Joint Beamforming and Jamming Optimization for Secure Transmission in MISO-NOMA Networks

Nan Zhao, *Senior Member, IEEE*, Wei Wang, Jingjing Wang, *Member, IEEE*,
Yunfei Chen, *Senior Member, IEEE*, Yun Lin, Zhiguo Ding, *Senior Member, IEEE*,
and Norman C. Beaulieu, *Life Fellow, IEEE*

***Abstract*—Non-orthogonal multiple access (NOMA) has been developed as a key multi-access technique for 5G. However, secure transmission remains a challenge in NOMA. Especially, the user with weakest channel is most threatened by eavesdropping, due to its highest transmit power. Two schemes are proposed to generate artificial jamming at the NOMA base station (BS), aiming at disrupting the potential eavesdropping without affecting the legitimate transmission. In the first scheme, the transmit power of artificial jamming is maximized, with its received power at each receiver higher than that of other users. Thus, the jamming signal can be eliminated via successive interference cancellation before others. When the transmit power of the BS is inadequate, the transmit jamming power is maximized with the jamming signal zero-forced at each receiver. Thus, the legitimate transmission is not affected by the jamming, and the eavesdropping can be disrupted effectively. Due to the non-convexity of these two optimization problems, we first convert them to convex ones and, then, provide an iterative algorithm to solve them. Simulation results are presented to show the effectiveness of the proposed schemes in guaranteeing the security of NOMA networks.**

***Index Terms*—Artificial jamming, beamforming optimization, non-orthogonal multiple access, physical layer security, zero-forcing.**

I. Introduction

NON-ORTHOGONAL multiple access (NOMA) has become an important multi-access technique for 5G networks due to its high efficiency and low latency [1]. Different from orthogonal multiple access [2], NOMA can accommodate multiple users that share a single orthogonal resource block to satisfy the requirement of massive connections [3]. There exist many kinds of NOMA techniques, and we mainly focus on the power-domain NOMA in this paper. It utilizes power allocation to control the transmit power of each user based on the difference in channel strengths. Then, successive interference cancellation (SIC) can be exploited to decode the signals from stronger channels at each receiver to recover the desired signal.

Due to its excellent performance, NOMA has attracted great interest from both academia and industry [4]–[14]. In [4], a cooperative NOMA scheme was proposed for 5G networks by Ding *et al*., and its outage probability and diversity order were derived. A novel design of precoding and decoding matrices for multiple-input multiple-output (MIMO) NOMA systems was proposed in [5], with power allocation and user pairing. Sun *et al*. [6] utilized power allocation to maximize the ergodic capacity of Rayleigh fading MIMO-NOMA systems. The downlink sum rate of a multiple-input single-output (MISO) NOMA network was maximized by Hanif *et al*. [7] via joint precoding optimization. Lin *et al*. [8] presented a novel view of multi-user hybrid massive MIMO systems, which can be deemed as a type of non-orthogonal angle division multiple access. Some technical issues on NOMA-based cognitive radio networks were discussed in [9]. Chen *et al*. [10] exploited a secondary NOMA relay to achieve spectrum sharing via connecting the long-distance primary transceivers. Power allocation and user scheduling were optimized by Wu *et al*. [11] for NOMA relay-assisted networks. Xiao *et al*. [12] proposed a power allocation scheme based on reinforcement learning to prevent the NOMA system from adversarial jamming attacks. The performance of a downlink NOMA relay system was studied by Wan *et al*. [13] over Nakagami-m fading with partial channel state information (CSI). Chen *et al*. [14] established a novel multi-antenna

Manuscript received June 18, 2018; revised September 22, 2018; accepted November 14, 2018. Date of publication November 23, 2018; date of current version March 15, 2019. The work of N. Zhao was supported by the National Natural Science Foundation of China (NSFC) under Grant 61871065, the open research fund of State Key Laboratory of Integrated Services Networks under Grant ISN19-02, the Fundamental Research Funds for the Central Universities under DUT17JC43, and the Xinghai Scholars Program. The work of Z. Ding was supported by the UK EPSRC under grant number EP/L025272/2 and by H2020-MSCA-RISE-2015 under grant number 690750. The work of Y. Lin was supported by the National Natural Science Foundation of China (NSFC) under Grant 61771154. This work of N. C. Beaulieu was supported by the China SAFEA Thousand Talents Program. The associate editor coordinating the review of this paper and approving it for publication was I. H. Kim. *(Corresponding author: Yun Lin.)*

N. Zhao and W. Wang are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: zhaonan@dlut.edu.cn; 21809066@mail.dlut.edu.cn).

J. Wang is with the School of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266000, China (e-mail: kathy1003@163.com).

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

Y. Lin is with the College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China (e-mail: linyun@hrbeu.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).

N. C. Beaulieu is with the Beijing Key Laboratory for Network System Architecture and Convergence, and the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: nborm@bupt.edu.cn).

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

Digital Object Identifier 10.1109/TCOMM.2018.2883079

NOMA framework including user clustering, CSI acquisition, beamforming and SIC, and the transmission rate performance was analyzed.

However, secure transmission still remains a key challenge for NOMA systems, due to the ostensible openness and vulnerability of wireless channels. In particular, in NOMA networks, the transmit power of the user with the weakest channel should be the highest to perform SIC when the quality of service (QoS) requirements of users are the same, leading to easy interception by potential eavesdroppers. To this end, physical layer security has become an effective method to prevent eavesdropping using physical techniques. Following Wyner's pioneering work in [15], much research has been conducted to improve the performance of secure transmission through the methods of physical layer security, such as beamforming optimization [16], [17], cooperative relaying [18], [19], artificial jamming [20], [21], and interference management [22]–[24], *etc*. Recently, there has also been some emerging research on the physical layer security of NOMA networks [25]–[31]. Zhang *et al.* [25] maximized the secrecy sum rate in single-input single-output (SISO) NOMA networks through power allocation. A transmit antenna selection based secure NOMA scheme was proposed by Lei *et al.* [26], in which an expression of secrecy outage probability with antenna selection was derived. He *et al.* [27] proposed a novel design of secure NOMA systems, in which the optimal decoding order, transmission rate and power allocation were considered. The physical layer security for cooperative NOMA systems was studied by Chen *et al.* [28], in which an expression of secrecy outage probability was derived. Li *et al.* [29] maximized the sum secrecy rate of central users via secure beamforming in downlink NOMA networks, in which users were grouped as multiple clusters. The physical layer security of NOMA in large-scale networks was investigated via stochastic geometry by Liu *et al.* [30], in both single-antenna and multi-antenna scenarios. In [31], beamforming and power allocation were exploited by Ding *et al.* to enhance the spectrum efficiency and security of NOMA assisted multicast-unicast streaming. Furthermore, artificial jamming can be exploited to guarantee the secure transmission in MISO-NOMA networks [32], [33]. In [32], artificial jamming was generated by using a portion of the antennas at the NOMA base station (BS) to constrain jamming into the null space of legitimate channels in a two-user NOMA network; while in [33], simultaneous wireless information and power transfer was considered in a cognitive MISO-NOMA network.

Based on the above observations, artificial jamming is generated together with the legitimate information using all the antennas at the NOMA BS in this paper, and the eavesdropping can be effectively disrupted by maximizing the transmit power of jamming without affecting the legitimate transmission. The motivations and contributions are summarized as follows.

- To the best of our knowledge, only a few works have focused on the artificial jamming based secure transmission for MISO-NOMA networks [32], [33]. Different from these works, we propose to combine artificial jamming with SIC, which means that the jamming signal can be completely eliminated at the legitimate receivers based on SIC, without affecting the legitimate transmission.

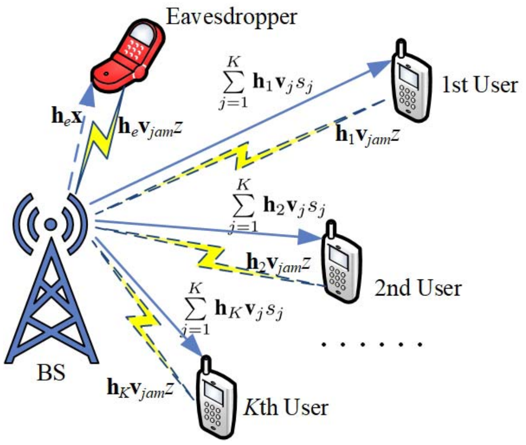

Eavesdropper
$\sum_{j=1}^{K} \mathbf{h}_1\mathbf{v}_j s_j$
1st User
$\mathbf{h}_e\mathbf{x}$
$\mathbf{h}_e\mathbf{v}_{jam}z$
$\mathbf{h}_1\mathbf{v}_{jam}z$
$\sum_{j=1}^{K} \mathbf{h}_2\mathbf{v}_j s_j$
$\mathbf{h}_2\mathbf{v}_{jam}z$
2nd User
$\sum_{j=1}^{K} \mathbf{h}_K\mathbf{v}_j s_j$
. . . . . .
BS
$\mathbf{h}_K\mathbf{v}_{jam}z$
*K*th User

Fig. 1. Demonstration of the artificial jamming assisted MISO-NOMA network with K legitimate users and one potential eavesdropper.

- In the first scheme, the transmit power of jamming is maximized to disrupt eavesdropping, with the modified SIC decoding order, the required signal-to-interference-plus-noise ratio (SINR) of each legitimate user, and the transmit power constraint of BS satisfied. In this scheme, the jamming signal can be eliminated via SIC before other users, as it has the highest received power.
- The optimization problem in the first scheme is non-convex. Thus, it is first converted to a convex problem by using the first-order Taylor approximation, which can be solved iteratively based on the conventional concave-convex procedure accordingly.
- A second scheme is proposed when the transmit power of BS is inadequate. In the scheme, the transmit jamming power is maximized to disrupt the eavesdropping, and the jamming signal is zero-forced at all the legitimate receivers, with the required SINR of each user and the transmit power constraint of the BS satisfied. The optimization problem is also non-convex and can be solved similarly to the first scheme.

The rest of this paper is organized as follows. In Section II, the system model is presented. In Section III, the optimization problem of the first scheme is formulated, and a low-complexity algorithm is proposed. The second zero-forcing scheme is proposed in Section IV. In Section V, simulation results are presented, followed by conclusions in Section VI.

Notation: $\mathbb{C}^{M\times N}$ is the space of complex matrices. $\mathbf{I}_N$ is the $N \times N$ identity matrix. $\mathcal{CN}(\mathbf{n}, \mathbf{N})$ is the complex Gaussian distribution with mean matrix $\mathbf{n}$ and covariance matrix $\mathbf{N}$. $\mathbf{A} \succeq 0$ means that $\mathbf{A}$ is a Hermitian positive semidefinite matrix. $Re(\cdot)$ is defined as the real operator. $\bigtriangledown$ denotes the gradient.

II. System Model

A MISO-NOMA wireless network is considered as shown in Fig. 1, in which a BS with M antennas sends the confidential information to K single-antenna users. We also assume that there exists a potential eavesdropper that intends to intercept the confidential information for the legitimate users, and its CSI is not available at the legitimate network. To disrupt the eavesdropping and guarantee the secure transmission of legitimate users, artificial jamming is generated together with the NOMA information at the BS, without affecting the legitimate transmission.

The transmit signal at the BS can be expressed as

$$\mathbf{x} = \sum\nolimits_{k=1}^{K} \mathbf{v}_k s_k + \mathbf{v}_{jam} z \tag{1}$$

where $\mathbf{v}_k \in \mathbb{C}^{M\times 1}$ denotes the beamforming vector for the kth user with $\|\mathbf{v}_k\|^2 = P_k, k \in \mathcal{K} \triangleq \{1, 2, \ldots, K\}$, s_k is the transmitted signal of the kth user with unit power $|s_k|^2 = 1$, $\mathbf{v}_{jam} \in \mathbb{C}^{M\times 1}$ is the beamforming vector for the artificial jamming with $\|\mathbf{v}_{jam}\|^2 = P_{jam}$, and z is the artificial jamming with unit power $|z|^2 = 1$, which is a zero-mean complex Gaussian random viable. We can conclude that the beamforming vector $\mathbf{v}_{jam}$ is specifically designed to avoid affecting the legitimate transmission, while the artificial jamming signal z is randomly generated to disrupt the eavesdropping effectively.

The received signal at the kth user can be given by

$$y_k = \mathbf{h}_k \mathbf{x} + n_k = \mathbf{h}_k \sum\nolimits_{j=1}^{K} \mathbf{v}_j s_j + \mathbf{h}_k \mathbf{v}_{jam} z + n_k, \quad k \in \mathcal{K} \tag{2}$$

where $n_k \sim \mathcal{CN}(0, \sigma^2)$ denotes the additive white Gaussian noise (AWGN) at the kth user, with zero mean and variance σ^2. The channel coefficient vector from the BS to the kth user can be expressed as

$$\mathbf{h}_k = \sqrt{\beta d_k^{-\alpha}} \mathbf{g}_k \in \mathbb{C}^{1\times M} \tag{3}$$

where the distance between them is d_k, β is defined as the channel power gain at the reference distance of 1 m, and $\alpha \geq 2$ denotes the path-loss exponent. In addition, $\mathbf{g}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ denotes the small-scale Rayleigh fading gain. Without loss of generality, we assume that the channel gains between the BS and legitimate users satisfy

$$0 < \|\mathbf{h}_1\|^2 \leq \cdots \leq \|\mathbf{h}_K\|^2 . \tag{4}$$

In NOMA systems, SIC should be utilized to remove the multi-access interference (MAI) at the receivers. Accordingly, a user with a stronger channel should first decode the messages from other users with weaker channels, and then remove the MAI from its received signal before decoding its own message. Therefore, the decoding order of SIC in MISO-NOMA networks can be represented as

$$\begin{cases} \max\limits_{m=2,\ldots,K} |\mathbf{h}_1 \mathbf{v}_m|^2 \leq |\mathbf{h}_1 \mathbf{v}_1|^2 \\ \ldots\ldots \\ \max\limits_{m=k+1,\ldots,K} |\mathbf{h}_k \mathbf{v}_m|^2 \leq |\mathbf{h}_k \mathbf{v}_k|^2 \leq \cdots \leq |\mathbf{h}_k \mathbf{v}_1|^2 \\ \ldots\ldots \\ |\mathbf{h}_K \mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K \mathbf{v}_1|^2 . \end{cases} \tag{5}$$

According to (5), SIC is adopted at each receiver to decode its own information, which can be performed based on the differences of channel gain among users. For example, at the kth receiver, $2 \leq k \leq K-1$, the receiver has to decode the messages of the 1st user to the $(k-1)$th user before recovering its own. Thus, the achievable SINR of the jth user $(1 \leq j \leq k-1)$ at the kth receiver can be expressed as

$$\mathrm{SINR}_k^j = \frac{|\mathbf{h}_k \mathbf{v}_j|^2}{\sum\nolimits_{m=j+1}^{K} |\mathbf{h}_k \mathbf{v}_m|^2 + |\mathbf{h}_k \mathbf{v}_{jam}|^2 + \sigma^2}, \quad 2 \leq k \leq K-1, \quad 1 \leq j \leq k-1. \tag{6}$$

Based on (6), the kth receiver can successfully decode the message of the jth user only when $\mathrm{SINR}_k^j \geq r_{th}^j$, where r_{th}^j is the received SINR threshold for the signal of the jth user. After subtracting all the MAIs successfully from the superimposed signal at the kth receiver, the desired message for the kth user can be retrieved by taking the interferences from the $(k+1)$th user to the Kth user as noise due to their lower powers. In this way, the received SINR of the desired signal at the kth receiver can be expressed as

$$\mathrm{SINR}_k^k = \frac{|\mathbf{h}_k \mathbf{v}_k|^2}{\sum\limits_{m=k+1}^{K} |\mathbf{h}_k \mathbf{v}_m|^2 + |\mathbf{h}_k \mathbf{v}_{jam}|^2 + \sigma^2}, \quad 2 \leq k \leq K-1. \tag{7}$$

For the Kth user, all the interference should be subtracted from its received signal, and the received SINR of its desired signal can be written as

$$\mathrm{SINR}_K^K = \frac{|\mathbf{h}_K \mathbf{v}_K|^2}{|\mathbf{h}_K \mathbf{v}_{jam}|^2 + \sigma^2}. \tag{8}$$

For the 1st user, the interference from the other $K-1$ users should all be taken as noise, and the received SINR of its desired signal can be denoted as

$$\mathrm{SINR}_1^1 = \frac{|\mathbf{h}_1 \mathbf{v}_1|^2}{\sum\nolimits_{m=2}^{K} |\mathbf{h}_1 \mathbf{v}_m|^2 + |\mathbf{h}_1 \mathbf{v}_{jam}|^2 + \sigma^2}. \tag{9}$$

From (7) to (9), we can observe that, although the potential eavesdropping can be effectively disrupted by the artificial jamming, the legitimate transmission in the network will also be degraded. Thus, two joint beamforming and jamming optimization schemes are proposed to disrupt the eavesdropping without affecting the legitimate transmission of the NOMA network in the following sections.

III. Joint Beamforming and Jamming Optimization

To guarantee the security of the MISO-NOMA network with legitimate transmission is not affected, in this section, we propose a joint beamforming and jamming optimization scheme, in which the jamming power is maximized to disrupt the eavesdropping with the QoS of legitimate users satisfied. In addition, an iterative algorithm is proposed to solve this non-convex optimization problem with low computational complexity.

A. Minimizing Transmit Power Without Jamming

According to the conventional decoding order of the SIC in (5), the sum transmit power at the BS for the users can be minimized with the QoS of each legitimate user satisfied, as follows.[1]

$$\begin{aligned}
&\min_{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_K} \sum\nolimits_{i=1}^{K} \|\mathbf{v}_i\|^2\\
&\quad s.t.\ \text{SINR}_k^k \geq r_k, \quad k \in \mathcal{K},\\
&\qquad \begin{cases}
\max\limits_{m=2,\ldots,K} |\mathbf{h}_1\mathbf{v}_m|^2 \leq |\mathbf{h}_1\mathbf{v}_1|^2\\
\cdots\cdots\\
\max\limits_{m=k+1,\ldots,K} |\mathbf{h}_k\mathbf{v}_m|^2 \leq |\mathbf{h}_k\mathbf{v}_k|^2 \leq \ldots \leq |\mathbf{h}_k\mathbf{v}_1|^2\\
\cdots\cdots\\
|\mathbf{h}_K\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_1|^2.
\end{cases}\\
&\qquad \sum\nolimits_{i=1}^{K} \|\mathbf{v}_i\|^2 < P_{BS} \qquad (10)
\end{aligned}$$

where r_k is the SINR requirement of the kth user and P_{BS} denotes the constraint of the total transmit power at the BS.

However, secure transmission in the network when (10) is adopted cannot be guaranteed. In addition, when P_{BS} is much higher than the value needed to satisfy the QoS of all users, the available power at BS is not fully utilized. Thus, the residual power of P_{BS} can be further exploited as artificial jamming to enhance the performance of secure transmission, as discussed in the following sections.

B. Modified SIC Decoding Order

We first consider the case when adequate transmit power can be allocated for jamming at the BS, and thus, we can enhance the received power of jamming at each user to first decode the jamming signal by SIC. In doing this, the transmit power of jamming can be increased significantly, through which the eavesdropping will be disrupted. Thus, the decoding order defined in (5) for the conventional MISO-NOMA scheme can be modified as

$$\begin{cases}
\max\limits_{m=2,\ldots,K} |\mathbf{h}_1\mathbf{v}_m|^2 \leq |\mathbf{h}_1\mathbf{v}_1|^2 \leq |\mathbf{h}_1\mathbf{v}_{jam}|^2\\
\cdots\cdots\\
\max\limits_{m=k+1,\underset{\cdot}{\mathrm{o}}ts,K} |\mathbf{h}_k\mathbf{v}_m|^2 \leq |\mathbf{h}_k\mathbf{v}_k|^2 \leq \ldots\\
\qquad\qquad\qquad \leq |\mathbf{h}_k\mathbf{v}_1|^2 \leq |\mathbf{h}_k\mathbf{v}_{jam}|^2\\
\cdots\cdots\\
|\mathbf{h}_K\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_1|^2 \leq |\mathbf{h}_K\mathbf{v}_{jam}|^2.
\end{cases} \qquad (11)$$

Accordingly, the jamming will be completely cancelled in the first step of SIC, which will not affect the following decoding procedure at each user. Therefore, the expressions for the received SINR of the desired signal for the kth user in (7) to (9) can be updated as

$$\text{SINR}_k^k = \frac{|\mathbf{h}_k\mathbf{v}_k|^2}{\sum\nolimits_{m=k+1}^{K} |\mathbf{h}_k\mathbf{v}_m|^2 + \sigma^2}, \quad 1 \leq k \leq K-1, \quad (12)$$

$$\text{SINR}_K^K = |\mathbf{h}_K\mathbf{v}_K|^2 / \sigma^2. \qquad (13)$$

Thus, we can conclude that SIC can be performed in the same way as in conventional NOMA as long as the transmit jamming power is high enough.

C. Scheme I

Based on the modified SIC decoding order in (11), the beamforming and jamming can be jointly optimized to maximize the transmit power of jamming, with the QoS of each legitimate user and the transmit power constraint satisfied, which can be formulated as

$$\max_{\substack{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_K,\\ \mathbf{v}_{jam}}} \|\mathbf{v}_{jam}\|^2 = P_{jam} \qquad (14a)$$

$$s.t.\ \text{SINR}_k^k \geq r_k, k \in \mathcal{K}, \qquad (14b)$$

$$\begin{cases}
\max_{m=2,\ldots,K} |\mathbf{h}_1\mathbf{v}_m|^2 \leq |\mathbf{h}_1\mathbf{v}_1|^2 \leq |\mathbf{h}_1\mathbf{v}_{jam}|^2\\
\cdots\cdots\\
\max_{m=k+1,\ldots,K} |\mathbf{h}_k\mathbf{v}_m|^2 \leq |\mathbf{h}_k\mathbf{v}_k|^2 \leq \ldots\\
\qquad\qquad\qquad \leq |\mathbf{h}_k\mathbf{v}_1|^2 \leq |\mathbf{h}_k\mathbf{v}_{jam}|^2\\
\cdots\cdots\\
|\mathbf{h}_K\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_1|^2 \leq |\mathbf{h}_K\mathbf{v}_{jam}|^2,
\end{cases} \qquad (14c)$$

$$\sum\nolimits_{i=1}^{K} \|\mathbf{v}_i\|^2 + \|\mathbf{v}_{jam}\|^2 = P_{BS}. \qquad (14d)$$

where P_{BS} is the constraint of the total transmit power at the BS, including the power for both the legitimate users and the jamming. In (14), the transmit power of the artificial jamming is maximized, instead of optimizing it, due to the fact that the eavesdropping CSI is not available in the legitimate network.

In addition, considering the potential eavesdropper, the received SINR of the kth legitimate user at the eavesdropper can be expressed as

$$\text{SINR}_e^k = \frac{|\mathbf{h}_e\mathbf{v}_k|^2}{\sum\nolimits_{m=1,m\neq k}^{K} |\mathbf{h}_e\mathbf{v}_m|^2 + |\mathbf{h}_e\mathbf{v}_{jam}|^2 + \sigma^2}. \quad (15)$$

Thus, the secrecy rate of the kth user can be expressed as (16) at the top of next page, $k = 1, 2, \ldots, K-1$. For the Kth user, the secrecy rate can be obtained by replacing SINR_k^k using (13). In (15) and (16), $\mathbf{h}_e$ is the channel coefficient vector from the BS to the eavesdropper.[2] Let $[x]^+ \triangleq \max(x, 0)$.

Remark: From (16), we can conclude that high-power jamming will disrupt the eavesdropping effectively, without affecting the decoding at legitimate receivers. In addition, we can also observe that the interference among users can also disrupt the eavesdropping. Particularly, the users with stronger channels from the BS will achieve better security performance when the QoS requirements of users are the same, due to the fact that the desired signal from stronger users tends to be hidden in the mixed signal transmitted by the BS. For the users with weaker channels, the jamming is important and it is necessary to guarantee the security, due to their higher transmit power.

D. Approximate Transformations

The proposed optimization problem in (14) is non-convex, which is difficult to solve. Thus, a suboptimal algorithm with low computational complexity is developed for a solution in

[1] The optimization problem (10) is utilized to bring forward Scheme I and serve as a benchmark in the simulations.

[2] In this paper, we do not need the eavesdropping CSI for the legitimate network. Nevertheless, the eavesdropping CSI is used to analyze the secure performance of the proposed schemes in (15) and (16), i.e., it is only used for the performance analysis, not for the design in the proposed schemes.

$$\begin{aligned} R_{sk} &= \left[\log_2\left(1+\mathrm{SINR}_k^k\right)-\log_2\left(1+\mathrm{SINR}_e^k\right)\right]^+ \\ &= \left[\log_2\left(1+\frac{\left|\mathbf{h}_k\mathbf{v}_k\right|^2}{\sum_{m=k+1}^{K}\left|\mathbf{h}_k\mathbf{v}_m\right|^2+\sigma^2}\right)-\log_2\left(1+\frac{\left|\mathbf{h}_e\mathbf{v}_k\right|^2}{\sum_{m=1,m\neq k}^{K}\left|\mathbf{h}_e\mathbf{v}_m\right|^2+\left|\mathbf{h}_e\mathbf{v}_{jam}\right|^2+\sigma^2}\right)\right]^+. \end{aligned} \tag{16}$$

this subsection. To achieve this, some necessary approximations are made first. According to (12) and (13), the problem (14) can be rewritten as

$$\max_{\substack{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_K,\\ \mathbf{v}_{jam}}} \left\|\mathbf{v}_{jam}\right\|^2 \tag{17a}$$

$$s.t. \begin{cases} \dfrac{\left|\mathbf{h}_k\mathbf{v}_k\right|^2}{\sum_{m=k+1}^{K}\left|\mathbf{h}_k\mathbf{v}_m\right|^2+\sigma^2}\geq r_k, k\neq K \\ \dfrac{\left|\mathbf{h}_K\mathbf{v}_K\right|^2}{\sigma^2}\geq r_K, \end{cases} \tag{17b}$$

$$\begin{cases} \max\limits_{m=2,\ldots,K}\left|\mathbf{h}_1\mathbf{v}_m\right|^2\leq\left|\mathbf{h}_1\mathbf{v}_1\right|^2\leq\left|\mathbf{h}_1\mathbf{v}_{jam}\right|^2 \\ \cdots\cdots \\ \max\limits_{m=k+1,\ldots,K}\left|\mathbf{h}_k\mathbf{v}_m\right|^2\leq\left|\mathbf{h}_k\mathbf{v}_k\right|^2\leq\ldots \\ \qquad\qquad\leq\left|\mathbf{h}_k\mathbf{v}_1\right|^2\leq\left|\mathbf{h}_k\mathbf{v}_{jam}\right|^2 \\ \cdots\cdots \\ |\mathbf{h}_K\mathbf{v}_K|^2\leq\cdots\leq|\mathbf{h}_K\mathbf{v}_1|^2\leq|\mathbf{h}_K\mathbf{v}_{jam}|^2, \end{cases} \tag{17c}$$

$$\sum\nolimits_{i=1}^{K}\left\|\mathbf{v}_i\right\|^2+\left\|\mathbf{v}_{jam}\right\|^2=P_{BS}. \tag{17d}$$

This gives

$$\max_{\substack{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_K,\\ \mathbf{v}_{jam}}} \left\|\mathbf{v}_{jam}\right\|^2 \tag{18a}$$

$$s.t. \begin{cases} \sum_{m=k+1}^{K}\left|\mathbf{h}_k\mathbf{v}_m\right|^2\leq\dfrac{\left|\mathbf{h}_k\mathbf{v}_k\right|^2}{r_k}-\sigma^2, \quad k\neq K \\ 0\leq\dfrac{\left|\mathbf{h}_K\mathbf{v}_K\right|^2}{r_K}-\sigma^2, \end{cases} \tag{18b}$$

$$\begin{cases} \max_{m=2,\ldots,K}\left|\mathbf{h}_1\mathbf{v}_m\right|^2\leq\left|\mathbf{h}_1\mathbf{v}_1\right|^2\leq\left|\mathbf{h}_1\mathbf{v}_{jam}\right|^2 \\ \cdots\cdots \\ \max\limits_{m=k+1,\ldots,K}\left|\mathbf{h}_k\mathbf{v}_m\right|^2\leq\left|\mathbf{h}_k\mathbf{v}_k\right|^2\leq\ldots \\ \qquad\qquad\leq\left|\mathbf{h}_k\mathbf{v}_1\right|^2\leq\left|\mathbf{h}_k\mathbf{v}_{jam}\right|^2 \\ \cdots\cdots \\ |\mathbf{h}_K\mathbf{v}_K|^2\leq\cdots\leq|\mathbf{h}_K\mathbf{v}_1|^2\leq|\mathbf{h}_K\mathbf{v}_{jam}|^2, \end{cases} \tag{18c}$$

$$\sum\nolimits_{i=1}^{K}\left\|\mathbf{v}_i\right\|^2+\left\|\mathbf{v}_{jam}\right\|^2=P_{BS}. \tag{18d}$$

The problem in (18) is still non-convex. Then, Property 1 is introduced as follows, which shows an efficient way to convert the problem (18) into a convex problem.

Property 1: In the problem of finding the extreme value of a function, a differentiable function can be replaced by its corresponding tangent function value at the tangent point. Simply, we define the tangential function as $g\left(x,x^{(m)}\right)$ and the point of tangency as $x^{(m)}$. Then, for a differentiable convex function $f(x)$, the expression is $f(x)\geq g\left(x,x^{(m)}\right)$, where the equality holds when $x=x^{(m)}$. Furthermore, $g\left(x,x^{(m)}\right)$ can be derived as the first order Taylor expansion around $x^{(m)}$. Thus, the inequality can be expressed as

$$f(x)\geq g\left(x,x^{(m)}\right)=f(x^{(m)})+\bigtriangledown f\left(x^{(m)}\right)^{\dagger}\left(x-x^{(m)}\right). \tag{19}$$

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

Based on Property 1, the constraints in (18b) can be transformed into convex ones, using the following proposition.

Proposition 1: From the above analysis and based on (18b), we define a function as

$$F(\mathbf{v}_k)=\left|\mathbf{h}_k\mathbf{v}_k\right|^2/r_k-\sigma^2, k\in\mathcal{K}. \tag{20}$$

The first order Taylor approximation to $F(\mathbf{v}_k)$ at a tangent point $\bar{\mathbf{v}}_k$ can be expressed as

$$\mathcal{F}\left(\mathbf{v}_k,\bar{\mathbf{v}}_k\right)=\frac{2Re\left(\mathbf{h}_k\mathbf{v}_k\bar{\mathbf{v}}_k^{\dagger}\mathbf{h}_k^{\dagger}\right)-Re\left(\mathbf{h}_k\bar{\mathbf{v}}_k\bar{\mathbf{v}}_k^{\dagger}\mathbf{h}_k^{\dagger}\right)}{r_k}-\sigma^2. \tag{21}$$

In this way, (20) can be replaced by (21), and the constraint (18b) can be approximated as a convex one.

Proof: According to Property 1, (20) is a differentiable convex function, which satisfies

$$F(\mathbf{v}_k)\geq F(\bar{\mathbf{v}}_k)+\bigtriangledown F(\bar{\mathbf{v}}_k)^{\dagger}(\mathbf{v}_k-\bar{\mathbf{v}}_k). \tag{22}$$

Substituting (20) into this inequality (22) based on the law of derivation, the expression can be calculated as

$$F(\mathbf{v}_k)\geq\frac{\mathbf{h}_k\bar{\mathbf{v}}_k\bar{\mathbf{v}}_k^{\dagger}\mathbf{h}_k^{\dagger}}{r_k}-\sigma^2+\frac{2\mathbf{h}_k\bar{\mathbf{v}}_k^{\dagger}\mathbf{h}_k^{\dagger}}{r_k}(\mathbf{v}_k-\bar{\mathbf{v}}_k). \tag{23}$$

When $\bar{\mathbf{v}}_k\bar{\mathbf{v}}_k^{\dagger}\succeq 0$ and $\mathbf{h}_k\mathbf{h}_k^{\dagger}\succeq 0$, we have

$$F(\mathbf{v}_k)\triangleq\mathcal{F}\left(\mathbf{v}_k,\bar{\mathbf{v}}_k\right). \tag{24}$$

Thus, we can substitute the right side of (18b) with (21), and the previous norm-squared function can be approximated as linear functions. Accordingly, the constraint (18b) can be transformed into a convex one. This approximation is reasonable when $\bar{\mathbf{v}}_k=\mathbf{v}_k$ is satisfied. ■

Similarly, we can also make the first order Taylor expansion for the objective function (18a) according to Property 1. First, define an auxiliary variable $t\geq 0$. Then, according to Property 1, we can transform the norm-squared objective function into a linear one as

$$\left\|\mathbf{v}_{jam}\right\|^2\geq 2Re\left(\mathbf{v}_{jam}^{\dagger}\bar{\mathbf{v}}_{jam}\right)-Re\left(\bar{\mathbf{v}}_{jam}^{\dagger}\bar{\mathbf{v}}_{jam}\right)\geq t. \tag{25}$$

Finally, both of constraint (18b) and the objective function (18a) can be converted into convex functions.

Nevertheless, the problem is still non-convex because of (18c), which can be regarded as a series of inequalities like

$$\left|\mathbf{h}_k\mathbf{v}_m\right|^2\leq\left|\mathbf{h}_k\mathbf{v}_i\right|^2. \tag{26}$$

It is worth noting that the right sides of these inequalities are quadratic functions for variable $\mathbf{v}_i$, which can be linearized by the same method used above. Define

$$H_{ki}(\mathbf{v}_i) = |\mathbf{h}_k \mathbf{v}_i|^2 . \tag{27}$$

and its corresponding first order Taylor approximation can be calculated as

$$\mathcal{H}_{ki}\left(\mathbf{v}_i, \bar{\mathbf{v}}_i\right) = 2Re\left(\mathbf{h}_k \mathbf{v}_i \bar{\mathbf{v}}_i^{\dagger} \mathbf{h}_k^{\dagger}\right) - Re\left(\mathbf{h}_k \bar{\mathbf{v}}_i \bar{\mathbf{v}}_i^{\dagger} \mathbf{h}_k^{\dagger}\right). \tag{28}$$

Based on the above approximations, all the inequalities in (18c) in the same form as (26) can be converted into convex functions. Then, the constraint (18c) can be replaced by

$$|\mathbf{h}_k \mathbf{v}_m|^2 \leq \mathcal{H}_{ki}\left(\mathbf{v}_i, \bar{\mathbf{v}}_i\right), \tag{29}$$

$$|\mathbf{h}_k \mathbf{v}_1|^2 \leq 2Re\left(\mathbf{h}_k \mathbf{v}_{jam} \bar{\mathbf{v}}_{jam}^{\dagger} \mathbf{h}_k^{\dagger}\right) - Re\left(\mathbf{h}_k \bar{\mathbf{v}}_{jam} \bar{\mathbf{v}}_{jam}^{\dagger} \mathbf{h}_k^{\dagger}\right). \tag{30}$$

In addition, the hyperbolic constraint

$$w^2 \leq xy, x \geq 0, y \geq 0 \tag{31}$$

can be converted into

$$\|[2w, x-y]^{\dagger}\| \leq x + y. \tag{32}$$

Thus, the problem (18) can be transformed into a convex one as given in (33), at the bottom of this page.

E. Iterative Algorithm

Eq. (33) can be effectively solved using existing toolboxes, such as CVX. Nevertheless, the solution of (33) is not completely equivalent to that of (18) owing to the approximations and transformations, and thus, Algorithm 1 is proposed to solve (18) based on the concave-convex procedure as follows.

The initial values can be generated randomly with the constraints in (33) considered, which can be obtained easily in practice [7].

In Proposition 2, it will be shown that the solution of Algorithm 1 is viable to the problem (18).

Proposition 2: The solution to (33) in each iteration of Algorithm 1 is a suboptimal solution to the problem (18).

Algorithm 1 Iterative Algorithm for Problem (18)

```
Initialization: Randomly set the initial values of $\bar{\mathbf{v}}_k$ and $\bar{\mathbf{v}}_{jam}$ in (33) and set $n = 1$.
Repeat
    Solve (33) using CVX, and get the optimal values $\mathbf{v}_k^*$ and $\mathbf{v}_{jam}^*$.
    Substitute the temporary optimal values for the previous set of values, i.e., $\bar{\mathbf{v}}_k = \mathbf{v}_k^*$ and $\bar{\mathbf{v}}_{jam} = \mathbf{v}_{jam}^*$.
    $n = n + 1$.
Until Convergence or the maximum number of iterations is satisfied.
Output: $\mathbf{v}_k^*$ and $\mathbf{v}_{jam}^*$, $\forall k \in \mathcal{K}$.
```

Proof: According to the principle of concave-convex procedure, the relationship between the two previously defined functions $F\left(\mathbf{v}_k\right)$ and $\mathcal{F}\left(\mathbf{v}_k, \bar{\mathbf{v}}_k\right)$ can be expressed as

$$F\left(\mathbf{v}_k\right) \geq \mathcal{F}\left(\mathbf{v}_k, \bar{\mathbf{v}}_k\right), \tag{34}$$

$$F\left(\mathbf{v}_k\right)|_{\mathbf{v}_k = \bar{\mathbf{v}}_k} = \mathcal{F}\left(\mathbf{v}_k, \bar{\mathbf{v}}_k\right)|_{\mathbf{v}_k = \bar{\mathbf{v}}_k}. \tag{35}$$

In addition, we define

$$G\left(\mathbf{v}_m\right) = \sum\nolimits_{m=k+1}^{K} |\mathbf{h}_k \mathbf{v}_m|^2 . \tag{36}$$

According to the constraint (18b), (36) can be expressed as

$$G\left(\mathbf{v}_m\right) - F\left(\mathbf{v}_k\right) \leq 0. \tag{37}$$

Thus, we can conclude

$$G\left(\mathbf{v}_m\right) - F\left(\mathbf{v}_k\right) \leq G\left(\mathbf{v}_m\right) - \mathcal{F}\left(\mathbf{v}_k, \bar{\mathbf{v}}_k\right) \leq 0. \tag{38}$$

Then, in the nth iteration, the inequality (38) can be denoted as

$$G\left(\mathbf{v}_m^{(n)}\right) - F\left(\mathbf{v}_k^{(n)}\right) \leq G\left(\mathbf{v}_m^{(n)}\right) - \mathcal{F}\left(\mathbf{v}_k^{(n)}, \mathbf{v}_k^{(n-1)}\right) \leq 0 \tag{39}$$

where the equality can be satisfied with $\mathbf{v}_k^{(n)} = \mathbf{v}_k^{(n-1)}$. We focus on the transformation of the constraint (18b) above, and all the other constraints in (18) can be proved similarly.

From the above derivations, we can conclude that the solution to (33) is a feasible subset of that to (18). ■

$$\max_{\substack{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_K, \\ \mathbf{v}_{jam}}} \; t \tag{33a}$$

$$s.t. \; t \geq 0, \tag{33b}$$

$$t \leq 2Re\left(\mathbf{v}_{jam}^{\dagger} \bar{\mathbf{v}}_{jam}\right) - Re\left(\bar{\mathbf{v}}_{jam}^{\dagger} \bar{\mathbf{v}}_{jam}\right), \tag{33c}$$

$$\begin{cases} \left\| [2\mathbf{h}_k \mathbf{v}_{k+1}, \ldots, 2\mathbf{h}_k \mathbf{v}_K, (\mathcal{F}_k - 1)]^{\dagger} \right\| \leq \mathcal{F}_k + 1, & k = 1, 2, \ldots, K-1 \\ 0 \leq \mathcal{F}_K, & k = K, \end{cases} \tag{33d}$$

$$|\mathbf{h}_k \mathbf{v}_m|^2 \leq \mathcal{H}_{ki}\left(\mathbf{v}_i, \bar{\mathbf{v}}_i\right), \tag{33e}$$

$$|\mathbf{h}_k \mathbf{v}_1|^2 \leq 2Re\left(\mathbf{h}_k \mathbf{v}_{jam} \bar{\mathbf{v}}_{jam}^{\dagger} \mathbf{h}_k^{\dagger}\right) - Re\left(\mathbf{h}_k \bar{\mathbf{v}}_{jam} \bar{\mathbf{v}}_{jam}^{\dagger} \mathbf{h}_k^{\dagger}\right), \tag{33f}$$

$$\left\| \left[\mathbf{v}_1^{\dagger}, \mathbf{v}_2^{\dagger}, \ldots, \mathbf{v}_K^{\dagger}, \mathbf{v}_{jam}^{\dagger}\right]^{\dagger} \right\| = \sqrt{P_{BS}}. \tag{33g}$$

The proposed Algorithm 1 converges, according to the results in [34]. Especially, in each iteration, the jamming transmit power $\|\mathbf{v}_{jam}\|^2$ becomes higher than or equal to the value in the previous iteration. On the other hand, due to the rate requirement of legitimate users and transmit power constraint of the BS, the maximum value of $\|\mathbf{v}_{jam}\|^2$ is limited. Thus, the convergence of Algorithm 1 can be guaranteed.

IV. Zero-Forcing Scheme for Jamming

In Section III, the jamming transmit power can be maximized to disrupt the potential eavesdropping, with the performance of legitimate users guaranteed. However, in (14), the total transmit power at the BS, P_{BS}, is also constrained. When P_{BS} is insufficient, the channels of legitimate users are under severe fading, or the legitimate users require high transmission rate, the constraint (14c) can be no longer satisfied. This is because the received jamming power cannot always be higher than the received signal power of all the other users at all legitimate receivers.

For example, when (14) cannot be effectively solved due to the transmit power constraint, assume that the order of received power at each receiver can be achieved as

$$\begin{cases} |\mathbf{h}_1\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_1\mathbf{v}_{jam}|^2 \leq |\mathbf{h}_1\mathbf{v}_l|^2 \leq \cdots \leq |\mathbf{h}_1\mathbf{v}_1|^2 \\ |\mathbf{h}_2\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_2\mathbf{v}_{jam}|^2 \leq |\mathbf{h}_2\mathbf{v}_l|^2 \leq \cdots \leq |\mathbf{h}_2\mathbf{v}_1|^2 \\ \cdots\cdots \\ |\mathbf{h}_K\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_{jam}|^2 \leq |\mathbf{h}_K\mathbf{v}_l|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_1|^2. \end{cases} \tag{40}$$

In this case, the legitimate transmission from the 1st user to the lth user will also be affected by artificial jamming, although the eavesdropping can be disrupted at the same time.

Thus, in this section, a zero-forcing scheme for jamming is proposed there are enough antennas equipped at the BS, in which the transmit jamming power is maximized, with its interference zero-forced at each legitimate receiver.

A. Scheme II

When the transmit power at the BS cannot satisfy (14), the artificial jamming can be zero-forced by the BS at each legitimate receiver via beamforming as

$$\mathbf{h}_1\mathbf{v}_{jam} = \mathbf{h}_2\mathbf{v}_{jam} = \ldots = \mathbf{h}_K\mathbf{v}_{jam} = 0. \tag{41}$$

Particularly, the SIC decoding order in Section II can be rewritten as

$$\begin{cases} 0 = |\mathbf{h}_1\mathbf{v}_{jam}|^2 \leq \max\limits_{m=2,\ldots,K} |\mathbf{h}_1\mathbf{v}_m|^2 \leq |\mathbf{h}_1\mathbf{v}_1|^2 \\ \cdots\cdots \\ 0 = |\mathbf{h}_k\mathbf{v}_{jam}|^2 \leq \max\limits_{m=k+1,\ldots,K} |\mathbf{h}_k\mathbf{v}_m|^2 \\ \qquad \leq |\mathbf{h}_k\mathbf{v}_k|^2 \leq \cdots \leq |\mathbf{h}_k\mathbf{v}_1|^2 \\ \cdots\cdots \\ 0 = |\mathbf{h}_K\mathbf{v}_{jam}|^2 \leq |\mathbf{h}_K\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_1|^2. \end{cases} \tag{42}$$

Thus, according to (42), the received SINR at the kth receiver can be also expressed as (12) and (13).

With the QoS requirements of all the legitimate users and the decoding order satisfied, the optimization problem can be formulated as

$$\max_{\substack{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_K,\\ \mathbf{v}_{jam}}} \|\mathbf{v}_{jam}\|^2 \tag{43a}$$

$$s.t.\ \mathrm{SINR}_k^k \geq r_k, \quad k \in \mathcal{K}, \tag{43b}$$

$$\begin{cases} 0 = |\mathbf{h}_1\mathbf{v}_{jam}|^2 \leq \max\limits_{m=2,\ldots,K} |\mathbf{h}_1\mathbf{v}_m|^2 \leq |\mathbf{h}_1\mathbf{v}_1|^2 \\ \cdots\cdots \\ 0 = |\mathbf{h}_k\mathbf{v}_{jam}|^2 \leq \max\limits_{m=k+1,\ldots,K} |\mathbf{h}_k\mathbf{v}_m|^2 \\ \qquad \leq |\mathbf{h}_k\mathbf{v}_k|^2 \leq \cdots \leq |\mathbf{h}_k\mathbf{v}_1|^2 \\ \cdots\cdots \\ 0 = |\mathbf{h}_K\mathbf{v}_{jam}|^2 \leq |\mathbf{h}_K\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_1|^2. \end{cases} \tag{43c}$$

$$\sum\nolimits_{i=1}^{K} \|\mathbf{v}_i\|^2 + \|\mathbf{v}_{jam}\|^2 = P_{BS}, \quad i \in \mathcal{K}. \tag{43d}$$

Thus, the potential eavesdropping can also be effectively disrupted by maximizing the transmit jamming power in (42), without affecting the legitimate transmission via zero-forcing.

The optimization problem (43) is non-convex, and is difficult to solve. Using similar approximations to (33), the problem (43) can be transformed into a convex one as (44) at the bottom of next page. Accordingly, Algorithm 1 can also be used to solve (43).

Nevertheless, sufficient antennas should be equipped at the BS to perform zero-forcing; otherwise, the problem still remains unsolvable. Lemma 1 is introduced to determine the minimum number of antennas required to perform zero-forcing at the BS as follows.

Lemma 1: Zero-forcing in (43c) can be achieved when

$$M \geq K + 1. \tag{45}$$

Proof: A generic polynomial system can be solved if and only if the number of variables is no less than the number of equations. For the zero-forcing in (43c), the number of equations can be denoted as

$$\mathcal{N}_e = K. \tag{46}$$

The number of effective variables in the zero-forcing of (43c) can be expressed as

$$\mathcal{N}_v = M - 1. \tag{47}$$

When the number of variables is no less than the number of equations, we have

$$\mathcal{N}_e \leq \mathcal{N}_v \Rightarrow K \leq M - 1 \Rightarrow M \geq K + 1 \tag{48}$$

which can guarantee the feasibility of zero-forcing. ■

On the other hand, when the number of antennas is not sufficient and the transmit power at BS P_BS is low, both optimization problems of (14) and (43) cannot be solved. In this case, we can relax the decoding order of (42) into

$$\begin{cases} 0 < |\mathbf{h}_1\mathbf{v}_{jam}|^2 \leq \max_{m=2,\ldots,K} |\mathbf{h}_1\mathbf{v}_m|^2 \leq |\mathbf{h}_1\mathbf{v}_1|^2 \\ \cdots\cdots \\ 0 < |\mathbf{h}_k\mathbf{v}_{jam}|^2 \leq \max_{m=k+1,\ldots,K} |\mathbf{h}_k\mathbf{v}_m|^2 \\ \qquad \leq |\mathbf{h}_k\mathbf{v}_k|^2 \leq \cdots \leq |\mathbf{h}_k\mathbf{v}_1|^2 \\ \cdots\cdots \\ 0 < |\mathbf{h}_K\mathbf{v}_{jam}|^2 \leq |\mathbf{h}_K\mathbf{v}_K|^2 \leq \cdots \leq |\mathbf{h}_K\mathbf{v}_1|^2. \end{cases} \tag{49}$$

which will not be further discussed in this paper.

B. Comparison of the Two Schemes

The key features of the proposed two schemes are compared as follows.

- *Feasibility:* Scheme I is most feasible when the transmit power of the BS, P_{BS}, is high enough, without considering the number of antennas at the BS. Scheme II is feasible only when enough antennas are equipped at the BS, i.e., $M \geq K+1$, but the transmit power of the BS can be lower.
- *Performance:* When the transmit power of the BS is sufficient, the secrecy rate of Scheme I is higher than that of Scheme II, as more transmit power can be allocated to artificial jamming. However, when the transmit power of the BS is low, only Scheme II is feasible.
- *Complexity:* Comparing the optimization problems of (14) and (43), the computational complexity of these two schemes is almost the same, with that of Scheme II a little lower than that of the first one. For the detail of complexity analysis, refer to Appendix.

Thus, the proposed two schemes should be utilized according to the practical requirements of the systems. When the transmit power of the BS is sufficient, Scheme I can achieve better performance. When the transmit power of the BS becomes lower, Scheme II can be utilized instead of Scheme I due to its better feasibility in this case.

V. Simulation Results and Discussion

Simulation results are provided to evaluate the performances of the two proposed schemes. In the simulation, we set $\beta = 10^{-4}$ and $\alpha = 2.5$, and the received SINR threshold at all users is assumed to be r. For simplicity, we denote the kth user as U_k, $k = 1, 2, \ldots, K$, and the distance from the BS to the users and eavesdropper can be denoted as D in meters, i.e., $D = (D_{U_1}, D_{U_2}, \ldots, D_{U_{K-1}}, D_{U_K}, D_e)$, where D_e denotes the distance from the BS to the eavesdropper.

The optimal jamming power in Scheme I is compared for different values of r and σ^2 in Fig. 2. We use values $M = 3$, $K = 3$, $P_{BS} = 10$ dBm and $D = (200, 100, 50, 90)$. From the results, we can see that the jamming power becomes higher when r is smaller. This is because more power can be allocated to the jamming when the QoS requirement of the users is relaxed. In addition, the jamming power increases when σ^2 decreases, due to the fact that the QoS of users can be achieved with less transmit power, and thus more power can be allocated for jamming.

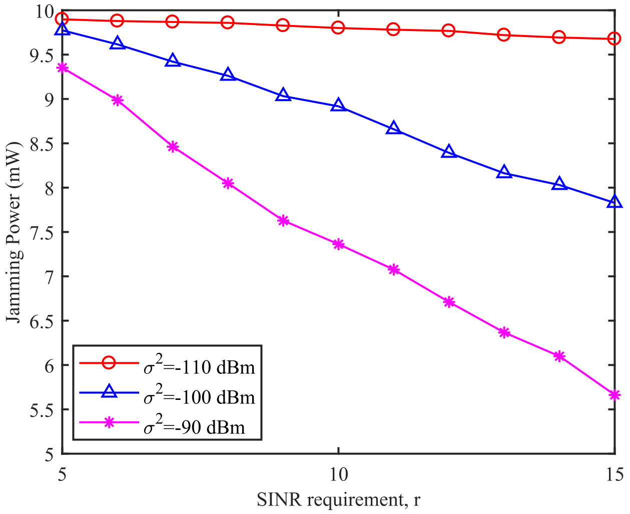


Fig. 2. Comparison of the optimal jamming power in Scheme I with different SINR threshold r and channel noise σ^2, for $M = 3$, $K = 3$, $P_{BS} = 10$ dBm and $D = (200, 100, 50, 90)$.

The average secrecy rate and eavesdropping rate of the users in Scheme I are compared in Fig. 3 for different values of r. $M = 3$, $K = 3$, $\sigma^2 = -110$ dBm, $P_{BS} = 10$ dBm and $D = (200, 100, 50, 90)$. From Fig. 3, we can see that the eavesdropping can be disrupted by the artificial jamming effectively in Scheme I, and the eavesdropping rate is close to 0. In addition, the secrecy rate of the users can be improved significantly when r is larger, due to the fact that the improvement of transmission rate results in higher secrecy rate with smaller eavesdropping rate.

In addition, taking (10) as a benchmark, the eavesdropping rate and secrecy rate of the users in Scheme I and Scheme (10) are compared in Fig. 4 and Fig. 5, respectively, for different values of P_{BS}. $M = 3$, $K = 3$, $\sigma^2 = -110$ dBm, $r = 12$ bit/s/Hz and $D = (200, 100, 50, 90)$. From Fig. 4, we can see that the eavesdropping rate of the users in Scheme I is reduced by artificial jamming compared to that of Scheme (10). Especially, the eavesdropping rate is lower than 0.2 bit/s/Hz in Scheme I, and decreases with higher P_{BS}, which means that more power can be allocated to the

$$\max_{\substack{\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_K,\\ \mathbf{v}_{jam}}} \; t \tag{44a}$$

$$s.t.\; t \geq 0, \tag{44b}$$

$$t \leq 2Re\left(\mathbf{v}_{jam}^{\dagger}\bar{\mathbf{v}}_{jam}\right) - Re\left(\bar{\mathbf{v}}_{jam}^{\dagger}\bar{\mathbf{v}}_{jam}\right), \tag{44c}$$

$$\begin{cases} \left\|\left[2\mathbf{h}_k\mathbf{v}_{k+1}, \ldots, 2\mathbf{h}_k\mathbf{v}_K, (\mathcal{F}_k - 1)\right]^{\dagger}\right\| \leq \mathcal{F}_k + 1, & k = 1, 2, \ldots, K-1 \\ 0 \leq \mathcal{F}_K, & k = K, \end{cases} \tag{44d}$$

$$|\mathbf{h}_k\mathbf{v}_m|^2 \leq \mathcal{H}_{ki}\left(\mathbf{v}_i, \bar{\mathbf{v}}_i\right), \tag{44e}$$

$$(41) \text{ and } \left\|\left[\mathbf{v}_1^{\dagger}, \mathbf{v}_2^{\dagger}, \ldots, \mathbf{v}_K^{\dagger}, \mathbf{v}_{jam}^{\dagger}\right]^{\dagger}\right\| = \sqrt{P_{BS}}. \tag{44f}$$

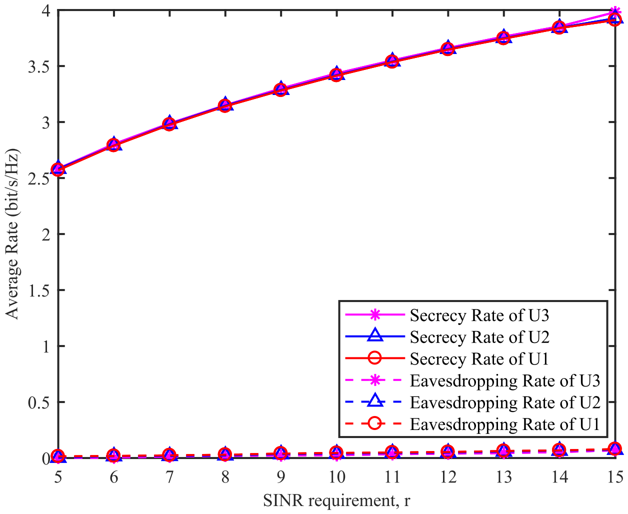


Fig. 3. Comparison of the secrecy rate and eavesdropping rate of the users in Scheme I with different SINR threshold r, for $M = 3$, $K = 3$, $\sigma^2 = -110$ dBm, $P_{BS} = 10$ dBm and $D = (200, 100, 50, 90)$.

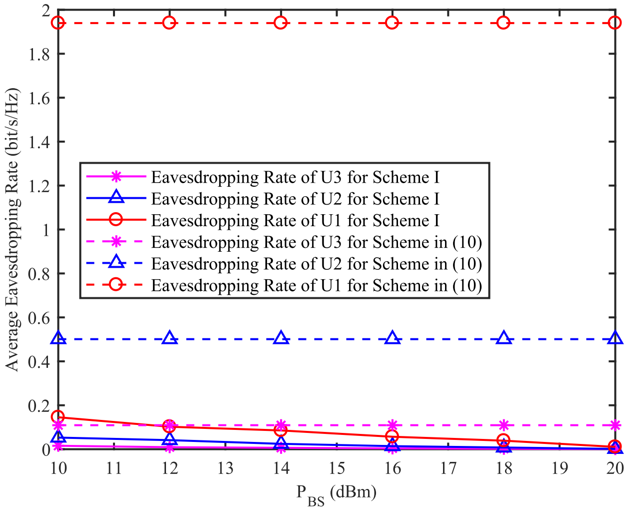


Fig. 4. Eavesdropping rate comparison of the users in Scheme I and Scheme (10) with different values of P_{BS}, for $M = 3$, $K = 3$, $\sigma^2 = -110$ dBm, $r = 12$ bit/s/Hz and $D = (200, 100, 50, 90)$.

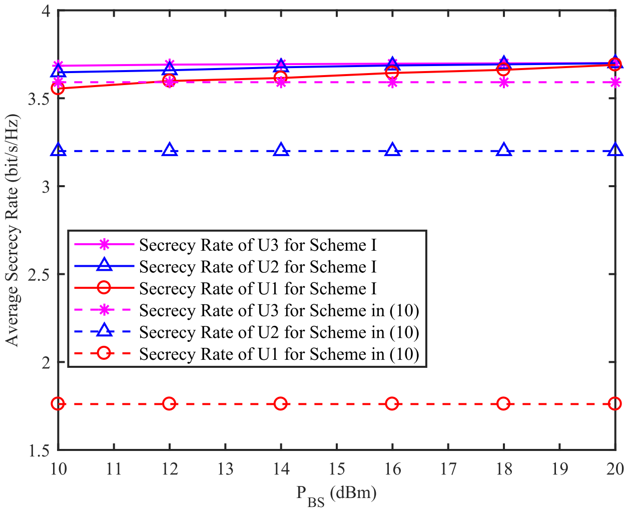


Fig. 5. Secrecy rate comparison of the users in Scheme I and Scheme (10) with different values of P_{BS}, for $M = 3$, $K = 3$, $\sigma^2 = -110$ dBm, $r = 12$ bit/s/Hz and $D = (200, 100, 50, 90)$.

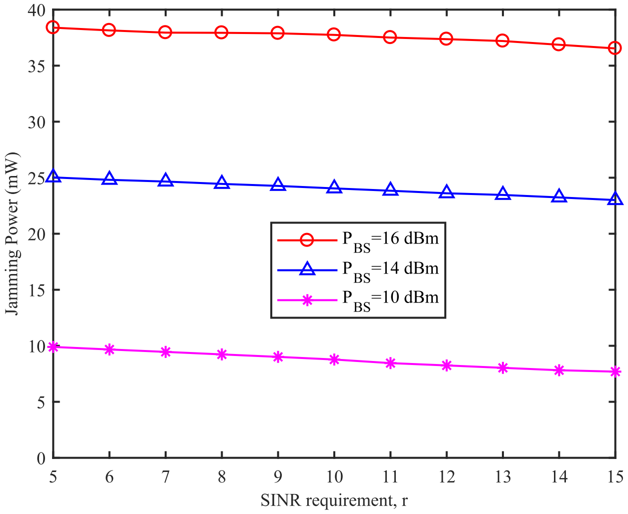


Fig. 6. Comparison of the optimal jamming power in Scheme II with different values of r and P_{BS}, for $M = 4$, $K = 3$, $\sigma^2 = -110$ dBm and $D = (200, 100, 50, 90)$.

jamming. In addition, we can also find that the eavesdropping rate of the 1st user is higher than that of the other two users, due to its highest transmit power. From Fig. 5, we can see that the secrecy rate of Scheme I is much higher than that of Scheme (10), as the eavesdropping rate can be disrupted effectively by artificial jamming. In addition, the secrecy rate increases with P_{BS} in Scheme I, which means that more power can be allocated to jamming when P_{BS} is higher.

In Fig. 6, the optimal jamming power in Scheme II is compared for different values of r and P_{BS}, with $M = 4$, $K = 3$, $\sigma^2 = -110$ dBm and $D = (200, 100, 50, 90)$. From the result, we can see that the jamming power at the NOMA BS increases with P_{BS} in Scheme II, as more power can be allocated for jamming when the total transmit power of the BS is higher. Thus, the security of the network can be enhanced with higher P_{BS}. In addition, the jamming power decreases with the SINR threshold r, because more transmit power is needed to satisfy the QoS needed by the users.

The secrecy rate and eavesdropping rate of U_1 in Scheme II are compared in Fig. 7 for different values of r and P_{BS}. Only U_1 is considered, due to the fact that its security is threatened most. We consider values $M = 4$, $K = 3$, $\sigma^2 = -110$ dBm and $D = (200, 100, 50, 90)$. From the results, we can observe that the eavesdropping rate can be reduced effectively by artificial jamming in Scheme II, although the eavesdropping rate increases a little with the SINR requirement r. Thus, the secrecy rate of U_1 increases with r, due to the enhancement of transmission rate. In addition, higher P_{BS} will reduce the eavesdropping rate, and thus improve the secrecy rate of U_1.

The secrecy rate of U_1 is compared for both Scheme I and Scheme II in Fig. 8, for different values of r and P_{BS}, for $M = 4$, $K = 3$, $\sigma^2 = -110$ dBm and $D = (200, 100, 50, 90)$. From the result, we can see that the secrecy

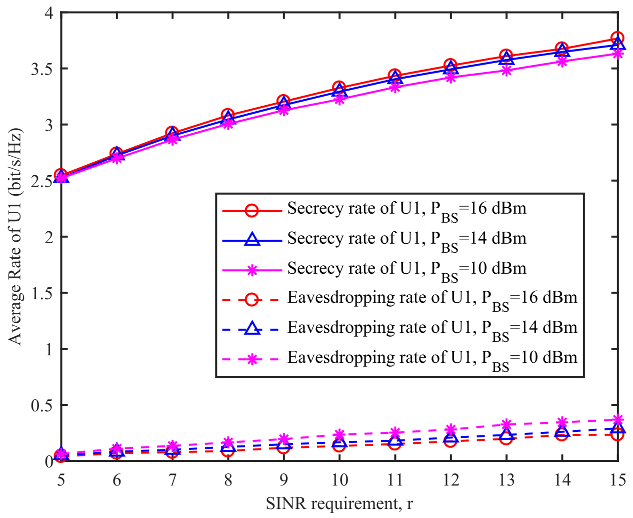


Fig. 7. Comparison of the secrecy rate and eavesdropping rate of U_1 in Scheme II, with different values of r and P_{BS}, for $M = 4$, $K = 3$, $\sigma^2 = -110$ dBm and $D = (200, 100, 50, 90)$.

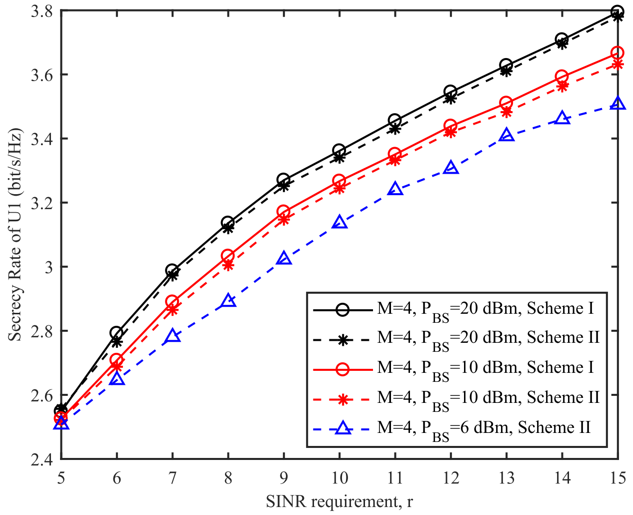


Fig. 8. Comparison of the secrecy rate of U_1 in both Scheme I and Scheme II with different values of r and P_{BS}, for $K = 3$, $\sigma^2 = -110$ dBm and $D = (200, 100, 50, 90)$.

rate in both Scheme I and Scheme II can be guaranteed by artificial jamming, which disrupts the potential eavesdropping effectively. In addition, the secrecy rate of U_1 increases with r, due to the fact that the transmission rate increases obviously with r, although the eavesdropping rate may also increase a little. Furthermore, the secrecy rate of Scheme I is a little higher than that of Scheme II when P_{BS} is relatively higher, i.e., for $P_{BS} = 20$ dBm and $P_{BS} = 10$ dBm. However, when P_{BS} becomes lower, e.g., $P_{BS} = 6$ dBm, the optimization problem (14) in Scheme I can no longer be solved, i.e., Scheme I becomes infeasible. While for Scheme II, it is always feasible even when the transmit power of the BS is lower, e.g., $P_{BS} = 6$ dBm, as long as enough antennas are equipped at the BS according to Lemma 1.

VI. Conclusions and Future Work

In this paper, through generating artificial jamming at the BS, we have proposed two joint beamforming and jamming optimization schemes for MISO-NOMA networks to guarantee security with the existence of a potential eavesdropper. In the first scheme, the transmit power of artificial jamming has been maximized, with its received power at each receiver higher than that of other users. Thus, the jamming signal can be cancelled via SIC before others, and the eavesdropping can be disrupted effectively without affecting the legitimate transmission. When the transmit power of the BS is not sufficient, a second scheme has been proposed, in which the transmit jamming power is maximized with the jamming signal zero-forced at each receiver. Due to the non-convexity of these two optimization problems, they have been first transformed into convex problems, and an iterative algorithm has been proposed to solve them based on conventional concave-convex procedure. Simulation results have shown the efficiency and effectiveness of the proposed two schemes. In our future work, dynamic decoding order of SIC will be further considered to guarantee the security of NOMA.

Appendix
Computational Complexity Analysis

According to [35], we can know that the computational complexity of the interior-point algorithm for second-order cone programming (SOCP) is normally based on the number of variables, constraints and its dimensions.

In Scheme I, the number of constraints in (33) can be expressed as $(K^2 + K + 3)$. Thus, the number of iterations exploited to reduce the duality gap to a threshold can be upper bounded by $\mathcal{O}\left(\sqrt{K^2 + K + 3}\right)$. The number of variables and dimensions for all constraints in (33) can be calculated as $(K^2+K+2(K+1)M+1)$ and $(3.5K^2+2.5K+(K+2)M+1)$, respectively. Therefore, the computational complexity of Algorithm 1 for Scheme I can be obtained as (50), at the bottom of this page.

Similarly, the number of constraints of Scheme II in (44) is $(K^2 + K + 3)$, and the items $(K^2 + K + 2(K + 1)M + 1)$ and $(3.5K^2 + 0.5K + (K + 2)M + 1)$ are the number of variables and dimensions, respectively. Thus, the complexity of Algorithm 1 for Scheme II can be obtained as (51), at the bottom of this page.

Comparing (50) with (51), we can conclude that the complexity of Scheme II is a little lower than that of Scheme I, which is consistent as the analysis in Section IV-B.

$$\mathcal{O}\left(N\sqrt{K^2+K+3}\left(K^2+K+2(K+1)M+1\right)^2\left(3.5K^2+2.5K+(K+2)M+1\right)\right). \tag{50}$$

$$\mathcal{O}\left(N\sqrt{K^2+K+3}\left(K^2+K+2(K+1)M+1\right)^2\left(3.5K^2+0.5K+(K+2)M+1\right)\right). \tag{51}$$

REFERENCES

[1] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. 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.

[2] H. Kim, D. J. Love, and S. Y. Park, "Optimal and successive approaches to signal design for multiple antenna physical layer multicasting," *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2316–2327, Aug. 2011.

[3] 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, Sep. 2015.

[4] 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.

[5] 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.

[6] Q. Sun, S. Han, C. L. I, and Z. Pan, "On the ergodic capacity of MIMO NOMA systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 405–408, Aug. 2015.

[7] 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.

[8] H. Lin, F. Gao, S. Jin, and G. Y. Li, "A new view of multi-user hybrid massive MIMO: Non-orthogonal angle division multiple access," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2268–2280, Oct. 2017.

[9] F. Zhou, Y. Wu, Y.-C. Liang, Z. Li, Y. Wang, and K.-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.

[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. 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. Mobile Comput.*, vol. 17, no. 11, pp. 2591–2606, Nov. 2018.

[12] L. Xiao, Y. Li, C. Dai, H. Dai, and H. V. Poor, "Reinforcement learning-based NOMA power allocation in the presence of smart jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3377–3389, Apr. 2018.

[13] D. Wan, M. Wen, F. Ji, Y. Liu, and Y. Huang, "Cooperative NOMA systems with partial channel state information over Nakagami-m fading channels," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 947–958, Mar. 2018.

[14] 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. 2207–2220, Oct. 2017.

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

[16] 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.

[17] Y. Cao *et al.*, "Optimization or alignment: Secure primary transmission assisted by secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, Apr. 2018.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] N. Zhao, F. R. Yu, M. Li, and V. C. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[23] N. Zhao *et al.*, "Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2281–2294, May 2018.

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

[25] 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.

[26] H. Lei *et al.*, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.

[27] 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.

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

[29] 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.

[30] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "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.

[31] 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.

[32] 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.

[33] 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.

[34] B. K. Sriperumbudur and G. R. G. Lanckriet, "A proof of convergence of the concave-convex procedure using Zangwill's theory," *Neural Comput.*, vol. 24, no. 6, pp. 1391–1407, 2012.

[35] M. S. Lobo, L. Vandenberghe, S. Boyd, and H. Lebret, "Applications of second-order cone programming," *Linear Algebra Appl.*, vol. 284, nos. 1–3, pp. 193–228, Nov. 1998.

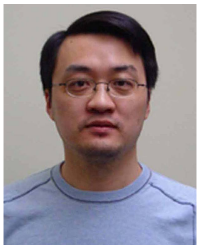
Nan Zhao (S'08–M'11–SM'16) received the Ph.D. degree in information and communication engineering from the Harbin Institute of Technology, Harbin, China, in 2011. He is currently an Associate Professor with the Dalian University of Technology, China.

Dr. Zhao received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018. He also received the Best Paper Awards in IEEE VTC 2017, MLICOM 2017, ICNC 2018, WCSP 2018, and CSPS 2018. He is serving or served on the Editorial Boards of seven SCI-indexed journals, including the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING.

Wei Wang received the B.S. degree from the Hefei University of Technology, China, in 2018. He is currently pursuing the degree with the School of Information and Communication Engineering, Dalian University of Technology, China.

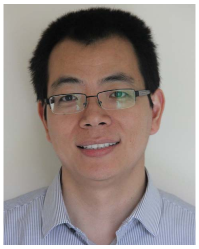
His current research interests include non-orthogonal multiple access, wireless power transfer, and physical layer security.

Jingjing Wang (M'15) received the B.S. degree in industrial automation from Shandong University, Jinan, China, in 1997, the M.Sc. degree in control theory and control engineering from the Qingdao University of Science and Technology, Qingdao, China, in 2002, and the Ph.D. degree in computer application technology from the Ocean University of China, Qingdao, in 2012. From 2014 to 2015, she was a Visiting Professor with The University of British Columbia. She is currently a Professor with the School of Information Science and Technology, Qingdao University of Science and Technology. Her research interests include underwater wireless sensor network, acoustic communications, ultra-wideband radio systems, and multiple-input multiple-output wireless communications.



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

Yun Lin received the B.S. degree from Dalian Maritime University in 2003, the M.S. degree from the Harbin Institute of Technology in 2005, and the Ph.D. degree from Harbin Engineering University in 2010. From 2014 to 2015, he was a Visiting Scholar with Wright State University, Dayton, OH, USA. He is currently an Associate Professor with Harbin Engineering University. His current research interests include communication technology, signal processing, information fusion, cognitive radio, and software-defined radio.



Zhiguo Ding (S'03–M'05–SM'14) received the B.Eng. degree in electrical engineering from the Beijing University of Posts and Telecommunications in 2000 and the Ph.D. degree in electrical engineering from the Imperial College London in 2005. From 2005 to 2018, he was with Queen's University Belfast, the Imperial College, Newcastle University, and Lancaster University. From 2012 to 2018, he has also been an academic visitor at Princeton University. Since 2018, he has been a Professor of communications with The University of Manchester.

Dr. Ding's research interests are 5G networks, game theory, cooperative and energy harvesting networks, and statistical signal processing. He was an Editor of the IEEE Wireless Communications Letters and the IEEE Communications Letters from 2013 to 2016. He is serving as an Editor for the IEEE Transactions on Communications, the IEEE Transactions on Vehicular Technology, and the *Journal of Wireless Communications and Mobile Computing*. 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, the IEEE Heinrich Hertz Award 2018, and the IEEE Jack Neubauer Memorial Award 2018.

Norman C. Beaulieu (S'82–M'84–SM'89–F'99–LF'18) received the B.A.Sc., M.A.Sc., and Ph.D. degrees from The University of British Columbia, Vancouver, Canada. He was a Queen's National Scholar Professor with Queen's University, Kingston, and an Alberta Informatics Circle of Research Excellence and Canada Research Chair Professor of broadband wireless communications with the University of Alberta, Edmonton, Canada. He is currently a Thousand Talents Research Professor with the Beijing University of Posts and Telecommunications, Beijing, China. He has authored or co-authored over 350 journal papers and over 430 conference papers. His current research interests are the statistical modeling of wireless channels, massive multiple-input multiple-output systems, heterogeneous wireless networks, femtocells, estimation theory, rapid simulation methods and techniques, cooperative communications, wideband wireless communications, cognitive radio, signal processing in communications, and impulse radio UWB.

Dr. Beaulieu is a fellow of the Royal Society of Canada, IET, EIC, and CAE and an NSERC E.W.R. Steacie Memorial Fellow. He was a recipient of number of awards. He is the only person in the world to hold both the IEEE Edwin Howard Armstrong Technical Achievement Award, named for the inventor of FM, and the IEEE Reginald Aubrey Fessenden Medal for Technical Achievement, named for the inventor of AM. In 2016, he received the title State Specially Recruited Experts bestowed upon him by the Minister of Human Resources and Social Insurance and the Vice Minister of the Organization Department, Y. Weimin. He has served as technical program chair or the symposium chair of multiple international conferences. He was the Editor-in-Chief of the IEEE Transactions on Communications for four years. He has served on funding committees in multiple countries and organizations. He has served on the Editorial Board of the Proceedings of the IEEE for six years. He has been a special editor, a senior editor, and an associate editor of a number of the IEEE and non-IEEE journals.