Secure MIMO AF Relaying Design: An Intercept Probability Constrained Approach

Jiaxin Yang*, Benoit Champagne*, Qiang Li†, and Lajos Hanzo‡
*Department of Electrical and Computer Engineering, McGill University, Montreal, Quebec, Canada
†School of Communication and Information Engineering,
University of Electronic Science and Technology of China, Chengdu, China
‡School of Electronics and Computer Science, University of Southampton, Southampton, U.K.
Emails: jiaxin.yang@mail.mcgill.ca; benoit.champagne@mcgill.ca; lq@uestc.edu.cn; lh@ecs.soton.ac.uk

***Abstract*—Multiple-input multiple-output (MIMO) amplify-and-forward (AF) relaying is designed for secure communication between a source-destination pair in the presence of multiple eavesdroppers. Assuming statistical knowledge of the eavesdroppers' channel state information (ECSI) errors, we introduce a probabilistically robust design method, which aims to optimize the source transmission power and AF relaying matrix by maximizing the received signal-to-interference-plus-noise ratio (SINR) at the destination, while satisfying a set of *intercept probability constraints*. The resultant optimization problem becomes non-convex, and hence we propose a conservative two-step solution, where the source transmission power and the relaying matrix are sequentially optimized. Our simulation results demonstrate the improved secrecy of the proposed relaying design against eavesdropping and its robustness against the channel uncertainties.**

I. INTRODUCTION

Due to the broadcast nature of signal propagation, wireless communication is vulnerable to eavesdropping [1]. The secrecy of wireless networks has traditionally been ensured by bit-level encryption techniques and by the associated protocols operating at various level of the Open Systems Interconnection (OSI) stack. Recently, physical layer security has attracted considerable attention in the research community as a complement to classic encryption techniques [2]. Physical layer security exploits the underlying characteristics of wireless channels and seeks to design advanced signal processing schemes that are capable of providing further security enhancements.

In particular, it has been demonstrated for the first time in [3] that relaying is capable of improving the physical layer security of data transmission. This seminal contribution has led to further research endeavours devoted to investigating secure transmission schemes in relay-assisted networks. For instance, cooperative beamforming relying on multiple single-antenna relays has been proposed for amplify-and-forward (AF) in [4] and for decode-and-forward (DF) relaying in [5] in the presence of multiple eavesdroppers, which attained the maximum achievable secrecy rate. Joint source and relay precoding exploiting the generalized singular-value decomposition (GSVD) is proposed for a multiple-input multiple-output (MIMO) relay wiretap channel in [6] when multiple antennas are employed both at the source and relay nodes,

The above relaying schemes rely on the idealized simplifying assumption of having perfect eavesdropper channel state information (ECSI), which is hard to acquire in practice. Assuming that the ECSI errors are norm-bounded within a predefined radius, robust secure relaying approaches are proposed in [7] for certain worst-case scenarios. However, when the statistical knowledge of the ECSI errors is known, usually a probabilistic approach is preferred, which leads to less conservative performance estimates than the worst-case approach. While the probabilistic approach has been studied in the context of the multiple-input single-output (MISO) [8] and MIMO wiretap channels [9], its applications in secure MIMO AF relaying design have remained largely unexplored.

To fill this need, in this paper, we study the problem of secure MIMO AF relaying design under the practical assumption of having statistical ECSI errors, where the potential information leakage of both the source to relay and relay to destination hops is considered. In contrast to the prior contributions [4]–[6], we propose a new *intercept probability-constrained* design approach, where both the source transmission power and the AF relaying matrix are optimized to maximize the received signal-to-interference-plus-noise ratio (SINR) at the legitimate destination while imposing a set of *intercept probability constraints* on all the eavesdroppers. The resultant optimization problem becomes non-convex. To overcome this impediment, we adopt a conservative two-step approach, where the source transmission power and the relaying matrix are optimized sequentially. Specifically, the subproblem solving for the relaying matrix is transformed into a so-called difference of convex (DC) functions program. Subsequently, an algorithmic solution resorting to a penalty-DC algorithm (P-DCA) is proposed, which iteratively solves the relaying matrix subproblem via a sequence of "convexified" problems. The efficiency of the proposed robust secure relaying design is demonstrated by numerical experiments.

The rest of the paper is organized as follows. Section II introduces our system model and formulates the design problem. A conservative two-step design approach is developed in

The work of J. Yang and B. Champagne was supported by a grant from the Natural Sciences and Engineering Research Council of Canada (NSERC). The work of Q. Li was supported by the National Natural Science Foundation of China under Grant 61401073 and the Starting Grant of UESTC (Y02002010101065).

978-1-4799-5952-5/15/$31.00 ©2015 IEEE

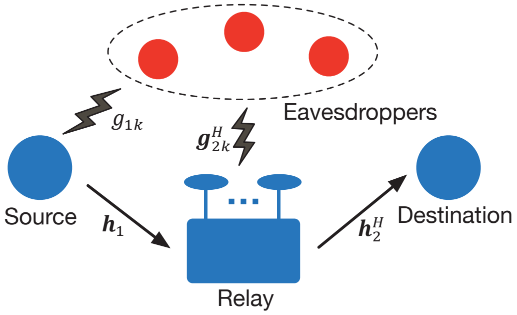

Fig. 1. MIMO relay network in the presence of multiple eavesdroppers where information leakage from both $\mathtt{S}$ and $\mathtt{R}$ is considered.

Section III. The simulation results are presented in Section IV. Finally, Section V concludes the paper.

II. System Model and Problem Formulation

Consider the wireless sub-network depicted in Fig. 1, consisting of a single source $\mathtt{S}$, a single relay $\mathtt{R}$, a destination node $\mathtt{D}$ and K independent eavesdroppers $\mathtt{E}_k$, $k \in \mathcal{K} \triangleq \{1, 2, \cdots, K\}$, where $\mathtt{S}$, $\mathtt{D}$ and $\mathtt{E}_k$, $\forall k \in \mathcal{K}$ are equipped with a single antenna, while $\mathtt{R}$ is equipped with N_{R} antennas. The relay $\mathtt{R}$ operates in half-duplex mode where a pair of time slots are needed for each transmission. We assume that no direct link is available between $\mathtt{S}$ and $\mathtt{D}$ due to its severe attenuation.

Denote the $\mathtt{S}$–$\mathtt{R}$ channel by $\mathbf{h}_1 \in \mathbb{C}^{N_{\mathrm{R}} \times 1}$ and the Hermitian transpose of the $\mathtt{R}$–$\mathtt{D}$ channel by $\mathbf{h}_2 \in \mathbb{C}^{N_{\mathrm{R}} \times 1}$. Let s denote the transmitted information symbol, modeled as a zero-mean Gaussian random variable having a power of $\mathrm{E}\{|s|^2\} = \sigma_{\mathrm{S}}^2 \leq P_{\mathrm{S}}$, where P_{S} is the power budget of $\mathtt{S}$. The channel's input-output relationship between $\mathtt{S}$–$\mathtt{D}$ is given by

$$y_{\mathrm{D}} = \mathbf{h}_2^H \mathbf{W} \mathbf{h}_1 s + \mathbf{h}_2^H \mathbf{W} \mathbf{n}_{\mathrm{R}} + n_{\mathrm{D}}, \tag{1}$$

where $\mathbf{W} \in \mathbb{C}^{N_{\mathrm{R}} \times N_{\mathrm{R}}}$ denotes the linear AF matrix applied at $\mathtt{R}$, while $\mathbf{n}_{\mathrm{R}}$ and n_{D} are the zero-mean additive noise contributions at $\mathtt{R}$ and $\mathtt{D}$, respectively, with covariances of $\sigma_{\mathrm{R}}^2 \mathbf{I}_{N_{\mathrm{R}}}$ and σ_{D}^2. The relay $\mathtt{R}$ obeys the power constraint $\sigma_{\mathrm{S}}^2 \|\mathbf{W}\mathbf{h}_1\|^2 + \sigma_{\mathrm{R}}^2 \|\mathbf{W}\|_F^2 \leq P_{\mathrm{R}}$, where P_{R} denotes the maximum affordable transmit power.

The attainable transmission reliability is determined by the SINR at $\mathtt{D}$, which is given by

$$\mathtt{SINR}_{\mathrm{D}} = \frac{\sigma_{\mathrm{S}}^2 |\mathbf{h}_2^H \mathbf{W} \mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2 \|\mathbf{h}_2^H \mathbf{W}\|^2 + \sigma_{\mathrm{D}}^2}. \tag{2}$$

Each eavesdropper $\mathtt{E}_k$ is potentially capable of overhearing the signals emanating from both $\mathtt{S}$ and $\mathtt{R}$. Let $g_{1k} \in \mathbb{C}$ and $\mathbf{g}_{2k} \in \mathbb{C}^{N_{\mathrm{R}} \times 1}$, respectively, denote the $\mathtt{S}$–$\mathtt{E}_k$ channel and the Hermitian transpose of the $\mathtt{R}$–$\mathtt{E}_k$ channel. The signals observed by $\mathtt{E}_k$ from $\mathtt{S}$ and $\mathtt{R}$ respectively are given by

$$y_{\mathrm{E},k}^{\mathrm{S}} = g_{1k} s + n_{\mathrm{E},1k} \tag{3}$$

$$y_{\mathrm{E},k}^{\mathrm{R}} = \mathbf{g}_{2k}^H \mathbf{W} \mathbf{h}_1 s + \mathbf{g}_{2k}^H \mathbf{W} \mathbf{n}_{\mathrm{R}} + n_{\mathrm{E},2k}, \tag{4}$$

where $n_{\mathrm{E},1k}$ and $n_{\mathrm{E},2k}$ denote the additive noise terms at $\mathtt{E}_k$ during the first and second time slots, respectively, which have a zero mean and a variance of $\sigma_{\mathrm{E},k}^2$.

In practice, due to the lack of explicit cooperation between the legitimate nodes and the eavesdroppers, only imperfect estimates of the ECSI $\mathtt{S}$–$\mathtt{E}_k$ and $\mathtt{R}$–$\mathtt{E}_k$, $\forall k \in \mathcal{K}$ may be available at the legitimate nodes. We can model the unknown $\mathtt{S}$–$\mathtt{E}_k$ and $\mathtt{R}$–$\mathtt{E}_k$ channels by taking into account the error terms Δg_{1k} and $\Delta \mathbf{g}_{2k}$, yielding:

$$g_{1k} = \hat{g}_{1k} + \Delta g_{1k}, \;\; \mathbf{g}_{2k} = \hat{\mathbf{g}}_{2k} + \Delta \mathbf{g}_{2k}, \tag{5}$$

where $\hat{g}_{1k}$ and $\hat{\mathbf{g}}_{2k}$ denote the imperfect ECSI estimates, while again, Δg_{1k} and $\Delta \mathbf{g}_{2k}$ capture the corresponding *uncertainties*. In this paper, the *channel uncertainties* are modeled as zero-mean circular complex Gaussian random variables, i.e.,

$$\Delta g_{1k} \sim \mathcal{CN}(0, \sigma_{1k}^2), \;\; \Delta \mathbf{g}_{2k} \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}_{2k}), \tag{6}$$

where σ_{1k}^2 and $\mathbf{\Sigma}_{2k}$, respectively, denote the variance of Δg_{1k} and the covariance matrix of $\Delta \mathbf{g}_{2k}$.

In contrast to the prior contributions [4]–[6], in this paper, we assume that the source $\mathtt{S}$ is operating at a pre-determined fixed data rate R_d which is lower than its maximum achievable secrecy rate. Our objective is to achieve the best attainable transmission reliability, i.e., the maximum $\mathtt{SINR}_{\mathrm{D}}$, subject to a set of *intercept probability constraints*.

Since each $\mathtt{E}_k$ should operate on an instantaneous basis, we assume that it adopts the selection diversity combining of $y_{\mathrm{E},k}^{\mathrm{S}}$ and $y_{\mathrm{E},k}^{\mathrm{R}}$ in (3)–(4) due to its simplicity of implementation. On this basis, the mutual information leakage to each $\mathtt{E}_k$ can therefore be expressed as

$$\mathtt{C}_{\mathrm{E},k}(\sigma_{\mathrm{S}}, \mathbf{W}) = \frac{1}{2} \max \left\{ \log_2 \left(1 + \frac{\sigma_{\mathrm{S}}^2 |g_{1k}|^2}{\sigma_{\mathrm{E},k}^2} \right), \right.$$
$$\left. \log_2 \left(1 + \frac{\sigma_{\mathrm{S}}^2 |\mathbf{g}_{2k}^H \mathbf{W} \mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2 \|\mathbf{g}_{2k}^H \mathbf{W}\|^2 + \sigma_{\mathrm{E},k}^2} \right) \right\}, \tag{7}$$

where the coefficient $\frac{1}{2}$ reflects the fact that the relay-assisted transmission requires a pair of orthogonal time slots. The *intercept probability constraint* is then derived from the perspective of information theoretical security. Specifically, an intercept event occurs if the mutual information leakage becomes higher than the rate of the legitimate user, i.e., provided that $\mathtt{C}_{\mathrm{E},k} \geq R_d$. Therefore, in order to introduce additional degrees of freedom to the design problem, we may allow a small intercept probability of $p_k > 0$ by $\mathtt{E}_k$, as encapsulated in the following constraint:

$$\Pr\left\{ \mathtt{C}_{\mathrm{E},k}(\sigma_{\mathrm{S}}, \mathbf{W}) \geq R_d \right\} \leq p_k, \tag{8}$$

where the probability is evaluated over the joint distribution of g_{1k} and $\mathbf{g}_{2k}$. Then the intercept probability constrained secure relaying problem can be formulated as

$$\max_{\sigma_{\mathrm{S}}, \mathbf{W}} \quad \mathtt{SINR}_{\mathrm{D}} \tag{9a}$$

$$\text{s.t.} \quad \sigma_{\mathrm{S}}^2 \leq P_{\mathrm{S}} \tag{9b}$$

$$\sigma_{\mathrm{S}}^2 \|\mathbf{W}\mathbf{h}_1\|^2 + \sigma_{\mathrm{R}}^2 \|\mathbf{W}\|_F^2 \leq P_{\mathrm{R}} \tag{9c}$$

$$\Pr\left\{ \mathtt{C}_{\mathrm{E},k}(\sigma_{\mathrm{S}}, \mathbf{W}) \geq R_d \right\} \leq p_k, \;\; k \in \mathcal{K}\,. \tag{9d}$$

Observe that problem (9) is non-convex in $(\sigma_{\mathrm{S}}^2, \mathbf{W})$ and the constraint (9d) in general does not have a closed-form expression, hence making the problem mathematically intractable. To circumvent this problem, we propose a *conservative* two-step approach in the next section.

III. Two-Step Conservative Approach

A two-step approach which sequentially determines σ_{S}^2 and $\mathbf{W}$ is proposed, leading to a pair of tractable subproblems.

A. *Conservative Transformation of* (9)

We commence by transforming the intercept probability constraint (9d) into a tractable form. The left hand side of (9d) can be written with the aid of (7) as:

$$\Pr\left\{\frac{1}{2}\max\left\{\log_2\left(1+\frac{\sigma_{\mathrm{S}}^2|g_{1k}|^2}{\sigma_{\mathrm{E},k}^2}\right),\right.\right.$$
$$\left.\left.\log_2\left(1+\frac{\sigma_{\mathrm{S}}^2|\mathbf{g}_{2k}^H\mathbf{W}\mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2+\sigma_{\mathrm{E},k}^2}\right)\right\}\geq R_d\right\}, \quad (10)$$

which is equivalent to

$$1-\Pr\left\{\frac{\sigma_{\mathrm{S}}^2|g_{1k}|^2}{\sigma_{\mathrm{E},k}^2}\leq\gamma\right\}\Pr\left\{\frac{\sigma_{\mathrm{S}}^2|\mathbf{g}_{2k}^H\mathbf{W}\mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2+\sigma_{\mathrm{E},k}^2}\leq\gamma\right\}, \quad (11)$$

where we have $\gamma \triangleq 2^{2R_d-1}$. Subsequently, we can arrive at:

$$\Pr\left\{\frac{\sigma_{\mathrm{S}}^2|g_{1k}|^2}{\sigma_{\mathrm{E},k}^2}\leq\gamma\right\}\Pr\left\{\frac{\sigma_{\mathrm{S}}^2|\mathbf{g}_{2k}^H\mathbf{W}\mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2+\sigma_{\mathrm{E},k}^2}\leq\gamma\right\}\geq 1-p_k. \quad (12)$$

Due to the product of two probabilities, the equivalent constraint (12) is still challenging to evaluate. To this end, we "decouple" the intercept probability by splitting the intercept probability p_k between the $\mathtt{S}$–$\mathtt{E}_k$ and $\mathtt{R}$–$\mathtt{E}_k$ wiretap links, i.e.,

$$\Pr\left\{\sigma_{\mathrm{S}}^2|g_{1k}|^2/\sigma_{\mathrm{E},k}^2\leq\gamma\right\}\geq\rho_{1k} \quad (13)$$

$$\Pr\left\{\frac{\sigma_{\mathrm{S}}^2|\mathbf{g}_{2k}^H\mathbf{W}\mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2+\sigma_{\mathrm{E},k}^2}\leq\gamma\right\}\geq\rho_{2k}, \quad (14)$$

where we have $\rho_{1k}\rho_{2k}=1-p_k$. Note that (13) and (14) can be viewed as the per-link intercept probability constraints for each of the $\mathtt{S}$–$\mathtt{E}_k$ and $\mathtt{R}$–$\mathtt{E}_k$ wiretap links, respectively. Since (13) and (14) imply (12), this transformation is conservative.

To simplify the subsequent derivations, we will focus on the case of $\rho_{1k}=\rho_{2k}=\sqrt{1-p_k}\triangleq p_k'$. Then a *conservative* form of the original optimization problem (9) can be formulated as

$$\max_{\sigma_{\mathrm{S}}\leq P_{\mathrm{S}},\mathbf{W}} \quad \mathtt{SINR}_{\mathrm{D}} \quad (15a)$$
$$\text{s.t.} \quad \sigma_{\mathrm{S}}^2\|\mathbf{W}\mathbf{h}_1\|^2+\sigma_{\mathrm{R}}^2\|\mathbf{W}\|_F^2\leq P_{\mathrm{R}} \quad (15b)$$
$$\Pr\left\{\sigma_{\mathrm{S}}^2|g_{1k}|^2/\sigma_{\mathrm{E},k}^2\leq\gamma\right\}\geq p_k',\ k\in\mathcal{K} \quad (15c)$$
$$\Pr\left\{\frac{\sigma_{\mathrm{S}}^2|\mathbf{g}_{2k}^H\mathbf{W}\mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2+\sigma_{\mathrm{E},k}^2}\leq\gamma\right\}\geq p_k',\ k\in\mathcal{K}. \quad (15d)$$

In the following subsections, a two-step approach will be proposed which sequentially finds σ_{S} and $\mathbf{W}$ will be proposed.

B. *Optimization of* σ_{S}

To make (15) tractable, we can first determine σ_{S} by dropping the coupled constraints (15b) and (15d) and solving the following relaxed subproblem:

$$\max_{\sigma_{\mathrm{S}}\leq P_{\mathrm{S}}} \quad \sigma_{\mathrm{S}}^2$$
$$\text{s.t.} \quad \Pr\left\{\sigma_{\mathrm{S}}^2|g_{1k}|^2/\sigma_{\mathrm{E},k}^2\leq\gamma\right\}\geq p_k',\ k\in\mathcal{K}. \quad (16)$$

The physical meaning of (16) is that we attempt to maximize the source transmission power (hence larger SINR at $\mathtt{D}$) while meeting the secrecy constraint on the mutual information leakage from the first-hop transmission, which is independent of $\mathbf{W}$.

To solve (16), we note that $g_{1k}\sim\mathcal{CN}(\hat{g}_{1k},\sigma_{1k}^2)$ and therefore, $\frac{|g_{1k}|^2}{\sigma_{1k}^2/2}$ is non-central chi-squared distributed with degrees of freedom 2, i.e., we have

$$\frac{|g_{1k}|^2}{\sigma_{1k}^2/2}\sim\chi^2(\lambda), \quad (17)$$

where $\lambda=\frac{2|\hat{g}_{1k}|^2}{\sigma_{1k}^2}$ is the non-centrality parameter. Subsequently, the probability in the constraint of (16) can be reformulated as

$$\Pr\left\{\frac{|g_{1k}|^2}{\sigma_{1k}^2/2}\leq\frac{\sigma_{\mathrm{E},k}^2\gamma}{\sigma_{\mathrm{S}}^2\sigma_{1k}^2/2}\right\}=1-Q_1\left(\sqrt{\lambda},\frac{\sigma_{\mathrm{E},k}}{\sigma_{\mathrm{S}}\sigma_{1k}}\sqrt{\frac{\gamma}{2}}\right), \quad (18)$$

where $Q_M(a,b)$ is the Marcum-Q function. Therefore, the constraint in (16) can be rewritten as

$$Q_1\left(\sqrt{\lambda},\frac{\sigma_{\mathrm{E},k}}{\sigma_{\mathrm{S}}\sigma_{1k}}\sqrt{\frac{\gamma}{2}}\right)\leq 1-p_k'. \quad (19)$$

To solve (19), we introduce the following definition:

Definition 1: Let us define the *inverse Marcum-Q function*, $Q_M^{-1}(a,q)$, with respect to the second input argument b, given that the other argument a is fixed. Explicitly if we have, if $Q_M(a,b)=q$, then

$$Q_M\left(a,Q_M^{-1}(a,q)\right)=q. \quad (20)$$

Using the above *inverse Marcum-Q function*, the optimal σ_{S} can be expressed as:

$$\sigma_{\mathrm{S}}=\min\left(\sqrt{P_{\mathrm{S}}},\ \min_{k\in\mathcal{K}}\ \frac{\sigma_{\mathrm{E},k}}{\sigma_{1k}}\sqrt{\frac{\gamma}{2}}\frac{1}{Q_1^{-1}(\sqrt{\lambda},1-p_k')}\right). \quad (21)$$

With the fixed transmission power of $\mathtt{S}$, the next step is to optimize $\mathbf{W}$ as it will be discussed in the next subsection.

C. *Optimization of* $\mathbf{W}$

Having optimized σ_{S}^2 from (21), we now aim for optimizing $\mathbf{W}$ by solving the following intercept probability-constrained SINR maximization problem

$$\max_{\mathbf{W}} \quad \mathtt{SINR}_{\mathrm{D}} \quad (22a)$$
$$\text{s.t.} \quad \sigma_{\mathrm{S}}^2\|\mathbf{W}\mathbf{h}_1\|^2+\sigma_{\mathrm{R}}^2\|\mathbf{W}\|^2\leq P_{\mathrm{R}} \quad (22b)$$
$$\Pr\left\{\frac{\sigma_{\mathrm{S}}^2|\mathbf{g}_{2k}^H\mathbf{W}\mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2\|\mathbf{g}_{2k}^H\mathbf{W}\|^2+\sigma_{\mathrm{E},k}^2}\leq\gamma\right\}\geq p_k',\ k\in\mathcal{K}. \quad (22c)$$

Observe that (22) in its current form is mathematically intractable due to the non-convex expression of $\mathtt{SINR}_{\mathrm{D}}$ in $\mathbf{W}$ and owing to the probabilistic constraint (22c), which motivates a conservative transformation of (22).

Lemma 1 (Bernstein-Type Inequality Approximation [10]): Let $c = \mathbf{x}^H \mathbf{A}\mathbf{x} + 2\Re\left\{\mathbf{a}^H \mathbf{x}\right\}$, where $\mathbf{A} = \mathbf{A}^H \in \mathbb{C}^{N\times N}$ is a complex Hermitian matrix, $\mathbf{a} \in \mathbb{C}^{N\times 1}$ and $\mathbf{x} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_N)$. Then for any $\delta > 0$, the following inequality holds:

$$\begin{aligned}&\Pr\left\{c \geq \mathrm{Tr}(\mathbf{A}) + \sqrt{2\delta}\sqrt{\|\mathbf{A}\|_F^2 + 2\|\mathbf{a}\|^2} + \delta s^+(\mathbf{A})\right\}\\ &\leq \exp(-\delta),\end{aligned} \tag{23}$$

where $s^+(\mathbf{A})$ denotes the maximum eigenvalue of $\mathbf{A}$.

From Lemma 1, it is not difficult to find that the following relationships hold:

$$\mathrm{Tr}(\mathbf{A}) + \sqrt{2\delta}\sqrt{\|\mathbf{A}\|_F^2 + 2\|\mathbf{a}\|^2} + \delta s^+(\mathbf{A}) \leq 0 \tag{24a}$$

$$\Rightarrow \Pr\left\{\mathbf{x}^H \mathbf{A}\mathbf{x} + 2\Re\left\{\mathbf{a}^H\mathbf{x}\right\} \geq 0\right\} \leq \exp(-\delta)$$

$$\Leftrightarrow \Pr\left\{\mathbf{x}^H \mathbf{A}\mathbf{x} + 2\Re\left\{\mathbf{a}^H\mathbf{x}\right\} \leq 0\right\} \geq 1 - \exp(-\delta), \tag{24b}$$

which provides an effective means of converting any probabilistic constraint in the form of (24b) into a *conservative* but *deterministic* constraint in the form of (24a). We rewrite the probabilistic constraint (22c) as (25), shown on top of the next page, where we have $\mathbf{\Theta}(\mathbf{W}) = \mathbf{W}\mathbf{\Phi}\mathbf{W}^H$ with $\mathbf{\Phi} = \sigma_{\mathrm{S}}^2 \mathbf{h}_1\mathbf{h}_1^H - \gamma\sigma_{\mathrm{R}}^2 \mathbf{I}_{N_{\mathrm{R}}}$ and $\Delta\overline{\mathbf{g}}_{2k} = \mathbf{\Sigma}_{2k}^{-\frac{1}{2}}\Delta\mathbf{g}_{2k} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_{\mathrm{R}}})$. Defining $\delta = \ln(1 - p_k')$ and exploiting the results in (24), (25) can further be conservatively transformed into (26), as shown below (25).

Therefore, the SINR maximization problem of (22) can be conservatively approximated as

$$\max_{t\geq 0, \mathbf{W}} \quad \frac{\sigma_{\mathrm{S}}^2 |\mathbf{h}_2^H \mathbf{W}\mathbf{h}_1|^2}{t} \tag{27a}$$

$$\text{s.t.} \quad \sigma_{\mathrm{R}}^2 \|\mathbf{h}_2^H \mathbf{W}\|^2 + \sigma_{\mathrm{D}}^2 \leq t \tag{27b}$$

$$\text{(22b) and (26)},$$

where t is an auxiliary variable introduced for simplifying the further derivation. Observe that (27) is still non-convex due to the following reasons. Firstly, the objective function (27a) is a quadratic-over-linear function, which is jointly convex in $(t, \mathbf{W}) \in \mathbb{R}^+ \times \mathbb{C}^{M\times M}$; therefore, the maximization of this convex objective function leads to a non-convex problem. Secondly, $\mathbf{\Theta}(\mathbf{W})$ is an indefinite quadratic function in $\mathbf{W}$, which makes the constraint (26) non-convex and hence difficult to tackle; for instance, the commonly adopted semidefinite relaxation technique is not applicable for "linearizing" an indefinite quadratic term.

To solve (27), we propose an efficient solution by exploiting the inherent "partial convexity" of (27) with the aid of appropriate transformations of the variables and matrices. Let us invoke the following change of variables:

$$\mathbf{Y} = \mathbf{\Theta}(\mathbf{W}). \tag{28}$$

Upon substituting (28) back into (27), we arrive at:

$$\max_{t\geq 0, \mathbf{W}, \mathbf{Y}} \quad \frac{\sigma_{\mathrm{S}}^2 |\mathbf{h}_2^H \mathbf{W}\mathbf{h}_1|^2}{t} \tag{29a}$$

$$\begin{aligned}\text{s.t.} \quad & \mathrm{Tr}\left(\overline{\mathbf{Y}}\right) + \sqrt{2\delta}\sqrt{\left\|\overline{\mathbf{Y}}\right\|_F^2 + 2\left\|\hat{\mathbf{g}}_{2k}^H \mathbf{\Sigma}_{2k}^{-\frac{1}{2}}\overline{\mathbf{Y}}\right\|^2}\\ & + \delta s^+\left(\overline{\mathbf{Y}}\right) + \hat{\mathbf{g}}_{2k}^H \mathbf{Y}\hat{\mathbf{g}}_{2k} - \gamma\sigma_{\mathrm{E},k}^2 \geq 0, \;\; k \in \mathcal{K}\end{aligned} \tag{29b}$$

$$\mathbf{Y} = \mathbf{W}\mathbf{\Phi}\mathbf{W}^H \tag{29c}$$

$$\text{(22b) and (27b)},$$

where we have $\overline{\mathbf{Y}} = \mathbf{\Sigma}_{2k}^{\frac{1}{2}}\mathbf{Y}\mathbf{\Sigma}_{2k}^{\frac{1}{2}}$. We exploit Lemma 1 of [11] and transform the matrix equality (29c) into

$$\begin{bmatrix} \boldsymbol{\mathcal{L}}_{11} & \mathbf{Y} & \mathbf{W}\mathbf{\Phi} \\ \mathbf{Y}^H & \boldsymbol{\mathcal{L}}_{22} & \mathbf{W} \\ \mathbf{\Phi}\mathbf{W}^H & \mathbf{W}^H & \mathbf{I}_{N_{\mathrm{R}}} \end{bmatrix} \succeq \mathbf{0} \tag{30}$$

$$\mathrm{Tr}\left(\boldsymbol{\mathcal{L}}_{11}\right) - \mathrm{Tr}\left(\mathbf{W}\mathbf{\Phi}^2\mathbf{W}^H\right) \leq 0. \tag{31}$$

It can be seen that (30) is a linear matrix inequality in the 3-tuple $(\boldsymbol{\mathcal{L}}_{11}, \boldsymbol{\mathcal{L}}_{22}, \mathbf{W})$ and (31) is expressed as a difference of two convex functions, i.e., in DC form.

Problem (29) can be further transformed into

$$\min_{\substack{t\geq 0, \mathbf{W}, \mathbf{Y}\\ \mathbf{x}, \mathbf{y}}} \quad -\frac{\sigma_{\mathrm{S}}^2 |\mathbf{h}_2^H \mathbf{W}\mathbf{h}_1|^2}{t} \tag{32a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left(\overline{\mathbf{Y}}\right) + \sqrt{2\delta}x_k + \delta y_k + \hat{\mathbf{g}}_{2k}^H \mathbf{Y}\hat{\mathbf{g}}_{2k} - \gamma\sigma_{\mathrm{E},k}^2 \geq 0 \tag{32b}$$

$$\sqrt{\left\|\overline{\mathbf{Y}}\right\|_F^2 + 2\left\|\hat{\mathbf{g}}_{2k}^H \mathbf{\Sigma}_{2k}^{-\frac{1}{2}}\overline{\mathbf{Y}}\right\|^2} \leq x_k \tag{32c}$$

$$y_k \mathbf{I}_{N_{\mathrm{R}}} \succeq \overline{\mathbf{Y}}, \;\; k \in \mathcal{K} \tag{32d}$$

$$\text{(22b)}, \text{(27b)}, \text{(30) and (31)},$$

where we have $\mathbf{x} = [x_1, \cdots, x_K]^T$ and $\mathbf{y} = [y_1, \cdots, y_K]^T$. In (29), the non-convex conservative intercept probability constraint (29c) is now converted to a linear constraint with the aid of the additional second-order cone constraint (32b) and the semidefinite cone constraint (32d). In fact, the transformed problem (32) is a DC program. To elaborate on this, let us define a tuple collectively denoting all the design and auxiliary variables

$$\mathbf{X} = \left\{t, \mathbf{W}, \mathbf{Y}, \boldsymbol{\mathcal{L}}_{11}, \boldsymbol{\mathcal{L}}_{22}, \mathbf{x}, \mathbf{y}\right\}, \tag{33}$$

and a compact convex set

$$\Omega = \left\{\mathbf{X} : \text{(22b)}, \text{(27b)}, \text{(30)}, \text{(32b)} - \text{(32d)}\right\}, \tag{34}$$

and then (32) can be rewritten in the following concise form

$$\min_{\mathbf{X}\in\Omega} \quad 0 - f_1(t, \mathbf{W}) \tag{35a}$$

$$\text{s.t.} \quad \mathrm{Tr}(\boldsymbol{\mathcal{L}}_{11}) - f_2(\mathbf{W}) \leq 0, \tag{35b}$$

where we have $f_1(t, \mathbf{W}) = \frac{\sigma_{\mathrm{S}}^2 |\mathbf{h}_2^H \mathbf{W}\mathbf{h}_1|^2}{t}$ and $f_2(\mathbf{W}) = \mathrm{Tr}\left(\mathbf{W}\mathbf{\Phi}^2\mathbf{W}^H\right)$. The above DC structure motivates the consideration of the standard DCA (also termed as concave-convex procedure) [12]. However, the main challenge of the

$$\Pr\left\{\Delta\overline{\mathbf{g}}_{2k}^H\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\mathbf{\Theta}(\mathbf{W})\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\Delta\overline{\mathbf{g}}_{2k}+2\Re\{\Delta\overline{\mathbf{g}}_{2k}^H\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\mathbf{\Theta}(\mathbf{W})\hat{\mathbf{g}}_{2k}\}+\hat{\mathbf{g}}_{2k}^H\mathbf{\Theta}(\mathbf{W})\hat{\mathbf{g}}_{2k}-\gamma\sigma_{\mathrm{E},k}^2\leq 0\right\}\geq p_k' \tag{25}$$

$$\mathrm{Tr}\left(\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\mathbf{\Theta}(\mathbf{W})\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\right)+\sqrt{2\delta}\sqrt{\left\|\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\mathbf{\Theta}(\mathbf{W})\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\right\|_F^2+2\left\|\hat{\mathbf{g}}_{2k}^H\mathbf{\Theta}(\mathbf{W})\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\right\|^2}+\delta s^+\left(\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\mathbf{\Theta}(\mathbf{W})\mathbf{\Sigma}_{2k}^{\frac{1}{2}}\right)+\hat{\mathbf{g}}_{2k}^H\mathbf{\Theta}(\mathbf{W})\hat{\mathbf{g}}_{2k}-\gamma\sigma_{\mathrm{E},k}^2\geq 0. \tag{26}$$

direct application of the standard DCA is that it requires a strictly feasible initialization, which is non-trivial in our problem considered in (32) due to its non-convex nature. Therefore, instead of relying on the standard DCA, we propose an iterative algorithm resorting to the P-DCA.

Based on (35), let us now consider the following problem in conjunction with an auxiliary variable s and an additional penalty term

$$\min_{\mathbf{X}\in\Omega,s}\quad -f_1(t,\mathbf{W})+\tau s \tag{36a}$$

$$\text{s.t.}\quad \mathrm{Tr}(\boldsymbol{\mathcal{L}}_{11})-f_2(\mathbf{W})\leq s,\ s\geq 0 \tag{36b}$$

where s can be considered as a measure of how gravely the inequality constraints (35b) are violated. Now focusing on (36), similar to the standard DCA, the concave parts $-f_1$ and $-f_2$ in (36a) and (36b) can be approximated by their first-order Taylor expansions around a point $(t^{(n)},\mathbf{W}^{(n)})$ obtained at the n^{th} iteration

$$\begin{aligned}&\hat{f}_1(t,\mathbf{W};t^{(n)},\mathbf{W}^{(n)})\\&=\frac{\sigma_{\mathrm{S}}^2|\mathbf{h}_2^H\mathbf{W}^{(n)}\mathbf{h}_1|^2}{t^{(n)}}-\frac{\sigma_{\mathrm{S}}^2|\mathbf{h}_2^H\mathbf{W}^{(n)}\mathbf{h}_1|^2}{t^{(n)}}\left(t-t^{(n)}\right)\\&+\frac{\sigma_{\mathrm{S}}^2}{t^{(n)}}2\Re\left\{\mathrm{Tr}\left(\mathbf{h}_1\mathbf{h}_1^H\left(\mathbf{W}^{(n)}\right)^H\mathbf{h}_2\mathbf{h}_2^H\left(\mathbf{W}-\mathbf{W}^{(n)}\right)\right)\right\}\end{aligned} \tag{37}$$

$$\begin{aligned}\hat{f}_2(\mathbf{W};\mathbf{W}^{(n)})&=\mathrm{Tr}\left(\mathbf{W}^{(n)}\mathbf{\Phi}^2\left(\mathbf{W}^{(n)}\right)^H\right)\\&+2\Re\left\{\mathrm{Tr}\left(\left(\mathbf{W}-\mathbf{W}^{(n)}\right)\mathbf{\Phi}^2\left(\mathbf{W}^{(n)}\right)^H\right)\right\}.\end{aligned} \tag{38}$$

Replacing f_1 and f_2 in (36), respectively with (37) and (38), we arrive at the following "convexified" subproblem:

$$\min_{\mathbf{X}\in\Omega,s}\quad -\hat{f}_1(t,\mathbf{W};t^{(n)},\mathbf{W}^{(n)})+\tau^{(n)}s \tag{39a}$$

$$\text{s.t.}\quad \mathrm{Tr}\left(\boldsymbol{\mathcal{L}}_{11}\right)-\hat{f}_2(\mathbf{W};\mathbf{W}^{(n)})\leq s,\ s\geq 0 \tag{39b}$$

The P-DCA, which solves a sequence of "convexified" subproblems formulated in (39) with penalty update is summarized in Algorithm 1. The iterative algorithm commences with a low penalty τ, thus allowing a fast descent of the objective function, while the constraint is temporarily allowed to be violated, i.e., we have $s>0$. Then the algorithm gradually increases τ in order to force the solution to lie in the feasible region of (35).

Let us now characterize the convergence properties of Algorithm 1, which is formulated in the following theorem:

Theorem 1: Let $\left\{\mathbf{X}^{(n)},n=1,2,\cdots\right\}$ denote a sequence of solutions generated by Algorithm 1. Then, every limit point of $\left\{\mathbf{X}^{(n)}\right\}$ is a stationary point of the DC program (35), and hence $(\mathbf{W}^{(\infty)},t^{(\infty)})$ is also a stationary point of the conservative problem (27).

Proof: Omitted due to the space limitation. ■

Algorithm 1 P-DCA for Optimizing $\mathbf{W}$

```
Initialization: An initial point $(t^{(0)},\mathbf{W}^{(0)})$, $\tau^{(0)}>0$,
  $\delta_1>0$ and $\delta_2>0$. Set $n=0$.
  repeat
    1. Convexify: Compute the first-order approximates
       via (37) and (38)
    2. Solve: Compute $\mathbf{W}^{(n+1)}$ by solving (39)
    3. Update $\tau$: Compute the dual variable $|\lambda^{(n+1)}|$ with
       (39b) and set
       $\tau^{(n+1)}=\begin{cases}\tau^{(n)} & \text{if } \tau^{(n)}\geq|\lambda^{(n+1)}|+\delta_1\\ \tau^{(n)}+\delta_2 & \text{if } \tau^{(n)}<|\lambda^{(n+1)}|+\delta_1\end{cases}$   (40)
    4. Update iteration: $n\leftarrow n+1$
  until Termination criterion is satisfied or a maximum
  number of iterations $n_{\max}$ are reached
Output: The optimized $\mathbf{W}^*$.
```

IV. Simulation Experiments and Discussions

In our simulations, a flat Rayleigh fading model is employed for the S–R, R–D channels and the available ECSI estimates. The maximum transmit powers are normalized as $P_{\mathrm{S}}=P_{\mathrm{R}}=1$ and the noise variances are set so that we have $\mathrm{SNR}\triangleq\frac{P_{\mathrm{S}}}{N_{\mathrm{R}}\sigma_{\mathrm{R}}^2}=\frac{P_{\mathrm{R}}}{\sigma_{\mathrm{D}}^2}$. The noise variances are identical for all the eavesdroppers and they are set to $\sigma_{\mathrm{E},k}^2=0.05$. The MATLAB-based optimization platform YALMIP [13] along with the external solver MOSEK [14] are used to solve each optimization problem.

A. Evaluation of the Mutual Information Leakage

In this experiment, the cumulative distribution functions (CDFs) of the mutual information leakage to each of the $K=2$ eavesdroppers E$_k$ are plotted in Fig. 2. The number of relay antennas is $N_{\mathrm{R}}=3$. The source S operates at a fixed data rate of $R_d=1$bps/Hz. The non-robust approach refers to the same design approach based on the imperfect ECSI and when the ECSI errors are neglected. It is observed that the intercept probabilities achieved by the robust approach are around 3%, which is lower than the target $p_1=p_2=0.1$. This is because the conservative nature of the transformations is exploited by our robust approach. However, for the non-robust approach, more than 70% of the experiments violate the predefined intercept probability target of 0.1. It is also

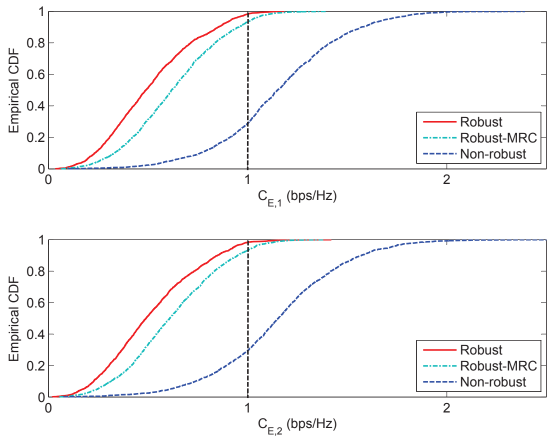

Fig. 2. CDFs of the mutual information leakage to each eavesdropper. (SNR=10dB, $p_1 = p_2 = 0.1$, $\sigma_{11}^2 = \sigma_{12}^2 = 0.1$, $\mathbf{\Sigma}_{21} = \mathbf{\Sigma}_{22} = 0.1\mathbf{I}_{N_\mathrm{R}}$. The CDF labeled "Robust–MRC" represents the scenario where the MRC is adopted by $\mathtt{E}_k$'s.)

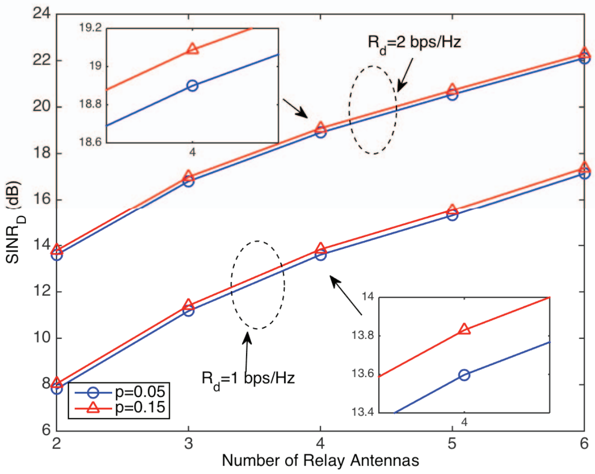

Fig. 3. SINR achieved at the destination with different number of relay antennas. (SNR=10dB, $\sigma_{11}^2 = \sigma_{12}^2 = 0.1$, $\mathbf{\Sigma}_{21} = \mathbf{\Sigma}_{22} = 0.1\mathbf{I}_{N_\mathrm{R}}$.)

worthwhile noting that when the MRC is adopted by the $\mathtt{E}_1$ and $\mathtt{E}_2$, the proposed robust approach can still achieve the intercept probabilities of less than 10%.

B. Impact of Relay Antenna Number on the Achievable SINR

In Fig. 3, the SINR achieved at the destination is presented as a function of the number of relay antennas. Two different data rates are adopted by the source $\mathtt{S}$, i.e., $R_d = 1$bps/Hz and $R_d = 2$bps/Hz. In both cases, two target values of the intercept probabilities are considered. When focusing our attention on the case of $R_d = 2$bps/Hz, it can be observed that the SINR achieved monotonically increases, as the number of relay antennas increases due to its higher diversity gain. When a less stringent intercept probability is required, a higher SINR can be obtained. For the case of a lower data rate, namely for $R_d = 1$bps/Hz, a lower SINR is observed than the case of $R_d = 2$bps/Hz, because the legitimate users are now confined to a relatively low transmit power in order to satisfy the probabilistic secrecy constraints.

V. Conclusions

Secure MIMO relaying optimization was investigated in the presence of eavesdroppers. Considering a more practical perspective on the security-reliability tradeoff, a robust design approach was formulated for maximizing the SINR achieved, while satisfying a set of intercept probability constraints, which allows us to keep the probability that eavesdroppers decode the confidential information below a predefined threshold. In order to solve the formulated non-convex and intractable problem, a conservative two-step approach was proposed, where the source power and the relaying AF matrix are sequentially optimized. Specifically, using the Bernstein-type inequality approximation, an iterative algorithm based on the P-DCA was developed, which exhibited provable convergence. Our simulation results over flat Rayleigh fading channels confirm the security and robustness of the proposed design approach against eavesdropping.

References

[1] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretical security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4-5, pp. 355–580, 2008.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[3] L. Lai and H. E. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sept 2008.

[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] J. Li, A. P. 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.

[6] H.-M. Wang, F. Liu, and P. Mu, "Joint GSVD-SVD precoding and power allocation for security of AF MIMO relay networks," in *Proc. 2014 IEEE Int. Conf. Commun.*, Sydney, Australia, Jun. 2014, pp. 5083–5088.

[7] 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.

[8] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage constrained robust secure transmission for MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558–5570, May 2014.

[9] Q. Li, W.-K. Ma, and A. M.-C. So, "A safe approximation approach to secrecy outage design for MIMO wiretap channels," *IEEE Signal Process. Lett.*, vol. 21, no. 1, pp. 118–121, Jan. 2014.

[10] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.

[11] U. Rashid, H. D. Tuan, H. H. Kha, and H. H. Nguyen, "Joint optimization of source precoding and relay beamforming in wireless MIMO relay networks," *IEEE Trans. Commun.*, vol. 62, no. 2, pp. 488–499, Feb. 2014.

[12] B. K. Sriperumbudur and G. R. G. Lanckriet, "On the convergence of the concave-convex procedure," *Advances Neural Inf. Process. Syst. 22*, pp. 1759–1767, 2009.

[13] J. Löfberg, "YALMIP: a toolbox for modeling and optimization in MATLAB," in *Proc. 2004 IEEE Int. Symp. Comput. Aided Control Syst. Design*, Taipei, Taiwan, Sep. 2004, pp. 284–289.

[14] E. D. Andersen and K. D. Andersen, "MOSEK modeling manual," http://mosek.com, Aug. 2013.