Amplify-and-Forward Relay Beamforming for Secrecy with Cooperative Jamming and Imperfect CSI

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

***Abstract*—In this paper, we compute worst case secrecy rates in amplify-and-forward (AF) relay beamforming with *cooperative jamming* (CJ) in the presence of *imperfect channel state information* (CSI). A source-destination pair aided by M relays is considered. Number of eavesdroppers J can be more than the number of relays. Out of the M relays, k_1 relays ($1 \leq k_1 \leq M$) act as *data relays* and the remaining $k_2 = M - k_1$ relays act as *jamming relays*. Data relays aid the communication by relaying data in AF mode, and jamming relays cooperate by transmitting jamming signals (artificial noise). The jamming signals are created such that they degrade the eavesdroppers' channels but do not significantly affect the intended receiver's channel, thereby improving secrecy rate. Imperfection in the CSI is modeled using a norm-bounded error model. We solve for the optimum (k_1, k_2) and the weights of data relays and jamming relays that maximize the secrecy rate subject to a total relay power constraint. We relax the rank-one constraint on the complex semi-definite data relays and jamming relays weight matrices and reformulate the optimization problem into a form that can be solved using convex semi-definite programming. Numerical results on the secrecy rate that illustrate the effect of cooperative jamming, imperfect CSI, and number of eavesdroppers are presented.**

keywords: Cooperative relay beamforming, physical layer security, secrecy rate, amplify-and-forward, cooperative jamming, imperfect CSI, multiple eavesdroppers, semi-definite programming.

I. INTRODUCTION

Wireless transmissions are prone to evesdropping due to their broadcast nature. Providing security through physical layer mechanisms where the intended receiver gets the information reliably while the eavesdroppers get no information is an active area of recent research [1]. Secrecy capacity results for fading channels have been widely reported [2], [3]. Also, secure wireless communications via cooperation is witnessing growing research interest [4]. In particular, cooperation based on amplify-and-forward (AF) and decode-and-forward (DF) relaying protocols for secure communication has been investigated in the literature, assuming perfect and imperfect channel state information (CSI) [5], [6], [7].

Secrecy rate can be improved by adding artificially generated noise (jamming signal) to the information bearing signal such that it degrades the channel towards the eavesdropper but does not degrade the intended receiver's channel [8]. This can be achieved by designing the jamming signal to be orthogonal to the information signal when it reaches the intended receiver, assuming perfect knowledge of CSI. When the sender node has more than one transmit antenna, the additional antennas can be used to transmit jamming signals. Alternately, if 'helper nodes' are available, they can be used to transmit the jamming signals. The idea of helper nodes transmitting jamming signals to improve secrecy rate - referred to as *cooperative jamming (CJ)* - has been attracting increased research attention [4], [9]- [12]. Our new contribution in this paper is the evaluation of secrecy rates in an *amplify-and-forward (AF) relay beamforming* scenario in the presence of *cooperative jamming* and *imperfect CSI*. Our work is different from the above works on CJ as follows.

In the secrecy rate computation in [4], the following two scenarios are considered. In one scenario, all the M relays are used for relaying data in either AF or DF mode, and there is no cooperative jamming. In the second scenario, all the relays are used for cooperative jamming, and there is no data relaying. These are two extreme cases of the use of relays, which are not necessarily optimal. A more general formulation would be to allow k_1 out of M relays ($1 \leq k_1 \leq M$) to act as data relays in AF or DF mode and the remaining $k_2 = M - k_1$ relays to act as cooperative jamming relays (see Fig. 1), and solve for the optimum (k_1, k_2) that maximizes the secrecy rate. In this paper, we consider this general formulation. In particular, we consider AF protocol for data relaying. We also consider that the knowledge of the CSI is imperfect, and the imperfection is modeled using a norm-bounded CSI error model.

In the above setting, our goal is to solve for the optimum relay beamforming weights (weights of both data relays and jamming relays) that maximize the worst case secrecy rate subject to a total relay power constraint and CSI error constraints. The solution approach adopted is to relax the rank-one constraint on the complex semi-definite weight matrices of the data relays and jamming relays and reformulate the optimization problem into a form that can be solved using convex semi-definite programming.

II. SYSTEM MODEL

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 $\{E_1, E_2, \cdots, E_J\}$, where J can be greater than M (i.e., more number of eavesdroppers than the number of relays). In addition to the links from relays to destination node and relays to eavesdropper nodes, we assume direct links from source to destination node and source to eavesdropper nodes. The complex fading channel gains between source to relays are denoted by $\{\gamma_1^*, \gamma_2^*, \cdots, \gamma_M^*\}$. Likewise, the channel gains between relays to destination and relays to the jth eavesdropper are denoted by $\{\alpha_1^*, \alpha_2^*, \cdots, \alpha_M^*\}$ and $\{\beta_{1j}^*, \beta_{2j}^*, \cdots, \beta_{Mj}^*\}$, respectively, where $j = 1, \cdots, J$. The channel gains on the direct links from source to destination and source to jth eavesdropper are

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

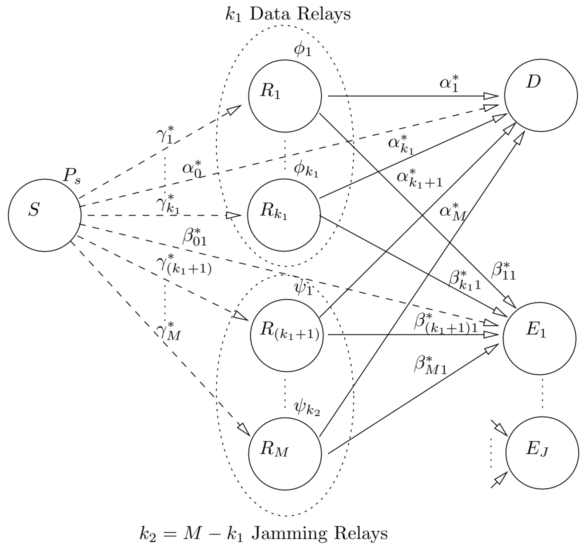


Fig. 1. Relay beamforming with data relays and cooperative jamming relays.

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 $\sigma^2_{\gamma_i^*}$, $\sigma^2_{\alpha_0^*}$, $\sigma^2_{\alpha_i^*}$, $\sigma^2_{\beta_{0j}^*}$, and $\sigma^2_{\beta_{ij}^*}$. Let P_0 denote the total transmit power budget in the system (i.e., source power plus relays power).

A. Relay Beamforming Using AF with Cooperative Jamming

The source transmits data in the first hop of transmission. Let x be the source symbol transmitted from the source with $\mathbb{E}\{|x|^2\} = 1$. In the second hop of transmission, let k_1 out of M relays, $1 \leq k_1 \leq M$, are selected to act as the data relays to aid communication from S to D and remaining $k_2 = M - k_1$ relays are selected to act as jamming relays for the transmission of jamming signals. Let P_s denote the power transmitted by the source in the first hop of transmission. Let $\{\phi_1, \phi_2, \cdots, \phi_{k_1}\}$ denote the complex weights applied on the transmitted signals from the k_1 data relays and let $\{\psi_1, \psi_2, \cdots, \psi_{k_2}\}$ denote the complex weights applied on the transmitted jamming signals from the k_2 jamming relays in the second hop of transmission. Let $\boldsymbol{y}_R^{k_1}$, y_{D_1} and $y_{E_{1j}}$ denote the received signals at the k_1 data 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

$$\boldsymbol{y}_R^{k_1} = \sqrt{P_s}\boldsymbol{\gamma}^{k_1 *} x + \boldsymbol{\eta}_R^{k_1}, \quad (1)$$

$$y_{D_1} = \sqrt{P_s}\alpha_0^* x + \eta_{D_1}, \quad (2)$$

$$y_{E_{1j}} = \sqrt{P_s}\beta_{0j}^* x + \eta_{E_{1j}}, \qquad j = 1, \cdots, J, \quad (3)$$

$$\begin{aligned} y_{D_2} &= \boldsymbol{y}_R^{k_1 T} diag(\boldsymbol{\phi}^{k_1})\boldsymbol{\alpha}^{k_1 *} + \boldsymbol{\alpha}^{k_2 \dagger} diag(\boldsymbol{\psi}^{k_2})\boldsymbol{z}^{k_2} + \eta_{D_2} \\ &= \sqrt{P_s}\boldsymbol{\gamma}^{k_1 \dagger} diag^\dagger(\boldsymbol{\alpha}^{k_1})\boldsymbol{\phi}^{k_1} x + \boldsymbol{\eta}_R^{k_1 T}\ diag^\dagger(\boldsymbol{\alpha}^{k_1})\boldsymbol{\phi}^{k_1} + \\ &\qquad \boldsymbol{\alpha}^{k_2 \dagger} diag(\boldsymbol{\psi}^{k_2})\boldsymbol{z}^{k_2} + \eta_{D_2}, \quad (4) \end{aligned}$$

$$\begin{aligned} y_{E_{2j}} &= \boldsymbol{y}_R^{k_1 T} diag(\boldsymbol{\phi}^{k_1})\boldsymbol{\beta}_j^{k_1 *} + \boldsymbol{\beta}_j^{k_2 \dagger} diag(\boldsymbol{\psi}^{k_2})\boldsymbol{z}^{k_2} + \eta_{E_{2j}} \\ &= \sqrt{P_s}\boldsymbol{\gamma}^{k_1 \dagger} diag^\dagger(\boldsymbol{\beta}_j^{k_1})\boldsymbol{\phi}^{k_1} x + \boldsymbol{\eta}_R^{k_1 T}\ diag^\dagger(\boldsymbol{\beta}_j^{k_1})\boldsymbol{\phi}^{k_1} + \\ &\qquad \boldsymbol{\beta}_j^{k_2 \dagger} diag(\boldsymbol{\psi}^{k_2})\boldsymbol{z}^{k_2} + \eta_{E_{2j}},\ \forall j = 1, \cdots, J, \quad (5) \end{aligned}$$

where $\boldsymbol{\gamma}^{k_1 *} = [\gamma_1^*, \cdots, \gamma_{k_1}^*]^T$, $\boldsymbol{\eta}_R^{k_1} = [\eta_{R_1}, \cdots, \eta_{R_{k_1}}]^T$, $\boldsymbol{\phi}^{k_1} = [\phi_1, \cdots, \phi_{k_1}]^T$, $\boldsymbol{\psi}^{k_2} = [\psi_1, \cdots, \psi_{k_2}]^T$, $\boldsymbol{\alpha}^{k_1 *} = [\alpha_1^*, \cdots, \alpha_{k_1}^*]^T$, $\boldsymbol{\alpha}^{k_2 *} = [\alpha_{(k_1+1)}^*, \cdots, \alpha_M^*]^T$, $\boldsymbol{\beta}_j^{k_1 *} = [\beta_{1j}^*, \cdots, \beta_{k_1 j}^*]^T$, $\boldsymbol{\beta}_j^{k_2 *} = [\beta_{(k_1+1)j}^*, \cdots, \beta_{Mj}^*]^T$, $j = 1, \cdots, J$, $\boldsymbol{z}^{k_2} = [z_1, \cdots, z_{k_2}]^T$, and $[.]^T$, $(.)^*$, $[.]^\dagger$ denote transpose, conjugate, conjugate transpose operations, respectively. The noise components, η's and z's are assumed to be i.i.d. $\mathcal{CN}(0, N_0)$ and $\mathcal{CN}(0, 1)$, respectively. Also, η's and z's are assumed to be independent.

1) Secrecy Rate with Perfect CSI: Let $R_D^{k_1 k_2}$ and $R_{E_j}^{k_1 k_2}$ denote the information rates at the destination D and jth eavesdropper E_j, respectively. Using (2) and (4), the expression for the information rate at the destination D is

$$R_D^{k_1 k_2} = \frac{1}{2}\log_2\left(1 + \frac{P_s \alpha_0^* \alpha_0}{N_0} + \frac{P_s t_{11}}{t_{12}}\right), \quad (6)$$

where

$$\begin{aligned} t_{11} &= \boldsymbol{\phi}^{k_1 \dagger} diag(\boldsymbol{\alpha}^{k_1})\boldsymbol{\gamma}^{k_1}\boldsymbol{\gamma}^{k_1 \dagger} diag^\dagger(\boldsymbol{\alpha}^{k_1})\boldsymbol{\phi}^{k_1}, \\ t_{12} &= N_0 + N_0 \boldsymbol{\phi}^{k_1 \dagger} diag^\dagger(\boldsymbol{\alpha}^{k_1}) diag(\boldsymbol{\alpha}^{k_1})\boldsymbol{\phi}^{k_1} + \\ &\qquad \boldsymbol{\psi}^{k_2 \dagger} diag^\dagger(\boldsymbol{\alpha}^{k_2}) diag(\boldsymbol{\alpha}^{k_2})\boldsymbol{\psi}^{k_2}. \end{aligned}$$

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

$$R_{E_j}^{k_1 k_2} = \frac{1}{2}\log_2\left(1 + \frac{P_s \beta_{0j}^* \beta_{0j}}{N_0} + \frac{P_s t_{21}}{t_{22}}\right), \quad (7)$$

where

$$\begin{aligned} t_{21} &= \boldsymbol{\phi}^{k_1 \dagger} diag(\boldsymbol{\beta}_j^{k_1})\boldsymbol{\gamma}^{k_1}\boldsymbol{\gamma}^{k_1 \dagger} diag^\dagger(\boldsymbol{\beta}_j^{k_1})\boldsymbol{\phi}^{k_1}, \\ t_{22} &= N_0 + N_0 \boldsymbol{\phi}^{k_1 \dagger} diag^\dagger(\boldsymbol{\beta}_j^{k_1}) diag(\boldsymbol{\beta}_j^{k_1})\boldsymbol{\phi}^{k_1} + \\ &\qquad \boldsymbol{\psi}^{k_2 \dagger} diag^\dagger(\boldsymbol{\beta}_j^{k_2}) diag(\boldsymbol{\beta}_j^{k_2})\boldsymbol{\psi}^{k_2},\ \forall j = 1, \cdots, J. \end{aligned}$$

The total power transmitted by all M relays is $P_s \boldsymbol{\phi}^{k_1 \dagger} diag(\boldsymbol{\gamma}^{k_1}) diag^\dagger(\boldsymbol{\gamma}^{k_1})\boldsymbol{\phi}^{k_1} + N_0 \boldsymbol{\phi}^{k_1 \dagger}\boldsymbol{\phi}^{k_1} + \boldsymbol{\psi}^{k_2 \dagger}\boldsymbol{\psi}^{k_2}$. The achievable secrecy rate $R_s^{k_1 k_2}$ for (k_1, k_2) relay combination is [4]:

$$\begin{aligned} R_s^{k_1 k_2} &= \max_{\boldsymbol{\phi}^{k_1},\ \boldsymbol{\psi}^{k_2}} \ \min_{j:1,\cdots,J} \ (R_D^{k_1 k_2} - R_{E_j}^{k_1 k_2}) \\ &= \max_{\boldsymbol{\phi}^{k_1},\ \boldsymbol{\psi}^{k_2}} \ \min_{j:1,\cdots,J} \ \frac{1}{2}\log_2 t_3 \quad (8) \end{aligned}$$

s.t.

$$\begin{aligned} & P_s \boldsymbol{\phi}^{k_1 \dagger} diag(\boldsymbol{\gamma}^{k_1}) diag^\dagger(\boldsymbol{\gamma}^{k_1})\boldsymbol{\phi}^{k_1} + N_0 \boldsymbol{\phi}^{k_1 \dagger}\boldsymbol{\phi}^{k_1} \\ & \qquad + \ \boldsymbol{\psi}^{k_2 \dagger}\boldsymbol{\psi}^{k_2} \leq \ P_0 - P_s, \quad (9) \\ & \text{where} \quad t_3 = \frac{1 + \frac{P_s \alpha_0^* \alpha_0}{N_0} + \frac{P_s t_{11}}{t_{12}}}{1 + \frac{P_s \beta_{0j}^* \beta_{0j}}{N_0} + \frac{P_s t_{21}}{t_{22}}}. \end{aligned}$$

Defining $\boldsymbol{\Phi}^{k_1} \triangleq \boldsymbol{\phi}^{k_1}\boldsymbol{\phi}^{k_1 \dagger}$ and $\boldsymbol{\Psi}^{k_2} \triangleq \boldsymbol{\psi}^{k_2}\boldsymbol{\psi}^{k_2 \dagger}$, the above secrecy rate expression can be written in the following equivalent optimization form:

$$R_s^{k_1 k_2} = \max_{\boldsymbol{\Phi}^{k_1},\ \boldsymbol{\Psi}^{k_2}} \ \min_{j:1,\cdots,J} \ \frac{1}{2}\log_2 t_4 \quad (10)$$

$$\text{s.t.} \quad \mathbf{\Phi}^{k_1} \succeq 0,\ rank(\mathbf{\Phi}^{k_1}) = 1,\ \mathbf{\Psi}^{k_2} \succeq 0,\ rank(\mathbf{\Psi}^{k_2}) = 1,$$
$$tr(\mathbf{\Phi}^{k_1}(P_s diag(\boldsymbol{\gamma}^{k_1}) diag^{\dagger}(\boldsymbol{\gamma}^{k_1}) + N_0 \boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \leq P_0 - P_s, \quad (11)$$
$$\text{where} \quad t_4 = \frac{(1 + \frac{P_s \alpha_0^* \alpha_0}{N_0} + \frac{P_s t_{411}}{t_{412}})}{(1 + \frac{P_s \beta_{0j}^* \beta_{0j}}{N_0} + \frac{P_s t_{421}}{t_{422}})},$$
$$t_{411} = tr(\mathbf{\Phi}^{k_1} diag(\boldsymbol{\alpha}^{k_1}) \boldsymbol{\gamma}^{k_1} \boldsymbol{\gamma}^{k_1 \dagger} diag^{\dagger}(\boldsymbol{\alpha}^{k_1})),$$
$$t_{412} = N_0 + N_0 tr(\mathbf{\Phi}^{k_1} diag(\boldsymbol{\alpha}^{k_1}) diag^{\dagger}(\boldsymbol{\alpha}^{k_1})) + tr(\mathbf{\Psi}^{k_2} diag(\boldsymbol{\alpha}^{k_2}) diag^{\dagger}(\boldsymbol{\alpha}^{k_2})),$$
$$t_{421} = tr(\mathbf{\Phi}^{k_1} diag(\boldsymbol{\beta}_j^{k_1}) \boldsymbol{\gamma}^{k_1} \boldsymbol{\gamma}^{k_1 \dagger} diag^{\dagger}(\boldsymbol{\beta}_j^{k_1})),$$
$$t_{422} = N_0 + N_0 tr(\mathbf{\Phi}^{k_1} diag(\boldsymbol{\beta}_j^{k_1}) diag^{\dagger}(\boldsymbol{\beta}_j^{k_1})) + tr(\mathbf{\Psi}^{k_2} diag(\boldsymbol{\beta}_j^{k_2}) diag^{\dagger}(\boldsymbol{\beta}_j^{k_2})).$$

Relaxing the rank constraint on $\mathbf{\Phi}^{k_1},\ \mathbf{\Psi}^{k_2}$ and dropping the logarithm [5]- [7], [10], [13], the optimization problem to compute the above secrecy rate expression can be written in the following equivalent optimization form:

$$\max_{\mathbf{\Phi}^{k_1},\ \mathbf{\Psi}^{k_2}} \ \min_{j:1,\cdots,J} \ t_4 \quad (12)$$
$$\text{s.t.} \quad \mathbf{\Phi}^{k_1} \succeq 0, \quad \mathbf{\Psi}^{k_2} \succeq 0,$$
$$tr(\mathbf{\Phi}^{k_1}(P_s diag(\boldsymbol{\gamma}^{k_1}) diag^{\dagger}(\boldsymbol{\gamma}^{k_1}) + N_0 \boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \leq P_0 - P_s. \quad (13)$$

B. Imperfect CSI Model

We consider imperfect CSI, modeled as $\gamma_i^* = \widehat{\gamma}_i^* + e_{\gamma_i^*}^*, i = 1,\cdots,k_1,\ \alpha_0^* = \widehat{\alpha}_0^* + e_{\alpha_0^*}^*,\ \beta_{0j}^* = \widehat{\beta}_{0j}^* + e_{\beta_{0j}^*}^*, j = 1,\cdots,J,$ $\boldsymbol{\alpha}^{k_1*} = \widehat{\boldsymbol{\alpha}}^{k_1*} + \boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}}^*,\ \boldsymbol{\alpha}^{k_2*} = \widehat{\boldsymbol{\alpha}}^{k_2*} + \boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}}^*,\ \boldsymbol{\beta}_j^{k_1*} = \widehat{\boldsymbol{\beta}}_j^{k_1*} + \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}}^*, j = 1,\cdots,J,\ \boldsymbol{\beta}_j^{k_2*} = \widehat{\boldsymbol{\beta}}_j^{k_2*} + \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}}^*, j = 1,\cdots,J,$ where γ_i^*'s, α_0^*, β_{0j}^*'s, $\boldsymbol{\alpha}^{k_1*}$, $\boldsymbol{\alpha}^{k_2*}$, $\boldsymbol{\beta}_j^{k_1*}$'s, $\boldsymbol{\beta}_j^{k_2*}$'s are the true CSI, $\widehat{\gamma}_i^*$'s, $\widehat{\alpha}_0^*$, $\widehat{\beta}_{0j}^*$'s, $\widehat{\boldsymbol{\alpha}}^{k_1*}$, $\widehat{\boldsymbol{\alpha}}^{k_2*}$ $\widehat{\boldsymbol{\beta}}_j^{k_1*}$'s, $\widehat{\boldsymbol{\beta}}_j^{k_2*}$'s are the corresponding imperfect CSI, and $e_{\gamma_i^*}^*$'s, $e_{\alpha_0^*}^*$, $e_{\beta_{0j}^*}^*$'s, $\boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}}^*$, $\boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}}^*$, $\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}}^*$'s, $\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}}^*$'s are the additive errors in the CSI. We consider a norm-bounded CSI error model, where it is assumed that

$$|e_{\gamma_i^*}| \leq \epsilon_{\gamma_i^*},\ |e_{\alpha_0^*}| \leq \epsilon_{\alpha_0^*},\ |e_{\beta_{0j}^*}| \leq \epsilon_{\beta_{0j}^*},\ \|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}}\| \leq \epsilon_{\boldsymbol{\alpha}^{k_1*}},$$
$$\|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}}\| \leq \epsilon_{\boldsymbol{\alpha}^{k_2*}},\ \|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}}\| \leq \epsilon_{\boldsymbol{\beta}_j^{k_1*}},\ \|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}}\| \leq \epsilon_{\boldsymbol{\beta}_j^{k_2*}}.$$

In addition to the above assumptions, we assume the knowledge of the combined channel gain vectors $(\boldsymbol{\gamma\alpha})^{k_1*} = [\gamma_1^*\alpha_1^*,\cdots,\gamma_{k_1}^*\alpha_{k_1}^*]^T$ and $(\boldsymbol{\gamma\beta})_j^{k_1*} = [\gamma_1^*\beta_{1j}^*,\cdots,\gamma_{k_1}^*\beta_{k_1j}^*]^T$, $j = 1,\cdots,J$. In support of this assumption, we note that estimates of the product channel gains $(\boldsymbol{\gamma\alpha})^{k_1*}$ and $(\boldsymbol{\gamma\beta})_j^{k_1*}$'s can be obtained using the techniques proposed in [14], [15]. The imperfections in the knowledge of these channel vectors are modeled as $(\boldsymbol{\gamma\alpha})^{k_1*} = (\widehat{\boldsymbol{\gamma\alpha}})^{k_1*} + \boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}}^*$ and $(\boldsymbol{\gamma\beta})_j^{k_1*} = (\widehat{\boldsymbol{\gamma\beta}})_j^{k_1*} + \boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}^*$, where $(\boldsymbol{\gamma\alpha})^{k_1*}$ and $(\boldsymbol{\gamma\beta})_j^{k_1*}$ are the perfect CSI, $(\widehat{\boldsymbol{\gamma\alpha}})^{k_1*}$ and $(\widehat{\boldsymbol{\gamma\beta}})_j^{k_1*}$ are the corresponding imperfect CSI, and $\boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}}^*$ and $\boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}^*$ are the additive errors in the CSI. A norm-bounded error model is assumed, i.e., $\|\boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}}\| \leq \epsilon_{(\boldsymbol{\gamma\alpha})^{k_1*}}$ and $\|\boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}\| \leq \epsilon_{(\boldsymbol{\gamma\beta})_j^{k_1*}}$, $j = 1,\cdots,J$.

III. Secrecy rate for AF Relay Beamforming with CJ and Imperfect CSI

The optimization problem (12) for computing the worst case secrecy rate of AF relay beamforming can be written in the following form:

$$\max_{\mathbf{\Phi}^{k_1},\ \mathbf{\Psi}^{k_2}} \ \min_{j:1,\cdots,J} \ \min_{\substack{e_{\gamma_i^*},\ e_{\alpha_0^*},\ \boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}},\ \boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}},\\ \boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}},\ e_{\beta_{0j}^*},\ \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}},\ \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}},\ \boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}}} t_5 \quad (14)$$
$$\text{s.t.} \quad \forall i:1,\cdots,k_1,\ |e_{\gamma_i^*}| \leq \epsilon_{\gamma_i^*}\ |e_{\alpha_0^*}| \leq \epsilon_{\alpha_0^*},$$
$$\|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}}\| \leq \epsilon_{\boldsymbol{\alpha}^{k_1*}},\ \|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}}\| \leq \epsilon_{\boldsymbol{\alpha}^{k_2*}},\ \|\boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}}\| \leq \epsilon_{(\boldsymbol{\gamma\alpha})^{k_1*}},$$
$$|e_{\beta_{0j}^*}| \leq \epsilon_{\beta_{0j}^*},\ \|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}}\| \leq \epsilon_{\boldsymbol{\beta}_j^{k_1*}},\ \|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}}\| \leq \epsilon_{\boldsymbol{\beta}_j^{k_2*}},$$
$$\|\boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}\| \leq \epsilon_{(\boldsymbol{\gamma\beta})_j^{k_1*}},\ \mathbf{\Phi}^{k_1} \succeq 0,\ \mathbf{\Psi}^{k_2} \succeq 0,$$
$$tr(\mathbf{\Phi}^{k_1}(P_s diag(\widehat{\boldsymbol{\gamma}}^{k_1} + e_{\boldsymbol{\gamma}^{k_1*}}) diag^{\dagger}(\widehat{\boldsymbol{\gamma}}^{k_1} + e_{\boldsymbol{\gamma}^{k_1*}}) + N_0\boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \leq P_0 - P_s, \quad (15)$$
$$\text{where} \quad \widehat{\boldsymbol{\gamma}}^{k_1*} = [\widehat{\gamma}_1^*,\cdots,\widehat{\gamma}_{k_1}^*]^T,\ e_{\boldsymbol{\gamma}^{k_1*}}^* = [e_{\boldsymbol{\gamma}_1^*}^*,\cdots,e_{\boldsymbol{\gamma}_{k_1}^*}^*]^T,$$
$$t_5 = \frac{1 + \frac{P_s(\widehat{\alpha}_0 + e_{\alpha_0^*})^*(\widehat{\alpha}_0 + e_{\alpha_0^*})}{N_0} + \frac{P_s t_{511}}{t_{512}}}{1 + \frac{P_s(\widehat{\beta}_{0j} + e_{\beta_{0j}^*})^*(\widehat{\beta}_{0j} + e_{\beta_{0j}^*})}{N_0} + \frac{P_s t_{521}}{t_{522}}},$$
$$t_{511} = ((\widehat{\boldsymbol{\gamma\alpha}})^{k_1} + \boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}})^{\dagger} \mathbf{\Phi}^{k_1} ((\widehat{\boldsymbol{\gamma\alpha}})^{k_1} + \boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}}),$$
$$t_{512} = N_0 + N_0(\widehat{\boldsymbol{\alpha}}^{k_1} + \boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}})^{\dagger} \boldsymbol{A}^{k_1} (\widehat{\boldsymbol{\alpha}}^{k_1} + \boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}}) + (\widehat{\boldsymbol{\alpha}}^{k_2} + \boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}})^{\dagger} \boldsymbol{B}^{k_2} (\widehat{\boldsymbol{\alpha}}^{k_2} + \boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}}),$$
$$t_{521} = ((\widehat{\boldsymbol{\gamma\beta}})_j^{k_1} + \boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}})^{\dagger} \mathbf{\Phi}^{k_1} ((\widehat{\boldsymbol{\gamma\beta}})_j^{k_1} + \boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}),$$
$$t_{522} = N_0 + N_0(\widehat{\boldsymbol{\beta}}_j^{k_1} + \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}})^{\dagger} \boldsymbol{A}^{k_1} (\widehat{\boldsymbol{\beta}}_j^{k_1} + \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}}) + (\widehat{\boldsymbol{\beta}}_j^{k_2} + \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}})^{\dagger} \boldsymbol{B}^{k_2} (\widehat{\boldsymbol{\beta}}_j^{k_2} + \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}}),$$
$$\boldsymbol{A}^{k_1} \triangleq diag(diag(\mathbf{\Phi}^{k_1})) \text{ and } \boldsymbol{B}^{k_2} \triangleq diag(diag(\mathbf{\Psi}^{k_2})).$$

$$\text{Let} \quad a = \min_{e_{\alpha_0^*}} \left(1 + \frac{P_s(\widehat{\alpha}_0 + e_{\alpha_0^*})^*(\widehat{\alpha}_0 + e_{\alpha_0^*})}{N_0}\right) \quad (16)$$
$$\text{s.t.}\ |e_{\alpha_0^*}| \leq \epsilon_{\alpha_0^*}. \quad (17)$$

Using the method of Lagrangian, the dual of the above problem is the following SDP problem [16]:

$$a = \max_{\eta,\ \nu} \ \eta \quad (18)$$
$$\text{s.t.}\ \nu \geq 0,\ \begin{bmatrix} (\frac{P_s}{N_0} + \nu) & \frac{P_s}{N_0}\widehat{\alpha}_0 \\ \widehat{\alpha}_0^* \frac{P_s}{N_0} & \widehat{\alpha}_0^* \frac{P_s}{N_0} \widehat{\alpha}_0 + 1 - \eta - \nu\epsilon_{\alpha_0^*}^2 \end{bmatrix} \succeq 0. \quad (19)$$

$$\text{Let} \quad b_j = \max_{e_{\beta_{0j}^*}} \left(1 + \frac{P_s(\widehat{\beta}_{0j} + e_{\beta_{0j}^*})^*(\widehat{\beta}_{0j} + e_{\beta_{0j}^*})}{N_0}\right), \quad (20)$$
$$\forall j:1,\cdots,J \quad \text{s.t.} \quad |e_{\beta_{0j}^*}| \leq \epsilon_{\beta_{0j}^*}. \quad (21)$$

The above problem can be written in the following SDP form:

$$b_j = -\max_{\eta,\ \nu} \ \eta, \quad \forall j:1,\cdots,J \quad \text{s.t.}\ \nu \geq 0, \quad (22)$$
$$\begin{bmatrix} (-\frac{P_s}{N_0} + \nu) & -\frac{P_s}{N_0}\widehat{\beta}_{0j} \\ -\widehat{\beta}_{0j}^* \frac{P_s}{N_0} & -\widehat{\beta}_{0j}^* \frac{P_s}{N_0} \widehat{\beta}_{0j} - 1 - \eta - \nu\epsilon_{\beta_{0j}^*}^2 \end{bmatrix} \succeq 0. \quad (23)$$

Since the objective function of the optimization problem (14) is independent of $e_{\gamma_i^*}$, we modify the power constraint

$$tr(\mathbf{\Phi}^{k_1}(P_s diag(\widehat{\boldsymbol{\gamma}}^{k_1}+e_{\boldsymbol{\gamma}^{k_1*}}) diag^{\dagger}(\widehat{\boldsymbol{\gamma}}^{k_1}+e_{\boldsymbol{\gamma}^{k_1*}})+N_0\boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \le P_0 - P_s,$$
$$|e_{\gamma_i^*}| \le \epsilon_{\gamma_i^*},\ \forall i:1,\cdots,k_1,$$

which is a function of $e_{\gamma_i^*}$, as follows:

$$\max_{e_{\gamma_i^*}} \ tr(\mathbf{\Phi}^{k_1}(P_s diag(\widehat{\boldsymbol{\gamma}}^{k_1}+e_{\boldsymbol{\gamma}^{k_1*}}) diag^{\dagger}(\widehat{\boldsymbol{\gamma}}^{k_1}+e_{\boldsymbol{\gamma}^{k_1*}})+N_0\boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \le P_0 - P_s,$$
$$\text{s.t.} \quad |e_{\gamma_i^*}| \le \epsilon_{\gamma_i^*},\ \forall i:1,\cdots,k_1.$$

Rewriting it in the following equivalent form, we have

$$tr(\mathbf{\Phi}^{k_1}(P_s diag(\boldsymbol{v})+N_0\boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \ \le \ P_0 - P_s, \quad (24)$$

where $\boldsymbol{v}=[v_1,v_2,\cdots,v_{k_1}]^T$, and $\forall i:1,\cdots,k_1$,

$$v_i = \max_{e^*_{\gamma_i^*}} \ (\widehat{\gamma}_i + e_{\gamma_i^*})^*(\widehat{\gamma}_i + e_{\gamma_i^*}) \quad \text{s.t.} \quad |e_{\gamma_i^*}| \le \epsilon_{\gamma_i^*},$$

which can be written in the following SDP form:

$$v_i = -\max_{\eta,\ \nu} \ \eta, \quad \forall i:1,\cdots,k_1$$
$$\text{s.t. } \nu \ge 0, \ \begin{bmatrix} (-1+\nu) & -\widehat{\gamma}_i \\ -\widehat{\gamma}_i^* & -\widehat{\gamma}_i^*\widehat{\gamma}_i - \eta - \nu\epsilon^2_{\gamma_i} \end{bmatrix} \succeq 0.$$

Substituting the values of a and $b_j,\ j:1,\cdots,J$ and the power constraint (24) in the optimization problem (14), we have

$$\max_{\mathbf{\Phi}^{k_1},\ \mathbf{\Psi}^{k_2}} \ \min_{j:1,\cdots,J} \ \min_{\substack{e_{\boldsymbol{\alpha}^{k_1*}},\ e_{\boldsymbol{\alpha}^{k_2*}},\ e_{(\boldsymbol{\gamma\alpha})^{k_1*}}, \\ e_{\boldsymbol{\beta}_j^{k_1*}},\ e_{\boldsymbol{\beta}_j^{k_2*}},\ e_{(\boldsymbol{\gamma\beta})_j^{k_1*}}}} \frac{a+P_s\frac{t_{511}}{t_{512}}}{b_j+P_s\frac{t_{521}}{t_{522}}}, \ (25)$$
$$\text{s.t.} \quad \mathbf{\Phi}^{k_1}\succeq 0,\ \mathbf{\Psi}^{k_2}\succeq 0,$$
$$\|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}}\| \le \epsilon_{\boldsymbol{\alpha}^{k_1*}},\ \|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}}\| \le \epsilon_{\boldsymbol{\alpha}^{k_2*}},$$
$$\|\boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}}\| \le \epsilon_{(\boldsymbol{\gamma\alpha})^{k_1*}},\ \|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}}\| \le \epsilon_{\boldsymbol{\beta}_j^{k_1*}},$$
$$\|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}}\| \le \epsilon_{\boldsymbol{\beta}_j^{k_2*}},\ \|\boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}\| \le \epsilon_{(\boldsymbol{\gamma\beta})_j^{k_1*}},$$
$$tr(\mathbf{\Phi}^{k_1}(P_s diag(\boldsymbol{v})+N_0\boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \ \le \ P_0 - P_s, \ (26)$$

We transform the innermost minimization in the optimization problem (25) as

$$\max_{\substack{e_{\boldsymbol{\alpha}^{k_1*}},\ e_{\boldsymbol{\alpha}^{k_2*}},\ e_{(\boldsymbol{\gamma\alpha})^{k_1*}},\ e_{\boldsymbol{\beta}_j^{k_1*}},\ e_{\boldsymbol{\beta}_j^{k_2*}} \\ e_{(\boldsymbol{\gamma\beta})_j^{k_1*}},t_6,\ t_7,\ t_8,\ t_{9j},\ t_{10j},\ t_{11j}}} \frac{a+P_s\frac{t_6}{t_7+t_8}}{b_j+P_s\frac{t_{9j}}{t_{10j}+t_{11j}}}, \quad (27)$$

with the constraints written in the equivalent LMIs (Linear Matrix Inequalities) using S-procedure [16] as follows:

$$\forall \boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}} \ \text{s.t.} \ \|\boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}}\| \le \epsilon_{(\boldsymbol{\gamma\alpha})^{k_1*}} \implies$$
$$-((\widehat{\boldsymbol{\gamma\alpha}})^{k_1}+\boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}})^{\dagger}\mathbf{\Phi}^{k_1}((\widehat{\boldsymbol{\gamma\alpha}})^{k_1}+\boldsymbol{e}_{(\boldsymbol{\gamma\alpha})^{k_1*}})+t_6 \le 0$$
$$\iff \quad \lambda \ge 0, \quad \boldsymbol{C}_{\lambda} \triangleq$$
$$\begin{bmatrix} \mathbf{\Phi}^{k_1}+\lambda\boldsymbol{I} & \mathbf{\Phi}^{k_1\dagger}(\widehat{\boldsymbol{\gamma\alpha}})^{k_1} \\ (\widehat{\boldsymbol{\gamma\alpha}})^{k_1\dagger}\mathbf{\Phi}^{k_1} & (\widehat{\boldsymbol{\gamma\alpha}})^{k_1\dagger}\mathbf{\Phi}^{k_1}(\widehat{\boldsymbol{\gamma\alpha}})^{k_1}-t_6-\lambda\epsilon^2_{(\boldsymbol{\gamma\alpha})^{k_1*}} \end{bmatrix} \succeq 0,$$
$$\forall \boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}} \ \text{s.t.} \ \|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}}\| \le \epsilon_{\boldsymbol{\alpha}^{k_1*}} \implies$$
$$N_0(\widehat{\boldsymbol{\alpha}}^{k_1}+\boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}})^{\dagger}\boldsymbol{A}^{k_1}(\widehat{\boldsymbol{\alpha}}^{k_1}+\boldsymbol{e}_{\boldsymbol{\alpha}^{k_1*}})+N_0-t_7 \le 0$$
$$\iff \quad \mu \ge 0, \quad \boldsymbol{C}_{\mu} \triangleq$$
$$\begin{bmatrix} -N_0\boldsymbol{A}^{k_1}+\mu\boldsymbol{I} & -N_0\boldsymbol{A}^{k_1\dagger}\widehat{\boldsymbol{\alpha}}^{k_1} \\ -N_0\widehat{\boldsymbol{\alpha}}^{k_1\dagger}\boldsymbol{A}^{k_1} & -N_0\widehat{\boldsymbol{\alpha}}^{k_1\dagger}\boldsymbol{A}^{k_1}\widehat{\boldsymbol{\alpha}}^{k_1}-N_0+t_7-\mu\epsilon^2_{(\boldsymbol{\alpha})^{k_1*}} \end{bmatrix} \succeq 0,$$
$$\forall \boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}} \ \text{s.t.} \ \|\boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}}\| \le \epsilon_{\boldsymbol{\alpha}^{k_2*}} \implies$$
$$(\widehat{\boldsymbol{\alpha}}^{k_2}+\boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}})^{\dagger}\boldsymbol{B}^{k_2}(\widehat{\boldsymbol{\alpha}}^{k_2}+\boldsymbol{e}_{\boldsymbol{\alpha}^{k_2*}})-t_8 \le 0$$
$$\iff \quad \xi \ge 0, \quad \boldsymbol{C}_{\xi} \triangleq$$
$$\begin{bmatrix} -\boldsymbol{B}^{k_2}+\xi\boldsymbol{I} & -\boldsymbol{B}^{k_2\dagger}\widehat{\boldsymbol{\alpha}}^{k_2} \\ -\widehat{\boldsymbol{\alpha}}^{k_2\dagger}\boldsymbol{B}^{k_2} & -\widehat{\boldsymbol{\alpha}}^{k_2\dagger}\boldsymbol{B}^{k_2}\widehat{\boldsymbol{\alpha}}^{k_2}+t_8-\xi\epsilon^2_{(\boldsymbol{\alpha})^{k_2*}} \end{bmatrix} \succeq 0,$$
$$\forall \boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}} \ s.t. \ \|\boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}}\| \le \epsilon_{(\boldsymbol{\gamma\beta})_j^{k_1*}} \implies$$
$$((\widehat{\boldsymbol{\gamma\beta}})_j^{k_1}+\boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}})^{\dagger}\mathbf{\Phi}^{k_1}((\widehat{\boldsymbol{\gamma\beta}})_j^{k_1}+\boldsymbol{e}_{(\boldsymbol{\gamma\beta})_j^{k_1*}})-t_{9j} \le 0$$
$$\iff \quad \lambda_j \ge 0, \quad \boldsymbol{C}_{\lambda_j} \triangleq$$
$$\begin{bmatrix} -\mathbf{\Phi}^{k_1}+\lambda_j\boldsymbol{I} & -\mathbf{\Phi}^{k_1\dagger}(\widehat{\boldsymbol{\gamma\beta}})_j^{k_1} \\ -(\widehat{\boldsymbol{\gamma\beta}})_j^{k_1\dagger}\mathbf{\Phi}^{k_1} & -(\widehat{\boldsymbol{\gamma\beta}})_j^{k_1\dagger}\mathbf{\Phi}^{k_1}(\widehat{\boldsymbol{\gamma\beta}})_j^{k_1}+t_{9j}-\lambda_j\epsilon^2_{(\boldsymbol{\gamma\beta})_j^{k_1*}} \end{bmatrix} \succeq 0,$$
$$\forall \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}} \ s.t. \ \|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}}\| \le \epsilon_{\boldsymbol{\beta}_j^{k_1*}} \implies$$
$$-N_0(\widehat{\boldsymbol{\beta}}_j^{k_1}+\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}})^{\dagger}\boldsymbol{A}^{k_1}(\widehat{\boldsymbol{\beta}}_j^{k_1}+\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_1*}})-N_0+t_{10j} \le 0$$
$$\iff \quad \mu_j \ge 0, \quad \boldsymbol{C}_{\mu_j} \triangleq$$
$$\begin{bmatrix} N_0\boldsymbol{A}^{k_1}+\mu_j\boldsymbol{I} & N_0\boldsymbol{A}^{k_1\dagger}\widehat{\boldsymbol{\beta}}_j^{k_1} \\ N_0\widehat{\boldsymbol{\beta}}_j^{k_1\dagger}\boldsymbol{A}^{k_1} & N_0\widehat{\boldsymbol{\beta}}_j^{k_1\dagger}\boldsymbol{A}^{k_1}\widehat{\boldsymbol{\beta}}_j^{k_1}+N_0-t_{10j}-\mu_j\epsilon^2_{\boldsymbol{\beta}_j^{k_1*}} \end{bmatrix} \succeq 0,$$
$$\forall \boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}} \ s.t. \ \|\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}}\| \le \epsilon_{\boldsymbol{\beta}_j^{k_2*}} \implies$$
$$-(\widehat{\boldsymbol{\beta}}_j^{k_2}+\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}})^{\dagger}\boldsymbol{B}^{k_2}(\widehat{\boldsymbol{\beta}}_j^{k_2}+\boldsymbol{e}_{\boldsymbol{\beta}_j^{k_2*}})+t_{11j} \le 0$$
$$\iff \quad \xi_j \ge 0, \quad \boldsymbol{C}_{\xi_j} \triangleq$$
$$\begin{bmatrix} \boldsymbol{B}^{k_2}+\xi_j\boldsymbol{I} & \boldsymbol{B}^{k_2\dagger}\widehat{\boldsymbol{\beta}}_j^{k_2} \\ \widehat{\boldsymbol{\beta}}_j^{k_2\dagger}\boldsymbol{B}^{k_2} & \widehat{\boldsymbol{\beta}}_j^{k_2\dagger}\boldsymbol{B}^{k_2}\widehat{\boldsymbol{\beta}}_j^{k_2}-t_{11j}-\xi_j\epsilon^2_{\boldsymbol{\beta}_j^{k_2*}} \end{bmatrix} \succeq 0,$$
$$\text{and} \quad t_6 \ge 0,\ t_{10j} \ge 0,\ t_{11j} \ge 0.$$

Substituting the maximization form (27) and the above LMI constraints in the optimization problem (25) and using the fact that min-max is greater the max-min, we get the following lower bound for the optimization problem (25):

$$\max_{\mathbf{\Phi}^{k_1},\ \mathbf{\Psi}^{k_2}} \ \max_{\substack{t_6,\ t_7,\ t_8,\ t_{9j},\ t_{10j},\ t_{11j}, \\ \lambda,\ \mu,\ \xi,\ \lambda_j,\ \mu_j,\ \xi_j,\ \forall j:1,\cdots,J}} \ \min_{j:1,\cdots,J} \frac{a+P_s\frac{t_6}{t_7+t_8}}{b_j+P_s\frac{t_{9j}}{t_{10j}+t_{11j}}} \quad (28)$$
$$\text{s.t.} \quad \mathbf{\Phi}^{k_1}\succeq 0,\ \mathbf{\Psi}^{k_2}\succeq 0,\ t_6 \ge 0,$$
$$tr(\mathbf{\Phi}^{k_1}(P_s diag(\boldsymbol{v})+N_0\boldsymbol{I})) + tr(\mathbf{\Psi}^{k_2}) \ \le \ P_0 - P_s,$$
$$\lambda \ge 0,\ \mu \ge 0,\ \xi \ge 0,\ \boldsymbol{C}_{\lambda}\succeq 0,\ \boldsymbol{C}_{\mu}\succeq 0,\ \boldsymbol{C}_{\xi}\succeq 0,$$
$$\forall j:1,\cdots,J,\ t_{10j} \ge 0,\ t_{11j} \ge 0,$$
$$\lambda_j \ge 0,\ \mu_j \ge 0,\ \xi_j \ge 0,\ \boldsymbol{C}_{\lambda_j}\succeq 0,\ \boldsymbol{C}_{\mu_j}\succeq 0,\ \boldsymbol{C}_{\xi_j}\succeq 0. \quad (29)$$

Transforming the innermost minimization in (28) to maximization operation, the optimization problem reduces to the following single maximization form:

$$\max_{\substack{\boldsymbol{\Phi}^{k1},\ \boldsymbol{\Psi}^{k2},\ t_6,\ t_7,\ t_8,\ t_{9j},\ t_{10j},\ t_{11j},\\ \lambda,\ \mu,\ \xi,\ \lambda_j,\ \mu_j,\ \xi_j,\ r,\ s,\ \forall j:1,\cdots,J}} rs \tag{30}$$

$$\begin{aligned}
\text{s.t.}\quad & \boldsymbol{\Phi}^{k_1} \succeq 0,\ \boldsymbol{\Psi}^{k_2} \succeq 0,\ t_6 \geq 0,\\
& tr(\boldsymbol{\Phi}^{k_1}(P_s diag(\boldsymbol{v}) + N_0\boldsymbol{I})) + tr(\boldsymbol{\Psi}^{k_2}) \ \leq\ P_0 - P_s,\\
& a(t_7+t_8) + P_s t_6 - r(t_7+t_8) \geq 0,\\
& \lambda \geq 0,\ \mu \geq 0,\ \xi \geq 0,\ \boldsymbol{C}_\lambda \succeq 0,\ \boldsymbol{C}_\mu \succeq 0,\ \boldsymbol{C}_\xi \succeq 0,\\
& \forall j: 1,\cdots,J,\ t_{10j} \geq 0,\ t_{11j} \geq 0,\\
& (t_{10j}+t_{11j}) - s(b_j(t_{10j}+t_{11j}) + P_s t_{9j}) \geq 0,\\
& \lambda_j \geq 0,\ \mu_j \geq 0,\ \xi_j \geq 0,\ \boldsymbol{C}_{\lambda_j} \succeq 0,\ \boldsymbol{C}_{\mu_j} \succeq 0,\ \boldsymbol{C}_{\xi_j} \succeq 0.
\end{aligned} \tag{31}$$

This is a non-convex optimization problem. We solve this problem using the algorithm described below.

Step1: Find r_{max} and s_{max} by solving the following two independent optimization problems:

$$r_{max} = \max_{\boldsymbol{\Phi}^{k1}, \boldsymbol{\Psi}^{k2},\ t6,\ t7,\ t8,\ \lambda,\ \mu,\ \xi,\ r} r \tag{32}$$

$$\begin{aligned}
\text{s.t.}\quad & \boldsymbol{\Phi}^{k_1} \succeq 0,\ \boldsymbol{\Psi}^{k_2} \succeq 0,\ t_6 \geq 0,\\
& tr(\boldsymbol{\Phi}^{k_1}(P_s diag(\boldsymbol{v}) + N_0\boldsymbol{I})) + tr(\boldsymbol{\Psi}^{k_2}) \ \leq\ P_0 - P_s,\\
& a(t_7+t_8) + P_s t_6 - r(t_7+t_8) \geq 0,\\
& \lambda \geq 0,\ \mu \geq 0,\ \xi \geq 0,\ \boldsymbol{C}_\lambda \succeq 0,\ \boldsymbol{C}_\mu \succeq 0,\ \boldsymbol{C}_\xi \succeq 0,
\end{aligned} \tag{33}$$

$$\text{and}\quad s_{max} = \max_{\substack{\boldsymbol{\Phi}^{k1},\ \boldsymbol{\Psi}^{k2},\ t_{9j},\ t_{10j},\ t_{11j},\\ \lambda_j,\ \mu_j,\ \xi_j,\ \forall j:1,\cdots,J,\ s}} s \tag{34}$$

$$\begin{aligned}
\text{s.t.}\quad & \boldsymbol{\Phi}^{k_1} \succeq 0,\ \boldsymbol{\Psi}^{k_2} \succeq 0,\\
& tr(\boldsymbol{\Phi}^{k_1}(P_s diag(\boldsymbol{v}) + N_0\boldsymbol{I})) + tr(\boldsymbol{\Psi}^{k_2}) \ \leq\ P_0 - P_s,\\
& \forall j: 1,\cdots,J,\ t_{10j} \geq 0,\ t_{11j} \geq 0,\\
& (t_{10j}+t_{11j}) - s(b_j(t_{10j}+t_{11j}) + P_s t_{9j}) \geq 0,\\
& \lambda_j \geq 0,\ \mu_j \geq 0,\ \xi_j \geq 0,\ \boldsymbol{C}_{\lambda_j} \succeq 0,\ \boldsymbol{C}_{\mu_j} \succeq 0,\ \boldsymbol{C}_{\xi_j} \succeq 0.
\end{aligned} \tag{35}$$

For a given r and s, both the problems are convex SDP feasibility problems and both are solved using bisection method. We describe the bisection method in short to solve (32) as follows. Let r_{max} lie in the interval $[r_{ll},\ r_{ul}]$. Check the feasibility of the constraints of (32) at $r = (r_{ll} + r_{ul})/2$. If feasible then $r_{ll} = r$ else $r_{ul} = r$. Repeat this until $r_{ul} = r_{ll}$ or the desired accuracy is achieved. 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 (30). This is due to the fact that 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 (30) will be upper bounded by the product $r_{max}s_{max}$.

Step2: We represent the optimum value of the optimization problem (30) by $r_{opt}s_{opt}$. Having obtained the values of r_{max} and s_{max} in Step 1, we obtain $r_{opt}s_{opt}$ sequentially by decreasing r from r_{max} towards zero in discrete steps of size $\triangle_r = r_{max}/N$, where N is a large positive integer, and finding the maximum s such that constraints in (31) are feasible and the product rs is maximum. The algorithm to obtain $r_{opt}s_{opt}$ as follows:

---

for (i = N : -1 : 1)
begin{
$r_i = i * \triangle_r$

$$s_i = \max_{\substack{\boldsymbol{\Phi}^{k1},\ \boldsymbol{\Psi}^{k2},\\ t_6,\ t_7,\ t_8,\ t_{9j},\ t_{10j},\ t_{11j},\\ \lambda,\ \mu,\ \xi,\ \lambda_j,\ \mu_j,\ \xi_j,\ s,\ \forall j:1,2,\cdots,J}} s$$

subject to all constraints in (31) with $r = r_i$

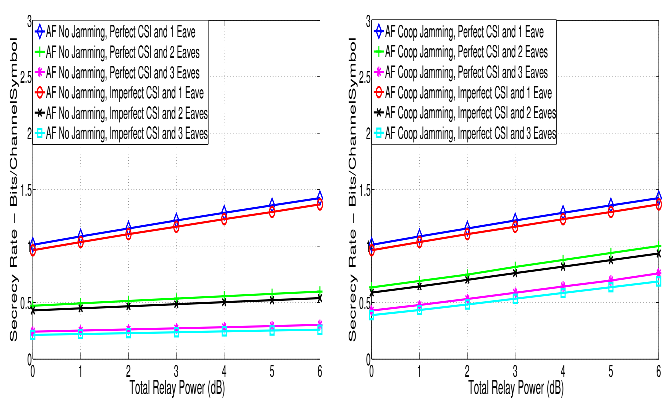
if $(i == N)$ **then** $r_{opt} = r_i,\ s_{opt} = s_i$
elseif $(r_{opt}s_{opt} \leq r_i s_i)$ **then** $r_{opt} = r_i,\ s_{opt} = s_i$
else exit for loop
endif
} **end for loop**

For a given value of r_i and s in the interval $[0, s_{max}]$, the constrained maximization problem in the for loop above is a SDP feasibility problem, and s_i can be obtained using the bisection method as described in Step1 to solve (32). With $r_{opt}s_{opt}$ from Step 2 above for (k_1, k_2) selected relays, worst case secrecy rate $R_s^{k_1k_2}$ for a given source power P_s is then given by $R_s^{k_1k_2} = \frac{1}{2}\log_2 r_{opt}s_{opt}$, and the maximum secrecy rate is $R_s^{max} = \max_{\text{all relay combinations}} R_s^{k_1k_2}$. Maximization is performed over all $2^M - 1$ possible relay combinations.

IV. Results and Discussions

We evaluated the secrecy rate for AF beamforming with/without cooperative jamming, perfect/imperfect CSI and multiple eavesdroppers for different system scenarios through simulations. The results are generated for $M = 2$, $J = 1, 2, 3$, $N_0 = 1$, $P_s = 3$ dB and $N = 50$. We take the norm of the CSI error vectors on all links to be equal, and we denote it by ϵ.

In Fig. 2(a), we plot the secrecy rate as a function of total



(a) No CJ (b) With CJ

Fig. 2. Secrecy rate versus total relay transmit power in AF relay beamforming with/without CJ, perfect/imperfect CSI, and multiple eavesdroppers. CJ gives significant gains with 2 and 3 eavesdroppers.

relay transmit power with the following system parameters:

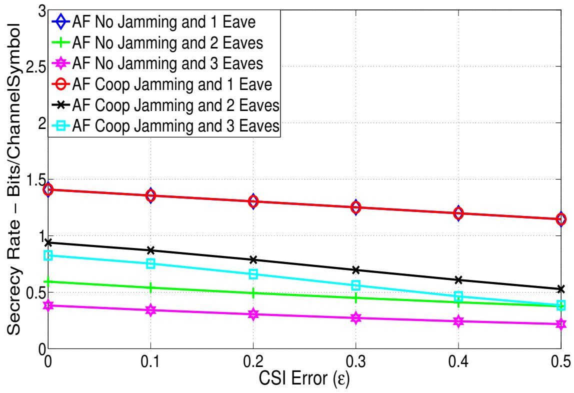
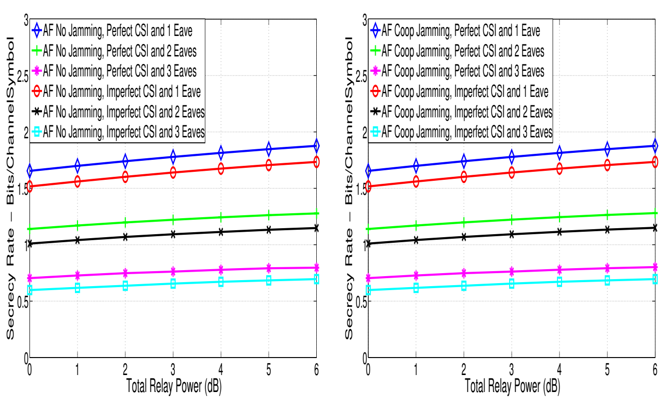


Fig. 3. Secrecy rate versus CSI error (ϵ) in AF relay beamforming with/without CJ, perfect/imperfect CSI and multiple eavesdroppers.

$\sigma_{\gamma_1^*} = \sigma_{\gamma_2^*} = 4.0$, $\sigma_{\alpha_1^*} = 4.0$, $\sigma_{\alpha_2^*} = 0.0$, $\sigma_{\beta_{11}^*} = \sigma_{\beta_{21}^*} = 4.0$, $\sigma_{\beta_{12}^*} = \sigma_{\beta_{22}^*} = 4.0$, $\sigma_{\beta_{13}^*} = \sigma_{\beta_{23}^*} = 4.0$, and $\epsilon = 0.1$. We assume that there is no direct path from source to destination and source to any eavesdropper. From Figs. 2 (a) and (b), we observe that $i)$ in the presence of only one eavesdropper ($J = 1$), the advantage of CJ compared to no CJ is not significant, and $ii)$ with 2 and 3 eavesdroppers ($J = 2, 3$), however, significant gains in secrecy rates due to CJ compared to no CJ are achieved. We also observe that imperfect CSI degrades secrecy rates compared to those with perfect CSI, and that increased number of eavesdroppers results in reduced secrecy rates. In Fig. 3, we plot the secrecy rate as a function of CSI error (ϵ) with $P_0 - P_s = 6$ dB and remaining system parameters are same as in Fig. 2. From Fig. 3, we observe that $i)$ CJ results in rate gains compared to no CJ for $J = 2, 3$, and $ii)$ the achieved rate gain due to CJ is maximum for perfect CSI case and the gain diminishes as the CSI error variance is increased. Next, Fig. 4 shows the secrecy rate results for a scenario where the rate gains due to CJ is not significant even for $J = 2, 3$. In this scenario, source-destination and relays-destination channels are stronger than the corresponding eaves channels. The corresponding parameters used are: $\sigma_{\gamma_1^*} = \sigma_{\gamma_2^*} = 4.0$, $\sigma_{\alpha_0^*} = 2.0$, $\sigma_{\alpha_1^*} = \sigma_{\alpha_2^*} = 4.0$, $\sigma_{\beta_{01}^*} = 0.5$, $\sigma_{\beta_{02}^*} = 1.0$, $\sigma_{\beta_{03}^*} = 1.5$, $\sigma_{\beta_{11}^*} = \sigma_{\beta_{21}^*} = 1.0$, $\sigma_{\beta_{12}^*} = \sigma_{\beta_{22}^*} = 2.0$, $\sigma_{\beta_{13}^*} = \sigma_{\beta_{23}^*} = 3.0$, and $\epsilon = 0.1$. In summary, the secrecy rate gains due to CJ depends on the channel/noise conditions, number of eavesdroppers, and CSI error variances, and the proposed solution allows us to compute the secrecy rate in AF beamforming with CJ under various channel conditions and scenarios.



(a) No CJ (b) With CJ

Fig. 4. Secrecy rate versus total relay transmit power in AF relay beamforming with/without CJ, perfect/imperfect CSI, and multiple eavesdroppers. Source-destination and relays-destination channels are stronger than the corresponding eaves channels.

V. Conclusions

We evaluated the worst case secrecy rates in AF relay beamforming scheme with cooperative jamming and 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 to find the optimum relay beamforming weights (weights of both data relays and jamming relays) subject to a total relay power constraint and CSI error constraints, and computed the worst case secrecy rate by relaxing the rank one constraint on the complex semi-definite data relays and jamming relays weight matrices and reformulated the optimization problem into a form that was solved using convex semi-definite programming.

References

[1] 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.

[2] 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.

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

[4] 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.

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

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

[7] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with imperfect CSI and multiple eavesdroppers," *Proc. IEEE SPAWC'2012*, June 2012.

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

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

[10] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696-1707, April 2012.

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

[12] A. Mukherjee and A. L. Swindlehurst,"Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, January 2011.

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

[14] F. Gao, T. Cui and A. Nallanathan, "On channel estimation and optimal training design for amplify-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1907-1916, May 2008.

[15] A. S. Behbahani and A. Eltawil, "On channel estimation and capacity for amplify-and-forward relay networks," *Proc. IEEE GLOBECOM'2008*, Dec. 2008.

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