Privacy Preservation via Beamforming for NOMA

Yang Cao, Nan Zhao, *Senior Member, IEEE,* Yunfei Chen, *Senior Member, IEEE,* Minglu Jin, *Member, IEEE,* Lisheng Fan, Zhiguo Ding, *Senior Member, IEEE* and F. Richard Yu, *Fellow, IEEE*

***Abstract*—Non-orthogonal multiple access (NOMA) has been proposed as a promising multiple access approach for 5G mobile systems because of its superior spectrum efficiency. However, the privacy between the NOMA users may be compromised due to the transmission of a superposition of all users' signals to successive interference cancellation (SIC) receivers. In this paper, we propose two schemes based on beamforming optimization for NOMA that can enhance the security of a specific private user while guaranteeing the other users' quality of service (QoS). Specifically, in the first scheme, when the transmit antennas are inadequate, we intend to maximize the secrecy rate of the private user, under the constraint that the other users' QoS is satisfied. In the second scheme, the private user's signal is zero-forced at the other users when redundant antennas are available. In this case, the transmission rate of the private user is also maximized while satisfying the QoS of the other users. Due to the non-convexity of optimization in these two schemes, we first convert them into convex forms and then, an iterative algorithm based on the ConCave-Convex Procedure is proposed to obtain their solutions. Extensive simulation results are presented to evaluate the effectiveness of the proposed schemes.**

***Index Terms*—Non-orthogonal multiple access, physical layer security, beamforming optimization, privacy protection, non-convex programming, zero-forcing.**

I. Introduction

Recently, non-orthogonal multiple access (NOMA) has emerged as a pivotal technique to satisfy the diverse requirements for the fifth-generation (5G) mobile networks, such as massive connectivity, high reliability and efficient spectrum utilization [2], [3]. Unlike conventional orthogonal multiple access (OMA), NOMA allows more than one users to simultaneously access a single orthogonal resource block, such as a time slot, a subcarrier, or a spreading code [2], [4]. Owing to the advantages of its high spectral efficiency and cell-edge throughput, NOMA has attracted great attention from both academia and industry. The NOMA principle can be implemented in two forms, one based on the use of a single resource block and the other relying on the hybrid implementation of NOMA [5], [6]. In this paper, we focus on the former, which is also termed power domain NOMA.

For power-domain NOMA, the users' signals are superposed through power multiplexing based on their channel conditions. To remove the interference at receivers, successive interference cancellation (SIC) is applied to retrieve the intended signal [5], [7]. The performance of power-domain NOMA for cellular radio access was studied by Saito *et al*. in [8], and both the capacity and cell-edge throughput in downlink NOMA with SIC were analyzed. In [9], Ding *et al*. proposed a cooperative NOMA scheme to further enhance the system reliability. Secondary NOMA relay was utilized by Chen *et al*. to access the spectrum while helping the long-distance primary transmission via relay [10]. In [11], using simultaneous wireless information and power transfer (SWIPT) in NOMA, Liu *et al*. presented a novel cooperative SWIPT NOMA protocol. Some basic work was done by Wu *et al*. on the optimal power allocation and scheduling for NOMA relay-assisted networks in [12], which can achieve significant improvement on performance. In [13], Lv *et al*. proposed a novel millimeter-wave NOMA scheme to guarantee the QoS of massive devices in cellular machine-to-machine systems. Moreover, to further enhance the performance of NOMA, novel frameworks for multi-antenna NOMA systems were investigated in [14] and [15]. In [16], Chen *et al*. studied the impact of quasi-degradation on NOMA, based on which, an effective precoding algorithm for downlink multi-input single-output (MISO) NOMA was proposed. In [17], the sum rate was optimized in the downlink MISO NOMA system by Hanif *et al*. via a minorization-maximization algorithm. Recently, some excellent work was done by Qiu *et al*. to achieve without SIC in [18].

However, due to the openness of wireless channels, there exist several security challenges in NOMA networks [2]. In particular, a user with stronger channel in NOMA systems has to decode some weaker users' messages before recovering its own signal. This potentially causes information leakage and intrudes their privacy. Hence, secure transmission is a challenging issue in NOMA systems, especially for internal private users [2]. To tackle with this issue, physical layer security (PLS) has been proposed to combat malicious eavesdroppers and guarantee the security and privacy of wireless networks [19], [20]. The inspirational work by Wyner in [21] illustrated

Manuscript received April 16, 2018; revised August 28, 2018, December 22, 2018 and March 23, 2019; accepted May 7, 2019. The work of N. Zhao was supported by the National Natural Science Foundation of China (NSFC) under Grant 61871065 and 61871139, the open research fund of State Key Laboratory of Integrated Services Networks under Grant ISN19-02, and the Xinghai Scholars Program. 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 has been published in preliminary form in the Proceedings of WCSP 2018 [1]. The associate editor coordinating the review of this paper and approving it for publication was J. Yuan. *(Corresponding author: Nan Zhao.)*

Y. Cao, N. Zhao and M. Jin are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, P. R. China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, P. R. China (email: cy216@mail.dlut.edu.cn, zhaonan@dlut.edu.cn, mljin@dlut.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).

L. Fan is with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China (e-mail: lsfan@gzhu.edu.cn).

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).

F.R. Yu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, K1S 5B6, Canada (email: richard.yu@carleton.ca).

a novel framework for wire-tap channels, and proved that nearly perfect secrecy can be achieved using the physical characteristics of wireless channels. Since then, PLS has been widely investigated to enhance the security of wireless communications, e.g., transceiver beamforming designs [22]–[24], cooperative relay/jamming [25]–[28], artificial noise [29], [30], interference alignment [31], [32], *etc*. Particularly, secure beamforming optimization can achieve reliable performance when multiple antennas are equipped. In [33], Lv *et al.* proposed three effective schemes based on secrecy transmit beamforming in a two-tier downlink heterogeneous network. Wang *et al.* studied the robust beamforming and power allocation in a DF relay system, with two practical channel state information (CSI) error models considered [34].

Despite the fact that great effort has been dedicated to the research on PLS in many wireless scenarios, only a few works have considered the security problem in NOMA systems [35]–[42]. In [35], a novel design was studied by He *et al*., with secrecy considered in a NOMA system with an external eavesdropper. In [36], Lei *et al*. exploited different antenna selection schemes to improve the secure performance of the single-input single-output (SISO) and MISO NOMA systems. For large-scale networks, Liu *et al*. leveraged the stochastic geometry method to model the locations of NOMA users and eavesdroppers, and the secrecy outage probability was derived for both single-antenna and multi-antenna cases [37]. In [38], an optimal scheme was developed by Zhang *et al*. to maximize the secrecy sum rate for a SISO NOMA system, with quality of service (QoS) constraints fulfilled. Lv *et al*. exploited artificial noise to guarantee the secure transmission of MISO-NOMA networks in [39]. In [40], beamforming was optimized by Li *et al*. to guarantee the secure transmission in the downlink MISO NOMA systems, in which the users are grouped as multiple clusters. The above works consider external eavesdropping. In [41], the internal security in NOMA networks was considered. Given the enhancement of spectral efficiency, Ding *et al*. investigated a hybrid broadcast NOMA network with multicast-unicast streaming, and the secure performance of the unicast user was analyzed in terms of the secrecy outage probability [41]. In [42], the beamforming and jamming were jointly optimized by Zhao *et al.* to enhance the security of MISO NOMA networks.

In this paper, we focus on the secure design of the private user for a NOMA system [1]. The privacy transmission of a specific user in a MISO NOMA system is considered. To this end, two effective schemes based on transmit beamforming are proposed to protect the confidential communication of this user, using special decoding order for SIC receivers. The key motivations and contributions of this paper are as follows:

- In NOMA systems, due to the fact that a weaker user's message has to be decoded at the stronger users with better channel conditions for the SIC, privacy between users cannot be guaranteed, especially for the weakest user. To the best of our knowledge, very few research works have discussed the security of the private message for NOMA users in the view of PLS [41].
- Motivated by this, a novel SIC decoding order based on joint transmit beamforming and power allocation is designed to ensure the privacy of a specific user in MISO NOMA systems. Specifically, for the private user, the transmit beamforming vector is designed to minimize its information leakage to the other users, while maximizing the received signal strength at its own receiver. The remaining decoding order is consistent with the conventional NOMA.
- To further improve the security of the private user, we propose two schemes, i.e., the secrecy rate maximization (SRM) and zero-forcing (ZF) based schemes. In the SRM scheme, the secrecy rate of the private user is maximized by jointly optimizing transmit beamforming vectors, with other users' QoS and power constraints of decoding order satisfied. Owing to its non-convexity, we first approximate it into a convex form using the ConCave-Convex procedure (CCCP) and then, a CCCP-based iterative algorithm is proposed to obtain its solutions.
- In the ZF-based scheme, the signal of the private user is zero-forced at other receivers via its transmit beamforming vector, and the feasibility of the zero-forcing condition is discussed as well. Similar to the SRM scheme, the secrecy rate of the private user is optimized via transmit beamforming optimization, with other users' QoS, the updated decoding order as well as the zero-forcing condition satisfied.

The rest of this paper is organized as follows. In Section II, the system model is portrayed, followed by a new decoding order design for SIC. The SRM scheme is proposed in Section III, and a CCCP-based algorithm is devised to obtain its solutions. In Section IV, the ZF-based scheme is proposed to mitigate the information leakage of the private user at other users. In Section V, simulation results are presented, and the conclusions are illustrated in Section VII.

Notation: $\mathbf{I}_N$ represents the $N \times N$ identity matrix. $\mathbf{A}^\dagger$ is the Hermitian transpose of matrix $\mathbf{A}$. $\|\mathbf{a}\|$ is the Euclidean norm of vector $\mathbf{a}$, and $\|\mathbf{A}\|$ means the Frobenius norm of matrix $\mathbf{A}$. $\mathbb{C}^{M\times N}$ is the space of complex $M \times N$ matrices. $\mathcal{CN}(\mathbf{a}, \mathbf{A})$ is the complex Gaussian distribution with mean $\mathbf{a}$ and covariance matrix $\mathbf{A}$. $\mathbf{A} \succeq 0$ means that $\mathbf{A}$ is a Hermitian positive semidefinite matrix. $\mathbf{0}_{M\times N}$ denotes an $M \times N$ zero matrix. $Re(\cdot)$ defines the real operator. $\bigtriangledown_x$ denotes the first-order differential operator of a variable x. $A\backslash\{x\}$ means the element x is excluded from the set A.

II. System Model

In this section, we first describe the considered downlink NOMA transmission scenario. Then, a novel decoding order for SIC receivers is presented, with the private transmission of the specific user considered.

A. System Model

We consider a downlink NOMA system as shown in Fig. 1, in which the base station (BS) with M antennas transmits information to K single-antenna users. For simplicity, we define the index set of users as $i \in \mathcal{K} \triangleq \{1, 2, \ldots, K\}$, and let U_i denote the ith user. In the system, we assume that U_k is the only prescribed user that requests private transmission from the

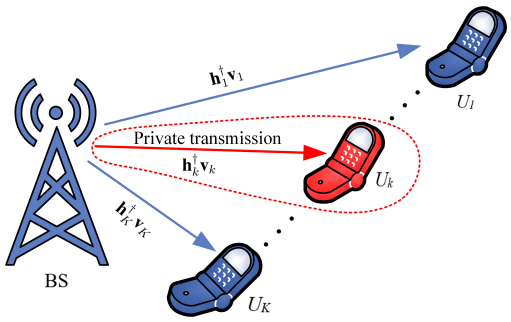


Fig. 1. Illustration of secure beamforming for MISO NOMA systems.

BS, while the other users need the public information during the current time slot[1]. Moreover, to save the spectrum resource, we employ NOMA at the BS to transmit the superposition of private and public messages to all the users. However, the privacy of U_k may be compromised due to the fact that the other users can be deemed as potential eavesdroppers that intend to intercept its information. Therefore, secure transmit beamforming should be designed to guarantee the transmission of the private message, i.e., the precoding vectors of all the users are optimized by the BS to enhance the privacy of U_k.

In a NOMA system, the transmitted signal at the BS can be denoted as

$$\mathbf{x} = \sum_{i=1}^{K} \mathbf{v}_i s_i, \tag{1}$$

where $\mathbf{v}_i \in \mathbb{C}^{M\times 1}$ is the precoding vector of the ith user, with $\|\mathbf{v}_i\|^2 = P_i$, $i \in \mathcal{K}$. s_i denotes the transmitted symbol of the ith user, satisfying $|s_i|^2 = 1$.

Then, the received signal at the ith user can be denoted as

$$y_i = \mathbf{h}_i^\dagger \mathbf{v}_i s_i + \sum_{j=1, j\neq i}^{K} \mathbf{h}_i^\dagger \mathbf{v}_j s_j + n_i, \ \forall i \in \mathcal{K}, \tag{2}$$

where $n_i \sim \mathcal{CN}(0, \sigma^2)$ represents the additive white Gaussian noise (AWGN) at the ith user. $\mathbf{h}_i = d_i^{-\frac{\alpha}{2}} \mathbf{g}_i \in \mathbb{C}^{M\times 1}$ is the channel gain vector from the BS to U_i, in which d_i is the distance between U_i and the BS, α is the path loss exponent and $\mathbf{g}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ denotes the Rayleigh fading channel vector. In addition, we assume that the distance order of all the users follows $d_K < \cdots < d_i < \cdots < d_1$, and the order of their channel-gain expectations can be expressed as $\mathbb{E}\left[\|\mathbf{h}_K\|^2\right] > \cdots > \mathbb{E}\left[\|\mathbf{h}_i\|^2\right] > \cdots > \mathbb{E}\left[\|\mathbf{h}_1\|^2\right]$.

According to the principle of NOMA, SIC is adopted at each receiver to decode information, which can be performed based on the channel difference between users [2], [5]. To further elaborate it, we take U_i $(1 \leq i \leq K-1)$ as an example. In conventional NOMA systems, it is necessary for U_i to decode messages from U_1 to U_{i-1} before retrieving its own information, and the achievable signal-to-interference-plus-noise-ratio (SINR) at U_i can be expressed as

$$\mathrm{SINR}_i^j = \frac{\left|\mathbf{h}_i^\dagger \mathbf{v}_j\right|^2}{\sum_{m=j+1}^{K} \left|\mathbf{h}_i^\dagger \mathbf{v}_m\right|^2 + \sigma^2}, \ 1 \leq j \leq i-1. \tag{3}$$

When $\min\{\mathrm{SINR}_j^j, \mathrm{SINR}_i^j\} \geq \gamma_j$, U_i can successfully decode the signal of U_j, and then can subtract it from the superposed signal, where γ_j is the SINR threshold required for decoding the information of U_j. After removing all signals from users before U_i, the received SINR of U_i can be denoted as

$$\mathrm{SINR}_i^i = \frac{\left|\mathbf{h}_i^\dagger \mathbf{v}_i\right|^2}{\sum_{j=i+1}^{K} \left|\mathbf{h}_i^\dagger \mathbf{v}_j\right|^2 + \sigma^2}, \ 1 \leq i \leq K-1. \tag{4}$$

For $i = K$, the decoding signal-to-noise ratio (SNR) of U_K can be expressed as

$$\mathrm{SNR}_K^K = \left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2 / \sigma^2, \tag{5}$$

if the other users' signals can be removed correctly.

From the above SIC decoding procedure, we can see that each user will receive the superposed signals from all users, and it has to decode the messages of the other users with the weaker channel strength before recovering its own message. This is a risk to the privacy of these users. In particular, if U_1 is the private user that has the weakest channel, all the other users can recover its message before decoding their own. On the other hand, if U_K is the private user that has the strongest channel, its information will be hidden to the other users with conventional SIC decoding order. In this paper, to guarantee the private transmission of an arbitrary user in NOMA systems, we adopt a novel SIC decoding order based on the joint beamforming optimization in the following subsection, which also includes transmit power information.

B. A New Decoding Order

Note that we treat U_k as the only private user in the rest of the paper. To ensure the privacy of the kth user, a novel decoding order for the SIC receivers is adopted in this paper. Unlike conventional NOMA, the decoding order of messages at each user is different when the privacy is considered. Specifically, to protect the privacy of a certain user, we introduce the transmit beamforming vector to make the received power of the private user the largest at its own receiver, and the weakest at other users' receivers. The remaining decoding order is consistent with conventional NOMA. To this end, the decoding order based on joint transmit beamforming and power allocation can be updated as

$$\begin{cases} \left|\mathbf{h}_1^\dagger \mathbf{v}_k\right|^2 \leq \left|\mathbf{h}_1^\dagger \mathbf{v}_K\right|^2 \leq \cdots \leq \left|\mathbf{h}_1^\dagger \mathbf{v}_1\right|^2, \\ \quad \cdots\cdots \\ \left|\mathbf{h}_k^\dagger \mathbf{v}_K\right|^2 \leq \cdots \leq \left|\mathbf{h}_k^\dagger \mathbf{v}_{k+1}\right|^2 \leq \left|\mathbf{h}_k^\dagger \mathbf{v}_{k-1}\right|^2 \leq \cdots \leq \left|\mathbf{h}_k^\dagger \mathbf{v}_1\right|^2 \leq \left|\mathbf{h}_k^\dagger \mathbf{v}_k\right|^2, \\ \quad \cdots\cdots \\ \left|\mathbf{h}_K^\dagger \mathbf{v}_k\right|^2 \leq \left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2 \leq \cdots \leq \left|\mathbf{h}_K^\dagger \mathbf{v}_1\right|^2, \ k \in \mathcal{K}. \end{cases} \tag{6}$$

[1]The proposed scheme can be extended to the case where more than one users require private transmission with more antennas at the BS, which is out of the scope of this paper.

which provides a great benefit to the privacy protection, because the weakest received signal strength of the private user at other users will reduce the eavesdropping rate, and the strongest signal strength of the private user at its own receiver will improve its transmission rate. Thus, the security of U_k can be guaranteed even when $\mathbf{v}_k$ is available at other users, due to the single antenna equipped and extremely low received power of U_k at other users.

In (6), higher received signal power of a specific user at a certain receiver does not mean higher transmit power for this user, due to the fact that the received signal power is not only determined by the transmit power and channel fading, but also by the transmit beamforming. In addition, unlike conventional single-antenna NOMA systems, joint transmit beamforming optimization can be leveraged to achieve the novel decoding order in (6), which is reasonable to realize when multiple antennas are equipped at the BS.

Using the decoding order in (6), the received SINR at U_k can be denoted as

$$\text{SINR}_k^k = \frac{\left|\mathbf{h}_k^\dagger \mathbf{v}_k\right|^2}{\sum\limits_{j=1,j\neq k}^{K}\left|\mathbf{h}_k^\dagger \mathbf{v}_j\right|^2+\sigma^2}. \tag{7}$$

Subsequently, the received SINR of U_j decoded at U_n can be given as

$$\text{SINR}_n^j=\frac{\left|\mathbf{h}_n^\dagger \mathbf{v}_j\right|^2}{\sum\limits_{m=j+1,m\neq k}^{K}\left|\mathbf{h}_n^\dagger \mathbf{v}_m\right|^2+\left|\mathbf{h}_n^\dagger \mathbf{v}_k\right|^2+\sigma^2}, j<n\leq K, n\neq k. \tag{8}$$

When SIC has been perfectly performed at U_j, its received SINR can be expressed as

$$\text{SINR}_j^j=\begin{cases} \dfrac{\left|\mathbf{h}_j^\dagger \mathbf{v}_j\right|^2}{\sum\limits_{m=j+1,m\neq k}^{K}\left|\mathbf{h}_j^\dagger \mathbf{v}_m\right|^2+\left|\mathbf{h}_j^\dagger \mathbf{v}_k\right|^2+\sigma^2}, & j\in\mathcal{K}\backslash\{k,K\}, \\ \dfrac{\left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2}{\left|\mathbf{h}_K^\dagger \mathbf{v}_k\right|^2+\sigma^2}, & j=K, j\neq k. \end{cases} \tag{9}$$

It is worth noticing that the underlying principle for perfect SIC should be satisfied, in order to eliminate the interference before decoding the desired message. This means the transmission rate for U_j cannot exceed the minimum between the achievable rate of U_j at $U_n (n>j, n\neq k)$ and that at U_j itself, for removing the message of U_j from the superposed signal received at U_n, i.e., the achievable rate of U_j should meet the condition $R_j \leq \min\{R_n^j, R_j^j\}$. Hence, combining (8) and (9), the achievable received SINR at U_j can be denoted as

$$\text{SINR}_j = \begin{cases} \min\limits_{j\leq n\leq K, n\neq k}\{\text{SINR}_n^j\}, & j\in\mathcal{K}\backslash\{k,K\}, \\ \text{SINR}_j^j, & j=K, j\neq k. \end{cases} \tag{10}$$

When $\text{SINR}_j \geq \gamma_j$, the interference caused by U_j at U_n can be perfectly removed via SIC before decoding its own message.

Next, we consider the eavesdropped SINR of the message for U_k at the other $(K-1)$ users. Due to the fact that the unintended signals at other users are difficult to remove by SIC, the eavesdropped SINR of U_k at U_m can be written as

$$\text{SINR}_m^k = \begin{cases} \dfrac{\left|\mathbf{h}_m^\dagger \mathbf{v}_k\right|^2}{\sum\limits_{q=m+1,q\neq k}^{K}\left|\mathbf{h}_m^\dagger \mathbf{v}_q\right|^2+\sigma^2}, & m\in\mathcal{K}\backslash\{k,K\}, \\ \left|\mathbf{h}_K^\dagger \mathbf{v}_k\right|^2/\sigma^2, & m=K, m\neq k. \end{cases} \tag{11}$$

To further enhance the privacy of information for a specific user, we propose a secrecy rate maximization (SRM) scheme based on beamforming optimization in the next section, which aims to maximize the private user's secrecy rate, on the premise that the QoS demands of the other users and the decoding order constraints in (6) are satisfied.

III. Secrecy Rate Maximization

In this section, the formulation of the SRM scheme is first presented and then, transformed into a convex problem via convex approximations. Finally, an iterative algorithm based on CCCP is proposed to obtain the Karush-Kuhn-Tucker (KKT) solution.

A. Problem Formulation

In the SRM scheme, we maximize the secrecy rate of the private user by optimizing the transmit beamforming design, with the constraints on the other users' QoS requirements and the decoding order. Based on (7) and (11), the secrecy rate of the kth user R_{sk} can be given by

$$R_{sk}=\left[\log_2\left(1+\text{SINR}_k^k\right)-\log_2\left(1+\max_{m\in\mathcal{K},m\neq k}\left\{\text{SINR}_m^k\right\}\right)\right]^+, \tag{12}$$

where $[x]^+ \triangleq \max(x,0)$.

In order to optimize the security performance of the private user and guarantee the QoS of other users, the optimization problem can be formulated as

$$\begin{aligned} \max_{\mathbf{v}_i}\ & R_{sk} \\ s.t.\ & \text{SINR}_j \geq \gamma_j,\ \ j\in\mathcal{K}\backslash\{k\}, \\ & (6) \text{ and } \sum_{i=1}^{K}\|\mathbf{v}_i\|^2 \leq P_{BS},\ i\in\mathcal{K}, \end{aligned} \tag{13}$$

where γ_j represents the received SINR threshold at U_j, and SINR_j can be found in (10). P_{BS} is the total transmit power of the BS. By solving (13), the security performance of U_k can be optimized via maximizing the transmission rate and minimizing the eavesdropping rate, while the QoS requirements of other users are satisfied as well. In addition, we assume that the BS has the knowledge of CSI from all the users in (13), including the potential eavesdroppers, which is also a reasonable assumption for conventional NOMA systems.

Note that, the optimization problem in (13) is not convex and its global optimum is difficult to obtain, due to the fact that the objective function and most constraints in (13) are non-convex. Consequently, in the next subsection, we first convert (13) into a convex one via approximations before solving it.

B. Approximate Transformations

The problem (13) is non-convex, and it is difficult to solve it directly. However, the original problem can be first transformed via CCCP, and then, an iterative algorithm can be presented to obtain its KKT solution. To do this, we first introduce the auxiliary variables t_1 and t_2 as

$$\begin{aligned} \max_{\mathbf{v}_i} \ & \log_2(t_1 t_2) \\ s.t. \ & 1+\text{SINR}_k^k \geq t_1, \\ & 1+\text{SINR}_m^k \leq \frac{1}{t_2}, \\ & \text{SINR}_j \geq \gamma_j, \\ & (6) \text{ and } \sum_{i=1}^{K} \|\mathbf{v}_i\|^2 \leq P_{BS}. \end{aligned} \tag{14}$$

Substituting (7), (10) and (11) into (14), it can be equivalently rewritten as

$$\max_{\mathbf{v}_i,t_1,t_2} \ \log_2(t_1 t_2) \tag{15a}$$

$$s.t. \ 1+\frac{\left|\mathbf{h}_k^\dagger \mathbf{v}_k\right|^2}{\sum_{j=1,j\neq k}^{K}\left|\mathbf{h}_k^\dagger \mathbf{v}_j\right|^2+\sigma^2} \geq t_1, \tag{15b}$$

$$\begin{cases} 1+\dfrac{\left|\mathbf{h}_m^\dagger \mathbf{v}_k\right|^2}{\sum_{q=m+1,q\neq k}^{K}\left|\mathbf{h}_m^\dagger \mathbf{v}_q\right|^2+\sigma^2} \leq \dfrac{1}{t_2}, m\in\mathcal{K}\backslash\{k,K\}, \\ 1+\dfrac{\left|\mathbf{h}_K^\dagger \mathbf{v}_k\right|^2}{\sigma^2} \leq \dfrac{1}{t_2}, \ m=K, m\neq k, \end{cases} \tag{15c}$$

$$\begin{cases} \dfrac{\left|\mathbf{h}_j^\dagger \mathbf{v}_j\right|^2}{\sum_{m=j+1,m\neq k}^{K}\left|\mathbf{h}_j^\dagger \mathbf{v}_m\right|^2+\left|\mathbf{h}_j^\dagger \mathbf{v}_k\right|^2+\sigma^2} \geq \gamma_j, \\ \dfrac{\left|\mathbf{h}_n^\dagger \mathbf{v}_j\right|^2}{\sum_{m=j+1,m\neq k}^{K}\left|\mathbf{h}_n^\dagger \mathbf{v}_m\right|^2+\left|\mathbf{h}_n^\dagger \mathbf{v}_k\right|^2+\sigma^2} \geq \gamma_j, \\ j\in\mathcal{K}\backslash\{k,K\}, j<n\leq K, n\neq k, \end{cases} \tag{15d}$$

$$\frac{\left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2}{\left|\mathbf{h}_K^\dagger \mathbf{v}_k\right|^2+\sigma^2} \geq \gamma_K, \tag{15e}$$

$$(6) \text{ and } \sum_{i=1}^{K} \|\mathbf{v}_i\|^2 \leq P_{BS}. \tag{15f}$$

Observe that (15a) is non-decreasing. Thus, it is equivalent to maximizing the geometric mean between t_1 and t_2, i.e., $\sqrt{t_1 t_2}$, which is concave and increasing. Based on this, problem (15) can be changed into problem (16).

For (16b), we can recast it as a second-order cone (SOC) constraint where the hyperbolic constraint $w^2 \leq xy$ $(x \geq 0, y \geq 0)$ can be transformed into the form of $\|[2w, x-y]^\dagger\| \leq x+y$. Thus, (16b) can be reformulated as $\left\|[2t,(t_1-t_2)]^\dagger\right\| \leq t_1+t_2$. However, it's worth noting that (16) is still non-convex in that both sides of the inequality in (16c)-(16f) are convex functions. Moreover, a series of inequalities in (6) also lead to the non-convexity of (16). To deal with them, we leverage the idea of CCCP to make prudent approximations and convert them into convex ones. Before the conversion, we first recall some conclusions in [43] as Lemma 1.

$$\max_{\mathbf{v}_i,t_1,t_2,t} \ t \tag{16a}$$

$$s.t. \ t_1 t_2 \geq t^2, \tag{16b}$$

$$\sum_{j\neq k}^{K}\left|\mathbf{h}_k^\dagger \mathbf{v}_j\right|^2+\sigma^2 \leq \frac{\left|\mathbf{h}_k^\dagger \mathbf{v}_k\right|^2}{t_1-1}, \tag{16c}$$

$$\begin{cases} \sum_{q=m+1,q\neq k}^{K}\left|\mathbf{h}_m^\dagger \mathbf{v}_q\right|^2+\left|\mathbf{h}_m^\dagger \mathbf{v}_k\right|^2+\sigma^2 \\ \qquad \leq \dfrac{\sum_{q=m+1,q\neq k}^{K}\left|\mathbf{h}_m^\dagger \mathbf{v}_q\right|^2+\sigma^2}{t_2}, \\ \left|\mathbf{h}_K^\dagger \mathbf{v}_k\right|^2+\sigma^2 \leq \dfrac{\sigma^2}{t_2}, m\in\mathcal{K}\backslash\{k,K\}, \end{cases} \tag{16d}$$

$$\begin{cases} \sum_{m=j+1,m\neq k}^{K}\left|\mathbf{h}_j^\dagger \mathbf{v}_m\right|^2+\left|\mathbf{h}_j^\dagger \mathbf{v}_k\right|^2+\sigma^2 \leq \dfrac{\left|\mathbf{h}_j^\dagger \mathbf{v}_j\right|^2}{\gamma_j}, \\ \sum_{m=j+1,m\neq k}^{K}\left|\mathbf{h}_n^\dagger \mathbf{v}_m\right|^2+\left|\mathbf{h}_n^\dagger \mathbf{v}_k\right|^2+\sigma^2 \leq \dfrac{\left|\mathbf{h}_n^\dagger \mathbf{v}_j\right|^2}{\gamma_j}, \\ j\in\mathcal{K}\backslash\{k,K\}, j<n\leq K, n\neq k, \end{cases} \tag{16e}$$

$$\left|\mathbf{h}_K^\dagger \mathbf{v}_k\right|^2+\sigma^2 \leq \left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2/\gamma_K, \tag{16f}$$

$$(6) \text{ and } \sum_{i=1}^{K} \|\mathbf{v}_i\|^2 \leq P_{BS}. \tag{16g}$$

Lemma 1: A differentiable convex function $f(x)$ can be approximated by its corresponding tangential function $g\left(x,x^{(m)}\right)$ at the point of tangency $x^{(m)}$, which can also be deemed as the first-order Taylor expansion around $x^{(m)}$ as

$$f(x) \geq g\left(x,x^{(m)}\right) = f\left(x^{(m)}\right)+\bigtriangledown f\left(x^{(m)}\right)^\dagger\left(x-x^{(m)}\right), \tag{17}$$

where the equality holds when $x=x^{(m)}$. ■

Based on Lemma 1, we can transform (16c)-(16f) into convex ones using the following presented proposition.

Proposition 1: For notational convenience, we define

$$F_1(\mathbf{v}_k,t_1) = \left|\mathbf{h}_k^\dagger \mathbf{v}_k\right|^2/(t_1-1), \tag{18a}$$

$$F_{2m}(\mathbf{v}_q,t_2) = \frac{\sum_{q=m+1,q\neq k}^{K}\left|\mathbf{h}_m^\dagger \mathbf{v}_q\right|^2+\sigma^2}{t_2}, m\in\mathcal{K}\backslash\{k,K\},$$

$$F_{2K}(t_2) = \frac{\sigma^2}{t_2}, \tag{18b}$$

$$\begin{cases} F_{3j}(\mathbf{v}_j) = \left|\mathbf{h}_j^\dagger \mathbf{v}_j\right|^2/\gamma_j, \\ F_{3n}(\mathbf{v}_j) = \left|\mathbf{h}_n^\dagger \mathbf{v}_j\right|^2/\gamma_j, j\in\mathcal{K}\backslash\{k\}, j<n\leq K, n\neq k, \end{cases} \tag{18c}$$

and their corresponding first-order Taylor approximation over

a certain point can be calculated as

$$\mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t_1}\right)=\frac{2Re\left(\mathbf{h}_k^\dagger\bar{\mathbf{v}}_k\mathbf{v}_k^\dagger\mathbf{h}_k\right)}{\bar{t_1}-1}-\frac{Re\left(\mathbf{h}_k^\dagger\bar{\mathbf{v}}_k\bar{\mathbf{v}}_k^\dagger\mathbf{h}_k\right)}{\left(\bar{t_1}-1\right)^2}\left(t_1-1\right). \tag{19a}$$

$$\mathcal{L}_{2m}\left(\mathbf{v}_q,t_2,\bar{\mathbf{v}}_q,\bar{t_2}\right)=\frac{\sum\limits_{q=m+1,q\neq k}^{K}2Re\left(\mathbf{h}_m^\dagger\bar{\mathbf{v}}_q\mathbf{v}_q^\dagger\mathbf{h}_m\right)}{\bar{t_2}}-\frac{\sum\limits_{q=m+1,q\neq k}^{K}Re\left(\mathbf{h}_m^\dagger\bar{\mathbf{v}}_q\bar{\mathbf{v}}_q^\dagger\mathbf{h}_m\right)}{\bar{t_2}^2}t_2+\frac{\sigma^2}{\bar{t_2}^2}\left(2\bar{t_2}-t_2\right),$$

$$\mathcal{L}_{2K}\left(t_2,\bar{t_2}\right)=\frac{\sigma^2}{\bar{t_2}^2}\left(2\bar{t_2}-t_2\right), \tag{19b}$$

$$\begin{cases}\mathcal{L}_{3j}\left(\mathbf{v}_j,\bar{\mathbf{v}}_j\right)=\left(2Re\left(\mathbf{h}_j^\dagger\mathbf{v}_j\bar{\mathbf{v}}_j^\dagger\mathbf{h}_j\right)-Re\left(\mathbf{h}_j^\dagger\bar{\mathbf{v}}_j\bar{\mathbf{v}}_j^\dagger\mathbf{h}_j\right)\right)/\gamma_j,\\ \mathcal{L}_{3n}\left(\mathbf{v}_j,\bar{\mathbf{v}}_j\right)=\left(2Re\left(\mathbf{h}_n^\dagger\mathbf{v}_j\bar{\mathbf{v}}_j^\dagger\mathbf{h}_n\right)-Re\left(\mathbf{h}_n^\dagger\bar{\mathbf{v}}_j\bar{\mathbf{v}}_j^\dagger\mathbf{h}_n\right)\right)/\gamma_j.\end{cases} \tag{19c}$$

By using (17) and (19), constraints (16c)-(16f) can be approximated as convex ones.

Proof: In (18a), the function is convex in a quadratic-over-linear form. According to Lemma 1, it satisfies

$$\begin{aligned}&F_1(\mathbf{v}_k,t_1)\geq F_1(\bar{\mathbf{v}}_k,\bar{t_1})+\bigtriangledown_{t_1}F_1|_{(\bar{\mathbf{v}}_k,\bar{t_1})}\left(t_1-\bar{t_1}\right)\\&+2Re\left(\bigtriangledown_{\mathbf{v}_k}F_1|_{(\bar{\mathbf{v}}_k,\bar{t_1})}(\mathbf{v}_k-\bar{\mathbf{v}}_k)\right)\triangleq\mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t_1}\right),\end{aligned} \tag{20}$$

where $\mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t_1}\right)$ can be derived as

$$\begin{aligned}\mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t_1}\right)=&\frac{\mathbf{h}_k^\dagger\bar{\mathbf{v}}_k\bar{\mathbf{v}}_k^\dagger\mathbf{h}_k}{\bar{t_1}-1}-\frac{\mathbf{h}_k^\dagger\bar{\mathbf{v}}_k\bar{\mathbf{v}}_k^\dagger\mathbf{h}_k}{(\bar{t_1}-1)^2}\left(t_1-\bar{t_1}\right)\\&+2Re\left(\frac{\bar{\mathbf{v}}_k^\dagger\mathbf{h}_k\mathbf{h}_k^\dagger}{\bar{t_1}-1}\left(\mathbf{v}_k-\bar{\mathbf{v}}_k\right)\right)=(19a).\end{aligned} \tag{21}$$

The second equality in (21) can hold owing to the fact that $\bar{\mathbf{v}}_k\bar{\mathbf{v}}_k^\dagger\succeq 0$ and $\mathbf{h}_k\mathbf{h}_k^\dagger\succeq 0$. Similarly, the same operation can be adapted to the functions (18b) and (18c), and their corresponding first order Taylor series can be obtained as (19b) and (19c), respectively.

Substituting the right sides of the constraints (16c)-(16f) with the formulas in (19), we can notice that the original norm-squared functions have been converted into linear functions. Consequently, the constraints (16c)-(16f) become convex through the above approximations. In addition, it's worth noting that the approximation is compact with the conditions $\bar{\mathbf{v}}_k=\mathbf{v}_k$, $\bar{t_1}=t_1$ and $\bar{t_2}=t_2$ satisfied, which can be achieved by an iterative algorithm based on the principle of CCCP that we will introduce later. ∎

Finally, for the non-convex condition (6), the decoding order for U_k is equivalent to

$$\mathcal{S}_k=\begin{cases}\left|\mathbf{h}_k^\dagger\mathbf{v}_K\right|^2\leq\min\left\{\left|\mathbf{h}_k^\dagger\mathbf{v}_{K-1}\right|^2,\ldots,\left|\mathbf{h}_k^\dagger\mathbf{v}_1\right|^2,\left|\mathbf{h}_k^\dagger\mathbf{v}_k\right|^2\right\},\\ \left|\mathbf{h}_k^\dagger\mathbf{v}_{K-1}\right|^2\leq\min\left\{\left|\mathbf{h}_k^\dagger\mathbf{v}_{K-2}\right|^2,\ldots,\left|\mathbf{h}_k^\dagger\mathbf{v}_1\right|^2,\left|\mathbf{h}_k^\dagger\mathbf{v}_k\right|^2\right\},\\ \ldots,\\ \left|\mathbf{h}_k^\dagger\mathbf{v}_1\right|^2\leq\left|\mathbf{h}_k^\dagger\mathbf{v}_k\right|^2.\end{cases} \tag{22}$$

Obviously, the right sides of the inequalities in (22) are the quadratic functions with variable $\mathbf{v}_k$, and thus, we can utilize the same method as above to linearize them. Particularly, we define

$$\Gamma_{ki}\left(\mathbf{v}_i\right)=\left|\mathbf{h}_k^\dagger\mathbf{v}_i\right|^2. \tag{23}$$

Then, the first-order Taylor approximation to (23) can be denoted as

$$\begin{aligned}\Gamma_{ki}(\mathbf{v}_i,\bar{\mathbf{v}}_i)\geq&\left|\bar{\mathbf{v}}_i^\dagger\mathbf{h}_k\right|^2+2Re\left(\bar{\mathbf{v}}_i^\dagger\mathbf{h}_k\mathbf{h}_k^\dagger(\mathbf{v}_i-\bar{\mathbf{v}}_i)\right)\\\geq&\bar{\mathbf{v}}_i^\dagger\mathbf{h}_k\mathbf{h}_k^\dagger\bar{\mathbf{v}}_i+2Re\left(\bar{\mathbf{v}}_i^\dagger\mathbf{h}_k\mathbf{h}_k^\dagger\mathbf{v}_i\right)-2Re\left(\bar{\mathbf{v}}_i^\dagger\mathbf{h}_k\mathbf{h}_k^\dagger\bar{\mathbf{v}}_i\right)\\\geq&2Re\left(\bar{\mathbf{v}}_i^\dagger\mathbf{h}_k\mathbf{h}_k^\dagger\mathbf{v}_i\right)-Re\left(\bar{\mathbf{v}}_i^\dagger\mathbf{h}_k\mathbf{h}_k^\dagger\bar{\mathbf{v}}_i\right)=\mathcal{L}_{ki}\left(\mathbf{v}_i,\bar{\mathbf{v}}_i\right).\end{aligned} \tag{24}$$

Using (24), the constraint in (22) can be transformed as

$$\widetilde{\mathcal{S}}_k=\begin{cases}\left|\mathbf{h}_k^\dagger\mathbf{v}_K\right|^2\leq\min_{i\in[1,K-1]}\mathcal{L}_{ki}\left(\mathbf{v}_i,\bar{\mathbf{v}}_i\right),\\ \left|\mathbf{h}_k^\dagger\mathbf{v}_{K-1}\right|^2\leq\min_{i\in[1,K-2]}\mathcal{L}_{ki}\left(\mathbf{v}_i,\bar{\mathbf{v}}_i\right),\\ \ldots,\\ \left|\mathbf{h}_k^\dagger\mathbf{v}_1\right|^2\leq\mathcal{L}_{kk}\left(\mathbf{v}_k,\bar{\mathbf{v}}_k\right),\end{cases} \tag{25}$$

which is convex and easy to solve. Similarly, other orders can be transformed, and we can use $\mathcal{S}\triangleq\left(\widetilde{\mathcal{S}}_1,\widetilde{\mathcal{S}}_2,\ldots,\widetilde{\mathcal{S}}_K\right)$ to represent the converted form of the constraint (6).

With all the above transformations, (13) can be reformulated as a solvable convex one. Furthermore, to reduce the computational complexity, the problem (13) is rewritten as a second-order cone programming (SOCP) problem [44], [45], which can be expressed as (26) at the top of the next page.

C. Proposed Algorithm

Based on the above transformations, the problem in (26) can be solved using the existing toolboxes, such as CVX. However, the optimal solution of (26) is not the same as that of problem (13), due to the transformations. Thus, we propose an iterative algorithm based on the idea of CCCP, to obtain the KKT values of (13). Details of the algorithm are summarized as Algorithm 1.

Algorithm 1 CCCP-based Algorithm for Problem (13)

1: Initialization: Randomly generate the feasible set of initial values $(\bar{\mathbf{v}}_i,\bar{t}_1,\bar{t}_2)$ for the problem (26). Set the maximum number of iterations as R, and set the initial index of iterations as $r=1$.
2: **Repeat**
3: Solve the SOCP problem (26) by CVX, and obtain the set of optimum values $(\mathbf{v}_i^*,t_1^*,t_2^*)$.
4: Substitute the current set of optimal values for the previous set of values, i.e., $(\bar{\mathbf{v}}_i,\bar{t}_1,\bar{t}_2)=(\mathbf{v}_i^*,t_1^*,t_2^*)$.
5: Update: $r=r+1$.
6: **Until** $r=R$ or convergence.
7: Output: $\mathbf{v}_i^*$, $\forall i\in\mathcal{K}$.

The feasibility of Algorithm 1 for the original problem (13) is proved in Proposition 2.

$$\max_{\mathbf{v}_i} \ t \tag{26a}$$

$$s.t. \ \ \left\|[2t,(t_1-t_2)]^\dagger\right\| \le t_1+t_2, \tag{26b}$$

$$\left\|\left[2\mathbf{h}_k^\dagger\mathbf{v}_1,\ldots,2\mathbf{h}_k^\dagger\mathbf{v}_{k-1},2\mathbf{h}_k^\dagger\mathbf{v}_{k+1},\ldots,2\mathbf{h}_k^\dagger\mathbf{v}_K,2\sigma,(\mathcal{L}_1-1)\right]^\dagger\right\| \le \mathcal{L}_1+1, \tag{26c}$$

$$\begin{cases} \left\|\left[2\mathbf{h}_m^\dagger\mathbf{v}_{m+1},\ldots,2\mathbf{h}_m^\dagger\mathbf{v}_{k-1},2\mathbf{h}_m^\dagger\mathbf{v}_{k+1},\ldots 2\mathbf{h}_m^\dagger\mathbf{v}_K,2\mathbf{h}_m^\dagger\mathbf{v}_k,2\sigma,(\mathcal{L}_{2m}-1)\right]^\dagger\right\| \le \mathcal{L}_{2m}+1,\ m\in\mathcal{K}\backslash\{k,K\}, \\ \left\|\left[2\mathbf{h}_K^\dagger\mathbf{v}_k,2\sigma,(\mathcal{L}_{2K}-1)\right]^\dagger\right\| \le \mathcal{L}_{2K}+1,\ m=K,m\ne k, \end{cases} \tag{26d}$$

$$\begin{cases} \left\|\left[2\mathbf{h}_j^\dagger\mathbf{v}_{j+1},\ldots,2\mathbf{h}_j^\dagger\mathbf{v}_{k-1},2\mathbf{h}_j^\dagger\mathbf{v}_{k+1},\ldots,2\mathbf{h}_j^\dagger\mathbf{v}_K,2\mathbf{h}_j^\dagger\mathbf{v}_k,2\sigma,(\mathcal{L}_{3j}-1)\right]^\dagger\right\| \le \mathcal{L}_{3j}+1,\ j\in\mathcal{K}\backslash\{k,K\}, \\ \left\|\left[2\mathbf{h}_n^\dagger\mathbf{v}_{j+1},\ldots,2\mathbf{h}_n^\dagger\mathbf{v}_{k-1},2\mathbf{h}_n^\dagger\mathbf{v}_{k+1},\ldots,2\mathbf{h}_n^\dagger\mathbf{v}_K,2\mathbf{h}_n^\dagger\mathbf{v}_k,2\sigma,(\mathcal{L}_{3n}-1)\right]^\dagger\right\| \le \mathcal{L}_{3n}+1,\ j<n\le K,n\ne k, \end{cases} \tag{26e}$$

$$\left\|\left[2\mathbf{h}_K^\dagger\mathbf{v}_k,2\sigma,(\mathcal{L}_{3K}-1)\right]^\dagger\right\| \le \mathcal{L}_{3K}+1, \tag{26f}$$

$$\mathcal{S} \text{ and } \left\|\left[\mathbf{v}_1^\dagger,\mathbf{v}_2^\dagger,\ldots,\mathbf{v}_K^\dagger\right]^\dagger\right\| \le \sqrt{P_{BS}}. \tag{26g}$$

Proposition 2: For Algorithm 1, the feasible set of problem (26) is within that of the original problem (13).

Proof: Without loss of generality, we mainly analyze the transformation of the constraint (16c). Considering the principle of CCCP, two important properties can be satisfied between the original function $F_1(\mathbf{v}_k,t_1)$ and the surrogate function $\mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t}_1\right)$, i.e.,

$$F_1(\mathbf{v}_k,t_1) \ge \mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t}_1\right) \tag{27a}$$

$$F_1(\mathbf{v}_k,t_1)|_{(\bar{\mathbf{v}}_k,\bar{t}_1)} = \mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t}_1\right)|_{(\bar{\mathbf{v}}_k,\bar{t}_1)}. \tag{27b}$$

For brevity, we define

$$g(\mathbf{v}_j) = \sum_{j\ne k}^{K}\left|\mathbf{h}_k^\dagger\mathbf{v}_j\right|^2+\sigma^2, \tag{28}$$

and the constraint (16c) can be rewritten as

$$g(\mathbf{v}_j)-F_1(\mathbf{v}_k,t_1)\le 0. \tag{29}$$

Apparently, the following inequality can be satisfied in terms of (27a).

$$g(\mathbf{v}_j)-F_1(\mathbf{v}_k,t_1) \le g(\mathbf{v}_j)-\mathcal{L}_1\left(\mathbf{v}_k,t_1,\bar{\mathbf{v}}_k,\bar{t}_1\right)\le 0. \tag{30}$$

Therefore, in the nth iteration, (29) can be equivalent to

$$\begin{aligned} &g\left(\mathbf{v}_j^{(n)}\right)-F_1\left(\mathbf{v}_k^{(n)},t_1^{(n)}\right)\le \\ &\qquad g\left(\mathbf{v}_j^{(n)}\right)-\mathcal{L}_1\left(\mathbf{v}_k^{(n)},t_1^{(n)},\mathbf{v}_k^{(n-1)},t_1^{(n-1)}\right)\le 0, \end{aligned} \tag{31}$$

where the equality can be achieved with $\mathbf{v}_k^{(n)}=\mathbf{v}_k^{(n-1)}$ and $t_1^{(n)}=t_1^{(n-1)}$ met, i.e., Algorithm 1 is convergent, which will be illustrated later.

The conclusion in (31) can be extended to all the other constraints that adopt the same approximation. Hence, we can conclude that the feasible set of (26) is a subset of that of the original problem (13), which indicates that a local optimum value of the problem (13) can be obtained using (26). ■

In addition, it's worth noticing that Algorithm 1 is convergent based on results in [46], [47]. In particular, in each iteration, the value of the objective function tends to be no less than its value in the preceding iteration, which demonstrates that the secrecy rate will not be decreasing with the increasing number of iterations. Moreover, both the QoS requirements of other users and the power constraint limit the growth of secrecy rate, which guarantees the convergence of Algorithm 1. According to [17] and [46], a KKT solution to the problem (13) can be obtained via Algorithm 1.

IV. Zero-Forcing Based Scheme

In Section III, we presented the SRM scheme to maximize the secrecy rate of the private user in NOMA systems, with guaranteed QoS for the other users, which can be solved using Algorithm 1. Nevertheless, the privacy and security of the specific user can be further improved by zero-forcing its signal at other users with lower computational complexity, when adequate antennas are equipped at the BS. Thus, a ZF-based scheme is proposed in this section.

A. ZF-based Scheme

In the ZF-based scheme, we zero-force the signal of the private user at other users via the transmit beamforming design, and thus, the other users cannot even receive the private information to perform eavesdropping. In this case, the decoding order defined in Section II can be modified as

$$\begin{cases} 0=\left|\mathbf{h}_1^\dagger\mathbf{v}_k\right|^2\le\left|\mathbf{h}_1^\dagger\mathbf{v}_K\right|^2\le\cdots\le\left|\mathbf{h}_1^\dagger\mathbf{v}_{k+1}\right|^2 \\ \qquad\le\left|\mathbf{h}_1^\dagger\mathbf{v}_{k-1}\right|^2\le\cdots\le\left|\mathbf{h}_1^\dagger\mathbf{v}_1\right|^2, \\ \cdots \\ \left|\mathbf{h}_k^\dagger\mathbf{v}_K\right|^2\le\ldots\left|\mathbf{h}_k^\dagger\mathbf{v}_{k+1}\right|^2\le\left|\mathbf{h}_k^\dagger\mathbf{v}_{k-1}\right|^2 \\ \qquad\le\cdots\le\left|\mathbf{h}_k^\dagger\mathbf{v}_1\right|^2\le\left|\mathbf{h}_k^\dagger\mathbf{v}_k\right|^2, \\ \cdots \\ 0=\left|\mathbf{h}_K^\dagger\mathbf{v}_k\right|^2\le\left|\mathbf{h}_K^\dagger\mathbf{v}_K\right|^2\le\ldots\le\left|\mathbf{h}_K^\dagger\mathbf{v}_{k+1}\right|^2 \\ \qquad\le\left|\mathbf{h}_K^\dagger\mathbf{v}_{k-1}\right|^2\le\ldots\le\left|\mathbf{h}_K^\dagger\mathbf{v}_1\right|^2,\ k\in\mathcal{K}. \end{cases} \tag{32}$$

According to (32), the received SINR of U_j decoded at U_n can be expressed as

$$\text{SINR}_n^j = \frac{\left|\mathbf{h}_n^\dagger \mathbf{v}_j\right|^2}{\sum\limits_{m=j+1, m\neq k}^{K} \left|\mathbf{h}_n^\dagger \mathbf{v}_m\right|^2 + \sigma^2}, j < n \leq K, n \neq k. \quad (33)$$

Then, the received SINR of U_j can be denoted as follows when SIC is perfectly carried out at all users.

$$\text{SINR}_j^j = \begin{cases} \dfrac{\left|\mathbf{h}_j^\dagger \mathbf{v}_j\right|^2}{\sum\limits_{m=j+1, m\neq k}^{K} \left|\mathbf{h}_j^\dagger \mathbf{v}_m\right|^2 + \sigma^2}, & j \in \mathcal{K}\backslash\{k, K\} \\ \dfrac{\left|\mathbf{h}_K^\dagger \mathbf{v}_K\right|^2}{\sigma^2}, & j = K. \end{cases} \quad (34)$$

Similarly, the achievable received SINR of U_j and the private user U_k can be given the same as (10) and (7), respectively. Besides, it's worth noting that the eavesdropped SINR becomes zero in this case, which means that the information of the private user is not leaked to the other users. Hence, the private transmission of the specific user can be perfectly guaranteed.

To further enhance the performance of the private user, we aim to maximize its transmission rate with SINR constraints for the other users and zero-forcing restrictions satisfied, under the condition of the given power threshold and the SIC decoding order (32). To this end, the optimization problem can be formulated as

$$\max_{\mathbf{v}_i} \ \log_2\left(1 + \text{SINR}_k^k\right) \quad (35a)$$

$$s.t. \ \ \text{SINR}_j \geq \gamma_j, \ \ j \in \mathcal{K}\backslash\{k\}, \quad (35b)$$

$$\mathbf{h}_j^\dagger \mathbf{v}_k = 0, \ \ j \in \mathcal{K}\backslash\{k\}, \quad (35c)$$

$$(32) \text{ and } \sum_{i=1}^{K} \|\mathbf{v}_i\|^2 \leq P_{BS}. \quad (35d)$$

Note that problem (35) is not convex due to the non-concave objective function (35a) and non-convex constraints (35b) and (32). Moreover, the restriction (35c) cannot be held unless the condition in the subsequent Lemma 2 is satisfied, which means that zero-forcing can be performed only when adequate antennas are equipped at the BS.

Lemma 2: The constraint in (35c) can be satisfied only when $M \geq K$.

Proof: (35c) can be regarded as a set of homogeneous linear equations. It can be solved only if the number of variables is not smaller than the number of equations. Thus, we need to analyze the relationship between the numbers of variables and equations in (35c).

In the zero-forcing scheme, the information of the private user needs to be zero-forced at all the other users in the NOMA system. Thus, the number of equations in (35c) is given by

$$\mathcal{N}_e = K - 1. \quad (36)$$

The number of variables in (35c) can be calculated as

$$\mathcal{N}_v = M - 1. \quad (37)$$

Thus, let $\mathcal{N}_e \leq \mathcal{N}_v$, and we can obtain the inequality as

$$K - 1 \leq M - 1 \Rightarrow M \geq K. \quad (38)$$

With (38) satisfied, the constraint (35c) can be solved. ■

Although the signal of the private user can also be zero-forced at other users in conventional MISO networks without NOMA when $M \geq K$, in this paper, we aim to solve the privacy problem of the NOMA systems, instead of using NOMA to solve the privacy problem.

Considering the objective function (35a) and constraints (35b) and (32), we can transform them by employing the similar approximate method that has been used in Section III-B. As a result, the problem (35) can be transformed as (39) at the top of the next page, where $\mathbf{H}_k = [\mathbf{h}_1, \ldots, \mathbf{h}_{k-1}, \mathbf{h}_{k+1}, \ldots, \mathbf{h}_K] \in \mathbb{C}^{M\times(K-1)}$.

Note that the difference between the decoding order constraint $\mathcal{S}$ in (26) and $\mathcal{S}'$ in (39) is that the items $\mathbf{h}_j^\dagger \mathbf{v}_k$ ($j \in \mathcal{K}\backslash\{k\}$) are removed from the decoding order of all the users except U_k. In addition, the zero-forced constraints have no impact on the convexity of problem (39). Therefore, we can run Algorithm 1 to solve (39) iteratively to calculate the KKT solutions of the problem (35).

According to Lemma 2, we can know that the ZF-based scheme is infeasible if $M < K$. In this case, we can force the private information to be 0 at only some of the common users, or we can adopt the SRM scheme instead.

B. Comparison of Two Schemes

In Section III and IV-A, the SRM and ZF-based schemes are proposed to guarantee the secure transmission of the private user in MISO NOMA systems, respectively. Both have their own features, which are discussed as follows.

- *Feasibility*: In the ZF-based scheme, the signal of the private user can be zero-forced at all the other users only when the condition (38) derived in Lemma 2 is satisfied, i.e., the problem (35) is able to be solved with the inequality $M \geq K$ held. However, in the SRM scheme, the solutions of the problem (13) can be obtained, even in the case that the number of users is larger than that of transmit antennas, i.e., $M < K$. Hence, the SRM scheme is more flexible to be utilized, especially when the antennas of the BS are inadequate.
- *Performance*: From Lemma 2, we can know that the ZF-based scheme cannot be performed in the case of $M < K$, while the SRM scheme can still work. When $M \geq K$, these two schemes may achieve almost the same performance, and we tend to choose the ZF-based scheme considering the computational complexity.
- *Complexity*: According to [44], we can see that the computational complexity of the interior-point algorithm for SOCP relies on the number of constraints and variables and the dimensions of all the SOC constraints, which become lower in the ZF-based scheme than that in the SRM scheme. Namely, compared with problem (26), the number of constraints and variables and the total dimensions of all the SOC constraints in problem (39) can be significantly reduced due to the zero-forcing

$$\max_{\mathbf{v}_i} \ t \tag{39a}$$

$$s.t. \ \ \left\|[2t,(t_1-1)]^\dagger\right\| \le t_1+1, \tag{39b}$$

$$\left\|\left[2\mathbf{h}_k^\dagger\mathbf{v}_1,\ldots,2\mathbf{h}_k^\dagger\mathbf{v}_{k-1},2\mathbf{h}_k^\dagger\mathbf{v}_{k+1},\ldots,2\mathbf{h}_k^\dagger\mathbf{v}_K,2\sigma,(\mathcal{L}_1-1)\right]^\dagger\right\| \le \mathcal{L}_1+1, \tag{39c}$$

$$\begin{cases} \left\|\left[2\mathbf{h}_j^\dagger\mathbf{v}_{j+1},\ldots,2\mathbf{h}_j^\dagger\mathbf{v}_{k-1},2\mathbf{h}_j^\dagger\mathbf{v}_{k+1},\ldots,2\mathbf{h}_j^\dagger\mathbf{v}_K,2\sigma,(\mathcal{L}_{3j}-1)\right]^\dagger\right\| \le \mathcal{L}_{3j}+1, \ j\in\mathcal{K}\backslash\{k,K\}, \\ \left\|\left[2\mathbf{h}_n^\dagger\mathbf{v}_{j+1},\ldots,2\mathbf{h}_n^\dagger\mathbf{v}_{k-1},2\mathbf{h}_n^\dagger\mathbf{v}_{k+1},\ldots,2\mathbf{h}_n^\dagger\mathbf{v}_K,2\sigma,(\mathcal{L}_{3n}-1)\right]^\dagger\right\| \le \mathcal{L}_{3n}+1, \ j<n\le K, n\ne k, \end{cases} \tag{39d}$$

$$\left\|[2\sigma,(\mathcal{L}_{3K}-1)]^\dagger\right\| \le \mathcal{L}_{3K}+1, \tag{39e}$$

$$\mathbf{H}_k^\dagger\mathbf{v}_k=\mathbf{0}_{(K-1)\times 1} \ \text{ and } \ \mathcal{S}' \tag{39f}$$

$$\left\|\left[\mathbf{v}_1^\dagger,\mathbf{v}_2^\dagger,\ldots,\mathbf{v}_K^\dagger\right]^\dagger\right\| \le \sqrt{P_{BS}}. \tag{39g}$$

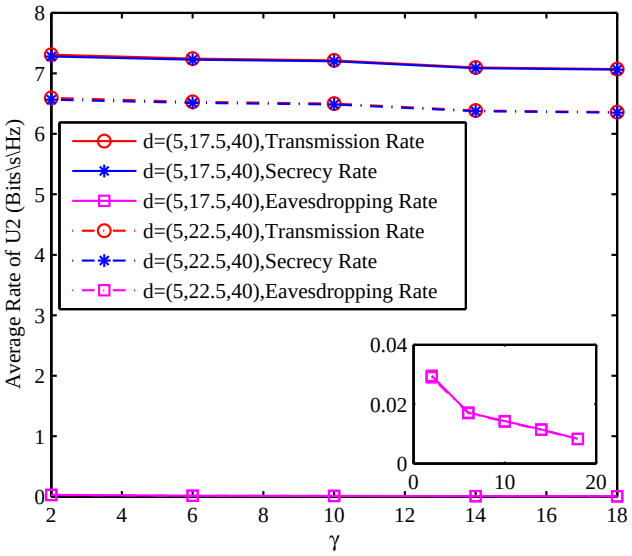


Fig. 2. Comparison of the secrecy rate, transmission rate and eavesdropping rate of the private user U_2 for the SRM scheme under different SINR thresholds of γ in a 3-user MISO NOMA network, with $d=(5,17.5,40)$ and $d=(5,22.5,40)$ considered, respectively.

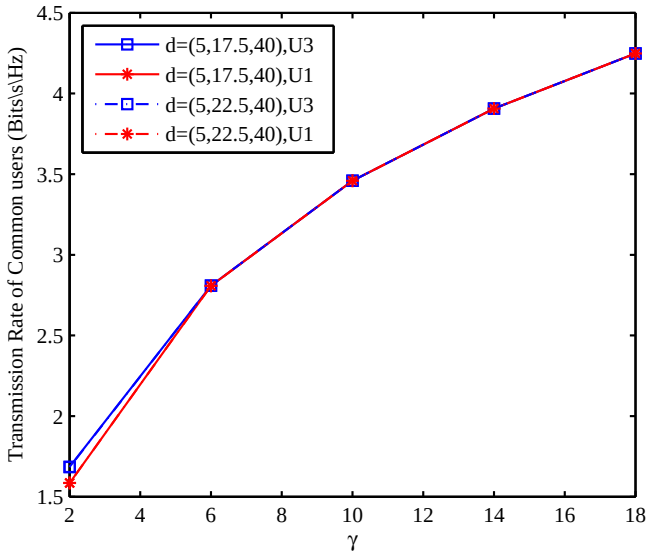


Fig. 3. Comparison of the transmission rate of other common users for the SRM scheme under different SINR thresholds of γ in a 3-user MISO NOMA network, with $d=(5,17.5,40)$ and $d=(5,22.5,40)$ considered, respectively.

operation. Thus, the computation complexity of the ZF-based scheme is lower than that of the SRM scheme. For the detail of complexity analysis, refer to Appendix A.

Therefore, when adequate antennas are available at the BS, the ZF-based scheme can be adopted to achieve perfect security for the private user with lower complexity. On the other hand, when antennas are inadequate at BS, i.e., the number of antennas at the BS is smaller than that of mobile users, the SRM scheme can be utilized with reliable performance.

V. Simulation Results and Discussions

Simulation results are presented to evaluate the performance of the two proposed schemes in this section. The distance between the BS and all the mobile users are defined via a set d for the locations of all the users as $d=(d_{U_K},d_{U_{K-1}},\ldots d_{U_1})$ in meters. In addition, we assume that all the channels are subject to slow Rayleigh block fading, and that the SINR constraints of common users are set to be equal, i.e., $\gamma_j=\gamma$. Also, set $\alpha=2$, $\sigma^2=-20$ dBm for all users.

First, we set U_2 as the private user, and the average rate of U_2 and the transmission rate of the other users for the SRM scheme are compared for different SINR thresholds of γ in Fig. 2 and Fig. 3, respectively, where $M=4$, $K=3$, and $P_{BS}=25$ dBm. From Fig. 2, we can observe that the secrecy rate, transmission rate and eavesdropping rate of U_2 all decrease when γ increases, due to the decrease of the transmit power allocated the private user with larger γ. In addition, both the secrecy rate and transmission rate of the private user will decrease as it becomes farther away from the BS, because the channel fading becomes more severe and the transmission rate is the main factor to determine the secrecy rate. From Fig. 3, we can see that the transmission rate of the other common users increases with γ, and their QoS demands can be always satisfied. Besides, the distance between the BS and the private user U_2 has little influence on the transmission rate of these

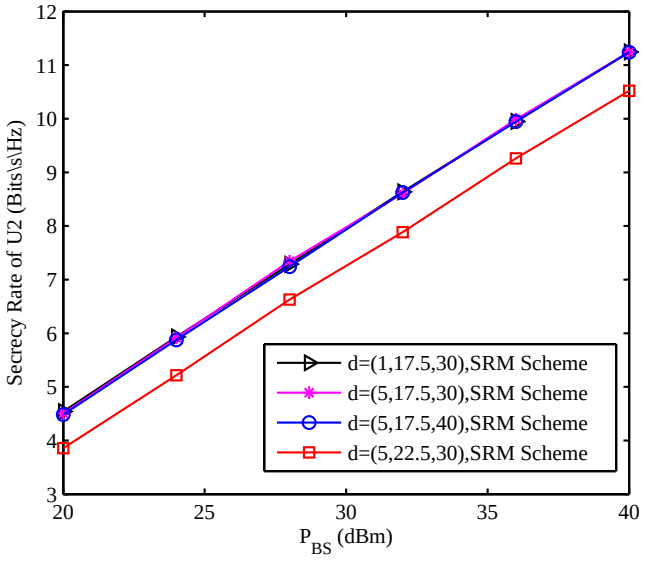


Fig. 4. Comparison of the secrecy rate of private user U_2 for the SRM scheme under different thresholds of P_{BS} in a 3-user MISO NOMA network. Four cases of $d = (1, 17.5, 30)$, $d = (5, 17.5, 30)$, $d = (5, 17.5, 40)$ and $d = (5, 22.5, 30)$ are considered.

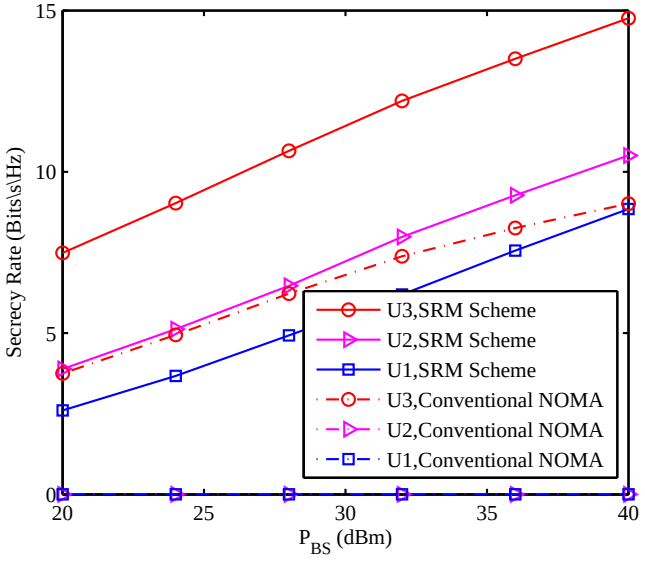


Fig. 5. Comparison of the secrecy rate of different users under varing thresholds of P_{BS} in a 3-user MISO NOMA network with both cases of the SRM scheme and conventional NOMA scheme considered.

users.

In Fig. 4, the impact of different transmit power thresholds P_{BS} on the secrecy rate in the SRM scheme is investigated, where $K = 3$, $M = 3$, $\gamma = 7$, and four cases, $d = (1, 17.5, 30)$, $d = (5, 17.5, 30)$, $d = (5, 17.5, 40)$ and $d = (5, 22.5, 30)$ are considered. U_2 is the private user. From the results, we can see that the secrecy rate of U_2 increases with P_{BS} at the BS, as the transmission rate of U_2 will become higher with higher transmit power. Besides, we can find that the secrecy rate of U2 is almost unchanged with a shorter distance between the BS and the other common users. In contrast, the secrecy rate of U2 will increase obviously when it becomes closer to the BS, due to less path loss.

The secrecy rate of different users is compared with the different transmit power thresholds of P_{BS} in Fig. 5, where $K = 3$, $M = 3$, $\gamma = 7$, and $d = (5, 22.5, 40)$. In the simulation, U_1, U_2, and U_3 are considered as the private user, respectively. To compare with the proposed SRM scheme, we adopt the same optimization problem for the conventional NOMA scheme with normal decoding order, i.e., $|\mathbf{h}_i^\dagger \mathbf{v}_1|^2 \geq \cdots \geq |\mathbf{h}_i^\dagger \mathbf{v}_k|^2 \geq \cdots \geq |\mathbf{h}_i^\dagger \mathbf{v}_K|^2, i \in \mathcal{K}$. From the results, we can observe that the secrecy rate for U_1 and U_2 in the conventional NOMA scheme is 0, while the secrecy rate in the SRM scheme can be significantly improved with P_{BS}. This is because the strongest user U_3 has to decode their messages before recovering its own signal according to the normal decoding order. Thus, there is no privacy preservation for the weaker users in the conventional NOMA scheme. For U_3, its secrecy rate in the SRM scheme is also higher than that in the conventional NOMA scheme, due to the novel decoding order used in this paper. In addition, it is worth noticing that U_3 has the highest secrecy rate in the SRM scheme, while U_1 has the lowest. This demonstrates that the private transmission is more secure for users closer to BS, which is consistent with the analysis in Section II.

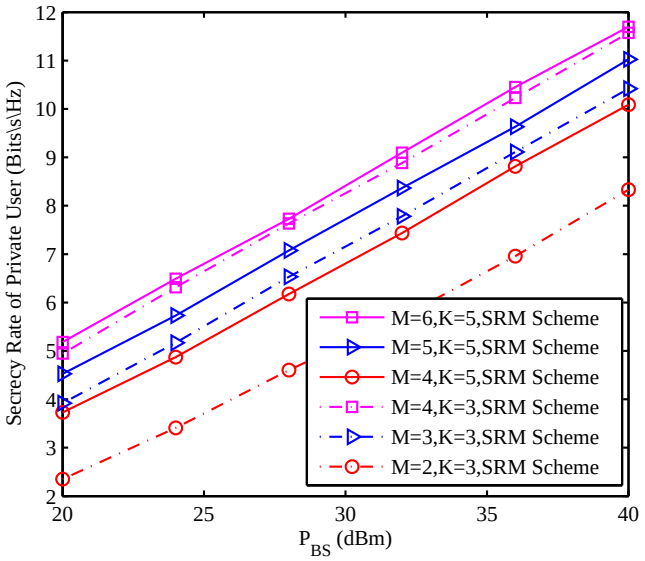


Fig. 6. Comparison of the secrecy rate of the private user for the SRM scheme with different values of M, K and P_{BS} in 3-user and 5-user MISO NOMA networks.

Subsequently, the secrecy rate of private user for the SRM scheme is compared with different values of M, K and P_{BS} in Fig. 6, where $\gamma = 1$. In addition, $d = (5, 22.5, 40)$ and $d = (5, 13.75, 22.5, 31.25, 40)$ are set and U_2 and U_3 are selected as the private user for the 3-user and 5-user MISO NOMA systems, respectively. From the results, we can see that the secrecy rate becomes higher with a larger number of antennas, especially when $M \geq K$, due to the fact that the transmission rate of the private user grows while the eavesdropping rate decreases, when more antennas are equipped at the BS. In addition, it can be seen that the secrecy rate of the private user when $K = 3$ is higher than that in the 5-user NOMA system with the same number of antennas equipped at the

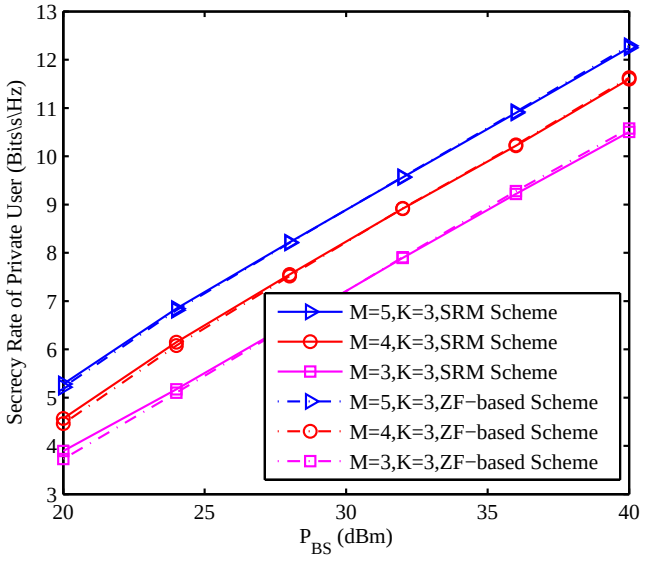


Fig. 7. Comparison of the secrecy rate of U_2 for the SRM and ZF-based schemes under varied thresholds of P_{BS} in a 3-user MISO NOMA network. Three cases of $M = 3$, $M = 4$ and $M = 5$ are considered.

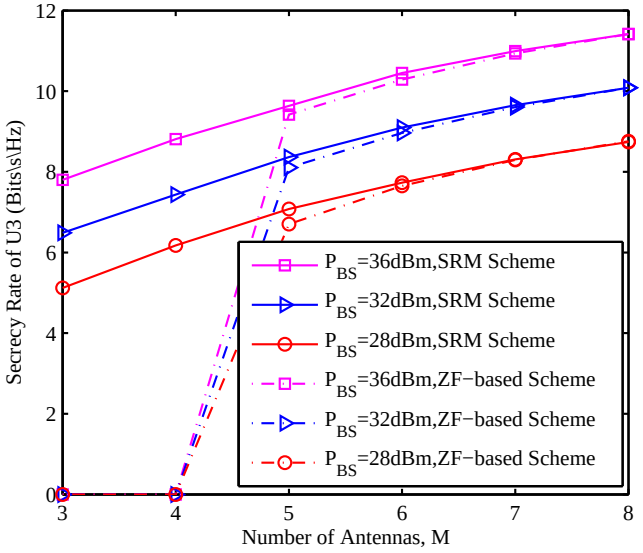


Fig. 9. Comparison of the secrecy rate of U_3 for the SRM and ZF-based scheme with different number of antennas in a 5-user MISO NOMA network. Three cases of $P = 28$ dBm, $P = 32$ dBm and $P = 36$ dBm are considered.

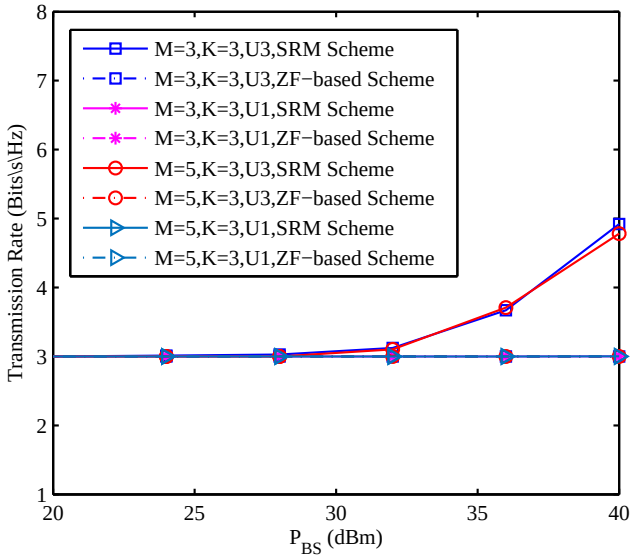


Fig. 8. Comparison of the transmission rate of all the other common users for the SRM and ZF-based schemes under varied thresholds of P_{BS} in a 3-user MISO NOMA network. Two cases of $M = 3$ and $M = 5$ are considered.

BS, i.e., the curve of $M = 4$ and $K = 3$ is much higher than that of $M = 4$ and $K = 5$. This indicates that the redundant antennas can be utilized to further enhance the security of the private user.

The secrecy rate of private user U_2 and the transmission rate of other common users in the SRM and ZF-based schemes are compared with different numbers of antennas in a 3-user MISO NOMA network in Fig. 7 and Fig. 8, respectively. In this simulation, we assume that $\gamma = 7$ and $d = (5, 22.5, 40)$. From Fig. 7, we can see that the secrecy rate of the SRM scheme and the ZF-based scheme is close to each other for the same number of antennas, when $M \geq K$. When $M < K$, only the SRM scheme is feasible in the system, whose performance has already been shown in Fig. 6. From Fig. 8, we can find that the transmission rate of all the other common users can satisfy their QoS requirements in both of these two schemes, which is consistent with their objectives in (13) and (36). Furthermore, the transmission rate of U_3 becomes higher as P_{BS} increases in the SRM scheme, due to the fact that according to (11), the increment of transmit power for U_3 can degrade the eavesdropping performance.

Finally, we study the performance of secrecy rate of private user U_3 for the SRM and ZF-based scheme in a 5-user MISO NOMA network with different numbers of antennas, as shown in Fig. 9, where $K = 5$, $\gamma = 1$, $d = (5, 13.75, 22.5, 31.25, 40)$, and three cases of $P = 28$ dBm, $P = 32$ dBm and $P = 36$ dBm are considered. From the results, we can see that the secrecy rate of the private user U_3 becomes higher with both the increasing of the transmit power and the number of antennas, which is consistent with previous analysis. In addition, when $M < K$, i.e., the zero-forcing constraints in (36c) cannot be satisfied, the secrecy rate of U_3 in the SRM scheme is much higher than that in the ZF-based scheme. Hence, the SRM scheme is more suitable to be used in the case of inadequate antennas equipped at the BS, which is agree with the analysis in Section IV-B. When $M \geq K$, as the performance of these two schemes is almost the same, we tend to choose the ZF-based Scheme allowing for the computational complexity.

VI. Conclusions

In this paper, we have investigated the security performance of the private user in MISO NOMA systems, and a novel decoding order for SIC was presented via beamforming to guarantee its privacy transmission. Furthermore, two schemes based on beamforming optimization were proposed to boost the security of the private user, i.e., the SRM scheme and the ZF-based scheme. In the SRM scheme, the secrecy rate of the private user was maximized with both other common users'

$$\mathcal{O}\left(N\sqrt{0.5K^3+0.5K+2}\left(1.5K^2-0.5K+2KM+3\right)^2\left(1.8333K^3+2.1667K+KM+3\right)\right). \quad (42)$$

$$\mathcal{O}\left(N\sqrt{0.5K^3-K^2+2.5K+1}\left(1.5K^2-2.5K+2KM+4\right)^2\left(1.8333K^3-4K^2+7.1667K+KM+2\right)\right). \quad (43)$$

QoS requirements and decoding order constraints satisfied. To solve the non-convex problem, we first converted it into a convex one, and then, a CCCP-based algorithm was developed to gain its solutions. In the ZF-based scheme, the information of the private user was zero-forced at other common users through beamforming, and its transmission rate could be maximized on the premise that the other common users' QoS, the updated decoding order and the zero-forcing constraints were fulfilled. Extensive simulation results were presented to verify their effectiveness.

Appendix A
Complexity Analysis

According to [44], we can know that the number of constraints and variables and the dimensions of all the SOC constraints needs to be calculated to analyze the complexity of the two schemes.

First, the total number of constraints in (26) and (39) can be obtained as $(0.5K^3+0.5K+2)$ and $(0.5K^3-K^2+2.5K+1)$, respectively. Thus, in each step, the number of iterations utilized to reduce the duality gap to a threshold can be upper bounded by

$$\mathcal{O}\left(\sqrt{0.5K^3+0.5K+2}\right), \quad (40)$$

and

$$\mathcal{O}\left(\sqrt{0.5K^3-K^2+2.5K+1}\right), \quad (41)$$

respectively.

Then, the number of variables and dimensions of all the SOC constraints for (26) can be calculated as $(1.5K^2-0.5K+2KM+3)$ and $(1.8333K^3+2.1667K+KM+3)$, respectively. Thus, according to [44], the complexity of Algorithm 1 for the SRM scheme can be obtained as (42). Similarly, the complexity of Algorithm 1 for the ZF-based scheme can be calculated as (43). In (43), the items $(1.5K^2-2.5K+2KM+4)$ and $(1.8333K^3-4K^2+7.1667K+KM+2)$ are the total number of variables and dimensions of all the SOC constraints, respectively.

Comparing (42) with (43), we can conclude that the complexity of ZF-based scheme is lower than that of SRM scheme.

References

[1] Y. Cao, N. Zhao, Y. Chen, M. Jin, L. Fan, Z. Ding, and F. R. Yu, "Privacy protection via beamforming optimization in MISO NOMA networks," in *Proc. WCSP'18*, pp. 1–6, Hangzhou, China, Oct. 2018.

[2] 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.

[3] Y. Cai, Z. Qin, F. Cui, G. Y. Li, and J. A. McCann, "Modulation and multiple access for 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 629–646, 1st Quart. 2018.

[4] Z. Chen, Z. Ding, X. Dai, and R. Zhang, "An optimization perspective of the superiority of NOMA compared to conventional OMA," *IEEE Trans. Signal Process.*, vol. 65, no. 19, pp. 5191–5202, Oct. 2017.

[5] S. M. R. Islam, N. Avazov, 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] L. Song, Y. Li, Z. Ding, and H. V. Poor, "Resource management in non-orthogonal multiple access networks for 5G and beyond," *IEEE Commun. Mag.*, vol. 31, no. 4, pp. 8–14, Jul. 2017.

[7] Z. Wei, D. W. K. Ng, and J. Yuan, "Joint pilot and payload power control for uplink MIMO-NOMA with MRC-SIC receivers," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 692–695, Apr. 2018.

[8] Y. Saito, Y. Kishiyama , A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE VTC'13-Spring*, pp. 1–5, Dresden, Germany, Jun. 2013.

[9] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[10] 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.

[11] Y. Liu, Z. Ding, M. Elkashlan, and H. V. Poor, "Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 4, pp. 938–952, Apr. 2016.

[12] 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.

[13] T. Lv, Y. Ma, J. Zeng, and P. T. Mathiopoulos, "Millimeter-wave NOMA transmission in cellular M2M communications for internet of things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1989–2000, Jun. 2018.

[14] Z. Ding, R. Schober, and H. V. Poor, "A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment," *IEEE Trans. wireless Commun.*, vol. 15, no. 6, pp. 938–952, Jun. 2016.

[15] X. Chen, Z. Zhang, C. Zhong, and D. W. K. Ng, "Exploiting multiple-antenna techniques for non-orthogonal multiple access," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 938–952, Oct. 2017.

[16] 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.

[17] 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.

[18] M. Qiu, Y. Huang, S. Shieh, and J. Yuan, "A lattice-partition framework of downlink non-orthogonal multiple access without SIC," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2532–2546, Jun. 2018.

[19] Y. Liu, H.-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, First Quart. 2017.

[20] 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.

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

[22] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[23] T. Lv, H. Gao, R. Cao, and J. Zhou, "Co-ordinated secure beamforming in K-user interference channel with multiple eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 212–215, Apr. 2016.

[24] 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

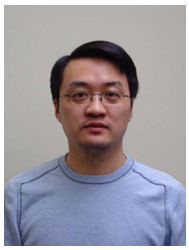
secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, Apr. 2018.
[25] L. Fan, R. Zhao, F. K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.
[26] H. Xing, K. K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 7971–7984, Dec. 2016.
[27] 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.
[28] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7599–7603, Aug. 2017.
[29] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[30] 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.
[31] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.
[32] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.
[33] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.
[34] W. Wang, T. Lv, and H. Gao, "Robust beamforming and power allocation for secrecy in DF relay networks with imperfect channel state information," *IEEE Access*, vol. 4, pp. 9520–9527, 2016.
[35] 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.
[36] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, Aug. 2017.
[37] Y. Liu, Z. Qin, M. Elkashlan, and Y. Gao, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
[38] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.
[39] 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.
[40] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO nonorthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7563–7567, Aug. 2017.
[41] 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, Apr. 2017.
[42] 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.
[43] D. R. Hunter and K. Lange, "A tutorial on MM algorithms," *Amer. Statist.*, vol. 58, no. 1, pp. 30–37, 2004.
[44] 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.
[45] Q. Shi, W. Xu, T. H. Chang, Y. Wang, and E. Song, "Joint beamforming and power splitting for MISO interference channel with SWIPT: An SOCP relaxation and decentralized algorithm," *IEEE Trans. Signal Process.*, vol. 62, no. 23, pp. 6194–6208, Dec. 2014.
[46] A. J. Smola and S. V. N. Vishwanathan, "Kernel methods for missing variables," in *Proc. 10th Int. Workshop Artif. Intell. Stat.*, pp. 325–332, Barbados, Jan. 2005.
[47] B. K. Sriperumbudur and G. R. G. Lanckriet, "On the convergence of the concave-convex procedure," in *Neural Information Processing Systems*, pp. 1–9, 2009.

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.

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.

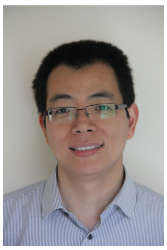
Dr. Zhao is serving or served on the editorial boards of 7 SCI-indexed journals, including IEEE Transactions on Green Communications and Networking. He won the best paper awards in IEEE VTC 2017 Spring, MLICOM 2017, ICNC 2018, WCSP 2018 and CSPS 2018. He also received the IEEE Communications Society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



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.

Minglu Jin (M'96) received the B.S degree from University of Science and Technology in 1982, M.S. and Ph. D degrees from Beijing University of Aeronautics and Astronautics in 1984 and 1995, respectively. He was a Visiting scholar in the Arimoto Lab. at Osaka University, Osaka, Japan, from 1987 to 1988. He was a Research Fellow in Radio & Broadcasting Research Lab at Electronics Telecommunications Research Institute (ETRI), Korea from 2001 to 2004. He is currently a professor at Dalian University of Technology. His research interests include wireless communication, wireless sensor networks, signal processing for wireless communication system.

Lisheng Fan received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from the Department of Electronic Engineering. He received the Ph.D degree from the Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. He is now a Professor with GuangZhou University. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. He is a guest editor of EURASIP Journal on Wireless Communications and Networking, and served as the chair of Wireless Communications and Networking Symposium for Chinacom 2014.



Zhiguo Ding (S'03-M'05) 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.

F. Richard Yu (S'00-M'04-SM'08-F'18) received the PhD degree in electrical engineering from the University of British Columbia (UBC) in 2003. From 2002 to 2006, he was with Ericsson (in Lund, Sweden) and a start-up in California, USA. He joined Carleton University in 2007, where he is currently a Professor. He received the IEEE Outstanding Service Award in 2016, IEEE Outstanding Leadership Award in 2013, Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly Premiers Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009 and the Best Paper Awards at IEEE VTC 2017 Spring, ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009 and Int'l Conference on Networking 2005. His research interests include cross-layer/cross-system design, connected vehicles, security, and green ICT.

He serves on the editorial boards of several journals, including Co-Editor-in-Chief for Ad Hoc & Sensor Wireless Networks, Lead Series Editor for IEEE Transactions on Vehicular Technology, IEEE Transactions on Green Communications and Networking, and IEEE Communications Surveys & Tutorials. He has served as the Technical Program Committee (TPC) Co-Chair of numerous conferences. Dr. Yu is a registered Professional Engineer in the province of Ontario, Canada, a Fellow of the Institution of Engineering and Technology (IET), and a Fellow of the IEEE. He is a Distinguished Lecturer, the Vice President - Membership, and an elected member of the Board of Governors (BoG) of the IEEE Vehicular Technology Society.