# MIMO AF Relaying Security: Robust Transceiver Design in the Presence of Multiple Eavesdroppers

Jiaxin Yang*, Benoit Champagne*, Yulong Zou†, and Lajos Hanzo‡
*Department of Electrical and Computer Engineering, McGill University, Montreal, Quebec, Canada
†School of Telecommunications and Information Engineering,
Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, P. R. China
‡School of Electronics and Computer Science, University of Southampton, Southampton, U.K.
Emails: jiaxin.yang@mail.mcgill.ca; benoit.champagne@mcgill.ca; yulong.zou@njupt.edu.cn; lh@ecs.soton.ac.uk

***Abstract*—This paper addresses the problem of secure amplify-and-forward (AF) relaying for multiple-input multiple output (MIMO) relaying networks in the presence of multiple eavesdroppers. Assuming practical imperfect eavesdroppers' channel state information (ECSI), we propose a robust approach to optimize the relay AF matrix, subject to power constraint, in order to maximize the received signal-to-interference-plus-noise ratio (SINR) at the destination while satisfying a set of *secrecy constraints*. The ECSI errors are assumed to fall within some predefined bounded sets. Since the resultant optimization problem is non-convex and semi-infinite, we transform it into a form constituted by the differences of convex functions (DC) using suitable matrix transformation techniques. Then an algorithmic solution with proven convergence is proposed by resorting to the penalty-DC algorithm (P-DCA). Experimental results show the security of the proposed transceiver design against eavesdropping and the robustness against the channel uncertainties.**

## I. Introduction

The broadcast nature of wireless propagation has posed significant challenges on the design of secure communications in the presence of unauthorized users, i.e., eavesdroppers, which try to retrieve information from an ongoing transmission without being detected [1]. Against this background, physical layer security, which exploits the signal processing techniques and wireless channel characteristics to enhance the transmission security, has received considerable interests as a complement to traditional encryption techniques.

Since the introduction of the notion of *secrecy capacity* in Wyner's pioneering work [2], the subject of improving secrecy in a range of communication channels has been a hot research topic (e.g., see [3] and references therein). In this era the physical layer security of cooperative relay-assisted networks has attracted a particularly intense attention. While the diversity gains gleaned from user cooperation have been extensively studied in conventional wireless networks [4], this feature can potentially be further exploited for improving the security. However, with additional relay nodes involved in the transmission, the confidentiality of the information may be more easily compromised, unless the transmission scheme is appropriately designed.

Motivated by the above considerations, there have been extensive research efforts recently devoted to the secure relaying design based on the criterion of secrecy capacity. To be specific, the relay weights are optimized in [5], [6] for single-antenna multi-relay network in the presence of multiple eavesdroppers, where the amplify-and-forward (AF) and decode-and-forward (DF) relaying strategies are considered. A similar scenario is considered in [7], where the AF beamformer is derived by resorting to the semidefinite relaxation (SDR) technique, however, without taking into account the information leakage from the source to the eavesdroppers. Power minimization subject to secrecy capacity constraints is proposed in [8]. While cooperative relaying is exploited in the aforementioned contributions to improve the communication secrecy, it has been realized that employing multi-antenna at the relay can further provide performance benefits by exploiting additional degrees of freedom. However, secure multiple-input multiple-output (MIMO) AF relaying design still remains largely unexplored in the literature. Recently, the authors in [9] propose an efficient, but suboptimal joint source and relay precoding scheme based on generalized singular value decomposition (GSVD) and SVD.

The efficacy of the above contributions relies on the assumption of perfect eavesdroppers' channel state information (ECSI). In practice, acquiring the ECSI at the legitimate nodes is quite challenging even when the eavesdroppers are active users supported along with the legitimate nodes within the same networks. This is primarily due to the lack of explicit cooperation between the legitimate nodes and the eavesdroppers, which have no incentive to feed back their ECSI. Unlike the prior contributions, we focus on the secure MIMO AF transceiver design with imperfect ECSI in this paper, where the information leakage at both hops from source to relay and relay to destination is considered[1]. Another main distinction between our work and [5]–[9] is that we do not rely on the secrecy capacity as an optimization criterion[2]. Instead, we consider a more practical perspective of security-reliability trade off (SRT), recently introduced in [12], aiming to achieve the best compromise between the information security and re-

[1]Joint beamforming and cooperative jamming approaches have also received considerable interests recently [10], [11]. As a notable difference, the proposed method lends itself to a self-protection mechanism for the legitimate users without incorporating external nodes or sending additional jamming signals, thus eliminating the possible issues related to node mobility, synchronization and trustworthiness.

[2]The existence of secrecy capacity-achieving codes for the MIMO relay system remains an open problem.

978-1-4673-6432-4/15/$31.00 ©2015 IEEE

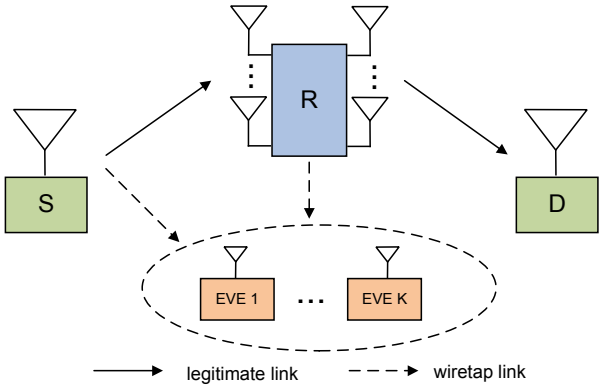


Fig. 1. MIMO relay network in the presence of multiple eavesdroppers with two-hop information leakage.

liability. Specifically, we optimize the AF relay matrix, subject to power constraints, in order to maximize the received signal-to-interference-plus-noise ratio (SINR) at the destination while imposing a set of *secrecy constraints* at all the eavesdroppers. The *secrecy constraints* are derived based on Shannon's theory [13], [14] by exploiting that if the mutual information leakage from the legitimate users to the eavesdroppers is lower than the data rate of the legitimate nodes, the eavesdroppers fail to decode the message. The resultant optimization problem is non-convex. To solve it, we first transform it into the form of a difference of convex functions (DC) program. Subsequently, an algorithmic solution resorting to a penalty-DC algorithm (P-DCA) is proposed, which iteratively solves the problem for the optimal AF matrix of the relay via a sequence of "convexified" problems until convergence is reached, which is guaranteed in this case. The efficiency of our proposed robust secure relaying design is demonstrated with the aid of our numerical experiments.

The rest of the paper is organized as follows. Section II introduces the system model and outlines the robust secure relaying problem. The iterative algorithm based on the P-DCA is developed in Section III. Experimental results are presented in Section IV. Finally, Section V concludes the paper.

## II. System Model and Problem Formulation

We consider a wireless scenario as depicted in Fig. 1, where a legitimate source node S communicates with the legitimate destination node D assisted via a trusted relay node R. The transmitted signals from both S and R are overheard by $K$ eavesdroppers. Each eavesdropper is assigned a unique index $k \in \mathcal{K} \triangleq \{1, 2, \cdots, K\}$ and denoted as $\mathtt{E}_k$. S, D and $\mathtt{E}_k$, $\forall k \in \mathcal{K}$ are equipped with single antenna, and R is equipped with $N_{\mathrm{R}}$ antennas. We assume that no direct link between S and D is available due to the severe attenuation.

A narrowband flat-fading propagation model is considered where $\mathbf{h}_1 \in \mathbb{C}^{N_{\mathrm{R}} \times 1}$ denotes the S–R channel vector and $\mathbf{h}_2 \in \mathbb{C}^{N_{\mathrm{R}} \times 1}$ denotes the complex conjugate R–D channel vector. Let $s$ denote the information symbol to be transmitted by S at a given time instant, modeled as a zero-mean Gaussian random variable with variance $\mathrm{E}\{|s|^2\} = \sigma_{\mathrm{S}}^2 \leq P_{\mathrm{S}}$, where $P_{\mathrm{S}}$ is the power budget of S. The channel input-output relation between S–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 R, and $\mathbf{n}_{\mathrm{R}}$ and $n_{\mathrm{D}}$ are the zero-mean additive noises at R and D, respectively, with covariances $\sigma_{\mathrm{R}}^2 \mathbf{I}_{N_{\mathrm{R}}}$ and $\sigma_{\mathrm{D}}^2$. The relay R is confined by the power constraint $\sigma_{\mathrm{S}}^2 \mathrm{Tr}\left(\mathbf{W}\mathbf{h}_1\mathbf{h}_1^H\mathbf{W}^H\right) + \sigma_{\mathrm{R}}^2 \mathrm{Tr}\left(\mathbf{W}\mathbf{W}^H\right) \leq P_{\mathrm{R}}$, where $P_{\mathrm{R}}$ denotes its maximum affordable transmit power.

We adopt, as a metric of transmission reliability, the received signal-to-interference-plus-noise ratio (SINR) at D, which is given by

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

During the transmission, $\mathtt{E}_k, \forall k \in \mathcal{K}$ can overhear signals from both S and R. Let $g_{1k} \in \mathbb{C}$ and $\mathbf{g}_{2k} \in \mathbb{C}^{N_{\mathrm{R}} \times 1}$, respectively, denote the S–$\mathtt{E}_k$ and complex conjugate R–$\mathtt{E}_k$ channels. The signals observed by $\mathtt{E}_k$, respectively, from S and R 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 additive noise terms with zero mean and variance $\sigma_{\mathrm{E},k}^2$.

In general, nearly perfect knowledge of S–R and R–D channels can be obtained by training-based channel estimation at the receiver and this information is subsequently fed back to the transmitter. However, due to the lack of explicit cooperation between the legitimate nodes and the eavesdroppers, only imperfect estimates of the ECSI S–$\mathtt{E}_k$ and R–$\mathtt{E}_k$, $\forall k \in \mathcal{K}$ can be available at the legitimate nodes[3] To model the ECSI errors, we consider expressing the true but unknown S–$\mathtt{E}_k$ and R–$\mathtt{E}_k$ channels as

$$g_{1k} = \hat{g}_{1k} + \Delta g_{1k} \tag{5}$$

$$\mathbf{g}_{2k} = \hat{\mathbf{g}}_{2k} + \Delta \mathbf{g}_{2k}, \ k \in \mathcal{K} \tag{6}$$

where $\hat{g}_{1k}$ and $\hat{\mathbf{g}}_{2k}$ denote the imperfect estimates while $\Delta g_{1k}$ and $\Delta \mathbf{g}_{2k}$ capture the corresponding *uncertainties*. Without any statistical knowledge of the channel uncertainties, we assume that they lie in the following bounded regions

$$\mathcal{G}_{1k} \triangleq \left\{\Delta g_{1k} : \ |\Delta g_{1k}|^2 \leq \varepsilon_{1k}\right\} \tag{7}$$

$$\mathcal{G}_{2k} \triangleq \left\{\Delta \mathbf{g}_{2k} : \ \|\Delta \mathbf{g}_{2k}\|^2 \leq \varepsilon_{2k}\right\} \tag{8}$$

where $\varepsilon_{1k}$ and $\varepsilon_{2k}$ denote the radius of the uncertainty regions.

In contrast to prior contributions [5]–[8], in this paper, assuming that S is operating at a fixed data rate $R_d$ which is

[3]If the eavesdroppers are active users which co-exist with the legitimate users in the same network, the legitimate nodes can resort to blind estimation of the ECSI based on the received signals from the eavesdroppers. If the eavesdroppers are passive entities or not part of the network, the legitimate users can derive a rough estimate of the ECSI using the deterministic path loss model given a specific range within which the signals can be overheard by the eavesdroppers.

lower than its maximum achievable secrecy rate, our objective is to achieve the best compromise between the transmission reliability and security. The rationale of the proposed design approach is based on a basic result in information theoretical security [13], [14] that if the maximum achievable mutual information leakage at $\mathtt{E}_k$ is lower than $R_d$, then $\mathtt{E}_k$ fails to decode the confidential information.

Since each $\mathtt{E}_k$ can receive signals from two-hop transmission, it is assumed that each $\mathtt{E}_k$ adopts the selection diversity combining[4] and therefore, from (3) and (4), the mutual information leakage to $\mathtt{E}_k$ can be given by

$$\mathtt{C}_{\mathrm{E},k}(\sigma_{\mathrm{S}}, \mathbf{W}) = \frac{1}{2} \max \left\{ \log_2 \left( 1 + \frac{\sigma_{\mathrm{S}}^2 |g_{1k}|^2}{\sigma_{\mathrm{E},k}^2} \right), \log_2 \left( 1 + \frac{\sigma_{\mathrm{S}}^2 |\mathbf{g}_{2k}^H \mathbf{W} \mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2 \|\mathbf{g}_{2k}^H \mathbf{W}\|^2 + \sigma_{\mathrm{E},k}^2} \right) \right\} \quad (9)$$

where the coefficient $\frac{1}{2}$ reflects that the data transmission requires two orthogonal time slots. The following *robust secrecy constraints* is then proposed, which guarantees the information security for all possible realizations of the ECSI errors:

$$\mathtt{C}_{\mathrm{E},k} \leq \kappa R_d, \ \forall \Delta g_{1k} \in \mathcal{G}_{1k}, \Delta \mathbf{g}_{2k} \in \mathcal{G}_{2k}, k \in \mathcal{K} \quad (10)$$

where the parameter $0 < \kappa \leq 1$ is introduced to provide additional flexibility for adjusting the level of security.

Observe that $\sigma_{\mathrm{S}}^2$ and $\mathbf{W}$ are coupled in (9), which makes the constraint (10) difficult to tackle. In order to simplify the design, the proposed approach follows two steps. Firstly, to ensure the security of the $\mathtt{S}$–$\mathtt{E}_k$ link, we have

$$\log_2 \left( 1 + \frac{\sigma_{\mathrm{S}}^2 |g_{1k}|^2}{\sigma_{\mathrm{E},k}^2} \right) \leq 2\kappa R_d, \quad \forall \Delta g_{1k} \in \mathcal{G}_{1k}, \ k \in \mathcal{K}. \quad (11)$$

We seek the maximum $\sigma_{\mathrm{S}}^2$ and the solution is given by $\sigma_{\mathrm{S}}^2 = \left( P_{\mathrm{S}}, \min\limits_{k \in \mathcal{K}} \left\{ \frac{\gamma \sigma_{\mathrm{E},k}^2}{||\hat{g}_{1k}| + \sqrt{\varepsilon_{1k}}|^2} \right\} \right)^-$, where $\gamma \triangleq 2^{2\kappa R_d} - 1$ and $(a,b)^- \triangleq \min(a,b)$.

Secondly, with fixed $\sigma_{\mathrm{S}}^2$, we then aim to optimize $\mathbf{W}$, subject to the power constraint, in order to maximize the received SINR at $\mathtt{D}$ while ensuring the *robust secrecy constraints*. Mathematically, the robust optimization problem can be formulated as

$$\max_{\mathbf{W}} \quad \mathtt{SINR}_{\mathrm{D}} \quad (12a)$$

$$\text{s.t.} \quad \frac{\sigma_{\mathrm{S}}^2 |\mathbf{g}_{2k}^H \mathbf{W} \mathbf{h}_1|^2}{\sigma_{\mathrm{R}}^2 \|\mathbf{g}_{2k}^H \mathbf{W}\|^2 + \sigma_{\mathrm{E},k}^2} \leq \gamma, \forall \Delta \mathbf{g}_{2k} \in \mathcal{G}_{2k}, k \in \mathcal{K} \quad (12b)$$

$$\sigma_{\mathrm{S}}^2 \operatorname{Tr}\left( \mathbf{W} \mathbf{h}_1 \mathbf{h}_1^H \mathbf{W}^H \right) + \sigma_{\mathrm{R}}^2 \operatorname{Tr}\left( \mathbf{W} \mathbf{W}^H \right) \leq P_{\mathrm{R}} \quad (12c)$$

which is non-convex in $\mathbf{W}$ and the constraint (12b) renders the problem *semi-infinite* due to the continuous channel uncertainties, which motives the transformation of (12). These issues will be addressed in the next section.

[4]In this paper, the selection diversity combining is assumed at each $\mathtt{E}_k$ due to its operational simplicity. However, the proposed algorithm can be extended to other combiner such as the optimal maximum ratio combiner.

## III. Robust Secure Relaying

In this section, we derive an algorithmic solution to the robust secure relaying problem (12) by exploiting its partial convexity property. We commence by transforming (12) into a finite DC program.

### A. Transformation of (12) into a DC Program

To simplify the derivation, problem (12) can be rewritten as the following form after introducing an auxiliary variable $t$:

$$\max_{t \geq 0, \mathbf{W}} \quad \frac{1}{t} \operatorname{Tr}(\mathbf{W}^H \mathbf{H}_2 \mathbf{W} \mathbf{H}_1) \quad (13a)$$

$$\text{s.t.} \quad \sigma_{\mathrm{R}}^2 \operatorname{Tr}\left( \mathbf{W}^H \mathbf{H}_2 \mathbf{W} \right) + \sigma_{\mathrm{D}}^2 \leq t \quad (13b)$$

$$\mathbf{g}_{2k}^H \boldsymbol{\Theta}(\mathbf{W}) \mathbf{g}_{2k} \leq \gamma \sigma_{\mathrm{E},k}^2, \forall \Delta \mathbf{g}_{2k} \in \mathcal{G}_{2k}, k \in \mathcal{K} \quad (13c)$$

$$\operatorname{Tr}\left( \mathbf{W} \mathbf{A} \mathbf{W}^H \right) \leq P_{\mathrm{R}} \quad (13d)$$

where $\mathbf{H}_1 \triangleq \sigma_{\mathrm{S}}^2 \mathbf{h}_1 \mathbf{h}_1^H$, $\mathbf{H}_2 \triangleq \mathbf{h}_2 \mathbf{h}_2^H$, $\mathbf{A} \triangleq \mathbf{H}_1 + \sigma_{\mathrm{R}}^2 \mathbf{I}$ and $\boldsymbol{\Theta}(\mathbf{W}) \triangleq \mathbf{W} \left( \mathbf{H}_1 - \gamma \sigma_{\mathrm{R}}^2 \mathbf{I} \right) \mathbf{W}^H$. To tackle the semi-infiniteness of (13c), we express it as

$$\Delta \mathbf{g}_{2k}^H \boldsymbol{\Theta}(\mathbf{W}) \Delta \mathbf{g}_{2k} + 2 \operatorname{Re}\left( \hat{\mathbf{g}}_{2k}^H \boldsymbol{\Theta}(\mathbf{W}) \Delta \mathbf{g}_{1k} \right) + \hat{\mathbf{g}}_{2k}^H \boldsymbol{\Theta}(\mathbf{W}) \hat{\mathbf{g}}_{2k} - \gamma \sigma_{\mathrm{E},k}^2 \leq 0. \quad (14)$$

Then as a direct application of the $\mathcal{S}$-Procedure [15], (13c) can be equivalently recast as (15), shown on top of the next page.

Now we observe that problem (13) is still non-convex due to the following reasons. First, the objective function (13a) is the so-called quadratic-over-linear function, which is jointly convex in $(t, \mathbf{W}) \in \mathbb{R}^+ \times \mathbb{C}^{M \times M}$; therefore, maximization of a convex function is a non-convex problem. Second, the matrix inequality constraint (15) is not linear in $\mathbf{W}$. In fact, the existence of the indefinite matrix $\mathbf{H}_1 - \gamma \sigma_{\mathrm{R}}^2 \mathbf{I}$ in $\boldsymbol{\Theta}(\mathbf{W})$ makes the problem even more difficult to solve, e.g., the SDR technique can not be applied to "linearize" an indefinite quadratic term.

To this end, we propose an efficient alternative by exploiting the inherent partial convexity property of (13). We first perform the following change of variable:

$$\mathbf{Y} = \boldsymbol{\Theta}(\mathbf{W}) = \mathbf{W} \left( \mathbf{H}_1 - \gamma \sigma_{\mathrm{R}}^2 \mathbf{I} \right) \mathbf{W}^H. \quad (16)$$

Substituting (16) back into (13) and (15), we can obtain

$$\min_{t \geq 0, \mathbf{W}, \mathbf{Y}, \boldsymbol{\rho}} \quad -\frac{1}{t} \operatorname{Tr}(\mathbf{W}^H \mathbf{H}_2 \mathbf{W} \mathbf{H}_1) \quad (17a)$$

$$\text{s.t.} \quad \sigma_{\mathrm{R}}^2 \operatorname{Tr}\left( \mathbf{W}^H \mathbf{H}_2 \mathbf{W} \right) + \sigma_{\mathrm{D}}^2 \leq t \quad (17b)$$

$$\mathbf{B}(\mathbf{Y}, \rho_k) \succeq \mathbf{0}, \ \forall k \in \mathcal{K} \quad (17c)$$

$$\operatorname{Tr}\left( \mathbf{W} \mathbf{A} \mathbf{W}^H \right) \leq P_{\mathrm{R}} \quad (17d)$$

$$\mathbf{Y} = \mathbf{W} \left( \mathbf{H}_1 - \gamma \sigma_{\mathrm{R}}^2 \mathbf{I} \right) \mathbf{W}^H \quad (17e)$$

$$\rho_k \geq 0, \ \forall k \in \mathcal{K} \quad (17f)$$

where $\boldsymbol{\rho} = [\rho_1, \cdots, \rho_K]^T$. With (15) being linearized, a new challenge arises from the non-convex quadratic matrix equality constraint (17e). To transform it into a tractable form, we need the following lemma:

$$\mathbf{B}(\mathbf{W},\rho_k) \triangleq \begin{bmatrix} \rho_k\mathbf{I}-\boldsymbol{\Theta}(\mathbf{W}) & -\boldsymbol{\Theta}(\mathbf{W})\hat{\mathbf{g}}_{2k} \\ -\hat{\mathbf{g}}_{2k}^H\boldsymbol{\Theta}(\mathbf{W}) & -\hat{\mathbf{g}}_{2k}^H\boldsymbol{\Theta}(\mathbf{W})\hat{\mathbf{g}}_{2k}-\gamma\sigma_{\mathrm{E},k}^2-\varepsilon_{2k}\rho_k \end{bmatrix} \succeq \mathbf{0}. \tag{15}$$

*Lemma 1 (Lemma 1 of [16]):* Given $\mathbf{X}$, $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ of appropriate dimensions, which satisfy

$$\mathbf{X} = \mathbf{ABC} \tag{18}$$

then the matrix equality (18) is equivalent to the following inequality constraints:

$$\begin{bmatrix} \boldsymbol{\mathcal{L}}_{11} & \mathbf{X} & \mathbf{AB} \\ \mathbf{X}^H & \boldsymbol{\mathcal{L}}_{22} & \mathbf{C}^H \\ \mathbf{B}^H\mathbf{A}^H & \mathbf{C} & \mathbf{I} \end{bmatrix} \succeq \mathbf{0} \tag{19}$$

$$\mathrm{Tr}\left(\boldsymbol{\mathcal{L}}_{11}-\mathbf{ABB}^H\mathbf{A}^H\right) \le 0 \tag{20}$$

where $\boldsymbol{\mathcal{L}}_{11}$ and $\boldsymbol{\mathcal{L}}_{22}$ are auxiliary matrix variables with appropriate dimensions.

By directly applying Lemma 1 to (17e), it can be equivalently expressed as

$$\begin{bmatrix} \boldsymbol{\mathcal{L}}_{11} & \mathbf{Y} & \mathbf{W}\left(\mathbf{H}_2-\gamma\sigma_{\mathrm{R}}^2\mathbf{I}\right) \\ \mathbf{Y}^H & \boldsymbol{\mathcal{L}}_{22} & \mathbf{W} \\ \left(\mathbf{H}_2-\gamma\sigma_{\mathrm{R}}^2\mathbf{I}\right)\mathbf{W}^H & \mathbf{W}^H & \mathbf{I} \end{bmatrix} \succeq \mathbf{0} \tag{21}$$

$$\mathrm{Tr}\left(\boldsymbol{\mathcal{L}}_{11}\right) - \mathrm{Tr}\left(\mathbf{W}\left(\mathbf{H}_2-\gamma\sigma_{\mathrm{R}}^2\mathbf{I}\right)^2\mathbf{W}^H\right) \le 0 \tag{22}$$

where (21) is a linear matrix inequality (LMI) in $(\boldsymbol{\mathcal{L}}_{11},\boldsymbol{\mathcal{L}}_{22},\mathbf{W})$ and (22) is expressed as a difference of two convex functions, i.e., in DC form. To simplify the exposition, we define the following sets of variables:

$$\mathcal{W} \triangleq \{t,\mathbf{W}\} \tag{23}$$

$$\mathcal{Y} \triangleq \{\mathbf{Y},\boldsymbol{\mathcal{L}}_{11},\boldsymbol{\mathcal{L}}_{22},\boldsymbol{\rho}\} \tag{24}$$

and the compact convex set

$$\mathcal{D} \triangleq \{\{\mathcal{W},\mathcal{Y}\} : \text{(17b)–(17d)}, (21)\}. \tag{25}$$

Then replacing (17e) with (21) and (22), problem (17) can be written in the form of a DC program

$$\min_{\{\mathcal{W},\mathcal{Y}\}\in\mathcal{D}} \quad 0-\mathcal{F}_1(\mathcal{W}) \tag{26a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left(\boldsymbol{\mathcal{L}}_{11}\right)-\mathcal{F}_2(\mathbf{W}) \le 0 \tag{26b}$$

where $\mathcal{F}_1(\mathcal{W}) \triangleq \frac{1}{t}\mathrm{Tr}(\mathbf{W}^H\mathbf{H}_2\mathbf{W}\mathbf{H}_1)$ and $\mathcal{F}_2(\mathbf{W}) \triangleq \mathrm{Tr}\left(\mathbf{W}\left(\mathbf{H}_1-\gamma\sigma_{\mathrm{R}}^2\mathbf{I}\right)^2\mathbf{W}^H\right)$. The above DC structure motivates the consideration of the standard DCA (also termed as concave-convex procedure) [17]. The main idea of this approach is to find a surrogate function, e.g., first-order Taylor expansion, which linearizes each non-convex part of (26a) and (26b) around a solution obtained in the current iterate such that the original non-convex problem can iteratively be solved via a sequence of convexified subproblems. However, there are two practical challenges associated with the considered problem (26), which prevent the direct application of the standard DCA.

1) *Feasible Initialization:* The standard DCA requires a feasible initialization to start with; otherwise, it can lead to infeasibility during the iterations. Finding a feasible point for the non-convex robust design problem (26) is in general NP-hard;
2) *Inaccurate Convex Approximation:* According to the standard DCA, the concave parts $-\mathcal{F}_1$ and $-\mathcal{F}_2$ in (26a) and (26b), respectively, are approximated by their first-order Taylor expansion around a current solution point. However, this convex approximation can often be inaccurate and lead to infeasibility issue.

Motivated by the above considerations, we propose an iterative solution relying on the P-DCA in the next subsection, which eliminates the needs of a non-trivial feasible initialization while significantly improving the feasibility of the algorithm.

### *B. Iterative Solution Based on P-DCA*

Instead of (26), we now consider the following problem in conjunction with an auxiliary variable $s$ and an additional penalty term

$$\min_{\{\mathcal{W},\mathcal{Y}\}\in\mathcal{D},s} \quad -\mathcal{F}_1(\mathcal{W})+\tau s \tag{27a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left(\boldsymbol{\mathcal{L}}_{11}\right)-\mathcal{F}_2(\mathbf{W}) \le s \tag{27b}$$

$$s \ge 0 \tag{27c}$$

where $s$ can be considered as a measure of the violation of the inequality constraints (26b). Now focusing on (27), similar to the standard DCA, the concave parts $-\mathcal{F}_1$ and $-\mathcal{F}_2$ in (27a) and (27b) can be approximated by their first-order Taylor expansions around a current point $\mathcal{W}^{(n)}$ at the $n$th iteration

$$\begin{aligned}\hat{\mathcal{F}}_1(\mathcal{W};\mathcal{W}^{(n)}) = {}& \frac{1}{t^{(n)}}\mathrm{Tr}\left((\mathbf{W}^{(n)})^H\mathbf{H}_2\mathbf{W}^{(n)}\mathbf{H}_1\right) \\ & + \frac{1}{t^{(n)}}2\,\mathrm{Re}\left\{\mathrm{Tr}\left((\mathbf{W}^{(n)})^H\mathbf{H}_2\left(\mathbf{W}-\mathbf{W}^{(n)}\right)\mathbf{H}_1\right)\right\} \\ & - \frac{1}{(t^{(n)})^2}\mathrm{Tr}\left((\mathbf{W}^{(n)})^H\mathbf{H}_2\mathbf{W}^{(n)}\mathbf{B}_2\right)(t-t^{(n)})\end{aligned} \tag{28}$$

$$\begin{aligned}\hat{\mathcal{F}}_2(\mathbf{W};\mathbf{W}^{(n)}) = {}& \mathrm{Tr}\left(\mathbf{W}^{(n)}\left(\mathbf{H}_1-\gamma\sigma_{\mathrm{R}}^2\mathbf{I}\right)^2(\mathbf{W}^{(n)})^H\right) \\ & + 2\,\mathrm{Re}\left\{\mathrm{Tr}\left(\left(\mathbf{W}-\mathbf{W}^{(n)}\right)\left(\mathbf{H}_1-\gamma\sigma_{\mathrm{R}}^2\mathbf{I}\right)^2(\mathbf{W}^{(n)})^H\right)\right\}.\end{aligned} \tag{29}$$

Replacing $\mathcal{F}_1$ and $\mathcal{F}_2$ in (27), respectively with (28) and (29), we arrive at the following convexified subproblem:

$$\min_{\{\mathcal{W},\mathcal{Y}\}\in\mathcal{D},s} \quad -\hat{\mathcal{F}}_1(\mathcal{W};\mathcal{W}^{(n)})+\tau^{(n)}s \tag{30a}$$

$$\text{s.t.} \quad \mathrm{Tr}\left(\boldsymbol{\mathcal{L}}_{11}\right)-\hat{\mathcal{F}}_2(\mathbf{W};\mathbf{W}^{(n)}) \le s \tag{30b}$$

$$s \ge 0. \tag{30c}$$

The P-DCA, which solves a sequence of subproblems formulated in (30) with penalty update is summarized in Algorithm 1.

**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 (28) and (29)
2. *Solve*: Compute $\mathbf{W}^{(n+1)}$ by solving (30)
3. *Update* $\tau$: Compute the dual variable $|\lambda^{(n+1)}|$ with (30b) and set

$$\tau^{(n+1)} = \begin{cases} \tau^{(n)} & \text{if } \tau^{(n)} \geq |\lambda^{(n+1)}| + \delta_1 \\ \tau^{(n)} + \delta_2 & \text{if } \tau^{(n)} < |\lambda^{(n+1)}| + \delta_1 \end{cases} \quad (31)$$

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 $\mathbf{W}^*$.

In Algorithm 1, each subproblem (30) is always feasible provided that $\mathcal{D}$ is non-empty, which solves the possible infeasibility issue of the standard DCA. The behavior of the P-DCA can be described as follows. At first, the iterative algorithm starts with a low penalty $\tau$, thus allowing fast descent of the objective function while the constraint is temporarily allowed to be violated, i.e., $s > 0$. Then the algorithm gradually increases $\tau$ in order to force the solution to lie in the feasible region of (26).

***Initialization:*** Since the non-convex DC constraint (26b) is now relaxed to (27b), we can select an arbitrary $\mathcal{W}^{(0)}$ given that $\{\mathcal{W}^{(0)}, \mathcal{Y}^{(n)}\} \in \mathcal{D}$. In $\mathcal{D}$ defined by (25), the only constraint that bounds $\mathbf{W}$ is the relay power constraint (17d) and therefore, a simple identity matrix initialization can be used, e.g., $\mathbf{W}^{(0)} = \sqrt{\frac{P_{\mathrm{R}}}{\mathrm{Tr}(\mathbf{A})}}\mathbf{I}$ and $t^{(0)} = \frac{P_{\mathrm{R}}\,\mathrm{Tr}(\mathbf{H}_2)}{\mathrm{Tr}(\mathbf{A})} + \sigma_{\mathrm{D}}^2$ can be derived by (17b) with equality.

We now establish the convergence property of Algorithm 1, which is given in the following theorem:

*Theorem 1:* Assume that Algorithm 1 stops after finitely many iterations, at $n_k$ where $0 < n_k \leq n_{\max}$, then $\mathbf{W}^{(n_k)}$ is a stationary point of the DC program (26), and hence also a stationary point of the robust design problem (12).

*Proof:* Omitted due to the space limitation. ■

*Remark 1:* If Algorithm 1 fails to find a feasible point within finite number of iterations, this does not imply that the original robust problem (12) is infeasible, since the proposed algorithm only operates on a subset of the feasible set of the original DC program (26). In this case, a procedure similar to the admission control problem of cellular networks can be applied to either change the secrecy level by varying $\kappa$ or to relax the secrecy constraints at certain eavesdroppers. However, the design of such a procedure goes beyond the scope of the present paper.

## IV. Numerical Experiments and Discussions

This section presents numerical simulation results to evaluate the performance of the proposed transceiver design algorithm for physical layer security. In all experiments, the number of relay antennas is $N_{\mathrm{R}} = 3$, unless otherwise stated. Four eavesdroppers are considered. A flat Rayleigh fading model is employed for S–R, R–D and the estimated eavesdroppers' channels. The maximum transmit powers are normalized as $P_{\mathrm{S}} = P_{\mathrm{R}} = 1$ and the noise variances are set so that we have SNR $\triangleq \frac{P_{\mathrm{S}}}{N_{\mathrm{R}}\sigma_{\mathrm{R}}^2} = \frac{P_{\mathrm{R}}}{\sigma_{\mathrm{D}}^2}$. The noise variances and the sizes of channel uncertainty regions are identical for all the eavesdroppers and they are set to $\sigma_{\mathrm{E},k}^2 = 0.01$, $\varepsilon_{1k} = \varepsilon_1$ and $\varepsilon_{2k} = \varepsilon_2$ for all $k$. All the results are obtained by averaging 200 independent Monte Carlo runs. The optimization solver MOSEK [18] is used to solve each optimization problem.

### A. Examining the Secrecy Constraints at the Eavesdroppers

We now examine how well the information secrecy is by applying the proposed algorithm. We compare the proposed robust approach to the nonrobust version of Algorithm 1, where the ECSI errors are neglected by the legitimate users. In Fig. 2, the capacity of the link leading to each eavesdropper is shown for 2 independent sets of channel realizations. It is clearly seen that the proposed robust approach strictly enforces the secrecy constraints in both experiments. The capacity of the link leading to each eavesdropper never exceeds the data rate of the legitimate users. By contrast, in the context of the nonrobust approach, the mutual information leakage frequently violates the data rate, which grants opportunities for the eavesdroppers to decode the confidential information.

### B. Parameters Affecting the SINR Achieved at the Destination

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 legitimate users, i.e., $R_d = 1$bps/Hz and $R_d = 2$bps/Hz. In both cases, two sizes of uncertainty region for the R–E$_k$ channel are considered. Focusing on $R_d = 2$bps/Hz, It can be observed that the achieved SINR monotonically increases as the number of relay antennas increases due to the higher diversity gain exploited. Also the SINR becomes lower with an increase in the uncertainty region. Notice also that for the case of a lower data rate $R_d = 1$bps/Hz, the SINR is obviously lower than the case of $R_d = 2$bps/Hz because the legitimate users are now confined to relatively low transmit power in order to satisfy the secrecy constraints.

## V. Conclusions

This paper studied robust transceiver optimization procedures conceived for MIMO-aided relaying networks in the presence of a set of eavesdroppers. Aiming for achieving the best SRT, a robust design approach was formulated for maximizing the SINR at the receiver, while satisfying the *secrecy constraints*, which prevents the eavesdroppers from decoding the confidential information. In order to solve the formulated non-convex problem, a P-DCA algorithm was developed, which is more suitable than the standard DCA in our considered problem, and its convergence to a stationary point was established. Results of simulation experiments over Rayleigh flat fading channels confirm the security of the proposed design approach against the eavesdropping.

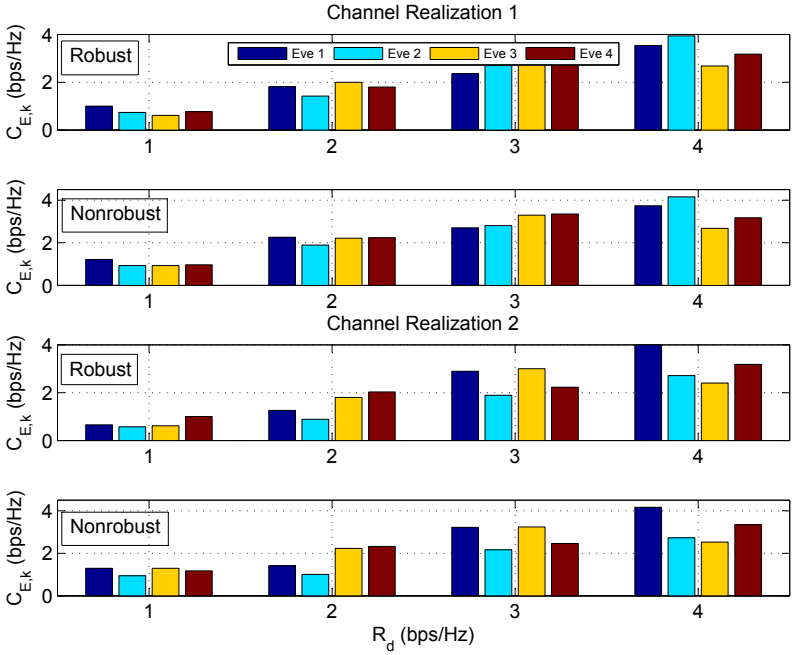


Fig. 2. Mutual information leakage to four eavesdroppers with robust and nonrobust approaches operating at different data rates for two independent experiments. (SNR=20dB, $\varepsilon_1 = 0.05$, $\varepsilon_2 = 0.1$.)

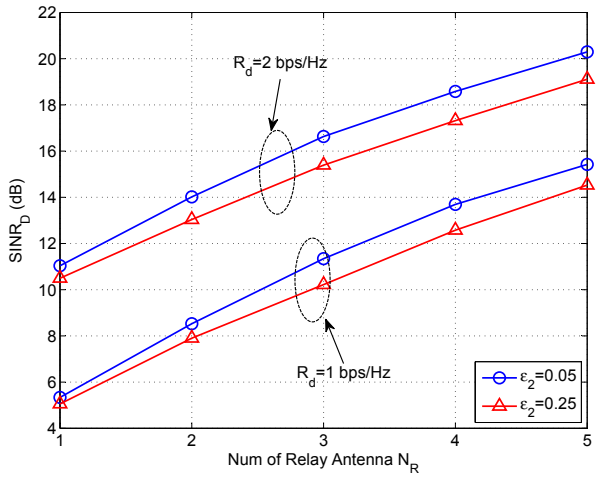


Fig. 3. The SINR achieved at the destination versus the number of relay antennas. (SNR=20dB, $\varepsilon_1 = 0.05$.)

## 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. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[3] 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.

[4] W. Chen, "CAO-SIR: Channel aware ordered successive relaying," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6513–6527, Dec. 2014.

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

[6] 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.

[7] 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.

[8] Z. Liu, C. Chen, L. Bai, H. Xiang, and J. Choi, "Transmit power minimization beamforming via amplify-and-forward relays in wireless networks with multiple eavesdroppers," in *Proc. 2014 IEEE Int. Conf. Commun. (ICC)*, Sydney, Australia, Jun. 2014, pp. 4698–4703.

[9] 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. (ICC)*, Sydney, Australia, Jun. 2014, pp. 5083–5088.

[10] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[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, Oct. 2011.

[12] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[13] C. E. Shannon, "A mathematical theory of communications," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 1948.

[14] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[16] P. Apkarian and H. D. Tuan, "Robust control via concave minimization local and global algorithms," *IEEE Trans. Autom. Control*, vol. 45, no. 2, pp. 299–305, Feb. 2000.

[17] B. K. Sriperumbudur and G. R. G. Lanckriet, "On the convergence of the concave-convex procedure," *Neural Inf. Process. Syst.*, pp. 1–9, 2009.

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