Secure Transmission for Interference Networks: User Selection and Transceiver Design

Nan Zhao, *Senior Member, IEEE,* Qiuyi Cao, Guan Gui, *Senior Member, IEEE,* Yang Cao, Shun Zhang, Yunfei Chen, *Senior Member, IEEE* and Hikmet Sari, *Fellow, IEEE*

***Abstract*—Interference is usually regarded as a detrimental factor that degrades the performance of a wireless network. However, when it is used properly, the security of transmission can be effectively improved. In this paper, user selection and transceiver design are proposed to guarantee the secure transmission in a multiple-input multiple-output interference network with an eavesdropper. First, user selection is performed to select the most suitable user to transmit confidential information according to the topology and path loss in each time slot among all users. Then, based on user selection, the transceivers of the users are jointly designed to maximize the secrecy rate of the selected user while guaranteeing a minimum transmission rate for other users. Due to the non-convexity of the optimization problem, it is transformed into a convex second-order cone programming with the help of successive approximations. An alternate iteration algorithm is proposed to obtain the optimal solution. The fairness of the user selection is considered, and a modified scheme is proposed to share the opportunity of secure transmission among users. Finally, simulation results are presented to show the effectiveness and efficiency of the proposed schemes.**

***Index Terms*—Interference networks, multiple-input multiple-output, physical layer security, secrecy rate, transceiver design, user selection.**

I. Introduction

Recently, 5G has become the main focus of wireless communications. It aims to achieve higher data rate, lower latency, more connections and better quality of service (QoS) [1], [2]. Due to the broadcasting nature of the wireless channel, secure transmission is always a challenge for mobile networks, especially 5G [3]. On the other hand, as massive connections are required for Internet of Things in 5G networks, severe interference among users will degrade the system performance seriously. This needs to be properly solved in order to guarantee the QoS [4]. On the other hand, if interference can be properly managed and controlled, it can actually benefit 5G networks, especially for the secure transmission [5].

When some potential eavesdroppers exist to wiretap the confidential message in the legitimate wireless networks, the security of transmission will be at risk [6]. Conventional anti-eavesdropping methods usually entrust the cryptography in the upper layer, which may endure heavy signal overhead and cause latency [7]. Recently, physical layer security has emerged as a promising solution to protecting the wireless transmission [8], [9]. In Wyner's landmark work, a discrete and memoryless channel subject to wiretap was described, and the conclusion was drawn that perfect secrecy rate can be nearly achieved in his hypothetical encoder-decoder wiretap channel model [10].

Following this pioneering research, extensive explorations have been conducted on the physical layer security in wireless networks, especially in the last decade [11]–[22]. In [11], a joint beamforming and jamming scheme was proposed by Wang *et al.*, to disturb the potential eavesdropping in a two-way relay network with single antenna. Some fundamental work was done on jointly optimizing the information and jamming beamforming by Zhu *et al.* in [12], to guarantee both the transmit and receive security for a full-duplex base station. In [13], Li and Ma designed an artificial noise (AN) aided secure transmission scheme for a multiple-input single-output (MISO) channel with multiple eavesdroppers. Shu *et al.* proposed two effective schemes in [14] to guarantee the secure transmission for directional modulation networks with the help of secure multicast precoding. In [15], the secrecy outage probability was analyzed in a multiple-input multiple-output (MIMO) network over Nakagami-m channels by Lei *et al.*, in which transmit antenna selection is performed to improve the security performance. Fan *et al.* analyzed the impact of cochannel interference on the secure transmission in [16], in which the secrecy information was transferred to the destination via several relays. In [17], Bi and Chen proposed a novel new cooperative jamming scheme, in which a full-duplex jammer was adopted to disrupt the eavesdropping with the power supply from energy harvesting. The secrecy outage probability was derived by Fan *et al.* in the secure cooperative networks via using outdated relay selection [18]. In [19], the transmit beamforming was optimized by Zhu *et al.* for secure transmission of full-duplex networks with self-interference mitigation. The transceiver design was performed by Kong *et*

Manuscript received April 29, 2018; revised October 20, 2018 and December 24, 2018; accepted January 4, 2019. The research was supported by the National Natural Science Foundation of China (NSFC) under Grant 61871065 and 61871455, 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. *(Corresponding author: Guan Gui.)*

N. Zhao, Q. Cao and Y. Cao are with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116023, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710071, P. R. China. (e-mail: zhaonan@dlut.edu.cn; Cao_qiuyi@mail.dlut.edu.cn; cy216@mail.dlut.edu.cn).

G. Gui is with the Nanjing University of Posts and Telecommunications, Nanjing 210028, China (e-mail: guiguan@njupt.edu.cn).

S. Zhang is with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, 710071, P. R. China. (Email: zhangshunsdu@xidian.edu.cn).

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

H. Sari is with the the Nanjing University of Posts and Telecommunications, Nanjing 210028, China, and also with Sequans Communications, 92700 Colombes, France (e-mail: hikmet@njupt.edu.cn).

al. in [20] to guarantee the secure transmission via minimum total mean-squared error criterion in interference networks. In [21], Zhou *et al.* proposed an AN-aided cooperative jamming scheme with wireless energy harvesting. Some excellent work was done by Cai *et al.* in [22] on jointly transceiver design to guarantee the secure transmission in a MIMO relay system.

On the other hand, the performance of secure transmission in multi-user networks can be guaranteed, if the interference can be properly managed and controlled, through which it can become beneficial [23]–[27]. In [23], Chen and Zhang proposed mode selection to guarantee the security of information transmission in MU-MIMO downlink networks. A tradeoff was made between a smaller number of accessing users to avoid high interference among users and a larger number of accessing users to generate strong interference to disrupt the eavesdropping. In our previous works, interference alignment (IA) was adopted to exploit the interference to achieve secure transmission [24]–[26]. In [24], two IA-based anti-eavesdropping schemes were proposed to guarantee the secure transmission via zero-forcing or AN, respectively, with or without the eavesdropping channel state information (CSI). In [25], beneficial jamming was leveraged via IA to protect the security of legitimate interference networks. However, the performance of IA is not optimal, due to the fact that interference alignment does not maximize the signal-to-interference-plus-noise ratio (SINR). When the transceivers are jointly optimized in interference networks, better performance can be achieved. In [26], an AN-assisted IA scheme was proposed to guarantee the secure transmission of interference network, in which the AN is also utilized for wireless power transfer. In [27], two schemes were proposed to guarantee the secrecy rate of the primary user with the help of secondary users in cognitive radio networks, by using optimal transceiver design and IA, respectively. In the research, the key features of these two interference management techniques were also demonstrated.

Based on the above observations, in this paper, the performance of secure transmission for interference networks is guaranteed through using user selection and transceiver design. The eavesdropping towards the secure user is disrupted by the interference from other users. The main contributions of this paper can be summarized as follows.

- User selection a kind of opportunistic communications [28], and it is performed in an interference network with multiple users, in which the most suitable user can be chosen to perform secure transmission in each time slot with the existence of an adversarial eavesdropper. To reduce the complexity of user selection effectively, a suboptimal scheme is proposed that only uses the distance information between the nodes in the network.
- Based on user selection, the legitimate transceivers are jointly designed to disrupt the eavesdropping, through which the secrecy rate of the secure user is maximized, with the rate threshold of other users guaranteed. This optimization is difficult to solve due to its non-convexity. Thus, an alternate optimization algorithm is proposed to calculate suboptimal solutions with lower complexity.
- In the proposed user selection scheme, the secure user may always be the same if the network topology does not change, which is unfair among users. Accordingly, a modified user selection scheme is proposed considering the fairness, to give all the legitimate users the opportunity of secure transmission. To further measure the fairness of these schemes, Jain's index is adopted.

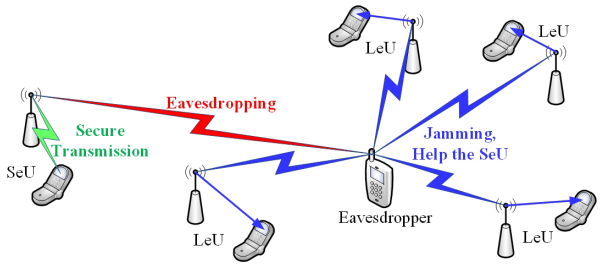


Fig. 1. Demonstration of the secure transmission in MIMO interference networks via user selection and transceiver design.

The rest of this paper is organized as follows. In Section II, the system model is presented. In Section III, the secure user selection scheme is proposed. Based on user selection, the joint optimal transceiver design is proposed in Section IV, with its low-complexity algorithm derived. In Section V, a modified user selection scheme is designed to improve the fairness among users. Simulation results are presented in Section VI, followed by the conclusions in Section VII.

Notation: $\mathbb{C}^{M\times N}$ is the space of complex $M\times N$ matrices. $\mathcal{CN}(\mathbf{a},\mathbf{A})$ represents the complex Gaussian distribution, where $\mathbf{a}$ and $\mathbf{A}$ are the mean and covariance matrices, respectively. $Re\{\cdot\}$ denotes the real operator and $\mathbb{E}(\cdot)$ is the expectation.

II. System Description

In this paper, a MIMO interference network with $K+1$ users is considered with an eavesdropper, as shown in Fig. 1. Assume that M_t, N_r and N_e antennas are equipped at each transmitter, each receiver, and the eavesdropper, respectively. To guarantee the secure transmission for the legitimate network, a specific user is selected to transmit confidential information in each time slot, denoted as the secure user (SeU), with the help of all the other K legitimate users (LeUs) as jamming signals. Thus, all the users in the network can have the opportunity to perform secure transmission within multiple time slots. The distance from the transmitter to its corresponding receiver is assumed to be equal for convenience. The path loss of all channels is given by

$$\rho = \beta d^{-\alpha}, \tag{1}$$

where d denotes the distance between the transceivers, α represents the path loss exponent, and β is the path loss at unit distance.

Thus, the decoded signal at the SeU receiver can be expressed as

$$\mathbf{y}_D=\sqrt{\rho_{DS}}\mathbf{u}_D^{\dagger}\mathbf{H}_{DS}\mathbf{v}_S x_S+\sum_{k=1}^{K}\sqrt{\rho_D^{[k]}}\mathbf{u}_D^{\dagger}\mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}x^{[k]}+\mathbf{u}_D^{\dagger}\mathbf{n}_D, \tag{2}$$

where x_S and $x^{[k]}$ are the transmitted signal from the SeU and the kth LeU with unit power, respectively. $\mathbf{v}_S\in\mathbb{C}^{M_t\times 1}$

and $\mathbf{v}_B^{[k]} \in \mathbb{C}^{M_t \times 1}$ are the precoding vectors of the SeU and the kth LeU, respectively, with transmit power $\|\mathbf{v}_S\|^2 = P_S$ and $\left\|\mathbf{v}_B^{[k]}\right\|^2 = P^{[k]}$. $\mathbf{u}_D \in \mathbb{C}^{N_r \times 1}$ is the unitary decoding vector at the SeU. $\mathbf{H}_{DS} \in \mathbb{C}^{N_r \times M_t}$ and $\mathbf{H}_D^{[k]} \in \mathbb{C}^{N_r \times M_t}$ represent the small-scale Rayleigh fading channel matrices from the SeU transmitter and the kth LeU transmitter to the SeU receiver, respectively, each entity of which is independent and identically distributed (i.i.d) complex Gaussian following $\mathcal{CN}(0,1)$. ρ_{DS} and $\rho_D^{[k]}$ represent the path loss from the SeU transmitter and the kth LeU transmitter to the SeU receiver, respectively, according to (1). The additive white gaussian noise (AWGN) vector at the SeU receiver can be expressed as $\mathbf{n}_D \in \mathcal{CN}\left(\mathbf{0}, \sigma_D^2 \mathbf{I}_{N_r}\right)$.

Then, the decoded signal at the receiver of the kth LeU can be presented as

$$\mathbf{y}_B^{[k]} = \sqrt{\rho_B^{[kk]}}\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kk]}\mathbf{v}_B^{[k]}x^{[k]} + \sqrt{\rho_S^{[k]}}\mathbf{u}_B^{[k]\dagger}\mathbf{H}_{BS}^{[k]}\mathbf{v}_S x_S + \sum\nolimits_{j=1,j\neq k}^{K} \sqrt{\rho_B^{[kj]}}\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kj]}\mathbf{v}_B^{[j]}x^{[j]} + \mathbf{u}_B^{[k]\dagger}\mathbf{n}_B, \quad (3)$$

where $\mathbf{u}_B^{[k]} \in \mathbb{C}^{N_r \times 1}$ is the unitary decoding vector at the kth LeU. $\mathbf{H}_B^{[kj]} \in \mathbb{C}^{N_r \times M_t}$ and $\mathbf{H}_{BS}^{[k]} \in \mathbb{C}^{N_r \times M_t}$ denote the small-scale Rayleigh fading channel matrices from the jth LeU transmitter and the SeU transmitter to the kth LeU receiver, respectively. $\rho_S^{[k]}$ and $\rho_B^{[kj]}$ are the path-loss gain from the SeU transmitter and the jth LeU transmitter to the kth LeU receiver, respectively. $\mathbf{n}_B \in \mathcal{CN}\left(\mathbf{0}, \sigma_B^2 \mathbf{I}_{N_r}\right)$ is the AWGN noise vector at the kth LeU receiver.

In addition, the decoded signal at the eavesdropper can be written as

$$\mathbf{y}_E = \sqrt{\rho_{ES}}\mathbf{u}_E^\dagger \mathbf{H}_{ES}\mathbf{v}_S x_S + \sum_{k=1}^{K} \sqrt{\rho_E^{[k]}}\mathbf{u}_E^\dagger \mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}x^{[k]} + \mathbf{u}_E^\dagger \mathbf{n}_E. \quad (4)$$

where $\mathbf{u}_E \in \mathbb{C}^{N_e \times 1}$ denotes the unitary decoding vector at the eavesdropper. $\mathbf{H}_{ES} \in \mathbb{C}^{N_e \times M_t}$ and $\mathbf{H}_E^{[k]} \in \mathbb{C}^{N_e \times M_t}$ are the small-scale Rayleigh fading channel matrices from the SeU transmitter and the kth LeU transmitter to the eavesdropper, respectively. ρ_{ES} and $\rho_E^{[k]}$ represent the path-loss gain from the SeU transmitter and the kth LeU transmitter to the eavesdropper, respectively. $\mathbf{n}_E \in \mathcal{CN}\left(\mathbf{0}, \sigma_E^2 \mathbf{I}_{N_e}\right)$ is the AWGN noise vector at the eavesdropper.

From (2), the received SINR at the SeU receiver can be expressed as

$$\mathrm{SINR}_D = \frac{\rho_{DS}\left|\mathbf{u}_D^\dagger \mathbf{H}_{DS}\mathbf{v}_S\right|^2}{\sigma_D^2 + \sum_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^\dagger \mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2}. \quad (5)$$

Also, from (3), the received SINR at the kth LeU receiver can be described as

$$\mathrm{SINR}_B^{[k]} = \frac{\rho_B^{[kk]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kk]}\mathbf{v}_B^{[k]}\right|^2}{\sigma_B^2 + \rho_S^{[k]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_S^{[k]}\mathbf{v}_S\right|^2 + \sum\limits_{j=1,j\neq k}^{K}\rho_B^{[kj]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kj]}\mathbf{v}_B^{[j]}\right|^2}. \quad (6)$$

In addition, from (4), the received SINR at the eavesdropper towards the SeU can be written as

$$\mathrm{SINR}_E = \frac{\rho_{ES}\left|\mathbf{u}_E^\dagger \mathbf{H}_{ES}\mathbf{v}_S\right|^2}{\sigma_E^2 + \sum_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^\dagger \mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2}. \quad (7)$$

From (5), the transmission rate of the SeU can be expressed as

$$R_D = \log_2\left(1 + \mathrm{SINR}_D\right) = \log_2\left(1 + \frac{\rho_{DS}\left|\mathbf{u}_D^\dagger \mathbf{H}_{DS}\mathbf{v}_S\right|^2}{\sigma_D^2 + \sum_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^\dagger \mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2}\right). \quad (8)$$

The eavesdropping rate can be derived from (7) as

$$R_E = \log_2\left(1 + \mathrm{SINR}_E\right) = \log_2\left(1 + \frac{\rho_{ES}\left|\mathbf{u}_E^\dagger \mathbf{H}_{ES}\mathbf{v}_S\right|^2}{\sigma_E^2 + \sum_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^\dagger \mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2}\right). \quad (9)$$

Thus, the secrecy rate of the SeU can be defined as the difference between its transmission rate and the eavesdropping rate as

$$R_S = (R_D - R_E)^+ = \left(\log_2 \frac{1 + \frac{\rho_{DS}\left|\mathbf{u}_D^\dagger \mathbf{H}_{DS}\mathbf{v}_S\right|^2}{\sigma_D^2 + \sum_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^\dagger \mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2}}{1 + \frac{\rho_{ES}\left|\mathbf{u}_E^\dagger \mathbf{H}_{ES}\mathbf{v}_S\right|^2}{\sigma_E^2 + \sum_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^\dagger \mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2}}\right)^+. \quad (10)$$

where $(\cdot)^+ \triangleq \max(0, \cdot)$. In this paper, user selection and transceiver design will be performed to guarantee the secure transmission of the SeU with the help of LeUs.

III. User Selection for Secure Transmission

To guarantee the secure transmission in MIMO interference networks, user selection and transceiver design should be jointly optimized to achieve the optimal performance. This is a mixed-integer non-convex problem. To do this, user selection should be performed $K+1$ times based on transceiver design when exhaustive search is utilized, i.e., the transceiver design should be optimized $K+1$ times to obtain the optimal selection. In Section IV, we will show that the computational complexity of transceiver design is relatively high, and thus, the overall computational complexity of this direct exhaustive search is $K+1$ times of that for the transceiver design, which may not be suitable for practical utilization.

In practical systems, path loss will cause severe performance degradation, which is a key factor that affects user selection. Therefore, user selection and transceiver design are separated, and a suboptimal user selection scheme is proposed only based on the path-loss information, which is much easier to implement. By doing so, the overall computational complexity will be reduced to nearly $\frac{1}{K+1}$ of that when the user selection and transceiver design are optimized jointly.

To make user selection much easier to achieve, we assume that the transmit power allocated to each LeU and SeU all equals to P_T. Thus, we have $\mathbb{E}\left[\left\|\mathbf{u}^{\dagger}\mathbf{H}\mathbf{v}\right\|^2\right] = P_T$, which has been proved in [29]. Based on this assumption, according to (8), the transmission rate of SeU can be approximated as

$$\bar{R}_D = \log_2\left(1 + \frac{P_T\rho_{DS}}{\sigma_D^2 + P_T\sum_{k=1}^{K}\rho_D^{[k]}}\right). \tag{11}$$

Similarly, according to (9), the eavesdropping rate at the eavesdropper can be approximated as

$$\bar{R}_E = \log_2\left(1 + \frac{P_T\rho_{ES}}{\sigma_E^2 + P_T\sum_{k=1}^{K}\rho_E^{[k]}}\right). \tag{12}$$

Thus, the secrecy rate for the SeU can be approximated as

$$\begin{aligned}\bar{R}_S &= \left(\bar{R}_D - \bar{R}_E\right)^+ \\ &= \log_2\left(\frac{1 + \frac{P_T\rho_{DS}}{\sigma_D^2 + P_T\sum_{k=1}^{K}\rho_D^{[k]}}}{1 + \frac{P_T\rho_{ES}}{\sigma_E^2 + P_T\sum_{k=1}^{K}\rho_E^{[k]}}}\right).\end{aligned} \tag{13}$$

To select the optimal user, the user with the highest secrecy rate should be chosen as SeU for secure transmission in the current time slot. The objective function of the optimization problem can be expressed as

$$\begin{aligned}\Omega^* &= \arg\max_{\Omega}\bar{R}_S \\ &= \arg\max_{\Omega}\left(\frac{1 + \frac{P_T\rho_{DS}}{\sigma_D^2 + P_T\sum_{k=1}^{K}\rho_D^{[k]}}}{1 + \frac{P_T\rho_{ES}}{\sigma_E^2 + P_T\sum_{k=1}^{K}\rho_E^{[k]}}}\right),\end{aligned} \tag{14}$$

where Ω is the set containing available solutions for the user selection.

The combinatorial optimization problem in (14) can be further simplified with some reasonable approximations when SINR is high or the noise power is small, as shown in Proposition 1.

Proposition 1: When SINR is high and the noise power is small, the optimization problem in (14) can be simplified as

$$\Omega^* = \arg\max_{\Omega}\frac{\rho_{DS}}{\rho_{ES}}\frac{\sum_{k=1}^{K}\rho_E^{[k]}}{\sum_{k=1}^{K}\rho_D^{[k]}}. \tag{15}$$

Proof: See Appendix A. ∎

Remark 1: ρ_{DS} in (15) is assumed to be a constant as the distance between each pair of transceiver is fixed. Thus, the optimal user selection is determined by ρ_{ES}, $\sum_{k=1}^{K}\rho_E^{[k]}$ and $\sum_{k=1}^{K}\rho_D^{[k]}$. Firstly, ρ_{ES} should be smaller, which means that the distance between the SeU transmitter and the eavesdropper should be longer to avoid eavesdropping. Secondly, $\sum_{k=1}^{K}\rho_E^{[k]}$ should be larger, due to the fact that the distance between LeU transmitters and the eavesdropper should be shorter to generate jamming signals to disrupt the eavesdropping. Lastly, $\sum_{k=1}^{K}\rho_D^{[k]}$ should be smaller, which means that the distance between the LeU transmitters and the SeU receiver should be longer to guarantee the QoS of secure transmission. Therefore, this suboptimal user selection scheme can be achieved with only the distance information between the nodes in the network considered, which can achieve reliable performance with extremely low computational complexity.

IV. Joint Optimal Transceiver Design

In this section, the performance of secure transmission for the SeU is optimized with the help of LeUs, via joint optimal transceiver design. First, the problem formulation is presented, and then an alternate iteration algorithm is proposed to solve this non-convex problem.

A. Problem Formulation

After determining the SeU using user selection, we can optimize the performance of secure transmission for the SeU via joint optimal transceiver design for both the SeU and LeUs, with the QoS of each LeU guaranteed and the constraint of total transmit power for the legitimate network satisfied. The optimization problem of the joint optimal transceiver design can be expressed as

$$\max_{\mathbf{u}_D,\mathbf{v}_S,\mathbf{u}_B^{[k]},\mathbf{v}_B^{[k]}}\left(\log_2\frac{1+\frac{\rho_{DS}\left|\mathbf{u}_D^{\dagger}\mathbf{H}_{DS}\mathbf{v}_S\right|^2}{\sigma_D^2+\sum_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^{\dagger}\mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2}}{1+\frac{\rho_{ES}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_{ES}\mathbf{v}_S\right|^2}{\sigma_E^2+\sum_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2}}\right)^+ \tag{16a}$$

$$s.t. \quad \mathrm{SINR}_B^{[k]} \geq \gamma_{lim}, \tag{16b}$$

$$\sum_{k=1}^{K}\left\|\mathbf{v}_B^{[k]}\right\|^2 + \|\mathbf{v}_S\|^2 \leq P_A, \tag{16c}$$

$$\left\|\mathbf{u}_B^{[k]}\right\|^2 = \|\mathbf{u}_D\|^2 = 1,\ \forall k = 1,2,\ldots,K. \tag{16d}$$

In (16), γ_{lim} is the SINR threshold for each LeU, and P_A is the constraint on the sum transmit power of the legitimate network. We should notice that the eavesdropping CSI is known by the legitimate users, which can be achieved when the eavesdropper is also a registered user of the network, but cannot participate in the secure transmission. Similar assumptions have also been made in many existing works [13], [20], [27], [30]. $\mathbf{u}_E$ is the decoding vector at the eavesdropper that aims to maximize the received SINR of the signal from SeU according to [31]. When $\mathbf{u}_E$ is developed through other methods at the eavesdropper, the eavesdropping rate will be lower than that using the MAX-SINR method. Thus, the lower bound to the secrecy rate for SeU can be achieved via (16).

We can observe that (16) is non-convex, which is difficult to solve. In the following, we will transform the problem into a convex one with some necessary approximations, and then solve the problem by an alternate iteration algorithm.

B. Alternate Optimization

First, we optimize the precoding vector $\mathbf{v}$ of each user with decoding vectors $\mathbf{u}$ fixed, which should satisfy $\|\mathbf{u}\|^2 = 1$. Furthermore, some auxiliary variables, i.e., $S_D \geq 1$ and $S_E \in$

$(0,1)$, are introduced to help the approximating. Consequently, the problem (16) can be changed into

$$\max_{\mathbf{v}_S,\mathbf{v}_B^{[k]},S_D,S_E} \quad \log_2 S_D S_E \tag{17a}$$

$$s.t. \quad 1+\frac{\rho_{DS}\left|\mathbf{u}_D^{\dagger}\mathbf{H}_{DS}\mathbf{v}_S\right|^2}{\sigma_D^2+\sum_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^{\dagger}\mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2}\geq S_D, \tag{17b}$$

$$1+\frac{\rho_{ES}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_{ES}\mathbf{v}_S\right|^2}{\sigma_E^2+\sum_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2}\leq \frac{1}{S_E}, \tag{17c}$$

$$\frac{\rho_B^{[kk]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kk]}\mathbf{v}_B^{[k]}\right|^2}{\sigma_B^2+\rho_S^{[k]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_S^{[k]}\mathbf{v}_S\right|^2+\sum\limits_{j=1,j\neq k}^{K}\rho_B^{[kj]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kj]}\mathbf{v}_B^{[j]}\right|^2}\geq\gamma_{lim}, \tag{17d}$$

$$\sum\nolimits_{i=1}^{K}\left|\left|\mathbf{v}_B^{[k]}\right|\right|^2+||\mathbf{v}_S||^2\leq P_A, \tag{17e}$$

$$\left\|\mathbf{u}_B^{[k]}\right\|^2=||\mathbf{u}_D||^2=1,\ \forall k=1,2,\ldots,K. \tag{17f}$$

The constraints (17b)-(17d) can be further rewritten as

$$\sigma_D^2+\sum\nolimits_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^{\dagger}\mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2\leq\frac{\rho_{DS}\left|\mathbf{u}_D^{\dagger}\mathbf{H}_{DS}\mathbf{v}_S\right|^2}{S_D-1}, \tag{18}$$

$$\sigma_E^2+\rho_{ES}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_{ES}\mathbf{v}_S\right|^2+\sum\nolimits_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2\leq\frac{\sigma_E^2+\sum_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2}{S_E}, \tag{19}$$

$$\sigma_B^2+\rho_S^{[k]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_S^{[k]}\mathbf{v}_S\right|^2+\sum\nolimits_{j=1,\ j\neq k}^{K}\rho_B^{[kj]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kj]}\mathbf{v}_B^{[j]}\right|^2\leq\frac{\rho_B^{[kk]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kk]}\mathbf{v}_B^{[k]}\right|^2}{\gamma_{lim}},\ \forall k=1,2,\ldots,K. \tag{20}$$

From (18)-(19), we can see that although the formulas on both sides of the inequalities are convex, these two constraints are still non-convex. Therefore, we can employ the first-order Taylor expansions to make them convex. Lemma 1 is first presented as follows.

Lemma 1 : For a specific quadratic-over-linear function $F_{\mathbf{A},\psi}(\mathbf{y},x)=\frac{\mathbf{A}^{\dagger}\mathbf{y}\mathbf{y}^{\dagger}\mathbf{A}}{x-\psi}$, where $\mathbf{A}$ satisfies $\mathbf{A}\mathbf{A}^{\dagger}\succeq 0$ and $x\geq\psi$, we can use the first-order Taylor expansion as

$$\mathcal{F}_{\mathbf{A},\psi}(\mathbf{y},x,\hat{\mathbf{y}},\hat{x})=\frac{2Re\left\{\hat{\mathbf{y}}^{\dagger}\mathbf{A}\mathbf{A}^{\dagger}\mathbf{y}\right\}}{\hat{x}-\psi}-\frac{\hat{\mathbf{y}}^{\dagger}\mathbf{A}\mathbf{A}^{\dagger}\hat{\mathbf{y}}}{(\hat{x}-\psi)^2}(x-\psi). \tag{21}$$

Proof: See Appendix B. ∎

Note that the approximations will not break the feasibility of the problem because $Re\left\{\mathbf{A}^{\dagger}\hat{\mathbf{y}}\hat{\mathbf{y}}^{\dagger}\mathbf{A}\right\}\leq\mathbf{A}^{\dagger}\hat{\mathbf{y}}\hat{\mathbf{y}}^{\dagger}\mathbf{A}$ for complex values.

By using the above transformation, the non-convex constraints (18) and (19) can be converted into convex ones. Specifically, we define two auxiliary variables as

$$\mathbf{A}_1=\left[\mathbf{u}_D^{\dagger}\mathbf{H}_{DS}\right]^{\dagger}, \tag{22}$$

$$\mathbf{A}_2=\left[\mathbf{u}_E^{\dagger}\mathbf{H}_E^{[k]}\right]^{\dagger}. \tag{23}$$

Furthermore, $\mathbf{y}$ can be substituted by the precoding vectors. Thus, the right side of the constraint (18) can be expressed as

$$\mathcal{R}_1=\rho_{DS}\left[\frac{2Re\left\{\hat{\mathbf{v}}_S^{\dagger}\mathbf{A}_1\mathbf{A}_1^{\dagger}\mathbf{v}_S\right\}}{\hat{S}_D-1}-\frac{\hat{\mathbf{v}}_S^{\dagger}\mathbf{A}_1\mathbf{A}_1^{\dagger}\hat{\mathbf{v}}_S}{\left(\hat{S}_D-1\right)^2}(S_D-1)\right]. \tag{24}$$

Similarly, the right side of the constraint (19) can be transformed into

$$\mathcal{R}_2=\frac{\sigma_E^2}{\hat{S}_E^2}\left(2\hat{S}_E-S_E\right)+\sum\nolimits_{k=1}^{K}\rho_E^{[k]}\left[\frac{2Re\left\{\hat{\mathbf{v}}_B^{[k]\dagger}\mathbf{A}_2\mathbf{A}_2^{\dagger}\mathbf{v}_B^{[k]}\right\}}{\hat{S}_E}-\frac{\hat{\mathbf{v}}_B^{[k]\dagger}\mathbf{A}_2\mathbf{A}_2^{\dagger}\hat{\mathbf{v}}_B^{[k]}}{\hat{S}_E^2}S_E\right]. \tag{25}$$

Thus, the constraints (18) and (19) can be transformed into convex ones. To make it concise, we can also define

$$\mathcal{R}_3^{[k]}=\frac{\sqrt{\rho_B^{[kk]}}\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kk]}\mathbf{v}_B^{[k]}}{\sqrt{\gamma_{lim}}},\ \forall k=1,2,\ldots,K, \tag{26}$$

$$\Gamma_1=\mathcal{R}_1-\sigma_D^2, \tag{27}$$

$$\Gamma_2=\mathcal{R}_2-\sigma_E^2, \tag{28}$$

$$\Gamma_3=\mathcal{R}_3^{[k]}. \tag{29}$$

Thus, the optimization problem (17), can be approximately rewritten as

$$\max_{\mathbf{v}_S,\mathbf{v}_B^{[k]},S_D,S_E} \quad S_D S_E \tag{30a}$$

$$s.t. \ \sum\nolimits_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^{\dagger}\mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2\leq\Gamma_1, \tag{30b}$$

$$\rho_{ES}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_{ES}\mathbf{v}_S\right|^2+\sum\nolimits_{k=1}^{K}\rho_E^{[k]}\left|\mathbf{u}_E^{\dagger}\mathbf{H}_E^{[k]}\mathbf{v}_B^{[k]}\right|^2\leq\Gamma_2, \tag{30c}$$

$$\rho_S^{[k]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_S^{[k]}\mathbf{v}_S\right|^2+\sum_{j=1,j\neq k}^{K}\rho_B^{[kj]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kj]}\mathbf{v}_B^{[j]}\right|^2+\sigma_B^2\leq\Gamma_3^2, \tag{30d}$$

$$\sum_{k=1}^{K}\left\|\mathbf{v}_B^{[k]}\right\|^2+\|\mathbf{v}_S\|^2\leq P_A,\forall k=1,2,\ldots,K. \tag{30e}$$

We can observe that the objective function is still not convex. Maximizing $S_D S_E$ is equivalent to maximizing $\sqrt{S_D S_E}$, due to the fact that both of them are nonnegative. Therefore, the problem (30) can be changed into

$$\max_{\mathbf{v}_S,\mathbf{v}_B^{[k]},S_D,S_E} \quad t>0 \tag{31a}$$

$$s.t. \quad t^2\leq S_D S_E, \tag{31b}$$

$$(30b)-(30e). \tag{31c}$$

$$\max_{\mathbf{v}_S,\mathbf{v}_B^{[k]},S_D,S_E} \quad \log_2 t \tag{32a}$$

$$s.t. \quad \left\|[2t, S_D - S_E]^\dagger\right\| \le S_D + S_E, \tag{32b}$$

$$\left\|\left[2\sqrt{\rho_D^{[1]}}|\mathbf{u}_D^\dagger \mathbf{H}_D^{[1]}\mathbf{v}_B^{[1]}|, 2\sqrt{\rho_D^{[2]}}|\mathbf{u}_D^\dagger \mathbf{H}_D^{[2]}\mathbf{v}_B^{[2]}|, \ldots, 2\sqrt{\rho_D^{[K]}}|\mathbf{u}_D^\dagger \mathbf{H}_D^{[K]}\mathbf{v}_B^{[K]}|, \Gamma_1 - 1\right]^\dagger\right\| \le \Gamma_1 + 1, \tag{32c}$$

$$\left\|\left[2\sqrt{\rho_{ES}}|\mathbf{u}_E^\dagger \mathbf{H}_{ES}\mathbf{v}_S|, 2\sqrt{\rho_E^{[1]}}|\mathbf{u}_E^\dagger \mathbf{H}_E^{[1]}\mathbf{v}_B^{[1]}|, \ldots, 2\sqrt{\rho_E^{[K]}}|\mathbf{u}_E^\dagger \mathbf{H}_E^{[K]}\mathbf{v}_B^{[K]}|, \Gamma_2 - 1\right]^\dagger\right\| \le \Gamma_2 + 1, \tag{32d}$$

$$\left\|\left[2\sigma_B, 2\sqrt{\rho_S^{[k]}}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_S^{[k]}\mathbf{v}_S\right|, 2\sqrt{\rho_B^{[k1]}}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}^{[k1]}\mathbf{v}_B^{[1]}\right|, \ldots, 2\sqrt{\rho_B^{[kK]}}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[k]}\mathbf{v}_B^{[K]}\right|\right]^\dagger\right\| \le 2\Gamma_3, \tag{32e}$$

$$\sum_{k=1}^{K}\left\|\mathbf{v}_B^{[k]}\right\|^2 + \|\mathbf{v}_S\|^2 \le P_A, \forall k = 1, 2, \ldots, K. \tag{32f}$$

It is worth noting that the constraints of (31) in the form of $x^2 \le x_1 x_2$ can be converted into the form of $\left\|[2x, (x_1 - x_2)]^\dagger\right\| \le x_1 + x_2$ by means of second-order cone programming (SOCP), $x_1 \ge 0$ and $x_2 \ge 0$. Thus, we can apply this transformation to (31), to give (32) on the top of next page. The problem (32) is convex, which can be solved through the existing toolboxes such as CVX easily.

Then, the decoding vector $\mathbf{u}$ of each user can be optimized with fixed precoding vectors $\mathbf{v}$, in which S_E is a fixed value. Thus, the optimization problem (16) can be changed into

$$\max_{\mathbf{u}_D,\mathbf{u}_B^{[k]},S_D} \quad S_D \tag{33a}$$

$$s.t. \quad 1 + \frac{\rho_{DS}\left|\mathbf{u}_D^\dagger \mathbf{H}_{DS}\mathbf{v}_S\right|^2}{\sigma_D^2 + \sum_{k=1}^{K}\rho_D^{[k]}\left|\mathbf{u}_D^\dagger \mathbf{H}_D^{[k]}\mathbf{v}_B^{[k]}\right|^2} \ge S_D, \tag{33b}$$

$$\frac{\rho_B^{[kk]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kk]}\mathbf{v}_B^{[k]}\right|^2}{\sigma_B^2 + \rho_S^{[k]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_S^{[k]}\mathbf{v}_S\right|^2 + \sum\limits_{j=1,\ j\ne k}^{K}\rho_B^{[kj]}\left|\mathbf{u}_B^{[k]\dagger}\mathbf{H}_B^{[kj]}\mathbf{v}_B^{[j]}\right|^2} \ge \gamma_{lim}, \tag{33c}$$

$$\left\|\mathbf{u}_B^{[k]}\right\|^2 = ||\mathbf{u}_D||^2 = 1, \ \forall k = 1, 2, \ldots, K. \tag{33d}$$

By exploiting the SOCP, (33) can also be changed into a convex one approximately, which can be solved by using existing toolboxes such as CVX.

Thus, the suboptimal solutions of (16) can be calculated by optimizing (32) and (33) alternately until convergence.

C. Proposed Alternate Optimization Algorithm

With all the derivations above, we can summarize the proposed alterative optimization algorithm for (16) as Algorithm 1 based on SOCP, which is guaranteed to be convergent according to [32]. Specifically, the value of t becomes larger than or is equal to its previous value at each iteration. In addition, due to the fact that the sum transmit power is limited and the resource is allocated to LeUs to guarantee their QoS, the secrecy rate has an upper bound. Therefore, we can conclude that Algorithm 1 is guaranteed to converge.

Algorithm 1 Alternate Optimization Algorithm for (16)

1: Start with initializing the number of iterations N and the basic feasible values of network $\left(\hat{\mathbf{v}}_S, \hat{\mathbf{v}}_B^{[k]}, \hat{S}_D, \hat{S}_E, \gamma_{lim}\right)$. Set $\left(\hat{\mathbf{u}}_D, \hat{\mathbf{u}}_B^{[k]}\right)$ satisfying $\|\hat{\mathbf{u}}_D\|^2 = 1$ and $\left\|\hat{\mathbf{u}}_B^{[k]}\right\|^2 = 1$.
2: **repeat**
3: Solve the issue (32) by CVX and save the solutions $\left(\mathbf{v}_S{}^*, \mathbf{v}_B^{[k]*}, S_{D_1}{}^*, S_E{}^*\right)$.
4: Solve the issue (33) with the initial values of the previous step $\left(\mathbf{v}_S{}^*, \mathbf{v}_B^{[k]*}, S_{D_1}{}^*\right)$ by CVX and obtain $\left(\mathbf{u}_D{}^*, \mathbf{u}_B^{[k]*}, S_{D_2}{}^*\right)$.
5: Update the elements $\left(\hat{\mathbf{v}}_S, \hat{\mathbf{v}}_B^{[k]}, \hat{\mathbf{u}}_D, \hat{\mathbf{u}}_B^{[k]}, \hat{S}_D, \hat{S}_E\right) = \left(\mathbf{v}_S{}^*, \mathbf{v}_B^{[k]*}, \mathbf{u}_D^*, \mathbf{u}_B^{[k]*}, S_{D_2}{}^*, S_E{}^*, \right)$.
6: $n = n + 1$
7: **until** $n = N$.
8: Output the solutions: $\mathbf{v}_B^{[k]}$, $\mathbf{v}_S$, $\mathbf{u}_B^{[k]}$ and $\mathbf{u}_D$, $k = 1, \ldots, K$.

Remark 2: The number of antennas can affect the performance of the proposed scheme. When the number of antennas increases, more resource can be exploited to improve the system performance, i.e., the secrecy rate of the SeU can be further enhanced. On the other hand, when the number of antennas decreases, the antenna resource will be limited, and the performance will be degraded. In some extreme cases, inadequate antennas can even make (16) unsolvable, i.e., the SINR requirements for the LeUs in (16b) cannot be satisfied.

V. User Selection with Fairness

In Section III, low-complexity user selection scheme was proposed to select the user with the maximum secrecy rate as the SeU. However, if the relative locations do not change, the results of the selection will not change either. This will result in the unfairness among users. In order to give the opportunity of secure transmission to all legitimate users, a modified user selection scheme is proposed considering fairness in this section. In addition, Jain's index is adopted to measure the fairness of the network.

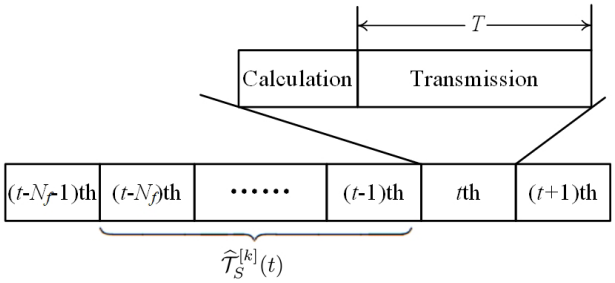


Fig. 2. Demonstration of the user selection scheme with fairness.

A. User Selection with Fairness

Considering fairness among users, we propose a modified user selection scheme to guarantee the secure transmission of interference networks, as shown in Fig. 2.

Assume that the transmission duration for each time slot is T. For the current tth time slot, the secrecy throughput for the kth user when selected as SeU during the last N_f time slots can be expressed as

$$\widehat{\mathcal{T}}_S^{[k]}(t)=\sum_{j=t-N_f}^{t-1} R_S^{[k]}(j)T,\ k=1,2,\ldots,K+1,\ t>N_f. \quad (34)$$

$R_S^{[k]}(j)$ is the secrecy rate of the kth user at the jth time slot, which equalled to 0 when it was selected as LeU in that time slot. Based on (34), we can define a factor for the kth user as

$$\Delta^{[k]}(t)=\frac{\frac{1}{\widehat{\mathcal{T}}_S^{[k]}(t)}}{\frac{1}{K+1}\sum_{l=1}^{K+1}\frac{1}{\widehat{\mathcal{T}}_S^{[l]}(t)}}=\frac{\frac{1}{\sum_{j=t-N_f}^{t-1}R_S^{[k]}(j)}}{\frac{1}{K+1}\sum_{l=1}^{K+1}\frac{1}{\sum_{j=t-N_f}^{t-1}R_S^{[l]}(j)}}, \quad (35)$$

where $\Delta^{[k]}(t)$ indicates the opportunity for the kth user to be selected as the SeU in the tth time slot. When $\Delta^{[k]}(t)$ is larger, it means that the secrecy throughput of the kth user is smaller in the last N_f time slots, and more opportunity should be allocated to the kth user to perform secure transmission in the current tth time slot.

Based on the above assumptions, the objective function for the user selection scheme with fairness can be presented as

$$\max_{s_1,s_2,\ldots,s_{K+1}} \sum_{k=1}^{K+1}\bar{R}_S^{[k]}s_k\Delta^{[k]} \quad (36a)$$

$$s.t. \quad \sum_{k=1}^{K+1}s_k=1, \quad (36b)$$

$$s_k\in\{0,1\},\ \forall k=1,2,\ldots,K+1. \quad (36c)$$

In (36), s_k=1 represents that the kth user is selected as SeU in the current time slot, while s_k=0 implies the opposite. $\bar{R}_S^{[k]}$ denotes the secrecy rate for the kth user that is calculated according to the optimization (16) in the current time slot, when the kth user is set as the SeU.

In our proposed user selection scheme with fairness in (36), the optimization for secrecy rate and the secrecy throughput in the last N_f slots for each user are jointly considered. Thus, tradeoff can be made between the performance of secure transmission and the fairness among users through our proposed user selection.

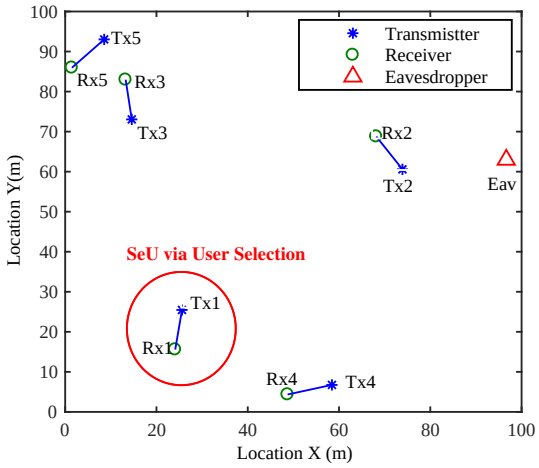


Fig. 3. Demonstration of the topology for a 5-user interference network with an eavesdropper, and the result of the proposed user selection scheme based on (15).

B. Jain's Index

To measure the fairness of the proposed user selection scheme in (36) effectively, Jain's index is adopted, which can be presented as

$$J=\frac{\left(\sum_{k=1}^{K+1}\mathcal{T}_S^{[k]}\right)^2}{(K+1)\sum_{k=1}^{K+1}\left(\mathcal{T}_S^{[k]}\right)^2}, \quad (37)$$

where $\mathcal{T}_S^{[k]}$ is the secrecy throughput for the kth users in the overall duration utilized to measure the fairness. It can be observed that J ranges from $1/(K+1)$ to 1 in (37). $J=1/N$ refers to the least fair case, in which the secure transmission is performed by only one user all the time, while $J=1$ stands for the fairest case, in which all the users have equal opportunity to perform secure transmission. In this paper, Jain's index will be adopted to measure the fairness of user selection in the simulation part.

VI. Simulation Results and Discussion

In the simulation, all users are randomly distributed in a 100 m×100 m area, where the distance between each transmitter and its corresponding receiver is set to be 10 m. For the path-loss model, we set $\alpha=2.6$ and $\beta=0.0001$ in (1). The noise power at each receiver is set to be -110 dBm. We set $M_t=N_r=N_e=5$. To show the rate performance much clearly, we will demonstrate the simulation with the rate threshold instead of the SINR threshold, which can be easily calculated as $r_{lim}=\log_2(1+\gamma_{lim})$. Without loss of generality, the 1st user is assumed to be selected as the SeU for secure transmission in the current time slot.

First, a 5-user interference network with one eavesdropper is considered, whose topology is depicted as Fig. 3. From the results, we can see that the 1st user is relatively far from

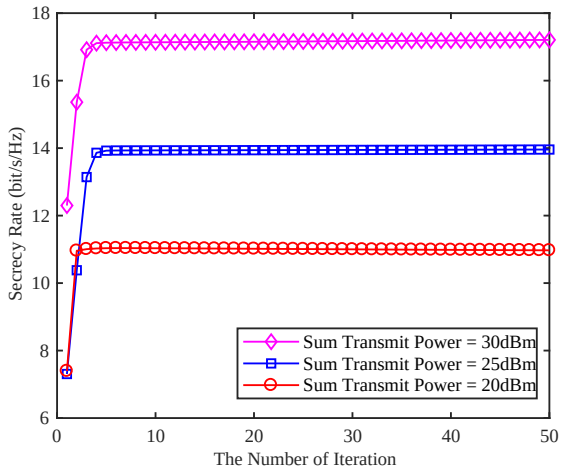


Fig. 4. Convergence of Algorithm 1 for the joint transceiver design scheme with different P_A. r_{lim} =2 bit/s/Hz.

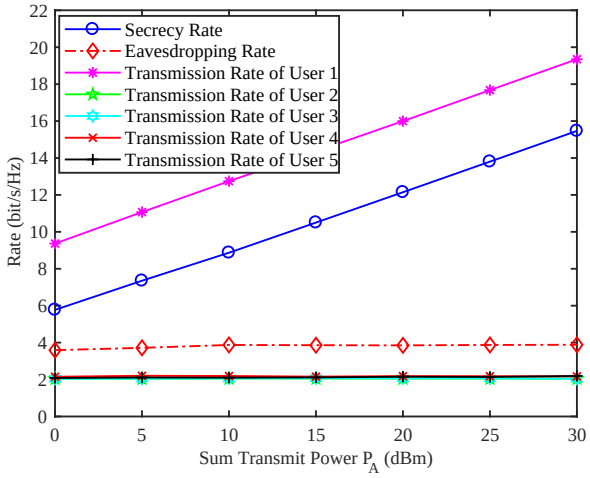


Fig. 5. Comparison of secrecy rate, eavesdropping rate and transmission rate of the SeU and the transmission rate of the LeUs with different values of P_A, when there are 5 users. r_{lim} =2 bit/s/Hz.

the eavesdropper and other users, which means that other users will not generate strong interference to the 1st user and the received signal from the 1st user at the eavesdropper is relatively weak. In addition, other users are all close to the eavesdropper, which indicates that other users will generate strong jamming signals at the eavesdropper to help the 1st user achieve secure transmission. Thus, with all these factors jointly considered, the 1st user can be selected as the SeU, and all the others as LeUs, according to our proposed user selection scheme in (15).

Then, the performance of the proposed joint transceiver design scheme is analyzed based on the user selection scheme in (15) in Figs. 4-7, with the topology depicted in Fig. 3. In Fig. 4, the convergence of Algorithm 1 for the joint transceiver design scheme is analyzed, with the rate threshold of each LeU r_{lim} equal 2 bit/s/Hz and different sum transmit power of the legitimate network P_A. From the results, we can see that the proposed algorithm can converge rapidly, within 5 iterations. In addition, we can also find that the secrecy rate of SeU will increase when sum transmit power increases, due to the fact that more resources can be allocated to improve its secrecy rate.

In Fig. 5, the secrecy rate, eavesdropping rate and transmission rate of the SeU, and the transmission rate of all the LeUs, are compared for different values of P_A at r_{lim} =2 bit/s/Hz. From the results, we can observe that the transmission rate of the SeU will increase with P_A, while the eavesdropping rate remains almost unchanged. Thus, the secrecy rate will increase with P_A with the help of all the LeUs. In addition, the transmission rate of all the LeUs remains almost the same, i.e., 2 bit/s/Hz, for different values of P_A, which is consistent with (16b). From the analysis, we can conclude that the LeUs will satisfy their minimum requirements to save power to improve performance of secure transmission for the SeU.

In Fig. 6, the secrecy rate, eavesdropping rate and transmission rate of the SeU is compared for different values of r_{lim} at P_A=20 dBm. From the results, we can see that the transmission rate of the SeU will decrease with r_{lim}, due to the fact that more transmit power will be allocated to LeUs

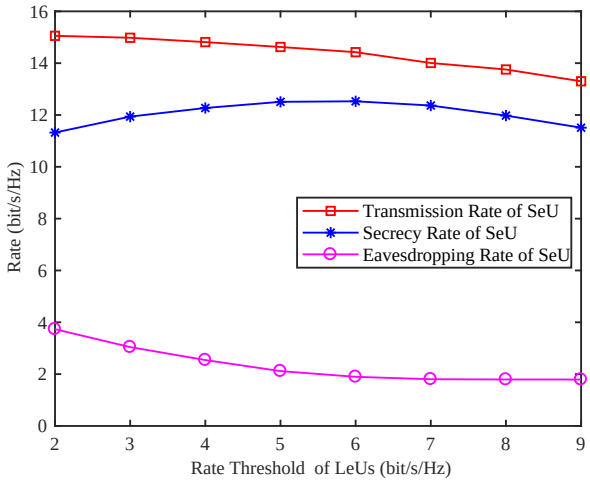


Fig. 6. Comparison of secrecy rate, eavesdropping rate and transmission rate of the SeU, with different values of r_{lim}. P_A=20 dBm.

to satisfy their requirements, thus with less remaining for the SeU. In addition, for the eavesdropping rate, it decreases first, and then remains almost unchanged. This is because larger r_{lim} means higher transmit power for LeUs, which will generate greater interference to disrupt the eavesdropping. Furthermore, the secrecy rate of the SeU will first increase and then decrease for the reason that increasing the transmit power of the LeUs will first decrease the eavesdropping rate obviously, which can make up the loss of the transmission rate for the SeU. However, when the transmit power still increase after r_{lim} = 6 bit/s/Hz, the eavesdropping rate will decrease very slowly, and thus, the transmission rate loss of the SeU will result in the decrease of its secrecy rate.

In Fig. 7, the secrecy rate, eavesdropping rate and the transmission rate of the SeU are compared with different values of P_A and r_{lim}. From the results, we can see that the transmission rate will increase with P_A, with the eavesdropping rate almost unchanged. Thus, the secrecy rate of the SeU will increase when P_A increases. In addition, we can

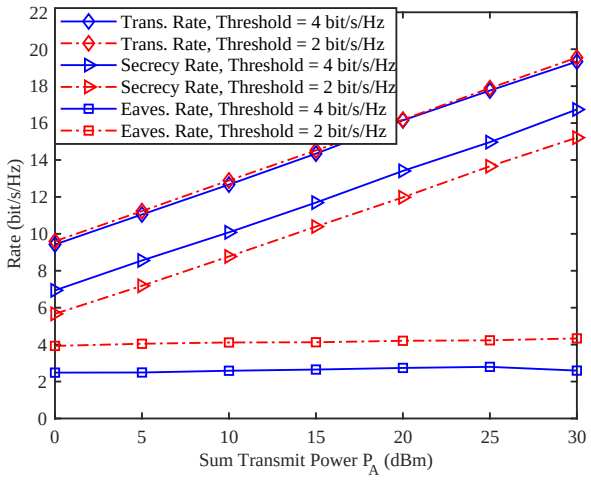


Fig. 7. Comparison of secrecy rate, eavesdropping rate and transmission rate of the SeU with different values of P_A and r_{lim}.

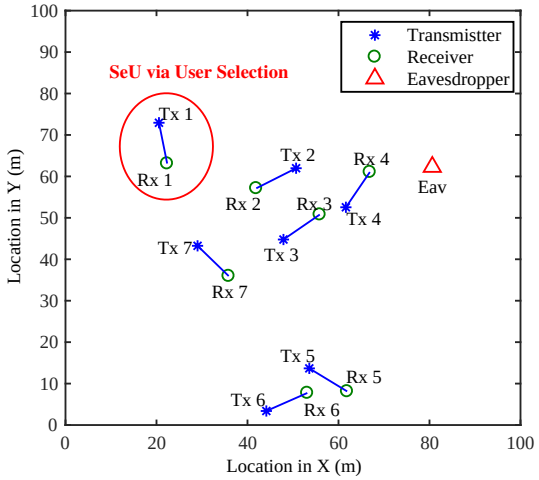


Fig. 8. Demonstration of the topology for a 7-user interference network with an eavesdropper, and the result of the proposed user selection scheme based on (15).

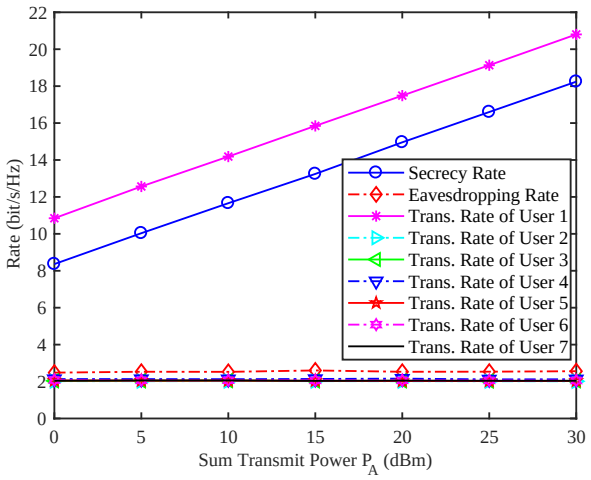


Fig. 9. Comparison of secrecy rate, eavesdropping rate and the transmission rate of the SeU and the transmission rate of the LeUs with different values of P_A, when there are 7 users. r_{lim} =2 bit/s/Hz.

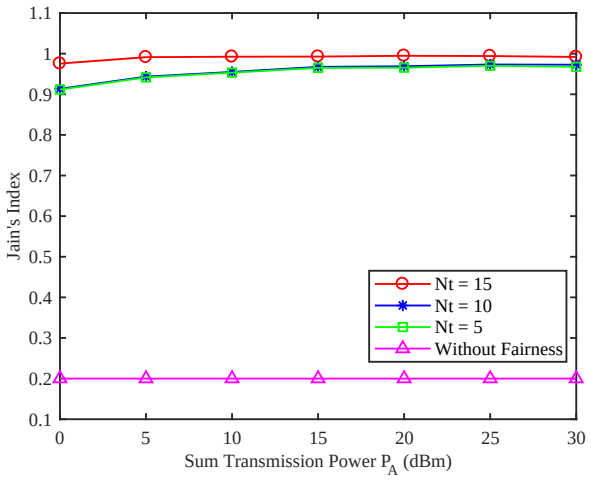


Fig. 10. Jain's index comparison of the proposed schemes in a 5-user network with different values of N_t and P_A according to the topology in Fig. 3. r_{lim} =4 bit/s/Hz

also observe that when r_{lim} is changed from 2 bit/s/Hz to 4 bit/s/Hz, the eavesdropping rate will decrease, with little loss in the transmission rate. Thus, the secrecy rate of the SeU will increase when r_{lim} changes from 2 bit/s/Hz to 4 bit/s/Hz, which is consistent with the results in Fig. 6.

Furthermore, the performance of our proposed schemes for more users are also analyzed in Figs. 8-9, i.e., 7 users. In Fig. 8, the topology of the 7-user network with existence of an eavesdropper is shown. From the results, we can see that the 1st user is relatively far from the eavesdropper and the other users, while the other users are all relatively near the eavesdropper. According to the similar analysis in Fig. 3, the 1st user can be selected as the SeU, with all the others as LeUs, according to our proposed user selection scheme in (15). In Fig. 9, the secrecy rate, eavesdropping rate and the transmission rate of the SeU and the transmission rate of the LeUs are compared with different values of P_A, when there are 7 users. r_{lim} =2 bit/s/Hz. From the results, we can see that the transmission rate of the SeU will increase with P_A, with the eavesdropping rate almost unchanged. Thus, the secrecy rate of the SeU will also increase with high P_A. To achieve this, the LeUs will satisfy the performance, with their transmission rate just equal to r_{lim} approximately. In addition, the eavesdropping rate becomes lower compared to that in Fig. 5, which reflects that security performance becomes better with more LeUs, due to stronger interference towards the eavesdropping. Thus, our proposed scheme is also suitable for dense networks.

To further guarantee the fairness of the user selection scheme, the Jain's index of the proposed user selection scheme with fairness for a 5-user interference network during 200 time slots is compared with different values of N_t and P_A in Fig. 10. r_{lim} =4 bit/s/Hz. From the results, we can see that when user selection is performed without fairness according to (15), Jain's index is 0.2 with different values of P_A, which means that the least fairness can be achieved when a specific user is always selected as the SeU, due to the fixed topology in Fig. 3. On the other hand, the Jain's index is close to 1 when

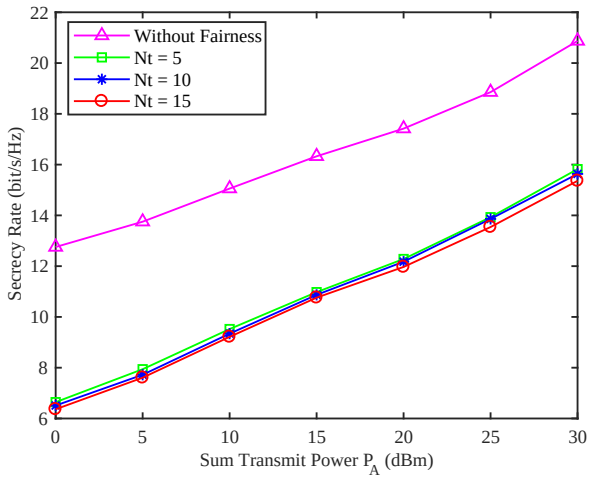


Fig. 11. Secrecy rate comparison of the proposed schemes in a 5-user network with different values of N_t and P_A according to the topology in Fig. 3. r_{lim} =4 bit/s/Hz.

the proposed user selection scheme with fairness in (36) is adopted, which means that the fairness among users can be guaranteed effectively when considering the fairness in user selection. Furthermore, the Jain's index will increase slightly with N_t. The secrecy rate of the proposed scheme with and without fairness is also compared in Fig. 11. From the results, we can see that the secrecy rate will decrease when the fairness among users is considered, although the Jain's index can be improved. Specifically, the secrecy rate will decrease slightly with N_t. This is natural due to the fact that we should sacrifice the secrecy rate for the fairness.

VII. Conclusions

In this paper, user selection and transceiver design have been proposed to guarantee the secure transmission of interference networks. First, the most suitable user was selected as SeU to perform secure transmission, with the help of the other users as LeUs. To reduce its computational complexity, a suboptimal user selection scheme was proposed only based on the distance information between nodes. Based on the results of user selection, the transceiver of the legitimate users were jointly designed to maximize the secrecy rate of SeU, with the rate requirement of LeUs guaranteed. The problem was difficult to solve due to its non-convexity. Thus, an alternate optimization algorithm was proposed via SOCP to calculate its suboptimal solutions with low complexity. Furthermore, to share the opportunity of secure transmission among all the legitimate users, a modified user selection scheme was proposed with the fairness fully considered. Finally, simulation results were presented to show the effectiveness and efficiency of the proposed schemes.

Appendix A
Proof of Proposition 1

Proof: When received SINR is high enough, we should notice that $\frac{P_T\rho_{DS}}{\sigma_D^2+P_T\sum_{k=1}^{K}\rho_D^{[k]}}$ and $\frac{P_T\rho_{ES}}{\sigma_E^2+P_T\sum_{k=1}^{K}\rho_E^{[k]}}$ are much larger than 1. Thus, 1 can be ignored in (14), which can be changed into

$$\Omega^* = \arg\max_{\Omega}\left(\frac{\frac{P_T\rho_{DS}}{\sigma_D^2+P_T\sum_{k=1}^{K}\rho_D^{[k]}}}{\frac{P_T\rho_{ES}}{\sigma_E^2+P_T\sum_{k=1}^{K}\rho_E^{[k]}}}\right). \quad (38)$$

In addition, when the channel noise σ_D and σ_E are much smaller than the received signal power, problem (38) can be further simplified as

$$\Omega^* = \arg\max_{\Omega}\bar{R}_S = \arg\max_{\Omega}\frac{\frac{P_T\rho_{DS}}{P_T\sum_{k=1}^{K}\rho_D^{[k]}}}{\frac{P_T\rho_{ES}}{P_T\sum_{k=1}^{K}\rho_E^{[k]}}}, \quad (39)$$

which can be simplified as (15). ■

Appendix B
Proof of Lemma 1

Proof: With respect to its two variables $\mathbf{y}$ and x, the first-order Taylor expansion of F can be derived as

$$\mathcal{F}_{\mathbf{A},\psi}(\mathbf{y},x,\hat{\mathbf{y}},\hat{x})=\frac{\mathbf{A}^\dagger\hat{\mathbf{y}}\hat{\mathbf{y}}^\dagger\mathbf{A}}{\hat{x}-\psi}-\frac{\mathbf{A}^\dagger\hat{\mathbf{y}}\hat{\mathbf{y}}^\dagger\mathbf{A}}{(\hat{x}-\psi)^2}(x-\hat{x})+\frac{2\hat{\mathbf{y}}^\dagger\mathbf{A}\mathbf{A}^\dagger}{(\hat{x}-\psi)}(\mathbf{y}-\hat{\mathbf{y}}). \quad (40)$$

Substituting the equation $\mathbf{A}^\dagger\hat{\mathbf{y}}\hat{\mathbf{y}}^\dagger\mathbf{A}=\hat{\mathbf{y}}^\dagger\mathbf{A}\mathbf{A}^\dagger\hat{\mathbf{y}}$ into (40), and it can be rewritten as

$$\mathcal{F}_{\mathbf{A},\psi}(\mathbf{y},x,\hat{\mathbf{y}},\hat{x})=\frac{2\hat{\mathbf{y}}^\dagger\mathbf{A}\mathbf{A}^\dagger\mathbf{y}}{\hat{x}-\psi}-\frac{\hat{\mathbf{y}}^\dagger\mathbf{A}\mathbf{A}^\dagger\hat{\mathbf{y}}}{(\hat{x}-\psi)^2}(x-\psi). \quad (41)$$

Due to the fact that $\mathbf{A}^\dagger\hat{\mathbf{y}}\hat{\mathbf{y}}^\dagger\mathbf{A}$ can be expressed as $Re\left\{\mathbf{A}^\dagger\hat{\mathbf{y}}\hat{\mathbf{y}}^\dagger\mathbf{A}\right\}$ approximately, the first-order series expansion (21) can be proved. ■

References

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[2] Z. Li, L. Guan, C. Li, and A. Radwan, "A secure intelligent spectrum control strategy for future THz mobile heterogeneous networks," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 116–123, Jun. 2018.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[4] W. Nam, D. Bai, J. Lee, and I. Kang, "Advanced interference management for 5G cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 52–60, May 2014.

[5] 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.

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

[7] A. Khisti, "Secret-key agreement over non-coherent block-fading channels with public discussion," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7164–7178, Dec. 2016.

[8] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[9] F. Zhu, F. Gao, H. Lin, S. Jin, J. Zhao, and G. Qian, "Robust beamforming for physical layer security in BDMA massive MIMO," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 775–787, Apr. 2018.

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

[11] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[12] 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.

[13] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

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

[15] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[16] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[17] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538–1550, Dec. 2016.

[18] 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, 2017.

[19] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[20] Z. Kong, S. Yang, F. Wu, S. Peng, L. Zhong, and L. Hanzo, "Iterative distributed minimum total MSE approach for secure communications in MIMO interference channels," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 594–608, Mar. 2016.

[21] 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.

[22] Y. Cai, Q. Shi, B. Champagne, and G. Y. Li, "Joint transceiver design for secure downlink communications over an amplify-and-forward MIMO relay," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3691–3704, Sept. 2017.

[23] X. Chen and Y. Zhang, "Mode selection in MU-MIMO downlink networks: A physical-layer security perspective," *IEEE Syst. J.*, vol. 11, no. 2, pp. 1128–1136, Jun. 2017.

[24] 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.

[25] J. Guo, N. Zhao, Z. Yang, F. R. Yu, Y. Chen, and V. C. M. Leung, "Proactive jamming toward interference alignment networks: Beneficial and adversarial aspects," *IEEE Syst. J.*, Online, DOI: 10.1109/JSYST.2017.2770174.

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

[27] Y. 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.

[28] N. Zhao, F. R. Yu, and V. C. M. Leung, "Opportunistic communications in interference alignment networks with wireless power transfer," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 88–95, Feb. 2015.

[29] N. Zhao, F. R. Yu, and H. Sun, "Adaptive energy-efficient power allocation in green interference-alignment-based wireless networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 9, pp. 4268–4281, Sept. 2015.

[30] 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.

[31] K. Gomadam, V. R. Cadambe, and S. A. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3309–3322, Jun. 2011.

[32] A. J. Smola, S. V. N. Vishwanathan, and T. Hofmann, "Kernel methods for missing variables," in *Proc. 10th Int. Workshop Artif. Intell. Stat.*, pp. 325–332, Barbados, Jan. 2005.

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.

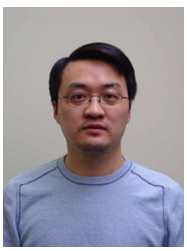
Qiuyi Cao received the B.S. degree from Dalian University of Technology, Dalian China. She is currently studying towards the M.S. degree at the School of Information and Communication Engineering, Dalian University of Technology, Dalian, China. Her current research interests are mainly focus on physical layer security.

Guan Gui (M'11-SM'17) received the Dr. Eng degree in Information and Communication Engineering from University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2012. From October 2009 to March 2012, with the financial supported from the China scholarship council (CSC) and the global center of education (ECOE) of Tohoku University, he joined the wireless signal processing and network laboratory (Prof. Fumiyuki Adachi laboratory), Department of Communications Engineering, Graduate School of Engineering, Tohoku University as for research assistant as well as postdoctoral research fellow, respectively. From September 2012 to March 2014, he was supported by Japan society for the promotion of science (JSPS) fellowship as postdoctoral research fellow at same laboratory. From April 2014 to October 2015, he was an Assistant Professor in Department of Electronics and Information System, Akita Prefectural University. Since November 2015, he has been a professor with Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. He is currently engaged in research of deep learning, compressive sensing and advanced wireless techniques. He is a senior member of Institute of Electrical and Electronics Engineers (IEEE). Dr. Gui has been Editor for Security and Communication Networks (2012–2016), editor of IEEE Transactions on Vehicular Technology (2017–) and KSII Transactions on Internet and Information System (2017–). He received several best paper awards such as CSPS2018, ICNC2018, ICC2017, ICC2014 and VTC2014-Spring. He was also selected as for Jiangsu Special Appointed Professor, Jiangsu High-level Innovation and Entrepreneurial Talent and Nanjing Youth Award.

Yang Cao is currently a graduate student 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 interference alignment, physical layer security, wireless energy harvesting, and resource allocation.

Shun Zhang received the B.S. degree in communication engineering from Shandong University, Jinan, China, in 2007 and the Ph.D. degree in communications and signal processing from Xidian University, Xi'an, China, in 2013. He is currently with the State Key Laboratory of Integrated Services Networks, Xidian University. His research interests include MIMO-OFDM systems, relay networks, and detection and parameter estimation theory.



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.

Hikmet Sari (F'95) is currently Professor of Nanjing University of Posts and Telecommunications (NUPT), and also Chief Scientist of Sequans Communications, a leading developer and supplier of LTE chipset solutions. He received his Engineering Degree and Ph.D. from the ENST, Paris, France, and the post-doctoral Habilitation degree from the University of Paris-Sud, Orsay. Prior to his current positions, he held various research and management positions in industry including Philips Research Laboratories, SAT, Alcatel, Pacific Broadband Communications, and Juniper Networks. His distinctions include the *IEEE Fellow Grade* (1995), the *Andre Blondel Medal* (also in 1995), the *Edwin H. Armstrong Achievement Award* in 2003, the *Harold Sobol Award* in 2012, as well as election to *Academia Europaea* (the Academy of Europe) and to the *Science Academy of Turkey* in 2012.

Prof. Sari has served as an Editor of the IEEE Transactions on Communications (1987-1981), a Guest Editor of the European Transactions on Telecommunications (1993) and of the IEEE JSAC (1999), and an Associate Editor of the IEEE Communications Letters (1999-2002). He served as a Distinguished Lecturer of the IEEE Communications Society in 2001-2006, as a member of the IEEE Fellow Evaluation Committee in 2002-2007, and as a member of the Awards Committee in 2005-2007.

Prof. Sari was Chair of the Communication Theory Symposium of ICC 2002 (New York), Technical Program Chair of ICC 2004 (Paris), Vice General Chair of ICC 2006 (Istanbul), General Chair of PIMRC 2010 (Istanbul), General Chair of WCNC 2012 (Paris), Executive Chair of WCNC 2014 (Istanbul), General Chair of ICUWB 2014 (Paris), General Co-Chair of IEEE BlackSeaCom 2015 (Constanta, Romania), Technical Program Chair of EuCNC 2015 (Paris), and Executive Co-Chair of ICC 2016 (Kuala Lumpur). He also chaired the Globecom and ICC Technical Content (GITC) Committee during the period of 2010 C 2011, and he was Vice President for Conferences of the IEEE Communications Society during 2014 C 2015. Currently, he is serving as General Co-Chair of ATC 2016 (Hanoi, Vietnam), Executive Chair of ICC 2017 (Paris), and General Chair of PIMRC 2018 (Istanbul).