Optimization or Alignment: Secure Primary Transmission Assisted by Secondary Networks

Yang Cao, *Student Member, IEEE,* Nan Zhao, *Senior Member, IEEE,* F. Richard Yu, *Fellow, IEEE,*
Minglu Jin, *Member, IEEE,* Yunfei Chen, *Senior Member, IEEE,* Jie Tang, *Member, IEEE*
and Victor C.M. Leung, *Fellow, IEEE*

***Abstract*—Security is a challenging issue for cognitive radio (CR) to be used in future 5G mobile systems. Conventionally, interference will degrade the performance of a primary user (PU) when the spectrum is shared with secondary users (SUs). However, when properly designed, SUs can serve as friendly jammers to guarantee the secure transmission of PU. Thus, in this paper, we propose two schemes to improve the sum rate of SUs while guaranteeing the secrecy rate of PU. In the first scheme, the secondary transceivers are jointly designed to maximize their sum rate while satisfying a threshold on the PU's secrecy rate. Due to the non-convex nature, it is first converted into a convex one and then, an alternating optimization algorithm based on the second-order cone programming is proposed to solve it. In the second scheme, the principle of interference alignment is employed to eliminate interference from PU and other SUs at each secondary receiver, and the interference from SUs is zero-forced at the primary receiver. Thus, interference-free transmission can be performed by the legitimate CR network, with eavesdropping towards PU disrupted by SUs. The key features and performances of the two proposed schemes are also compared. Finally, simulation results are presented to verify the effectiveness of the two proposed schemes for secure CR networks.**

***Index Terms*—Cognitive radio, interference alignment, physical layer security, second-order cone programming, optimal transceiver design, zero-forcing.**

I. Introduction

Recently, the research on 5G mobile systems is emerging as a hot topic. To satisfy the explosive growth of data traffic and provide a better quality of service (QoS) for mobile users, challenging requirements are imposed on the future 5G networks for system capacity and transmission rate [2], which can be relieved by improving the spectrum utilization of mobile systems. To this end, cognitive radio (CR) has been regarded as a promising technique for 5G, to fully utilize the spectrum via spectrum sharing [3], [4]. In CR networks, using its capability of sensing and adapting to the surrounding radio environment, dynamic spectrum allocation can be realized between the primary users (PUs) and secondary users (SUs) to enhance spectrum efficiency [5], [6]. This is significant for the bandwidth-hungry 5G.

Despite the enhancement of spectrum efficiency via CR, secure transmission becomes a challenging issue due to the inherent characteristics of CR networks and the open nature of wireless channels [7], [8]. Particularly, potential eavesdroppers in the CR network can severely compromise its security, which can be deemed as illegal users who intend to wiretap the confidential information transmitted by PUs [7]. The conventional methods to combat with the eavesdropping rely on the cryptography of the upper layer [9], which might not be trustable due to the solvability of secret keys and the unavailability of a trusted key management center [10]. Therefore, a novel alternative security mechanism, physical layer security, has emerged, and the secure transmission of confidential message can be achieved using the physical characteristics of wireless channels [11]. To this end, the pioneering study by Wyner [12] demonstrated that nearly perfect secure communication is possible in degraded broadcast channels without secret keys considered. Following Wyner's research, considerable efforts have been dedicated to improve the secure transmission at physical layer in the past decade, including node beamforming and jamming optimization [13], [14], node cooperation [15], relay selection [16], [17], artificial noise [18], [19], etc. In addition, the interference between legitimate users can also disrupt the potential eavesdropping effectively, if properly managed, by using interference alignment (IA) technique [20]–[22].

As for CR networks, several physical-layer methods have also been conducted to guarantee the secure transmission [23]–[29]. In [23], SU selection was proposed by Zhang *et al.* through a coalition formation game model, to improve PU's secrecy capacity. In [24], Pei *et al.* investigated the optimal transmitter design to achieve secure communication in multiple-input single-output (MISO) CR network with imperfect channel state information (CSI). In [25], Zou *et al.* designed the optimal user scheduling in a multi-user

This research was supported in part by the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2018D03), the Xinghai Scholars Program, the National Natural Science Foundation of China (NSFC) under Grant 61601186, 61771089 and 61671101, and the Fundamental Research Funds for the Central Universities under DUT17JC43. Part of this work has been published in preliminary form in the Proceedings of 2018 IEEE 87th Vehicular Technology Conference (VTC'2018-Spring) [1]. *(Corresponding author: Jie Tang.)*

Y. Cao, N. Zhao and M. Jin are with the School of Info. and Commun. Eng., Dalian University of Technology, Dalian, China. Y. Cao and N. Zhao are also with National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (email: cy216@mail.dlut.edu.cn, zhaonan@dlut.edu.cn, mljin@dlut.edu.cn).

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

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

J. Tang is with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, Guangdong, P. R. China (Email: eejtang@scut.edu.cn).

V.C.M. Leung is with the Depart. of Electrical and Computer Eng., the University of British Columbia, Vancouver, Canada (email: vleung@ece.ubc.ca).

multi-eavesdropper cognitive radio system, and the secrecy outage and diversity were derived in the proposed scheduling schemes, respectively. In [26], Al-Talabani *et al.* proposed to leverage secondary transmitter as a trusted relay for PU to improve its security. In [27], Xu *et al.* studied the secure transmission in an underlay CR network with Poisson distributed eavesdroppers, and presented four transmission protocols to realize the security in terms of different CSI assumptions. In [28], cooperative beamforming is designed by Zhu and Yao to enhance security performance for both PUs and SUs in a CR network with an eavesdropper. In [29], Fan *et al.* proposed a relay selection scheme to improve the security of cognitive relay network.

The key principle of CR networks is that SUs can only access the licensed spectrum when they will not affect the transmission of PU or can provide benefit. Thus, the secondary transceivers can be jointly optimized to assist the secure transmission of PU, which will generate more opportunities for SUs to share the spectrum. On the other hand, IA is a promising technique for interference management in wireless networks [30]–[33], and it can also be exploited to guarantee the security of CR networks. Thus, the idea of IA can also be leveraged to perform interference-free transmission and improve the secrecy rate of PU. In this paper, two effective schemes based on transceiver design and IA are proposed, respectively. Both schemes aim to guarantee the secure transmission of PU in CR networks. The key motivations and contributions of this paper are summarized as follows.

- In CR networks, opportunities are provided for SUs to access spectrum only if they will not degrade the transmission of PU. Following this basic principle, the SUs are proposed to assist PU to achieve secure transmission in this paper, in order to have more opportunities to share the spectrum.
- Interference from SUs can be exploited to disrupt eavesdropping in this paper. There are two main methods to achieve interference management in multiuser MIMO networks, i.e., optimal transceiver design (OTD) and IA. To the best of our knowledge, this is the first research that adopts these two methods to guarantee the secure transmission of PU in CR networks.
- In the proposed OTD scheme, the transceiver beamforming is designed to maximize the sum rate of SUs, with the threshold of PU's secrecy rate satisfied. Due to the non-convex nature of the optimization, we first transform it into a convex one via convex approximation, and then, an alternating optimization algorithm based on the second-order cone programming (SOCPAO) is proposed to obtain the solutions.
- In the IA-based scheme, the interference from PU and other SUs is aligned and eliminated at each secondary receiver by exploiting IA, and meanwhile, the interference from all the SUs are zero-forced at the primary receiver. Thus, interference-free transmission can be achieved by the legitimate PU and SUs, with the eavesdropping towards PU disrupted by the signal from SUs.
- The proposed two schemes have their own features, which are compared in this paper.

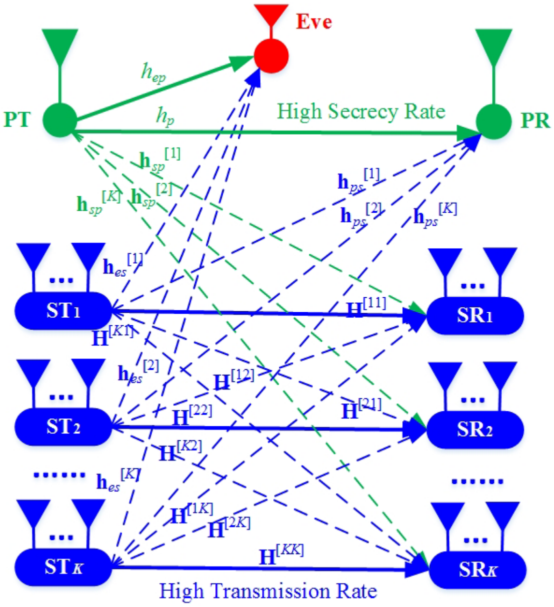


Fig. 1. System model of the CR network with an eavesdropper.

The rest of this paper is organized as follows. In Section II, the system model is presented, followed by the problem formulation. The OTD scheme is proposed in Section III, and an SOCPAO algorithm is developed to obtain its solutions. In Section IV, the IA-based scheme is proposed to eliminate or zero-force the interference between legitimate users with the secrecy rate of PU improved. In Section V, the key features of these two schemes are compared. Simulation results are presented in Section VI, and the conclusions and future work are provided in Section VII.

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

II. System Model and Problem Formulation

In this section, we first present the system model of the CR network with an eavesdropper, and then the problem of transceiver beamforming design is formulated.

A. System Model

Consider a CR network with one PU, one malicious eavesdropper and K trustable SUs, as shown in Fig. 1. Let $\mathcal{K}$ denote the set of the indices of all the SUs, i.e., $k \in \mathcal{K} \triangleq \{1, 2, \ldots, K\}$. We assume that both the PU and the eavesdropper are equipped with a single antenna[1], while

[1] The proposed schemes can be easily extended to the case of a single multi-antenna eavesdropper or several eavesdroppers, although more antennas need to be equipped at SUs to guarantee the performance, which is beyond the scope of this paper.

$M^{[k]}$ and $N^{[k]}$ antennas are equipped at the kth secondary transmitter and receiver, respectively. To improve the spectrum efficiency, we assume that the underlay model is used for spectrum sharing between PU and SUs, which means that the SUs can always access the spectrum as long as the interference from SUs is acceptable.

The decoded signal at the kth secondary receiver is

$$\begin{aligned} y_d^{[k]} =& \mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}x_s^{[k]} + \sum_{j=1,j\neq k}^{K} \mathbf{u}^{[k]\dagger}\mathbf{H}^{[kj]}\mathbf{v}^{[j]}x_s^{[j]} \\ &+ \mathbf{u}^{[k]\dagger}\mathbf{h}_{sp}^{[k]}x_p + \mathbf{u}^{[k]\dagger}\mathbf{n}_s^{[k]}, \end{aligned} \tag{1}$$

where $\mathbf{v}^{[k]} \in \mathbb{C}^{M^{[k]}\times 1}$ and $\mathbf{u}^{[k]} \in \mathbb{C}^{N^{[k]}\times 1}$ are the precoding and decoding vectors of the kth SU, respectively, with $\left\|\mathbf{v}^{[k]}\right\|^2 = P^{[k]}$ and $\left\|\mathbf{u}^{[k]}\right\|^2 = 1$. $\mathbf{H}^{[kj]} \in \mathbb{C}^{N^{[k]}\times M^{[j]}}$ denotes the channel matrix from the jth secondary transmitter to the kth secondary receiver, each entity of which is independent and identically distributed (i.i.d) and follows $\mathcal{CN}(0,1)$. Similarly, $\mathbf{h}_{sp}^{[k]} \in \mathbb{C}^{N^{[k]}\times 1}$ is the channel vector from the primary transmitter to the kth secondary receiver. $\mathbf{n}_s^{[k]} \in \mathbb{C}^{N^{[k]}\times 1}$ represents the additive white Gaussian noise (AWGN) vector with distribution $\mathcal{CN}(\mathbf{0},\sigma_s^2\mathbf{I}_{N^{[k]}})$ at the kth secondary receiver. $x_s^{[k]}$ and x_p denote the data streams transmitted by the kth secondary transmitter and the primary receiver, respectively, with $\left|x_s^{[k]}\right|^2 = 1$ and $|x_p|^2 = P_p$. Then, the received signal-to-interference-plus-noise ratio (SINR) at the kth secondary receiver can be calculated as

$$\text{SINR}_d^{[k]} = \frac{\left|\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\right|^2}{\sum\limits_{j=1,j\neq k}^{K}\left|\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kj]}\mathbf{v}^{[j]}\right|^2 + P_p\left|\mathbf{u}^{[k]\dagger}\mathbf{h}_{sp}^{[k]}\right|^2 + \sigma_s^2}. \tag{2}$$

The received signal at the primary receiver can be denoted as

$$y_p = h_p x_p + \sum_{j=1}^{K}\mathbf{h}_{ps}^{[j]}\mathbf{v}^{[j]}x_s^{[j]} + n_p, \tag{3}$$

where h_p is the channel gain of PU, and $\mathbf{h}_{ps}^{[j]} \in \mathbb{C}^{1\times M^{[j]}}$ represents the channel coefficient vector from jth secondary transmitter to the primary receiver. n_p is the AWGN with zero mean and σ_p^2 variance at the primary receiver. The received SINR at the primary receiver can be expressed as

$$\text{SINR}_p = \frac{P_p\left|h_p\right|^2}{\sum\limits_{j=1}^{K}\left|\mathbf{h}_{ps}^{[j]}\mathbf{v}^{[j]}\right|^2 + \sigma_p^2}. \tag{4}$$

For the eavesdropper, its wiretapped signal from the PU can be expressed as

$$y_e = h_{ep}x_p + \sum_{j=1}^{K}\mathbf{h}_{es}^{[j]}\mathbf{v}^{[j]}x_s^{[j]} + n_e, \tag{5}$$

where h_{ep} denotes the channel gain from the primary transmitter to the eavesdropper, and $\mathbf{h}_{es}^{[j]} \in \mathbb{C}^{1\times M^{[j]}}$ is the channel coefficient vector from jth secondary transmitter to the eavesdropper. n_e is the AWGN with zero mean and σ_e^2 variance at the eavesdropper. Similar to the PU, the received SINR at the eavesdropper can be denoted as

$$\text{SINR}_e = \frac{P_p\left|h_{ep}\right|^2}{\sum\limits_{j=1}^{K}\left|\mathbf{h}_{es}^{[j]}\mathbf{v}^{[j]}\right|^2 + \sigma_e^2}. \tag{6}$$

B. Problem Formulation

In this paper, we aim to maximize the sum rate of secondary network by optimizing their transceiver design, with the requirement of PU's secrecy rate satisfied. According to (2), the transmission rate of the kth SU can be denoted as

$$R_D^{[k]} = \log_2\left(1 + \text{SINR}_d^{[k]}\right). \tag{7}$$

Based on (4) and (6), the achievable secrecy rate of PU can be obtained as [34], [35]

$$R_s = \left[\log_2\left(1 + \text{SINR}_p\right) - \log_2\left(1 + \text{SINR}_e\right)\right]^+, \tag{8}$$

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

In the underlay CR network, the SUs can access the network only when the performance of PU is guaranteed. In this paper, the security metric is adopted for the PU, and to achieve the requirement, we intend to optimize the sum rate of SUs provided that the secure transmission of PU can be satisfied. In other words, the secrecy rate of PU should be guaranteed to be no less than a given threshold with the help of SUs. Thus, the optimization problem can be expressed as

$$\max_{\mathbf{u}^{[k]},\mathbf{v}^{[k]}} \ \sum\nolimits_{k=1}^{K} R_D^{[k]} \tag{9a}$$

$$s.t. \ R_s \geq r_s, \tag{9b}$$

$$\sum\nolimits_{k=1}^{K}\left\|\mathbf{v}^{[k]}\right\|^2 \leq P_S, \tag{9c}$$

$$\left\|\mathbf{u}^{[k]}\right\|^2 = 1, \ \forall k, \tag{9d}$$

where r_s is the secrecy rate threshold of PU, and P_S denotes the constraint of the total transmit power of all the secondary transmitters. It's worth noting that the CSI of the eavesdropper should be available in the legitimate network. This is reasonable in situations where the eavesdroppers serve as registered users of the network, but they cannot participate in the transmission of the confidential information. The same hypotheses have also been adopted in many existing works [36]–[38].

From the problem (9), we can see that (9a) is non-convex in that the variables $\mathbf{u}^{[k]}$ and $\mathbf{v}^{[k]}$ are coupled, and the constraint for secrecy rate is not convex as well, due to the difference of two quadratical logarithmic functions. Therefore, (9) is non-convex and its global optimum is difficult to achieve. In Section III, we will transform (9) into a convex problem through convex approximation, and obtain its optimal solution through an effective alternating optimization algorithm.

III. Optimal Transceiver Design Scheme

In this section, we propose an alternating optimization algorithm to calculate the optimal solutions to (9) in the OTD scheme with two steps.

A. Step One: Optimization of $\mathbf{v}^{[k]}$

First, we generate random variates of $\mathbf{u}^{[k]}$ that satisfy $\left\|\mathbf{u}^{[k]}\right\|^2 = 1$, $k = 1, 2, \ldots, K$. Then, (9) can be reduced to

$$\max_{\mathbf{v}^{[k]}} \ \sum\nolimits_{k=1}^{K} R_D^{[k]} \tag{10a}$$

$$s.t. \ \ R_s \geq r_s, \tag{10b}$$

$$\sum\nolimits_{k=1}^{K} \left\|\mathbf{v}^{[k]}\right\|^2 \leq P_S. \tag{10c}$$

It's worth noting that (10) is still non-convex in its current form, and we can reformulate it as follows through introducing some auxiliary variables.

$$\max_{\mathbf{v}^{[k]}, s_k, m, n} \ \sum\nolimits_{k=1}^{K} \log_2(s_k) \tag{11a}$$

$$s.t. \ \frac{\left|\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\right|^2}{\sum\limits_{j=1, j\neq k}^{K} \left|\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kj]}\mathbf{v}^{[j]}\right|^2 + P_p \left|\mathbf{u}^{[k]\dagger}\mathbf{h}_{sp}^{[k]}\right|^2 + \sigma_s^2} \geq s_k - 1, \tag{11b}$$

$$\frac{P_p \left|h_p\right|^2}{\sum\nolimits_{j=1}^{K} \left|\mathbf{h}_{ps}^{[j]}\mathbf{v}^{[j]}\right|^2 + \sigma_p^2} \geq m - 1, \tag{11c}$$

$$1 + \frac{P_p \left|h_{ep}\right|^2}{\sum\nolimits_{j=1}^{K} \left|\mathbf{h}_{es}^{[j]}\mathbf{v}^{[j]}\right|^2 + \sigma_e^2} \leq \frac{1}{n}, \tag{11d}$$

$$\log_2(m) - \log_2(\frac{1}{n}) \geq r_s, \tag{11e}$$

$$\sum\nolimits_{k=1}^{K} \left\|\mathbf{v}^{[k]}\right\|^2 \leq P_S. \tag{11f}$$

Obviously, (11) is equivalent to

$$\max_{\mathbf{v}^{[k]}, s_k, m, n} \ \prod_{k=1}^{K} s_k \tag{12a}$$

$$\begin{aligned} s.t. \ \sum\nolimits_{j=1, j\neq k}^{K} \left|\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kj]}\mathbf{v}^{[j]}\right|^2 + P_p \left|\mathbf{u}^{[k]\dagger}\mathbf{h}_{sp}^{[k]}\right|^2 + \sigma_s^2 \\ \leq \frac{\left|\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\right|^2}{s_k - 1}, \end{aligned} \tag{12b}$$

$$\sum\nolimits_{j=1}^{K} \left|\mathbf{h}_{ps}^{[j]}\mathbf{v}^{[j]}\right|^2 + \sigma_p^2 \leq \frac{P_p \left|h_p\right|^2}{m - 1}, \tag{12c}$$

$$\begin{aligned} \sum\nolimits_{j=1}^{K} \left|\mathbf{h}_{es}^{[j]}\mathbf{v}^{[j]}\right|^2 + P_p \left|h_{ep}\right|^2 + \sigma_e^2 \\ \leq \frac{\sum\nolimits_{j=1}^{K} \left|\mathbf{h}_{es}^{[j]}\mathbf{v}^{[j]}\right|^2 + \sigma_e^2}{n}, \end{aligned} \tag{12d}$$

$$m \times n \geq 2^{r_s}, \tag{12e}$$

$$\sum\nolimits_{k=1}^{K} \left\|\mathbf{v}^{[k]}\right\|^2 \leq P_S. \tag{12f}$$

From (12), we can see that the constraints (12b), (12c) and (12d) are all non-convex in the form of $g_1(x) \leq g_2(x)$. This is due to the fact that both $g_1(x)$ and $g_2(x)$ are convex and the difference of the two convex functions is nonconvex, i.e., the left side of the inequality $g_1(x) - g_2(x) \leq 0$ is not convex. However, in terms of the constrained concave convex procedure in [39], the functions of the right side in the constraints (12b), (12c) and (12d) can be approximated by their corresponding first-order Taylor expansion, and then, we can convert these constraints into convex ones. Before performing the conversion, we introduce Lemma 1 as follows.

Lemma 1: Define the quadratic-over-linear function as

$$F(\mathbf{y}, x) = \frac{\mathbf{a}^\dagger\mathbf{y}\mathbf{y}^\dagger\mathbf{a}}{x - c}, \tag{13}$$

where c is a constant and $x > c$. $\mathbf{A} = \mathbf{a}\mathbf{a}^\dagger \succeq 0$ and $\mathbf{Y} = \mathbf{y}\mathbf{y}^\dagger \succeq 0$. The first-order Taylor expansion of the convex function (13) can be derived as

$$\Re(\mathbf{y}, x, \bar{\mathbf{y}}, \bar{x}) = \frac{2Re(\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\mathbf{y})}{\bar{x} - c} - \frac{\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\bar{\mathbf{y}}}{(\bar{x} - c)^2}\left(x - c\right). \tag{14}$$

For the convex function (13), it satisfies the inequality $F(\mathbf{y}, x) \geq \Re(\mathbf{y}, x, \bar{\mathbf{y}}, \bar{x})$.

Proof: $F(\mathbf{y}, x)$ is a function of two variables, and its first-order Taylor expansion can be calculated as

$$\begin{aligned} \Re(\mathbf{y}, x, \bar{\mathbf{y}}, \bar{x}) &= F(\bar{\mathbf{y}}, \bar{x}) + \partial_x F|_{(\bar{\mathbf{y}}, \bar{x})}(x - \bar{x}) + \partial_{\mathbf{y}} F|_{(\bar{\mathbf{y}}, \bar{x})}(\mathbf{y} - \bar{\mathbf{y}}) \\ &= \frac{\mathbf{a}^\dagger\bar{\mathbf{y}}\bar{\mathbf{y}}^\dagger\mathbf{a}}{\bar{x} - c} - \frac{\mathbf{a}^\dagger\bar{\mathbf{y}}\bar{\mathbf{y}}^\dagger\mathbf{a}}{(\bar{x} - c)^2}(x - \bar{x}) + \frac{2\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger}{\bar{x} - c}\left(\mathbf{y} - \bar{\mathbf{y}}\right). \end{aligned} \tag{15}$$

Using $\mathbf{a}^\dagger\bar{\mathbf{y}}\bar{\mathbf{y}}^\dagger\mathbf{a} = \bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\bar{\mathbf{y}}$, the above expression can be simplified as

$$\Re(\mathbf{y}, x, \bar{\mathbf{y}}, \bar{x}) = \frac{2\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\mathbf{y}}{\bar{x} - c} - \frac{\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\bar{\mathbf{y}}}{(\bar{x} - c)^2}\left(x - c\right). \tag{16}$$

For convenience, the term $\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\mathbf{y}$ can be prudently approximated with $Re(\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\mathbf{y})$, and finally the first-order Taylor expansion of function (13) can be expressed as

$$\Re(\mathbf{y}, x, \bar{\mathbf{y}}, \bar{x}) = \frac{2Re(\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\mathbf{y})}{\bar{x} - c} - \frac{\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\bar{\mathbf{y}}}{(\bar{x} - c)^2}\left(x - c\right). \tag{17}$$

Note that the above approximation will not affect the feasibility of the original problem due to the fact that $Re(\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\mathbf{y}) \leq \left|\bar{\mathbf{y}}^\dagger\mathbf{a}\mathbf{a}^\dagger\mathbf{y}\right|$ for a complex number.

Using the first-order convexity condition, we can obtain $F(\mathbf{y}, x) \geq \Re(\mathbf{y}, x, \bar{\mathbf{y}}, \bar{x})$, i.e., the first-order Tayor approximation is a global lower bound of the initial convex function. Thus, Lemma 1 is proved. ■

According to Lemma 1, for the constraints (12b), (12c) and (12d), we define

$$F_1(\mathbf{v}^{[k]}, s_k) = \frac{\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\mathbf{v}^{[k]\dagger}\mathbf{H}^{[kk]\dagger}\mathbf{u}^{[k]}}{s_k - 1}, \tag{18}$$

$$F_2(m) = \frac{P_p \left|h_p\right|^2}{m - 1}, \tag{19}$$

$$F_3(\mathbf{v}^{[k]}, n) = \frac{\sum\limits_{j=1}^{K} \mathbf{h}_{es}^{[j]}\mathbf{v}^{[j]}\mathbf{v}^{[j]\dagger}\mathbf{h}_{es}^{[j]\dagger} + \sigma_e^2}{n}. \tag{20}$$

The first-order Taylor approximation of (18) at a certain point $(\bar{\mathbf{v}}^{[k]}, \ \bar{s}_k)$ can be expressed as

$$\begin{aligned} \Re_1(\mathbf{v}^{[k]}, s_k, \bar{\mathbf{v}}^{[k]}, \bar{s}_k) = &\frac{2Re(\bar{\mathbf{v}}^{[k]\dagger}\mathbf{b}^{[k]}\mathbf{b}^{[k]\dagger}\mathbf{v}^{[k]})}{\bar{s}_k - 1} \\ &- \frac{\bar{\mathbf{v}}^{[k]\dagger}\mathbf{b}^{[k]}\mathbf{b}^{[k]\dagger}\bar{\mathbf{v}}^{[k]}}{(\bar{s}_k - 1)^2}\left(s_k - 1\right), \end{aligned} \tag{21}$$

where $\mathbf{b}^{[k]} = \mathbf{H}^{[kk]\dagger}\mathbf{u}^{[k]}$. Similarly, the approximate expression for (20) at a certain point ($\bar{\mathbf{v}}^{[k]}$, $\bar{n}$) can be expressed as

$$\begin{aligned}\Re_2(\mathbf{v}^{[j]}, n, \bar{\mathbf{v}}^{[j]},\bar{n}) = &\frac{2\sum\limits_{j=1}^{K} Re(\bar{\mathbf{v}}^{[j]\dagger}\mathbf{h}_{es}^{[j]\dagger}\mathbf{h}_{es}^{[j]}\mathbf{v}^{[j]})}{\bar{n}} \\ &- \frac{\sum\limits_{j=1}^{K} \bar{\mathbf{v}}^{[j]\dagger}\mathbf{h}_{es}^{[j]\dagger}\mathbf{h}_{es}^{[j]}\bar{\mathbf{v}}^{[j]}}{\bar{n}^2} n + \frac{\sigma_e^2}{\bar{n}^2}\left(2\bar{n} - n\right).\end{aligned} \tag{22}$$

Moreover, the first-order Taylor expansion for (19) at a certain point ($\bar{m}$) can be denoted as

$$\Re_3(m, \bar{m}) = \frac{P_p\left|hp\right|^2}{\bar{m}-1} - \frac{P_p\left|hp\right|^2}{(\bar{m}-1)^2}\left(m - \bar{m}\right). \tag{23}$$

Based on the above approximations, we can substitute the lower bounds in (21), (22) and (23) for the right side of the constraints (12b), (12d) and (12c), respectively, and then, all the constraints can be formulated as convex ones. Furthermore, note that the objective function (12a) is formulated as a product of s_k, which can be transformed into a form of second-order cone programming (SOCP) in order to reduce the computational complexity. To this end, we first recall the following lemma in [40].

Lemma 2: The hyperbolic constraints of the convex problem can be cast as SOCPs utilizing the following fact. $w^2 \leq xy, x \geq 0, y \geq 0 \Longleftrightarrow \|[2w, x-y]^\dagger\| \leq x + y$. ■

Therefore, in terms of Lemma 2, we can recast (12a) into a sequence of second-order cone (SOC) constraints (24a)-(24d). In addition, it is obvious that the constraint (12e) can be transformed as (24h) in the same way. Consequently, with all the transformations above, we can reformulate the problem in (12) into a SOCP problem, which is expressed as (24) at the top of the next page. In (24), Γ_{1k}, Γ_2 and Γ_3 can be denoted as follows, respectively,

$$\Gamma_{1k} = \Re_1(\mathbf{v}^{[k]}, s_k, \bar{\mathbf{v}}^{[k]}, \bar{s}_k) - P_p\left|\mathbf{u}^{[k]\dagger}\mathbf{h}_{sp}^{[k]}\right|^2 - \sigma_s^2, \tag{25}$$

$$\Gamma_2 = \Re_2(\mathbf{v}^{[j]}, n, \bar{\mathbf{v}}^{[j]}, \bar{n}) - P_p|h_{ep}|^2 - \sigma_e^2, \tag{26}$$

$$\Gamma_3 = \Re_3(m, \bar{m}) - \sigma_p^2. \tag{27}$$

In (24b), $C = \lceil \log_2 K \rceil$, where $\lceil . \rceil$ is the ceiling function, and we define $s_j = 1$ for the case $K < 2^C$, where $j = \left\{K+1, \ldots, 2^{\lceil \log_2 K \rceil}\right\}$. Then, set $(\bar{\mathbf{v}}^{[k]}, \bar{s}_k, \bar{m}, \bar{n})$ as the initial values. The solution to the SOCP problem (24) can be obtained by utilizing existing toolboxes, such as CVX in [41].

Remark: The optimal solution of (24) is not equivalent to that of problem (10), due to the approximate transformations that we adopt above. Specifically, the idea of successive approximations presented in [42] is leveraged in the above conversions, which means that we can only get a feasible solution of $\mathbf{v}^{[k]}$ by solving (24) in each iteration, while an optimal solution $\mathbf{v}^{[k]*}$ can be achieved by updating the variables involved until convergence. Thus, an iterative algorithm needs to be proposed to obtain the optimal solutions of problem (10), and the approximations are compact when it is convergent.

B. Step Two: Optimization of $\mathbf{u}^{[k]}$

In this step, we will fix $\mathbf{v}^{[k]}$ and optimize $\mathbf{u}^{[k]}$. When $\mathbf{v}^{[k]}$ is fixed, problem (9) can be reduced to

$$\begin{aligned}\max_{\mathbf{u}^{[k]}} \quad & \sum_{k=1}^{K} R_D^{[k]} \\ s.t. \quad & \left\|\mathbf{u}^{[k]}\right\|^2 = 1, \ \forall k.\end{aligned} \tag{28}$$

We can decompose (28) into K feasible subproblems, i.e., the kth subproblem corresponding to the kth secondary receiver can be written as

$$\begin{aligned}\max_{\mathbf{u}^{[k]}} \quad & R_D^{[k]} \\ s.t. \quad & \left\|\mathbf{u}^{[k]}\right\|^2 = 1, \ \forall k.\end{aligned} \tag{29}$$

It can be seen that the subproblem (29) is equivalent to the problem that maximize $\text{SINR}_d^{[k]}$ with respect to $\mathbf{u}^{[k]}$, which can be expressed as

$$\text{SINR}_d^{[k]} = \frac{\mathbf{u}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\mathbf{v}^{[k]\dagger}\mathbf{H}^{[kk]\dagger}\mathbf{u}^{[k]}}{\mathbf{u}^{[k]\dagger}\mathbf{Q}^{[k]}\mathbf{u}^{[k]}}, \ \forall k, \tag{30}$$

where $\mathbf{Q}^{[k]} = \sum_{j\neq k}^{K}\mathbf{H}^{[kj]}\mathbf{v}^{[j]}\mathbf{v}^{[j]\dagger}\mathbf{H}^{[kj]\dagger} + P_p\mathbf{h}_{sp}^{[k]}\mathbf{h}_{sp}^{[k]\dagger} + \sigma_s^2\mathbf{I}_N^{[k]}$. Then, the optimal solution of $\mathbf{u}^{[k]}$ that maximizes $\text{SINR}_d^{[k]}$ can be derived as

$$\mathbf{u}^{[k]*} = \frac{(\mathbf{Q}^{[k]})^{-1}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}}{\left\|(\mathbf{Q}^{[k]})^{-1}\mathbf{H}^{[kk]}\mathbf{v}^{[k]}\right\|}. \tag{31}$$

C. Proposed SOCPAO Algorithm

With all the above derivations done, we propose an alternating iterative optimization algorithm based on the SOCP problem to obtain the optimal solution to (9) in the OTD scheme, which is also denoted the SOCPAO algorithm. Details of the SOCPAO algorithm are summarized as Algorithm 1.

Algorithm 1 SOCPAO Algorithm

```
Initialization: Set the maximum number of iterations $T$, and randomly generate feasible values $(\bar{\mathbf{v}}^{[k]}, \bar{s}_k, \bar{m}, \bar{n})$ for the problem (24). Fix $\bar{\mathbf{u}}^{[k]}$ satisfying $\|\bar{\mathbf{u}}^{[k]}\|^2 = 1$.
Repeat
Solve the SOCP problem (24) by CVX, and obtain the solutions $(\mathbf{v}^{[k]*}, s_k^*, m^*, n^*)$.
Calculate (31) with $\mathbf{v}^{[k]*}$ and obtain $\mathbf{u}^{[k]*}$.
Update $(\bar{\mathbf{v}}^{[k]}, \bar{s}_k, \bar{m}, \bar{n}, \bar{\mathbf{u}}^{[k]}) = (\mathbf{v}^{[k]*}, s_k^*, m^*, n^*, \mathbf{u}^{[k]*})$.
$t = t + 1$.
Until $t = T$.
Output: $\mathbf{v}^{[k]*}$ and $\mathbf{u}^{[k]*}, \forall k$.
```

Note that, according to [39], Algorithm 1 is convergent. Specifically, at each iteration, the value of $t^{(0)}$ will be larger than or equal to its value in the previous iteration, which reveals that the transmission rate will be monotonically increasing or nondecreasing as the iteration proceeds. Besides, there also exists an upper bound for the transmission rate owing to the limited transmit power of each SU. Thus, the

$$\max_{\mathbf{v}^{[k]},s_k,m,n} \quad t^{(0)} \tag{24a}$$

$$s.t. \quad \left\| \left[2t_i^{(C-1)}, (s_{2i-1}-s_{2i})\right]^{\dagger} \right\| \leq s_{2i-1}+s_{2i}, i=1,2,...,2^{C-1}, \tag{24b}$$

$$\left\| \left[2t_i^{(C-2)}, \left(t_{2i-1}^{(C-1)}-t_{2i}^{(C-1)}\right)\right]^{\dagger} \right\| \leq t_{2i-1}^{(C-1)}+t_{2i}^{(C-1)}, i=1,2,...,2^{C-2}, \tag{24c}$$

$$\cdots\cdots$$

$$\left\| \left[2t^{(0)}, \left(t_1^{(1)}-t_2^{(1)}\right)\right]^{\dagger} \right\| \leq t_1^{(1)}+t_2^{(1)}, i=1, \tag{24d}$$

$$\left\| \left[2\mathbf{v}^{[1]\dagger}\mathbf{H}^{[k1]\dagger}\mathbf{u}^{[k]},\ldots,2\mathbf{v}^{[j]\dagger}\mathbf{H}^{[kj]\dagger}\mathbf{u}^{[k]},\ldots,2\mathbf{v}^{[K]\dagger}\mathbf{H}^{[kK]\dagger}\mathbf{u}^{[k]},\Gamma_{1k}-1\right]^{\dagger} \right\| \leq \Gamma_{1k}+1,\ j\neq k, j,k\in\mathcal{K}, \tag{24e}$$

$$\left\| \left[2\mathbf{v}^{[1]\dagger}\mathbf{h}_{es}^{[1]\dagger},\ldots,2\mathbf{v}^{[K]\dagger}\mathbf{h}_{es}^{[K]\dagger},\Gamma_2-1\right]^{\dagger} \right\| \leq \Gamma_2+1, \tag{24f}$$

$$\left\| \left[2\mathbf{v}^{[1]\dagger}\mathbf{h}_{ps}^{[1]\dagger},\ldots,2\mathbf{v}^{[K]\dagger}\mathbf{h}_{ps}^{[K]\dagger},\Gamma_3-1\right]^{\dagger} \right\| \leq \Gamma_3+1, \tag{24g}$$

$$\left\| \left[2\sqrt{2^{r_s}}, (m-n)\right]^{\dagger} \right\| \leq m+n, \tag{24h}$$

$$\left\| \left[\mathbf{v}^{[1]\dagger}, \mathbf{v}^{[2]\dagger}\ldots,\mathbf{v}^{[K]\dagger}\right]^{\dagger} \right\| \leq \sqrt{P_S},\ \forall k. \tag{24i}$$

convergence of Algorithm 1 can be ensured, and we can always obtain a local optimal solution to (9) or even a global optimal solution if proper initial values are selected. Nevertheless, the global optimal solution to (9) cannot always be guaranteed due to its non-convexity.

IV. Interference Alignment Based Scheme

In Section III, the OTD scheme is proposed to maximize the sum rate of SUs with PU's secure transmission guaranteed, by solving (9) using the SOCPAO algorithm. Nevertheless, the computational complexity of SOCPAO algorithm is high. Furthermore, the CSI of eavesdropper may not be available in some scenarios. Therefore, in this section, the idea of IA is exploited to guarantee the interference-free transmission of the CR network, with the eavesdropping towards PU disrupted by the interference from SUs. To achieve the IA-based scheme, some requirements should be satisfied as follows:

- The interference from other SUs should be constrained into the same subspace as that from the PU at each secondary receiver, which can be perfectly eliminated.
- The interference from SUs should be zero-forced at the primary receiver, i.e., no residual interference will be imposed on the PU.

When the above two requirements can be met, the legitimate CR network can perform transmission without interference, and the potential eavesdropping toward PU can also be disrupted. In this case, the most important issue is the feasibility condition, based on which we can know at least how many antennas should be equipped at each secondary transceiver to make the interference completely mitigated. Thus, in this section, we first review the feasibility condition of IA, and then, derive the feasibility condition for the proposed IA-based scheme. Finally, we design an iterative algorithm to obtain the solutions of the scheme.

A. Feasibility Condition of Interference Alignment

IA is a promising technique for interference management in wireless networks. Its main idea is to restrict the interference into the same subspace through cooperative precoding, and then, eliminate the interference and recover the desired signal with the decoding matrix at each receiver. To this end, the following conditions should be satisfied to achieve IA.

$$\mathbf{U}^{[k]\dagger}\mathbf{H}^{[kj]}\mathbf{V}^{[j]} = \mathbf{0}_{d^{[k]}\times d^{[j]}},\ \forall j\neq k,\ j,k\in\mathcal{K}, \tag{32}$$

$$\text{rank}\left(\mathbf{U}^{[k]\dagger}\mathbf{H}^{[kk]}\mathbf{V}^{[k]}\right) = d^{[k]},\ k\in\mathcal{K}, \tag{33}$$

where $\mathbf{V}^{[k]}\in\mathbb{C}^{M^{[k]}\times d^{[k]}}$ and $\mathbf{U}^{[k]}\in\mathbb{C}^{N^{[k]}\times d^{[k]}}$ are the unitary precoding and decoding matrices for $d^{[k]}$ data streams of the kth user, respectively. With (32) satisfied, the interference between users can be removed perfectly.

Furthermore, the feasibility condition of (32) has been derived based on Bezout's theorem in [43]. Specifically, (32) can be deemed as a multivariate polynomial system, which can be solved only if the number of equations is not larger than the number of variables. Therefore, a given IA-based MIMO network can be identified as feasible or infeasible using the relationship between the number of variables and equations. Before considering the CR network with an eavesdropper, we first recall some conclusions in [43] as Lemma 3.

Lemma 3: The number of equations in (32) can be expressed as

$$\mathcal{N}_{\varepsilon} = \sum_{j\neq k,j,k\in\mathcal{K}} d^{[k]}d^{[j]}. \tag{34}$$

The number of variables in (32) can be calculated as

$$\mathcal{N}_\nu = \sum_{k=1}^{K} d^{[k]} \left(M^{[k]} + N^{[k]} - 2d^{[k]} \right). \tag{35}$$

Consequently, a symmetric IA-based MIMO network is feasible if and only if $\mathcal{N}_\nu \geq \mathcal{N}_\varepsilon$. ■

Specially, we assume that all the users have the same parameters due to the symmetry of IA networks, i.e., $M^{[k]} = M, N^{[k]} = N, d^{[k]} = d$ for all IA users. Then, the feasibility condition can be denoted as follows in terms of Lemma 3.

$$dK(M + N - 2d) \geq d^2 K(K-1), \tag{36}$$

which can be simplified as

$$M + N \geq d(K+1). \tag{37}$$

According to the degree of freedom (DoF) requirement of a point-to-point MIMO channel, the value of M and N should also satisfy $M \geq d$ and $N \geq d$.

B. Feasibility Condition of the Proposed IA-Based Scheme

Consider the CR network with an eavesdropper, as demonstrated in Section II. We aim to align and then eliminate the interference from other SUs and PU at each secondary receiver. Meanwhile, the interference from SUs is zero-forced at the primary receiver to guarantee the interference-free transmission of PU. Thus, the secure transmission of PU can be achieved by disrupting the eavesdropper via the signals from SUs. To achieve this goal, the following conditions should be satisfied.

$$\mathbf{u}^{[k]\dagger} \mathbf{H}^{[kj]} \mathbf{v}^{[j]} = 0, \;\; j \neq k, \; j,k \in \mathcal{K}, \tag{38}$$

$$\mathbf{u}^{[k]\dagger} \mathbf{h}_{sp}^{[k]} = 0, \;\; k \in \mathcal{K}, \tag{39}$$

$$\mathbf{h}_{ps}^{[j]} \mathbf{v}^{[j]} = 0, \;\; j \in \mathcal{K}. \tag{40}$$

With conditions (38) and (39) satisfied, the interference from other SUs and PU can be perfectly eliminated at each secondary receiver. Moreover, the interference from SUs can be zero-forced at the primary receiver when the condition (40) is met. In addition, we assume that only one data stream is transmitted by each SU, which is consistent with Section III. Thus, the feasibility condition of the proposed IA-based scheme can be derived in Theorem 1.

Theorem 1: The feasibility condition of the proposed IA-based scheme for the CR network with an eavesdropper, can be expressed as

$$\begin{aligned} M + N &\geq K + 3, \\ M &\geq 2, \\ N &\geq 2. \end{aligned} \tag{41}$$

Proof: The total number of variables in (38)-(40) can be calculated as

$$\mathcal{N}_\nu = K(M + N - 2). \tag{42}$$

The number of equations in (38) can be obtained as

$$\mathcal{N}_{\varepsilon 1} = K(K-1). \tag{43}$$

The number of equations in (39) can be expressed as

$$\mathcal{N}_{\varepsilon 2} = K. \tag{44}$$

Besides, the number of equations in (40) can be denoted as

$$\mathcal{N}_{\varepsilon 3} = K. \tag{45}$$

Therefore, according to Lemma 3, the following inequality should be satisfied to make the proposed IA-based scheme feasible.

$$\mathcal{N}_\nu \geq \mathcal{N}_\varepsilon = \mathcal{N}_{\varepsilon 1} + \mathcal{N}_{\varepsilon 2} + \mathcal{N}_{\varepsilon 3}, \tag{46}$$

which can be simplified as

$$M + N \geq K + 3. \tag{47}$$

Define $\mathcal{N}_\varepsilon^p$ and $\mathcal{N}_\nu^p$ as the total number of equations and the total number of variables in (39), respectively. The problem (39) can be solved if and only if

$$\mathcal{N}_\nu^p \geq \mathcal{N}_\varepsilon^p \Rightarrow K(N-1) \geq K \Rightarrow N \geq 2. \tag{48}$$

Similarly, define $\mathcal{N}_\varepsilon^s$ and $\mathcal{N}_\nu^s$ as the total number of equations and the total number of variables in (40), respectively. The problem (40) can be solved if and only if

$$\mathcal{N}_\nu^s \geq \mathcal{N}_\varepsilon^s \Rightarrow K(M-1) \geq K \Rightarrow M \geq 2. \tag{49}$$

Based on the above analysis, we can obtain the feasibility condition of the proposed IA-based scheme as (41). ■

From Theorem 1, we can conclude that 2 more antennas should be added at each secondary pair in the proposed IA-based scheme for secure CR network to make it feasible ($M + N \geq K + 3$), compared to that in the conventional IA network. In addition, at least 2 antennas should be added at each secondary transceiver to make it feasible, and this requirement is also higher than that in the conventional IA network, which needs at least 1 antenna at each node when $d = 1$.

C. Iterative Algorithm

With the feasibility condition derived in Theorem 1, we can design an iterative algorithm to achieve the proposed IA-based scheme, similar to the MinIL algorithm in [44].

For the forward direction, the interference covariance matrix at the kth secondary receiver can be expressed as

$$\mathbf{Q}^{[k]} = \sum_{j \neq k}^{K} P^{[j]} \mathbf{H}^{[kj]} \mathbf{v}^{[j]} \mathbf{v}^{[j]\dagger} \mathbf{H}^{[kj]\dagger} + P_p \mathbf{h}_{sp}^{[k]} \mathbf{h}_{sp}^{[k]\dagger}. \tag{50}$$

Similarly, for the reverse direction, the interference covariance matrix at the kth secondary transmitter can be denoted as

$$\overleftarrow{\mathbf{Q}}^{[k]} = \sum_{j \neq k}^{K} P^{[j]} \overleftarrow{\mathbf{H}}^{[kj]} \overleftarrow{\mathbf{v}}^{[j]} \overleftarrow{\mathbf{v}}^{[j]\dagger} \overleftarrow{\mathbf{H}}^{[kj]\dagger} + P^{[k]} \mathbf{h}_{ps}^{[k]} \mathbf{h}_{ps}^{[k]\dagger}, \tag{51}$$

where $\overleftarrow{\mathbf{H}}^{[kj]} = \mathbf{H}^{[jk]}$, $\overleftarrow{\mathbf{v}}^{[j]} = \mathbf{u}^{[k]}$.

Therefore, the iterative process based on (50) and (51) can be summarized as Algorithm 2, to obtain the precoding and decoding vectors of SUs in the proposed IA-based scheme, with conditions (38)-(40) satisfied.

TABLE I
COMPARISON OF THE PROPOSED TWO SCHEMES

	CSI of Eavesdropper	Performance	Complexity	Feasibility
OTD Scheme	Required	Higher sum rate	Relatively High	Unknown (verified by numerical methods)
IA-Based Scheme	Not Required	Higher secrecy rate	Relatively Low	$M+N \geq K+3, M \geq 2, N \geq 2$

Algorithm 2 Iterative Algorithm for IA-Based Scheme

```
Begin with random $M \times 1$ vectors $\mathbf{v}^{[j]}$ with $\mathbf{v}^{[j]}\mathbf{v}^{[j]\dagger} = 1, \forall j \in \mathcal{K}$.
Repeat
    Compute the interference covariance matrix $\mathbf{Q}^{[k]}$ based on (50), $k \in \mathcal{K}$.
    Obtain the decoding vector $\mathbf{u}^{[k]}$ of the $k$th secondary receiver as
        $\mathbf{u}^{[k]} = \nu\left[\mathbf{Q}^{[k]}\right], k \in \mathcal{K},$   (52)
    where $\nu[\mathbf{A}]$ denotes eigenvector corresponding to the smallest eigenvalue of $\mathbf{A}$.
    Reverse the direction. Set $\overleftarrow{\mathbf{v}}^{[k]} = \mathbf{u}^{[k]}, k \in \mathcal{K}$.
    Calculate $\overleftarrow{\mathbf{Q}}^{[k]}$ according to (51), $k \in \mathcal{K}$.
    Compute the reverse decoding vector $\overleftarrow{\mathbf{u}}^{[k]}$ as
        $\overleftarrow{\mathbf{u}}^{[k]} = \nu\left[\overleftarrow{\mathbf{Q}}^{[k]}\right], k \in \mathcal{K}.$   (53)
    Reverse the direction and update the precoding vectors as $\mathbf{v}^{[k]} = \overleftarrow{\mathbf{u}}^{[k]}, k \in \mathcal{K}$.
Until the maximum number of iterations is satisfied.
Output the solutions as $\mathbf{v}^{[k]}$ and $\mathbf{u}^{[k]}$, $k \in \mathcal{K}$.
```

With the proposed IA-based scheme for secure CR network, the sum rate of SUs can be improved due to the fact that both interferences from the PU and other SUs are eliminated at each secondary receiver. In addition, the secrecy rate of PU can be enhanced because the interference from SUs is zero-forced at the primary receiver while the potential eavesdropping is disrupted by the secondary signal.

V. Comparison of the Proposed Two Schemes

In Sections III and IV, the OTD scheme and the IA-based scheme for secure CR network are proposed, respectively, both of which aim to improve the sum rate of SUs with the secure transmission of PU guaranteed. These two schemes have their special features, which are compared as follows.

- *CSI of Eavesdropper:* In the OTD scheme, the CSI of eavesdropper has to be known at legitimate SUs, which may not be true in some scenarios. On the other hand, the CSI of eavesdropper need not be available at the SUs in the IA-based scheme. Thus, the IA-based scheme is more useful than the OTD scheme in these scenarios.
- *Performance:* For the OTD scheme, the precoding and decoding vectors are designed to achieve the highest sum rate for SUs with the basic requirement of security for PU. As for the IA-based scheme, no optimization is performed. Instead, the interference between the legitimate users can be perfectly eliminated or zero-forced. Therefore, when the transmit power is high enough and the antennas are adequate, the secrecy rate of PU is higher in the IA-based scheme, while the sum rate of SUs is higher in the OTD scheme.
- *Complexity:* To solve the non-convex problem (9) in the OTD scheme, Algorithm 1 can be performed iteratively utilizing CVX. In the IA-based scheme, the solutions can be achieved via Algorithm 2 iteratively, whose computational complexity is a little lower than that of the OTD scheme.
- *Feasibility:* For the problem in (9), we cannot obtain any feasibility conditions like IA scheme. Instead, we can only know whether it can be solved by numerical methods, such as CVX. As for the IA-based scheme, its feasibility condition can be derived as (41) in Theorem 1, i.e., only when the feasibility condition is met, the IA-based scheme can be solved. Thus, the feasibility condition can provide the conclusion on the minimal number of antennas to remove interference in the legitimate network, which is also helpful to the OTD scheme.

To make it clear, we summarize them in Table I.

VI. Simulation Results and Discussions

In this section, extensive simulation results are presented to evaluate the performances of the two proposed schemes. In the simulation, we assume that $\sigma_p^2 = \sigma_s^2 = \sigma_e^2 = \sigma^2$. All the channels follow slow Rayleigh block fading.

First, to investigate the influence of r_s on the performance of the OTD scheme, the secrecy rate of PU and the sum rate of SUs are compared for different values of r_s in Fig. 2 and Fig. 3, respectively, where $K = 3, M = 3, N = 3, \sigma^2 = -20$dBm, and three cases, $P_S = 25$mW, $P_S = 15$mW and $P_S = 5$mW, are considered. In Fig. 2, the secrecy rate of PU is compared for different thresholds r_s. From this figure, we can observe that the secrecy rate of PU will increase with r_s, and we have $R_s \approx r_s$ for different values of P_S. Thus, we can conclude that the basic requirement of security for PU can be guaranteed in the OTD scheme, which is consistent with the objective function (9). In Fig. 3, the sum rate of SUs is compared for different thresholds r_s. From the result, we can see that the sum rate of SUs decreases with r_s. This is due to the fact that SUs should sacrifice their performance to guarantee higher security requirement of PU. In addition, the sum rate of SUs will increase with higher P_S, due to the fact that higher transmit power will result in higher transmission rate, if interference can be properly managed.

Then, the secrecy rate of PU and the transmission rate of an individual SU in the IA-based scheme are compared in Fig. 4 and Fig. 5, with different number of antennas equipped at each SU, when $K = 3$ and $K = 4$ are considered, respectively. In this simulation, assume that $P_p = 5$mW and the transmit power of each SU equals to 5mW, i.e., $P^{[k]} = 5$mW. In Fig. 4,

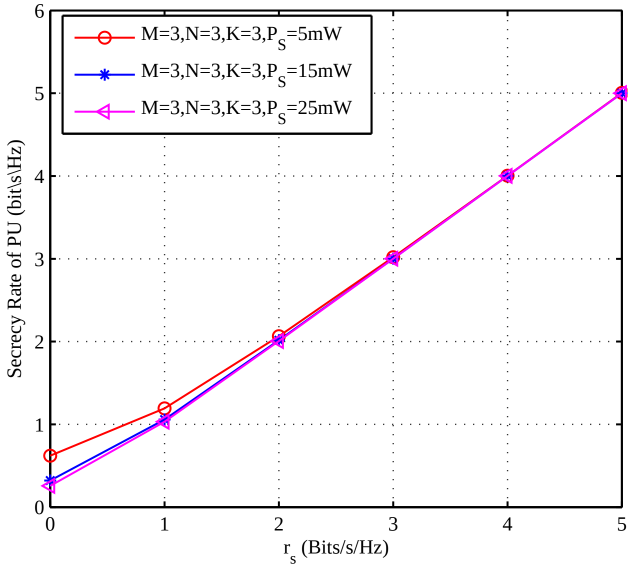


Fig. 2. Comparison of the secrecy rate of PU for the OTD scheme under different thresholds of r_s in a 3-user secondary network. Three cases of $P_S = 25\text{mW}$, $P_S = 15\text{mW}$ and $P_S = 5\text{mW}$ are considered.

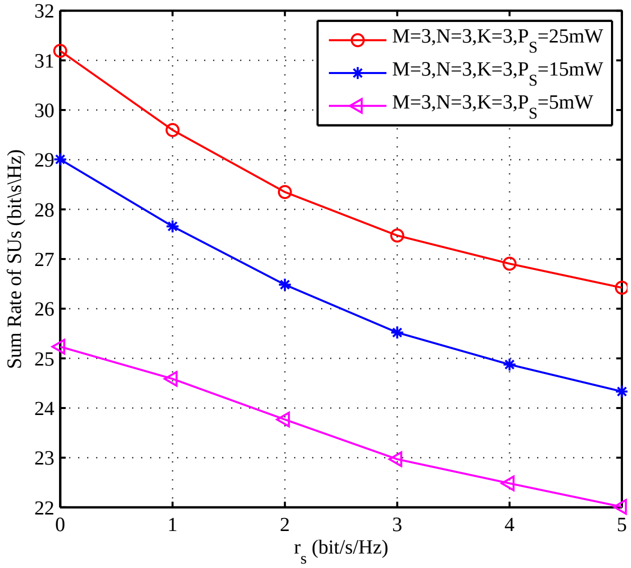


Fig. 3. Comparison of the sum rate of SUs for the OTD scheme under different thresholds of r_s in a 3-user secondary network. Three cases of $P_S = 25\text{mW}$, $P_S = 15\text{mW}$ and $P_S = 5\text{mW}$ are considered.

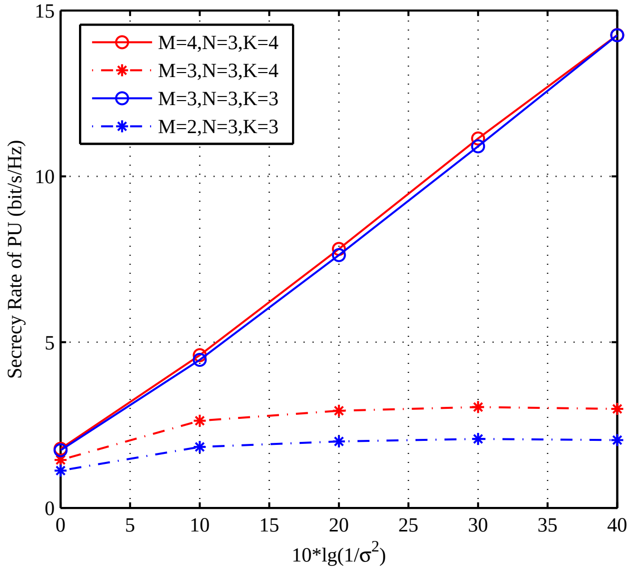


Fig. 4. Comparison of the secrecy rate of PU for the IA-based scheme with different number of antennas equipped at each SU, when the noise power is varying. $K = 3$ and $K = 4$ are considered, respectively.

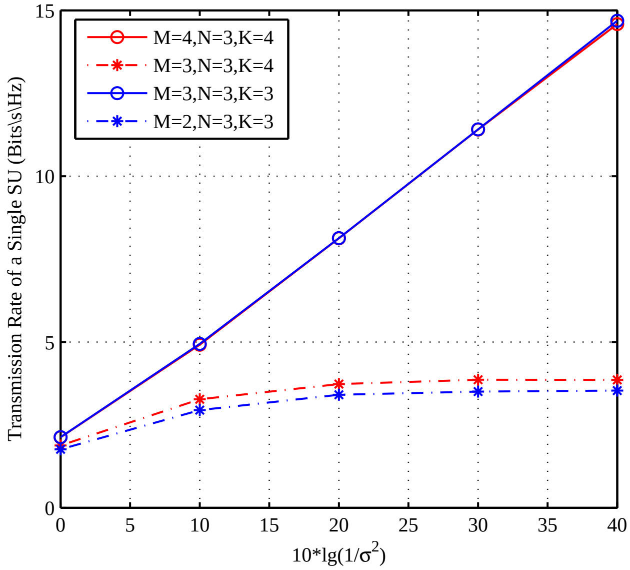


Fig. 5. Comparison of the transmission rate of a certain SU for the IA-based scheme with different number of antennas equipped at each SU, when the noise power is varying. $K = 3$ and $K = 4$ are considered, respectively.

the secrecy rate of PU with different values of σ^2 is compared. From the result, we can see that, when the IA-based scheme is feasible, i.e., $M + N = 6 \geq K + 3 = 6$ or $M + N = 7 \geq K + 3 = 7$, the secrecy rate of PU grows linearly with the decreasing noise power, due to the fact that the interference from all the SUs has been zero-forced at the primary receiver. However, when the IA-based scheme is not feasible, i.e., $M + N < 6$ $(K = 3)$ or $M + N < 7$ $(K = 4)$, the secrecy rate of PU will be much lower than that when it is feasible. This is because the interference from the SUs will not be eliminated, which will affect the transmission of PU. In Fig. 5, the transmission rate of a certain SU with different values of σ^2 is compared. From the result, we can see that the transmission rate of a certain SU linearly increases as the channel noise becomes smaller when the IA-based scheme is feasible. In addition, we can see that the average transmission rate of each user is close to others in different feasible cases. However, when the IA-based scheme is not feasible, the transmission rate of a certain SU becomes much lower than that when it is feasible.

The secrecy rate of PU and the sum rate of SUs in the proposed OTD and IA-based schemes is compared under different thresholds of P_S in Fig. 6 and Fig. 7, respectively. Assume that $r_s = 3\text{bits/s/Hz}$ and $\sigma^2 = -20\text{dBm}$. From Fig. 6, we can see that the secrecy rate of PU is always fixed and equal to that of the threshold r_s in the OTD scheme, which is

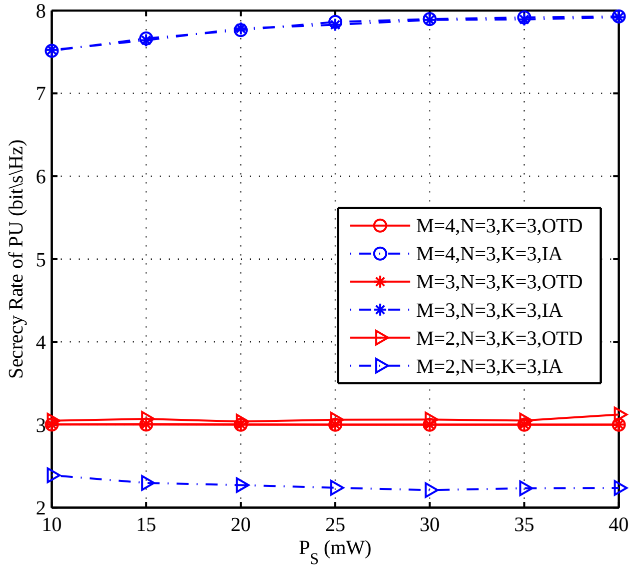


Fig. 6. Comparison of PU's secrecy rate for the OTD and IA-based schemes with different thresholds of P_S in a CR network with 3 SUs.

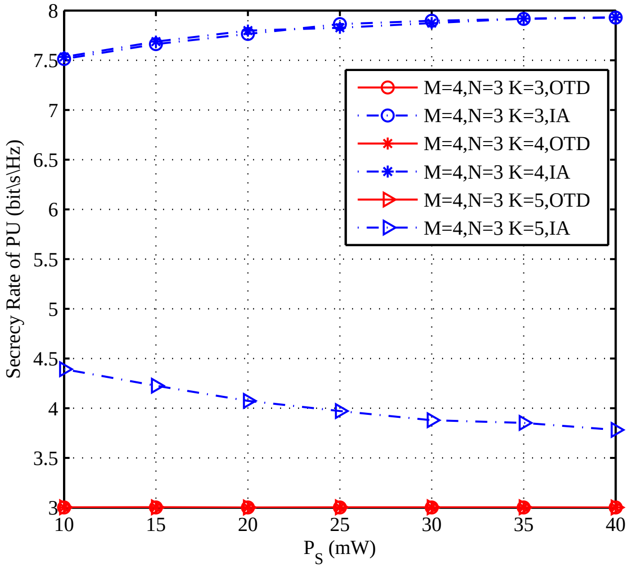


Fig. 8. Comparison of PU's secrecy rate for the OTD and IA-based schemes with different number of SUs. $M = 4$ and $N = 3$.

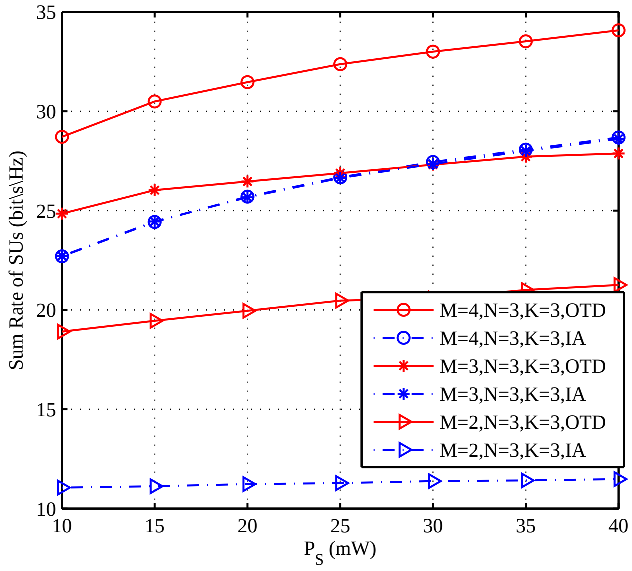


Fig. 7. Comparison of the sum rate of SUs for the OTD and IA-based schemes with different thresholds of P_S in a CR network with 3 SUs.

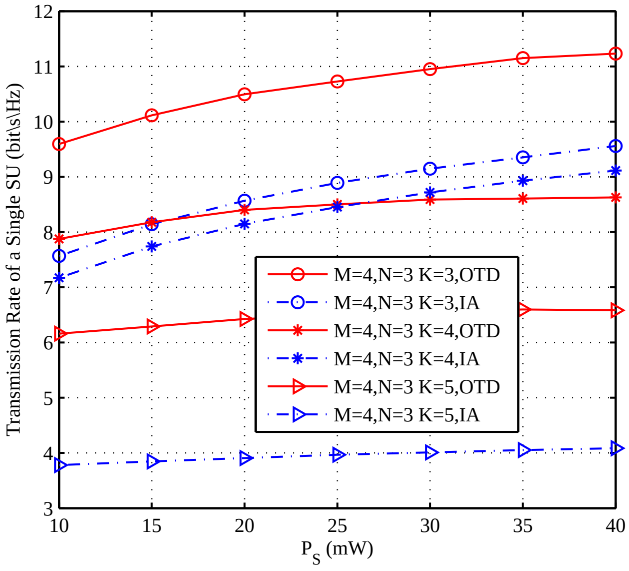


Fig. 9. Comparison of the transmission rate of a certain SU for the OTD and IA-based schemes with different number of SUs. $M = 4$ and $N = 3$.

consistent with the objective function (9). On the other hand, the secrecy rate of PU in the IA-based scheme is much higher than that in the OTD scheme, when the feasibility condition in Theorem 1 can be satisfied, i.e., $M + N \geq K + 3 = 6$, and it will increase as P_S becomes higher. However, when the IA-based scheme is not feasible, the secrecy rate of the IA-based scheme will become much worse than that in the OTD scheme. From the result in Fig. 7, we can find that the sum rate of SUs in the IA-based scheme is close to that in the OTD scheme, when it is feasible, i.e., $M + N = 6 = K + 3$, and will increase with higher P_S. When the number of antennas becomes larger than feasible, i.e., $M + N > K + 3 = 6$, the sum rate of SUs in the IA-based scheme will not increase any longer, while the sum rate of SUs in the OTD scheme will still become higher. However, when the IA-based scheme becomes infeasible, the sum rate of SUs of both schemes will become much lower, especially the IA-based scheme, due to the residual interference. Thus, we can conclude that the simulation results in Fig. 6 and Fig. 7 are consistent with the analysis in Section V.

Finally, the secrecy rate of PU and the transmission rate of a certain SU in the OTD and IA-based schemes are compared in Fig. 8 and Fig. 9, respectively, with different number of SUs. Assume that all the SUs are equipped with the equal number of antennas, i.e., $M = 4, N = 3$. $\sigma^2 = -20$dBm, $r_s = 3$bits/s/Hz, and three cases, $K = 3$, $K = 4$ and $K = 5$ are considered. From the result in Fig. 8, we can see that the secrecy rate of PU is always equal to r_s in the OTD scheme, with different number of SUs and different values of P_S, which is consistent with the objective function (9). In the IA-based scheme, the secrecy rate of PU will not changed with different number of SUs, when it is feasible, which is much higher than that in the OTD scheme. Besides, the secrecy rate of PU will become higher with larger value of P_S. However, when the IA-based scheme is not feasible, the secrecy rate of PU in the IA-based will become much worse, and will decrease with higher P_S, due to the fact that higher transmit power of SUs will generate larger interference at the primary receiver. From the result in Fig. 9, we can find that the transmission rate of a certain SU in the OTD scheme is higher than that in the IA-based scheme with the same number of antennas when it is infeasible ($M + N = 7 < K + 3$) or more than feasible ($M + N = 7 > K + 3$), due to the fact that the sum rate of SUs is maximized with the secrecy of PU guaranteed in the OTD scheme. When it is just exactly feasible, i.e., $M + N = 7 = K + 3$, the transmission rate of a single SU in these two schemes is close to each other. Besides, the transmission rate of a certain SU in the OTD scheme will decrease almost linearly with the number of SUs increases, due to the fact that more resource will be devoted to each SU when the number of SUs is less in the OTD scheme. In the IA-based scheme, the transmission rate of a certain SU will be almost stable and unchanged with different number of SUs, when it is feasible. However, the transmission rate of a certain SU will decrease seriously when the IA-based scheme is infeasible, due to the leaked interference.

VII. Conclusions and Future Work

In this paper, we proposed two schemes, i.e., OTD scheme and IA-based scheme, to achieve secure transmission of PU assisted by SUs in CR networks. In the OTD scheme, the secondary transceivers are jointly designed to maximize the sum rate of SUs with the secrecy rate of PU guaranteed. To solve the problem, it is converted into a convex one, and an SOCPAO algorithm is proposed to calculate the solutions. In the IA-based scheme, IA is exploited to eliminate and zero-force the interference at each SU and PU. Thus interference-free transmission can be achieved by the legitimate CR network, and the eavesdropping towards PU can be disrupted by the signal from SUs effectively. The feasibility conditions of the IA-based scheme are also derived. In addition, the key features of these two schemes are compared, and plenty of simulation results are presented to show their effectiveness. In our future work, we will focus on the design of the schemes in the case of a single multi-antenna eavesdropper or several eavesdroppers, and the imperfect CSI problem will also be considered.

References

[1] Y. Cao, N. Zhao, F. R. Yu, M. Jin, Y. Chen, and V. C. M. Leung, "Secondary transceiver design for secure primary transmission," in *Proc. IEEE VTC-Spring'18*, pp. 1–5, Porto, Portugal, Jun. 2018.

[2] D. Liu, L. Wang, Y. Chen, M. Elkashlan, K. K. Wong, R. Schober, and L. Hanzo, "User association in 5G networks: A survey and an outlook," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1018–1044, 2nd Quart. 2016.

[3] C. Yang, J. Li, M. Guizani, A. Anpalagan, and M. Elkashlan, "Advanced spectrum sharing in 5G cognitive heterogeneous networks," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 94–101, May 2016.

[4] G. Ding, J. Wang, Q. Wu, Y. d. Yao, R. Li, H. Zhang, and Y. Zou, "On the limits of predictability in real-world radio spectrum state dynamics: from entropy theory to 5G spectrum sharing," *IEEE Commun. Mag.*, vol. 53, no. 7, pp. 178–183, Jul. 2015.

[5] H. Xie, B. Wang, F. Gao, and S. Jin, "A full-space spectrum-sharing strategy for massive MIMO cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2537–2549, Oct. 2016.

[6] N. Zhao, F. R. Yu, H. Sun, and M. Li, "Adaptive power allocation schemes for spectrum sharing in interference-alignment-based cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3700–3714, May 2016.

[7] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart. 2015.

[8] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart. 2014.

[9] 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.

[10] 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.

[11] H. Xing, K. K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 7971–7984, Dec. 2016.

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

[13] 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.

[14] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[15] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[16] 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.

[17] 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.

[18] 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.

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

[20] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[21] 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.

[22] Y. Wu, C. Xiao, X. Gao, J. D. Matyjas, and Z. Ding, "Linear precoder design for MIMO interference channels with finite-alphabet signaling," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3766–3780, Sept. 2013.

[23] H. Zhang, T. Wang, L. Song, and Z. Han, "Interference improves PHY security for cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 609–620, Mar. 2016.

[24] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[25] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[26] A. Al-Talabani, Y. Deng, A. Nallanathan, and H. X. Nguyen, "Enhancing secrecy rate in cognitive radio networks via multilevel stackelberg game," *IEEE Commun. lett.*, vol. 20, no. 6, pp. 1112–1115, Jun. 2016.

[27] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

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

[29] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.

[30] N. Zhao, F. R. Yu, M. Jin, Q. Yan, and V. C. M. Leung, "Interference alignment and its applications: A survey, research issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1779–1803, 3rd Quart. 2016.

[31] A. Dong, H. Zhang, D. Yuan, and X. Zhou, "Interference alignment transceiver design by minimizing the maximum mean square error for MIMO interfering broadcast channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6024–6037, Aug. 2016.

[32] V. Ntranos, M. A. Maddah-Ali, and G. Caire, "Cellular interference alignment," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1194–1217, Mar. 2015.

[33] J. Tang, D. K. C. So, A. Shojaeifard, K. K. Wong, and J. Wen, "Joint antenna selection and spatial switching for energy efficient MIMO SWIPT system," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4754–4769, Jul. 2017.

[34] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[35] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[36] Z. Kong, S. Yang, F. 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.

[37] 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.

[38] 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.

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

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

[41] M. C. Grant and S. P. Boyd, "CVX: Matlab software for disciplined convex programming." Available online [ver. 2.1 (beta)]: http://web.cvxr.com/cvx/doc/, Dec. 2016.

[42] A. Beck, A. Ben-Tal, and L. Tetruashvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *J. Global Optim.*, vol. 47, no. 1, pp. 29–51, 2010.

[43] C. Yetis, T. Gou, S. A. Jafar, and A. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Proc.*, vol. 58, no. 9, pp. 4771–4782, Sep. 2010.

[44] 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.

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.

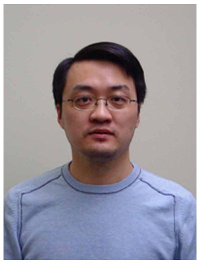
Nan Zhao (S'08-M'11-SM'16) is currently an Associate Professor at Dalian University of Technology, China. He received the B.S. degree in electronics and information engineering in 2005, the M.E. degree in signal and information processing in 2007, and the Ph.D. degree in information and communication 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, and as the TPC Co-Chair for IEEE/CIC ICCC 2018 - SPC: Signal Processign for Communications symposium. He received Top Reviewer Award from IEEE Transactions on Vehicular Technology in 2016, and was nominated as an Exemplary Reviewer by IEEE Communications Letters in 2016. He won the best paper awards in IEEE VTC'2017-Spring and MLICOM 2017.

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

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

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



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.

Jie Tang (S'10-M'13) received the B.Eng. degree in Information Engineering from the South China University of Technology, Guangzhou, China, in 2008, the M.Sc. degree (with Distinction) in Communication Systems and Signal Processing from the University of Bristol, UK, in 2009, and the Ph.D. degree from Loughborough University, Leicestershire, UK, in 2012. He is currently an associate professor in the School of Electronic and Information Engineering, South China University of Technology, China. He previously held Postdoctoral research positions at the School of Electrical and Electronic Engineering, University of Manchester, UK.

His research interests include green communications, NOMA, 5G networks, SWIPT, heterogeneous networks, cognitive radio and D2D communications. He is currently serving as an associate editor for *EURASIP Journal on Wireless Communications and Networking*, *Physical Communications* and *Ad Hoc & Sensor Wireless Networks*. He also served as a track co-chair for *IEEE Vehicular Technology Conference (VTC) Spring 2018*.

Victor C. M. Leung (S'75-M'89-SM'97-F'03) received the B.A.Sc. (Hons.) degree in electrical engineering from the University of British Columbia (UBC) in 1977, and was awarded the APEBC Gold Medal as the head of the graduating class in the Faculty of Applied Science. He attended graduate school at UBC on a Canadian Natural Sciences and Engineering Research Council Postgraduate Scholarship and received the Ph.D. degree in electrical engineering in 1982.

From 1981 to 1987, Dr. Leung was a Senior Member of Technical Staff and satellite system specialist at MPR Teltech Ltd., Canada. In 1988, he was a Lecturer in the Department of Electronics at the Chinese University of Hong Kong. He returned to UBC as a faculty member in 1989, and currently holds the positions of Professor and TELUS Mobility Research Chair in Advanced Telecommunications Engineering in the Department of Electrical and Computer Engineering. Dr. Leung has co-authored more than 1000 journal/conference papers, 38 book chapters, and co-edited 14 book titles. Several of his papers had been selected for best paper awards. His research interests are in the broad areas of wireless networks and mobile systems.

Dr. Leung is a registered Professional Engineer in the Province of British Columbia, Canada. He is a Fellow of IEEE, the Royal Society of Canada, the Engineering Institute of Canada, and the Canadian Academy of Engineering. He was a Distinguished Lecturer of the IEEE Communications Society. He is serving on the editorial boards of the IEEE Transactions on Green Communications and Networking, IEEE Transactions on Cloud Computing, IEEE Access, Computer Communications, and several other journals, and has previously served on the editorial boards of the IEEE Journal on Selected Areas in Communications - Wireless Communications Series and Series on Green Communications and Networking, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, IEEE Transactions on Computers, IEEE Wireless Communications Letters, and Journal of Communications and Networks. He has guest-edited many journal special issues, and provided leadership to the organizing committees and technical program committees of numerous conferences and workshops. He received the IEEE Vancouver Section Centennial Award, the 2011 UBC Killam Research Prize, and the 2017 Canadian Award for Telecommunications Research. He co-authored papers that won the 2017 IEEE ComSoc Fred W. Ellersick Prize and the 2017 IEEE Systems Journal Best Paper Award.