Secure Transmission via Joint Precoding Optimization for Downlink MISO NOMA

Nan Zhao, *Senior Member, IEEE,* Dongdong Li, Mingqian Liu, *Member, IEEE,* Yang Cao, Yunfei Chen, *Senior Member, IEEE,* Zhiguo Ding, *Senior Member, IEEE,* Xianbin Wang, *Fellow, IEEE,*

***Abstract*—Non-orthogonal multiple access (NOMA) is a prospective technology for radio resource constrained future mobile networks. However, NOMA users far from base station (BS) tend to be more susceptible to eavesdropping because they are allocated more transmit power. In this paper, we aim to jointly optimize the precoding vectors at BS to ensure the legitimate security in a downlink multiple-input single-output (MISO) NOMA network. When the eavesdropping channel state information (CSI) is available at BS, we can maximize the sum secrecy rate by joint precoding optimization. Owing to its non-convexity, the problem is converted into a convex one, which is solved by a second-order cone programming based iterative algorithm. When the CSI of the eavesdropping channel is not available, we first consider the case that the secure user is not the farthest from BS, and the transmit power of the farther users is maximized via joint precoding optimization to guarantee its security. Then, we consider the case when the farthest user from BS requires secure transmission, and the modified successive interference cancellation order and joint precoding optimization can be adopted to ensure its security. Similar method can be exploited to solve the two non-convex problems when the CSI is unknown. Simulation results demonstrate that the proposed schemes can improve the security performance for MISO NOMA systems effectively, with and without eavesdropping CSI.**

***Index Terms*—Joint precoding optimization, NOMA, secure transmission, successive interference cancellation.**

I. Introduction

Non-orthogonal multiple access (NOMA) is a prospective technology for the future resource-constrained mobile networks by offering high transmission rate, spectrum efficiency and user density [2], [3]. NOMA can be mainly classified into power-domain and code-domain [4]. In this paper, we focus on the power-domain NOMA [5], which does not require complex encoding or decoding schemes to achieve the desired requirements. In the power-domain NOMA, transmit power is allocated according to the channel strengths of users, i.e., the user with a weaker channel will be allocated with higher transmit power. Then, successive interference cancellation (SIC) is utilized at each receiver to extract the signals from the users with higher transmit power to recover its own.

Owing to the superior nature of NOMA [4], a lot of significant progresses have been made recently on its design and implementation, including capacity analysis [6], power allocation [7], fairness between users [8], user pairing [9], and performance analysis [10]. In addition, NOMA can also be integrated with other existing communication technologies to achieve better performance [11], e.g., multiple-input multiple-output (MIMO) [12], multiple-input single-output (MISO) [13], cooperative communications [14], cognitive radio [15], unmanned aerial vehicle (UAV) aided communications [16], [17], multiuser diversity [18], *etc*. In particular, for the MISO-NOMA networks, Hanif *et al.* did some fundamental work in [19] to maximize the downlink sum rate via joint precoding optimization with a minorization-maximization algorithm. However, these works did not consider the privacy among users and secure transmission.

The security vulnerability of wireless networks, especially the weakness from adversarial eavesdropping, always remains a challenge, due to the open nature of wireless medium [20], [21]. Different from the conventional encryption, physical layer security has been widely studied to enhance the security in recent years, through physical-layer adaptive transmission and physical link attributes based authentication [22]. Some initial information theoretic work on physical layer security was done by Wyner in [23], following which many recent works have been conducted to mitigate the eavesdropping by using different techniques, such as artificial noise (AN) or jamming [24]–[26], joint beamforming [27], relaying [28], [29], interference management [30], [31], *etc*. In addition, the security performance such as secrecy outage probability has also been analyzed in existing research works [32].

In NOMA networks, achieving secure transmission is also a great challenge due to the specific requirement on the transmission power among the paired NOMA users. To make the SIC of NOMA achievable, the users that are far from the BS should be allocated higher transmit power. This will dramatically

Manuscript received December 3, 2018; revised April 5, 2019 and May 27, 2019; accepted May 27, 2019. The work of N. Zhao was supported by the National Natural Science Foundation of China (NSFC) under Grant 61871065. The work of M. Liu was supported by China Scholarship Council under Grant No. 201806965031. The work of Z. Ding was supported by the UK EPSRC under grant number EP/L025272/2, NSFC under grant number 61728101 and H2020-MSCA-RISE-2015 under grant number 690750. Part of this work will be published in preliminary form in the Proceedings of IEEE PIMRC 2019 [1]. The associate editor coordinating the review of this paper and approving it for publication was K. Le. *(Corresponding author: Mingqian Liu.)*

N. Zhao, D. Li and Y. Cao are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China, and also with the School of Information Science and Technology, Qingdao University of Science and Technology, Qingdao, 266000, P. R. China. (email: zhaonan@dlut.edu.cn, DRldd@mail.dlut.edu.cn, cy216@mail.dlut.edu.cn).

M. Liu is with the State Key Laboratory of Integrated Service Networks, Xidian University, Shaanxi, Xi'an 710071, China (e-mail: mqliu@mail.xidian.edu.cn).

Y. Chen is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: Yunfei.Chen@warwick.ac.uk).

Z. Ding is with the School of Electrical and Electronic Engineering, The University of Manchester, Manchester, M13 9PL, U.K. (e-mail: zhiguo.ding@manchester.ac.uk).

X. Wang is with the Department of Electrical and Computer Engineering, University of Western Ontario, London, ON N6A 5B9, Canada (e-mail: xianbin.wang@uwo.ca).

increase the chance of being intercepted by the adversarial eavesdropper. In addition, SIC decodes the signals from all the far users, and the privacy between NOMA users may not be guaranteed. Thus, the weak-channel user with higher transmit power is more vulnerable to eavesdropping attack. To solve these problems, several works have been conducted. In [33], Ding *et al.* exploited beamforming and power allocation to improve the security performance for NOMA based multicast-unicast transmission. The optimal power allocation, SIC order and transmission rate were demonstrated by He *et al.* in [34] to guarantee the security for NOMA networks. In [35], Chen *et al.* analyzed the secrecy performance for cooperative NOMA networks. In [36], Xu *et al.* proposed a security-aware resource allocation scheme considering delay constraint in NOMA-based cognitive radio networks. Cao *et al.* proposed to protect the privacy of MISO-NOMA networks via beamforming optimization in [37]. AN can also be utilized to guarantee the security performance for NOMA systems. In [38], Lv *et al.* proposed a secrecy beamforming scheme to exploit AN to achieve secure NOMA transmission. Zhou *et al.* adopted AN in [39] to perform secure simultaneous wireless information and power transfer for MISO-NOMA networks. In [40], Zhao *et al.* jointly optimized beamforming and jamming to disrupt the eavesdropping for MISO-NOMA networks.

Different from the above-mentioned research, we aim to guarantee the secure transmission for downlink MISO-NOMA networks via joint precoding optimization in this paper. By changing the signal strength of some specific users, the eavesdropping can be effectively disrupted, in both cases with and without the eavesdropping channel state information (CSI) at BS. The SIC order is also different from that of the conventional NOMA scheme when the farthest user from BS requires secure transmission without eavesdropping CSI. The key contributions of this paper are summarized as follows.

- To achieve SIC in NOMA, the users with weaker channel gains are allocated higher transmit power, which increases the risk of adversarial eavesdropping. In addressing this issue, we propose to leverage joint precoding optimization to guarantee the secure transmission for downlink MISO-NOMA networks, in the cases with or without eavesdropping CSI, respectively.
- For the case when the eavesdropping CSI is available at BS, the precoding vectors are jointly optimized to maximize the sum secrecy rate. Since the optimization is non-convex, we transform it into a convex one via the second-order cone (SOC) programming. Thus, the suboptimal solution to the original problem can be effectively calculated by solving this convex-problem iteratively.
- When the eavesdropping CSI is unavailable, we first consider that the secure user is not the farthest one from BS. We can maximize the transmit power of the farther users via joint precoding optimization to guarantee its own security. When the farthest user from BS requires secure transmission, the modified SIC order and joint precoding optimization can be leveraged to ensure its security. Similar method to the scheme with CSI can be adopted to solve these two non-convex problems.

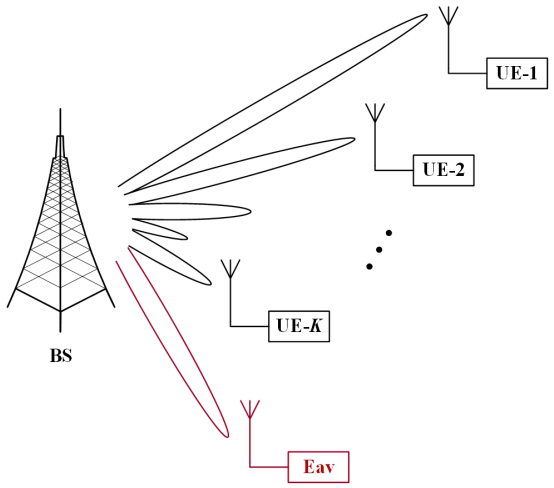


Fig. 1. A downlink MISO-NOMA network with a potential eavesdropper.

The rest of this paper is organized as follows. In Section II, the considered system model in this paper is presented. The secure transmission scheme for MISO-NOMA networks with eavesdropping CSI is proposed in Section III. In Section IV, the secure transmission schemes without eavesdropping CSI are proposed when the secure user is or is not the farthest one from BS, respectively. In Section V, simulation results are presented to show the effectiveness of the schemes. Finally, the conclusion is drawn in Section VI.

Notation: $\mathbf{I}$ denotes the identity matrix. $\mathbf{0}$ represents the zero matrix. $\mathbf{A}^{\dagger}$ is the Hermitian transpose of matrix $\mathbf{A}$. $\|\mathbf{a}\|$ is the Euclidean norm of vector $\mathbf{a}$. $\mathcal{CN}(\mathbf{a},\mathbf{A})$ is the complex Gaussian distribution with mean $\mathbf{a}$ and covariance matrix $\mathbf{A}$. $\mathfrak{Re}(\cdot)$ defines the real operator.

II. System Model

Consider a system where a M-antenna BS transmits information to K single-antenna users via NOMA as shown in Fig. 1. There is a single-antenna eavesdropper aiming at intercepting the legitimate information. We define UE-i as the ith user, $i \in \mathcal{K} \triangleq \{1, 2, \cdots, K\}$. The received signal at UE-i can be expressed as

$$\widehat{y_i} = \mathbf{h}_i \sum_{j=1}^{K} \mathbf{w}_j x_j + n_i,\ i \in \mathcal{K}, \tag{1}$$

where $\mathbf{w}_j \in \mathbb{C}^{M\times 1}$ is defined as the precoding vector for UE-j, x_j is the transmitted information for UE-j with $\mathbb{E}\{\|x_j\|^2\} = 1$, and $n_i \sim \mathcal{CN}\left(0, \sigma^2\right)$ is the additive white Gaussian noise. The MISO channel vector from the BS to UE-i can be written as

$$\mathbf{h}_i = \sqrt{\beta d_i^{-\alpha}}\mathbf{g}_i \in \mathbb{C}^{1\times M},\ i \in \mathcal{K}, \tag{2}$$

which is subject to block Rayleigh fading. d_i is the distance between the BS and UE-i. α is the path-loss exponent and β is the channel gain at the unit distance. $\mathbf{g}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ represents the normalized Rayleigh fading vector.

Assume that UE-1 is the farthest user from the BS with the weakest channel, and it can decode its own information by treating the interference from other users as noise. UE-K is

the nearest user with the strongest channel. It can remove the signals of all the other users according to SIC, to recover its own information. Other users are arranged according to their distances from the BS. According to the above requirements, the following conditions should be satisfied for the conventional NOMA as

$$|\mathbf{h}_i\mathbf{w}_1|^2 \geq |\mathbf{h}_i\mathbf{w}_2|^2 \geq \cdots |\mathbf{h}_i\mathbf{w}_{K-1}|^2 \geq |\mathbf{h}_i\mathbf{w}_K|^2, \forall i \in \mathcal{K}. \quad (3)$$

According to (3), we define $R_t^{[i]}$ as the transmission rate of UE-i, which can be expressed as

$$R_t^{[i]} = \log_2\left(1 + \frac{|\mathbf{h}_i\mathbf{w}_i|^2}{\sum\limits_{j=i+1}^{K}|\mathbf{h}_i\mathbf{w}_j|^2 + \sigma^2}\right), i = 1, \cdots, K-1. \quad (4)$$

When $i = K$, its transmission rate is

$$R_t^{[K]} = \log_2\left(1 + |\mathbf{h}_K\mathbf{w}_K|^2/\sigma^2\right). \quad (5)$$

Furthermore, the achievable rate at UE-k to decode the signal for UE-i, $i < k$, can be expressed as

$$R_k^i = \log_2\left(1 + \frac{|\mathbf{h}_k\mathbf{w}_i|^2}{\sum\limits_{j=i+1}^{K}|\mathbf{h}_k\mathbf{w}_j|^2 + \sigma^2}\right), i = 1, \cdots, K-1. \quad (6)$$

To make NOMA feasible, we should guarantee that the signal-to-interference-plus-noise ratio (SINR) at UE-k to decode the signal of UE-i should be no less than the SINR at UE-i to decode its own signal, and we have

$$\min\left\{R_{i+1}^i, R_{i+2}^i, \ldots, R_K^i\right\} \geq R_t^{[i]}, \forall i = 1, \cdots, K-1. \quad (7)$$

In conventional MISO-NOMA networks, the sum rate of users should be maximized as

$$\begin{aligned} \max_{\mathbf{w}_i} \ & \sum_{i\in K} R_t^{[i]} \\ s.t. \ & |\mathbf{h}_i\mathbf{w}_1|^2 \geq |\mathbf{h}_i\mathbf{w}_2|^2 \geq \cdots |\mathbf{h}_i\mathbf{w}_K|^2, \ i \in \mathcal{K}, \\ & \sum_{i=1}^{K}\|\mathbf{w}_i\|^2 \leq P_s, \\ & \min\left\{R_{i+1}^i, \ldots, R_K^i\right\} \geq R_t^{[i]} \geq r_t, i = 1, \cdots, K-1, \\ & R_t^{[K]} \geq r_t, \end{aligned} \quad (8)$$

where P_s is the limitation of BS transmit power and r_t is the rate requirement for each user.

However, the security of users, especially the farther users with higher transmit power, will be threatened by eavesdropping. The eavesdropping rate towards UE-i can be written as

$$R_e^{[i]} = \log_2\left(1 + \frac{|\mathbf{h}_e\mathbf{w}_i|^2}{\sum\limits_{j=1,j\neq i}^{K}|\mathbf{h}_e\mathbf{w}_j|^2 + \sigma^2}\right), \ i \in \mathcal{K}, \quad (9)$$

where $\mathbf{h}_e$ is the MISO channel vector from the BS to eavesdropper. Thus, the secrecy rate of UE-i can be expressed as

$$R_s^{[i]} = \left[R_t^{[i]} - R_e^{[i]}\right]^+, \ i \in \mathcal{K}. \quad (10)$$

where $[\cdot]^+$ means that when $R_t^{[i]} < R_e^{[i]}$, $R_s^{[i]}$ equals zero.

Therefore, joint precoding optimization will be leveraged to develop three schemes based on different scenarios, with or without eavesdropping CSI.

III. Secure Transmission Scheme with Eavesdropping CSI

In this section, we assume that the eavesdropping CSI is available at the BS[1], and propose Scheme I in order to maximize the sum secrecy rate via joint precoding optimization when all the users require secure transmission. When only some of the users require secure transmission, the corresponding problem can be solved similarly.

A. Problem Formulation of *Scheme I*

The joint precoding optimization problem of Scheme I can be formulated as

$$\begin{aligned} \max_{\mathbf{w}_i} \ & \sum_{i\in K} R_s^{[i]} \\ s.t. \ & |\mathbf{h}_i\mathbf{w}_1|^2 \geq |\mathbf{h}_i\mathbf{w}_2|^2 \geq \cdots |\mathbf{h}_i\mathbf{w}_K|^2, \ i \in \mathcal{K}, \\ & \sum_{i=1}^{K}\|\mathbf{w}_i\|^2 \leq P_s, \\ & \min\left\{R_{i+1}^i, \ldots, R_K^i\right\} \geq R_t^{[i]} \geq r_t, i = 1, \cdots, K-1, \\ & R_t^{[K]} \geq r_t, \end{aligned} \quad (11)$$

in which the sum secrecy rate can be maximized. Notice that the objective function and most of the constraints are non-convex in (11), which will be approximately transformed into a convex one in the next subsection.

B. Approximate Transformations

To calculate the solutions to the non-convex problem in (11) effectively, we should transform it using necessary approximations. First, we have

$$|\mathbf{h}_i\mathbf{w}_j|^2 = \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger. \quad (12)$$

This gives the sum secrecy rate as (13) at the top of the next page. Thus, (11) can be transformed into

$$\begin{aligned} \max_{\mathbf{w}_i} \ & \sum_{i=1}^{K-1}\log_2\left(\frac{\sum_{j=i}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2}{\sum_{j=i+1}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2}\right) \\ & + \log_2\left(\frac{\mathbf{h}_K\mathbf{w}_K\mathbf{w}_K^\dagger\mathbf{h}_K^\dagger + \sigma^2}{\sigma^2}\right) \\ & - \sum_{i=1}^{K}\log_2\left(\frac{\sum_{j=1}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger + \sigma^2}{\sum_{j=1,j\neq i}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger + \sigma^2}\right) \\ s.t. \ & |\mathbf{h}_i\mathbf{w}_1|^2 \geq |\mathbf{h}_i\mathbf{w}_2|^2 \geq \cdots |\mathbf{h}_i\mathbf{w}_K|^2, \ i \in \mathcal{K}, \\ & \sum_{i=1}^{K}\|\mathbf{w}_i\|^2 \leq P_s, \\ & \min\left\{R_{i+1}^i, \ldots, R_K^i\right\} \geq R_t^{[i]} \geq r_t, i = 1, \cdots, K-1, \\ & R_t^{[K]} \geq r_t. \end{aligned} \quad (14)$$

[1]In this scenario, the eavesdropper can act as a registered user of the network, without the authorization to access the confidential information of other legitimate users. In addition, the eavesdropper cannot obtain enough information to perform SIC towards the legitimate users.

$$\sum_{i=1}^{K} R_s^{[i]} = \sum_{i=1}^{K-1}\left[\log_2\left(1+\frac{|\mathbf{h}_i\mathbf{w}_i|^2}{\sum_{j=i+1}^{K}|\mathbf{h}_i\mathbf{w}_j|^2+\sigma^2}\right)-\log_2\left(1+\frac{|\mathbf{h}_e\mathbf{w}_i|^2}{\sum_{j=1,j\neq i}^{K}|\mathbf{h}_e\mathbf{v}_j|^2+\sigma^2}\right)\right]+\left[\log_2\left(1+\frac{|\mathbf{h}_K\mathbf{w}_K|^2}{\sigma^2}\right)-\log_2\left(1+\frac{|\mathbf{h}_e\mathbf{w}_K|^2}{\sum_{j=1}^{K-1}|\mathbf{h}_e\mathbf{w}_j|^2+\sigma^2}\right)\right]$$
$$= \sum_{i=1}^{K-1}\left[\log_2\left(\frac{\sum_{j=i}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2}{\sum_{j=i+1}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2}\right)-\log_2\left(\frac{\sum_{j=1}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2}{\sum_{j=1,j\neq i}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2}\right)\right] + \left[\log_2\left(\frac{\mathbf{h}_K\mathbf{w}_K\mathbf{w}_K^\dagger\mathbf{h}_K^\dagger+\sigma^2}{\sigma^2}\right)-\log_2\left(\frac{\sum_{j=1}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2}{\sum_{j=1}^{K-1}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2}\right)\right]. \tag{13}$$

Using auxiliary variables a_i, b_i, z_K, c_i and d_i, we can derive the upper and lower bounds for (14) as

$$\sum_{j=i}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2\geq e^{a_i}, i=1,2,\cdots,K-1, \tag{15}$$

$$\sum_{j=i+1}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2\leq e^{b_i}, i=1,2,\cdots,K-1, \tag{16}$$

$$\mathbf{h}_K\mathbf{w}_K\mathbf{w}_K^\dagger\mathbf{h}_K^\dagger+\sigma^2\geq e^{z_K}, \tag{17}$$

$$\sum_{j=1}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2\leq e^{c_i}, i\in\mathcal{K}, \tag{18}$$

$$\sum_{j=1,j\neq i}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2\geq e^{d_i}, i\in\mathcal{K}. \tag{19}$$

According to (15)-(19), we have

$$\begin{aligned}&\sum_{i=1}^{K}R_s^{[i]}\\ &\geq\log_2\prod_{i=1}^{K-1}e^{a_i}-\log_2\prod_{i=1}^{K-1}e^{b_i}+\log_2 e^{z_K}-\log_2\sigma^2\\ &\quad-\log_2\prod_{i=1}^{K}e^{c_i}+\log_2\prod_{i=1}^{K}e^{d_i}\\ &=\log_2 e^{\sum_{i=1}^{K-1}(a_i-b_i)+\sum_{i=1}^{K}(d_i-c_i)+z_K}-2\cdot\log_2\sigma\\ &=\left[\sum_{i=1}^{K-1}(a_i-b_i)+\sum_{i=1}^{K}(d_i-c_i)+z_K\right]\cdot\log_2 e-2\cdot\log_2\sigma.\end{aligned} \tag{20}$$

Subsequently, (14) can be transformed as

$$\begin{aligned}\max_{a_i,b_i,z_K,c_i,d_i,\mathbf{w}_i}\ &\sum_{i=1}^{K-1}(a_i-b_i)+\sum_{i=1}^{K}(d_i-c_i)+z_K\\ s.t.\ &\sum_{j=i}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2\geq e^{a_i}, i=1,\cdots,K-1,\\ &\sum_{j=i+1}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2\leq e^{b_i}, i=1,\cdots,K-1,\\ &\sum_{j=1}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2\leq e^{c_i},\ i\in\mathcal{K},\\ &\sum_{j=1,j\neq i}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2\geq e^{d_i},\ i\in\mathcal{K},\\ &\mathbf{h}_K\mathbf{w}_K\mathbf{w}_K^\dagger\mathbf{h}_K^\dagger+\sigma^2\geq e^{z_K},\\ &\sum_{i=1}^{K}\|\mathbf{w}_i\|^2\leq P_s,\\ &|\mathbf{h}_i\mathbf{w}_1|^2\geq|\mathbf{h}_i\mathbf{w}_2|^2\geq\cdots|\mathbf{h}_i\mathbf{w}_K|^2, i\in\mathcal{K},\\ &\min\left\{R_{i+1}^i,\ldots,R_K^i\right\}\geq R_t^{[i]}\geq r_t, i=1,\cdots,K-1,\\ &R_t^{[K]}\geq r_t.\end{aligned} \tag{21}$$

Although the objective function in (21) $\sum_{i=1}^{K-1}(a_i-b_i)+\sum_{i=1}^{K}(d_i-c_i)+z_K$ is convex, some constraints are still non-convex. Based on the Taylor's expansion, the first-order expansion at $\bar{b}_i$ and $\bar{c}_i$ can be given by $T_1=e^{\bar{b}_i}(b_i-\bar{b}_i+1)$ and $T_2=e^{\bar{c}_i}(c_i-\bar{c}_i+1)$, respectively. Thus, (16) and (18) can be changed into

$$\sum_{j=i+1}^{K}\mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2\leq e^{\bar{b}_i}(b_i-\bar{b}_i+1), i=1,\cdots,K-1, \tag{22}$$

$$\sum_{j=1}^{K}\mathbf{h}_e\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_e^\dagger+\sigma^2\leq e^{\bar{c}_i}(c_i-\bar{c}_i+1), i=1,\cdots,K. \tag{23}$$

Based on the SOC constraint, we have

$$\xi^2\leq\mu\nu\ (\mu\geq0,\nu\geq0)\Longrightarrow\|[2\xi,\mu-\nu]^\dagger\|\leq\mu+\nu. \tag{24}$$

Thus, (22) and (23) can be rewritten as

$$\left\|[2\mathbf{h}_i\mathbf{w}_{i+1},\cdots,2\mathbf{h}_i\mathbf{w}_K,2\sigma,T_1-1]^\dagger\right\|\leq T_1+1, i=1,\cdots,K-1, \tag{25}$$

$$\left\|[2\mathbf{h}_e\mathbf{w}_1,\cdots,2\mathbf{h}_e\mathbf{w}_K,2\sigma,T_2-1]^\dagger\right\|\leq T_2+1, i\in\mathcal{K}. \tag{26}$$

In addition, the left sides of (15), (17) and (19) are quadratic functions. We define

$$\mathcal{F}_{ij}(\mathbf{w}_j)=|\mathbf{h}_i\mathbf{w}_j|^2. \tag{27}$$

Then, the first order Taylor's approximation (27) can be expressed as

$$\mathcal{T}_{ij}(\mathbf{w}_j,\overline{\mathbf{w}}_j)=2\mathfrak{Re}\left(\overline{\mathbf{w}}_j^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{w}_j\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_j^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\overline{\mathbf{w}}_j\right). \quad (28)$$

Using this method, the inequalities (15), (17) and (19) can be transformed as (29) at the top of the next page.

For the decoding order of users, it equals

$$\mathcal{C}_i=\begin{cases}|\mathbf{h}_i\mathbf{w}_K|^2\le\min\left\{|\mathbf{h}_i\mathbf{w}_{K-1}|^2,\ldots,|\mathbf{h}_i\mathbf{w}_1|^2\right\},\\ |\mathbf{h}_i\mathbf{w}_{K-1}|^2\le\min\left\{|\mathbf{h}_i\mathbf{w}_{K-2}|^2,\ldots,|\mathbf{h}_i\mathbf{w}_1|^2\right\},\\ \ldots,\\ |\mathbf{h}_i\mathbf{w}_2|^2\le|\mathbf{h}_i\mathbf{w}_1|^2.\end{cases} \quad (30)$$

The right sides of these inequalities in (30) are quadratic functions of variables $\mathbf{w}_i$. Thus, we can also use the same method to linearize them. Using (27) and (28), the order constraint (30) can be transformed as

$$\widetilde{\mathcal{C}}_i=\begin{cases}|\mathbf{h}_i\mathbf{w}_K|^2\le\min_{j\in[1,K-1]}\mathcal{T}_{ij}\left(\mathbf{w}_j,\overline{\mathbf{w}}_j\right),\\ |\mathbf{h}_i\mathbf{w}_{K-1}|^2\le\min_{j\in[1,K-2]}\mathcal{T}_{ij}\left(\mathbf{w}_j,\overline{\mathbf{w}}_j\right),\\ \ldots,\\ |\mathbf{h}_i\mathbf{w}_2|^2\le\mathcal{T}_{11}\left(\mathbf{w}_1,\overline{\mathbf{w}}_1\right).\end{cases} \quad (31)$$

In order to guarantee the quality of transmission and make all the rates in (6) achievable, we also need to constrain and transform the transmission rate of legitimate users and the condition of (7) according to the following proposition.

Proposition 1: $R_t^{[i]}\ge r_t$ and (7) can be transformed as

$$s_i\ge 2^{r_t},\ i\in\mathcal{K},\quad (56),\quad (57). \quad (32a)$$

$$\mathcal{O}_i, i=1,\cdots,K-1,\quad (63). \quad (32b)$$

Proof: Refer to Appendix A. ∎

Therefore, according to the above derivation, the original problem can be transformed into a convex one in (33) at the top of the next page, which can be solved using existing toolboxes such as CVX.

C. Iterative Algorithm

With all above transformations, (11) can be solved via Algorithm 1.

Algorithm 1 Iterative Algorithm for (11)

1: Set the maximum number of iterations T and randomly generate $(\overline{\mathbf{w}}_i,\overline{a}_i,\overline{b}_i,\overline{z}_K,\overline{c}_i,\overline{d}_i)$ for (33).
2: **Repeat**
3: Using CVX to calculate the solutions to (33) as $(\mathbf{w}_i^*,a_i^*,b_i^*,z_K^*,c_i^*,d_i^*)$.
4: Update $(\overline{\mathbf{w}}_i,\overline{a}_i,\overline{b}_i,\overline{z}_K,\overline{c}_i,\overline{d}_i)=(\mathbf{w}_i^*,a_i^*,b_i^*,z_K^*,c_i^*,d_i^*)$
5: $t=t+1$.
6: **Until** $t=T$.
7: Output $\mathbf{w}_i^*, i\in\mathcal{K}$.

Remark: In each iteration, the value of the sum secrecy rate will be no less than the value in the previous iteration, which indicates that the secrecy rate will monotonically increase or non-decrease as iterations proceed. Furthermore, due to the transmit power constraint at BS, there also exists an upper bound of sum rate. Therefore, we conclude that Algorithm 1 is guaranteed to be convergent.

D. Computational Complexity Analysis

We solve an SOC program in every iteration of Algorithm 1 for Scheme I, and utilize the computational complexity of the SOCP in (33) to estimate the computational complexity [41]. The total number of constraints in the formulations of (33) is $1.5K^2+4.5K$. The iteration number needed to reduce the duality gap to a small constant, which is upper bounded by $\mathcal{O}(\sqrt{1.5K^2+4.5K})$. Then, we calculate the upper bound $8K^2+(M+1)K-1$ in order to represent the sum dimensions of all SOCs in (33). The amount of work per iteration is $\mathcal{O}((0.5K^2+5.5K-1)^2(8K^2+MK+K-1))$ by the interior-point method. Therefore, the worst-case complexity of the SOCP in (33) can be estimated as $\mathcal{O}((0.5K^2+5.5K-1)^2(8K^2+MK+K-1)(\sqrt{1.5K^2+4.5K}))$.

IV. Secure Transmission Scheme without Eavesdropping CSI

The secrecy rate of some specific users in the network will be guaranteed by the modified SIC order and joint precoding optimization in this section, when the eavesdropping CSI is not available at the BS.

A. *Scheme II: UE-k is the Secure User, $2\le k\le K$*

We first consider that the secure user is not the farthest one from BS, i.e., UE-k aims to perform secure transmission, where $2\le k\le K$. To improve the security of UE-k, we can maximize the transmit power of the users whose distance from BS is larger than that of UE-k. Thus, the confidential information can be hidden in the larger signals of these users, and its security can be enhanced. The optimization problem can be presented as

$$\begin{aligned}\max_{\mathbf{w}_i}\ &\sum_{i=1}^{k-1}|\mathbf{w}_i|^2\\ s.t.\ &|\mathbf{h}_i\mathbf{w}_1|^2\ge|\mathbf{h}_i\mathbf{w}_2|^2\ge\cdots|\mathbf{h}_i\mathbf{w}_K|^2, i\in\mathcal{K},\\ &\sum_{i=1}^{K}\|\mathbf{w}_i\|^2\le P_s,\\ &\min\left\{R_{i+1}^i,\ldots,R_K^i\right\}\ge R_t^{[i]}\ge r_t, i=1,\cdots,K-1,\\ &R_t^{[K]}\ge r_t.\end{aligned} \quad (34)$$

In this case, the eavesdropping rate towards UE-k can be given by

$$R_e^{[k]}=\log_2\left(1+\frac{|\mathbf{h}_e\mathbf{w}_k|^2}{\sum\limits_{i=1}^{k-1}|\mathbf{h}_e\mathbf{w}_i|^2+\sum\limits_{j=k+1}^{K}|\mathbf{h}_e\mathbf{w}_j|^2+\sigma^2}\right). \quad (35)$$

We can observe that the denominator of (35) includes $\sum_{i=1}^{k-1}|\mathbf{h}_e\mathbf{w}_i|^2$, which is maximized by (34) to disrupt the eavesdropping toward UE-k. Thus, the secure transmission of UE-k can be guaranteed.

Duo to the non-convexity of (34), we should change it into a convex one based on the SOC and some transformations. Specifically, the transformation of SIC order is the same as the inequalities in (30) and (31). The transformation of the

$$2\mathfrak{Re}\left(\overline{\mathbf{w}}_i^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{w}_i\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_i^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\overline{\mathbf{w}}_i\right)+2\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{w}_K\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\overline{\mathbf{w}}_K\right)+\sigma^2\geq e^{a_i}, i=1,2,\cdots,K-1, \tag{29a}$$

$$2\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_K^{\dagger}\mathbf{h}_K\mathbf{w}_K\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_K^{\dagger}\mathbf{h}_K\overline{\mathbf{w}}_K\right)+\sigma^2\geq e^{z_K} \tag{29b}$$

$$\begin{aligned}&2\mathfrak{Re}\left(\overline{\mathbf{w}}_1^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_1\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_1^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_1\right)+\cdots+2\mathfrak{Re}\left(\overline{\mathbf{w}}_{i-1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_{i-1}\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_{i-1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_{i-1}\right)+2\mathfrak{Re}\left(\overline{\mathbf{w}}_{i+1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_{i+1}\right)\\&-\mathfrak{Re}\left(\overline{\mathbf{w}}_{i+1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_{i+1}\right)+\cdots+2\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_K\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_K\right)+\sigma^2\geq e^{d_i}, i=1,2,\cdots,K.\end{aligned} \tag{29c}$$

$$\max_{\substack{a_i,b_i,z_K,c_i,d_i\\ \mathbf{w}_i,s_i}}\ \sum_{i=1}^{K-1}(a_i-b_i)+\sum_{i=1}^{K}(d_i-c_i)+z_K \tag{33a}$$

$$s.t.\ \ T_1=e^{\overline{b}_i}(b_i-\overline{b}_i+1),\quad \left\|[2\mathbf{h}_i\mathbf{w}_{i+1},2\mathbf{h}_i\mathbf{w}_{i+2},\cdots,2\mathbf{h}_i\mathbf{w}_K,2\sigma,T_1-1]^{\dagger}\right\|\leq T_1+1, i=1,2,\cdots,K-1, \tag{33b}$$

$$T_2=e^{\overline{c}_i}(c_i-\overline{c}_i+1),\quad \left\|[2\mathbf{h}_e\mathbf{w}_1,2\mathbf{h}_e\mathbf{w}_2,\cdots,2\mathbf{h}_e\mathbf{w}_K,2\sigma,T_2-1]^{\dagger}\right\|\leq T_2+1,\ i\in\mathcal{K}, \tag{33c}$$

$$\begin{aligned}&2\mathfrak{Re}\left(\overline{\mathbf{w}}_i^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{w}_i\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_i^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\overline{\mathbf{w}}_i\right)+2\mathfrak{Re}\left(\overline{\mathbf{w}}_{i+1}^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{w}_{i+1}\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_{i+1}^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\overline{\mathbf{w}}_{i+1}\right)+\cdots\\&+2\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{w}_K\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\overline{\mathbf{w}}_K\right)+\sigma^2\geq e^{a_i}, i=1,2,\cdots,K-1,\end{aligned} \tag{33d}$$

$$2\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_K^{\dagger}\mathbf{h}_K\mathbf{w}_K\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_K^{\dagger}\mathbf{h}_K\overline{\mathbf{w}}_K\right)+\sigma^2\geq e^{z_K}, \tag{33e}$$

$$\begin{aligned}&2\mathfrak{Re}\left(\overline{\mathbf{w}}_1^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_1\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_1^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_1\right)+2\mathfrak{Re}\left(\overline{\mathbf{w}}_2^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_2\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_2^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_2\right)+\cdots\\&2\mathfrak{Re}\left(\overline{\mathbf{w}}_{i-1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_{i-1}\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_{i-1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_{i-1}\right)+2\mathfrak{Re}\left(\overline{\mathbf{w}}_{i+1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_{i+1}\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_{i+1}^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_{i+1}\right)+\cdots\\&+2\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\mathbf{w}_K\right)-\mathfrak{Re}\left(\overline{\mathbf{w}}_K^{\dagger}\mathbf{h}_e^{\dagger}\mathbf{h}_e\overline{\mathbf{w}}_K\right)+\sigma^2\geq e^{d_i},\ i\in\mathcal{K},\end{aligned} \tag{33f}$$

$$\|[\mathbf{w}_1,\mathbf{w}_2,\cdots,\mathbf{w}_K]^{\dagger}\|\leq\sqrt{P_s}, \tag{33g}$$

$$\widetilde{\mathcal{C}}_i,\ i\in\mathcal{K}, \tag{33h}$$

$$s_i\geq 2^{r_t},\ i\in\mathcal{K},\ \ (56)\ ,\ (57)\ ,\ \mathcal{O}_i,\ i=1,\cdots,K-1,\ \ (63). \tag{33i}$$

---

lower limitation of transmission rate in (34) is the same as that in Proposition 1. Thus, we can convert (34) into a convex one as

$$\begin{aligned}\max_{\mathbf{w}_i}\ &\sum_{i=1}^{k-1}|\mathbf{w}_i|^2\\ s.t.\ &\sum_{i=1}^{K}\|\mathbf{w}_i\|^2\leq P_s,\\ &\widetilde{\mathcal{C}}_i,\ i\in\mathcal{K},\\ &s_i\geq 2^{r_t},\ i\in\mathcal{K},\ \ (56),\ \ (57),\\ &\mathcal{O}_i,\ i=1,\cdots,K-1,\ \ (63),\end{aligned} \tag{36}$$

which can be easily solved by existing toolboxes such as CVX. Therefore, the solution to (34) can be calculated by solving (36) iteratively, according to Algorithm 1.

*B. **Scheme III:** UE-1 is the Secure User*

In this subsection, we consider the scenario when the farthest user UE-1 from the BS requires secure transmission. In this case, the transmit power allocated to UE-1 will be highest according to conventional NOMA, and it will be severely threatened by eavesdropping. To guarantee the secure transmission of UE-1, its signal should be hidden in the signals of other users by maximizing the transmit power of UE-2, with the SIC order at each receiver modified as

$$|\mathbf{h}_i\mathbf{w}_2|^2\geq|\mathbf{h}_i\mathbf{w}_1|^2\geq|\mathbf{h}_i\mathbf{w}_3|^2\cdots\geq|\mathbf{h}_i\mathbf{w}_K|^2,\ \forall i\in\mathcal{K}. \tag{37}$$

For UE-2, it decodes its own information directly , and its SINR is expressed as

$$\mathrm{SINR}_2^2=\frac{|\mathbf{h}_2\mathbf{w}_2|^2}{\sum\limits_{j=1,j\neq 2}^{K}|\mathbf{h}_2\mathbf{w}_j|^2+\sigma^2}. \tag{38}$$

For UE-1, it first removes the signal for UE-2 and then decodes its own signal with SINR denoted as

$$\mathrm{SINR}_1^1=\frac{|\mathbf{h}_1\mathbf{w}_1|^2}{\sum\limits_{j=3}^{K}|\mathbf{h}_1\mathbf{w}_j|^2+\sigma^2}. \tag{39}$$

For UE-i, $3\leq i\leq K$, it extracts the signals of farther users from the BS, and then decodes its own signal with the SINR expressed as

$$\mathrm{SINR}_i^i=\frac{|\mathbf{h}_i\mathbf{w}_i|^2}{\sum\limits_{j=i+1}^{K}|\mathbf{h}_i\mathbf{w}_j|^2+\sigma^2},\ i=3,4,\cdots,K-1, \tag{40}$$

$$\text{SINR}_K^K = \frac{|\mathbf{h}_K\mathbf{w}_K|^2}{\sigma^2}. \tag{41}$$

Thus, the optimization problem to guarantee the security of the farthest UE-1 can be written as

$$\begin{aligned}
&\max_{\mathbf{w}_i} \ |\mathbf{w}_2|^2 \\
&s.t. \ |\mathbf{h}_i\mathbf{w}_2|^2 \geq |\mathbf{h}_i\mathbf{w}_1|^2 \geq |\mathbf{h}_i\mathbf{w}_3|^2 \cdots \geq |\mathbf{h}_i\mathbf{w}_K|^2, i \in \mathcal{K}, \\
&\quad \sum_{i=1}^{K} \|\mathbf{w}_i\|^2 \leq P_s, \\
&\quad \min\left\{R_1^2, R_3^2, \ldots, R_K^2\right\} \geq R_t^{[2]} \geq r_t, \\
&\quad \min\left\{R_3^1, R_4^1, \ldots, R_K^1\right\} \geq R_t^{[1]} \geq r_t, \\
&\quad \min\left\{R_{i+1}^i, \ldots, R_K^i\right\} \geq R_t^{[i]} \geq r_t, i = 3, \cdots, K-1, \\
&\quad R_t^{[K]} \geq r_t.
\end{aligned} \tag{42}$$

In Scheme III, the eavesdropping rate towards UE-1 can be expressed as

$$R_e^{[1]} = \log_2\left(1 + \frac{|\mathbf{h}_e\mathbf{w}_1|^2}{|\mathbf{h}_e\mathbf{w}_2|^2 + \sum_{i=3}^{K}|\mathbf{h}_e\mathbf{w}_i|^2 + \sigma^2}\right). \tag{43}$$

We can observe that the denominator of (43) includes $|\mathbf{h}_e\mathbf{w}_2|^2$, which is maximized by (42) to disrupt the eavesdropping toward UE-1. Thus, the secure transmission of UE-1 can be guaranteed.

Owing to the non-convexity of (42), we should approximately transform it into a convex one. The modified SIC order for users is

$$\mathcal{Q}_i = \begin{cases} |\mathbf{h}_i\mathbf{w}_K|^2 \leq \min\left\{|\mathbf{h}_i\mathbf{w}_{K-1}|^2, \ldots, |\mathbf{h}_i\mathbf{w}_1|^2, |\mathbf{h}_i\mathbf{w}_2|^2\right\}, \\ |\mathbf{h}_i\mathbf{w}_{K-1}|^2 \leq \min\left\{|\mathbf{h}_i\mathbf{w}_{K-2}|^2, \ldots, |\mathbf{h}_i\mathbf{w}_1|^2, |\mathbf{h}_i\mathbf{w}_2|^2\right\}, \\ \cdots, \\ |\mathbf{h}_i\mathbf{w}_1|^2 \leq |\mathbf{h}_i\mathbf{w}_2|^2. \end{cases} \tag{44}$$

According to (27) and (28), the constraint (44) can be transformed as

$$\widetilde{\mathcal{Q}}_i = \begin{cases} |\mathbf{h}_i\mathbf{w}_K|^2 \leq \min_{j\in[1,K-1]} \mathcal{T}_{ij}\left(\mathbf{w}_j, \overline{\mathbf{w}}_j\right), \\ |\mathbf{h}_i\mathbf{w}_{K-1}|^2 \leq \min_{j\in[1,K-2]} \mathcal{T}_{ij}\left(\mathbf{w}_j, \overline{\mathbf{w}}_j\right), \\ \cdots, \\ |\mathbf{h}_i\mathbf{w}_1|^2 \leq \mathcal{T}_{i2}\left(\mathbf{w}_2, \overline{\mathbf{w}}_2\right). \end{cases} \tag{45}$$

For UE-3 to UE-K, a method similar to that in Appendix A can be utilized to transform the lower limitation of transmission rate and make the rate achievable in (42).

On the other hand, for UE-1 and UE-2, we need a different derivation due to the modified SIC order.

First, variables $\widetilde{s_1}$ and $\widetilde{s_2}$ can be introduced, and we have

$$\widetilde{\mathcal{L}_i} = \frac{2\mathfrak{Re}\left(\overline{\mathbf{w}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\mathbf{w}_i\right)}{\widetilde{\overline{s}_i} - 1} - \frac{\mathfrak{Re}\left(\overline{\mathbf{w}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\overline{\mathbf{w}}_i\right)}{(\widetilde{\overline{s}_i} - 1)^2}(\widetilde{s_i} - 1), i = 1, 2, \tag{46a}$$

$$\left\|\left[2\mathbf{h}_1\mathbf{w}_3, 2\mathbf{h}_1\mathbf{w}_4, \cdots, 2\mathbf{h}_1\mathbf{w}_K, 2\sigma, \widetilde{\mathcal{L}_1} - 1\right]^\dagger\right\| \leq \widetilde{\mathcal{L}_1} + 1, \tag{46b}$$

$$\left\|\left[2\mathbf{h}_2\mathbf{w}_1, 2\mathbf{h}_2\mathbf{w}_3, \cdots, 2\mathbf{h}_2\mathbf{w}_K, 2\sigma, \widetilde{\mathcal{L}_2} - 1\right]^\dagger\right\| \leq \widetilde{\mathcal{L}_2} + 1. \tag{46c}$$

Then, we should also introduce variables $\widetilde{f_i}$, $\widetilde{g_i}$, $\widetilde{h_i}$ and $\widetilde{q_i}$ to obtain the upper and lower bounds as

$$\sum_{j=1}^{K} \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2 \geq e^{\widetilde{f_i}}, i = 1, 3, 4, \cdots, K, \tag{47a}$$

$$\sum_{j=1, j\neq 2}^{K} \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2 \leq e^{\widetilde{g_i}}, i = 1, 3, 4, \cdots, K, \tag{47b}$$

$$\sum_{j=1}^{K} \mathbf{h}_2\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_2^\dagger + \sigma^2 \geq e^{\widetilde{h_2}}, \tag{47c}$$

$$\sum_{j=1, j\neq 2}^{K} \mathbf{h}_2\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_2^\dagger + \sigma^2 \leq e^{\widetilde{q_2}}, \tag{47d}$$

and thus the inequality in (42) $\min\left\{R_1^2, R_3^2, \ldots, R_K^2\right\} \geq R_t^{[2]}$ can be transformed as

$$\widetilde{f_i} - \widetilde{g_i} + \widetilde{h_2} - \widetilde{q_2} \geq 0, \ i = 1, 3, 4, \cdots, K. \tag{48}$$

In addition, we introduce $\widehat{f_i}$, $\widehat{g_i}$, $\widehat{h_i}$ and $\widehat{q_i}$ to obtain

$$\sum_{j=1, j\neq 2}^{K} \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2 \geq e^{\widehat{f_i}}, i = 3, 4 \cdots, K, \tag{49a}$$

$$\sum_{j=3}^{K} \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2 \leq e^{\widehat{g_i}}, i = 3, 4 \cdots, K, \tag{49b}$$

$$\sum_{j=1, j\neq 2}^{K} \mathbf{h}_1\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_1^\dagger + \sigma^2 \geq e^{\widehat{h_1}}, \tag{49c}$$

$$\sum_{j=3}^{K} \mathbf{h}_1\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_1^\dagger + \sigma^2 \leq e^{\widehat{q_1}}, \tag{49d}$$

and thus the inequality in (42) $\min\left\{R_3^1, R_4^1, \ldots, R_K^1\right\} \geq R_t^{[1]}$ is equivalent to

$$\widehat{f_i} - \widehat{g_i} + \widehat{h_1} - \widehat{q_1} \geq 0, \ i = 3, 4 \cdots, K. \tag{50}$$

According to above derivations, the optimization problem (42) can be transformed as

$$\begin{aligned}
&\max_{\mathbf{w}_i} \ |\mathbf{w}_2|^2 \\
&s.t. \ \sum_{i\in K} \|\mathbf{w}_i\|^2 \leq P_s, \\
&\quad \widetilde{\mathcal{Q}}_i, \ i \in \mathcal{K}, \\
&\quad s_i \geq 2^{r_t}, \ i = 3, 4, \cdots, K, \ (56), \quad (57), \\
&\quad \widetilde{s_i} \geq 2^{r_t}, \ i = 1, 2, \ (46), \\
&\quad \mathcal{O}_i, i = 3, 4, \cdots, K{-}1, (63), (47), (48), (49), (50).
\end{aligned} \tag{51}$$

which is convex, and can be solved by existing toolboxes such as CVX. Therefore, the solution to (42) can be calculated by solving (51) iteratively, according to Algorithm 1.

C. Multiple Secure Users

In the above two schemes, we aim to guarantee the security of a single secure user. If we want to ensure the secure transmission of multiple users simultaneously, it can be solved

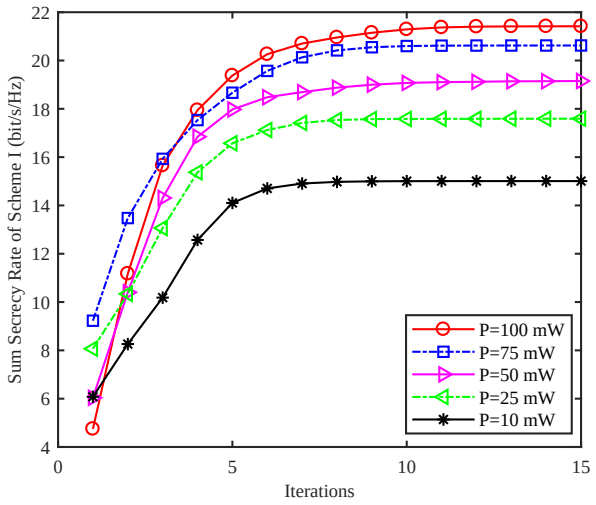


Fig. 2. Convergence of the sum secrecy rate for Scheme I with different values of transmit power P_s. $M = 3$, $r_t = 1$ bit/s/Hz, $d_e = 200$ m.

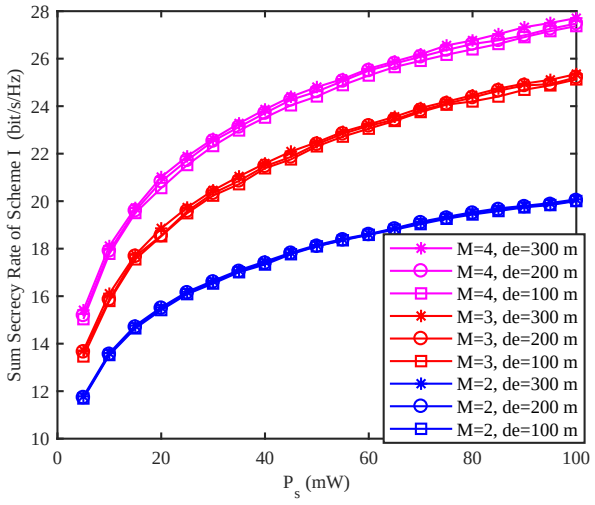


Fig. 3. Sum secrecy rate comparison of Scheme I with different P_s, M and d_e. $r_t = 1$ bit/s/Hz.

in a similar way. For example, we assume that UE-1 and UE-4 are secure users. The optimization problem can be written as

$$\begin{aligned} \max_{\mathbf{w}_i} \quad & \sum_{i=2}^{3} |\mathbf{w}_i|^2 \\ s.t. \quad & |\mathbf{h}_i\mathbf{w}_2|^2 \geq |\mathbf{h}_i\mathbf{w}_1|^2 \geq \cdots |\mathbf{h}_i\mathbf{w}_K|^2, \ i \in \mathcal{K}, \\ & \sum_{i=1}^{K} \|\mathbf{w}_i\|^2 \leq P_s, \\ & \min\left\{R_1^2, R_3^2, \ldots, R_K^2\right\} \geq R_t^{[2]} \geq r_t, \\ & \min\left\{R_3^1, R_4^1, \ldots, R_K^1\right\} \geq R_t^{[1]} \geq r_t, \\ & \min\left\{R_{i+1}^i, \ldots, R_K^i\right\} \geq R_t^{[i]} \geq r_t, i = 3, \cdots, K-1, \\ & R_t^{[K]} \geq r_t, \end{aligned} \tag{52}$$

which can be solved similarly according to Section IV-B.

In the extreme case when all the users require secure transmission, we should exploit other methods to guarantee the legitimate security, such as AN in [40].

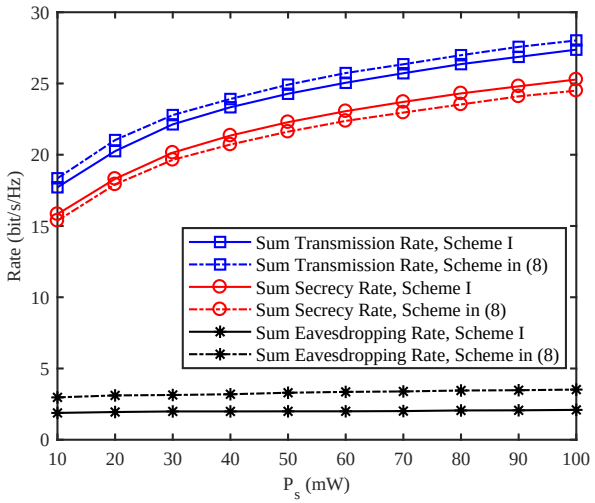


Fig. 4. Sum secrecy rate, sum transmission rate and sum eavesdropping rate comparison of Scheme I and Scheme in (8). $M = 3$, $r_t = 1$ bit/s/Hz, $d_e = 50$ m.

V. Simulation Results and Discussion

Simulation results are presented to evaluate the performance of the proposed joint precoding optimization schemes for MISO-NOMA networks in this section. Consider a MISO-NOMA network with 3 users and an eavesdropper, in which UE-1, UE-2 and UE-3 are 450 m, 250 m and 50 m from the BS, respectively. We set $\alpha = 2.6$, $\beta = 10^{-4}$ and $\sigma^2 = 10^{-11}$ mW.

First, the performance of Scheme I is analyzed. The convergence of the sum secrecy rate for Scheme I with different values of transmit power P_s is shown in Fig. 2, when $M = 3$, $r_t = 1$ bit/s/Hz. The distance between the BS and the eavesdropper $d_e = 200$ m. From the results, we can see that Algorithm 1 for Scheme I converges after about only 10 iterations, for different transmit power. In addition, the sum secrecy rate of the legitimate network increases from 15 bit/s/Hz to 21.4 bit/s/Hz when the sum transmit power ranges from 10 mW to 100 mW.

We compare the sum secrecy rate of Scheme I under different P_s, M and d_e in Fig. 3. $r_t = 1$ bit/s/Hz. From the results, we can observe that the sum secrecy rate of Scheme I increases with M and P_s, which means that larger M and higher P_s can improve the security performance of the legitimate network. In addition, although the sum secrecy rate is a little higher when d_e is larger, the improvement is marginal to be ignored. This indicates that Scheme I can ensure reliable security even when the eavesdropper is located near the BS.

The sum secrecy rate, sum transmission rate and sum eavesdropping rate of Scheme I and the conventional scheme in (8) are compared in Fig. 4. $M = 3$, $r_t = 1$ bit/s/Hz and $d_e = 50$ m. From the results, we can notice that although the sum transmission rate of Scheme in (8) is higher than that of the proposed Scheme I, the sum secrecy rate of Scheme I is higher. This is because the sum eavesdropping rate can be effectively decreased by Scheme I, as shown in the figure. Thus, the security performance of the MISO-NOMA network

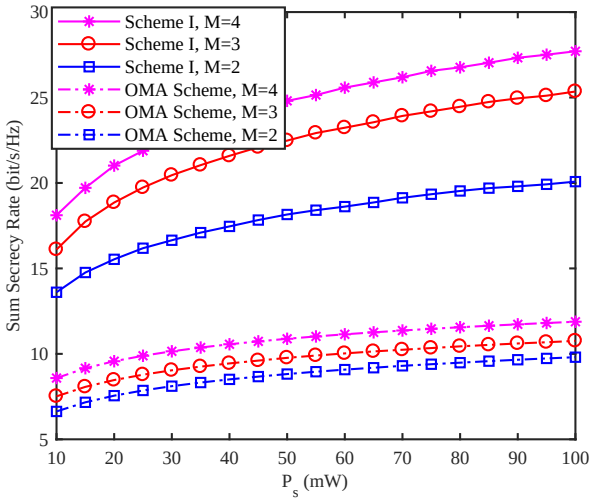


Fig. 5. Sum secrecy rate comparison of Scheme I and the OMA Scheme with different P_s and M. $r_t = 1$ bit/s/Hz and $d_e = 300$ m.

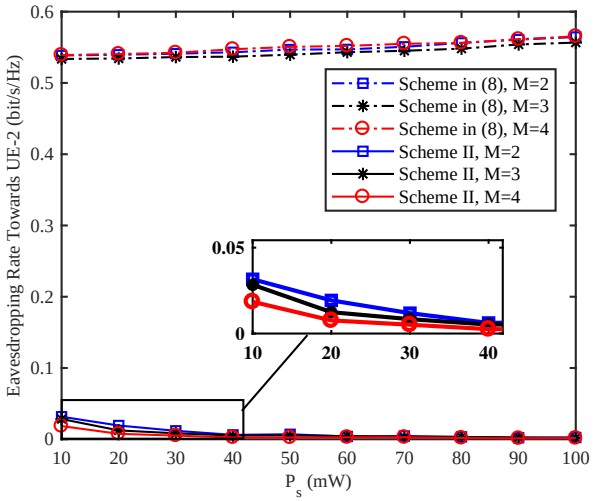


Fig. 6. Eavesdropping rate towards UE-2 comparison in Scheme II and Scheme in (8) with different values of P_s and M. $r_t = 1$ bit/s/Hz and $d_e = 50$ m.

can be effectively guaranteed by Scheme I, especially for the farthest UE-1. In addition, the proportional relationship between the transmit power of each user is almost unchanged when P_s is high, which also results in the almost unchanged eavesdropping rate.

The sum secrecy rate of Scheme I and the orthogonal multiple access (OMA) scheme is compared under different P_s and M in Fig. 5. $r_t = 1$ bit/s/Hz and $d_e = 300$ m. In the OMA Scheme, we adopt the time division multiple access mode and maximize the secrecy rate of a specific legitimate user in each time slot. From the results, we can see that the sum secrecy rate of Scheme I is much higher than that of the OMA scheme. Thus, the superiority of Scheme I in improving the spectrum efficiency and security performance over the OMA scheme can be verified.

Then, the performance of Scheme II is evaluated. The eavesdropping rate towards UE-2 of Scheme II and the conventional scheme in (8) is compared with different P_s and M in Fig. 6. $r_t = 1$ bit/s/Hz and $d_e = 50$ m. From the results, we can notice that the eavesdropping rate towards UE-2 of Scheme II is close to 0, and much lower than that of Scheme in (8). Thus, we can conclude that the proposed Scheme II can effectively guarantee the security performance of UE-2 by hiding its signal in the larger signal of UE-1. In addition, the number of antennas at BS will not obviously affect the security performance in Scheme II.

The secrecy rate of UE-2 of Scheme II is compared with different P_s and r_t in Fig. 7. $M = 3$ and $d_e = 100$ m. From the results, we can see that the secrecy rate can be guaranteed to be close to r_t. This is because according to (34), the transmit power of UE-2 is saved to disrupt the eavesdropping by maximizing the transmit power of UE-1, with the transmission rate of UE-2 equal to r_t. Thus, the eavesdropping towards UE-2 can be disrupted effectively, and the secrecy rate is close to the transmission rate when P_s is high enough.

Last, the performance of Scheme III is demonstrated. The eavesdropping rate towards UE-1 of Scheme III and the

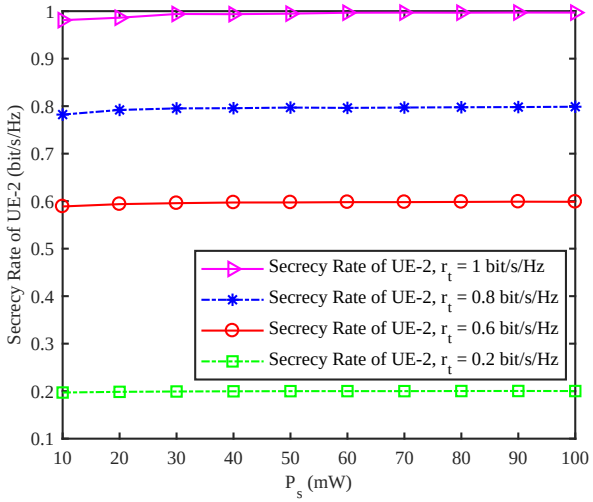


Fig. 7. Secrecy rate of UE-2 comparison in Scheme II with different P_s and r_t. $M = 3$ and $d_e = 100$ m.

conventional scheme in (8) is compared with different P_s and M in Fig. 8. $r_t = 1$ bit/s/Hz and $d_e = 50$ m. From the results, we can see that the eavesdropping rate towards UE-1 of Scheme III is close to 0, and much lower than that of Scheme in (8). Thus, we can conclude that the proposed Scheme III can effectively guarantee the security performance of UE-1 by hiding its signal in the larger signal of UE-2, which can be achieved by modified SIC order via joint precoding. In addition, we can also observe that the number of antennas at BS will not affect the security performance in Scheme III.

We compare the secrecy rate of UE-1 of Scheme III with different P_s and r_t in Fig. 9. $M = 3$ and $d_e = 300$ m. From the results, we can see that the secrecy rate can be guaranteed to be close to r_t. According to (42), the transmit power of UE-1 is saved to disrupt the eavesdropping by maximizing the transmit power of UE-2, with the transmission rate of UE-1 equal to r_t. This can be achieved by modified SIC order via joint precoding. Thus, the eavesdropping towards UE-1

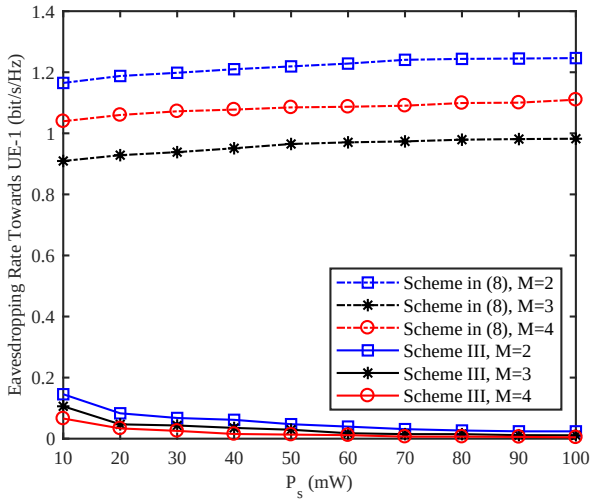


Fig. 8. Eavesdropping rate towards UE-1 comparison in Scheme III and Scheme in (8) with different P_s and M. $r_t = 1$ bit/s/Hz and $d_e = 50$ m.

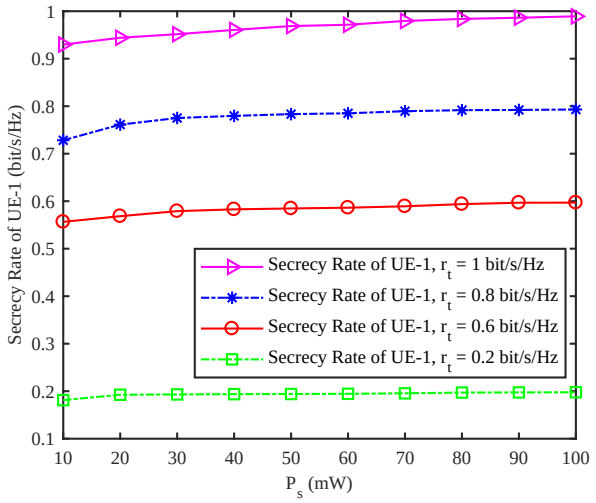


Fig. 9. Secrecy rate of UE-1 comparison in Scheme III with different P_s and r_t. $M = 3$ and $d_e = 300$ m.

can be disrupted effectively, and the secrecy rate is close to the transmission rate when P_s is high enough. In addition, comparing Fig. 7 and Fig. 9, we can observe that the secrecy rate of UE-1 in Scheme III is slightly lower than the secrecy rate of UE-2 in Scheme II. This is because the modified SIC order in Scheme III requires more resource to achieve, and thus higher transmit power is required at BS to achieve same security performance in Scheme III.

VI. Conclusion and Future Work

In this paper, three secure transmission schemes are proposed for MISO-NOMA networks via joint precoding optimization, with and without eavesdropping CSI, respectively. For the case when the eavesdropping CSI is available at BS, the precoding vectors are jointly optimized to maximize the sum secrecy rate. The problem is non-convex, and we transform it into a convex one via SOC programming, which can be solved iteratively. When the eavesdropping CSI is unavailable, we first consider that the secure user is not the farthest from BS, and the transmit power of the farther users is maximized via joint precoding optimization to ensure its own security. We then consider the case when the farthest user from BS requires secure transmission, and the modified SIC order and joint precoding optimization can be leveraged to guarantee its security. Similar method to the scheme with CSI can also be exploited to calculate the suboptimal solutions to these two non-convex problems. Simulation results are shown to verify the effectiveness and efficiency of the proposed schemes in enhancing the security for downlink MISO NOMA. In the future work, we will continue to carry out the secrecy outage probability (SOP) analysis for the proposed schemes.

Acknowledgment

We thank the editor and reviewers for their detailed reviews and constructive comments, which have greatly improved the quality of this paper.

Appendix

Proof of Proposition 1

First, to transform $R_t^{[i]} \geq r_t$, we introduce a variable s_i, and let

$$1 + \frac{|\mathbf{h}_i\mathbf{w}_i|^2}{\sum_{j=i+1}^{K}|\mathbf{h}_i\mathbf{w}_j|^2 + \sigma^2} \geq s_i, i = 1, 2, \cdots, K-1, \quad (53a)$$

$$1 + |\mathbf{h}_K\mathbf{w}_K|^2/\sigma^2 \geq s_K, \quad (53b)$$

which are equal to

$$\frac{|\mathbf{h}_i\mathbf{w}_i|^2}{s_i - 1} \geq \sum_{j=i+1}^{K}|\mathbf{h}_i\mathbf{w}_j|^2 + \sigma^2, i = 1, 2, \cdots, K-1, \quad (54a)$$

$$\frac{|\mathbf{h}_K\mathbf{w}_K|^2}{s_K - 1} \geq \sigma^2. \quad (54b)$$

The left sides of the inequalities in (54) can be written as

$$\Gamma_i(\mathbf{w}_i, s_i) = \frac{\mathbf{h}_i\mathbf{w}_i\mathbf{w}_i^\dagger\mathbf{h}_i^\dagger}{s_i - 1}, \ i \in \mathcal{K}. \quad (55)$$

Then, the first order Taylor's approximation for (55) can be derived as

$$\begin{aligned}\mathcal{L}_i(\mathbf{w}_i, s_i, \overline{\mathbf{w}}_i, \overline{s}_i) =& \frac{2\mathfrak{Re}\left(\overline{\mathbf{w}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\mathbf{w}_i\right)}{\overline{s}_i - 1} \\ &- \frac{\mathfrak{Re}\left(\overline{\mathbf{w}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\overline{\mathbf{w}}_i\right)}{(\overline{s}_i - 1)^2}(s_i - 1), i \in \mathcal{K}.\end{aligned} \quad (56)$$

Therefore, according to the SOC constraint (24), the inequalities (54) can be transformed into

$$\left\|\left[2\mathbf{h}_i\mathbf{w}_{i+1}, 2\mathbf{h}_1\mathbf{w}_{i+2}, \cdots, 2\mathbf{h}_i\mathbf{w}_K, 2\sigma, \mathcal{L}_i - 1\right]^\dagger\right\| \leq \mathcal{L}_i + 1, \quad i = 1, 2, \cdots, K-1, \quad (57a)$$

$$\left\|\left[2\sigma, \mathcal{L}_K - 1\right]^\dagger\right\| \leq \mathcal{L}_K + 1. \quad (57b)$$

With the above transformations, the lower limitation of transmission rate $R_t^{[i]} \geq r_t$ can be changed into

$$s_i \geq 2^{r_t}, \ i \in \mathcal{K}. \quad (58)$$

Then, we consider the transformation of (7). In order to make all the rate R_k^i achievable, we have

$$\min\left\{R_{i+1}^i, R_{i+2}^i, \ldots, R_K^i\right\} \geq R_t^{[i]}, i=1,\cdots,K-1, \quad (59)$$

which is equivalent to

$$\begin{cases} R_{i+1}^i \geq R_t^{[i]}, \\ R_{i+2}^i \geq R_t^{[i]}, \\ \cdots\cdots, \\ R_{K-1}^i \geq R_t^{[i]}, \\ R_K^i \geq R_t^{[i]}. \end{cases} \quad (60)$$

Each of these inequalities in (60) can be transformed individually. For example, $R_{i+1}^i \geq R_t^{[i]}$ can be written as

$$R_{i+1}^i - R_t^{[i]} \geq 0,\ i = 1, \cdots, K-1, \quad (61)$$

which is equivalent to

$$\begin{aligned} &\log_2\left(\frac{\sum_{j=i}^K \mathbf{h}_{i+1}\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_{i+1}^\dagger+\sigma^2}{\sum_{j=i+1}^K \mathbf{h}_{i+1}\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_{i+1}^\dagger+\sigma^2}\right) \\ &-\log_2\left(\frac{\sum_{j=i}^K \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2}{\sum_{j=i+1}^K \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger+\sigma^2}\right)\geq 0, i=1,\cdots,K-1. \end{aligned} \quad (62)$$

Through introducing auxiliary variables f_{i+1}, g_{i+1}, h_{i+1} and q_{i+1}, we can get some upper and lower bounds as

$$\sum_{j=i}^K \mathbf{h}_{i+1}\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_{i+1}^\dagger + \sigma^2 \geq e^{f_{i+1}}, i=1,\cdots,K-1, \quad (63a)$$

$$\sum_{j=i+1}^K \mathbf{h}_{i+1}\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_{i+1}^\dagger+\sigma^2 \leq e^{g_{i+1}}, i=1,\cdots,K-1, \quad (63b)$$

$$\sum_{j=i}^K \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2 \geq e^{h_{i+1}}, i=1,\cdots,K-1, \quad (63c)$$

$$\sum_{j=i+1}^K \mathbf{h}_i\mathbf{w}_j\mathbf{w}_j^\dagger\mathbf{h}_i^\dagger + \sigma^2 \leq e^{q_{i+1}}, i=1,\cdots,K-1, \quad (63d)$$

according to which, (62) can be transformed into

$$\log_2 e\cdot(f_{i+1}-g_{i+1}+h_{i+1}-q_{i+1}) \geq 0, i=1,\cdots,K-1, \quad (64)$$

which can be equivalently formulated as

$$f_{i+1} - g_{i+1} + h_{i+1} - q_{i+1} \geq 0, i = 1, \cdots, K-1. \quad (65)$$

Therefore, (59) can be transformed into the following series of inequalities, $i = 1, \cdots, K-1$.

$$\mathcal{O}_i = \begin{cases} f_{i+1} - g_{i+1} + h_{i+1} - q_{i+1} \geq 0, \\ f_{i+2} - g_{i+2} + h_{i+2} - q_{i+2} \geq 0, \\ \cdots\cdots, \\ f_{K-1} - g_{K-1} + h_{K-1} - q_{K-1} \geq 0, \\ f_K - g_K + h_K - q_K \geq 0. \end{cases} \quad (66)$$

REFERENCES

[1] D. Li, N. Zhao, Y. Chen, A. Nallanathan, Z. Ding, and M.-S. Alouini, "Joint precoding optimization for secure transmission in downlink MISO-NOMA networks," in *Proc. PIMRC'19*, pp. 1–6, Istanbul, Turkey, Oct. 2018.

[2] L. Dai, B. Wang, Y. Yuan, S. Han, C. l. I, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sept. 2015.

[3] S. Chen, B. Ren, Q. Gao, S. Kang, S. Sun, and K. Niu, "Pattern division multiple access-A novel nonorthogonal multiple access for fifth-generation radio networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3185–3196, Apr. 2017.

[4] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[5] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. s. Kwak, "Power-domain non-orthogonal multiple access NOMA in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2nd Quart. 2017.

[6] D. Zhang, Z. Zhou, C. Xu, Y. Zhang, J. Rodriguez, and T. Sato, "Capacity analysis of NOMA with mmwave massive MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1606–1618, Jul. 2017.

[7] Y. Wu, L. P. Qian, H. Mao, X. Yang, H. Zhou, and X. S. Shen, "Optimal power allocation and scheduling for non-orthogonal multiple access relay-assisted networks," *IEEE Trans. Mob. Comput.*, vol. 17, no. 11, pp. 2591–2606, Nov. 2018.

[8] L. Yang, H. Jiang, Q. Ye, Z. Ding, L. Lv, and J. Chen, "On the impact of user scheduling on diversity and fairness in cooperative NOMA," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11296–11301, Nov. 2018.

[9] X. Chen, F. Gong, G. Li, H. Zhang, and P. Song, "User pairing and pair scheduling in massive MIMO-NOMA systems," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 788–791, Apr. 2018.

[10] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[11] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *Proc. IEEE*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[12] Z. Ding, F. Adachi, and H. V. Poor, "The application of MIMO to non-orthogonal multiple access," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 537–552, Jan. 2016.

[13] Z. Chen, Z. Ding, X. Dai, and G. K. Karagiannidis, "On the application of quasi-degradation to MISO-NOMA downlink," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6174–6189, Dec. 2016.

[14] B. Chen, Y. Chen, Y. Chen, Y. Cao, N. Zhao, and Z. Ding, "A novel spectrum sharing scheme assisted by secondary NOMA relay," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 732–735, Oct. 2018.

[15] F. Zhou, Y. Wu, Y. Liang, Z. Li, Y. Wang, and K. Wong, "State of the art, taxonomy, and open issues on cognitive radio networks with NOMA," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 100–108, Apr. 2018.

[16] T. Hou, Y. Liu, Z. Song, X. Sun, and Y. Chen, "Multiple antenna aided NOMA in UAV networks: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1031–1044, Feb. 2019.

[17] N. Zhao, X. Pang, Z. Li, Y. Chen, F. Li, Z. Ding, and M. Alouini, "Joint trajectory and precoding optimization for UAV-assisted NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3723–3735, May 2019.

[18] L. Bai, L. Zhu, T. Li, J. Choi, and W. Zhuang, "An efficient hybrid transmission method: Using nonorthogonal multiple access and multiuser diversity," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2276–2288, Mar. 2018.

[19] M. F. Hanif, Z. Ding, T. Ratnarajah, and G. K. Karagiannidis, "A minorization-maximization method for optimizing sum rate in the downlink of non-orthogonal multiple access systems," *IEEE Trans. Signal Process.*, vol. 64, no. 1, pp. 76–88, Jan. 2016.

[20] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept. 2016.

[21] K. N. Le, "Performance analysis of secure communications over dual correlated Rician fading channels," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6659–6673, Dec. 2018.

[22] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart. 2017.

[23] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[24] F. Shu, L. Xu, J. Wang, W. Zhu, and X. Zhou, "Artificial-noise-aided secure multicast precoding for directional modulation systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6658–6662, Jul. 2018.

[25] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[26] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, Feb. 2018.

[27] Y. Cai, C. Zhao, Q. Shi, G. Y. Li, and B. Champagne, "Joint beamforming and jamming design for mmWave information surveillance systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1410–1425, Jul. 2018.

[28] L. Fan, R. Zhao, F. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[29] K. N. Le and T. A. Tsiftsis, "Wireless security employing opportunistic relays and an adaptive encoder under outdated CSI and dual-correlated Nakagami-m fading," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2405–2419, Mar. 2019.

[30] Y. Cao, N. Zhao, F. R. Yu, M. Jin, Y. Chen, J. Tang, and V. C. M. Leung, "Optimization or alignment: Secure primary transmission assisted by secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, Apr. 2018.

[31] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[32] G. Pan, H. Lei, Y. Deng, L. Fan, J. Yang, Y. Chen, and Z. Ding, "On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831–3843, Sept. 2016.

[33] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, Jul. 2017.

[34] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct. 2017.

[35] J. Chen, L. Yang, and M. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[36] L. Xu, A. Nallanathan, X. Pan, J. Yang, and W. Liao, "Security-aware resource allocation with delay constraint for NOMA-based cognitive radio network," *IEEE Trans. Inf. Forens. Security*, vol. 13, no. 2, pp. 366–376, Feb. 2018.

[37] Y. Cao, N. Zhao, Y. Chen, M. Jin, L. Fan, Z. Ding, and F. R. Yu, "Privacy preservation via beamforming for NOMA," *IEEE Trans. Wireless Commun.*, Online. DOI: 10.1109/TWC.2019.2916363.

[38] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[39] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 918–931, Apr. 2018.

[40] N. Zhao, W. Wang, J. Wang, Y. Chen, Y. Lin, Z. Ding, and N. C. Beaulieu, "Joint beamforming and jamming optimization for secure transmission in MISO-NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2294–2305, Mar. 2019.

[41] M. Lobo, L. Vandenberghe, S. Boyd, and H. Lebret, "Applications of second-order cone programming," *Lin. Alg. Applicat.*, vol. 248, pp. 193–228, Nov. 1998.

Nan Zhao (S'08-M'11-SM'16) is currently an Associate Professor at Dalian University of Technology, China. He received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China.

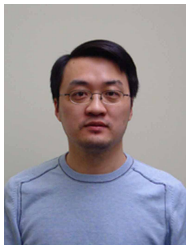
Dr. Zhao is serving or served on the editorial boards of 7 SCI-indexed journals, including IEEE Transactions on Green Communications and Networking. He won the best paper awards in IEEE VTC 2017 Spring, MLICOM 2017, ICNC 2018, WCSP 2018 and CSPS 2018. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018.

Dongdong Li received the B.S. degree from the Dalian University of Technology, Dalian, China, in 2018, where she is currently working toward the M.S. degree at the School of Information and Communication Engineering. Her current research interests include nonorthogonal multiple access, physical layer security, and UAV communications.

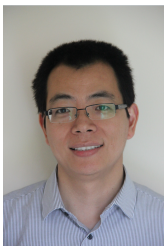
Mingqian Liu (M'13) received the B. S. degree in electrical engineering from Information Engineering University, in 2006, the M.S. degree from the Xian University of Technology, in 2009, and the Ph.D. degree in communication and information system from Xidian University, Xian, China, in 2013, where he is currently with the State Key Laboratory of Integrated Services Networks and did postdoctoral research, from 2014 to 2016. His research interests include communication signal processing and statistical signal processing.

Yang Cao is currently pursuing Ph.D. degree in the School of Information and Communication Engineering at Dalian University of Technology, China. She received the B.S. degree from HeFei University of Technology, China.

Her current research interests include non-orthogonal multiple access, interference alignment, physical layer security, wireless energy harvesting, and resource allocation.



Yunfei Chen (S'02-M'06-SM'10) received his B.E. and M.E. degrees in electronics engineering from Shanghai Jiaotong University, Shanghai, P.R.China, in 1998 and 2001, respectively. He received his Ph.D. degree from the University of Alberta in 2006. He is currently working as an Associate Professor at the University of Warwick, U.K. His research interests include wireless communications, cognitive radios, wireless relaying and energy harvesting.



Zhiguo Ding (S'03-M'05-SM'14) received his B.Eng in Electrical Engineering from the Beijing University of Posts and Telecommunications in 2000, and the Ph.D degree in Electrical Engineering from Imperial College London in 2005. From Jul. 2005 to Apr. 2018, he was working in Queen's University Belfast, Imperial College, Newcastle University and Lancaster University. Since Apr. 2018, he has been with the University of Manchester as a Professor in Communications. From Oct. 2012 to Sept. 2018, he has also been an academic visitor in Princeton University.

Dr Ding' research interests are 5G networks, game theory, cooperative and energy harvesting networks and statistical signal processing. He is serving as an Editor for *IEEE Transactions on Communications*, *IEEE Transactions on Vehicular Technology*, and *Journal of Wireless Communications and Mobile Computing*, and was an Editor for *IEEE Wireless Communication Letters*, *IEEE Communication Letters* from 2013 to 2016. He received the best paper award in IET ICWMC-2009 and IEEE WCSP-2014, the EU Marie Curie Fellowship 2012-2014, the Top IEEE TVT Editor 2017, IEEE Heinrich Hertz Award 2018, the IEEE Jack Neubauer Memorial Award 2018 and the IEEE Best Signal Processing Letter Award 2018.

Xianbin Wang (S'98-M'99-SM'06-F'17) is a Professor and Tier 1 Canada Research Chair at Western University, Canada. He received his Ph.D. degree in electrical and computer engineering from National University of Singapore in 2001.

Prior to joining Western, he was with Communications Research Centre Canada (CRC) as a Research Scientist/Senior Research Scientist between July 2002 and Dec. 2007. From Jan. 2001 to July 2002, he was a system designer at STMicroelectronics. His current research interests include 5G technologies, Internet-of-Things, communications security, machine learning and locationing technologies. Dr. Wang has over 350 peer-reviewed journal and conference papers, in addition to 29 granted and pending patents and several standard contributions.

Dr. Wang is a Fellow of Canadian Academy of Engineering, a Fellow of IEEE and an IEEE Distinguished Lecturer. He has received many awards and recognitions, including Canada Research Chair, CRC Presidents Excellence Award, Canadian Federal Government Public Service Award, Ontario Early Researcher Award and six IEEE Best Paper Awards. He currently serves as an Editor/Associate Editor for IEEE Transactions on Communications, IEEE Transactions on Broadcasting, and IEEE Transactions on Vehicular Technology and He was also an Associate Editor for IEEE Transactions on Wireless Communications between 2007 and 2011, and IEEE Wireless Communications Letters between 2011 and 2016. Dr. Wang was involved in many IEEE conferences including GLOBECOM, ICC, VTC, PIMRC, WCNC and CWIT, in different roles such as symposium chair, tutorial instructor, track chair, session chair and TPC co-chair.