Peer-reviewed version available at Entropy 2017, 19, 522; doi:10.3390/e19100522

Article

Secure Communication for Two-way Relay Networks with Imperfect CSI

Cong Sun , Ke Liu, Dahu Zheng and Wenbao Ai *

School of Science, Beijing University of Posts and Telecommunications, No. 10, Xi Tu Cheng Lu, Beijing, 100876, China; suncong86@bupt.edu.cn

* Correspondence: wenbaoaibupt@vip.126.com; Tel.: +86-10-62281800

Abstract: This paper considers a two-way relay network, where two source nodes exchange messages through several relays in the presence of an eavesdropper, and the channel state information (CSI) of the eavesdropper is imperfectly known. The amplify-and-forward relay protocol is used and the relay beamforming weights are designed. The model is built up to minimize the total relay transmit power while guaranteeing the quality of service at users and preventing the eavesdropper from decoding the signals. Due to the imperfect CSI, a semi-infinite programming problem is obtained. An algorithm is proposed to solve the problem, and the iterative points are updated through the linesearch technique, where the feasibility are preserved during iterations. The optimality property is analyzed. The obtained subproblems are quadratic constrained quadratic programming problems, either with less than 4 constraints or with only one variable, which are solved optimally. Simulation results demonstrate the importance of the proposed model, and imply that the proposed algorithm is efficient and converges very fast, where more than 85% of the problems are solved optimally.

Keywords: physical layer security; semi-infinite programming; amplify-and-forward two-way relay; imperfect CSI; robust optimization

1. Introduction

Due to the openness and the broadcast property of wireless communication, the network security becomes a challenging issue. The physical layer security technique becomes appealing, because it guarantees the information being only accessed by the legitimate users rather than eavesdroppers. It makes use of the physical characteristics of wireless channels and is free of security key, so that the information is transmitted securely in the sense that it cannot be decoded by eavesdroppers but the legitimate users.

Physical layer security is widely studied from both information theory aspect and signal processing aspect for wiretap channels, like broadcast wiretap channels and MIMO wiretap channels. The secure communication is managed through multiple-antenna system [1–9] or node cooperation [10,11]. Researches on node cooperation are well explored. It is suitable for low-complex networks which cannot afford multiple antennas. Cooperative relay networks with amplify-and-forward (AF) [12–15] or decode-and-forward (DF) [16,17] protocols are mostly investigated. For one-way relay networks, the authors in [18,19] designs the relay beamforming weights to maximize the secrecy rate and to minimize the relay transmit power; the secrecy outage probability is analyzed for both half-duplex [20] and full-duplex relay networks [21]; in [22], the optimal relay selection schemes are considered, for both AF and DF protocols; the secure energy efficiency maximization model is proposed in [23]; the asymptotic secrecy performance for the large-scale MIMO relaying scenario is analyzed in [24], which concludes that AF protocol is a better choice compared to DF under large transmit powers. Compared to one-way relay, two-way relay networks are more efficient for communications between user pairs. In [25], the minimum per-user secrecy rate is maximized and the source power allocation is analyzed, where the relay breamforming vector lies in the nullspace of the equivalent channel of relay link from user nodes to the eavesdropper.

All the aforementioned references suppose that the CSI from users and from relays to eavesdroppers are perfectly known. In fact, it is very difficult to obtain the perfect CSI of the eavesdroppers. Assuming that no CSI of eavesdroppers is known, artificial noise is introduced in the literatures, and enhances security: [14] proposes a cooperative artificial noise transmission based secrecy strategy, and summarizes the relay beamforming design and power allocation problems as second order cone programming and linear programming problems, respectively; [15] sends the artificial noise in the nullspace of the legitimate channel, and compares the cases that all relays are working and that only the best relay is used. In [26], no CSI of eavesdroppers and imperfect CSI between users and jammers are assumed, and the secrecy performance is analyzed for the cooperative jamming (CJ) technique. Networks with imperfect CSI are often considered, too. The multi-user downlink channel is considered in [27], where the lower bound of the sum secrecy rate is maximized, and semi-definite relaxation and first order Tailor extension techniques are applied. In [28], it considers a multiple-antenna AF relay network with partial CSI and bounded error region, and maximizes the worst case secrecy rate, where a rank 2 relay beamformer is constructed via singular value decomposition (SVD). The secure communication switches between the DF relay protocol and the CJ technique in [29], and the authors provide robust designs for the secrecy rate maximization and secrecy outage probability minimization problems. In [30], both the source and the relay have multiple antennas, where it jointly designs source and relay beamforming matrices, to minimize the relay power with quality of service (QoS) constraints. The worst case Signal-to-Noise-Ratio (SNR) at the eavesdropper is considered, which is approximated by its upper bound.

As listed above, models to design relay beamforming weights with imperfect CSI are usually formulated as semi-infinite programming optimization problems. That is, some constraints should be satisfied with infinite choices of parameters [31]. Almost all the references in the wireless communication literatures deal with such problems by relaxing or tightening the corresponding constraints, so as to eliminate the semi-infinite parts and to solve the approximated problem with classical optimization techniques. This makes the optimization problem much easier. However, the approximation cuts off parts of the feasible region of the original problem, and consequently loses optimality property or even feasibility. This paper also builds up a model with imperfect CSI and formulates a semi-infinite programming problem. But the idea of the propose algorithm is quite different from the usual way, which will be introduced in detail.

In this paper, we consider a two-way relay network, with imperfect CSI from user nodes and from relays to the eavesdropper, where the eavesdropper receives signals from both user nodes and relays, and decodes signals combining the two phases. By designing the relay beamforming weights, we build up the model to minimize the relay transmit power, while the QoS of the legitimate users are guaranteed and the worst case rate of the eavesdropper is upper bounded. Rather than solving an approximated problem directly, we propose an algorithm, to solve the problem iteratively and keep the feasibility during iterations. The optimality property is analyzed. Simulations show that the curves representing the imperfect and perfect CSI models have similar trends. It is also demonstrated that the proposed model is meaningful, and the proposed algorithm is efficient and converges very fast. Numerically more than 85% of the problems are solved optimally. The rest of the paper is organized as follows. The system model of the two-way relay network with one eavesdropper is shown in Section 2. In Section 3, the corresponding optimization problem is summarized and an algorithm is proposed to solve the problem. Simulation results are shown in Section 4. The conclusion is summarized in Section 5.

Notations: Uppercase and lowercase bold-faced letters denote matrices and column vectors, respectively. $(\cdot)^H$, $(\cdot)^T$ and $(\cdot)^*$ represent the Hermitian, transpose and conjugate of a matrix, respectively. $\|\cdot\|_F$ is the Frobenius norm of a matrix. $\mathbb{E}(\cdot)$ is the mathematical expectation of a random variable. $\mathrm{Tr}(\cdot)$ represents the trace of a matrix. $\mathrm{Re}(\cdot)$ means the real part of a scaler, a vector or a matrix. $\lambda_{\max}(\cdot)$ represents for the largest eigenvalue of a Hermitian matrix. $\mathrm{Diag}(\mathbf{a})$ is the diagonal

matrix with diagonal elements as the elements of vector $\mathbf{a}$; $\mathrm{Diag}(\mathbf{A})$ is the diagonal matrix with the same diagonal elements as matrix $\mathbf{A}$.

2. System Model

We consider a half-duplex wireless communication system where two source nodes Alice (S_1) and Bob (S_2) exchange messages with N relay nodes $R_n, n = 1, 2, \ldots, N$, in the presence of an eavesdropper Eve, which eavesdrops signals from the two source nodes and relay nodes passively, as illustrated in Fig. 1. Each relay node has a single antenna and the AF protocol is applied. We

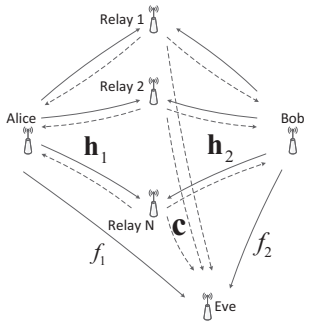

Figure 1. Secure communication model for the two-way relay network

assume perfect CSI between users and relays is known. However, the CSI between the users and the eavesdropper, and that between relays and the eavesdropper is assumed to be imperfect, where it is estimated with bounded error. The channel vector between source node S_j and the N relay nodes is $\mathbf{h}_j \in \mathbb{C}^{N\times 1}$, $j = 1, 2$. The channel vector between relay nodes and the eavesdropper is

$$\mathbf{c} = \mathbf{c}_0 + \Delta\mathbf{c}, \|\Delta\mathbf{c}\| \leq \varepsilon, \tag{1}$$

where $\mathbf{c}_0 \in \mathbb{C}^{N\times 1}$ is perfectly known, $\Delta\mathbf{c} \in \mathbb{C}^{N\times 1}$ is the estimated error vector and $\|\Delta\mathbf{c}\|_2 \leq \varepsilon_0$. Similarly, the imperfect CSI from the two source nodes to Eve are $f_1 \in \mathbb{C}$ and $f_2 \in \mathbb{C}$, respectively, where

$$f_j = f_j^0 + \Delta f_j, \quad |\Delta f_j| \leq \varepsilon_j, \quad j = 1, 2, \tag{2}$$

f_j^0 is the estimated channel, and Δf_j satisfying $|\Delta f_j| \leq \varepsilon_j$ is the channel estimated error.

In the first phase, Alice and Bob transmit $x_j = \sqrt{P_j}s_j$, $j = 1, 2$ to all relays, respectively, where P_j is the transmit power and $s_j \in \mathbb{C}$ is the information symbol with $\mathbb{E}(|s_j|^2) = 1$. Then relays receive

$$\mathbf{y}_R = \mathbf{h}_1 x_1 + \mathbf{h}_2 x_2 + \mathbf{n}_R,$$

where $\mathbf{n}_R \in \mathbb{C}^{N\times 1}$ is the local noise at relays with zero mean and covariance matrix as $\sigma_R^2\mathbf{I}_N$. Besides, Eve also receives signals from Alice and Bob as

$$y_{E1} = f_1 x_1 + f_2 x_2 + n_{E1},$$

where $n_{E1} \sim \mathcal{N}(0, \sigma_{E1}^2)$ is the local noise at Eve in the first phase.

In the second phase, the ith relay multiples its received signal by its beamforming weight w_i and then broadcast the signal to both users. Thus, the vector transmitted by relays is represented as $\mathbf{x} = \mathbf{W}^H\mathbf{y}_R + \mathbf{n}_R$, where $\mathbf{W} = \mathrm{Diag}(\mathbf{w})$ and $\mathbf{w} = (w_1, w_2, \ldots, w_N)^T$. Alice receives

$$y_1 = \mathbf{h}_1^T\mathbf{x} + n_1 = \underbrace{\mathbf{h}_1^T\mathbf{W}^H\mathbf{h}_1\sqrt{P_1}s_1}_{\text{self-cancelled signal}} + \underbrace{\mathbf{h}_1^T\mathbf{W}^H\mathbf{h}_2\sqrt{P_2}s_2}_{\text{desired signal}} + \underbrace{\mathbf{h}_1^T\mathbf{W}^H\mathbf{n}_R + z_1}_{\text{noise}},$$

where $z_1 \sim \mathcal{N}(0, \sigma_1^2)$ is the local noise. It consists of the self-canceled signal, which is perfectly known by Alice and is canceled locally, the desired signal from Bob and the noise. The received signal at Bob has similar expression. Meanwhile, Eve receives signals from relays as

$$y_{E2} = \mathbf{c}^T \mathbf{W}^H \mathbf{y}_R + n_{E2} = \mathbf{c}^T \mathbf{W}^H (\mathbf{h}_1 \sqrt{P_1} s_1 + \mathbf{h}_2 \sqrt{P_2} s_2 + \mathbf{n}_R) + n_{E2},$$

where $n_{E2} \sim \mathcal{N}(0, \sigma_{E2}^2)$ is the local noise at Eve in the second phase.

Since the two source nodes subtract their self-canceled terms, the SNRs achieved at Alice and Bob can be respectively expressed as

$$\begin{aligned} \mathrm{SNR}_1 &= \frac{P_2 |\mathbf{h}_1^T \mathbf{W}^H \mathbf{h}_2|^2}{\sigma_R^2 \|\mathbf{h}_1^T \mathbf{W}^H\|^2 + \sigma_1^2} = \frac{P_2 |\mathbf{w}^H \mathbf{H}_1 \mathbf{h}_2|^2}{\sigma_R^2 \|\mathbf{w}^H \mathbf{H}_1\|^2 + \sigma_1^2}, \\ \mathrm{SNR}_2 &= \frac{P_1 |\mathbf{h}_2^T \mathbf{W}^H \mathbf{h}_1|^2}{\sigma_R^2 \|\mathbf{h}_2^T \mathbf{W}^H\|^2 + \sigma_2^2} = \frac{P_1 |\mathbf{w}^H \mathbf{H}_2 \mathbf{h}_1|^2}{\sigma_R^2 \|\mathbf{w}^H \mathbf{H}_2\|^2 + \sigma_2^2}. \end{aligned}$$

Suppose Eve is intelligent and tries to decode signals s_1 and s_2 by combining the information received in both phases, which is expressed as

$$y_E = \mathbf{H}_E \mathbf{x} + \mathbf{n}_E,$$

where

$$\mathbf{H}_E = \begin{pmatrix} f_1 & f_2 \\ \mathbf{w}^H \mathbf{C} \mathbf{h}_1 & \mathbf{w}^H \mathbf{C} \mathbf{h}_2 \end{pmatrix}, \text{ and } \mathbf{n}_E = (n_{E1}, n_{E2})^T.$$

Suppose all the transmit signals and all the local noises are independent of each other. The achievable rate of Eve is denoted as

$$R_E = \frac{1}{2} \log_2 |\mathbf{I}_2 + \mathbf{K}_E^{-1} \mathbf{H}_E \mathbf{Q} \mathbf{H}_E^H|.$$

Here $\mathbf{K}_E = \mathrm{Diag}(\sigma_{E1}^2, \sigma_{E2}^2 + \sigma_R^2 \mathbf{w}^H \mathbf{C} \mathbf{C}^H \mathbf{w})$ and $\mathbf{Q} = \mathrm{Diag}(P_1, P_2)$. Accordingly, the achievable rate of Eve is simplified as

$$\begin{aligned} R_E &= \frac{1}{2} \log_2 \Big(1 + \frac{P_1 |f_1|^2 + P_2 |f_2|^2}{\sigma_{E1}^2} + \frac{P_1 |\mathbf{w}^H \mathbf{C} \mathbf{h}_1|^2 + P_2 |\mathbf{w}^H \mathbf{C} \mathbf{h}_2|^2}{\sigma_{E2}^2 + \sigma_R^2 \mathbf{w}^H \mathbf{C} \mathbf{C}^H \mathbf{w}} \\ &\quad + \frac{(P_1 |f_1|^2 + P_2 |f_2|^2)(P_1 |\mathbf{w}^H \mathbf{C} \mathbf{h}_1|^2 + P_2 |\mathbf{w}^H \mathbf{C} \mathbf{h}_2|^2)}{\sigma_{E1}^2 (\sigma_{E2}^2 + \sigma_R^2 \mathbf{w}^H \mathbf{C} \mathbf{C}^H \mathbf{w})} - \frac{|P_1 f_1 \mathbf{h}_1^H \mathbf{C}^H \mathbf{w} + P_2 f_2 \mathbf{h}_2^H \mathbf{C}^H \mathbf{w}|^2}{\sigma_{E1}^2 (\sigma_{E2}^2 + \sigma_R^2 \mathbf{w}^H \mathbf{C} \mathbf{C}^H \mathbf{w})} \Big) \\ &= \frac{1}{2} \log_2 (1 + Rf) \end{aligned}$$

where[1]

$$Rf = \frac{P_1 |f_1|^2 + P_2 |f_2|^2}{\sigma_{E1}^2} + \frac{P_1 |\mathbf{w}^H \mathbf{C} \mathbf{h}_1|^2 + P_2 |\mathbf{w}^H \mathbf{C} \mathbf{h}_2|^2}{\sigma_{E2}^2 + \sigma_R^2 \mathbf{w}^H \mathbf{C} \mathbf{C}^H \mathbf{w}} + \frac{P_1 P_2 |f_1 \mathbf{w}^H \mathbf{C} \mathbf{h}_2 - f_2 \mathbf{w}^H \mathbf{C} \mathbf{h}_1|^2}{\sigma_{E1}^2 (\sigma_{E2}^2 + \sigma_R^2 \mathbf{w}^H \mathbf{C} \mathbf{C}^H \mathbf{w})},$$

$\mathbf{C} = \mathrm{Diag}(\mathbf{c})$ and $\mathbf{H}_j = \mathrm{Diag}(\mathbf{h}_j)$, $j = 1, 2$.

In the following, we will design the relay beamforming vector $\mathbf{w}$, aiming to minimize the total relay transmit power. Meanwhile we maintain the SNRs at both legitimate users above some thresholds, so that the communication between the user pair is guaranteed; we require the achievable rate of the eavesdropper to be below some standard, in order to prevent Eve from decoding

[1] This deduces from the fact that $(|a_1|^2 + |a_2|^2)(|b_1|^2 + |b_2|^2) - |a_1 b_1^* + a_2 b_2^*|^2 = |a_1 b_2 - a_2 b_1|^2$, which holds for any complex scalars a_j, b_j. Here $a_j = \sqrt{P_j} f_j$, $b_j = \sqrt{P_j} \mathbf{w}^H \mathbf{C} \mathbf{h}_j$, $j = 1, 2$.

the communicating signals. We summarize the optimization model as the following semi-infinite programming problem:

$$\begin{aligned} \min_{\mathbf{w}\in\mathbb{C}^{N\times 1}} \quad & P_R(\mathbf{w}) && \text{(3a)}\\ \text{s.t.} \quad & \mathrm{SNR}_j(\mathbf{w}) \geq \gamma_j, \quad j=1,2; && \text{(3b)}\\ & R_E(\Delta\mathbf{c},\Delta f_1,\Delta f_2;\mathbf{w}) = \frac{1}{2}\log_2(1+Rf) \leq r_E, \\ & \text{for all } \|\Delta\mathbf{c}\|_2 \leq \varepsilon, |\Delta f_j| \leq \varepsilon_j, j=1,2. && \text{(3c)} \end{aligned}$$

where the relay transmit power is

$$\begin{aligned} P_R &= E(\mathbf{x}^H\mathbf{x}) = Tr(E((\mathbf{W}^H\mathbf{y}_R)(\mathbf{W}^H\mathbf{y}_R)^H)) \\ &= P_1\mathbf{w}^H\mathbf{H}_1\mathbf{H}_1^H\mathbf{w} + P_2\mathbf{w}^H\mathbf{H}_2\mathbf{H}_2^H\mathbf{w} + \sigma_R^2\mathbf{w}^H\mathbf{w}, \end{aligned}$$

and γ_1, γ_2, r_E are the given thresholds. Due to the imperfect CSI of Eve, we require that the achievable rate of Eve should be less than some threshold under all possible channel coefficients, so that Eve cannot decode the signals and obtain the useful information even in the worst case.

3. The robust model against the imperfect CSI

In this section, we propose a robust model as well as an efficient algorithm to solve problem (3).

3.1. Robust model formulation

In this subsection, we eliminate the parameters $\Delta f_j, j=1,2$ and obtain a new robust optimization problem. There are several parameters in the semi-indefinite constraint (3c), which are coupled together and thus make the problem intractable. We tighten the constraint (3c) by replacing it with the upper bound, which holds for all $|\Delta f_j| \leq \varepsilon_j, j=1,2$. To obtain the upper bound, we apply the following lemma. Suppose $\mathbf{x}$ and $\mathbf{y}$ are two n-dimensional complex vectors. Then $\mathrm{Re}(\mathbf{x}^H\mathbf{y}) \leq \eta\|\mathbf{y}\|_2$ holds for any $\|\mathbf{x}\|_2 \leq \eta$. The equality holds if and only if $\mathbf{x} = \eta\mathbf{y}/\|\mathbf{y}\|_2$.

Proof. Let $\mathbf{x}_R$ and $\mathbf{x}_I$ be the real and imaginary part of $\mathbf{x}$, respectively, and define $\mathbf{y}_R$ and $\mathbf{y}_I$ similarly. Then

$$\mathbf{x}^H\mathbf{y} = (\mathbf{x}_R + i\mathbf{x}_I)^H(\mathbf{y}_R + i\mathbf{y}_I) = (\mathbf{x}_R^T\mathbf{y}_R + \mathbf{x}_I^T\mathbf{y}_I) + i(\mathbf{x}_R^T\mathbf{y}_I - \mathbf{x}_I^T\mathbf{y}_R).$$

Thus $\mathrm{Re}(\mathbf{x}^H\mathbf{y}) = \mathbf{x}_R^T\mathbf{y}_R + \mathbf{x}_I^T\mathbf{y}_I$. The necessary condition to maximize $\mathrm{Re}(\mathbf{x}^H\mathbf{y})$ is that $\mathbf{x}_R$ and $\mathbf{x}_I$ are parallel to $\mathbf{y}_R$ and $\mathbf{y}_I$, respectively. This means that $\mathbf{x}$ should be parallel to $\mathbf{y}$. Further with the condition $\|\mathbf{x}\|_2 \leq \eta$, we can deduce the conclusion. □

By applying Lemma 3.1, we deduce that

$$Rf(\Delta\mathbf{c},\Delta f_1,\Delta f_2;\mathbf{w}) \leq \frac{\sum_{j=1}^2 P_j(|f_j^0|+\varepsilon_j)^2}{\sigma_{E1}^2} + \bar{Rf}(\Delta\mathbf{c};\mathbf{w}), \tag{4}$$

where

$$a_0 = \frac{P_1P_2\sum_{j=1}^2(|f_j^0|+\varepsilon_j)^2}{\sigma_{E1}^2} \text{ and } \bar{Rf}(\Delta\mathbf{c};\mathbf{w}) = \frac{(P_1+a_0)|\mathbf{w}^H\mathbf{C}\mathbf{h}_1|^2 + (P_2+a_0)|\mathbf{w}^H\mathbf{C}\mathbf{h}_2|^2}{\sigma_{E2}^2 + \sigma_R^2\mathbf{w}^H\mathbf{C}\mathbf{C}^H\mathbf{w}}.$$

The detailed deduction is shown in Appendix A.

The tightened problem becomes:

$$\min_{\mathbf{w}\in\mathbb{C}^{N\times 1}} \quad P_R(\mathbf{w}) \tag{5a}$$
$$\text{s.t.} \quad \text{SNR}_j(\mathbf{w}) \geq \gamma_j, \ \ j=1,2; \tag{5b}$$
$$\bar{Rf}(\Delta\mathbf{c};\mathbf{w}) \leq \gamma_E, \text{for all } \|\Delta\mathbf{c}\|_2 \leq \varepsilon, \tag{5c}$$

where

$$\gamma_E = 2^{2r_E} - 1 - \frac{\sum_{j=1}^{2} P_j(|f_j^0| + \varepsilon_j)^2}{\sigma_{E1}^2}.$$

In this robust optimization problem, $\Delta\mathbf{c}$ is the parametric vector with uncertainty. In the rest of this section, we focus on the tightened problem (5).

3.2. Algorithm preserving feasibility

With the constraint (5c), problem (5) is still a semi-infinite programming problem and difficult to solve directly. In this subsection, we will propose an efficient algorithm to solve the problem (5) iteratively and preserves feasibility during iterations.

First, we tighten the constraints and eliminate the vector $\Delta\mathbf{c}$. The algorithm is initialized by solving the following tightened subproblem:

$$\min_{\mathbf{w}\in\mathbb{C}^{N\times 1}} \quad P_R(\mathbf{w}) \tag{6a}$$
$$\text{s.t.} \quad \text{SNR}_j(\mathbf{w}) \geq (1+\beta^{\delta_0})\gamma_j, \ \ j=1,2; \tag{6b}$$
$$\hat{Rf}(\mathbf{w}) \leq (1-\beta^{\delta_0})\gamma_E. \tag{6c}$$

Here $\hat{Rf}(\mathbf{w}) = \frac{1}{\sigma_{E2}^2}[\mathbf{w}^H\mathbf{C}_0\mathbf{Q}\mathbf{C}_0^H\mathbf{w} + 2\varepsilon\|\mathbf{c}_0\|_2\|\mathbf{Q}\|_F\|\mathbf{w}\|_2^2 + \varepsilon^2\mathbf{w}^H\text{Diag}(\mathbf{Q}_0)\mathbf{w}]$. $\mathbf{C}_0 = \text{Diag}(\mathbf{c}_0)$, $\Delta\mathbf{C} = \text{Diag}(\Delta\mathbf{c})$, $\mathbf{Q}_0 = \sum_{j=1}^{2}(P_j + a_0)\mathbf{h}_j\mathbf{h}_j^H$ and $\mathbf{Q} = \mathbf{Q}_0 - \sigma_R^2\gamma_E\mathbf{I}_N$; $0 < \beta < 1$ is a scalar, and $\delta \geq 1$ is a positive integer.

By transformation, (6) is equivalent to the following Quadratic Constrained Quadratic Programming (QCQP) problem.

$$\min_{\mathbf{w}\in\mathbb{C}^{N\times 1}} \quad \mathbf{w}^H\mathbf{A}_0\mathbf{w}$$
$$\text{s.t.} \quad \mathbf{w}^H\mathbf{A}_j\mathbf{w} \leq a_j, \ \ j=1,2,3, \tag{7}$$

where $\mathbf{A}_0 = P_1\mathbf{H}_1\mathbf{H}_1^H + P_2\mathbf{H}_2\mathbf{H}_2^H + \sigma_R^2\mathbf{I}_N$, $\mathbf{A}_1 = \mathbf{H}_1(\sigma_R^2\mathbf{I}_N - P_2\mathbf{h}_2\mathbf{h}_2^H)\mathbf{H}_1^H$, $\mathbf{A}_2 = \mathbf{H}_2(\sigma_R^2\mathbf{I}_N - P_1\mathbf{h}_1\mathbf{h}_1^H)\mathbf{H}_2^H$, $\mathbf{A}_3 = \mathbf{C}_0\mathbf{Q}\mathbf{C}_0^H + 2\varepsilon\|\mathbf{c}_0\|_2\|\mathbf{Q}\|_F\mathbf{I}_N + \varepsilon^2\text{Diag}(\mathbf{Q}_0)$, $a_3 = \sigma_{E2}^2(1-\beta^{\delta_0})\gamma_E$, and $a_j = -\sigma_j^2(1+\beta^{\delta_0})\gamma_j$ for $j=1,2$. It is solved optimally by semi-definite relaxation method, because subproblem (7) only has 3 constraints [32,33]. The following lemma shows that solving (6) provides an initial feasible point of problem (5). The solution of subproblem (6) $\mathbf{w}_0$ is a strictly feasible point of problem (5). The proof is shown in Appendix B. $\mathbf{w}_0$ is a strictly feasible rather than a feasible point of problem (5), thanks to the parameters β and δ_0 in subproblem (6). It is an important technique for the improvement of the objective function during the iterations.

In the kth iteration, suppose we have the iterative point $\mathbf{w}_k$ which is a strictly feasible point of problem (5). Specifically it satisfies:

$$\text{SNR}_j(\mathbf{w}) \geq (1+\beta^{\delta_k})\gamma_j, \ \ j=1,2; \tag{8a}$$
$$\bar{Rf}(\Delta\mathbf{c};\mathbf{w}) \leq (1-\beta^{\delta_k})\gamma_E, \text{for all } \|\Delta\mathbf{c}\|_2 \leq \varepsilon. \tag{8b}$$

We will update the iterative point using the linesearch technique [34] and preserve its feasibility according to problem (5). First we solve the following subproblem and achieve its optimal solution $\Delta\mathbf{c}_k$:

$$\max_{\Delta\mathbf{c}} \ \bar{Rf}(\Delta\mathbf{c};\mathbf{w}_k) \ \text{ s. t. } \ \|\Delta\mathbf{c}\| \le \varepsilon. \tag{9}$$

It is equivalent to the subproblem below:

$$\begin{aligned} \min_{\Delta\mathbf{c},r} \ & \frac{\sigma_{E2}^2 + \sigma_R^2(\mathbf{c}_0+\Delta\mathbf{c})^T\mathbf{W}_k^H\mathbf{W}_k(\mathbf{c}_0+\Delta\mathbf{c})^*}{r^2} \\ \text{s. t.} \ & \sum_{j=1}^{2}(P_j+a_0)|(\mathbf{c}_0+\Delta\mathbf{c})^T\mathbf{W}_k^H\mathbf{h}_j|^2 = r^2, \\ & \|\Delta\mathbf{c}\| \le \varepsilon, \end{aligned} \tag{10}$$

where $\mathbf{W}_k = \mathrm{Diag}(\mathbf{w}_k)$. Let $\mathbf{x} = ((\mathbf{c}_0+\Delta\mathbf{c})^H, 1)^T/r$, and it is further transformed into the following QCQP problem:

$$\begin{aligned} \min_{\mathbf{x}\in\mathbb{C}^{N+1}} \ & \mathbf{x}^H\mathbf{B}_0\mathbf{x} \\ \text{s. t.} \ & \mathbf{x}^H\mathbf{B}_1\mathbf{x} = 1, \\ & \mathbf{x}^H\mathbf{B}_2\mathbf{x} \le 0. \end{aligned}$$

Here

$$B_0 = \begin{bmatrix} \sigma_R^2\mathbf{W}_k^H\mathbf{W}_k & \mathbf{0} \\ \mathbf{0} & \sigma_{E2}^2 \end{bmatrix}, B_1 = \begin{bmatrix} \sum_{j=1}^2(P_j+a_0)\mathbf{W}_k^H\mathbf{h}_j\mathbf{h}_j^H\mathbf{W}_k & \mathbf{0} \\ \mathbf{0} & 0 \end{bmatrix}, B_2 = \begin{bmatrix} \mathbf{I}_N & -\mathbf{c}_0^* \\ -\mathbf{c}_0^T & \mathbf{c}_0^H\mathbf{c}_0 - \varepsilon^2 \end{bmatrix}.$$

With only 2 constraints, it is solved optimally by the semi-definite relaxation method. It holds that $\bar{Rf}(\Delta\mathbf{c}_k;\mathbf{w}_k) \le (1-\beta^{\delta_k})\gamma_E$, as $\mathbf{w}_k$ satisfies (8b).

Then we plug in $\Delta\mathbf{c}_k$ into constraint (8b), and obtain the subproblem below:

$$\begin{aligned} \min_{\mathbf{w}\in\mathbb{C}^{N\times 1}} \ & P_R(\mathbf{w}) \\ \text{s.t.} \ & \mathrm{SNR}_j(\mathbf{w}) \ge (1+\beta^{\delta_k})\gamma_j, \ \ j=1,2; \\ & \bar{Rf}(\Delta\mathbf{c}_k;\mathbf{w}) \le (1-\beta^{\delta_k})\gamma_E. \end{aligned} \tag{11}$$

It is equivalent to the QCQP subproblem with 3 constraints:

$$\begin{aligned} \min_{\mathbf{w}\in\mathbb{C}^{N\times 1}} \ & \mathbf{w}^H\mathbf{A}_0\mathbf{w} \\ \text{s.t.} \ & \mathbf{w}^H\mathbf{A}_j\mathbf{w} \le -\sigma_j^2(1+\beta^{\delta_k})\gamma_j, \ \ j=1,2; \\ & \mathbf{w}^H\mathbf{C}_k\mathbf{Q}\mathbf{C}_k^H\mathbf{w} \le (1-\beta^{\delta_k})\sigma_{E2}^2\gamma_E, \end{aligned}$$

where $\mathbf{C}_k = \mathrm{Diag}(\mathbf{c}_k)$ and $\mathbf{c}_k = \mathbf{c}_0 + \Delta\mathbf{c}_k$. $\mathbf{A}_0$ and $\mathbf{A}_j$, $j = 1,2$ are defined below (7). It is solved optimally by the semi-definite relaxation method. Let its solution be $\tilde{\mathbf{w}}_{k+1}$. Apparently $\tilde{\mathbf{w}}_{k+1}$ satisfies constraint (8a), but it may not satisfy constraint (8b).

Next, we introduce a new scalar variable t as the stepsize, and search along the line of $(\tilde{\mathbf{w}}_{k+1} - \mathbf{w}_k)$, to obtain the new iterative point $\mathbf{w}_{k+1}(t) := \mathbf{w}_k + t(\tilde{\mathbf{w}}_{k+1} - \mathbf{w}_k)$ which satisfies (8) and improves the objective function value. The corresponding subproblem is:

$$\min_{t\in\mathbb{R}} \quad P_R(\mathbf{w}_{k+1}(t)) \tag{12a}$$
$$\text{s.t.} \quad \mathrm{SNR}_j(\mathbf{w}_{k+1}(t)) \geq (1+\beta^{\delta_k})\gamma_j, \quad j=1,2; \tag{12b}$$
$$g_k(t) \leq 0, \tag{12c}$$

where $g_k(t) = m_1 t^2 + m_2 t + m_3|t| + m_4$ with

$$\begin{aligned}
m_1 &= \mathbf{c}_0^T(\mathbf{V}_1-\mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1-\mathbf{V}_0)\mathbf{c}_0^* + 2\varepsilon\|(\mathbf{V}_1-\mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1-\mathbf{V}_0)\mathbf{c}_0^*\| \\
&\quad +\varepsilon^2\lambda_{\max}[(\mathbf{V}_1-\mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1-\mathbf{V}_0)], \\
m_2 &= 2\mathrm{Re}[\mathbf{c}_0^T\mathbf{V}_0^H\mathbf{Q}(\mathbf{V}_1-\mathbf{V}_0)\mathbf{c}_0^*], \\
m_3 &= 2\varepsilon[\|\mathbf{V}_0^H\mathbf{Q}(\mathbf{V}_1-\mathbf{V}_0)\mathbf{c}_0^*\| + \|(\mathbf{V}_1-\mathbf{V}_0)^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^*\|] \\
&\quad +\varepsilon^2\lambda_{\max}[\mathbf{V}_0^H\mathbf{Q}(\mathbf{V}_1-\mathbf{V}_0) + (\mathbf{V}_1-\mathbf{V}_0)^H\mathbf{Q}\mathbf{V}_0], \\
m_4 &= \mathbf{c}_0^T\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^* + 2\varepsilon\|\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^*\| + \varepsilon^2\lambda_{\max}(\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0) - (1-\beta^{\delta_k})\sigma_{E2}^2\gamma_E.
\end{aligned}$$

Here $\mathbf{V}_0$ and $\mathbf{V}_1$ represents for $\mathrm{Diag}(\mathbf{w}_k)$ and $\mathrm{Diag}(\tilde{\mathbf{w}}_{k+1})$, respectively.

$t=0$ is always a feasible point of (12). $\mathbf{w}_{k+1}(t)$ satisfies constraints (8), where t is any feasible point of subproblem (12). The detailed proof is shown in Appendix C. As a one-dimensional QCQP problem, subproblem (12) can be solved optimally by the discussion of line segment intersections. Suppose t_k is the optimal stepsize. Theorem 3.2 shows that the updated iterative point $\mathbf{w}_{k+1} := \mathbf{w}_{k+1}(t_k)$ is a feasible point of problem (5). As $t=0$ is a feasible point of (12), we can deduce that $P_R(\mathbf{w}_{k+1}) \leq P_R(\mathbf{w}_k)$, that is, the objective function value decreases monotonically. It is possible that $t_k = 0$. This means the iterative point might stuck at some point. In such situation, we increase the parameter δ_k in subproblem (12), to seek for further improvement of the objective function. The complete algorithm framework is described as Algorithm 1 in next page.

input : β, δ and η.
output: the relay beamforming vector $\mathbf{w}_k$
0. Solve subproblem (6) and obtain its solution $\mathbf{w}_0$. $k=0$.
repeat
  1. Obtain $\Delta\mathbf{c}_k$ by solving subproblem (9);
  2. Obtain $\tilde{\mathbf{w}}_{k+1}$ by solving subproblem (9);
  if $\delta_k \geq \delta$ *and* $\|\tilde{\mathbf{w}}_{k+1}-\mathbf{w}_k\| \leq \eta\|\mathbf{w}_k\|$ **then**
    Stop the algorithm;
  end
  3. Obtain t_k by solving subproblem (12);
  4. **if** $t_k = 0$ **then**
    if $\delta_k \geq \delta$ **then**
      Stop the algorithm;
    end
    Let $\delta_k := \delta_k + 1$. Go back to Step 3;
  end
  Let $\mathbf{w}_{k+1} := \mathbf{w}_k + t_k(\tilde{\mathbf{w}}_{k+1}-\mathbf{w}_k)$, $k := k+1$;
until *The objective function value converges*;

Algorithm 1: Robust optimization algorithm

The algorithm framework shows that the solution obtained by Algorithm 1 is at least a feasible point of problem (5). The following theorem shows the optimality property of the achieved solution, whose proof is given in Appendix D. If δ_k goes to infinity and $\tilde{\mathbf{w}}_{k+1} = \mathbf{w}_k$, then $\mathbf{w}_k$ is the optimal solution of problem (5).

4. Simulations

In this section, the performances of the proposed model and algorithm are evaluated. Each element of the channel coefficients $\mathbf{h}_j, j = 1, 2$ and $\mathbf{c}_0$ obeys Gaussian random distribution as $\mathcal{CN}(0, 1)$. Here we suppose that users have used some techniques, such like artificial noise, to reduce the possibility to be eavesdropped directly, so that the channel from users to Eve is very weak: $f_j^0, j = 1, 2$ obey $\mathcal{CN}(0, 0.01)$. The uncertainty of the parameters are bounded according to their estimated values: $\varepsilon = 0.1\|\mathbf{c}_0\|_2$, $\varepsilon_j = 0.1|f_j^0|$, $j = 1, 2$. Let $\sigma_j = \sigma_{E1} = \sigma_{E2} = 1$ and $\gamma_j = \gamma$, $j = 1, 2$. The stopping parameter η in the proposed algorithm is set as 10^{-4}. For each plotted point, 1000 realizations are generated and the average result is shown. The semi-definite relaxation method is implemented based on the software CVX [35].

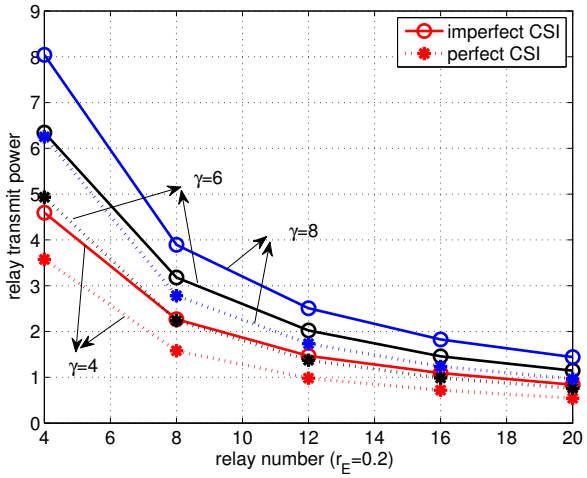

Figure 2. Comparison between imperfect and perfect CSI models, with respect to different relay numbers and different γ. Here $r_E = 0.2$.

The performances of the imperfect CSI model and the perfect CSI model are compared. The curves representing the imperfect CSI model show the relay transmit power obtained by the proposed algorithm, with $\beta = 0.1$ and $\delta_0 = 15$; in the perfect CSI model, the uncertain parameters are specified and fixed, where the corresponding optimization problem is equivalent to a QCQP problem similar to (7), and is solved optimally by the semi-definite relaxation method. The results of both imperfect and perfect CSI models with respect to different relay numbers are depicted in Fig. 2 and Fig. 3. In Fig. 2, the SNR threshold for users, γ, varies from 4 to 8, while the rate upper bound for Eve, r_E is fixed as 0.2. To the contrary, in Fig. 3, $\gamma = 6$, while r_E is set as $0.15, 0.2$ and 0.25 for comparison. For the same parameters, the relay transmit power obtained by the perfect CSI model is always smaller than that by the imperfect CSI. This phenomenon is reasonable. Because in the imperfect CSI model the rate constraint for Eve is satisfied for all possible parameters $\Delta\mathbf{c}$ and $\Delta f_j, j = 1, 2$, while in the perfect CSI model, it is satisfied for fixed parameters. The curves representing the imperfect CSI have similar trends as those representing the perfect CSI. It is observed that the relay transmit power, P_R, reduces significantly when the number of relays, N, increases from 4 to 8, and P_R reduces smoothly when N further increases. It illustrates the effectiveness of node cooperation. Fig. 2 and Fig. 3 also show that P_R increases with the increment of γ and r_E, respectively. This implies that the relay transmit power should be increased if the system requires higher QoS of users; however this also provides more information to Eve. Such contradiction highlights the importance of the proposed model in Section 2, which balances between the users' QoS requirements and the security demand.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 July 2017 doi:10.20944/preprints201707.0088.v1

Peer-reviewed version available at Entropy 2017, 19, 522; doi:10.3390/e19100522

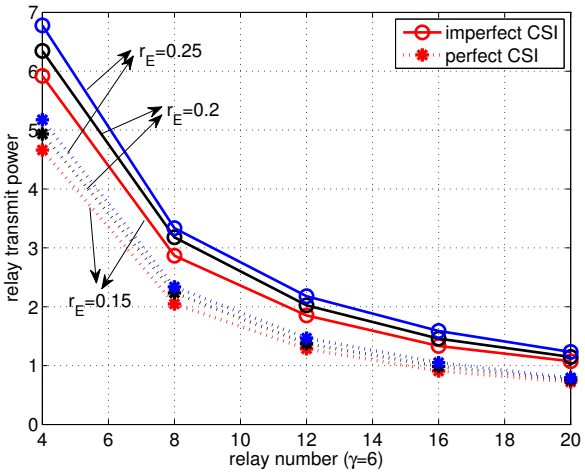

Figure 3. Comparison between imperfect and perfect CSI models, with respect to different relay numbers and different r_E. Here $\gamma = 6$.

Next, we test the sensitivity of the proposed algorithm according to different parameters. Fig. 4 shows the results by the proposed algorithm with three groups of parameters: $\beta = 0.1, \delta = 15$; $\beta = 0.1, \delta = 20$; $\beta = 0.01, \delta = 15$. The three curves representing three groups are close to each other, which implies that the algorithm is not sensitive to the parameters. By zooming in we observe that smaller β and larger δ improve the performance of the algorithm. In fact, smaller β and larger δ makes $1 + \beta^\delta$ and $1 - \beta^\delta$ closer to 1, and thus the constraints in the subproblems are more approaching the original constraints.

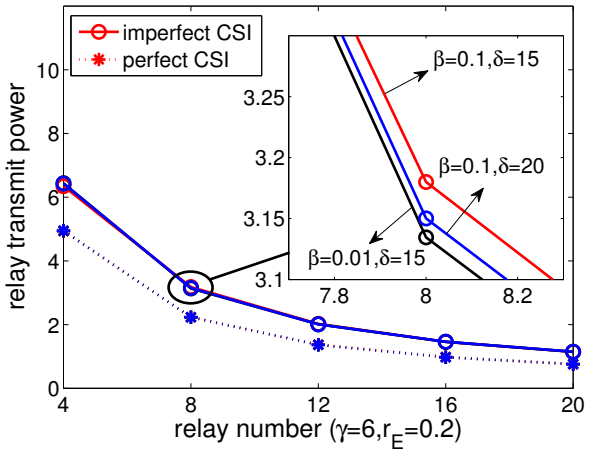

Figure 4. Achieved relay transmit power by the proposed algorithm with different parameters. Here $\gamma = 6$, $r_E = 0.2$.

Third, the achieved relay transmit power with respect to iterations are plotted in Fig. 5. From top to bottom are the curves representing $N = 4, 8$ and 12. The three convergence curves show similar trends, regardless of N. Fig. 5 shows that the objective function reduces rapidly in the first 3 iterations, and converges in about 5 iteration. The observation coincides with our analysis below Theorem 3.2, that the objective function value decreases monotonically. It also provides an numerical evidence that our proposed algorithm converges very fast.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 31 July 2017 doi:10.20944/preprints201707.0088.v1

Peer-reviewed version available at Entropy 2017, 19, 522; doi:10.3390/e19100522

Table 1. Number of realizations out of 1000 to exit Algorithm 1 by satisfying the first stopping criterion.

relay number	4	8	12	16	20
number of realizations	882	863	870	861	877

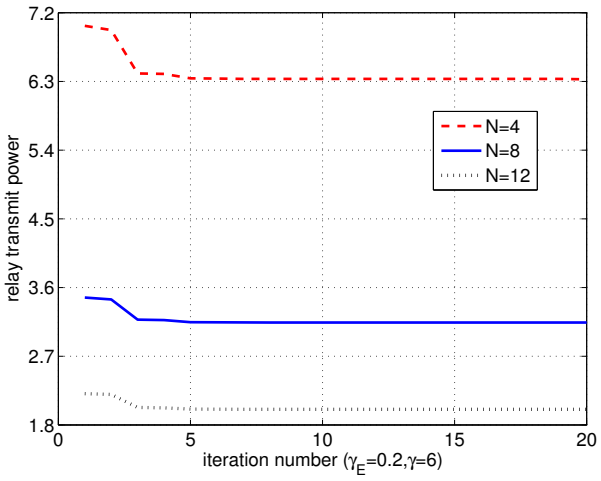

Figure 5. Convergence curves for $N = 4, 8, 12$. Here $\gamma = 6$, $r_E = 0.2$, $\beta = 0.1, \delta_0 = 15$.

Fourth, we analyze the optimality of the achieved solutions by our proposed algorithm. In the algorithm framework, there are two stopping criterions. The first criterion is that $\delta_k \geq \delta$, and $\mathbf{w}_k$ and $\tilde{\mathbf{w}}_{k+1}$ are sufficiently close to each other. Supported by Theorem 3.2, we can deduce that satisfying this criterion means it is roughly the optimal solution of problem (5). The second criterion is simply that $\delta_k \geq \delta$. It only guarantees feasibility rather than optimality. In Table 1, we list the number of realizations out of 1000 which exit the algorithm by satisfying the first stopping criterion,with $\gamma = 4$, $r_E = 0.2$, $\beta = 0.1, \delta_0 = 15$. It indicates that more than 85% of the realizations obtain the optimal solution of problem (5). This shows that our proposed algorithm is efficient to solve the problem.

From the above simulation results, we can see that our proposed imperfect CSI model is meaning, the proposed algorithm is efficient, and the curves representing the imperfect and converges very fast.

5. Conclusions

In this paper, we consider the two-way relay wiretap channel, with two users, N relays and one eavesdropper. The CSI from users and from relays to Eve is estimated with bounded error. We design the relay beamforming weights to minimize the total relay transmit power, while requiring the users' SNRs to be higher than some thresholds, and guaranteeing Eve's worst case rate to be upper bounded. To solve the corresponding semi-infinite programming problem, we propose an algorithm to solve the problem iteratively and preserve feasibility during iterations. The optimality property is analyzed as well. The subproblems are QCQP problems with less than 4 constraints or with only one variable, which are solved optimally. In simulations, we find out that the curves representing the imperfect and perfect CSI models have similar trends. Through observations and analysis, we conclude that the proposed model is important, which balance between users' QoS and security demand; the proposed algorithm is efficient and converges very fast. Numerically we observe that more than 85% of the problems are solved optimally.

Acknowledgments: This work is partly supported by the the National Natural Science Foundation of China (NSFC) 11401039, 11471052, 91630202 and 11331012.

Author Contributions: Wenbao Ai and Cong Sun conceived and designed the model and the algorithm; Ke Liu and Dahu Zheng performed the experiments; Cong Sun and Ke Liu analyzed the data; Cong Sun wrote the paper.

Conflict of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analysis, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

Appendix A Deduction of (4)

First, we have that

$$|f_j|^2 = |f_j^0 + \Delta f_j|^2 = |f_j^0|^2 + 2\mathrm{Re}[(\Delta f_j)^* f_j^0] + |\Delta f_j|^2 \le |f_j^0|^2 + 2\varepsilon_j|f_j^0| + \varepsilon_j^2 = (|f_j^0| + \varepsilon_j)^2$$

holds for all $|\Delta f_j| \le \varepsilon_j$, $j = 1, 2$, and

$$\begin{aligned} |f_1\mathbf{w}^H\mathbf{C}\mathbf{h}_2 - f_2\mathbf{w}^H\mathbf{C}\mathbf{h}_1|^2 &= \left|(f_1, f_2)\begin{pmatrix} \mathbf{w}^H\mathbf{C}\mathbf{h}_2 \\ -\mathbf{w}^H\mathbf{C}\mathbf{h}_1 \end{pmatrix}\right|^2 \le \left\|\begin{pmatrix} \mathbf{w}^H\mathbf{C}\mathbf{h}_2 \\ -\mathbf{w}^H\mathbf{C}\mathbf{h}_1 \end{pmatrix}\right\|^2 \cdot \|(f_1, f_2)\|^2 \\ &= (|f_1|^2 + |f_2|^2)(|\mathbf{w}^H\mathbf{C}\mathbf{h}_1|^2 + |\mathbf{w}^H\mathbf{C}\mathbf{h}_2|^2), \end{aligned}$$

where the first inequality comes from Lemma 3.1.

Then, we can deduce that

$$\begin{aligned} Rf &= \frac{P_1|f_1|^2 + P_2|f_2|^2}{\sigma_{E1}^2} + \frac{P_1|\mathbf{w}^H\mathbf{C}\mathbf{h}_1|^2 + P_2|\mathbf{w}^H\mathbf{C}\mathbf{h}_2|^2}{\sigma_{E2}^2 + \sigma_R^2\mathbf{w}^H\mathbf{C}\mathbf{C}^H\mathbf{w}} + \frac{P_1P_2|f_1\mathbf{w}^H\mathbf{C}\mathbf{h}_1 - f_2\mathbf{w}^H\mathbf{C}\mathbf{h}_2|^2}{\sigma_{E1}^2(\sigma_{E2}^2 + \sigma_R^2\mathbf{w}^H\mathbf{C}\mathbf{C}^H\mathbf{w})} \\ &\le \frac{\sum_{j=1}^2 P_j(|f_j^0| + \varepsilon_j)^2}{\sigma_{E1}^2} + \frac{P_1|\mathbf{w}^H\mathbf{C}\mathbf{h}_1|^2 + P_2|\mathbf{w}^H\mathbf{C}\mathbf{h}_2|^2}{\sigma_{E2}^2 + \sigma_R^2\mathbf{w}^H\mathbf{C}\mathbf{C}^H\mathbf{w}} \\ &\quad + \frac{P_1P_2\sum_{j=1}^2(|f_j^0| + \varepsilon_j)^2}{\sigma_{E1}^2} \cdot \frac{|\mathbf{w}^H\mathbf{C}\mathbf{h}_1|^2 + |\mathbf{w}^H\mathbf{C}\mathbf{h}_2|^2}{\sigma_{E2}^2 + \sigma_R^2\mathbf{w}^H\mathbf{C}\mathbf{C}^H\mathbf{w}}. \end{aligned} \tag{13}$$

Let $a_0 = \frac{P_1P_2\sum_{j=1}^2(|f_j^0|+\varepsilon_j)^2}{\sigma_{E1}^2}$ and $\bar{R}f = \frac{(P_1+a_0)|\mathbf{w}^H\mathbf{C}\mathbf{h}_1|^2+(P_2+a_0)|\mathbf{w}^H\mathbf{C}\mathbf{h}_2|^2}{\sigma_{E2}^2+\sigma_R^2\mathbf{w}^H\mathbf{C}\mathbf{C}^H\mathbf{w}}$, then (13) is written as (4).

Appendix B Proof of Lemma 3.2

It is clear that any $\mathbf{w}$ satisfying constraint (6b) satisfies constraint (5b) strictly. Thus we only need to prove that all $\mathbf{w}$ satisfying constraint (6c) satisfy the semi-infinite constraint (5c) strictly, which is reformulated as

$$\mathbf{w}^H\mathbf{C}\mathbf{Q}\mathbf{C}^H\mathbf{w} \le \sigma_{E2}^2\gamma_E,$$

which holds for all $\|\Delta\mathbf{c}\|_2 \le \varepsilon$, given that $\mathbf{C} = \mathrm{Diag}(\mathbf{c})$ and $\mathbf{c} = \mathbf{c}_0 + \Delta\mathbf{c}$.

Next, we prove that $\mathbf{w}^H\mathbf{C}\mathbf{Q}\mathbf{C}^H\mathbf{w} \le \sigma_{E2}^2\hat{R}f(\mathbf{w})$ holds for all $\|\Delta\mathbf{c}\|_2 \le \varepsilon$.

$$\begin{aligned} \mathbf{w}^H\mathbf{C}\mathbf{Q}\mathbf{C}^H\mathbf{w} &= \mathbf{w}^H\mathbf{C}_0\mathbf{Q}\mathbf{C}_0^H\mathbf{w} + \mathbf{c}_0^T\mathbf{W}^H\mathbf{Q}\mathbf{W}(\Delta\mathbf{c})^* + (\Delta\mathbf{c})^T\mathbf{W}^H\mathbf{Q}\mathbf{W}\mathbf{c}_0^* + (\Delta\mathbf{c})^T\mathbf{W}^H\mathbf{Q}\mathbf{W}(\Delta\mathbf{c})^* \\ &\le \mathbf{w}^H\mathbf{C}_0\mathbf{Q}\mathbf{C}_0^H\mathbf{w} + 2\|\Delta\mathbf{c}\|_2\|\mathbf{c}_0\|_2\|\mathbf{Q}\|_F\|\mathbf{W}\|_F^2 + \varepsilon^2\lambda_{\max}(\mathbf{W}^H\mathbf{Q}\mathbf{W}) \\ &\le \mathbf{w}^H\mathbf{C}_0\mathbf{Q}\mathbf{C}_0^H\mathbf{w} + 2\varepsilon\|\mathbf{c}_0\|_2\|\mathbf{Q}\|_F\|\mathbf{w}\|_2^2 + \varepsilon^2\mathbf{w}^H\mathrm{Diag}(\mathbf{Q}_0)\mathbf{w} \\ &= \sigma_{E2}^2\hat{R}f(\mathbf{w}). \end{aligned} \tag{14}$$

Here $\mathbf{W} = \mathrm{Diag}(\mathbf{w})$, and the first inequality applies the norm compatibility and the property of rayleigh quotient, and the second inequality comes from that

$$\lambda_{\max}(\mathbf{W}^H\mathbf{Q}\mathbf{W}) \le \lambda_{\max}(\mathbf{W}^H\mathbf{Q}_0\mathbf{W}) \le \mathrm{tr}(\mathbf{W}^H\mathbf{Q}_0\mathbf{W}) = \mathbf{w}^H\mathrm{Diag}(\mathbf{Q}_0)\mathbf{w},$$

where $\mathbf{Q}_0 = \mathbf{Q} + \sigma_R^2\gamma\mathbf{I}$ is positive semi-definite.

Thus for any $\mathbf{w}$ satisfying $\hat{Rf}(\mathbf{w}) \leq \gamma_E$, it satisfies that

$$\mathbf{w}^H\mathbf{C}\mathbf{Q}\mathbf{C}^H\mathbf{w} \leq \sigma_{E2}^2\hat{Rf}(\mathbf{w}) \leq \sigma_{E2}^2(1-\beta^\delta)\gamma_E < \sigma_{E2}^2\gamma_E,$$

which holds for all $\|\Delta\mathbf{c}\|_2 \leq \varepsilon$. Based on the above analysis, we deduce the conclusion. □

Appendix C Proof of Theorem 3.2

When $t=0$, $\mathbf{w}_{k+1}(0)$ reduces to $\mathbf{w}_k$. It is trivial to show that $t=0$ is feasible for subproblem (12), as long as $k>0$, that is, when $\mathbf{w}_k$ was obtained from subproblem (12) in the $(k-1)$th iteration. Thus we only need to prove the situation when $k=0$.

When $k=0$, $\mathbf{w}_k$ satisfies (6b) as it is the solution of the initial subproblem (6). This deduces that $t=0$ satisfies constraint (12b). As $\mathbf{w}_k$ satisfies (6c), we have that

$$\begin{aligned} m_4 + (1-\beta^{\delta_k})\sigma_{E2}^2\gamma_E &= \mathbf{c}_0^T\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^* + 2\varepsilon\|\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^*\| + \varepsilon^2\lambda_{\max}(\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0) \\ &\leq \mathbf{c}_0^T\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^* + 2\varepsilon\|\mathbf{c}_0\|_2\|\mathbf{Q}\|_F\|\mathbf{v}_0\|_2^2 + \varepsilon^2\mathbf{v}_0^H\mathrm{Diag}(\mathbf{Q}_0)\mathbf{v}_0 \\ &\leq (1-\beta^{\delta_k})\sigma_{E2}^2\gamma_E. \end{aligned}$$

Here $\mathbf{v}_0$ represents for $\mathbf{w}_k$. It is deduced similarly as (14). Thus $g_k(0) = m_4 \leq 0$, that is, $t=0$ satisfies (12c). So we conclude that $t=0$ is always a feasible point of subproblem (12).

Next, suppose t_0 is any feasible point of (12). Then $g_k(t_0) \leq 0$. Obviously $\mathbf{w}_{k+1}(t_0)$ satisfies constraint (8a). That "$\mathbf{w}_{k+1}(t_0)$ satisfies constraint (8b)" is equivalent to that "$[\mathbf{v}_0 + t_0(\mathbf{v}_1 - \mathbf{v}_0)]^H\mathbf{C}\mathbf{Q}\mathbf{C}^H[\mathbf{v}_0 + t_0(\mathbf{v}_1 - \mathbf{v}_0)] \leq (1-\beta^{\delta_k})\sigma_{E2}^2\gamma_E$, for all $\|\Delta\mathbf{c}\|_2 \leq \varepsilon$", where $\mathbf{v}_1$ represents for $\tilde{\mathbf{w}}_{k+1}$. We prove the above result in the following steps.

We rewrite that

$$[\mathbf{v}_0 + t_0(\mathbf{v}_1 - \mathbf{v}_0)]^H\mathbf{C}\mathbf{Q}\mathbf{C}^H[\mathbf{v}_0 + t_0(\mathbf{v}_1 - \mathbf{v}_0)] = t_0^2 s_1 + t_0 s_2 + s_3,$$

where $s_1 = (\mathbf{v}_1 - \mathbf{v}_0)^H\mathbf{C}\mathbf{Q}\mathbf{C}^H(\mathbf{v}_1 - \mathbf{v}_0)$, $s_2 = 2\mathrm{Re}[\mathbf{v}_0^H\mathbf{C}\mathbf{Q}\mathbf{C}^H(\mathbf{v}_1 - \mathbf{v}_0)]$ and $s_3 = \mathbf{v}_0^H\mathbf{C}\mathbf{Q}\mathbf{C}^H\mathbf{v}_0$.

For all $\|\Delta\mathbf{c}\|_2 \leq \varepsilon$, we deduce that

$$\begin{aligned} s_1 &= \mathbf{c}_0^T(\mathbf{V}_1 - \mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1 - \mathbf{V}_0)\mathbf{c}_0^* + 2\mathrm{Re}[\mathbf{c}_0^T(\mathbf{V}_1 - \mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1 - \mathbf{V}_0)(\Delta\mathbf{c})^*] \\ &\quad + (\Delta\mathbf{c})^T(\mathbf{V}_1 - \mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1 - \mathbf{V}_0)(\Delta\mathbf{c})^* \\ &\leq \mathbf{c}_0^T(\mathbf{V}_1 - \mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1 - \mathbf{V}_0)\mathbf{c}_0^* + 2\varepsilon\|(\mathbf{V}_1 - \mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1 - \mathbf{V}_0)\mathbf{c}_0^*\| \\ &\quad + \varepsilon^2\lambda_{\max}[(\mathbf{V}_1 - \mathbf{V}_0)^H\mathbf{Q}(\mathbf{V}_1 - \mathbf{V}_0)] \\ &= m_1. \end{aligned}$$

Similarly, we deduce that

$$s_3 \leq \mathbf{c}_0^T\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^* + 2\varepsilon\|\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0\mathbf{c}_0^*\| + \varepsilon^2\lambda_{\max}(\mathbf{V}_0^H\mathbf{Q}\mathbf{V}_0) = m_4 + (1-\beta^{\delta_k})\sigma_{E2}^2\gamma_E.$$

For simplicity, denote $\mathbf{Q}_v = \mathbf{V}_0^H\mathbf{Q}(\mathbf{V}_1 - \mathbf{V}_0)$. So we have

$$t_0 s_2 = t_0 \cdot 2\mathrm{Re}(\mathbf{c}_0^T\mathbf{Q}_v\mathbf{c}_0^*) + t_0 \cdot 2\mathrm{Re}[(\Delta\mathbf{c})^T\mathbf{Q}_v\mathbf{c}_0^*] + t_0 \cdot 2\mathrm{Re}[\mathbf{c}_0^T\mathbf{Q}_v(\Delta\mathbf{c})^*] + t_0 \cdot 2\mathrm{Re}[(\Delta\mathbf{c})^T\mathbf{Q}_v(\Delta\mathbf{c})^*].$$

Then we deduce that

$$\begin{aligned} t_0 \cdot 2\mathrm{Re}[(\Delta\mathbf{c})^T\mathbf{Q}_v\mathbf{c}_0^*] = t_0[(\Delta\mathbf{c})^T\mathbf{Q}_v\mathbf{c}_0^* + \mathbf{c}_0^T\mathbf{Q}_v^H(\Delta\mathbf{c})^*] &\leq |t_0| \cdot 2\varepsilon\|\mathbf{Q}_v\mathbf{c}_0^*\|_2, \\ t_0 \cdot 2\mathrm{Re}[\mathbf{c}_0^T\mathbf{Q}_v(\Delta\mathbf{c})^*] &\leq |t_0| \cdot 2\varepsilon\|\mathbf{Q}_v^H\mathbf{c}_0^*\|_2, \\ t_0 \cdot 2\mathrm{Re}[(\Delta\mathbf{c})^T\mathbf{Q}_v(\Delta\mathbf{c})^*] = t_0(\Delta\mathbf{c})^T(\mathbf{Q}_v + \mathbf{Q}_v^H)(\Delta\mathbf{c})^* &\leq |t_0|\varepsilon^2\lambda_{\max}(\mathbf{Q}_v + \mathbf{Q}_v^H). \end{aligned}$$

Thus $t_0 s_2 \leq t_0 m_2 + |t_0| m_3$. Consequently, we have

$$\begin{aligned} t_0^2 s_1 + t_0 s_2 + s_3 &\leq t_0^2 m_1 + t_0 m_2 + |t_0| m_3 + m_4 + (1-\beta^{\delta_k})\sigma_{E2}^2 \gamma_E \\ &= g_k(t_0) + (1-\beta^{\delta_k})\sigma_{E2}^2 \gamma_E \leq (1-\beta^{\delta_k})\sigma_{E2}^2 \gamma_E. \end{aligned}$$

So $\mathbf{w}_{k+1}(t_0)$ satisfies constraints (8). □

Appendix D Proof of Theorem 3.2

considering constraint (5c), for any feasible point $\mathbf{w}_\flat$, there exists a vector $\Delta\mathbf{c}_\flat$, such that $\bar{Rf}(\Delta\mathbf{c}; \mathbf{w}_\flat) \leq \bar{Rf}(\Delta\mathbf{c}_\flat; \mathbf{w}_\flat) \leq \gamma_E$ holds for all $\|\Delta\mathbf{c}\|_2 \leq \varepsilon$. Suppose $\mathbf{w}_*$ and $\Delta\mathbf{c}_*$ are a pair satisfying the above conditions, and that $\mathbf{w}_*$ is also the optimal solution of the following subproblem with parameter $\Delta\mathbf{c}_*$:

$$\begin{aligned} \min_{\mathbf{w}\in\mathbb{C}^{N\times 1}} \quad & P_R(\mathbf{w}) \\ \text{s.t.} \quad & \mathrm{SNR}_j(\mathbf{w}) \geq \gamma_j, \quad j = 1, 2; \\ & \bar{Rf}(\Delta\mathbf{c}_*; \mathbf{w}) \leq \gamma_E. \end{aligned} \tag{15}$$

Here β^δ is omitted because δ goes to infinity and $0 < \beta < 1$.

Next we shall prove the conclusion by contradiction. Suppose there exists $\mathbf{w}_\sharp$ as a feasible point of (5), and $P_R(\mathbf{w}_\sharp) < P_R(\mathbf{w}_*)$. Let its corresponding vector be $\Delta\mathbf{c}_\sharp$. Then the following inequalities hold:

$$\begin{aligned} \bar{Rf}(\Delta\mathbf{c}_*; \mathbf{w}_\sharp) \leq \bar{Rf}(\Delta\mathbf{c}_\sharp; \mathbf{w}_\sharp) \leq \gamma_E; \\ \mathrm{SNR}_j(\mathbf{w}_\sharp) \geq \gamma_j, \quad j = 1, 2. \end{aligned}$$

It means that $\mathbf{w}_\sharp$ is a feasible point of (15), and it has lower objective function value than $\mathbf{w}_*$. This contradicts with the fact that $\mathbf{w}_*$ is the optimal solution of (15). Thus the assumption of $\mathbf{w}_\sharp$ is incorrect. $\mathbf{w}_*$ must be the optimal solution of problem (5). □

Bibliography

1. Oggier, F and Hassibi, B. The Secrecy Capacity of the MIMO Wiretap Channel. *IEEE Trans. Inf. Theo.* **2011**, *57*, 4961-4972.
2. Lin, P H; Lai, S H; Lin, S C and Su, H J. On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels. *IEEE Journal on Selected Areas in Communications* **2013**, *31*, 1728-1740.
3. Wang, H M; Zheng, T and Xia, X G. Secure MISO Wiretap Channels With Multiantenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading. *IEEE Trans. Wireless Commun.* **2015**, *14*, 94-106.
4. Chen X, Zhang Y. Mode Selection in MU-MIMO Downlink Networks: A Physical-Layer Security Perspective. *IEEE Systems Journal* **2015**, *11*, 1128-1136.
5. Kapetanovic, D; Zheng, G and Rusek, F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Magazine* **2015**, *53*, 21-27.
6. Cumanan, K; Ding, Z; Sharif, B; Tian, G Y and Leung, K K. Secrecy Rate Optimizations for a MIMO Secrecy Channel With a Multiple-Antenna Eavesdropper. *IEEE Trans. Vehicular Technology* **2014**, *63*, 1678-1690.
7. Zappone, A; Lin, P H and Jorswieck, E A. Energy efficiency in secure multi-antenna systems. *arXiv preprint*, **2015**, http://arxiv.org/abs/1505.02385.
8. Zhang, J; Yuen, C; Wen, C K; Jin, S and Wong, K K. Large System Secrecy Rate Analysis for SWIPT MIMO Wiretap Channels. *IEEE Trans. Information Forensics & Security* **2015**, *11*, 74-85.
9. Zheng, C; Cumanan, K; Ding, Z; Johnston, M and Goff, S L. Robust Outage Secrecy Rate Optimizations for a MIMO Secrecy Channel. *IEEE Wireless Commun. Letters* **2015**, *4*, 86-89.
10. Jimenez Rodriguez, L; Tran, N H; Duong, T Q; Tho L-N; Elkashlan, M and Shetty S. Physical layer security in wireless cooperative relay networks: state of the art and beyond. *IEEE Commun. Magazine* **2015**, *12*, 32-39.

11. Liu, Y; Li, L; Alexandropoulos, G C and Pesavento, M. Securing Relay Networks with Artificial Noise: An Error Performance-Based Approach. *Entropy* **2017**, *19*, 1-21, DOI: 10.3390/e19080384.
12. Sun, L; Zhang, T; Li, Y and Niu, H. Performance Study of Two-Hop Amplify-and-Forward Systems With Untrustworthy Relay Nodes. *IEEE Trans. Vehicular Technology* **2012**, *61*, 3801-3807.
13. Jeong, C; Kim, I M and Kim, D I. Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System. *IEEE Trans. Signal Process.* **2012**, *60*, 310-325.
14. Wang, H M; Luo, M; Xia, X G and Yin, Q Y. Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems With Individual Power Constraint and No Eavesdropper's CSI. *IEEE Signal Process. Letters* **2013**, *20*, 39-42.
15. Salem, A and Hamdi, K A. Improving Physical Layer Security of AF Relay Networks via Beam-forming and Jamming. *Vehicular Technology Conference. IEEE* **2017**.
16. Lee, J H. Optimal Power Allocation for Physical Layer Security in Multi-Hop DF Relay Networks. *IEEE Trans. Wireless Commun.* **2016**, *15*, 28-38.
17. Kolokotronis, N; Athanasakos, M. Improving physical layer security in DF relay networks via two-stage cooperative jamming[C]// European Signal Processing Conference. 2016:1173-1177.
18. Dong, L; Han, Z; Petropulu, A P and Vincent Poor, H. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875-1888.
19. Li, J Y; Petropulu, A P and Weber, S. On Cooperative Relaying Schemes for Wireless Physical Layer Security. *IEEE Trans. Signal Process.* **2011**, *59*, 4985-4997.
20. Hui, H; Swindlehurst, A L; Li, G B and Liang, J L. Secure Relay and Jammer Selection for Physical Layer Security. *IEEE Signal Process. Letters* **2015**, *22*, 1147-1151.
21. Chen, G; Yu, G; Xiao, P and Chambers, J. Physical Layer Network Security in the Full-Duplex Relay System. *IEEE Trans. Information Forensics & Security* **2015**, *10*, 574-583.
22. Zou, Y L; Wang, X B and Shen, W M. Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks. *IEEE Journal on Selected Areas in Communications* **2013**, *10*, 2099-2111.
23. Wang, D; Bai, B; Chen, W and Han, Z. Achieving High Energy Efficiency and Physical-Layer Security in AF Relaying. *IEEE Trans. Wireless Commun.* **2016**, *15*, 740-752.
24. Chen, X; Lei, L; Zhang, H and Yuen, C. Large-Scale MIMO Relaying Techniques for Physical Layer Security: AF or DF? *IEEE Int. Conf. Commun. IEEE* **2015**, 2052-2057.
25. Yang, Y C; Sun, C; Zhao, H; Long, H and Wang, W B. Algorithms for Secrecy Guarantee With Null Space Beamforming in Two-Way Relay Networks. *IEEE Trans. Signal Process.* **2014**, *62*, 2111-2126.
26. Chen, X; Chen, J; Zhang, H; Zhang, Y and Yuen, C. On Secrecy Performance of Multiantenna-Jammer-Aided Secure Communications With Imperfect CSI. *IEEE Trans. Vehicular Technology* **2016**, *65*, 8014-8024.
27. Zhao, P; Zhang, M; Yu, H; Luo, H W and Chen, W. Robust Beamforming Design for Sum Secrecy Rate Optimization in MU-MISO Networks. *IEEE Trans. Information Forensics & Security* **2015**, *10*, 1812-1823.
28. Wang, X; Zhang, Z and Long, K. Robust relay beamforming for multiple-antenna amplify-and-forward relay system in the presence of eavesdropper. *IEEE Int. Conf. Acoust. Speech & Signal Process.* **2014**, 5710-5714.
29. Lin, Z; Cai, Y; Yang, W and Wang, L. Robust secure switching transmission in multi-antenna relaying systems: cooperative jamming or decode-and-forward beamforming. *IET Communications* **2016**, *10*, 1673-1681.
30. Zhang, M; Huang, J; Yu, H; Luo, H W and Chen, W. QoS-Based Source and Relay Secure Optimization Design with Presence of Channel Uncertainty. *IEEE Commun. Letters* **2013**, *17*, 1544-1547.
31. López, M and Still, G. Semi-infinite programming. *European J. Operational Research* **2007**, *180*, 491-518.
32. Luo, Z Q; Ma, W K; So, M C and Ye, Y Y. Semidefinite Relaxation of Quadratic Optimization Problems. *IEEE Signal Process. Magazine* **2010**, *27*, 20-34.
33. Ai, W B; Huang, Y and Zhang, S Z. New results on Hermitian matrix rank-one decomposition. *Math. Program.* **2011**, *128*, 253-283.

34. Sun, W Y and Yuan, Y X. Optimization theory and methods: nonlinear programming. In *Sringer Optimization and its applications*; Pardalos, P M, Eds.; Springer: New York, USA, 2006; ISBN: 0-387-24975-3.
35. Grant, M and Boyd, S. CVX: Matlab software for disciplined convex programming, version 2.0 beta. **2011**, http://cvxr.com/cvx.