

# Sum Secrecy Rate Maximization for Relay-Aided Multiple-Source Multiple-Destination Networks

Meng Zhang, Ming Ding, *Member, IEEE*, Lin Gui, Hanwen Luo, and Mehdi Bennis, *Senior Member, IEEE*

**Abstract**—This paper studies a multiple-source multiple-destination network with the presence of multiple eavesdroppers, in which an amplify-and-forward (AF) relay is used to bridge the communication between the source–destination pairs to overcome the long-distance attenuation. Considering the physical-layer security issues, we aim to maximize the sum secrecy rate subject to the relay power constraint and the quality-of-service (QoS) requirements for legitimate user equipment. First, we propose an algorithm based on the monotonic optimization and the semidefinite programming (MO-SDP). Simulation results show that our proposed MO-SDP algorithm exhibits almost the same performance as the optimal solution. To alleviate the problem of high complexity associated with the MO-SDP algorithm, we then propose an alternative solution based on the null-space (NuS) relay precoding, the complexity of which is significantly reduced, and it yields a semiclosed-form expression for the solution. Moreover, the performance of the proposed NuS algorithm is evaluated via simulations, and the performance of the NuS algorithm and that of the MO-SDP algorithm are shown to converge at the high signal-to-noise ratio (SNR) region.

**Index Terms**—Monotonic optimization, null space (NuS), precoding, relay, semidefinite programming, sum secrecy rate (SSR).

## I. INTRODUCTION

**M**OST modern commercial telecommunication systems, including the fourth generation (4G) long-term evolution advanced (LTE-A) networks [1], apply high-layer encryption methods to achieve secure communication. The basic concept of such implementation was first proposed by Shannon [2].

Recently, with the development of advanced wireless communication networks, it has been realized that the unique feature of the wireless channel associated with a specific transceiver pair can also be utilized as an encryption medium. Relevant studies have been carried out in the booming branch of physical-layer security. In particular, the beamforming technique has been

viewed as a promising technique to enhance secrecy rate in multiple-input multiple-output (MIMO) systems. In [3], Jeong *et al.* studied an amplify-and-forward (AF) relay-aided system with the assumption that relay may also wiretap the legitimate user equipment's (L-UE) data apart from the function of relaying data, and proposed a joint source and relay beamforming design to maximize the secrecy rate. Furthermore, distributed beamforming and power allocation for the two-way relay systems were discussed in [4], which increase the sum secrecy rate (SSR) of the data exchange. In [5], Wang *et al.* proposed a hybrid cooperative beamforming and jamming scheme to enhance the physical-layer security of a single-antenna two-way relay network in the presence of an eavesdropper, which has the capability to wiretap the signals within two-hop two-way relay transmissions. Furthermore, in [6], Wang *et al.* studied the cooperative transmission for securing a decode-and-forward two-hop network where multiple cooperative nodes coexist with a potential eavesdropper. Similarly, the eavesdropper can also wiretap both of the two hops' transmission. Although the mentioned papers assume that the first hop between enhanced Node B (eNB) and relay can be wiretapped by eavesdropper, it is difficult to be implemented in the existing 4G networks. Considering the secrecy level for the protocol between an eNB and a relay node is much higher than the protocol between a relay and an UE, it is much more difficult, if not impossible, for the eavesdropper to wiretap the first hop transmission than the second hop. In this paper, we consider a practical assumption that the eavesdropper cannot infiltrate the infrastructure network as a fake relay node, but it is able to sleep in the network as an UE to wiretap another UE. In our previous work [7], we investigated a coordinated beamforming/coordinated scheduling system, in which one eavesdropper wiretaps one specific legitimate user in the network. For the case with preknown wiretapping information and the case without preknown wiretapping information, we proposed suboptimal coordinated beamforming algorithms to maximize secrecy rate. Moreover, in [8] an SSR optimization is proposed by beamforming together with artificial noise (AN). In [9], Lin *et al.* investigated a multiple-input single-output single-antenna eavesdropper (MISOSE) system, and proposed a generalized AN assisted secure beamforming design. Later, a cooperative beamforming on top of AN was proposed for two-way relay networks in [10]. In [11], Wang *et al.* investigated a relay-aided multiple-source multiple-destination (MSMD) system with the existence of one eavesdropper, which can wiretaps both transmission data of the two hops. With the assumption of imperfect channel state information (CSI), Li and Ma [12] proposed a robust precoding design for an MISO

Manuscript received June 4, 2015; revised November 19, 2015, April 10, 2016, and August 6, 2016; accepted August 15, 2016. Date of publication September 16, 2016; date of current version May 12, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61471236 and in part by the National Science and Technology Major Project under Grant 2011ZX03001-007-03. The review of this paper was coordinated by Prof. M. C. Gursoy.

M. Zhang, L. Gui, and H. Luo are with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200030, China (e-mail: mengzhang@sjtu.edu.cn; guilin@sjtu.edu.cn; hwluo@sjtu.edu.cn).

M. Ding is with Data61, Sydney, NSW 2612, Australia (e-mail: Ming.Ding@nicta.com.au).

M. Bennis is with the Department of Electrical Engineering, University of Oulu, Oulu 90570, Finland (e-mail: bennis@ee.oulu.fi).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TVT.2016.2609934

channel with the objective of maximizing the secrecy rate. Furthermore, in [13], a one-way two-hop relay wiretap channel is considered, and robust precoding, together with AN design, are proposed.

In this paper, we study a relay-aided MSMD network with the presence of multiple eavesdroppers. Due to the severe signal attenuation caused by the long distance between the source and the destination, an AF relay is employed with the purpose of enhancing the transmission reliability. We assume that each eavesdropper wiretaps only one specific L-UE. Moreover, the scenario that multiple eavesdroppers wiretap a single L-UE can be regarded as a special case of our model. It should be noted that perfect CSI has been assumed for the eavesdroppers in our paper, whereas imperfect CSI is a more practical assumption which shall be considered in our future work. Our objective is to optimize the relay precoder with the objective of maximizing the SSR. The objective of our optimization problem leads to the formation of multiplication of  $N$  generalized Rayleigh quotients. For  $N = 1$ , the optimal solution can be obtained by finding the largest eigen mode. For  $N = 2$ , Li *et al.* [14] provided an algorithm consisting of bisection and one-dimensional search to obtain the global optimal solution. However, to the best of our knowledge, the optimal solution for the case of  $N \geq 3$  has yet to be found, and we intend to tackle this problem in this paper. Our contributions are summarized as follows.

- 1) For the first time, we propose to use monotonic optimization and semidefinite programming (MO-SDP) to solve the SSR optimization problem for the case of  $N \geq 3$ . The cost function is in the form of multiplication of multiple Rayleigh quotients, and both the relay precoder and the AN are considered. Our simulation results show the MO-SDP scheme with AN slightly outperforms without AN, and it achieve better performance than the other reference algorithms.
- 2) The complexity associated with the MO-SDP algorithm is extremely high, especially for the case with a large number of relay antennas or user pairs. Therefore, we proposed a null-space (NuS) based algorithm that projects the transmitted signal into the NuS of channels between the AF relay and eavesdroppers. Simulation results show that at high signal-to-noise ratio (SNR) regime, the performance of the NuS-based algorithm is very close to that of the MO-SDP-based algorithm.

**Organization:** The rest of this paper is organized as follows. In Section II, the system model and the problem formulation are discussed. In Section III, we present some preliminary knowledge on monotonic optimization, and propose the MO-SDP-based algorithm that can maximize the SSR subject to the quality-of-service (QoS) requirements of L-UE as well as the relay power constraint. To alleviate the problem of high complexity of the MO-SDP algorithm, a low-complexity NuS algorithm is proposed in Section IV. Section V shows the performance of our proposed algorithm, followed by our concluding remarks and discussion on future work in Section VI.

**Notation:** In this paper, we use bold uppercase and lowercase letters to denote the matrices and vectors, respectively;  $(\cdot)^T$ ,  $(\cdot)^H$ , denote the transpose, and conjugate transpose of a

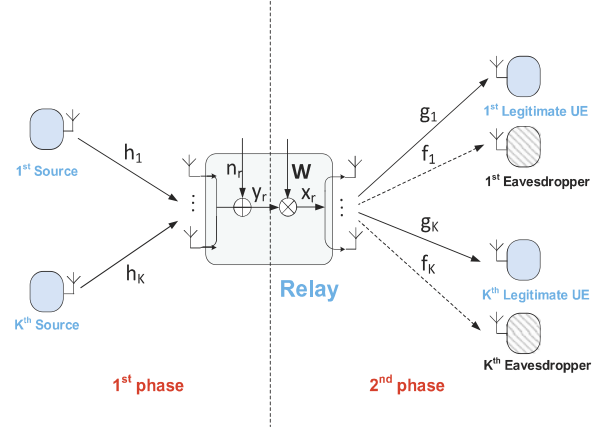


Fig. 1. System model.

matrix or a vector, respectively;  $\mathbf{I}_N$  is an  $N \times N$  identity matrix;  $\text{Tr}(\cdot)$  is the trace of a matrix;  $\text{vec}(\cdot)$  represents the matrix vectorization;  $\mathbf{x} \in \mathbb{C}^{N^2 \times 1}$ ,  $\text{mat}(\mathbf{x})$  represents the reshape of  $\mathbf{x}$  to an  $N \times N$  matrix;  $\otimes$  denotes the Kronecker product;  $\|\cdot\|$  denotes the Frobenius norm;  $\succeq$  represents the property of semidefinite;  $\mathcal{NUL}(\mathbf{X})$  denotes the NuS of matrix  $\mathbf{X}$ ; and  $\pi_i(\mathbf{X})$  denotes the  $i$ th largest eigenvalue of matrix  $\mathbf{X}$ ;  $\mathcal{CN}(\mathbf{a}, \mathbf{X})$  stands for the complex Gaussian distribution with mean  $\mathbf{a}$  and variance  $\mathbf{X}$ .

## II. SYSTEM MODEL AND PROBLEM FORMULATION

In this paper, we consider a wireless network that is composed of  $K$  sources,  $K$  destinations, and one AF relay operating on the same frequency band. Each destination is paired with and wiretapped by one eavesdropper. We assume that each node of sources, destinations, and eavesdroppers is equipped with a single antenna, and the AF relay is equipped with  $N$  antennas. Let  $s_i$  be the transmitted symbol from the  $i$ th source and intended for the  $i$ th destination, which satisfy  $E\{|s_i|^2\} = 1$ . Without loss of generality, all sources are assumed to transmit signals with normalized power. Due to the AF relaying protocol, the whole transmission process is divided into two phases. In more detail, in the first phase, all sources broadcast the signals with normalized power, and the signal received by the relay is given by

$$\mathbf{y}_r = \sum_i^K \mathbf{h}_i s_i + \mathbf{n}_r \quad (1)$$

where  $\mathbf{h}_i \in \mathbb{C}^{N \times 1}$  denotes the channel vector between the  $i$ th source and the relay, and  $\mathbf{n}_r \in \mathbb{C}^{N \times 1}$  denotes the additive white Gaussian noise (AWGN) at the relay satisfying  $\mathbf{n}_r \sim \mathcal{CN}(0, \sigma_n^2 \mathbf{I})$ .

Then, the AF relay performs a linear processing function on the received signal by multiplying a precoding matrix  $\mathbf{W} \in \mathbb{C}^{N \times N}$  and adding an AN vector to it, and thus, the signal transmitted by the relay is written as

$$\begin{aligned} \mathbf{x}_r &= \mathbf{W} \mathbf{y}_r \\ &= \mathbf{W} \sum_i^K \mathbf{h}_i s_i + \mathbf{W} \mathbf{n}_r + \mathbf{a} \end{aligned} \quad (2)$$

where  $\mathbf{a} \in \mathbb{C}^{N \times 1}$  stands for the AN vector with  $E\{\mathbf{a}^H \mathbf{a}\} = \Sigma$ . Note that  $\Sigma$  is not necessarily a diagonal matrix since the AN vector might be colored.

The power constraint of the relay is then formulated as

$$\|\mathbf{x}_r\|^2 \leq P_r. \quad (3)$$

In the second phase, the signals received at the  $i$ th legitimate user and the  $i$ th eavesdropper can be, respectively, expressed as

$$y_i = \mathbf{g}_i^H \mathbf{W} \mathbf{h}_i s_i + \mathbf{g}_i^H \mathbf{W} \sum_{j, j \neq i}^K \mathbf{h}_j s_j + \mathbf{g}_i^H \mathbf{W} \mathbf{n}_r + \mathbf{g}_i^H \mathbf{a} + n_i \quad (4)$$

and

$$y_i^e = \mathbf{f}_i^H \mathbf{W} \mathbf{h}_i s_i + \mathbf{f}_i^H \mathbf{W} \sum_{j, j \neq i}^K \mathbf{h}_j s_j + \mathbf{f}_i^H \mathbf{W} \mathbf{n}_r + \mathbf{f}_i^H \mathbf{a} + n_i^e \quad (5)$$

where  $\mathbf{g}_i \in \mathbb{C}^{1 \times N}$  and  $\mathbf{f}_i \in \mathbb{C}^{1 \times N}$  denote the channel vector between the relay and the  $i$ th legitimate user, and the channel vector between the relay and the  $i$ th eavesdropper, respectively. In addition,  $n_i, n_i^e \sim \mathcal{CN}(0, \sigma_n^2)$  are the independent AWGN values at the  $i$ th legitimate user and the  $i$ th eavesdropper, respectively.

As a result, the signal-to-interference-plus-noise ratio (SINR) of the  $i$ th legitimate user and the  $i$ th eavesdropper can be, respectively, written as

$$\text{SINR}_i = \frac{\|\mathbf{g}_i^H \mathbf{W} \mathbf{h}_i s_i\|^2}{\|\mathbf{g}_i^H \mathbf{W} \sum_{j, j \neq i}^K \mathbf{h}_j s_j\|^2 + \sigma_n^2 \|\mathbf{g}_i^H \mathbf{W}\|^2 + \|\mathbf{g}_i^H \mathbf{a}\|^2 + \sigma_n^2} \quad (6)$$

and

$$\text{SINR}_i^e = \frac{\|\mathbf{f}_i^H \mathbf{W} \mathbf{h}_i s_i\|^2}{\|\mathbf{f}_i^H \mathbf{W} \sum_{j, j \neq i}^K \mathbf{h}_j s_j\|^2 + \sigma_n^2 \|\mathbf{f}_i^H \mathbf{W}\|^2 + \|\mathbf{f}_i^H \mathbf{a}\|^2 + \sigma_n^2}. \quad (7)$$

Then, the SSR problem can be formulated as

$$\max_{\mathbf{W}, \Sigma} \sum_{i=1}^K (\log(1 + \text{SINR}_i) - \log(1 + \text{SINR}_i^e)) \quad (8a)$$

$$\text{s.t.} \quad \log(1 + \text{SINR}_i) \geq \gamma_i, i = 1, \dots, K \quad (8b)$$

$$\|\mathbf{x}_r\|^2 \leq P_r. \quad (8c)$$

The objective function of problem (8) is straightforwardly defined as the sum of all secrecy rates. In addition, to prevent the extreme cases that some L-UEs may exhibit positive secrecy rates while only getting very low self-rates, we add an individual rate requirement for each L-UE to achieve a minimum QoS requirement. To the best of our knowledge, our work is the first one to treat the SSR maximization problem in the scenario with multiple eavesdroppers. The difficulty of solving problem (8) lies in dealing with the complex form of (8a). Furthermore, problem (8) is nonconvex over  $\mathbf{W}$  and  $\Sigma$ , even without the summation operation, and the optimal solution is extremely difficult to obtain. In the following sections, first, we propose a high-complexity MO-SDP-based algorithm to find the solutions of problem (8). Second, we design a low-complexity algorithm with closed-form expressions to find a suboptimal solution for problem (8).

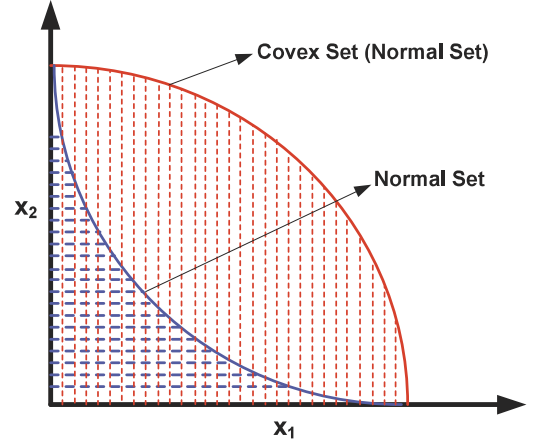


Fig. 2. Normal/convex set.

### III. MONOTONIC OPTIMIZATION AND THE SEMIDEFINITE PROGRAMMING-BASED RELAY PRECODER DESIGN

Conventional convex optimization theories cannot be directly applied to the SSR maximization problem due to the nonconvex feature of problem (8). In this section, we resort to the monotonic optimization theory, a powerful mathematical tool to solve some specific kinds of nonconvex optimization problems. As an example, although it is a nonconvex problem for finding the optimal beamforming vectors for sum-rate maximization in multiuser MIMO systems with perantenna power constraints and quantized CSI, Ding *et al.* [15] proposed an algorithm to find the solution based on the monotonic optimization theory.

In the following, we first provide some preliminary knowledge on the monotonic optimization theory [16].

#### A. Preliminary Knowledge on Monotonic Optimization

**Definition 1 (Increasing/Decreasing Function):** A function  $f: \mathcal{R}_+^n \rightarrow \mathcal{R}$  is increasing, if  $f(\mathbf{x}) \leq f(\mathbf{y})$  always holds when  $\mathbf{0} \leq \mathbf{x} \leq \mathbf{y}$ . The inequality between two vectors means the inequality is element-wise for each of their entries. Besides, a function  $f$  is decreasing, if  $-f$  is increasing.

**Definition 2 (Normal Set):** A set  $\mathcal{G}$  is normal if  $\forall \mathbf{x} \in \mathcal{G}$ , all the points  $\mathbf{x}'$  that  $\mathbf{0} \leq \mathbf{x}' \leq \mathbf{x}$  also belong to set  $\mathcal{G}$ .

Specifically, THE convex set can be regarded as a special case of normal set shown in Fig. 2.

**Definition 3 (Polyblock):** A set  $\mathcal{P} \subset \mathcal{R}_+^n$  is called a polyblock if it is a union of a finite number of boxes  $[\mathbf{0}, \mathbf{z}]$ , where  $\mathbf{z} \in \mathcal{T}$  and  $\mathcal{T} < +\infty$ .

From the definition above, a polyblock is clearly a normal set. If the achievable region satisfies the definition of a normal set and the cost function is an increasing function. Then, we can resort to the monotonic optimization theory to find the optimal solution. The core idea of the monotonic optimization theory is to use polyblocks to approximate the contour of achievable region as shown in Fig. 3. Then, after continuous searching the vertexes on the polyblocks until a predefined precision is met, the vertex that exhibits the best performance can be extracted as the optimal solution.

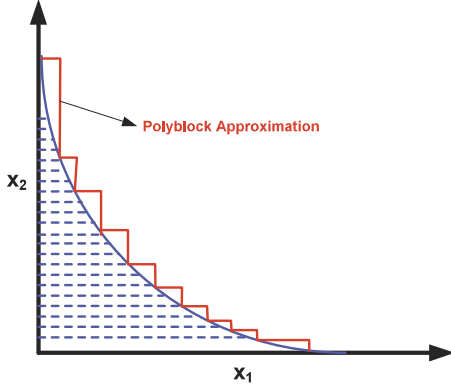


Fig. 3. Polyblock approximation upon normal set.

### B. MO-SDP-Based Relay Precoder Design

First, we need to transform (8) into a more tractable form. Using  $\text{vec}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\text{vec}(\mathbf{B})$  [17], the SINR of the  $i$ th L-UE and the  $i$ th eavesdropper can be, respectively, expressed as

$$\begin{aligned} \text{SINR}_i &= \frac{\|(\mathbf{h}_i^T \otimes \mathbf{g}_i)\mathbf{w}\|^2}{\sum_{j \neq i}^K \|(\mathbf{h}_j^T \otimes \mathbf{g}_i)\mathbf{w}\|^2 + \sigma_n^2 \|(\mathbf{I} \otimes \mathbf{g}_i)\mathbf{w}\|^2 + \|\mathbf{g}_i \mathbf{a}\|^2 + \sigma_n^2} \\ &= \frac{\mathbf{w}^H \mathbf{Q}_i \mathbf{w}}{\mathbf{w}^H \mathbf{Z}_i \mathbf{w} + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2} \end{aligned} \quad (9)$$

and

$$\begin{aligned} \text{SINR}_i^e &= \frac{\|(\mathbf{h}_i^T \otimes \mathbf{f}_i)\mathbf{w}\|^2}{\sum_{j \neq i}^K \|(\mathbf{h}_j^T \otimes \mathbf{f}_i)\mathbf{w}\|^2 + \sigma_n^2 \|(\mathbf{I} \otimes \mathbf{f}_i)\mathbf{w}\|^2 + \|\mathbf{f}_i \mathbf{a}\|^2 + \sigma_n^2} \\ &= \frac{\mathbf{w}^H \mathbf{Q}_i^e \mathbf{w}}{\mathbf{w}^H \mathbf{Z}_i^e \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2} \end{aligned} \quad (10)$$

where

$$\mathbf{w} = \text{vec}(\mathbf{W}) \quad (11)$$

$$\mathbf{Q}_i = (\mathbf{h}_i^T \otimes \mathbf{g}_i)^H (\mathbf{h}_i^T \otimes \mathbf{g}_i) \quad (12)$$

$$\begin{aligned} \mathbf{Z}_i &= \sum_{j \neq i}^K (\mathbf{h}_j^T \otimes \mathbf{f}_i)^H (\mathbf{h}_j^T \otimes \mathbf{f}_i) \\ &\quad + \sigma_n^2 (\mathbf{I} \otimes \mathbf{g}_i)^H (\mathbf{I} \otimes \mathbf{g}_i) \end{aligned} \quad (13)$$

$$\mathbf{L}_i = \mathbf{g}_i \mathbf{g}_i^H \quad (14)$$

$$\mathbf{Q}_i^e = (\mathbf{h}_i^T \otimes \mathbf{f}_i)^H (\mathbf{h}_i^T \otimes \mathbf{f}_i) \quad (15)$$

$$\begin{aligned} \mathbf{Z}_i^e &= \sum_{j \neq i}^K (\mathbf{h}_j^T \otimes \mathbf{f}_i)^H (\mathbf{h}_j^T \otimes \mathbf{f}_i) \\ &\quad + \sigma_n^2 (\mathbf{I} \otimes \mathbf{f}_i)^H (\mathbf{I} \otimes \mathbf{f}_i) \end{aligned} \quad (16)$$

$$\mathbf{L}_i^e = \mathbf{f}_i \mathbf{f}_i^H. \quad (17)$$

Furthermore, the relay power constraint (8c) can be reformulated as

$$\mathbf{w}^H ((\mathbf{y}_r^H \mathbf{y}_r) \otimes \mathbf{I}_N) \mathbf{w} + \text{Tr}(\Sigma) \leq P_r. \quad (18)$$

Consequently, the cost function of (8) can be rewritten as

$$\begin{aligned} &\sum_{i=1}^K \left( \log \left( 1 + \frac{\mathbf{w}^H \mathbf{Q}_i \mathbf{w}}{\mathbf{w}^H \mathbf{Z}_i \mathbf{w} + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2} \right) \right. \\ &\quad \left. - \log \left( 1 + \frac{\mathbf{w}^H \mathbf{Q}_i^e \mathbf{w}}{\mathbf{w}^H \mathbf{Z}_i^e \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2} \right) \right) \\ &= \log \left( \prod_{i=1}^K \underbrace{\frac{\mathbf{w}^H (\mathbf{Z}_i + \mathbf{Q}_i) \mathbf{w} + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2}{\mathbf{w}^H \mathbf{Z}_i \mathbf{w} + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2}}_{\mathcal{T}_i^1} \right. \\ &\quad \left. \cdot \underbrace{\frac{\mathbf{w}^H \mathbf{Z}_i^e \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2}{\mathbf{w}^H (\mathbf{Z}_i^e + \mathbf{Q}_i^e) \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2}}_{\mathcal{T}_i^2} \right) \\ &\triangleq \log(\mathcal{F}(\mathbf{w}, \Sigma)) \end{aligned} \quad (19)$$

where  $\mathcal{F}(\mathbf{w}, \Sigma) = \prod_{i=1}^K \mathcal{T}_i^1 \mathcal{T}_i^2$ .

As a result, we propose the following Lemma 1 to transform problem (8) into a more tractable form.

*Lemma 1:* Problem (8) is equivalent to the following problem:

$$\max_{\mathbf{w}, \Sigma} \mathcal{F}(\mathbf{w}, \Sigma) \quad (20a)$$

$$\text{s.t.} \quad \mathcal{C1} : \log \left( 1 + \frac{\mathbf{w}^H \mathbf{Q}_i \mathbf{w}}{\mathbf{w}^H \mathbf{Z}_i \mathbf{w} + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2} \right) \geq \gamma_i \quad (20b)$$

$$\mathcal{C2} : \mathbf{w}^H ((\mathbf{y}_r^H \mathbf{y}_r) \otimes \mathbf{I}_N) \mathbf{w} + \text{Tr}(\Sigma) \leq P_r. \quad (20c)$$

*Proof:* Proof of the Lemma 1 utilizes the feature of monotonic increasing for the function of  $\log(x)$ . ■

A simple checking on the Hessian matrix of the cost function (20a) reveals that (20a) is not concave with respect to the variable vector  $\mathbf{w}$  and  $\Sigma$ . Therefore, conventional convex optimization theories cannot be directly applied to problem (20). Instead, we transform problem (20) to another problem that can be solved with the theory of monotonic optimization.

New variables  $t_{1,i}$ ,  $t_{2,i}$  are introduced to serve as the lower bounds for  $\mathcal{T}_i^1$  and  $\mathcal{T}_i^2$ , respectively. Hence, (20) can be



transformed into another problem represented as

$$\max_{\mathbf{w}, \Sigma, t_{1,i}, t_{2,i}} \prod_{i=1}^K t_{1,i} t_{2,i} \quad (21a)$$

$$\text{s.t. } C1: \frac{\mathbf{w}^H (\mathbf{Z}_i + \mathbf{Q}_i) \mathbf{w} + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2}{\mathbf{w}^H \mathbf{Z}_i \mathbf{w} + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2} \geq \max\{2^{\gamma_i}, t_{1,i}\} \quad (21b)$$

$$C2: \frac{\mathbf{w}^H \mathbf{Z}_i^e \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2}{\mathbf{w}^H (\mathbf{Z}_i^e + \mathbf{Q}_i^e) \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2} \geq t_{2,i} \quad (21c)$$

$$C3: \mathbf{w}^H ((\mathbf{y}_r^H \mathbf{y}_r) \otimes \mathbf{I}_N) \mathbf{w} + \text{Tr}(\Sigma) \leq P_r. \quad (21d)$$

However, problem (21) is in the form of quadratic constrained quadratic programming, which is generally nonconvex, and difficult to deal with. For further simplification, we introduce  $\mathbf{X} = \mathbf{w}^H \mathbf{w}$ , and the optimization problem (21) can be transformed into the form of SDP with an additional rank-one constraint on  $\mathbf{X}$  as follows:

$$\max_{\mathbf{X}, \Sigma, t_{1,i}, t_{2,i}} \prod_{i=1}^K t_{1,i} t_{2,i} \quad (22a)$$

$$\text{s.t. } C1: \frac{\text{Tr}((\mathbf{Z}_i + \mathbf{Q}_i) \mathbf{X}) + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2}{\text{Tr}(\mathbf{Z}_i \mathbf{X}) + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2} \geq \max\{2^{\gamma_i}, t_{1,i}\} \quad (22b)$$

$$C2: \frac{\text{Tr}(\mathbf{Z}_i^e \mathbf{X}) + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2}{\text{Tr}((\mathbf{Z}_i^e + \mathbf{Q}_i^e) \mathbf{X}) + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2} \geq t_{2,i} \quad (22c)$$

$$C3: \text{Tr}(((\mathbf{y}_r^H \mathbf{y}_r) \otimes \mathbf{I}_N) \mathbf{X}) + \text{Tr}(\Sigma) \leq P_r \quad (22d)$$

$$C4: \text{Rank}(\mathbf{X}) = 1. \quad (22e)$$

Let  $\tilde{\mathbf{r}}^{\max} = [t_{1,1}^{\max}, \dots, t_{1,K}^{\max}, t_{2,1}^{\max}, \dots, t_{2,K}^{\max}]$  and  $\tilde{\mathbf{r}}^{\text{inner}} = [2^{\gamma_1}, 2^{\gamma_2}, \dots, 2^{\gamma_K}, 0]$  denote the upper bound and the lower bound of the achievable region, respectively. The prerequisite for applying the monotonic optimization on problem (22) is to create a feasibility problem to test whether a proposed rate tuple  $\tilde{\mathbf{r}}^{\text{inner}} + z(\tilde{\mathbf{r}}^{\max} - \tilde{\mathbf{r}}^{\text{inner}})$ ,  $z \in [0, 1]$  is achievable. Here, the feasibility problem can be constructed according to the original problem (20) as

$$\max_{\mathbf{X}, \Sigma, \tilde{t}_{1,i}, \tilde{t}_{2,i}} 0 \quad (23a)$$

$$\text{s.t. } C1: \frac{\text{Tr}((\mathbf{Z}_i + \mathbf{Q}_i) \mathbf{X}) + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2}{\text{Tr}(\mathbf{Z}_i \mathbf{X}) + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2} \geq \max\{2^{\gamma_i} - 1, z\tilde{t}_{1,i}\} \quad (23b)$$

$$C2: \frac{\text{Tr}(\mathbf{Z}_i^e \mathbf{X}) + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2}{\text{Tr}((\mathbf{Z}_i^e + \mathbf{Q}_i^e) \mathbf{X}) + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2} \geq z\tilde{t}_{2,i} \quad (23c)$$

$$C3: \text{Tr}(((\mathbf{y}_r^H \mathbf{y}_r) \otimes \mathbf{I}_N) \mathbf{X}) + \text{Tr}(\Sigma) \leq P_r \quad (23d)$$

$$C4: \text{Rank}(\mathbf{X}) = 1. \quad (23e)$$

Generally speaking, it is difficult to handle this rank constraint. Therefore, we resort to the semidefinite relaxation

---

**Algorithm 1** The Proposed MO-SDP Algorithm for the Design of Relay Precoder and AN.

---

**Step 1: Initialization**

- Compute  $\tilde{\mathbf{r}}^{\max} = [t_{1,1}^{\max}, \dots, t_{1,K}^{\max}, t_{2,1}^{\max}, \dots, t_{2,K}^{\max}]$ .
  - 1) Set  $\hat{r}_{i,j}^{\max} = [0, \dots, t_{i,j}^{\max}, \dots, 0]$ ,  $\forall i \in \{1, 2\}$ ,  $j \in 1, \dots, K$
  - 2) Insert  $\hat{r}_{i,j}^{\max}$ ,  $\forall i \in \{1, 2\}$ ,  $j \in 1, \dots, K$  to (24), and resort to bisection method to solve  $t_{i,j}^{\max}$ .
- Construct the set containing the outer boundary points:  $\mathcal{B}^{(1)} = \{\tilde{\mathbf{r}}^{\max}\}$ . Set the feasible tuple  $\tilde{\mathbf{r}}^{\text{inner}} = [2^{\gamma_1}, 2^{\gamma_2}, \dots, 2^{\gamma_K}, 0]$ ,  $\epsilon = 0.001$ ,  $\eta = 0.001$ ,  $L_{\max} = 20$  and  $l = 1$ .

**Step 2: Iteration**

- $\tilde{\mathbf{r}}^{\text{outer}} = \arg \max\{g(\tilde{\mathbf{r}}) | \tilde{\mathbf{r}} \in \mathcal{B}^{(1)}\}$ .
- Find the intersection point of the boundary of achievable region with the segment between  $\tilde{\mathbf{r}}^{\text{inner}}$  and  $\tilde{\mathbf{r}}^{\max}$  through bisection method. The problem is formulated as follows and its solution is denoted as  $z^{\text{opt}}$

$$\begin{aligned} \max \quad & z \in [0, 1] \\ \text{s.t.} \quad & \text{Problem (24) is feasible with} \\ & z\tilde{\mathbf{r}}^{\text{outer}} \text{ satisfying} \\ & \text{precision } \eta. \end{aligned} \quad (25)$$

- $\tilde{r}^{(l)} = z\tilde{\mathbf{r}}^{\text{outer}}$  and  $\tilde{\mathbf{r}}^{\text{inner}} = \arg \max\{g(\tilde{\mathbf{r}}^{\text{inner}}), g(\tilde{\mathbf{r}}^{(l)})\}$
- If  $g(\tilde{\mathbf{r}}^{\text{inner}}) + \epsilon \geq g(\tilde{\mathbf{r}}^{\text{outer}})$ , terminate the iteration and go to Step 4; Else,  $l = l + 1$ , return to Step 2.

**Step 3: Termination**

- $l = L_{\max}$ ; Else,  $l = l + 1$ , return to Step 2.

**Step 4: Output**

- Solve problem (24) on condition of  $\tilde{\mathbf{r}}^{\text{inner}}$  and obtain the solutions  $\mathbf{X}^*$  and  $\Sigma^*$ , which respectively correspond to the solution of  $\mathbf{X}$  and  $\Sigma$ .
  - If  $\mathbf{X}^* = \mathbf{I}$ , use eigen-value decomposition to obtain  $\mathbf{X}^* = \mathbf{w}^{*H} \mathbf{w}^*$ . Otherwise, use randomization technique to get an approximate rank-one solution  $\mathbf{w}^*$  [20].
  - Output  $\mathbf{W}^* = \text{mat}(\mathbf{w}^*)$  and  $\Sigma^*$ .
- 

by neglecting this rank constraint so that the feasibility problem turns into a standard SDP problem as follows:

$$\max_{\mathbf{X}, \Sigma, \tilde{t}_{1,i}, \tilde{t}_{2,i}} 0 \quad (24a)$$

$$\text{s.t. } C1: \frac{\text{Tr}((\mathbf{Z}_i + \mathbf{Q}_i) \mathbf{X}) + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2}{\text{Tr}(\mathbf{Z}_i \mathbf{X}) + \text{Tr}(\mathbf{L}_i \Sigma) + \sigma_n^2} \geq \max\{2^{\gamma_i} - 1, z\tilde{t}_{1,i}\} \quad (24b)$$

$$C2: \frac{\text{Tr}(\mathbf{Z}_i^e \mathbf{X}) + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2}{\text{Tr}((\mathbf{Z}_i^e + \mathbf{Q}_i^e) \mathbf{X}) + \text{Tr}(\mathbf{L}_i^e \Sigma) + \sigma_n^2} \geq z\tilde{t}_{2,i} \quad (24c)$$

$$C3: \text{Tr}(((\mathbf{y}_r^H \mathbf{y}_r) \otimes \mathbf{I}_N) \mathbf{X}) + \text{Tr}(\Sigma) \leq P_r. \quad (24d)$$

With respect to QoS requirements for L-UE and the power constraint of relay, the achievable region  $\Upsilon$  of multiple Rayleigh

quotients should conform with the concept of normal set. Specifically, it should be confined within a box. To determine the exact position of a box, its lower and upper vertex should be specified.

In our case, the lower vertex is denoted as  $\tilde{\mathbf{r}}^{\min} = [2^{\gamma_1}, 2^{\gamma_2}, \dots, 2^{\gamma_K}, 0]$ , of which the first  $K$  entries correspond to the minimum requirements for L-UE's SINR, the rest entries are set to zeros for no specific requirement for eavesdropper. The upper vertex of achievable region is denoted as  $\tilde{\mathbf{r}}^{\max} = [t_{1,1}^{\max}, \dots, t_{1,K}^{\max}, t_{2,1}^{\max}, \dots, t_{2,K}^{\max}]$ , and the ways of calculating  $\tilde{\mathbf{r}}^{\max}$  will be explained later. Obviously, the achievable region  $\Upsilon$  will be confined in the box  $[\tilde{\mathbf{r}}^{\min}, \tilde{\mathbf{r}}^{\max}]$ , i.e., for any achievable Rayleigh quotient set  $\mathbf{r}$ ,  $\tilde{\mathbf{r}}^{\min} \leq \mathbf{r} \leq \tilde{\mathbf{r}}^{\max}$  must be satisfied. The next move will focus on determining the exact shape of the boundaries of an achievable region  $\Upsilon$ .

We propose that the monotonic optimization algorithm can be used to approximate the exact shape of the boundaries of achievable region  $\Upsilon$  by successively constructing polyblocks. First, we set  $\tilde{\mathbf{r}}^{\min}$  as the origin and  $\tilde{\mathbf{r}}^{\max}$  as the first candidate for outer boundary set. For the direction along  $\tilde{\mathbf{r}}^{\min}\tilde{\mathbf{r}}^{\max}$ , we need to determine the intersection between line  $[\tilde{\mathbf{r}}^{\min}, \tilde{\mathbf{r}}^{\max}]$  and the achievable region of problem (22). Accordingly, we need to verify whether  $\tilde{\mathbf{r}}^{\min} + z(\tilde{\mathbf{r}}^{\max} - \tilde{\mathbf{r}}^{\min})$ ,  $z \in [0, 1]$  falls in the achievable region or not, which corresponds to the following optimization problem (23). Bisection method can be applied to find the value of  $z$  that stands for the intersection point.

Generally speaking, it is difficult to deal with this rank constraint. Traditional method is to resort to semidefinite relaxation by neglecting this rank constraint. Therefore, the feasibility problem can be turned into a standard SDP problem (24), which can be solved efficiently by convex software package, i.e., CVX [21], [22].

However, the MO-SDP algorithm cannot guarantee the acquired solution  $\mathbf{X}^{\text{opt}}$  conforms with the rank-one constraint. Therefore, we resort to randomization technique to get an approximate rank-one solution [20]. We can first generate a series of random vector  $\bar{\mathbf{x}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{X}^{\text{opt}})$  and scale it by a factor of  $\rho$  to satisfy all the constraints in (24), i.e.,

$$\mathbf{x} = \rho \bar{\mathbf{x}} \quad (26)$$

where  $\rho$  can be expressed as

$$\rho = \sqrt{\frac{P_r - \text{Tr}(\mathbf{\Sigma}^{\text{opt}})}{\text{Tr}((\mathbf{y}_r^H \mathbf{y}_r) \otimes \mathbf{I}_N) \mathbf{X}^{\text{opt}}}}. \quad (27)$$

For each vector variables, we compute their corresponding SSRs by (8 a). Among all candidates, we choose the one that achieve best SSR as the approximate rank-one solution.

For the MO-SDP algorithm, it is a suboptimal algorithm since the rank constraint could not always be guaranteed. The procedure of the MO-SDP algorithm is summarized in Algorithm 1.

### C. Complexity Analysis

For a small number of relay antennas as well as pairs of L-UE and eavesdropper, the MO-SDP algorithm works fine with a tolerable complexity. The main computation complexity is incurred from the bisection algorithm for specifying the inter-

sections of achievable region's boundary and the line between origin and outer vertexes. Considering the convex form of feasibility problem (24), the complexity of each feasibility problem can be expressed as  $\lceil \log_2(\frac{r^{\max}}{\eta}) \rceil \mathcal{O}(\max\{2K + 1, N^2\}^4 N \log(\frac{1}{\kappa}))$ . Specifically,  $\lceil \log_2(\frac{r^{\max}}{\eta}) \rceil$  indicates the number of feasibility problems for each bisection algorithm with precision  $\eta$ , and  $\mathcal{O}(\max\{2K + 1, N^2\}^4 N \log(\frac{1}{\kappa}))$  reflects the worst-case complexity for solving (24) with precision  $\kappa$  [18]–[20]. However, with the increase of relay antennas and pairs of L-UEs and eavesdroppers, the complexity of the MO-SDP algorithm increases exponentially, mainly due to the expanded searching dimension and variables. Therefore, in the next section, we will propose a low-complexity relay precoder algorithm to alleviate the complexity issue.

## IV. LOW-COMPLEXITY RELAY PRECODER DESIGN

In practice, the proposed MO-SDP algorithm is of very high complexity and might be difficult to be put into use, if not impossible. For example, if fast fading exists in the considered channels, the available time for computing the optimal relay precoder will be very limited. Therefore, it is desirable to design an alternative low-complexity algorithm that can achieve comparable performance with the MO-SDP algorithm. In this section, we propose a low-complexity algorithm based on the NuS projection, which places the relay's transmitting signal into the NuS of channels between the relay and each eavesdropper. It should be mentioned that the NuS projection method has been employed in the existing studies [23], [24]. In our NuS design, since the rate achieved by each eavesdropper is zero in ideal cases, the introduction of AN in this circumstance can only is a waste of relay power that leads to worse secrecy performance. Thus, we only focus on the relay precoder design for the NuS algorithm. The NuS-based method puts constraints on the structure of the relay precoder, thus turning the optimization problem into a power allocation problem. In addition, a user selection algorithm is proposed for the case without enough spatial degrees of freedom.

### A. NuS Algorithm for $N \geq 2K$

For the case of  $N \geq 2K$ , there are enough spatial degrees of freedom to nullify the eavesdropper's receiving signal. Inspired by the concept of the block diagonalization precoder and the zero forcing precoder, we assume that the relay's precoder takes the following form:

$$\mathbf{W} = \mathbf{U} \underbrace{\tilde{\mathbf{G}}^H (\tilde{\mathbf{G}} \tilde{\mathbf{G}}^H)^{-1} \mathbf{\Theta}}_{\mathbf{F}_{\tilde{\mathbf{G}}}} \underbrace{(\mathbf{H}^H \mathbf{H})^{-1} \mathbf{H}^H}_{\mathbf{F}_{\mathbf{H}}} \quad (28)$$

where  $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_K]$ ,  $\mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_K]$ , and  $\tilde{\mathbf{G}} = \mathbf{G}\mathbf{U}$ . The relay precoder is composed of four parts. Specifically,  $\mathbf{U} \in \mathcal{NUL}(\{\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_K\})$  corresponds to the block diagonalization precoder, which nullifies the leakage of the L-UEs' data to all eavesdroppers. Note that after introducing the matrix  $\mathbf{U}$ , the equivalent forward channel becomes  $\mathbf{G}\mathbf{U}$ , instead of  $\mathbf{G}$ . Besides,  $\mathbf{F}_{\tilde{\mathbf{G}}}$  and  $\mathbf{F}_{\mathbf{H}}$  are the zero forcing precoders for forward channels and backward channels, respectively. Finally,  $\mathbf{\Theta}$  is a

scalar and diagonal matrix with entries  $\lambda_i, i = 1, \dots, K$ , which can be regarded as a power allocation matrix.

Next, the broadcast signal transmitted by a relay can be written as

$$\mathbf{U}\tilde{\mathbf{G}}^H(\tilde{\mathbf{G}}\tilde{\mathbf{G}}^H)^{-1}\boldsymbol{\Theta}\mathbf{s} + \mathbf{U}\tilde{\mathbf{G}}^H(\tilde{\mathbf{G}}\tilde{\mathbf{G}}^H)^{-1}\boldsymbol{\Theta}(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H\mathbf{n}_r. \quad (29)$$

Consequently, the signal received by all L-UEs can be stacked into

$$\mathbf{y} = \boldsymbol{\Theta}\mathbf{s} + \boldsymbol{\Theta}(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H\mathbf{n}_r + \mathbf{n} \quad (30)$$

where  $\mathbf{y} = [y_1, \dots, y_i, \dots, y_K]^T$ ,  $y_i$  is the received signal by the  $i$ th L-UE.

Therefore, the cost function of (8) can be simplified to the form of sum-rate maximization of L-UEs, which can be expressed as

$$\max_{\mathbf{w}} \quad \sum_{i=1}^K \log(1 + \text{SINR}_i) \quad (31a)$$

$$\text{s.t.} \quad \|\mathbf{x}_r\|^2 \leq P_r \quad (31b)$$

$$\log(1 + \text{SINR}_i) \geq \gamma_i, i = 1, \dots, K \quad (31c)$$

$$\text{SINR}_i^e = 0. \quad (31d)$$

If we let  $\sigma_{\mathbf{h}_i}^2 = \|[(\mathbf{H}^H\mathbf{H})^{-1}\mathbf{H}^H]_{i,:}\|^2$ , the SINR of the  $i$ th legitimate user becomes

$$\text{SINR}_i = \frac{\lambda_i^2}{\sigma_n^2 \sigma_{\mathbf{h}_i}^2 \lambda_i^2 + \sigma_n^2}. \quad (32)$$

Moreover, the relay power constraint (31b) can be formulated as

$$\begin{aligned} \|\mathbf{x}_r\|^2 &= \sum_{i=1}^K \sigma_{\mathbf{g}_i}^2 \lambda_i^2 + \sigma_n^2 \text{Tr}(\mathbf{J}\boldsymbol{\Theta}\mathbf{K}\boldsymbol{\Theta}^H) \\ &\stackrel{(a)}{\leq} \sum_{i=1}^K \sigma_{\mathbf{g}_i}^2 \lambda_i^2 + \sigma_n^2 \pi_1(\mathbf{J})\pi_1(\mathbf{K})\text{Tr}(\boldsymbol{\Theta}^H\boldsymbol{\Theta}) \\ &= \sum_{i=1}^K (\sigma_{\mathbf{g}_i}^2 + \sigma_n^2 \pi_1(\mathbf{J})\pi_1(\mathbf{K}))\lambda_i^2 \end{aligned} \quad (33)$$

where  $\sigma_{\mathbf{g}_i}^2 = \|[\mathbf{U}\tilde{\mathbf{G}}^H(\tilde{\mathbf{G}}\tilde{\mathbf{G}}^H)^{-1}]_{i,:}\|^2$ , and  $\pi_1(\mathbf{J})$  and  $\pi_1(\mathbf{K})$  denote the largest eigenvalue of  $\mathbf{J}$  and  $\mathbf{K}$ , respectively. The inequality (a) holds because of  $\text{Tr}(\mathbf{A}\mathbf{B}) \leq \pi_1(\mathbf{A})\text{Tr}(\mathbf{B})$ .

Therefore, the optimization problem (31) turns into

$$\max_{\lambda_i} \quad \sum_{i=1}^K \log(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{\mathbf{h}_i}^2 \lambda_i^2 + \sigma_n^2}) \quad (34a)$$

$$\text{s.t.} \quad \sum_{i=1}^K (\sigma_{\mathbf{g}_i}^2 + \sigma_n^2 \pi_1(\mathbf{J})\pi_1(\mathbf{K}))\lambda_i^2 \leq P_r \quad (34b)$$

$$\log(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{\mathbf{h}_i}^2 \lambda_i^2 + \sigma_n^2}) \geq \gamma_i \quad (34c)$$

$$\lambda_i \geq 0. \quad (34d)$$

Regarding the solution of problem (34), we propose Lemma 2 and 3.

*Lemma 2:* For the optimal solution of (34), (34b) must be achieved with equality, i.e.,

$$\sum_{i=1}^K (\sigma_{\mathbf{g}_i}^2 + \sigma_n^2 \pi_1(\mathbf{J})\pi_1(\mathbf{K}))\lambda_i^2 = P_r. \quad (35)$$

*Proof:* The proof is straightforward by using the monotonic property of function  $\sum_{i=1}^K \log(1 + \frac{\lambda_i^{(o)2}}{\sigma_n^2 \sigma_{\mathbf{h}_i}^2 \lambda_i^{(o)2} + \sigma_n^2})$  with respect to  $\lambda_i$ . ■

*Lemma 3:* The optimal solution of (34) can be expressed as

$$|\lambda_i|^2 = \begin{cases} 0, & \text{if } b_i^2 - 4a_i c_i \geq 0 \\ \max \left\{ \frac{-b_i \pm \sqrt{(b_i^2 - 4a_i c_i)}}{2a_i}, 0 \right\}, & \text{if } b_i^2 - 4a_i c_i \leq 0 \end{cases} \quad (36)$$

where

$$a_i = \ln 2 \cdot \alpha \sigma_n^2 \sigma_{\mathbf{h}_i}^2 (\sigma_n^2 \sigma_{\mathbf{h}_i}^2 + 1) (\sigma_{\mathbf{g}_i}^2 + \sigma_n^2 \pi_1(\mathbf{J})\pi_1(\mathbf{K}))$$

$$b_i = \ln 2 \cdot \alpha \sigma_n^4 \sigma_{\mathbf{h}_i}^2 (\sigma_{\mathbf{g}_i}^2 + \sigma_n^2 \lambda_1 \pi_1(\mathbf{J})\pi_1(\mathbf{K})) \quad (37)$$

$$+ \ln 2 \cdot \alpha (\sigma_n^2 \sigma_{\mathbf{h}_i}^2 + 1) (\sigma_{\mathbf{g}_i}^2 + \sigma_n^2 \lambda_1 \pi_1(\mathbf{J})\pi_1(\mathbf{K})) \quad (38)$$

$$c_i = \ln 2 \cdot \alpha \sigma_n^4 (\sigma_{\mathbf{g}_i}^2 + \sigma_n^2 \pi_1(\mathbf{J})\pi_1(\mathbf{K})) + (1 - \beta_i) \sigma_n^2. \quad (39)$$

$\alpha$  and  $\beta_i$  are the dual variables related to (34b) and (34c), respectively.

*Proof:* See Appendix. A. ■

The exact values of  $\alpha$  and  $\beta_i$  are unknown, hence we cannot directly calculate  $\lambda_i$  via (36). Nevertheless, inspired by the key idea of the water-filling algorithm, we propose an iterative algorithm summarized in Algorithm 2 for updating  $\alpha$  and  $\beta_i$ .

First, we assume  $\beta_i = 0 \forall i$ , and from Karush-Kuhn-Tucker (KKT) condition of (45) it means that (34c) always holds. If  $b_i^2 - 4a_i c_i \geq 0$ , let  $|\lambda_i|^2 = 0$ , otherwise,  $|\lambda_i|^2 = \frac{-b_i \pm \sqrt{(b_i^2 - 4a_i c_i)}}{2a_i}$ . Together with (35), we can calculate the value of  $\alpha$ . With the update of  $\alpha$ , explicit value of  $\lambda_i$  can be obtained. Then, we check whether the inequality of (34c) holds with the calculated  $\lambda_i$ . For the violations, we simply set the equality to compute the relevant value of  $\lambda_i$  as the final result. This process is repeated until (34c) holds for each  $i$ .

### B. NuS Algorithm $N \leq 2K$

For the case of  $N \leq 2K$ , there are not enough spatial degrees of freedom to project all transmitted signals into the NuS of eavesdropper's channels. Instead, we consider a user selection algorithm to serve  $\lfloor N/2 \rfloor$  out of  $2K$  L-UEs that can maximize the SSR performance. The problem is then formulated as

$$\mathbb{S}^{\text{opt}} = \underset{\mathbb{S} \subset \mathbb{T}}{\text{argmax}} \sum_{i=1}^K (\log(1 + \text{SINR}_i) - \log(1 + \text{SINR}_i^e)) \quad (40)$$

where  $\mathbb{S}$  and  $\mathbb{T}$  denote the set of selected  $\lfloor N/2 \rfloor$  users and the set of total  $K$  L-UEs, respectively.

**Algorithm 2: NuS Algorithm Based Relay Precoder Design.**

Step 1:

- Assume  $\beta_i = 0, \forall i \in \Omega$  and  $\Omega = \{1, 2, \dots, K\}$ .
- $\forall i \in \Omega$ , If  $b_i^2 - 4a_i c_i \geq 0$ , let  $|\lambda_i|^2 = 0$ , else  $|\lambda_i|^2 = \frac{-b_i \pm \sqrt{(b_i^2 - 4a_i c_i)}}{2a_i}$ .

Step 2:

- Insert the calculated  $|\lambda_i|^2$  into (44) and compute  $\alpha$ .
- Update  $\lambda_i$  by (36) via inserting  $\alpha_i$  and  $\beta_i$ .

Step 3:

- Set  $\Psi = \phi$ . Check the validity of the inequalities  $\forall i \in \Omega$ ,  $\log(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{h_i}^2 \lambda_i^2 + \sigma_n^2}) \geq \gamma_i$ .
- For the  $\lambda_i$  violating the inequality,
  - 1) Compute the value of  $\Delta_i = \gamma_i - \log(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{h_i}^2 \lambda_i^2 + \sigma_n^2})$  and  $\Psi = \Psi \cup \{i\}$ .
  - 2) Compute  $\hat{i} = \arg\max \Delta_i, \forall i \in \Psi$ .
  - 3) Set the  $\log(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{h_i}^2 \lambda_i^2 + \sigma_n^2}) = \gamma_{\hat{i}}$ , and recompute  $\lambda_i$ .
  - 4)  $\Omega = \Omega / \{\hat{i}\}$  and go to Step 2.

Step 4:

- If  $\forall i \in \Omega$ ,  $\log(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{h_i}^2 \lambda_i^2 + \sigma_n^2}) \geq \gamma_i$  holds, stop and output  $\lambda_i$ .

The optimal user selection can be found by exhaustive searching over the set of  $\mathbb{T}$ . However, this brute-force algorithm is of high complexity, which might deny its application in practical networks.

As an alternative, we propose a suboptimal and greedy user selection algorithm with relatively low complexity. First, we check each L-UE from  $\mathbb{T}$  and calculate its corresponding precoders via Algorithm 2. With the calculated precoders, we can obtain each L-UE's secrecy rate. Then, we select the user achieving the maximum secrecy rate and add it into  $\mathbb{S}$ . For the rest of the L-UEs, we choose them one by one from  $\mathbb{T}$  to maximize the SSR performance until  $\lfloor N/2 \rfloor$  users are selected, i.e.,  $|\mathbb{S}| = \lfloor N/2 \rfloor$ . The proposed algorithm is presented in Algorithm 3.

### C. Complexity Analysis

Since we have a quasiclosed-form expression for the relay precoder, the complexity has been significantly reduced compared with the MO-SDP algorithm. Based on the description in Algorithm 2, we can conclude that the complexity of the NuS algorithm is in the order of  $\mathcal{O}(K^2)$  for  $N \geq 2K$ . For the case of  $N \leq 2K$ , its complexity is  $\mathcal{O}(KN^2)$  mainly because of Algorithm 3.

## V. SIMULATION RESULTS AND ANALYSIS

In this section, we evaluate the performance of the proposed algorithms via simulation. For convenience, we use  $[N, K]$  to denote the case with  $N$  antenna relay and  $K$  pairs of L-UE and eavesdropper. Additionally, all channels are assumed to experience Rayleigh fading and remain unchanged during a complete transmission. All simulation results are averaged over

**Algorithm 3: Low Complexity User Selection Algorithm**

Step 1:

- Assume  $n = 1, \mathbb{S} = \phi, \mathbb{T} = \{U_1, U_2, \dots, U_{K-1}, U_K\}$ .

Step 2:

- Enumerate each remaining L-UE from  $\mathbb{T}$ , together with the users in  $\mathbb{S}$  calculate the precoders via Algorithm 2, denoted as  $\mathbf{W}_i^{(n)}, i = 1, \dots, K - n$ .

Step 3:

- With the calculated precoders  $\mathbf{W}_i^{(n)}$ , choose the L-UE that can achieve the maximum SSR as

$$\mathbf{U}^* = \arg\max_{\mathbf{U}_i \in \mathbb{T}} \sum_{i=1}^K (\log(1 + \text{SINR}_i) - \log(1 + \text{SINR}_i^e)). \quad (41)$$

Step 4:

- Add  $\mathbf{U}^*$  into  $\mathbb{S}$ , remove  $\mathbf{U}^*$  out of  $\mathbb{T}$ .
- If  $n \leq \lfloor N/2 \rfloor$ , go back to Step.2, else output  $\mathbb{S}$ .

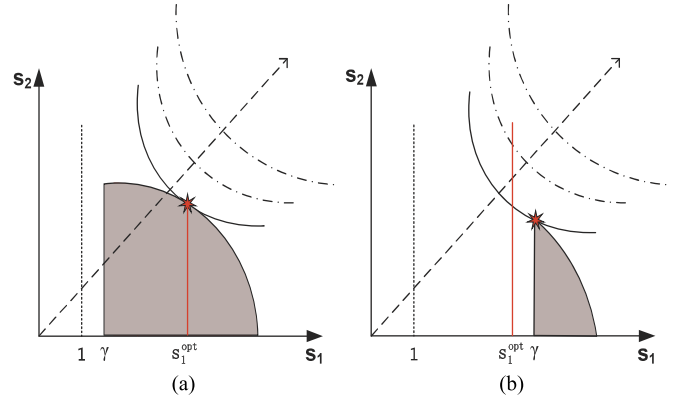


Fig. 4. Achievable region for a single pair of L-UE and eavesdropper.

100 channel realizations, except the results for the examination of the achievable region (fixed channel vectors, see Table 1). Furthermore, SNR is denoted as  $\frac{P_r}{\sigma_n^2}$ , and we assume  $\gamma_i = \gamma \forall i$ .

### A. Achievable Region for Single Pair of L-UE and Eavesdropper

For the single pair case, we investigate the achievable region of two Rayleigh quotients, which is defined as

$$\mathcal{S} = \left\{ \{s_1, s_2\} \left| \begin{aligned} s_1 &= \frac{\mathbf{w}^H (\mathbf{Z}_1 + \mathbf{Q}_1) \mathbf{w} + \text{Tr}(\mathbf{L}_i \mathbf{\Sigma}) + \sigma_n^2}{\mathbf{w}^H \mathbf{Z}_1 \mathbf{w} + \text{Tr}(\mathbf{L}_i \mathbf{\Sigma}) + \sigma_n^2} \\ s_2 &= \frac{\mathbf{w}^H \mathbf{Z}_1^e \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \mathbf{\Sigma}) + \sigma_n^2}{\mathbf{w}^H (\mathbf{Z}_1^e + \mathbf{Q}_1^e) \mathbf{w} + \text{Tr}(\mathbf{L}_i^e \mathbf{\Sigma}) + \sigma_n^2} \end{aligned} \right. \right\}. \quad (42)$$

Since  $\mathbf{Z}_1 \geq \mathbf{0}, \mathbf{Z}_1^e \geq \mathbf{0}, \mathbf{Q}_1 \geq \mathbf{0}$ , and  $\mathbf{Q}_1^e \geq \mathbf{0}$ , the minimum of  $s_1$  is less than 1 for its denominator is larger than the numerator. Similarly, the maximum of  $s_2$  cannot exceed 1 for its numerator is always larger than the denominator. In Fig. 4, the shaded region illustrates the achievable region  $\mathcal{S}$ . Since the



TABLE I  
CHANNELS USED FOR EVALUATION OF ACHIEVABLE REGION FOR SINGLE PAIR OF L-UE AND EAVESDROPPER

$K = 1$	
$N = 2$	$\mathbf{h} = [-0.9330 - 0.1373i, 0.6457 - 0.4958i]^T$ $\mathbf{g} = [0.6031 - 0.8004i, 0.3893 - 0.5248i]$ $\mathbf{f} = [-0.3617 - 2.3395i, -0.7935 - 0.5434i]$
$N = 3$	$\mathbf{h} = [-0.8244 + 0.5664i, 0.7778 - 0.5211i, 0.7869 + 0.0909i]^T$ $\mathbf{g} = [-1.2812 - 0.7337i, 0.4838 - 0.3295i, 0.4411 - 0.1069i]$ $\mathbf{f} = [0.4848 - 0.8359i, 0.0330 - 0.1309i, 0.9149 + 0.2455i]$
$N = 4$	$\mathbf{h} = [0.8576 + 1.3809i, 0.3070 - 0.7095i, 0.2146 - 0.5851i, -0.1260 + 0.6932i]^T$ $\mathbf{g} = [-1.2592 - 0.5144i, 0.5696 - 0.2819i, -0.8380 - 0.1668i, 0.0919 + 0.4464i]$ $\mathbf{f} = [-0.5888 - 1.8019i, -0.5206 + 0.6147i, 0.6240 - 0.4560i, -0.0978 + 0.1421i]$
$N = 5$	$\mathbf{h} = [0.1481 + 0.6904i, -0.2929 + 0.6966i, -0.1382 - 1.7217i, -0.5443 + 0.1309i, 0.9169 - 0.3372i]^T$ $\mathbf{g} = [-1.0275 + 1.2590i, 0.2917 + 0.2583i, -0.4531 - 0.3828i, -0.0626 + 0.2260i, -0.1845 + 0.4669i]$ $\mathbf{f} = [0.6072 - 1.4111i, -0.0030 + 0.5002i, 0.2417 + 0.4216i, -0.7797 - 0.1996i, -0.3278 + 0.0521i]$

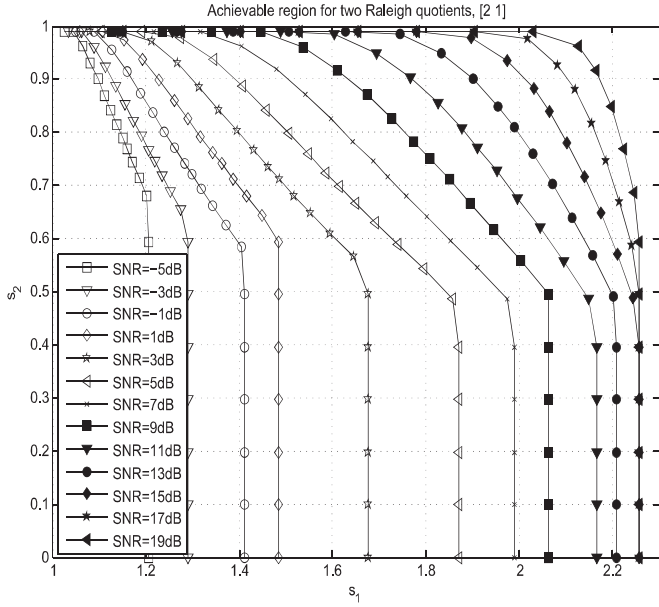


Fig. 5. Achievable region for [21] with SNR ranging from  $-5$  to  $19$  dB.

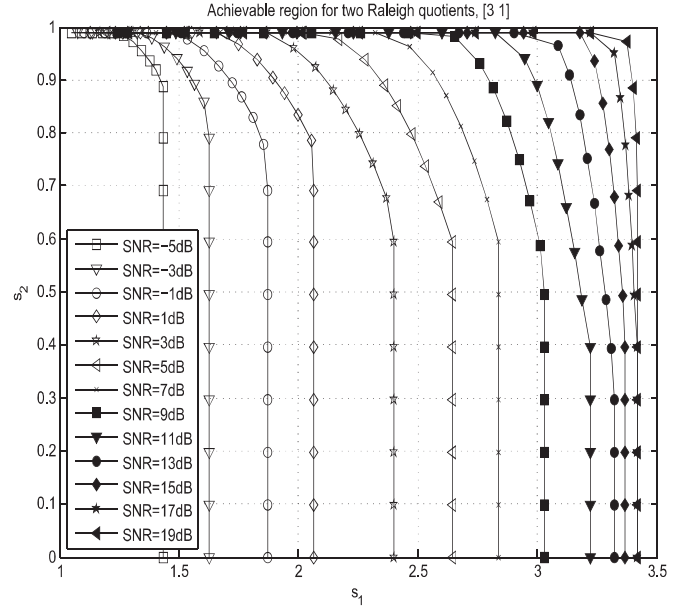


Fig. 6. Achievable region for [31] with SNR ranging from  $-5$  to  $19$  dB.

objective is to maximize  $s_1 \cdot s_2$ , and thus, the optimal solution should be the largest value of  $a$  to satisfy that  $s_2 = \frac{a}{s_1}$  and  $\mathcal{S}$  at least have one intersection point, as shown in Fig. 4. Note that in Fig. 4 the star represents the optimal values of  $s_1$  and  $s_2$  with a given  $\gamma$ .

Then, we investigate the achievable regions with the given channel vectors listed in Table I. Specifically, in Fig. 5, the case of [2 1] is evaluated. As SNR increases, the achievable region is gradually enlarged. According to the monotonic optimization theory, the optimal value should be found at the boundary of achievable region.

Furthermore, we can predict that the NuS algorithm can achieve the comparable performance as the MO-SDP algorithm in high SNR region. This is because the corner part of the achievable region's boundary becomes much sharper for the high SNR case, and the optimal value of  $s_2$  is very close to 1, which means that eavesdroppers barely receive data.

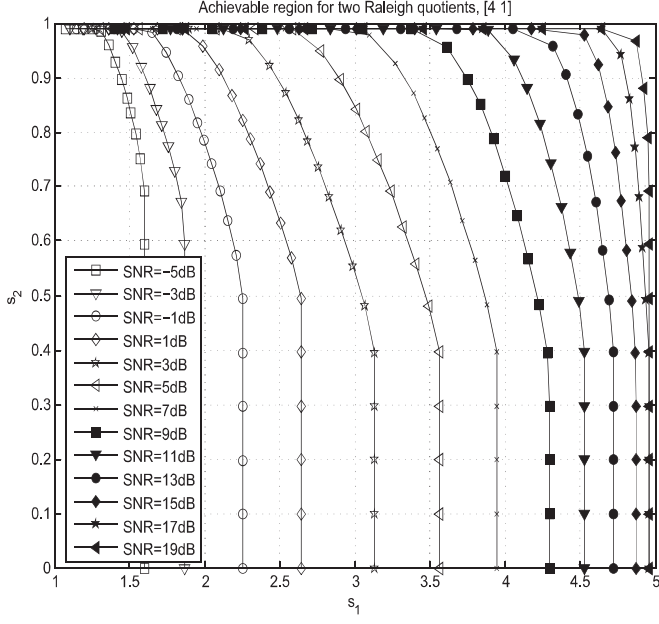
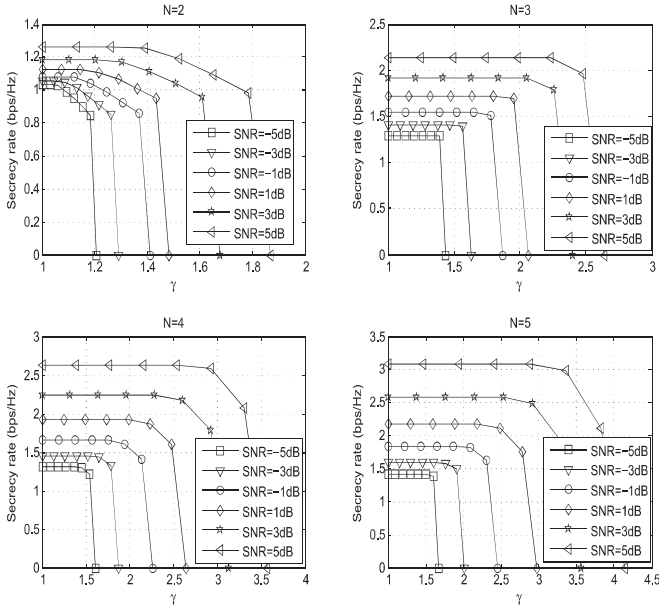
In addition, in Figs. 6 and 7, we examine the achievable region for the cases of [3 1] and [4 1], respectively, and similar observation can be drawn for these figures as well. The corresponding channels are shown in Table I.

### B. Secrecy Rate Versus Various Thresholds

Additionally, in Fig. 8 we display the performance of secrecy rate with respect to  $\gamma$  for various relay antenna numbers by using the channels in Table I. It should be noted that the secrecy rate is a constant for the case of  $\gamma \leq a^{\text{opt}}$ , where  $a^{\text{opt}}$  corresponds to the optimal value by setting  $\gamma = 1$ . When  $\gamma \geq a^{\text{opt}}$ , the optimal value decreases as  $\gamma$  increases because the feasible set of problem (10) shrinks. This kind of phenomenon is consistent with the illustrations in Fig. 4(a) and (b).

### C. SSR Evaluation for One or Multiple Pairs of L-UE and Eavesdropper

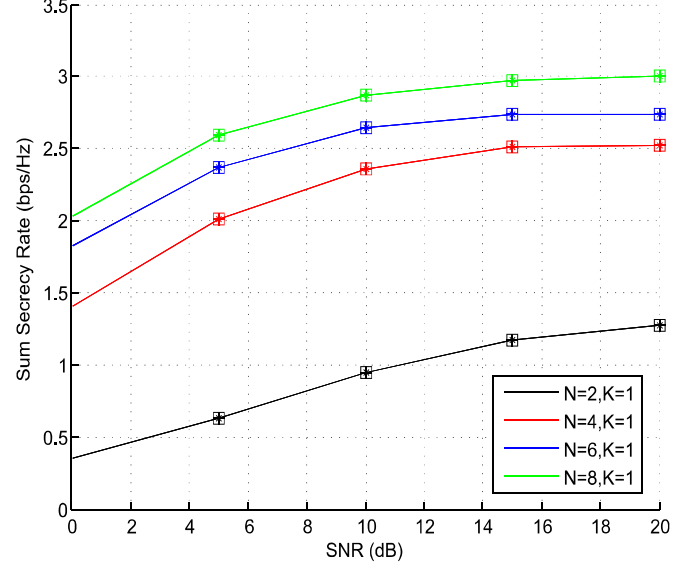
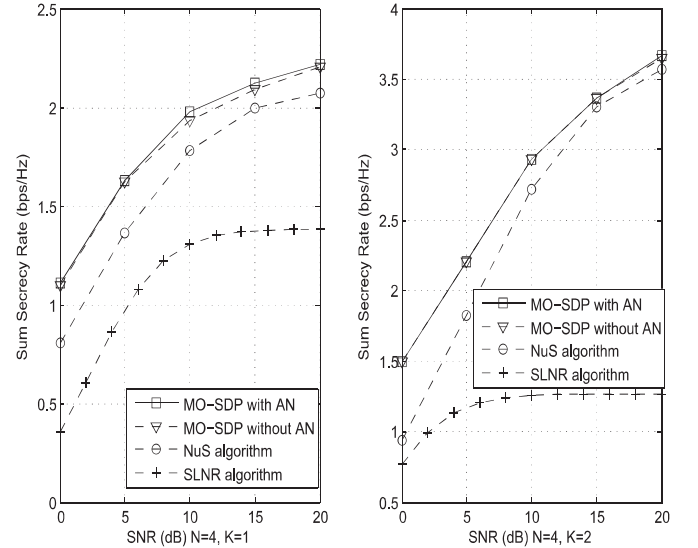
In this Section, we evaluate the SSR performance for various numbers of L-UE and eavesdropper pairs. For the purpose of fair comparison,  $\gamma$  is set to 1, indicating that no QoS requirements is forced for L-UEs. The solution of problem (24) without the rank-one constraint can be regarded as an upper bound for problem (8). After the utilization of randomization technique, the resulting solution can be viewed as an lower bound for


 Fig. 7. Achievable region for [4 1] with SNR ranging from  $-5$  to  $19$  dB.

 Fig. 8. Secrecy rate versus various threshold  $\gamma$ .

problem (8). From our simulation results, we will see that the upper bound and the lower bound are very close to each other.

In Fig. 9, we consider the simplest case, where there are only one source and one destination. In this case, the optimal solution can be obtained by using the mathematical technique introduced in [25]. From the simulation, we can see that our proposed MO-SDP algorithm can achieve the same performance with the algorithm proposed in [25], which instead shows its effectiveness.

In Fig. 10, the SSRs are shown for one pair and two pairs of L-UE and eavesdropper, respectively. Specifically, we investigate the performance of SSRs for the upper bound, the MO-SDP


 Fig. 9. Comparisons of SSR performance between the MO-SDP algorithm and the method proposed in [25] for single-user-eavesdropper case. \* denotes the MO-SDP algorithm, and  $\square$  denotes the method in [25]

 Fig. 10. Performance of SSR with  $N = 4$ , for the upper bound, the MO-SDP with/without AN algorithm, the NuS algorithm, and the SLNR algorithm.

with/without AN algorithm, and the NuS algorithm. The relay precoding matrix for the MO-SDP algorithm without AN can be obtained by fixing  $\Sigma = \mathbf{0}$  in Section III. Furthermore, we also compare the proposed algorithms with some precoding schemes of fixed structure. Specifically, we choose the signal-to-leakage-plus-noise (SLNR) precoding scheme [26], which has been widely used in many secrecy-related literatures [7], [27]. In accordance with our specific system model, we assume that the SLNR precoding matrix is composed of three parts, e.g.,  $\mathbf{W} = \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{C}$ , where  $\mathbf{A} \in \mathcal{NUL}([f_1, f_2, \dots, f_K])$ ,  $\mathbf{B}$  is the SLNR precoding matrix with respect to equivalent channel  $\mathbf{G}\mathbf{A}$  [26], and  $\mathbf{C} = (\mathbf{H}^H \mathbf{H})^{-1} \mathbf{H}^H$ .

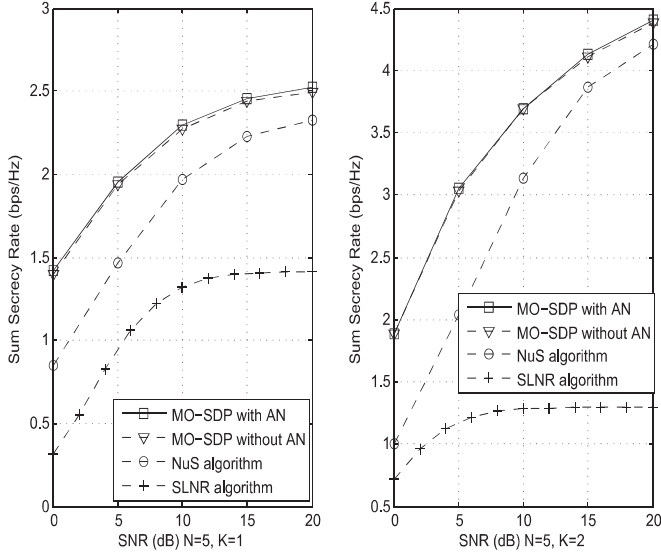


Fig. 11. Performance of SSR with  $N = 5$  for the upper bound, the MO-SDP with/without AN algorithm, the NuS algorithm, and the SLNR algorithm.

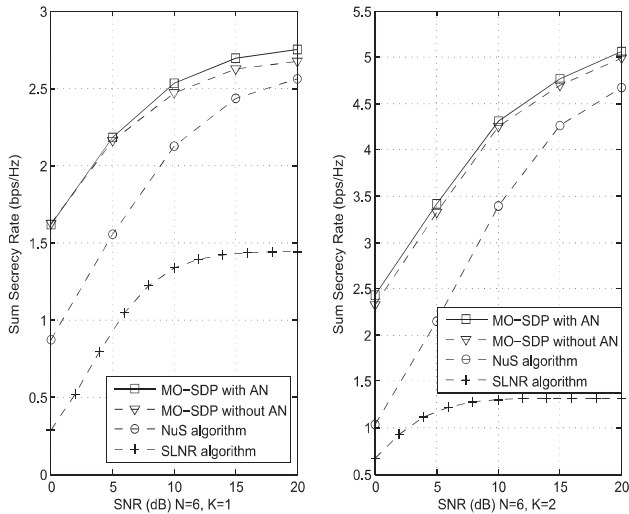


Fig. 12. Performance of SSR with  $N = 6$  for the upper bound, the MO-SDP with/without AN algorithm, the NuS algorithm, and the SLNR algorithm.

As can be seen from Fig. 10, using our proposed algorithms, both the MO-SDP algorithm with/without AN and the NuS algorithm exhibit better performance in terms of the SSRs than the SLNR precoding scheme. Besides, more pairs of L-UE and eavesdroppers lead to a higher SSR. Furthermore, with the introduction of AN, the performance of the SSR for the MO-SDP algorithm has been slightly improved compared with that of without AN, which implies that a very limited amount of power is allocated for the AN generation.

For the comparison between the MO-SDP algorithm and the upper-bound performance, the performance gap is very small, indicating the nearly global optimality for the proposed MO-SDP algorithm. Besides, the NuS algorithm exhibits worse performance than the MO-SDP algorithm in low SNR regime, and its performance gradually converges to that of the MO-SDP algorithm in high SNR regime, which is in line with our former analysis. Similar performance can also be observed in

Figs. 11 and 12. Moreover, by increasing the number of the relay antennas, the SSR can be further enhanced.

## VI. CONCLUSION

In this paper, we studied a relay-aided multiple-source multiple-destination network with the presence of multiple eavesdroppers. With the aim of maximizing the SSR, we first propose an MO-SDP algorithm, and simulation results demonstrate that it can nearly achieve the same performance as the optimal solution. Considering the high complexity incurred by the MO-SDP algorithm, we then propose a low-complexity algorithm that can nullify the received signals at the eavesdroppers. Finally, simulation results verify the effectiveness of the proposed algorithms.

## APPENDIX A

### PROOF OF LEMMA 3

The Lagrangian function of (34) is given by

$$\mathcal{L} = \sum_{i=1}^K \log\left(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{h_i}^2 \lambda_i^2 + \sigma_n^2}\right) + \alpha \left( \sum_{i=1}^K (\sigma_{g_i}^2 + \sigma_n^2 \lambda_1(\mathbf{J})) \lambda_i^2 - P_r \right) + \sum_{i=1}^K \beta_i \left( \gamma_i - \log\left(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{h_i}^2 \lambda_i^2 + \sigma_n^2}\right) \right) \quad (43)$$

where  $\alpha$  and  $\beta_i$  are the dual coefficients related to (34b) and (34c), respectively.

It can be easily verified that equality shall be held at the optimal solution, and the KKT conditions of (34) are given by

$$\sum_{i=1}^K (\sigma_{g_i}^2 + \sigma_n^2 \lambda_1(\mathbf{J})) \lambda_i^2 - P_r = 0 \quad (44)$$

$$\beta_i \left( \gamma_i - \log\left(1 + \frac{\lambda_i^2}{\sigma_n^2 \sigma_{h_i}^2 \lambda_i^2 + \sigma_n^2}\right) \right), i = 1, \dots, K \quad (45)$$

$$\alpha \geq 0 \quad (46)$$

$$\beta_i \geq 0 \quad (47)$$

$$\frac{\partial \mathcal{L}}{\partial \lambda_i} = 0, i = 1, \dots, K. \quad (48)$$

Let  $x_i = \lambda_i^2$ , and after several transformations (48) can be expressed as

$$a_i x_i^2 + b_i x_i + c = 0 \quad (49)$$

where  $a_i$ ,  $b_i$ , and  $c_i$  are given in (37)–(39), respectively.

Considering  $x_i \geq 0$ ,  $\lambda_i$  can be computed as the positive root of second-order equation shown in (36).

## REFERENCES

- [1] 3GPP TS 36.300, "Evolved universal terrestrial radio access (E-UTRA) and evolved universal terrestrial radio access network (E-UTRAN)," Mar. 2015.
- [2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
- [3] C. Jeong, I. Kim, and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

- [4] H. Wang, Q. Yin, and X. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.
- [5] H. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.
- [6] C. Wang, H. Wang, and X. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.
- [7] M. Zhang, R. Xue, H. Yu, H. Luo, and W. Chen, "Secrecy capacity optimization in coordinated multi-point processing," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2013, pp. 5845–5849.
- [8] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [9] P. Lin, S. Lai, S. Lin, and H. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.
- [10] M. Lin, J. Ge, Y. Yang, and Y. Ji, "Joint cooperative beamforming and artificial noise design for secrecy sum rate maximization in two-way AF relay networks," *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 380–383, Feb. 2014.
- [11] C. Wang, H. Wang, D. Ng, and X. Xie, "Joint beamforming and power allocation for secrecy in peer-to-peer relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.
- [12] Q. Li and W. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.
- [13] Q. Li, Y. Yang, W. K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.
- [14] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for simultaneous wireless information and power transfer in nonregenerative relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2462–2467, Jun. 2014.
- [15] M. Ding, H. Luo, and W. Chen, "Polyblock algorithm-based robust beamforming for downlink multi-user systems with per-antenna power constraints," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4560–4573, Aug. 2014.
- [16] Y. Zhang, L. Qian, and J. Huang, "Monotonic optimization in communication and networking systems," *Found. Trends Netw.*, vol. 7, no. 1, pp. 1–75, 2013.
- [17] R. A. Horn and C. A. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
- [18] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Rev.*, vol. 38, no. 1, pp. 49–95, 1996.
- [19] C. Helmberg, "Semidefinite programming for combinatorial optimization," Konrad-Zuse-Zentrum für Informationstechnik Berlin, Berlin, Germany, *ZIB-Rep.* 00–34, 2000.
- [20] Z. Luo, W. Ma, A. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Trans. Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
- [21] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [22] CVX Research, Inc, "CVX: Matlab software for disciplined convex programming, version 2.0 beta," Sep. 2012. [Online]. Available: <http://cvxr.com/cvx>
- [23] Z. Ding, K. Leung, D. Goeckel, and Don Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, Jun. 2011.
- [24] H. Wang, F. Liu, and X. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward MIMO relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1240–1250, Aug. 2014.
- [25] C. Jeong, I. Kim, and D. Kim, "Joint Secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 55, no. 4, pp. 310–325, Jan. 2012.
- [26] M. Sadek, A. Tarighat, and H. Sayed, "Active antenna selection in multiuser MIMO communications," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 1498–1510, Apr. 2007.
- [27] P. Zhao, M. Zhang, H. Yu, H. Luo, and W. Chen, "Robust beamforming design for sum secrecy rate optimization in MU-MISO networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1812–1823, Sep. 2015.

**Meng Zhang** received the B.S. and M.S. degrees in electronic engineering (EE) from Southwest Jiaotong University, Chengdu, China, in 2007 and 2010, respectively, and the Ph.D. degree in EE from Shanghai Jiao Tong University, Shanghai, China, in 2014.

He is a currently a Senior Researcher with Sharp Laboratories of China. His research interests include the wireless standardization, including the topics of short transmission time interval and new radio. He also works on deep-learning-related projects.

**Ming Ding** (M'12) received the B.S. and M.S. degrees with first-class honours in electronics engineering from Shanghai Jiao Tong University (SJTU), Shanghai, China, in 2004 and 2007, respectively, and the Ph.D. degree in electronic engineering from SJTU in 2011.

In April 2007, he joined Sharp Laboratories of China (SLC) as a Researcher. From September 2007 to September 2011, he was a Researcher/Senior Researcher at SLC. From December 2011, he was with SLC as a Senior Researcher/Principal Researcher until September 2014, when he joined National Information and Communications Technology Australia (NICTA). In September 2015, Commonwealth Scientific and Industrial Research Organization (CSIRO) and NICTA joined forces to create Data 61, where he continued his research in this new R&D center located in Australia. He is a Researcher with Data 61, Australia. He has also served as the Algorithm Design Director and the Programming Director for a system-level simulator of future telecommunication networks with SLC for more than 7 years. Up to now, he has published more than 30 papers in IEEE journals and conferences, all in recognized venues, and about 20 Third-Generation Partnership Project standardization contributions, as well as a Springer book *Multi-Point Cooperative Communication Systems: Theory and Applications* (Springer-Verlag, 2013). In addition, as the first inventor, he holds eight CN, two JP, and two KR patents and has filed another 30 patent applications on fourth-generation/fifth-generation (4G/5G) technologies. He has been working on beyond third-generation, 4G, and 5G wireless communication networks for more than 9 years, and his research interests include synchronization, multiple-input multiple-output technology, cooperative communications, heterogeneous networks, device-to-device communications, and modeling of wireless communication systems.

Dr. Ming is or has been a Guest Editor/Co-Chair/Technical Program Committee member of several IEEE top-tier journals/conferences, e.g., IEEE JOURNAL ON SELECTED AREAS ON COMMUNICATIONS, IEEE COMMUNICATIONS MAGAZINE, IEEE Globecom workshops. He received the Presidents Award from SLC in 2012 for his inventions and publications and served as one of the key members in the 4G/5G standardization team when it was awarded the Sharp Company Best Team: LTE Standardization Patent Portfolio, in 2014.

**Lin Gui** received the Ph.D. degree from Zhejiang University, Hangzhou, China, in 2002.

Since 2002, she has been an Associate Professor with the Institute of Wireless Communication Technology, Shanghai Jiao Tong University, Shanghai, China. Her research interests include the areas of high-definition television and wireless communications.

**Hanwen Luo** received the Bachelor degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 1971 and is currently a full Professor with the Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai, China, where he has held several positions, including the Vice Director of Shanghai Institute of Wireless Communications Technology and the Vice Director of Institute of Wireless Communication Technology. He used to be the leading specialist of China 863 high-tech program on beyond third-generation wireless communication systems and China 973 high-tech program on the research of military equipment. His research interests include mobile and personal communications.

**Mehdi Bennis** (SM'15) received the M.Sc. degree in electrical engineering jointly from the Ecole Polytechnique Federale de Lausanne, Switzerland, and the Eurecom Institute, Sophia Antipolis, France, in 2002 and the Ph.D. degree in electrical engineering from the University of Oulu, Oulu, Finland, in spectrum sharing for future mobile cellular systems in December 2009.

From 2002 to 2004, he was a Research Engineer with IMRA-EUROPE, investigating adaptive equalization algorithms for mobile digital TV. In 2004, he joined the Centre for Wireless Communications, University of Oulu, Finland, as a Research Scientist. In 2008, he was a Visiting Researcher with the Alcatel-Lucent chair on flexible radio, SUPELEC. He is currently managing the Broadband Evolved FEMTO (FP7-BeFEMTO) project with the University of Oulu. He has published more than 50 research papers in international conferences, journals, and book chapters. His main research interests include radio resource management, heterogeneous networks, game theory, and machine learning in the context of broadband wireless communications.