ROBUST JOINT BEAMFORMING AND ARTIFICIAL NOISE DESIGN FOR AMPLIFY-AND-FORWARD MULTI-ANTENNA RELAY SYSTEMS

Lijian Zhang, Liang Jin, Wenyu Luo, Yanqun Tang and Dingjiu Yu

Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, China

ABSTRACT

In this paper, we address physical layer security for amplify-and-forward (AF) multi-antenna relay systems in the presence of multiple eavesdroppers. A robust joint design of cooperative beamforming (CB) and artificial noise (AN) is proposed with imperfect channel state information (CSI) of both the destination and the eavesdroppers. We aim to maximize the worst-case secrecy rate subject to the sum power and the per-antenna power constraints at the relay. Such joint design problem is non-convex. By utilizing the semidefinite relaxation (SDR) technique, $\mathcal{S}$-procedure and the successive convex approximation (SCA) algorithm, the original non-convex optimization problem is recast into a series of semidefinite programs (SDPs) which can be efficiently solved using interior-methods. Simulation results are presented to verify the effectiveness of the proposed design.

***Index Terms*—** Physical layer security, amplify-and-forward relaying, cooperative beamforming, artificial noise, secrecy rate

1. INTRODUCTION

As a complement to cryptographic methods on upper layers, physical layer security has been regarded as a promising technique to provide secure data communication. Recently, substantial research has been dedicated toward improving the secrecy rate of various wireless communication systems [1], [2], among which the cooperative relay system has attracted considerable attention [3]. The secrecy rate maximization problem for the single-antenna relay systems has been explored in [4–9]. And the secure transmission approaches for multi-antenna relay systems have been investigated in [10–14].

In this paper, we focus on the robust joint design of cooperative beamforming (CB) and artificial noise (AN) for amplify-and-forward (AF) multi-antenna relay systems. The imperfect channel state information (CSI) of both the destination and the eavesdroppers is assumed to be available at the relay. The worst-case secrecy rate is maximized by jointly optimizing the beamforming and AN covariance matrices at the relay subject to the sum power and the per-antenna power constraints. Even if the worst-case secrecy rate maximization (WCSRM) problem is non-convex, we can find the suboptimal solution using the semidefinite relaxation (SDR) technique [15], $\mathcal{S}$-procedure [16], and the successive convex approximation (SCA) algorithm [17], [18].

This paper addresses the WCSRM problem for AF multi-antenna relay systems. It is worthwhile to mention some related works. In [8] and [9], the robust design for secure single-antenna relay systems was investigated, while we consider the case with a multi-antenna relay. The works [10] and [11] considered a multi-antenna relay scenario, but the method is only applicable for the single eavesdropper case. Besides, it is assumed that only the CSI of the eavesdropper(s) is imperfect in [8–11, 19]. Actually, the CSI of the destination may be also imperfect, which is considered in this paper. To the best of our knowledge, robust approaches to the WCSRM problem for AF multi-antenna relay systems overheard by multiple eavesdroppers are not available in the literature.

Notations: We use $\otimes$, $\odot$, $\mathbf{I}_N$ and $\mathbf{1}_{N\times 1}$ to denote the Hadamard product, Kronecker product, identity matrix of dimension N and the all-one column vector of dimension N, respectively. $\mathbf{D}(\mathbf{q})$ represents a diagonal matrix with $\mathbf{q}$ on the main diagonal. Re$(\cdot)$ extracts the real part of a complex variable. $\mathbf{q}$=vec$(\mathbf{Q})$ denotes a column vector by stacking all the elements of $\mathbf{Q}$ and vec$^{-1}(\mathbf{q})$ is the inverse operation of vec$(\mathbf{Q})$ for recovering $\mathbf{Q}$.

2. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a two-hop AF relay system, which consists of one source (Alice), one relay, one legitimate destination (Bob) and multiple eavesdroppers (Eves). All the nodes are equipped with a single antenna, except that the relay is equipped with N $(N \geq 2)$ antennas. We assumed that the direct links between Alice and Bob as well as Alice and Eves can be ignored due to the weak quality of the channels. Alice intends to transmit confidential information to Bob aided by the trusted relay, while keeping it secret from the Eves.

The whole information transmission includes two phases. In the first phase, Alice transmits a symbol s with the average power P_s to the relay. The received signal vector at the relay is

$$\mathbf{y}_r = \mathbf{f}s + \mathbf{n}_r, \tag{1}$$

where $\mathbf{f} \in \mathbb{C}^N$ represents the channel vector from Alice to the relay; $\mathbf{n}_r \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is the additive white Gaussian noise (AWGN) vector received at the relay. In the second phase, the relay forwards the signal multiplied by a beamforming matrix $\mathbf{A} \in \mathbb{C}^{N\times N}$. Concurrently, the AN is transmitted for confusing the Eves. Hence, the signal vector to be transmitted by the relay is $\mathbf{x}_R = \mathbf{A}\mathbf{f}s + \mathbf{A}\mathbf{n}_r + \mathbf{v}$. Here $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma})$ is the artificial noise vector with $\mathbf{\Sigma} \succeq \mathbf{0}$ being the AN covariance matrix.

According to the expression of $\mathbf{x}_R$, the sum power of all antennas and the power of the nth antenna can be computed, respectively, as

$$P_r = \text{Tr}(P_s\mathbf{A}\mathbf{f}\mathbf{f}^H\mathbf{A}^H) + \text{Tr}(\mathbf{A}\mathbf{A}^H) + \text{Tr}(\mathbf{\Sigma}), \tag{2a}$$

$$P_n = \mathbf{e}_n^T(P_s\mathbf{A}\mathbf{f}\mathbf{f}^H\mathbf{A}^H + \mathbf{A}\mathbf{A}^H + \mathbf{\Sigma})\mathbf{e}_n, \ \forall n \in \mathcal{N}, \tag{2b}$$

where $\mathbf{e}_n$ is a unit vector with the nth entry being one; and $\mathcal{N} \triangleq \{1, \cdots, N\}$. Let $\mathbf{h} \in \mathbb{C}^N$ and $\mathbf{g}_k \in \mathbb{C}^N$, $\forall k \in \mathcal{K}$, $\mathcal{K} \triangleq \{1, \cdots, K\}$, denote the channel vector from the relay to Bob and the channel vector from the relay to the kth Eve, respectively. Then the signals received at Bob and the kth Eve is expressed,

Corresponding author: Liang Jin, Email: liangjin_ndsc@163.com. This work was supported in part by the National Natural Science Foundation of China under Grants 61171108, 61401510 and 61379006.

respectively, as

$$y_b = \mathbf{h}^H\mathbf{A}\mathbf{f}s + \mathbf{h}^H\mathbf{A}\mathbf{n}_r + \mathbf{h}^H\mathbf{v} + n_b, \quad (3a)$$

$$y_k = \mathbf{g}_k^H\mathbf{A}\mathbf{f}s + \mathbf{g}_k^H\mathbf{A}\mathbf{n}_r + \mathbf{g}_k^H\mathbf{v} + n_k,\ \forall k \in \mathcal{K}, \quad (3b)$$

where $n_b \sim \mathcal{CN}(0,1)$ and $n_k \sim \mathcal{CN}(0,1)$ are the AWGN terms at the receivers. According to (3), the received signal-to-interference-plus-noise ratios (SINRs) at Bob and the kth Eve are, respectively,

$$\gamma_b = \frac{P_s|\mathbf{h}^H\mathbf{A}\mathbf{f}|^2}{1+\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h}+\|\mathbf{h}^H\mathbf{A}\|^2}, \quad (4a)$$

$$\gamma_{e,k} = \frac{P_s|\mathbf{g}_k^H\mathbf{A}\mathbf{f}|^2}{1+\mathbf{g}_k^H\boldsymbol{\Sigma}\mathbf{g}_k+\|\mathbf{g}_k^H\mathbf{A}\|^2},\ k \in \mathcal{K}. \quad (4b)$$

For the case of imperfect CSI, it is assumed that the relay has perfect CSI from Alice to the relay, but knows only imperfect CSI of both Bob and Eves. The worst-case ellipsoidal error model is adopted to characterize the imperfect CSI. In this model, the actual channel vectors of Bob and the kth Eve take the following forms

$$\mathbf{h} = \hat{\mathbf{h}} + \Delta\mathbf{h}, \quad \mathbf{g}_k = \hat{\mathbf{g}}_k + \Delta\mathbf{g}_k,\ \forall k \in \mathcal{K}, \quad (5)$$

where $\hat{\mathbf{h}}$ and $\hat{\mathbf{g}}_k$ are the estimated channel vector from the relay to Bob and to the kth Eve, respectively; $\Delta\mathbf{h}$ and $\Delta\mathbf{g}_k$ represent the the corresponding error vectors, which are assumed to be bounded in the ellipsoidal uncertainty regions [20]

$$\Delta\mathbf{h} \in \mathcal{H} \triangleq \{\Delta\mathbf{h}|\Delta\mathbf{h}^H\boldsymbol{\Omega}_b\Delta\mathbf{h} \le \varepsilon_b^2\}, \quad (6a)$$

$$\Delta\mathbf{g}_k \in \mathcal{G}_k \triangleq \{\Delta\mathbf{g}_k|\Delta\mathbf{g}_k^H\boldsymbol{\Omega}_k\Delta\mathbf{g}_k \le \varepsilon_k^2\},\ \forall k \in \mathcal{K}, \quad (6b)$$

where $\boldsymbol{\Omega}_b \succ \mathbf{0}$ and $\boldsymbol{\Omega}_k \succ \mathbf{0}$ define the shapes of the uncertainty regions; and $\varepsilon_b \ge 0$ and $\varepsilon_k \ge 0$ control the sizes of the uncertainty regions.

In this paper, our objective is to maximize the worst-case secrecy rate by jointly designing the beamforming matrix $\mathbf{A}$ and the AN covariance matrix $\boldsymbol{\Sigma}$. According to [21], the WCSRM problem can be formulated as

$$\max_{\mathbf{A},\boldsymbol{\Sigma}\succeq\mathbf{0}} \min_{k\in\mathcal{K}} \Big\{ \min_{\Delta\mathbf{h}\in\mathcal{H}} \frac{1}{2}\log(1+\gamma_b) - \max_{\Delta\mathbf{g}_k\in\mathcal{G}_k} \frac{1}{2}\log(1+\gamma_{e,k}) \Big\}$$
$$\text{s.t. } P_r \le P_{max},\ P_n \le \rho_n,\ \forall n \in \mathcal{N}, \quad (7)$$

where P_{max} and ρ_n are the sum power limit and the power limit of the nth antenna at the relay, respectively; and $\log(\cdot)$ represents the base-2 logarithmic function.

3. ROBUST JOINT CB AND AN DESIGN

The problem (7) is non-convex, and it is intractable to get the global optimal solution. In what follows, we will develop a suboptimal design to handle the non-convex WCSRM problem (7) by using the SDR, $\mathcal{S}$-procedure and the SCA algorithm.

Substituting the expressions of P_r and P_n in (2) as well as the expressions of γ_b and $\gamma_{e,k}$ in (4) into (7), we can obtain

$$\max_{\mathbf{A},\boldsymbol{\Sigma}\succeq\mathbf{0},r_b,r_e} \quad r_b - r_e$$
$$\text{s.t. } \min_{\Delta\mathbf{h}\in\mathcal{H}} \frac{1}{2}\log(1+\frac{P_s|\mathbf{h}^H\mathbf{A}\mathbf{f}|^2}{1+\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h}+\|\mathbf{h}^H\mathbf{A}\|^2}) \ge r_b,$$
$$\max_{\Delta\mathbf{g}_k\in\mathcal{G}_k} \frac{1}{2}\log(1+\frac{P_s|\mathbf{g}_k^H\mathbf{A}\mathbf{f}|^2}{1+\mathbf{g}_k^H\boldsymbol{\Sigma}\mathbf{g}_k+\|\mathbf{g}_k^H\mathbf{A}\|^2}) \le r_e, \forall k \in \mathcal{K},$$
$$\mathrm{Tr}(P_s\mathbf{A}\mathbf{f}\mathbf{f}^H\mathbf{A}^H + \mathbf{A}\mathbf{A}^H + \boldsymbol{\Sigma}) \le P_{max},$$
$$\mathbf{e}_n^T(P_s\mathbf{A}\mathbf{f}\mathbf{f}^H\mathbf{A}^H + \mathbf{A}\mathbf{A}^H + \boldsymbol{\Sigma})\mathbf{e}_n \le \rho_n,\ \forall n \in \mathcal{N}, \quad (8)$$

where r_b and r_e are slack variables. Applying the matrix identities $\mathrm{Tr}(\mathbf{B}^H\mathbf{C}\mathbf{D}\mathbf{F}) = \mathrm{vec}(\mathbf{B})^H(\mathbf{F}^T \otimes \mathbf{C})\mathrm{vec}(\mathbf{D})$ and $\mathrm{Tr}(\mathbf{B}\mathbf{C}) = \mathrm{Tr}(\mathbf{C}\mathbf{B})$, the problem (8) can be equivalently expressed as

$$\max_{\mathbf{a},\boldsymbol{\Sigma}\succeq\mathbf{0},r_b,r_e} \quad r_b - r_e \quad (9a)$$

$$\text{s.t. } \min_{\Delta\mathbf{h}\in\mathcal{H}} \frac{\mathbf{a}^H\mathbf{B}_1\mathbf{a}}{1+\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h}+\mathbf{a}^H\mathbf{B}_2\mathbf{a}} \ge 2^{2r_b}-1, \quad (9b)$$

$$\max_{\Delta\mathbf{g}_k\in\mathcal{G}_k} \frac{\mathbf{a}^H\mathbf{C}_{1,k}\mathbf{a}}{1+\mathbf{g}_k^H\boldsymbol{\Sigma}\mathbf{g}_k+\mathbf{a}^H\mathbf{C}_{2,k}\mathbf{a}} \le 2^{2r_e}-1,\ \forall k \in \mathcal{K}, \quad (9c)$$

$$\mathbf{a}^H\mathbf{D}_1\mathbf{a} + \mathrm{Tr}(\boldsymbol{\Sigma}) \le P_{max}, \quad (9d)$$

$$\mathbf{a}^H\mathbf{D}_{2,n}\mathbf{a} + \mathrm{Tr}(\mathbf{e}_n\mathbf{e}_n^T\boldsymbol{\Sigma}) \le \rho_n,\ \forall n \in \mathcal{N}, \quad (9e)$$

where $\mathbf{a} = \mathrm{vec}(\mathbf{A})$; $\mathbf{B}_1 = P_s(\mathbf{f}^* \otimes \mathbf{h})(\mathbf{f}^* \otimes \mathbf{h})^H$; $\mathbf{B}_2 = \mathbf{I}_N \otimes (\mathbf{h}\mathbf{h}^H)$; $\mathbf{C}_{1,k} = P_s(\mathbf{f}^* \otimes \mathbf{g}_k)(\mathbf{f}^* \otimes \mathbf{g}_k)^H$; $\mathbf{C}_{2,k} = \mathbf{I}_N \otimes (\mathbf{g}_k\mathbf{g}_k^H)$; $\mathbf{D}_1 = (P_s\mathbf{f}^*\mathbf{f}^T + \mathbf{I}_N) \otimes \mathbf{I}_N$; $\mathbf{D}_{2,n} = (P_s\mathbf{f}^*\mathbf{f}^T + \mathbf{I}_N) \otimes (\mathbf{e}_n\mathbf{e}_n^T)$. The problem (9) can be approximated by

$$\max_{\mathbf{a},\boldsymbol{\Sigma}\succeq\mathbf{0},r_b,r_e} \quad r_b - r_e \quad (10a)$$

$$\text{s.t. } \frac{\min_{\Delta\mathbf{h}\in\mathcal{H}} \mathbf{a}^H\mathbf{B}_1\mathbf{a}}{\max_{\Delta\mathbf{h}\in\mathcal{H}} 1+\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h}+\mathbf{a}^H\mathbf{B}_2\mathbf{a}} \ge 2^{2r_b}-1, \quad (10b)$$

$$\frac{\max_{\Delta\mathbf{g}_k\in\mathcal{G}_k} \mathbf{a}^H\mathbf{C}_{1,k}\mathbf{a}}{\min_{\Delta\mathbf{g}_k\in\mathcal{G}_k} 1+\mathbf{g}_k^H\boldsymbol{\Sigma}\mathbf{g}_k+\mathbf{a}^H\mathbf{C}_{2,k}\mathbf{a}} \le 2^{2r_e}-1,\ \forall k \in \mathcal{K}, \quad (10c)$$

$$\text{(9d), (9e).} \quad (10d)$$

Note that we have replaced the left-hand sides of constraints (9b) and (9c) with the corresponding lower bound in (10b) and the corresponding upper bounds in (10c), respectively. The optimal objective value of the problem (10) is a lower bound of the secrecy capacity. Hence, the scheme is suboptimal.

3.1. Semidefinite Relaxation

To further simplify the problem, we resort to the SDR technique [15]. Specifically, we define $\bar{\mathbf{A}} = \mathbf{a}\mathbf{a}^H$ and drop the non-convex constraint $\mathrm{Rank}(\bar{\mathbf{A}}) = 1$. Then the problem (10) can be relaxed into

$$\max_{\substack{\bar{\mathbf{A}}\succeq\mathbf{0},\boldsymbol{\Sigma}\succeq\mathbf{0},r_b,r_e,\\ v_1,v_2,u_1,u_2}} \quad r_b - r_e \quad (11a)$$

$$\text{s.t. } \min_{\Delta\mathbf{h}\in\mathcal{H}} \mathrm{Tr}(\mathbf{B}_1\bar{\mathbf{A}}) \ge v_1, \quad (11b)$$

$$\max_{\Delta\mathbf{h}\in\mathcal{H}} \mathrm{Tr}(\mathbf{B}_2\bar{\mathbf{A}}) + \mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h} + 1 \le v_2, \quad (11c)$$

$$\frac{v_1}{v_2} \ge 2^{2r_b}-1, \quad (11d)$$

$$\max_{\Delta\mathbf{g}_k\in\mathcal{G}_k} \mathrm{Tr}(\mathbf{C}_{1,k}\bar{\mathbf{A}}) \le u_1,\ \forall k \in \mathcal{K}, \quad (11e)$$

$$\min_{\Delta\mathbf{g}_k\in\mathcal{G}_k} \mathrm{Tr}(\mathbf{C}_{2,k}\bar{\mathbf{A}}) + \mathbf{g}_k^H\boldsymbol{\Sigma}\mathbf{g}_k + 1 \ge u_2,\ \forall k \in \mathcal{K}, \quad (11f)$$

$$\frac{u_1}{u_2} \le 2^{2r_e}-1, \quad (11g)$$

$$\mathrm{Tr}(\mathbf{D}_1\bar{\mathbf{A}}) + \mathrm{Tr}(\boldsymbol{\Sigma}) \le P_{max}, \quad (11h)$$

$$\mathrm{Tr}(\mathbf{D}_{2,n}\bar{\mathbf{A}}) + \mathrm{Tr}(\mathbf{e}_n\mathbf{e}_n^T\boldsymbol{\Sigma}) \le \rho_n,\ \forall n \in \mathcal{N}, \quad (11i)$$

where v_1, v_2, u_1 and u_2 are the introduced slack variables; (11b)-(11d) are deduced from (10b); and (11e)-(11g) are deduced from (10c). We can find that the constraints in (11h) and (11i) are convex with respect to $\bar{\mathbf{A}}$ and $\boldsymbol{\Sigma}$. Now, the difficulties in solving the problem (11) lie in two points: one is the infinitely many constraints in (11b), (11c), (11e) and (11f), and the other is the non-convex constraints in (11d) and (11g). In the following two subsections, we will handle theses constraints which introduce the difficulties.

3.2. Robust Transformation of (11b), (11c), (11e) and (11f)

In this subsection, we will transform the infinitely many constraints in (11b), (11c), (11e) and (11f) into tractable forms using the $\mathcal{S}$-procedure [16].

To proceed, we define the following notations:

$$\begin{cases} \tilde{\mathbf{f}} \triangleq \mathbf{f} \otimes \mathbf{1}_{N\times 1},\ \mathbf{\Lambda} \triangleq \mathbf{1}_{N\times 1} \otimes \mathbf{I}_N, \\ \bar{\mathbf{h}} \triangleq \mathbf{\Lambda}\hat{\mathbf{h}},\ \Delta\bar{\mathbf{h}} \triangleq \mathbf{\Lambda}\Delta\mathbf{h},\ \check{\mathbf{h}} \triangleq \mathbf{\Lambda}\mathbf{h} = \bar{\mathbf{h}} + \Delta\bar{\mathbf{h}}, \\ \bar{\mathbf{g}}_k \triangleq \mathbf{\Lambda}\hat{\mathbf{g}}_k,\ \Delta\bar{\mathbf{g}}_k \triangleq \mathbf{\Lambda}\Delta\mathbf{g}_k,\ \check{\mathbf{g}}_k \triangleq \mathbf{\Lambda}\mathbf{g}_k = \bar{\mathbf{g}}_k + \Delta\bar{\mathbf{g}}_k,\ \forall k \in \mathcal{K}, \\ \mathbf{E} \triangleq \mathbf{I}_N \otimes \mathbf{E}_N,\ \text{with } \mathbf{E}_N \text{ being an all-one } N \times N \text{ matrix.} \end{cases}$$

First, we consider the constraint in (11b). It can be easily shown that $\mathbf{f}^* \otimes \mathbf{h} = \tilde{\mathbf{f}}^* \odot \check{\mathbf{h}}$. Then, after some mathematical manipulations, the left side of the inequality in (11b) can be written as

$$\begin{aligned} &P_s(\mathbf{f}^* \otimes \mathbf{h})^H \bar{\mathbf{A}}(\mathbf{f}^* \otimes \mathbf{h}) \\ &= P_s(\tilde{\mathbf{f}}^* \odot \check{\mathbf{h}})^H \bar{\mathbf{A}}(\tilde{\mathbf{f}}^* \odot \check{\mathbf{h}}) = P_s\check{\mathbf{h}}^H\mathbf{D}(\tilde{\mathbf{f}})\bar{\mathbf{A}}\mathbf{D}(\tilde{\mathbf{f}}^*)\check{\mathbf{h}} \\ &= \Delta\mathbf{h}^H\mathbf{T}_1\Delta\mathbf{h} + 2\text{Re}(\mathbf{t}_1^H\Delta\mathbf{h}) + t_1 \end{aligned} \tag{12}$$

where $\mathbf{T}_1 = P_s\mathbf{\Lambda}^T\mathbf{D}(\tilde{\mathbf{f}})\bar{\mathbf{A}}\mathbf{D}(\tilde{\mathbf{f}}^*)\mathbf{\Lambda}$, $\mathbf{t}_1^H = P_s(\tilde{\mathbf{f}}^* \odot \bar{\mathbf{h}})^H\bar{\mathbf{A}}\mathbf{D}(\tilde{\mathbf{f}}^*)\mathbf{\Lambda}$, $t_1 = P_s(\tilde{\mathbf{f}}^* \odot \bar{\mathbf{h}})^H\bar{\mathbf{A}}(\tilde{\mathbf{f}}^* \odot \bar{\mathbf{h}})$. According to (12), the constraint in (11b) can be interpreted as the following implication:

$$\begin{aligned} &\Delta\mathbf{h}^H\mathbf{\Omega}_b\Delta\mathbf{h} - \varepsilon_b^2 \le 0 \\ &\Rightarrow \Delta\mathbf{h}^H\mathbf{T}_1\Delta\mathbf{h} + 2\text{Re}(\mathbf{t}_1^H\Delta\mathbf{h}) + t_1 - v_1 \ge 0. \end{aligned} \tag{13}$$

By applying the $\mathcal{S}$-procedure, the above implication in (13) can be equivalently expressed as the following linear matrix inequality (LMI):

$$\begin{bmatrix} \lambda_1\mathbf{\Omega}_b + \mathbf{T}_1 & \mathbf{t}_1 \\ \mathbf{t}_1^H & -\lambda_1\varepsilon_b^2 + t_1 - v_1 \end{bmatrix} \succeq \mathbf{0}, \tag{14}$$

for some $\lambda_1 \ge 0$.

Next, we deal with (11c). It can be checked that the relation $\mathbf{I}_N \otimes (\mathbf{h}\mathbf{h}^H) = \mathbf{E} \odot (\check{\mathbf{h}}\check{\mathbf{h}})$ holds true. Then, after some mathematical manipulations, the first term on the left hand side (LHS) of the inequality in (11c) can be expressed as

$$\begin{aligned} &\text{Tr}((\mathbf{I}_N \otimes (\mathbf{h}\mathbf{h}^H))\bar{\mathbf{A}}) \\ &= \text{Tr}((\mathbf{E} \odot (\check{\mathbf{h}}\check{\mathbf{h}}^H))\bar{\mathbf{A}}) = \check{\mathbf{h}}^H(\mathbf{E} \odot \bar{\mathbf{A}})\check{\mathbf{h}} \\ &= \Delta\mathbf{h}^H(\mathbf{\Lambda}^T(\mathbf{E} \odot \bar{\mathbf{A}})\mathbf{\Lambda})\Delta\mathbf{h} + 2\text{Re}((\bar{\mathbf{h}}^H(\mathbf{E} \odot \bar{\mathbf{A}})\mathbf{\Lambda})\Delta\mathbf{h}) \\ &\quad + \bar{\mathbf{h}}^H(\mathbf{E} \odot \bar{\mathbf{A}})\bar{\mathbf{h}}. \end{aligned} \tag{15}$$

Besides, substituting the expression of $\mathbf{h}$ in (5) into the second term on the LHS of the inequality in (11c), we can rewrite this term as

$$\Delta\mathbf{h}^H\mathbf{\Sigma}\Delta\mathbf{h} + 2\text{Re}(\hat{\mathbf{h}}^H\mathbf{\Sigma}\Delta\mathbf{h}) + \hat{\mathbf{h}}^H\mathbf{\Sigma}\hat{\mathbf{h}}. \tag{16}$$

Based on (15) and (16), the constraint in (11c) can be rewritten as

$$\begin{aligned} &\Delta\mathbf{h}^H\mathbf{\Omega}_b\Delta\mathbf{h} - \varepsilon_b^2 \le 0, \\ &\Rightarrow \Delta\mathbf{h}^H\mathbf{T}_2\Delta\mathbf{h} + 2\text{Re}(\mathbf{t}_2^H\Delta\mathbf{h}) + t_2 \le 0. \end{aligned} \tag{17}$$

where $\mathbf{T}_2 = \mathbf{\Lambda}^T(\mathbf{E} \odot \bar{\mathbf{A}})\mathbf{\Lambda} + \mathbf{\Sigma}$, $\mathbf{t}_2^H = \bar{\mathbf{h}}^H(\mathbf{E} \odot \bar{\mathbf{A}})\mathbf{\Lambda} + \hat{\mathbf{h}}^H\mathbf{\Sigma}$, $t_2 = \bar{\mathbf{h}}^H(\mathbf{E}\odot\bar{\mathbf{A}})\bar{\mathbf{h}} + \hat{\mathbf{h}}^H\mathbf{\Sigma}\hat{\mathbf{h}} - v_2 + 1$. By applying the $\mathcal{S}$-procedure, the implication in (17) can be guaranteed by the following LMI:

$$\begin{bmatrix} \lambda_2\mathbf{\Omega}_b - \mathbf{T}_2 & -\mathbf{t}_2 \\ -\mathbf{t}_2^H & -\lambda_2\varepsilon_b^2 - t_2 \end{bmatrix} \succeq \mathbf{0}, \tag{18}$$

for some $\lambda_2 \ge 0$.

Using the similar method of dealing with (11b), the constraints in (11e) can be equivalently expressed as

$$\begin{bmatrix} \lambda_{3,k}\mathbf{\Omega}_k - \mathbf{T}_3 & -\mathbf{t}_{3,k} \\ -\mathbf{t}_{3,k}^H & -\lambda_{3,k}\varepsilon_k^2 - t_{3,k} + u_1 \end{bmatrix} \succeq \mathbf{0},\ \forall k \in \mathcal{K}, \tag{19}$$

for some $\lambda_{3,k} \ge 0$, where $\mathbf{T}_3 = \mathbf{T}_1 = P_s\mathbf{\Lambda}^T\mathbf{D}(\tilde{\mathbf{f}})\bar{\mathbf{A}}\mathbf{D}(\tilde{\mathbf{f}}^*)\mathbf{\Lambda}$, $\mathbf{t}_{3,k}^H = P_s(\tilde{\mathbf{f}}^* \odot \bar{\mathbf{g}}_k)^H\bar{\mathbf{A}}\mathbf{D}(\tilde{\mathbf{f}}^*)\mathbf{\Lambda}$, $t_{3,k} = P_s(\tilde{\mathbf{f}}^* \odot \bar{\mathbf{g}}_k)^H\bar{\mathbf{A}}(\tilde{\mathbf{f}}^* \odot \bar{\mathbf{g}}_k)$.

Following similar steps for handling (11c), the constraints in (11f) is equivalent to

$$\begin{bmatrix} \lambda_{4,k}\mathbf{\Omega}_k + \mathbf{T}_4 & \mathbf{t}_{4,k} \\ \mathbf{t}_{4,k}^H & -\lambda_{4,k}\varepsilon_k^2 + t_{4,k} \end{bmatrix} \succeq \mathbf{0},\ \forall k \in \mathcal{K}, \tag{20}$$

for some $\lambda_{4,k} \ge 0$, where $\mathbf{T}_4 = \mathbf{T}_2 = \mathbf{\Lambda}^T(\mathbf{E} \odot \bar{\mathbf{A}})\mathbf{\Lambda} + \mathbf{\Sigma}$, $\mathbf{t}_{4,k}^H = \bar{\mathbf{g}}_k^H(\mathbf{E} \odot \bar{\mathbf{A}})\mathbf{\Lambda} + \hat{\mathbf{g}}_k^H\mathbf{\Sigma}$, $t_{4,k} = \bar{\mathbf{g}}_k^H(\mathbf{E} \odot \bar{\mathbf{A}})\bar{\mathbf{g}}_k + \hat{\mathbf{g}}_k^H\mathbf{\Sigma}\hat{\mathbf{g}}_k - u_2 + 1$.

Therefore, substituting (14), (18)-(20) into the problem (11), we can get the following optimization problem:

$$\max_{\substack{\bar{\mathbf{A}}\succeq\mathbf{0},\mathbf{\Sigma}\succeq\mathbf{0},\boldsymbol{\lambda}\succeq\mathbf{0}, \\ r_b,r_e,v_1,v_2,u_1,u_2}} \quad r_b - r_e \tag{21a}$$

$$\text{s.t.}\ (14),\ (18)-(20),\ (11\text{h})\ \text{and}\ (11\text{i}), \tag{21b}$$

$$(11\text{d})\ \text{and}\ (11\text{g}), \tag{21c}$$

where $\boldsymbol{\lambda} \triangleq [\lambda_1, \lambda_2, \lambda_{3,1}, \ldots, \lambda_{3,K}, \lambda_{4,1}, \ldots, \lambda_{4,K}]$. Obviously, the constraints in (14), (18)-(20), (11h) and (11i) are all linear constraints. But the problem (21) is still non-convex due to the non-convex constraint in (11d) and (11g) which are the remaining obstacles in getting the solution. In the following subsection, we will focus on handling the remaining non-convex constraints.

3.3. Approximation of (11d) and (11g)

Following the idea of [22], we will resort to the SCA algorithm [17] to deal with these two non-convex constraints in (21c). By introducing slack variables, the problem (21) can be equivalently reformulated as

$$\max_{\substack{\bar{\mathbf{A}}\succeq\mathbf{0},\mathbf{\Sigma}\succeq\mathbf{0},\boldsymbol{\lambda}\succeq\mathbf{0}, \\ r_b,r_e,v_1,v_2,u_1,u_2,\mathbf{x}}} \quad r_b - r_e \tag{22a}$$

$$\text{s.t.}\ (14),\ (18)-(20),\ (11\text{h})\ \text{and}\ (11\text{i}), \tag{22b}$$

$$v_1 \ge e^{x_1}, \tag{22c}$$

$$v_2 \le e^{x_2}, \tag{22d}$$

$$2^{2r_b} - 1 \le e^{x_3}, \tag{22e}$$

$$x_1 - x_2 \ge x_3, \tag{22f}$$

$$u_1 \le e^{x_4}, \tag{22g}$$

$$u_2 \ge e^{x_5}, \tag{22h}$$

$$2^{2r_e} - 1 \ge e^{x_6}, \tag{22i}$$

$$x_4 - x_5 \le x_6, \tag{22j}$$

where $\mathbf{x} \triangleq [x_1, \ldots, x_6]$; (22c)-(22f) and (22g)-(22j) are deduced from (11d) and (11g), respectively. It can be verified that the inequality constraints in (22c)-(22j) are active at the optimal points by contradiction. Hence, the problem (22) are equivalent to the problem (21).

It is clear that the constraints in (22d), (22e), (22g) and (22i) are non-convex. However, we find that the functions e^{x_2}, e^{x_3}, e^{x_4} and $2^{r_e} - 1$ are convex. Similar to [22], the first order Taylor series approximation can be used as the linear lower bounds of these functions. By exploiting the idea of SCA [17], [22], in the ith iteration, the constraints in (22d), (22e), (22g) and (22i) can be replaced with the following linear constraints, respectively

$$v_2 \leq e^{\bar{x}_2[i]}(x_2 - \bar{x}_2[i] + 1), \tag{23}$$

$$2^{2r_b} - 1 \leq e^{\bar{x}_3[i]}(x_3 - \bar{x}_3[i] + 1), \tag{24}$$

$$u_1 \leq e^{\bar{x}_4[i]}(x_4 - \bar{x}_4[i] + 1), \tag{25}$$

$$2^{2\bar{r}_e[i]}((r_e - \bar{r}_e[i]) \ln 4 + 1) - 1 \geq e^{x_6}, \tag{26}$$

where $\bar{x}_2[i]$, $\bar{x}_3[i]$, $\bar{x}_4[i]$ and $\bar{r}_e[i]$ are the optimal values of x_2, x_3, x_4 and r_e , respectively, in the $(i-1)$th iteration.

Based on the discussions above, the solution to the problem (21) can be iteratively obtained by solving the following convex approximate problem:

$$\begin{aligned} &\max_{\substack{\bar{\mathbf{A}}\succeq\mathbf{0},\boldsymbol{\Sigma}\succeq\mathbf{0},\boldsymbol{\lambda}\succeq\mathbf{0},\\ r_b,r_e,v_1,v_2,u_1,u_2,\mathbf{x}}} \quad r_b - r_e \\ &\text{s.t.}\ (14),\ (18)-(20),\ (11h),\ (11i), \\ &\qquad (22c),\ (22f),\ (22h),\ (22j) \text{ and } (23)-(26). \end{aligned} \tag{27}$$

The problem (27) is a convex SDP which can be efficiently solved by available softwares, e.g., CVX [23]. Now, the SCA based algorithm for solving the problem (11) is summarized in Algorithm 1.

Algorithm 1 SCA based algorithm for solving the problem (11)

1: **Initialization:** set $i = 0$, find arbitrary $\bar{x}_2[i]$, $\bar{x}_3[i]$, $\bar{x}_4[i]$ and $\bar{r}_e[i]$ that are feasible to the problem (27);
2: **repeat**
3: solve the problem (27); let $(x_2^\star, x_3^\star, x_4^\star, r_e^\star)$ represent the optimal values of (x_2, x_3, x_4, r_e);
4: set $(\bar{x}_2[i+1],\ \bar{x}_3[i+1],\ \bar{x}_4[i+1], \bar{r}_e[i+1]) = (x_2^\star, x_3^\star, x_4^\star, r_e^\star)$ and $i := i + 1$;
5: **ultil** the stopping criterion is met or the iteration number reaches the maximum value;
6: **output:** $\bar{\mathbf{A}}^\star, \boldsymbol{\Sigma}^\star$.

Note that if the optimal solution $\bar{\mathbf{A}}^\star$ of the problem (11) is of rank one, a suboptimal beamforming matrix $\mathbf{A}^\star$ of the problem (7) can be obtained by $\mathbf{A}^\star = \text{vec}^{-1}(\mathbf{a}_{opt})$ with $\bar{\mathbf{A}}^\star = \mathbf{a}_{opt}\mathbf{a}_{opt}^H$. If the rank of $\bar{\mathbf{A}}^\star$ is larger than one, the Gaussian randomization procedure [15] can be used to get a rank-one approximate solution of the problem (11). Then, an approximated suboptimal beamforming matrix of the problem (7) can be constructed.

Proposition 1. Let $R_s[i]$ denote the optimal objective value of the problem (27) in the ith iteration. Then the sequence $\{R_s[i]\}$ converges. Further, each limit point is a Karush-Kuhn-Tucker (KKT) point of the problem (11).

Proof: Proof is omitted due to space limitation, but it can be proved following the arguments presented in [17] and [22]. ■

4. SIMULATION RESULTS

In this section, simulation results are presented to evaluate the performance and the convergence behaviors of the proposed joint CB and AN design based on Algorithm 1. In the simulations, the channel coefficients are independently generated following the complex Gaussian distribution with zero-mean and unit covariance. We set $N = 4$, $K = 3$, $P_s = 20$ dB, $\rho_n = P_{max}/N$, $\forall n \in \mathcal{N}$, $\varepsilon_k = \varepsilon_e$, $\forall k \in \mathcal{K}$. The convex optimization problem (27) is solved using the

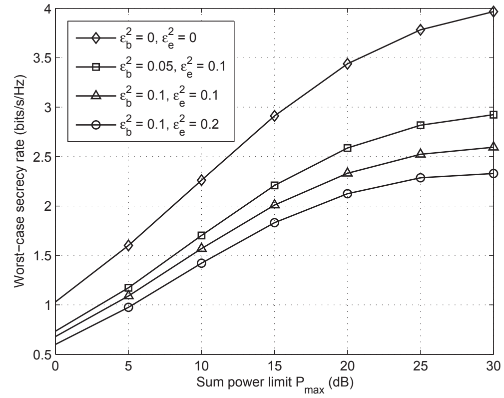

Fig. 1. Worst-case secrecy rate versus the sum power limit at the relay with $N = 4$, $K = 3$ and $P_s = 20$dB.

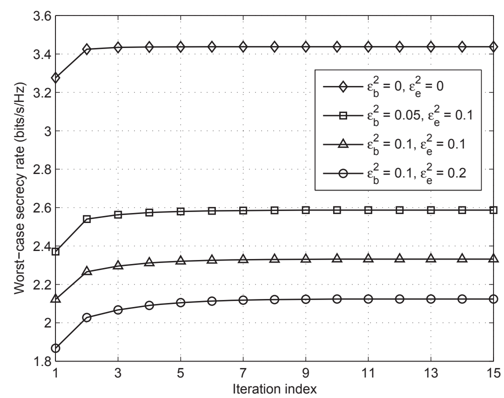

Fig. 2. Worst-case secrecy rate versus versus iteration index with $N = 4$, $K = 3$, $P_{max} = 20$dB and $P_s = 20$dB.

CVX [23]. Each curve is obtained by averaging over 100 independent channel realizations.

Fig. 1 plots the worst-case secrecy rate of the proposed design against the sum power limit P_{max} for different ε_b^2 and ε_e^2. As expected, for a given sum power limit P_{max}, the worst-case secrecy rate decreases with the increases of ε_b^2 and ε_e^2. In addition, it can be observed that the worst-case secrecy rate is very sensitive to ε_b^2 and ε_e^2 at higher values of the sum power limit P_{max}.

In Fig. 2, the convergence behaviors of Algorithm 1 is illustrated with $P_{max} = 20$ dB for different channel error bounds ε_b^2 and ε_e^2. We can see that the proposed algorithm converges within a few steps, and is independent of channel error bounds.

5. CONCLUSIONS

In this paper, we considered the joint optimization of CB and AN for AF multi-antenna AF relay systems with imperfect CSI of both the destination and the eavesdroppers. While the WCSRM problem is non-convex, it could be handled based on the SDR technique, $\mathcal{S}$-procedure and the SCA algorithm. As a future direction, it would be interesting to extend the proposed method to solve a robust design problem for the scenario where the CSI between the source and the relay is also imperfect.

6. REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, July 2014.

[2] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. KuoE, “Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches,” *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sept. 2013.

[3] R. Bassily, E. Ekrem, X. He, E. tekin, J. Xie, M. R. bloch, S. Ulukus, and A. Yener, “Cooperative security at the physical layer a summary of recent advances,” *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sept. 2013.

[4] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, “Cooperative secure beamforming for AF relay networks with multiple eavesdroppers,” *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[5] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, “Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper’s CSI,” *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[6] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and M. Lin, “Optimal joint cooperative beamforming and artificial noise design for secrecy rate maximization in af relay networks,” in *Signal Processing Advances in Wireless Communications (SPAWC), 2013 IEEE 14th Workshop on*, Darmstadt, June 2013, pp. 360–364.

[7] Y. Cai, X. Guan, and W. Yang, “Secure transmission design and performance analysis for cooperation exploring outdated csi,” *Communications Letters, IEEE*, vol. 18, no. 9, pp. 1637–1640, Sept. 2014.

[8] C. Wang and H.-M. Wang, “Robust joint beamforming and jamming for secure af networks: Low complexity design,” IEEE Transactions on Vehicular Technology, 2014, to be published.

[9] L. Li, Z. Chen, and J. Fang, “Robust transmit design for secure af relay networks based on worst-case optimization,” in *IEEE ICASSP*, FLORENCE, ITALY, May 2014, pp. 2719–2723.

[10] X. Wang, Z. Zhang, and K. Long, “Robust relay beamforming for multiple-antenna amplify-and-forward relay system in the presence of eavesdropper,” in *IEEE ICASSP*, FLORENCE, ITALY, May 2014.

[11] X. Wang, K. Wang, and X.-D. Zhang, “Secure relay beamforming with imperfect channel side information,” *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, 2013.

[12] H.-M. Wang, F. Liu, and X.-G. Xia, “Joint source-relay precoding and power allocation for secure amplify-and-forward mimo relay networks,” *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 8, pp. 1240–1250, Aug 2014.

[13] Z. Ding, K. K. Leung, D. Goeckel, and D. Towsley, “On the application of cooperative transmission to secrecy communications,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[14] Q. Li, Q. Zhang, and J. Qin, “Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks,” *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2462–2467, June 2014.

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

[16] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge, UK New York: Cambridge University Press, 2004.

[17] A. Beck, A. Ben-Tal, and L. Tetruashvili, “A sequential parametric convex approximation method with applications to nonconvex truss topology design problems,” *J. Global Optimization*, vol. 47, no. 1, pp. 29–51, May 2010.

[18] B. R. Marks and G. P. Wright, “A general inner approximation algorithm for nonconvex mathematical programs,” *Operat. Res.*, vol. 26, no. 4, pp. 681–683, July 1978.

[19] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, “Robust cooperative beamforming and artificial noise design for physical-layer secrecy in af multi-antenna multi-relay networks,” *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan 2015.

[20] J. Ni, Z. Fei, K.-K. Wong, C. Xing, J. Kuang, and K.-F. Tong, “Robust coordinated beamforming for secure MISO interference channels with bounded ellipsoidal uncertainties,” *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 407–410, Aug. 2013.

[21] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[22] W.-C. Li, T.-H. Chang, C. Lin, and C.-Y. Chi, “Coordinated beamforming for multiuser miso interference channel under rate outage constraints,” *Signal Processing, IEEE Transactions on*, vol. 61, no. 5, pp. 1087–1103, Mar. 2013.

[23] I. CVX Research, “CVX: Matlab software for disciplined convex programming, version 2.0,” http://cvxr.com/cvx, 2012.