original joint optimization problem (17). This is due to the fact that the maximum over a larger set (or unconstrained set) is larger than the maximum over the smaller set (or constrained set). So the maximum value of the product rs obtained in the constrained optimization problem (17) will be upper bounded by the product $r_{max}s_{max}$.

Step 2: We denote the optimum value of the optimization problem (17) by $r_{opt}s_{opt}$. For positive secrecy rate, $r_{max}\ge r_{opt}>1,\ 1\ge s_{max}\ge s_{opt}>0$ and $r_{opt}s_{opt}>1$. Having obtained the values of r_{max} and s_{max} in Step 1, we obtain $r_{opt}s_{opt}$ sequentially by increasing r from 1 towards r_{max} in discrete steps of size $\triangle_r=(r_{max}-1)/L$, where L is a large positive integer, and finding the maximum s such that the constraints in (18) are feasible and the product rs is maximum. The algorithm to obtain $r_{opt}s_{opt}$ is as follows:

---

1. **for** $(i\ =\ 1\ :\ 1\ :\ L)$
2. **begin**
3. $r_i\ =\ 1+(i\ *\ \triangle_r)$

4. $s_i\ =\ \max_{\mathbf{\Phi},\ \mathbf{\Psi},\ s,\ r=r_i}\ s$
5. s.t. to all constraints in (18) with $r=r_i$ in (18.4)

6. **if** $(i=1)$ **then** $r_{opt}=r_i,\ s_{opt}=s_i$
7. **elseif** $(r_{opt}s_{opt}\ \le\ r_is_i)$ **then** $r_{opt}=r_i,\ s_{opt}=s_i$
8. **else** $r_{opt}=r_{opt},\ s_{opt}=s_{opt}$
9. **endif**
10. **end for loop**

The constrained maximization problem in the for loop above can be solved using the bisection method, as described in Step 1 to solve (19), by checking the feasibility of the constraints in (18) at $r=r_i$ and s in the interval $[0,s_{max}]$.

With $r_{opt}s_{opt}$ obtained from Step 2, the secrecy rate $R_s(m\triangle)$ for a given source power $P_s = m\triangle$ is then given by

$$R_s(m\triangle) = \frac{1}{2}\log_2 r_{opt}s_{opt}, \tag{25}$$

and the optimum secrecy rate R_s for $0 \le P_s \le P_S$ is

$$R_s = \max_{m:1,2,\cdots,M} R_s(m\triangle). \tag{26}$$

IV. Results and Discussions

We computed the secrecy rate as a function of total relay power through simulations for the following set of system parameters: $N = 2$, $N_0 = 1$, $J = 1,2,3$, $L = 50$, and fixed $P_s = 0$ dB. The following channel gains are used: $\boldsymbol{g} = [-0.5839 + 2.2907i,\ -0.7158 + 0.1144i]^T$, $h_0 = -0.3822 - 0.3976i$, $z_{01} = 0.0123 + 0.0137i$, $z_{02} = 0.0231 - 0.0178i$, $z_{03} = -0.0045 - 0.0042i$, $\boldsymbol{h} = [0.2174 - 0.6913i,\ -0.4047 - 0.3159i]$, $\boldsymbol{z}_1 = [0.3826 + 0.0811i,\ 0.8389 - 0.0943i]$, $\boldsymbol{z}_2 = [0.2977 + 0.7902i,\ -0.2069 + 0.4696i]$, $\boldsymbol{z}_3 = [-0.6076 + 0.6637i,\ -0.3316 + 0.1921i]$.

In Fig. 2, we plot the secrecy rate with/without CJ versus total relay power for $J = 1,2,3$ eavesdroppers. In this figure, we observe that when only one eavesdropper is present, the secrecy rate plots with/without CJ overlap. This is due to the null signal beamforming by the MIMO relay at the eavesdropper. This is possible only when the number of eavesdroppers is strictly less than the number of antennas in the MIMO relay which happens to be true for this case with $N = 2$ and $J = 1$. We also observe that the secrecy rate increases with increase in relay power, and exhibits saturation behavior for large relay powers. This is due to the constraint (18.3) being upper bounded by factor c for a fixed source power P_s. This behavior is discussed in detail in the appendix. For the system parameter setting in Fig. 2, we also observe a clear advantage of using the jamming signal in improving the secrecy rate when more than two eavesdroppers are present.

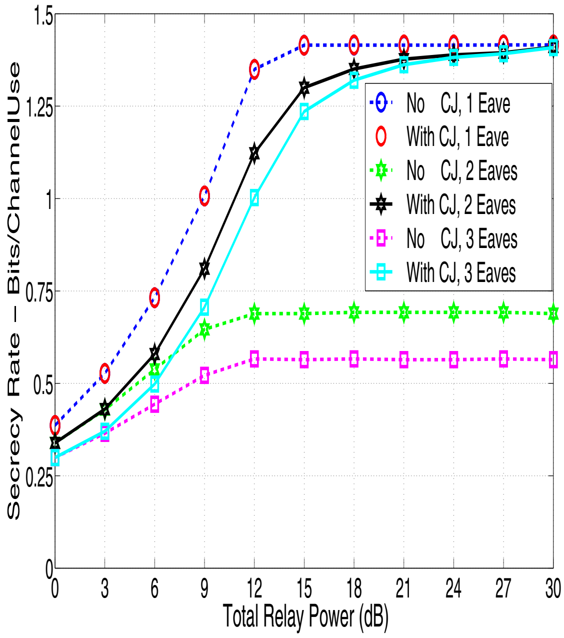

Fig. 2. Secrecy rate in DF MIMO relay beamforming with/without jamming signal versus total relay power. $N = 2$, $N_0 = 1$, $J = 1,2,3$, $L = 50$, and fixed $P_s = 0$ dB.

V. Conclusions

We investigated decode-and-forward MIMO relay beamforming for secrecy with cooperative jamming and in the presence of multiple eavesdroppers. We solved the secrecy rate max-min optimization problem by relaxing the rank-1 constraint on the signal beamforming matrix and transformed the problem into a single maximization problem, which was then solved using semidefinite programming. We showed that the solution of the rank-relaxed optimization problem was rank-1. We obtained the optimum source power, signal relay weights, and jamming covariance matrix. Cooperative jamming was shown to improve the secrecy rate.

Appendix

In this appendix, we show that the solution $\boldsymbol{\Phi}$ of the optimization problem (17) has rank-1. Take the Lagrangian of the optimization problem (17) as follows:

$$\begin{aligned}
&\ell(r, s, \boldsymbol{\Phi}, \boldsymbol{\Psi}, \lambda_r, \lambda_s, \boldsymbol{\Lambda}_\Phi, \boldsymbol{\Lambda}_\Psi, \lambda_{P_R}, \xi, \mu, \nu_j) \ = \\
&\qquad -rs - \lambda_r r - \lambda_s s \\
&\qquad -trace(\boldsymbol{\Lambda}_\Phi \boldsymbol{\Phi}) - trace(\boldsymbol{\Lambda}_\Psi \boldsymbol{\Psi}) \\
&\qquad + \lambda_{P_R}\Big(trace(\boldsymbol{\Phi}) + \ trace(\boldsymbol{\Psi}) - P_R\Big) \\
&+ \xi\Big(a\big(N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*\big) + \big(\boldsymbol{h}\boldsymbol{\Phi}\boldsymbol{h}^*\big) - c\big(N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*\big)\Big) \\
&+ \mu\Big(r\big(N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*\big) - a\big(N_0 + \boldsymbol{h}\boldsymbol{\Psi}\boldsymbol{h}^*\big) - \big(\boldsymbol{h}\boldsymbol{\Phi}\boldsymbol{h}^*\big)\Big) \\
&\qquad + \sum_{j=1}^{J}\nu_j\Big(s\Big(b_j\big(N_0 + \boldsymbol{z}_j\boldsymbol{\Psi}\boldsymbol{z}_j^*\big) + \big(\boldsymbol{z}_j\boldsymbol{\Phi}\boldsymbol{z}_j^*\big)\Big) \\
&\qquad\qquad - \big(N_0 + \boldsymbol{z}_j\boldsymbol{\Psi}\boldsymbol{z}_j^*\big)\Big),
\end{aligned}$$

where $\lambda_r \ge 0$, $\lambda_s \ge 0$, $\boldsymbol{\Lambda}_\Phi \succeq \boldsymbol{0}$, $\boldsymbol{\Lambda}_\Psi \succeq \boldsymbol{0}$, $\lambda_{P_R} \ge 0$, $\xi \ge 0$, $\mu \ge 0$, and $\nu_j \ge 0$ are Lagrangian multipliers. The KKT conditions are as follows:

(K1) all the constraints in (18).

(K2) $\lambda_r r = 0$ and $\lambda_s s = 0$. Since for positive secrecy rate, $r > 1$, $1 \ge s > 0$ and $rs > 1$, this implies that $\lambda_r = 0$ and $\lambda_s = 0$.

(K3) $trace(\boldsymbol{\Lambda}_\Phi \boldsymbol{\Phi}) = 0$. Since $\boldsymbol{\Lambda}_\Phi \succeq \boldsymbol{0}$ and $\boldsymbol{\Phi} \succeq \boldsymbol{0}$, this implies that $\boldsymbol{\Lambda}_\Phi \boldsymbol{\Phi} = \boldsymbol{0}$.

(K4) $trace(\boldsymbol{\Lambda}_\Psi \boldsymbol{\Psi}) = 0$. Since $\boldsymbol{\Lambda}_\Psi \succeq \boldsymbol{0}$ and $\boldsymbol{\Psi} \succeq \boldsymbol{0}$, this implies that $\boldsymbol{\Lambda}_\Psi \boldsymbol{\Psi} = \boldsymbol{0}$.

(K5) $\lambda_{P_R}\Big(trace(\mathbf{\Phi})+trace(\mathbf{\Psi})-P_R\Big)=0$.

(K6) $\xi\Big(a\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)+\big(\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*\big)-c\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)\Big)=0$.

(K7) $\mu\Big(r\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)-a\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)-\big(\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*\big)\Big)=0$.

(K8) $\nu_j\Bigg(s\Big(b_j\big(N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*\big)+\big(\boldsymbol{z}_j\mathbf{\Phi}\boldsymbol{z}_j^*\big)\Big)-\big(N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*\big)\Bigg)=0,\ \ \forall j=1,2,\cdots,J$.

(K9) $\frac{\partial \ell}{\partial r}=0 \implies s+\lambda_r=\mu\big(N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*\big)$. Since $\lambda_r=0$ from $(K2)$, this implies that $\mu>0$. With $\mu>0$ in $(K7)$, constraint (18.4) will be satisfied with equality.

(K10) $\frac{\partial \ell}{\partial s}=0 \implies r+\lambda_s=\sum_{j=1}^{J}\nu_j\Big(b_j\big(N_0+\boldsymbol{z}_j\mathbf{\Psi}\boldsymbol{z}_j^*\big)+\big(\boldsymbol{z}_j\mathbf{\Phi}\boldsymbol{z}_j^*\big)\Big)$. Since $\lambda_s=0$ from (K2), this implies that not all ν_js can be zero simultaneously and some constraints in (18.5) will be satisfied with equality.

(K11) $\frac{\partial \ell}{\partial \mathbf{\Phi}}=\mathbf{0} \implies \mathbf{\Lambda}_\Phi=\lambda_{P_R}\boldsymbol{I}+(\xi-\mu)(\boldsymbol{h}^*\boldsymbol{h})+s\sum_{j=1}^{J}\nu_j(\boldsymbol{z}_j^*\boldsymbol{z}_j)\succeq\mathbf{0}$.

(K12) $\frac{\partial \ell}{\partial \mathbf{\Psi}}=\mathbf{0} \implies \mathbf{\Lambda}_\Psi=\lambda_{P_R}\boldsymbol{I}+(\xi a-\xi c+\mu r-\mu a)(\boldsymbol{h}^*\boldsymbol{h})+\sum_{j=1}^{J}\nu_j(sb_j-1)(\boldsymbol{z}_j^*\boldsymbol{z}_j)\succeq\mathbf{0}$.

For $\mathbf{\Phi}\neq\mathbf{0}$, the constraint (18.3) will be satisfied only if $c>a$. We assume that $c>a$. Let P_R be small enough such that the constraint (18.3) is satisfied with strict inequality. With this, (K6) implies that $\xi=0$. (K3), and (K4) imply that $trace(\mathbf{\Lambda}_\Phi\mathbf{\Phi})+trace(\mathbf{\Lambda}_\Psi\mathbf{\Psi})=0$. (K11), (K12), (K5), (K6), (K7), and (K8) further imply that

$$\lambda_{P_R}P_R+\xi(c-a)N_0+\mu(a-r)N_0+\sum_{j=1}^{J}\nu_j(1-sb_j)N_0=0. \tag{27}$$

(K9) and (18.4) imply that $\mu(a-r)N_0<0$. Similarly, (K10) and (18.5) imply that $\sum_{j=1}^{J}\nu_j(1-sb_j)N_0\geq 0$. With this, (27) will be satisfied when $\lambda_{P_R}>0$. With $\lambda_{P_R}>0$, (K5) imply that (18.2) will be satisfied with equality, i.e., the entire relay power, P_R, will be used for transmission. From (K11),

$$\mathbf{\Lambda}_\Phi+\mu(\boldsymbol{h}^*\boldsymbol{h})=\lambda_{P_R}\boldsymbol{I}+s\sum_{j=1}^{J}\nu_j(\boldsymbol{z}_j^*\boldsymbol{z}_j)\succeq\mathbf{0}. \tag{28}$$

With $\lambda_{P_R}>0$, the right hand side of the above expression is a full rank positive definite matrix. This implies that $\mathbf{\Lambda}_\Phi+\mu(\boldsymbol{h}^*\boldsymbol{h})\succ\mathbf{0}$ and $rank(\mathbf{\Lambda}_\Phi+\mu(\boldsymbol{h}^*\boldsymbol{h}))=N$. Since $rank(\mu(\boldsymbol{h}^*\boldsymbol{h}))=1$, this implies that $rank(\mathbf{\Lambda}_\Phi)\geq N-1$. With $\mathbf{\Phi}\neq\mathbf{0}$, (K3) implies that $rank(\mathbf{\Lambda}_\Phi)\neq N$. This means that $rank(\mathbf{\Lambda}_\Phi)=N-1$. This further implies that $rank(\mathbf{\Phi})=1$.

We now show that the solution $\mathbf{\Phi}$ of the optimization problem (17) has rank-1 even for large values of P_R. Let $\mathbf{\Phi}\neq\mathbf{0}$ ($\succeq\mathbf{0}$) and $\mathbf{\Psi}$ ($\succeq\mathbf{0}$) be the optimal solution of (17) with

$$trace(\mathbf{\Phi})+trace(\mathbf{\Psi})=P\leq P_R,$$

and the objective function value $rs>1$ with $1\geq s>0$ and $r>1$. Define

$$\mathbf{\Phi}_0=\frac{\mathbf{\Phi}}{trace(\mathbf{\Phi})+trace(\mathbf{\Psi})}=\frac{\mathbf{\Phi}}{P},$$
$$\mathbf{\Psi}_0=\frac{\mathbf{\Psi}}{trace(\mathbf{\Phi})+trace(\mathbf{\Psi})}=\frac{\mathbf{\Psi}}{P}.$$

It is obvious that the objective function value, rs, in the optimization problem (17) is a non-decreasing function in P_R. As discussed previously for small values of P_R, the optimization problem (17) attains it's maximum value when entire power is used, i.e., $(\mathbf{\Phi},\ \mathbf{\Psi})=(P\mathbf{\Phi}_0,\ P\mathbf{\Psi}_0)=(P_R\mathbf{\Phi}_0,\ P_R\mathbf{\Psi}_0)$. This implies that the objective function value, rs, in (17) is a strictly increasing function in P_R for small values of P_R. We now fix the directional matrices $(\mathbf{\Phi}_0,\ \mathbf{\Psi}_0)$ which are obtained for small values of P_R such that the constraint (18.3) is satisfied with strict inequality. We consider the following two cases.

Case 1: We assume that $\mathbf{\Psi}_0=\mathbf{0}$ or $\boldsymbol{h}\mathbf{\Psi}_0\boldsymbol{h}^*\neq 0$. We rewrite the constraint (18.3) in the following form:

$$c\ \geq\ \Big(a+\frac{\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*}{N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*}\Big). \tag{29}$$

In the above inequality, the derivative of the function $(\frac{\boldsymbol{h}\mathbf{\Phi}\boldsymbol{h}^*}{N_0+\boldsymbol{h}\mathbf{\Psi}\boldsymbol{h}^*})$ w.r.t. P when evaluated at $(P\mathbf{\Phi}_0,\ P\mathbf{\Psi}_0)$ is strictly greater than zero. This implies that the right hand side of the above inequality is also a strictly increasing function in P at $(P\mathbf{\Phi}_0,\ P\mathbf{\Psi}_0)$. Since c in the above inequality is upper bounded due to fixed source power, this inequality will be satisfied only when $c>a$ and P is small. The above analysis implies that if the above inequality is satisfied at $(P_R\mathbf{\Phi}_0,\ P_R\mathbf{\Psi}_0)$, the optimization problem (17) subject to the constraints in (18) will attain its maximum value at $(P_R\mathbf{\Phi}_0,\ P_R\mathbf{\Psi}_0)$, i.e., when the entire available relay power, P_R, is used. When P_R is large such that the above inequality fails to satisfy at $(P_R\mathbf{\Phi}_0,\ P_R\mathbf{\Psi}_0)$, the optimization problem (17) will attain its maximum value at $(P\mathbf{\Phi}_0,\ P\mathbf{\Psi}_0)$, where P $(<P_R)$ is the maximum power at which the above inequality is satisfied at $(P\mathbf{\Phi}_0,\ P\mathbf{\Psi}_0)$. The excess power (P_R-P) will remain unused.

Case 2: In this case, we assume that $\mathbf{\Psi}_0\neq\mathbf{0}$ and $\boldsymbol{h}\mathbf{\Psi}_0\boldsymbol{h}^*=0$. If the inequality in (29) is satisfied at $(P_R\mathbf{\Phi}_0,\ P_R\mathbf{\Psi}_0)$, the analysis presented in Case 1 applies in this case also. When P_R is large such that (29) fails to satisfy at $(P_R\mathbf{\Phi}_0,\ P_R\mathbf{\Psi}_0)$, the optimization problem (17) will attain its maximum value at $\mathbf{\Phi}=P\mathbf{\Phi}_0$ and $\mathbf{\Psi}=\Big(\frac{P_R-Ptrace(\mathbf{\Phi}_0)}{trace(\mathbf{\Psi}_0)}\Big)\mathbf{\Psi}_0$, where P $(<P_R)$ is the maximum power at which (29) is satisfied at $(P\mathbf{\Phi}_0,\ P\mathbf{\Psi}_0)$. The excess power $\big(P_R-Ptrace(\mathbf{\Phi}_0)\big)$ will be used for jamming purposes.

The analysis presented in Case 1 and Case 2 imply that the rank of $\mathbf{\Phi}$ remains constant for all values of P_R.

References

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

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

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

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, NOW Publishers, vol. 5, no. 4-5, 2009.

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

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

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

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

[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[10] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory.*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

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

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

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

[14] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[15] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with finite-alphabet input," *IEEE Commun. Letters*, vol. 17, no. 5, pp. 912-915, May 2013.

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