IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURE MODULATIONS FOR FUTURE WIRELESS COMMUNICATIONS AND MOBILE NETWORKS

Received April 21, 2018, accepted May 19, 2018, date of publication May 29, 2018, date of current version June 29, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2841875

Enhancing Security of Primary User in Underlay Cognitive Radio Networks With Secondary User Selection

MIAN QIN[1,2], SHOUYI YANG[1], HAO DENG[2], AND MOON HO LEE[3], (Life Senior Member, IEEE)

[1]School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China
[2]School of Physics and Electronics, Henan University, Kaifeng 475000, China
[3]Division of Electronics Engineering, Chonbuk National University, Jeonju 561-756, South Korea

Corresponding author: Hao Deng (gavind@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grants 61640005 and U1604159 and in part by the Special Project for Inter-Government Collaboration of State Key Research and Development Program under Grant 2016YFE0118400.

ABSTRACT This paper investigates the effect of multiuser gain provided by the secondary user selection on the secrecy performance of the primary users. We first propose a simple scheme where the user with the minimal interference channel is selected, and derive a closed-form lower bound of the achievable ergodic secrecy rate (ESR) of the primary users. In the high signal-to-noise ratio (SNR) regime, asymptotic result shows that the multiuser gain scales logarithmically with the number of the secondary users for a fixed interference temperature. Inspired by non-orthogonal multiple access strategy, we then propose a maximal jamming rate-based scheme, where the secondary with maximal interference channel is selected and it will transmit with an elaborately designed rate so that the primary receiver can cancel out the interference completely with successive interference cancellation. A closed-form expression of achievable ESR is also presented. Theoretical and simulation results show that the both proposed schemes can achieve multiuser gain and improve the security of the primary users significantly.

INDEX TERMS Physical layer security, cognitive radio networks, user selection, multiuser secrecy gain, successive interference cancellation.

I. INTRODUCTION

Due to its ability to improve spectrum utilization, cognitive radio (CR) has been received considerable attention in recent years [1]. By introducing CR to the fifth generation (5G) mobile networks, the primary users (base station (BS) and mobile users served by the BS) and the secondary users (mobile users non-served by the BS) can coexist in a same licensed band [2]. In such a underlay approach, it is known that the interference from the secondary users is harmful for the primary users and thus the interference should below a certain level [3].

Security is always an important issue for wireless networks since the broadcast nature of wireless channels make it easily be overheard by eavesdroppers. It is more important in CR networks because that both of the primary user and the secondary users should be protected [4]. Among various ways to protect security of CR systems, physical layer security is quite attractive since it can exploit the difference between the main channel and wiretap channel to protect secrecy transmission [5]. Due to its advantage, the application of physical layer security to cooperative networks and multiple antenna systems has been extensively studied [6]–[12], where the authors employed transmit beamforming or artificial noise to create a better main channel to achieve a positive secrecy rate. Moreover, directional modulation can project modulated signals into a predetermined spatial direction, and thus can be utilized to achieve security at physical layer [13]–[15]. Certainly, secrecy transmission scheme in cognitive networks has been widely investigated [16]–[19], [21]. Note that the primary users share their licensed channel with secondary users resulted in a loss of achievable rate, it is reasonable for the secondary users to cooperate with the primary users in return [16]. In a cooperative mode, the secondary users can act as a relay or a friendly jammer to improve the primary user's secrecy [16]. Obviously, resource allocation is crucial for guaranteing the primary user's security requirement

while making the cooperative secondary user achieve a large rate [17], [18]. It is worth pointing out that the proposed scheme in [17] provided secure communications for both primary and secondary services. This is different from the works which investigated the problem that maximizes the secondary secrecy rate [19], [20], or minimizes the secondary secrecy outage probability [21], under an interference threshed constraint.

Apart from the aforementioned cooperative transmission, user selection is also an efficient way to utilize the spatial resource. Since it can provide multiuser gain to enhance the security, user selection has been investigated in many works [22], [23]. Note that Yang *et al.* [22] and Zou *et al.* [23] employed multiuser gain to enhance the security of the secondary users. Seldom existing works considered the problem of improving the security of the primary users with secondary user selection. However, this is a common scenario in 5G cognitive networks, where device-to-device transmission coexists in the uplink or downlink of the base station. Thus it is of interesting to reveal that how the multiuser gain provided by the secondary user improves the secrecy performance of the primary users.

Note that, primary users and secondary users coexisting in a network can be regarded as a special case of multiple access. In non-orthogonal multiple access (NOMA), successive interference cancellation (SIC) can be used to manage interference. The use of NOMA to CR ensures that both primary user and secondary user can be served simultaneously, without causing too much performance degradation at primary users [2]. As pointed out in [24], in NOMA systems, a user with a strong channel condition, viewed as a secondary user, is squeezed into the spectrum occupied by a user with a poor channel condition, viewed as a primary user. Therefore, when NOMA is employed in a cognitive network, the interference of secondary user is controllable. Recalling that interference plays an important role in secure communications. When the secondary user transmits with a proper rate, the interference from the secondary user can be canceled out completely at the primary user, whereas the eavesdropper is still suffering from interference. It is shown in [25] and [26] that friendly jamming with a carefully designed rate significantly improves the security. The secrecy performance of cooperative NOMA systems was investigated in [27] and [28], which verified that a significant security improvement by NOMA compared with conventional orthogonal multiple access. However, whether the combination of SIC and user selection in the underlying cognitive radio network can improve the security of the primary user remains unclear.

To answer this question, a cognitive network with a pair of primary users and many secondary users is investigated in this paper. We propose two secondary user selection schemes and provide a comprehensive analysis of the effect of multiuser gain on the security of the primary user. The main contributions of this work can be summarized as follows.

1) In this work, we exploit secondary user selection to enhance the security of primary users, which has seldom been reported in the existing literatures. In order to achieve multiuser gain, two secondary user selection schemes are proposed, referred to as *minimal interference based scheme* and *maximal jamming rate based scheme*, respectively.
2) For the minimal interference based scheme, a closed-form lower bound of the achievable ESR and the corresponding asymptotic result in the high SNR regime are presented. The scaling law of the multiuser gain is well revealed and the relation between the secrecy performance and the interference temperature is also demonstrated.
3) For the maximal jamming rate based scheme, we assume that the primary user and the eavesdropper equip with a SIC receiver. We exploit the knowledge of main channel to determinate the information rate of the selected secondary user so that the interference from the secondary user at the primary user can be canceled completely. A closed-form expression of the ESR is also provided in the high SNR regime. It is shown that the security of the primary user can be significantly improved.

The remaining of this paper is organized as follows. In Section II, we describe the system model. Section III provides the minimal interference based scheme and investigates its achieved multiuser secrecy gain. Section IV introduces the maximal jamming rate based scheme and investigates its secrecy performance. Finally, we demonstrate and discuss numerical results in Section V and conclude our work in Section VI.

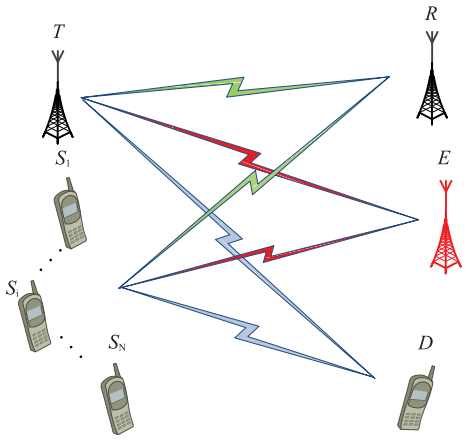


FIGURE 1. An illustration of system model.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider an underlay cognitive network sharing a licensed channel that used by a pair of primary users, denoted by T and R, and a secondary network consisting of N users S_i for $i = 1, \cdots, N$ and a receiver D, as illustrated in Fig. 1. The primary transmitter T sends confidential messages to

the primary receiver R in the presence of a passive eavesdropper E. Since the secondary network benefits from the sharing of licensed channel of the primary users, it is willing to help the primary user to enhance their security. Without loss of generality, all the users are assumed to be equipped with a single antenna and work in a half-duplex mode.[1] The channel gain from T to R, D and E are represented by h_{TR}, h_{TD} and h_{TE}, respectively. Also, h_{S_iJ} for $J = R, E, D$ denoted the channel from the i-th secondary user to R, D and E respectively. We assume that all the channel experience with independent Rayleigh fading. We also assume that the CSIs of primary and secondary links are available at the secondary transmitter as in [17] and [30].

The basic idea of physical layer security is to exploit spatial resource, provided by multiple antennas and/or multiuser, to enhance the security of wireless communications. In underlay cognitive networks, the primary users share its licensed band with secondary users to improve the spectral efficiency. When there are multiple secondary users in the networks, if user selection is adopt, their transmit signals may impose less interference on the primary receiver than that on the eavesdroppers. Thus it is of interesting to investigate that how multiuser gain from secondary user selection improves the security of the primary users. Inspired by the NOMA, knowledge of the main channel can be further exploited to determinate the transmit rate so that the receiver can employ SIC to decode its receiving signal. In this sense, the elaborately designed signal of selected secondary user can be seen as jamming signal. In the following, we will propose two user selection scheme to investigate the secrecy gain of user selection and friendly jamming.

In order to offer insight of multi-user diversity gain to improve the security of primary networks and investigate the impact of interference temperature I and transmit peak power P_S on the secrecy performance, we use ergodic secrecy rate (ESR) as the performance metric. The ESR of primary networks can be given as [31]

$$R_s = \left\{ \mathbb{E}\left[C_R\right] - \mathbb{E}\left[C_E\right] \right\}^+, \tag{1}$$

where $\{x\}^+ = \max(0, x)$ and $\mathbb{E}[x]$ denotes the expectation of random variable x.

III. MINIMAL INTERFERENCE BASED SECONDARY USER SELECTION

A. SECONDARY USER SELECTION SCHEME

It is well known that the interference perceived at the primary user from the secondary transmitter is harmful when there is no security considerations [3], [32]. Therefore, such interference should be below a given interference temperature level I. Accordingly, the secondary transmitter will adjust its transmitted power adaptively according to the channel gain so that it satisfies the interference requirement. Therefore, the transmit power of the i-th secondary transmitter is given by

$$P_i = \begin{cases} P_S, & |h_{S_iR}|^2 \le \dfrac{I}{P_S}, \\ \dfrac{I}{|h_{S_iR}|^2}, & |h_{S_iR}|^2 > \dfrac{I}{P_S}, \end{cases} \tag{2}$$

where P_S is the peak power of secondary users. Note that, this is different from the work [22] which only consider the interference limit. Previous studies show that the interference can bring benefit to secure communications when it degrades the wiretap channel worse than the main channel. Therefore, we can mitigate the interference at primary user via secondary user selection in CRN. In such a case, the traditional harmful interference can work in a way as friendly jamming. Also, it is interesting to investigate that how the values of P_S and I impact on the achievable secrecy rate of the primary users.

According to the above discussion, we should select a secondary transmitter which can degrade the wiretap channel most severely while the interference at primary user is also below a threshold. Since the interference level at the eavesdropper is mainly relied on the transmit power of the selected secondary user, a secondary user with the worst channel from it to the primary receiver R is selected to communicate with the seconder receiver D, and we call this scheme as *minimal interference based scheme.*

Under such a transmission scheme, the selected secondary user can transmit with a power as large as possible. Thus it would degrade the received SNR at the eavesdropper severely. On the other hand, the secondary receiver also can achieve a high rate. Accordingly, the transmit power of the selected secondary transmitter, denoted by S_*, is given by

$$P_* = \begin{cases} P_S, & |h_{S_*R}|^2 \le \dfrac{I}{P_S}, \\ \dfrac{I}{|h_{S_*R}|^2}, & |h_{S_*R}|^2 > \dfrac{I}{P_S}, \end{cases} \tag{3}$$

where $|h_{S_*R}|^2 = \min\limits_{1\le i\le N} |h_{S_iR}|^2$. It is worth pointing out that the secondary user selection is different from that in [32] and [33] where the multi-user diversity was employed to improve the throughput of secondary systems. Although Yang *et al.* [22] considered a similar communication scenario as ours, the proposed secondary user scheduling schemes target at maximizing the achievable secrecy rate of secondary users. However, in this paper, we want to exploit multi-user diversity to enhance the security of the primary networks.

[1] We assume that a single antenna (as reported in [17] and [23]) will be equipped by the eavesdropper, probably an unlicensed or an untrusted user in a cognitive network, to overhear the confidential messages transmitted by the BS. Accordingly, when multiple antenna are used by the eavesdropper, the achievable secrecy rate of the primary user would decrease. However, we have verified that secure communications, aided by multiuser gain, is still guaranteed even more antennas are utilized by eavesdropper than BS [29]. The present study is based on the power of multiuser secrecy gain, and its impact on secure transmission with a multiple-antenna eavesdropper will be examined in our future study.

Once the secondary user is selected, the received SNRs at R, E and D can be expressed respectively as

$$\Gamma_R = \frac{P_T|h_{TR}|^2}{P_*|h_{S_*R}|^2+\sigma^2}, \tag{4}$$

$$\Gamma_E = \frac{P_T|h_{TE}|^2}{P_*|h_{S_*E}|^2+\sigma^2}, \tag{5}$$

$$\Gamma_D = \frac{P_*|h_{S_*D}|^2}{P_T|h_{TD}|^2+\sigma^2}, \tag{6}$$

where P_T is the transmit power of the primary transmitter and σ^2 is the variance of additive white Gaussian noise. Without loss of generality, we assume that all receivers have the same variance of noise and it holds $P_T > P_S$. Note that in (4) and (5), we assume that the signals from selected secondary user are treated as noise at both R and E as in [18]. Consequently, the achievable rate at R and E are given respectively as

$$C_R = \begin{cases} \log\left(1+\dfrac{\rho_T|h_{TR}|^2}{\rho_S|h_{S_*R}|^2+1}\right), & |h_{S_*R}|^2 \le \dfrac{\rho_I}{\rho_S}, \\ \log\left(1+\dfrac{\rho_T|h_{TR}|^2}{\rho_I+1}\right), & |h_{S_*R}|^2 > \dfrac{\rho_I}{\rho_S}, \end{cases} \tag{7}$$

$$C_E = \begin{cases} \log\left(1+\dfrac{\rho_T|h_{TE}|^2}{\rho_S|h_{S_*E}|^2+1}\right), & |h_{S_*R}|^2 \le \dfrac{\rho_I}{\rho_S}, \\ \log\left(1+\dfrac{\rho_T|h_{TE}|^2}{\frac{\rho_I|h_{S_*E}|^2}{|h_{S_*R}|^2}+1}\right), & |h_{S_*R}|^2 > \dfrac{\rho_I}{\rho_S}, \end{cases} \tag{8}$$

$$C_D = \begin{cases} \log\left(1+\dfrac{\rho_S|h_{S_*D}|^2}{\rho_T|h_{TD}|^2+1}\right), & |h_{S_*R}|^2 \le \dfrac{\rho_I}{\rho_S}, \\ \log\left(1+\dfrac{\frac{\rho_I}{|h_{S_*R}|^2}|h_{S_*D}|^2}{\rho_T|h_{TD}|^2+1}\right), & |h_{S_*R}|^2 > \dfrac{\rho_I}{\rho_S}, \end{cases} \tag{9}$$

where $\rho_T \triangleq \frac{P_R}{\sigma^2}$, $\rho_S \triangleq \frac{P_S}{\sigma^2}$ and $\rho_I \triangleq \frac{I}{\sigma^2}$. It is worth pointing out that the secondary receiver also achieves benefit of multiuser gain. We will compare the achievable rate of D in Eqn. (9) with that of the proposed scheme in Section-IV. In the following, we will give a closed-form lower bound of the ESR and show how secondary user selection improves the security of primary networks.

B. ACHIEVABLE ERGODIC SECRECY RATE

Before proceeding, we first give the following lemma to address the statistics characteristic of $|h_{S_*R}|^2$.

Lemma 1: Let $X_{min} = \min_{1\le i\le N}|h_{S_iR}|^2$, where $|h_{S_iR}|^2$'s are i.i.d. and exponentially distributed variables with mean 1. The PDF of X_{min} is

$$f_{X_{min}}(x) = Ne^{-Nx}. \tag{10}$$

Proof: Proof can be easily completed by using the result in appendix of [32]. ■

It is known that the interference temperature I must be as small as possible since it can hurt the quality of the primary user's channel without security consideration. However, when security is taken into account, it is still not clear how secrecy rate scales with I. This is interesting to understand the relation between ESR and I. To reveal the effects of parameters such as P_R and P_S on the secrecy performance of primary user, we want to obtain an explicit expression of the ESR. Unfortunately, a closed-form of the ESR is unlikely to obtain by the mathematical method. Thus, we turn to derive a lower bound of ESR. As will be seen in the simulations, this lower bound agrees with simulation results.

Theorem 1: When a secondary user with minimal interference channel is selected, the achievable ESR of primary user satisfies

$$R_s \gtrapprox \{R_R - R_E\}^+, \tag{11}$$

where R_R and R_E are shown on the bottom of this page. In Eq. (11) and (12), Ξ_R and Ξ_E are given as

$$\Xi_R = e^{-\frac{N\rho_I}{\rho_S}+\frac{\rho_I+1}{\rho_T}}E_1\Big(\frac{\rho_I+1}{\rho_T}\Big), \tag{14}$$

$$\Xi_E = \begin{cases} e^{-\frac{1}{\rho_S}} - \frac{1}{\rho_S}E_1\big(\frac{1}{\rho_S}\big), & \rho_I = \frac{1}{N}, \\ \frac{N\rho_I}{N\rho_I-1}\Big(e^{\frac{1-N\rho_I}{\rho_S}}E_1\big(\frac{1}{\rho_S}\big) - E_1\big(\frac{N\rho_I}{\rho_S}\big)\Big), & \rho_I \ne \frac{1}{N}, \end{cases} \tag{15}$$

Note that in Eq. (12) and (13), $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt$ is the zeroth incomplete gamma function, $\mathcal{S}_{u,v}(\cdot)$ denotes the Lommel function, and $\mathcal{G}$ represents the Meijer-G function [34].

Proof: Please see Appendix A. ■

Theorem 1 gives a lower bound of the achievable ESR, which will be verified by simulations to examine how well it describe the behavior of ESR. Using this lower bound, we can

$$R_R = \frac{N\rho_T e^{\frac{N}{\rho_S}}}{N\rho_T-\rho_S}\left(e^{-\frac{N\rho_T-\rho_S}{\rho_T\rho_S}}E_1\Big(\frac{1}{\rho_T}\Big) - e^{-\frac{(N\rho_T-\rho_S)(\rho_I+1)}{\rho_T\rho_S}}E_1\Big(\frac{\rho_I+1}{\rho_T}\Big) + E_1\Big(\frac{N(\rho_I+1)}{\rho_S}\Big) - E_1\Big(\frac{N}{\rho_S}\Big)\right) + \Xi_R, \tag{12}$$

$$R_E = \frac{\rho_T\left(1-e^{-\frac{N\rho_I}{\rho_S}}\right)}{\rho_T-\rho_S}\left(e^{\frac{1}{\rho_T}}E_1\Big(\frac{1}{\rho_T}\Big) - e^{\frac{1}{\rho_S}}E_1\Big(\frac{1}{\rho_S}\Big)\right) + e^{-\frac{N\rho_I}{\rho_S}}\log\rho_I + 8e^{\frac{1}{\rho_T}}\sqrt{\frac{\rho_I}{\rho_T}}\mathcal{S}_{-2,1}\Big(2\sqrt{\frac{\rho_I}{\rho_T}}\Big)$$
$$-\big(e^{\frac{1}{\rho_T}}-1\big)\mathcal{G}_{3,2}^{1,3}\left[\frac{\rho_I\big(1-e^{-\frac{1}{\rho_T}}\big)}{\rho_T}\middle|\begin{matrix}1,1,0\\1,-1\end{matrix}\right] - \log\frac{\rho_I}{\rho_S}e^{-\frac{N\rho_I}{\rho_S}} - E_1\Big(\frac{N\rho_I}{\rho_S}\Big) - \Xi_E. \tag{13}$$

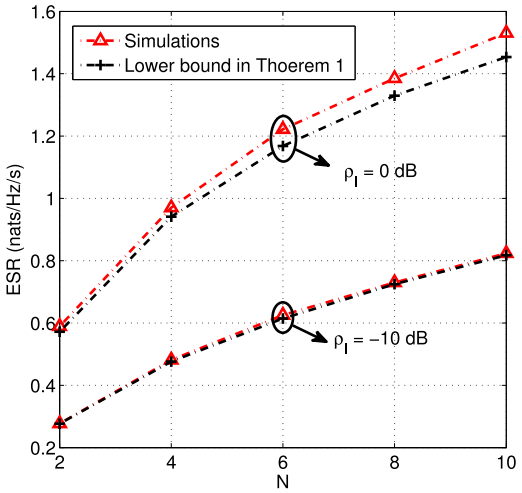


FIGURE 2. ESR vs. the number of the secondary users.

investigate the impact of I, P_R on the secrecy performance of the primary users numerically.

In order to verify the accuracy of Theorem 1, Fig. 2 shows the achievable ESR versus the numbers of secondary users, where $\rho_T = 22\ dB$ and $\rho_S = 20\ dB$. It is shown that the theoretical results agree well with the simulation results. As expected, the achievable ESR increases with N, implying that the secondary user selection indeed improves the secrecy performance of the primary users. Another interesting observation is that the primary user would achieve a higher secrecy rate when the interference temperature I gets large. This is quite different from the case without security consideration. That is, interference from the secondary user is helpful rather than harmful in secure cognitive communications.

The expression of theorem 1 is quite complicated, it can not offer insight to the diversity gain and the effect of interference straightforwardly. Therefore, we give an asymptotically analysis in the following subsection.

C. ASYMPTOTIC ANALYSIS IN THE HIGH SNR REGIME

Since the interference temperature I denotes the most negligible power form the secondary users to the primary one, it is reasonable to assume that $P_T \gg I$. In this subsection, we focus on the high SNR regime assuming that ρ_T and ρ_S are large enough and thus the random event $|h_{S_*R}|^2 \leq \frac{\rho_I}{\rho_S}$ would happen with a negligible probability. Then, the achievable rate at R and E are approximated as

$$C_R \approx \log\left(1 + \frac{\rho_T |h_{TR}|^2}{\rho_I + 1}\right), \tag{16}$$

$$C_E \approx \log\left(1 + \frac{\rho_T |h_{TE}|^2}{\frac{\rho_I |h_{S_*E}|^2}{|h_{S_*R}|^2} + 1}\right). \tag{17}$$

Using the result $e^{\frac{1}{x}} E_1\left(\frac{1}{x}\right) \approx \log x - \gamma$ as $x \to \infty$, the expression of $\mathbb{E}[C_R]$ can be derived as

$$\mathbb{E}[C_R] \approx \log \frac{\rho_T}{\rho_I + 1} - \gamma, \tag{18}$$

where $\gamma = 0.57721566\cdots$ is the Euler-Mascheroni constant.

Following with the definition in (47), the expression of $\mathbb{E}[C_E]$ can be rewritten as

$$\begin{aligned}\mathbb{E}[C_E] \approx &-\int_0^\infty \int_0^\infty \log\left(\rho_I z + x\right) e^{-z} N e^{-Nx} dz dx \\ &+ \int_0^\infty \int_0^\infty \int_0^\infty \log\left(\rho_I z + x + \rho_T t x\right) \\ &\times e^{-t} e^{-z} N e^{-Nx} dt dz dx \end{aligned} \tag{19}$$

Based on the result in (48) and (49), using the result $e^{\frac{1}{x}} E_1\left(\frac{1}{x}\right) \approx \log x - \gamma$ again yields

$$\mathbb{E}[C_E] \approx \begin{cases} \log \rho_T - \gamma - 1, & \rho_I = \frac{1}{N}, \\ \log \rho_T - \gamma - \frac{N\rho_I \log N\rho_I}{N\rho_I - 1}, & \rho_I \neq \frac{1}{N}. \end{cases} \tag{20}$$

With the above high SNR approximations, we have the following theorem.

Theorem 2: For $\rho_T \gg I$, the achievable ESR of the primary user in the high SNR regime is approximated as

$$R_s \approx \begin{cases} 1 + \log \frac{N}{N+1}, & \rho_I = \frac{1}{N}, \\ \frac{N\rho_I \log N\rho_I}{N\rho_I - 1} - \log(\rho_I + 1), & \rho_I \neq \frac{1}{N}. \end{cases} \tag{21}$$

As $\rho_I = \frac{1}{N}$, theorem 2 indicates that the multiuser gain in terms of secrecy rate in a cognitive networks grows with $\log \frac{N}{N+1}$. For a big N, such multiuser gain converges to zero. While for $\rho_I > \frac{1}{N}$, the term $\frac{N\rho_I \log N\rho_I}{N\rho_I - 1}$ in (21) holds $\frac{N\rho_I \log N\rho_I}{N\rho_I - 1} > \log N\rho_I$. This implies that the secrecy rate at least scales with $\log N$, and thus it would achieve more multiuser gain. Similarly, we can analyze the case $\rho_I < \frac{1}{N}$.

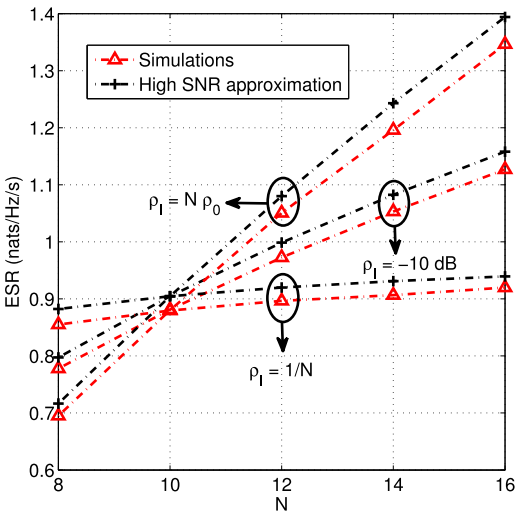


FIGURE 3. ESR vs. the number of the secondary users in the high SNR regime.

Fig. 3 plots the asymptotic results given in Theorem 2. We set the transmit power P_T and P_S as $\rho_T = 30\ dB$ and $\rho_S = 25\ dB$, respectively. The value of ρ_0 is $-20\ dB$. It can be seen that all the asymptotic results are almost consistent with the simulation results. Fig. 3 verifies that the scheme

with $\rho_I = \frac{1}{N}$ achieves a fairly small multiuser gain. It is not surprising that the adaptive scheme with $N\rho_0$ has the highest increasing rate as N gets larger. Observing Fig. 3, we can conclude that the primary user can tolerate a large interference temperature with secondary user selection, and thus the achievable multiuser gain can improve the security greatly.

Recalling the equations (16) and (17), we can see that the peak power of secondary users P_S disappears in the expression. That is, it can be regarded as a scheme without peak power constraints in the high SNR regime. In contrast, there is another special case without interference temperature constraints. In the following subsection, we will give a comprehensive study for such a case.

D. NO INTERFERENCE TEMPERATURE CONSTRAINT

When there is no constraint of interference temperature, the selected secondary user will transmit with an average power constraint P_S. Therefore, the achievable rate at R and E can be rewritten as

$$C_R = \log\left(1 + \frac{\rho_T |h_{TR}|^2}{\rho_S |h_{S_*R}|^2 + 1}\right), \tag{22}$$

$$C_E = \log\left(1 + \frac{\rho_T |h_{TE}|^2}{\rho_S |h_{S_*E}|^2 + 1}\right). \tag{23}$$

Comparing the above equations with (16) and (17), we can find that the two special scheme i) without peak power constraint and ii) without interference temperature constraint can achieve secrecy rate gain by secondary user selection. However, they work in different ways. The former one is to deteriorate the eavesdropper' channel as serious as possible, whereas the latter one is to make the lowest interference at the primary user. Similar to the procedure of Appendix A, we can have the following result.

Theorem 3: when there is no interference temperature constraint, the achievable ESR of the primary user is

$$R_s = \left\{\frac{N\rho_T}{N\rho_T - \rho_S}\left(e^{\frac{1}{\rho_T}} E_1\left(\frac{1}{\rho_T}\right) - e^{\frac{N}{\rho_S}} E_1\left(\frac{N}{\rho_S}\right)\right) - \frac{\rho_T}{\rho_T - \rho_S}\left(e^{\frac{1}{\rho_T}} E_1\left(\frac{1}{\rho_T}\right) - e^{\frac{1}{\rho_S}} E_1\left(\frac{1}{\rho_S}\right)\right)\right\}^+. \tag{24}$$

Note that the variance of $|h_{S_*R}|^2$ is $\frac{1}{N}$, which would approach to zero for a large N. When N is large, the achievable rate of the primary user can be approximated as $\mathbb{E}[C_R] \approx e^{\frac{\rho_S/N+1}{\rho_T}} E_1\left(\frac{\rho_S/N+1}{\rho_T}\right)$. Based on the inequality $e^x E_1(x) > \frac{1}{2}\log\left(1+\frac{1}{x}\right)$ [35], we have $\mathbb{E}[C_R] > \frac{1}{2}\log\left(1+\frac{\rho_T}{\rho_S/N+1}\right)$. In the high SNR regime, we further have $\mathbb{E}[C_R] > \frac{1}{2}\log\rho_T - \frac{1}{2}\log\left(1+\frac{\rho_S}{N}\right)$. One can easily see that the term $\frac{1}{2}\log\left(1+\frac{\rho_S}{N}\right)$ would decrease with N and thus the primary user achieves a higher secrecy rate.

Fig. 4 shows the achievable ESR versus N when there is no interference temperature constraint. We set $\rho_T = 20\ dB$. It can be seen from Fig. 4 that all the ESRs increase as N grows. It should be noted that when ρ_S becomes larger, ESR would increase faster. This is because that the item $\frac{1}{2}\log\left(1+\frac{\rho_S}{N}\right)$ which represents the multiuser gain would be small for a small ρ_S. In Fig. 4, we also consider a special case $\rho_S > \rho_T$. As seen in Fig. 4, although the case $\rho_S = 22\ dB$ achieves a smaller ESR than the case $\rho_S = 15\ dB$ for a small N, it can achieve a higher ESR when N is large. This further verifies that the interference is helpful in secure cognitive communications.

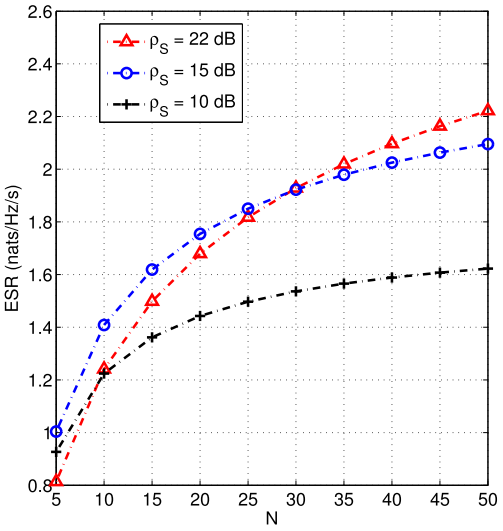


FIGURE 4. ESR vs. the number of the secondary users when there is no interference temperature constraint.

IV. MAXIMAL JAMMING RATE BASED SECONDARY USER SELECTION

As we have discussed before, by exploiting prior channel state information (CSI) of the main channels, the selected secondary user will transmit its signal with a certain rate so that the primary receiver can cancel out such signals by applying SIC. Note that the signal from the selected secondary user can be regarded as jamming signal to degrade eavesdropper's channel, and this jamming effect can be enhanced by maximizing transmission rate of the secondary. Therefore, we call the following proposed scheme as *maximal jamming rate based scheme*.

A. SECONDARY USER SECTION

With such a transmission scheme, the primary user can cancel out the interference from the secondary user completely. On the contrary, the eavesdropper will decode the signal from the secondary user successfully with a low probability. When the i-th secondary user is selected, this user will transmit jamming signal z with power P_S. Then the received SNR for decoding z at R and E can be written as

$$\Gamma^i_{R,z} = \frac{P_S |h_{S_iR}|^2}{P_T |h_{TR}|^2 + \sigma^2}, \tag{25}$$

$$\Gamma^i_{E,z} = \frac{P_S |h_{S_iE}|^2}{P_T |h_{TE}|^2 + \sigma^2}. \tag{26}$$

For fair comparison with the proposed scheme in Section-III, we still assume that the transmit power of the selected secondary user is P_S. If the secondary user transmit with a rate R_J holding $R_J \leq \log(1+\Gamma^{R,z})$, R can cancel out the interference before detecting the information signal from T. On the other hand, if it holds $R_J > \log(1+\Gamma^{E,z})$, the eavesdropper cannot decode the interference correctly and it will treat interference as noise as in Section-III. Accordingly, the secondary user should transmit with a rate as high as possible. Therefore, we have $R_J = \log(1+\Gamma^{R,z})$. Obviously, a bigger $\Gamma^{R,z}$ corresponds to a larger R_J. Consequently, the secondary user with the strongest interference channel is selected and transmits a rate in the form of

$$R_J = \log\left(1+\frac{P_S|h_{S_\#R}|^2}{P_T|h_{TR}|^2+\sigma^2}\right), \tag{27}$$

where $|h_{S_\#R}|^2 = \max\limits_{1\leq i\leq N}|h_{S_iR}|^2$. This is quite different from the proposed scheme in Section-III where the secondary user with lowest interference channel is selected.

Since the primary receiver can cancel the interference completely before decoding s, the achievable rate of s at R is

$$C_{R,s} = \log\left(1+\rho_T|h_{TR}|^2\right). \tag{28}$$

If $R_J > \log(1+\Gamma_{E,z})$, the eavesdropper can not decode the interference from the selected secondary user, and thus would be interfered with. If $R_J \leq \log(1+\Gamma_{E,z})$, the interference can be cancelled out at the eavesdropper. Hence, the achievable rate at the eavesdropper is

$$C_{E,s} = \begin{cases} \log\left(1+\rho_T|h_{TE}|^2\right), & R_J \leq \log(1+\Gamma^{\#}_{E,z}), \\ \log\left(1+\frac{\rho_T|h_{TE}|^2}{\rho_S|h_{S_\#E}|^2+1}\right), & R_J > \log(1+\Gamma^{\#}_{E,z}). \end{cases} \tag{29}$$

Using the result in Eqn. (27), we further have

$$C_{E,s} = \begin{cases} \log\left(1+\rho_T|h_{TE}|^2\right), & \frac{\rho_S|h_{S_\#R}|^2}{\rho_T|h_{TR}|^2+1} \leq \frac{\rho_S|h_{S_\#E}|^2}{\rho_T|h_{TE}|^2+1}, \\ \log\left(1+\frac{\rho_T|h_{TE}|^2}{\rho_S|h_{S_\#E}|^2+1}\right), & \frac{\rho_S|h_{S_\#R}|^2}{\rho_T|h_{TR}|^2+1} > \frac{\rho_S|h_{S_\#E}|^2}{\rho_T|h_{TE}|^2+1}. \end{cases} \tag{30}$$

We still assume that it holds $P_S < P_T$ to maintain consistency with Section-III. However, our results can be easily to be generalized to the case $P_S \geq P_T$.

Under the above transmission scheme, the achievable rate at D is given as

$$C_{D,z} = \begin{cases} R_J, & \frac{\rho_S|h_{S_\#R}|^2}{\rho_T|h_{TR}|^2+1} \leq \frac{\rho_S|h_{S_\#D}|^2}{\rho_T|h_{TD}|^2+1}, \\ 0, & \frac{\rho_S|h_{S_\#R}|^2}{\rho_T|h_{TR}|^2+1} > \frac{\rho_S|h_{S_\#D}|^2}{\rho_T|h_{TD}|^2+1}. \end{cases} \tag{31}$$

From (31), we know that the achievable rate is upper bounded by R_J. Although R_J grows with N, the probability $\mathcal{P}\left\{\frac{\rho_S|h_{S_\#R}|^2}{\rho_T|h_{TR}|^2+1} \leq \frac{\rho_S|h_{S_\#D}|^2}{\rho_T|h_{TD}|^2+1}\right\}$ would decrease as N increases. This is different from that in (9) where the multiuser gain improves the achievable rate at secondary receiver. From (27), we know that in order to achieve a higher rate at D, the selected secondary user can transmit with a larger power. On the other hand, since it satisfies the condition $\frac{\rho_S|h_{S_\#R}|^2}{\rho_T|h_{TR}|^2+1} \leq \frac{\rho_S|h_{S_\#E}|^2}{\rho_T|h_{TE}|^2+1}$ with a big probability, the eavesdropper would suffer more interference for a larger ρ_S.

In the following, we will give an explicit expression of the achievable ESR of maximal jamming rate based secondary user selection.

B. ACHIEVABLE ERGODIC SECRECY RATE

Before proceeding, we give a lemma will be used to derive the result of ESR.

Lemma 2: Let $U = \frac{\rho_S|h_{S_\#R}|^2}{\rho_T|h_{TR}|^2+1}$, the CDF of U is

$$F_U(u) = \sum_{n=0}^{N}(-1)^n C_N^n \frac{e^{-\frac{nu}{\rho_S}}}{1+\frac{n\rho_T u}{\rho_S}}, \tag{32}$$

where C_m^n denotes the combinatorial number m over n.

Proof: Let $X_{max} = |h_{S_\#R}|^2 = \max\limits_{1\leq i\leq N}|h_{S_iR}|^2$, where $|h_{S_iR}|^2$'s are i.i.d. and exponentially distributed variables with mean 1. We can easily obtain that the cumulative distribution function (CDF) of X_{max} has the form of $(1-e^{-x})^N$. Accordingly, the PDF of X_{max} can be obtained as $f_{X_{max}}(x) = Ne^{-x}(1-e^{-x})^{N-1}$. Let $Y = |h_{TR}|^2$, the CDF of U can be calculated as

$$\begin{aligned} \mathcal{P}\{U \leq u\} &= \mathcal{P}\{\frac{P_S x}{P_T y+1} \leq u\} \\ &= \int_0^{\frac{\rho_T y+1}{\rho_S}u} f_{X_{max}}(x)dx \int_0^{\infty} e^{-y}dy \\ &= \int_0^{\infty}\left(1-e^{-\frac{\rho_T y+1}{\rho_S}u}\right)^N e^{-y}dy \\ &= \sum_{n=0}^{N}(-1)^n C_N^n e^{-\frac{nu}{\rho_S}}\int_0^{\infty} e^{-\left(1+\frac{n\rho_T u}{\rho_S}\right)y} \\ &= \sum_{n=0}^{N}(-1)^n C_N^n \frac{e^{-\frac{nu}{\rho_S}}}{1+\frac{n\rho_T u}{\rho_S}}. \end{aligned} \tag{33}$$

The proof is completed. ■

Similar to the analysis given in Section-III, we present an expression of ESR for the maximal jamming rate based scheme to illustrate its secrecy performance. Therefore, we give a theorem in the following.

Theorem 4: When a secondary user with strongest interference channel is selected, the achievable ESR of primary user can be given as

$$R_s = \left\{\frac{\left(\rho_T e^{\frac{1}{\rho_S}}E_1\left(\frac{1}{\rho_S}\right) - \rho_S e^{\frac{1}{\rho_T}}E_1\left(\frac{1}{\rho_T}\right)\right)}{\rho_T-\rho_S} - \Theta\right\}^+, \tag{34}$$

where the expression of Θ is

$$\Theta = e^{\frac{1}{\rho_T}} \int_0^\infty \frac{\rho_T \rho_S \left(1 + e^{\frac{1}{\rho_S}+\frac{1}{\rho_T x}} E_1\left(\frac{1}{\rho_S}+\frac{1}{\rho_T x}\right)\right) F_U(x)}{(\rho_T x + \rho_S)^2} dx - e^{\frac{1}{\rho_T}} \int_0^\infty \frac{\left(e^{\frac{1}{\rho_S}+\frac{1}{\rho_T x}} E_1\left(\frac{1}{\rho_S}+\frac{1}{\rho_T x}\right)\right) F_U(x)}{x(\rho_T x + \rho_S)} dx - e^{\frac{1}{\rho_T}} \int_0^\infty \frac{\rho_T \rho_S \log(1+x) F_U(x)}{(\rho_T x + \rho_S)^2} dx. \quad (35)$$

Proof: Please see Appendix B. ■

Using the result in Theorem 4, the secrecy performance of the maximal interference rate based scheme can be investigated numerically. However, it cannot offer insight to the secrecy gain of secondary user selection. Similar to Section-III, we assume that both ρ_T and ρ_S are sufficiently large. Under such an assumption, we also give an asymptotic analysis of ESR for the proposed scheme in the high SNR regime.

C. ASYMPTOTIC ANALYSIS IN THE HIGH SNR REGIME

We further assume that there is a fixed ratio $\beta = \frac{\rho_T}{\rho_S}$ and it holds $\beta > 1$. When ρ_T is large enough, the achievable rate at R is approximated as

$$\mathbb{E}[C_{R,s}] \approx \log \rho_T - \gamma. \quad (36)$$

In the high SNR regime, the achievable rate at the eavesdropper can be approximated as

$$C_{E,s} \approx \begin{cases} \log\left(\rho_T |h_{TE}|^2\right), & \frac{|h_{S_\# R}|^2}{|h_{TR}|^2} \le \frac{|h_{S_\# E}|^2}{|h_{TE}|^2}, \\ \log\left(1 + \beta \frac{|h_{TE}|^2}{|h_{S_\# E}|^2}\right), & \frac{|h_{S_\# R}|^2}{|h_{TR}|^2} > \frac{|h_{S_\# E}|^2}{|h_{TE}|^2}. \end{cases} \quad (37)$$

Let $U = \frac{|h_{S_\# R}|^2}{|h_{TR}|^2}$, its CDF is

$$F'_U(u) = 1 + \sum_{n=1}^{N} (-1)^n C_N^n \frac{1}{1+nu}. \quad (38)$$

Similar to Appendix B, we let $V = |h_{S_\# E}|^2$ and $T = |h_{TE}|^2$. Then, the expression of $\mathbb{E}[C_{E,s}]$ is approximated as

$$\mathbb{E}[C_{E,s}] \approx \int_0^{\frac{v}{t}} dF'_U(u) \int_0^\infty \int_0^\infty \log(\rho_T t) e^{-t} e^{-v} dt dv + \int_{\frac{v}{t}}^\infty dF'_U(u) \int_0^\infty \int_0^\infty \log\left(1 + \beta \frac{t}{v}\right) e^{-t} e^{-v} dt dv$$

$$= \int_0^\infty \int_0^\infty \log\left(1 + \beta \frac{t}{v}\right) e^{-t} e^{-v} dt dv + \int_0^\infty \int_0^\infty F'_U\left(\frac{v}{t}\right) \log \frac{\rho_T t}{1 + \beta \frac{t}{v}} e^{-t} e^{-v} dt dv$$

$$\overset{(a)}{=} -1 + \sum_{n=0}^{N} (-1)^n C_N^n \int_0^\infty \frac{\log \rho_T - \gamma + 1}{(1+x)^2(1+nx)} dx + \sum_{n=1}^{N} (-1)^n C_N^n \int_0^\infty \frac{\log \frac{x}{(1+x)(\beta+x)}}{(1+x)^2(1+nx)} dx, \quad (39)$$

where step (a) changes the integral variables $\frac{v}{t+1}$ and v to x and y, respectively. The proof of obtaining a closed-form expression of $\mathbb{E}[C_{E,s}]$ is shown in Appendix C. After some mathematical manipulations, we have the following theorem.

Theorem 5: In the high SNR regime, when a secondary user with strongest interference channel is selected, the achievable ESR of primary user can be approximated as

$$R_s = \left\{R_{s,1} - R_{s,2}\right\}^+, \quad (40)$$

where $R_{s,1}$ and $R_{s,2}$ are shown at bottom of this page. In Eqn. (42), $\text{dilog}(x) = \int_1^x \frac{\log t}{1-t} dt$ represents the dilogarithm function.

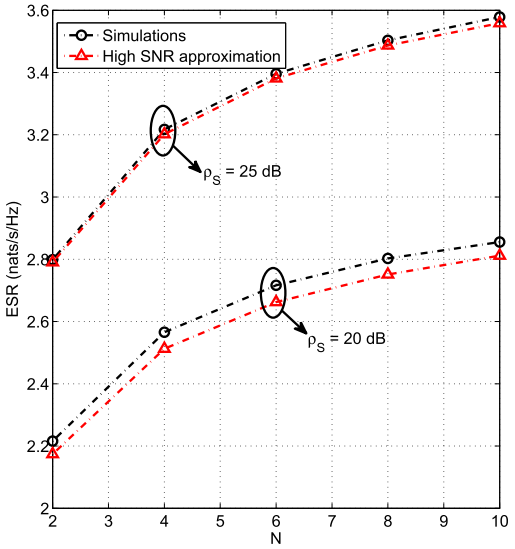


FIGURE 5. ESR vs. the number of the secondary users in the high SNR regime.

Fig. 5 plots the asymptotic results given in Theorem 5. We set the transmit power P_T as $\rho_T = 30$ dB. As can be

$$R_{s,1} = (\log \rho_T - \gamma + 1)\left(\frac{N}{2} - \sum_{n=2}^{N} (-1)^n C_N^n \frac{n(\log n - 1) + 1}{(n-1)^2}\right), \quad (41)$$

$$R_{s,2} = \sum_{n=2}^{N} (-1)^n C_N^n \left(\frac{n}{(n-1)^2}\left(\text{dilog}\left(\frac{1}{\beta}\right) - \text{dilog}\left(\frac{1}{n}\right) - \text{dilog}\left(\frac{1}{n\beta}\right) - \frac{\log^2 n}{2}\right) + \frac{\beta + \beta \log \beta - 1}{(n-1)(\beta-1)}\right) - N\left(\frac{\log \beta - \beta + 1}{2(\beta-1)^2} - \frac{\log \beta}{2} - \frac{3}{4}\right). \quad (42)$$

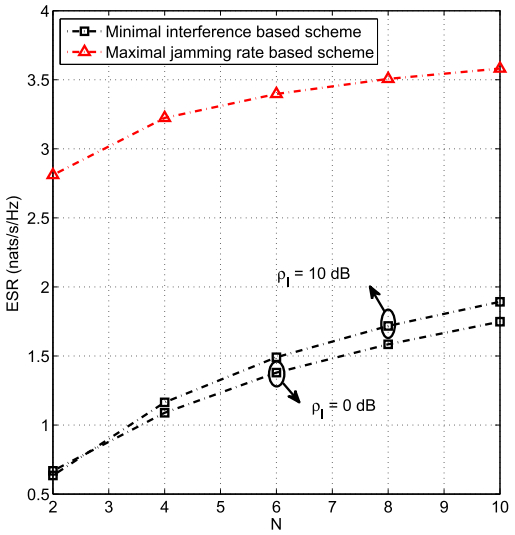


FIGURE 6. Comparisons of ESR in the high SNR regime.

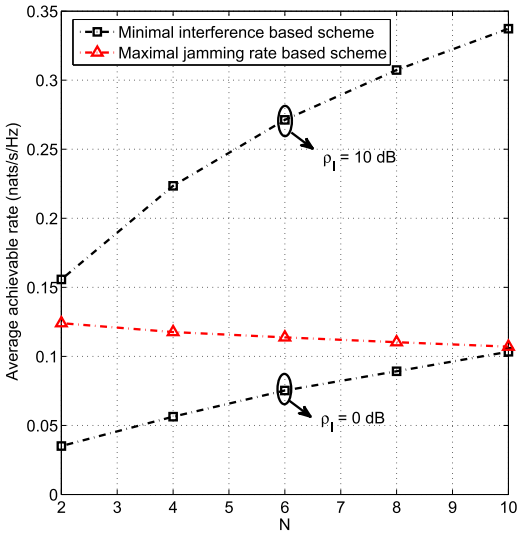


FIGURE 7. Comparisons of achievable rate at the secondary receiver in the high SNR regime.

seen, all the asymptotic results agree well with the simulation results. As expected, ESR grows with N, implying that the proposed scheme can merit the benefit of multiuser secrecy gain. Besides, one can note that as ρ_S gets large, the achievable ESR also becomes large.

V. SIMULATION RESULTS

In this section, we further give comparisons of the secrecy performance for the two proposed schemes. Monte Carlo experiments each with 10000 independent trials is performed to obtain the numerical results.

Fig. 6 gives a comparison of secrecy performance between the two proposed schemes. As can be seen from Fig. 6, the both scheme can achieve secrecy gain via secondary user selection. Although increasing ρ_I improves the secrecy rate, the minimal interference based scheme has a much lower secrecy rate than the maximal jamming rate based scheme for all the cases. Hence, the maximal jamming rate scheme is a better choice from the perspective of enhancing primary user's security at the cost of lowing achievable rate of the secondary receiver.

Fig. 7 provides a comparison of the achievable average rate at the secondary receiver between the two proposed secondary user selection schemes. Note that the secondary receiver also gains benefit of user selection and achieves a higher rate as I becomes larger for the minimal interference based scheme. In contrast, it achieves a lower rate as N gets larger for the maximal jamming rate based scheme. Nonetheless, the minimal interference based scheme does not achieves better performance than the maximal jamming rate based scheme for all the cases. To sum up, the maximal jamming rate based scheme is a good choice which can improve the primary user's security greatly while guaranteeing that the cooperative secondary user achieves an acceptable rate.

VI. CONCLUSIONS

In this paper, we propose two secondary user selection schemes, named minimal interference based scheme and maximal jamming rate based scheme, to enhance the security of the primary user. We give a comprehensive analysis of the multiuser gain in secure cognitive communications. For the minimal interference based scheme, a closed-form lower bound of the achieve ESR is derived and the impact of I, P_S on the secrecy performance of the primary users is well investigated. In the high SNR regime, we find that the multiuser gain scales like $\log N$ for a fixed interference temperature. For the the maximal jamming rate based scheme, we also provides this scheme a closed-form expression of the achievable ESR and show that it significantly enhances the security of primary user. Our results indicate that the multiuser gain is crucial for the secrecy performance of the primary user, and the maximal jamming rate based scheme is a better choice for secure communications in underlay cognitive radio networks.

APPENDIX A
PROOF OF THEOREM 1

Recalling that the ESR expression is $R_s = \left\{\mathbb{E}[C_R] - \mathbb{E}[C_E]\right\}^+$. We first calculate the item $\mathbb{E}[C_R]$. Let $X \triangleq |h_{S_*R}|^2$ and $Y \triangleq |h_{TR}|^2$. It is widely accepted that X and Y are exponentially distributed variables with mean $1/N$ and 1, respectively. Then we have

$$\begin{aligned}\mathbb{E}[C_R] &= \int_0^{\frac{\rho_I}{\rho_S}}\int_0^{\infty} \log\Big(1+\frac{\rho_T y}{\rho_S x+1}\Big)e^{-y}Ne^{-Nx}dydx \\ &\quad + \int_{\frac{\rho_I}{\rho_S}}^{\infty}\int_0^{\infty} \log\Big(1+\frac{\rho_T y}{\rho_I+1}\Big)e^{-y}Ne^{-Nx}dydx \\ &= \underbrace{e^{\frac{1}{\rho_T}}\int_0^{\frac{\rho_I}{\rho_S}} E_1\Big(\frac{\rho_S x+1}{\rho_T}\Big)Ne^{-\left(N-\frac{\rho_S}{\rho_T}\right)x}dx}_{\Psi} \\ &\quad + e^{-\frac{N\rho_I}{\rho_S}+\frac{\rho_I+1}{\rho_T}}E_1\Big(\frac{\rho_I+1}{\rho_T}\Big), \end{aligned} \tag{43}$$

where $E_1(x) = \int_x^\infty \frac{e^{-t}}{t} dt$ is the zero-th incomplete gamma function. Note that we have assumed $P_T > P_S$, thus $N - \frac{\rho_S}{\rho_T} > 0$. Then the calculation of Ψ can be further given as

$$\begin{aligned}\Psi &\overset{(a)}{=} \frac{N\rho_T e^{\frac{N}{\rho_S}}}{\rho_S} \int_{\frac{1}{\rho_T}}^{\frac{\rho_I+1}{\rho_T}} E_1(x) e^{-\frac{N\rho_T-\rho_S}{\rho_S}x} dx \\ &\overset{(b)}{=} \frac{N\rho_T e^{\frac{N}{\rho_S}}}{N\rho_T-\rho_S}\Big(e^{-\frac{N\rho_T-\rho_S}{\rho_T\rho_S}} E_1\Big(\frac{1}{\rho_T}\Big) - e^{-\frac{(N\rho_T-\rho_S)(\rho_I+1)}{\rho_T\rho_S}} \\ &\quad \times E_1\Big(\frac{\rho_I+1}{\rho_T}\Big) - \int_{\frac{1}{\rho_T}}^{\frac{\rho_I+1}{\rho_T}} \frac{e^{-\frac{N\rho_T}{\rho_S}x}}{x} dx\Big) \\ &\overset{(c)}{=} \frac{N\rho_T e^{\frac{N}{\rho_S}}}{N\rho_T-\rho_S}\Big(e^{-\frac{N\rho_T-\rho_S}{\rho_T\rho_S}} E_1\Big(\frac{1}{\rho_T}\Big) - e^{-\frac{(N\rho_T-\rho_S)(\rho_I+1)}{\rho_T\rho_S}} \\ &\quad \times E_1\Big(\frac{\rho_I+1}{\rho_T}\Big) + E_1\Big(\frac{N(\rho_I+1)}{\rho_S}\Big) - E_1\Big(\frac{N}{\rho_S}\Big)\Big), \quad (44)\end{aligned}$$

where step (a) makes a change of integral variable, step (b) follows from integral by parts, and step (c) is derived by using the definition of $E_1(x)$. Substituting the result in (44) into (43), a closed-form expression of $\mathbb{E}[C_R]$ is obtained.

We now turn to obtain the expression of $\mathbb{E}[C_E]$. Let $T \triangleq |h_{TE}|^2$ and $Z \triangleq |h_{S_*E}|^2$. According to the channel model, T and Z are exponentially distributed variables with mean 1. Then $\mathbb{E}[C_E]$ can be given as

$$\mathbb{E}[C_E] = \Omega_1 + \Omega_2, \quad (45)$$

where

$$\begin{aligned}\Omega_1 &\triangleq \int_0^{\frac{\rho_I}{\rho_S}} \int_0^\infty \int_0^\infty \log\Big(1 + \frac{\rho_T t}{\rho_S z + 1}\Big) e^{-t} e^{-z} N e^{-Nx} dt dz dx, \\ \Omega_2 &\triangleq \int_{\frac{\rho_I}{\rho_S}}^\infty \int_0^\infty \int_0^\infty \log\Big(1 + \frac{\rho_T t}{\frac{\rho_I}{x} z + 1}\Big) e^{-t} e^{-z} N e^{-Nx} dt dz dx.\end{aligned}$$

The first item in the right-hand-side of (45), denoted by Ω_1, can be further given as

$$\begin{aligned}\Omega_1 &= \Big(1 - e^{-\frac{N\rho_I}{\rho_S}}\Big) \int_0^\infty \int_0^\infty \log\Big(1 + \frac{\rho_T t}{\rho_S z + 1}\Big) e^{-t-z} dt dz \\ &= e^{\frac{1}{\rho_T}} \Big(1 - e^{-\frac{N\rho_I}{\rho_S}}\Big) \int_0^\infty E_1\Big(\frac{\rho_S z + 1}{\rho_T}\Big) e^{-\left(1-\frac{\rho_S}{\rho_R}\right)z} dz \\ &\overset{(a)}{=} \frac{\rho_T\big(1 - e^{-\frac{N\rho_I}{\rho_S}}\big)}{\rho_T - \rho_S}\Big(e^{\frac{1}{\rho_R}} E_1\Big(\frac{1}{\rho_R}\Big) - \int_0^\infty \frac{e^{-z}}{z + \frac{1}{\rho_S}} dz\Big) \\ &\overset{(b)}{=} \frac{\rho_T\big(1 - e^{-\frac{N\rho_I}{\rho_S}}\big)}{\rho_T - \rho_S}\Big(e^{\frac{1}{\rho_T}} E_1\Big(\frac{1}{\rho_T}\Big) - e^{\frac{1}{\rho_S}} E_1\Big(\frac{1}{\rho_S}\Big)\Big), \quad (46)\end{aligned}$$

where step (a) follows from integral by parts, and step (b) is derived by using the definition of $E_1(x)$. The second item in the right-hand-side of (45), denoted by Ω_2, can be further obtained as

$$\Omega_2 = \Omega_{21} - \Omega_{22}, \quad (47)$$

where

$$\begin{aligned}\Omega_{21} &\triangleq \int_{\frac{\rho_I}{\rho_S}}^\infty \int_0^\infty \int_0^\infty \log\big(\rho_I z + x + \rho_T t x\big) \\ &\qquad \times e^{-t} e^{-z} N e^{-Nx} dt dz dx, \\ \Omega_{22} &\triangleq \int_{\frac{\rho_I}{\rho_S}}^\infty \int_0^\infty \log\big(\rho_I z + x\big) e^{-z} N e^{-Nx} dz dx.\end{aligned}$$

Unfortunately, there is no closed-form expression for Ω_{21} in (47). Therefore, we will derive a upper bound for Ω_{21} by using Jensen's and Steffensen's inequality, which is given as

$$\begin{aligned}\Omega_{21} &\overset{(a)}{\le} \int_{\frac{\rho_I}{\rho_S}}^\infty \int_0^\infty \log\big(\rho_I + x + \rho_T t x\big) e^{-t} N e^{-Nx} dt dx \\ &= \int_{\frac{\rho_I}{\rho_S}}^\infty \int_0^\infty \log\Big(1 + \frac{\rho_T t + 1}{\rho_I} x\Big) e^{-t} N e^{-Nx} dt dx \\ &\quad + e^{-\frac{N\rho_I}{\rho_S}} \log\rho_I \\ &\overset{(b)}{\le} \int_0^\infty e^{\frac{N\rho_I}{\rho_T t + 1}} E_1\Big(\frac{N\rho_I}{\rho_T t + 1}\Big) e^{-t} dt + e^{-\frac{N\rho_I}{\rho_S}} \log\rho_I \\ &\overset{(c)}{=} e^{-\frac{N\rho_I}{\rho_S}} \log\rho_I + e^{\frac{1}{\rho_T}} \int_0^\infty e^{\frac{N\rho_I}{\rho_T t}} E_1\Big(\frac{N\rho_I}{\rho_T t}\Big) e^{-t} dt \\ &\quad - e^{\frac{1}{\rho_T}} \int_0^{\frac{1}{\rho_T}} e^{\frac{N\rho_I}{\rho_T t}} E_1\Big(\frac{N\rho_I}{\rho_T t}\Big) e^{-t} dt \\ &\overset{(d)}{\le} e^{-\frac{N\rho_I}{\rho_S}} \log\rho_I + 8 e^{\frac{1}{\rho_T}} \sqrt{\frac{\rho_I}{\rho_T}} \mathcal{S}_{-2,1}\Big(2\sqrt{\frac{\rho_I}{\rho_T}}\Big) \\ &\quad - \big(e^{\frac{1}{\rho_T}} - 1\big) \mathcal{G}_{3,2}^{1,3}\left[\frac{\rho_I\big(1 - e^{-\frac{1}{\rho_T}}\big)}{\rho_T} \middle| \begin{matrix}1, 1, 0 \\ 1, -1\end{matrix}\right], \quad (48)\end{aligned}$$

where step (a) utilizes Jensen's inequality, step (b) holds by changing the lower limit of integral $\frac{\rho_I}{\rho_S}$ to zero, step (c) follows from changing variable $t + 1/\rho_T$ to t, and step (d) uses the results in [36, eqs. (8) and (10)]. $\mathcal{S}_{u,v}(\cdot)$ denotes the Lommel function and $\mathcal{G}$ represents the Meijer-G function [34].

Next we calculate the item Ω_{22}, which can be further expressed as

$$\begin{aligned}\Omega_{22} &= \int_{\frac{\rho_I}{\rho_S}}^\infty \log x N e^{-Nx} dx + \int_{\frac{\rho_I}{\rho_S}}^\infty E_1\big(\frac{x}{\rho_I}\big) N e^{-\left(N - \frac{1}{\rho_I}\right)x} dx \\ &= \log\frac{\rho_I}{\rho_S} e^{-\frac{N\rho_I}{\rho_S}} + E_1\Big(\frac{N\rho_I}{\rho_S}\Big) \\ &\quad + \int_{\frac{\rho_I}{\rho_S}}^\infty E_1\big(\frac{x}{\rho_I}\big) N e^{-\left(N - \frac{1}{\rho_I}\right)x} dx. \quad (49)\end{aligned}$$

Observing Eq. (49), we can find that for a special case $\rho_I = \frac{1}{N}$, the item $e^{-\left(N - \frac{1}{\rho_I}\right)x}$ becomes a constant of 1. Therefore, we need to consider two cases: i) $\rho_I = \frac{1}{N}$ and ii) $\rho_I \neq \frac{1}{N}$, respectively. As $\rho_I = \frac{1}{N}$, we have

$$\begin{aligned}\Omega_{22} &= \log\frac{\rho_I}{\rho_S} e^{-\frac{1}{\rho_S}} + E_1\Big(\frac{1}{\rho_S}\Big) + \int_{\frac{\rho_I}{\rho_S}}^\infty N E_1\big(\frac{x}{\rho_I}\big) dx \\ &= \log\frac{\rho_I}{\rho_S} e^{-\frac{N\rho_I}{\rho_S}} + E_1\Big(\frac{N\rho_I}{\rho_S}\Big) + e^{-\frac{1}{\rho_S}} - \frac{1}{\rho_S} E_1\big(\frac{1}{\rho_S}\big). \quad (50)\end{aligned}$$

As $\rho_I \neq \frac{1}{N}$, we have

$$\Omega_{22} = \log\frac{\rho_I}{\rho_S}e^{-\frac{N\rho_I}{\rho_S}} + E_1\Big(\frac{N\rho_I}{\rho_S}\Big) + \frac{N\rho_I}{N\rho_I - 1}\Big(e^{\frac{1-N\rho_I}{\rho_S}}E_1\big(\frac{1}{\rho_S}\big) - E_1\big(\frac{N\rho_I}{\rho_S}\big)\Big). \quad (51)$$

Based on the above results, we can completed the proof.

APPENDIX B
PROOF OF THEOREM 4

The ESR expression of the proposed scheme is

$$R_s = \Big\{\mathbb{E}\left[C_{R,s}\right] - \mathbb{E}\left[C_{E,s}\right]\Big\}^+. \quad (52)$$

We first calculate the expression of $\mathbb{E}[C_{R,s}]$, which can be easily given as

$$\mathbb{E}[C_{R,s}] = e^{\frac{1}{\rho_T}}E_1\Big(\frac{1}{\rho_T}\Big). \quad (53)$$

Let $V = |h_{S_{\#}E}|^2$ and $T = |h_{TE}|^2$. Both U and T obey exponential distribution with mean 1. Then, the expression of $\mathbb{E}[C_{E,s}]$ can be written as

$$\begin{aligned}
&\mathbb{E}[C_{E,s}] \\
&= \int_0^{\frac{\rho_S v}{\rho_T t+1}} dF_U(u)\int_0^\infty\int_0^\infty \log(1+\rho_T t)e^{-t}e^{-v}dtdv \\
&\quad + \int_{\frac{\rho_S v}{\rho_T t+1}}^\infty dF_U(u)\int_0^\infty\int_0^\infty \log\Big(1+\frac{\rho_T t}{\rho_S v+1}\Big)e^{-t}e^{-v}dtdv \\
&= \int_0^\infty\int_0^\infty \log\Big(1+\frac{\rho_T t}{\rho_S v+1}\Big)e^{-t}e^{-v}dtdv \\
&\quad + \underbrace{\int_0^\infty\int_0^\infty F_U\Big(\frac{\rho_S v}{\rho_T t+1}\Big)\log\frac{1+\rho_T t}{1+\frac{\rho_T t}{\rho_S v+1}}e^{-t}e^{-v}dtdv}_{\Theta} \\
&= \frac{\rho_T}{\rho_T-\rho_S}\Big(e^{\frac{1}{\rho_T}}E_1\big(\frac{1}{\rho_T}\big) - e^{\frac{1}{\rho_S}}E_1\big(\frac{1}{\rho_S}\big)\Big) + \Theta. \quad (54)
\end{aligned}$$

In order to calculate Θ, we take a change of integral variable and define $\frac{\rho_S v}{\rho_T t+1} = x$ as well as $v = y$. The Jacobian matrix is

$$\begin{aligned}
\mathbf{J}(x,y) &= \begin{bmatrix} \frac{\partial t}{\partial x} & \frac{\partial t}{\partial y} \\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial y} \end{bmatrix} \\
&= \begin{bmatrix} -\frac{\rho_S y}{\rho_T x^2} & \frac{\rho_S}{\rho_T x} \\ 0 & 1 \end{bmatrix}. \quad (55)
\end{aligned}$$

The determinant of $\mathbf{J}(x,y)$ is $-\frac{\rho_S y}{\rho_T x^2}$. Then we can further rewrite Θ as

$$\begin{aligned}
\Theta &= \frac{\rho_S e^{\frac{1}{\rho_T}}}{\rho_T}\int_0^\infty\int_0^\infty \frac{yF_u(x)}{x^2}\log\frac{1+\rho_S y}{1+x}e^{-\left(1+\frac{\rho_S}{\rho_T x}\right)y}dxdy \\
&= e^{\frac{1}{\rho_T}}\int_0^\infty \frac{\rho_T\rho_S\Big(1+e^{\frac{1}{\rho_S}+\frac{1}{\rho_T x}}E_1\big(\frac{1}{\rho_S}+\frac{1}{\rho_T x}\big)\Big)F_U(x)}{(\rho_T x+\rho_S)^2}dx \\
&\quad - e^{\frac{1}{\rho_T}}\int_0^\infty \frac{\rho_T\rho_S\log(1+x)F_U(x)}{(\rho_T x+\rho_S)^2}dx \\
&\quad - e^{\frac{1}{\rho_T}}\int_0^\infty \frac{\Big(e^{\frac{1}{\rho_S}+\frac{1}{\rho_T x}}E_1\big(\frac{1}{\rho_S}+\frac{1}{\rho_T x}\big)\Big)F_U(x)}{x(\rho_T x+\rho_S)}dx \quad (56)
\end{aligned}$$

Substituting the results in (53) and (54) into (52), we can complete the result.

APPENDIX C

To obtain a closed-form expression of $\mathbb{E}[C_{E,s}]$, we need to calculate the following integrals

$$\Delta_1 = \int_0^\infty \frac{\log\rho_T - \gamma + 1}{(1+x)^2(1+nx)}dx, \quad n = 0, 1, \cdots, N, \quad (57)$$

$$\Delta_2 = \int_0^\infty \frac{\log\frac{x}{(1+x)(\beta+x)}}{(1+x)^2(1+nx)}dx, \quad n = 1, \cdots, N. \quad (58)$$

We first calculate the item Δ_1. There are three cases to consider, which are $n = 0$, $n = 1$ and $n \geq 2$. As $n = 0$ and $n = 1$, we can readily have

$$\begin{aligned}
\Delta_1 &= \int_0^\infty \frac{\log\rho_T - \gamma + 1}{(1+x)^2}dx \\
&= \log\rho_T - \gamma + 1, \quad n = 0, \quad (59) \\
\Delta_1 &= \int_0^\infty \frac{\log\rho_T - \gamma + 1}{(1+x)^3}dx \\
&= \frac{1}{2}(\log\rho_T - \gamma + 1), \quad n = 1. \quad (60)
\end{aligned}$$

As $n \geq 2$, we have

$$\begin{aligned}
\Delta_1 &= \int_0^\infty \frac{\log\rho_T - \gamma + 1}{(1+x)^2(1+nx)}dx \\
&= \frac{\log\rho_T - \gamma + 1}{n-1}\int_0^\infty\Big(\frac{1}{(1+x)(\frac{1}{n}+x)} - \frac{1}{(1+x)^2}\Big)dx \\
&= (\log\rho_T - \gamma + 1)\frac{n(\log n - 1) + 1}{(n-1)^2}, \quad n \geq 2. \quad (61)
\end{aligned}$$

Next we calculate the item Δ_2. There are two cases to consider, which are $n = 1$ and $n \geq 2$. As $n = 1$, it yields

$$\begin{aligned}
\Delta_2 &= \int_0^\infty \frac{\log x - \log(1+x) - \log(\beta+x)}{(1+x)^3}dx \\
&= \frac{\log\beta - \beta + 1}{2(\beta-1)^2} - \frac{\log\beta}{2} - \frac{3}{4}. \quad (62)
\end{aligned}$$

As $n \geq 2$, we further have

$$\begin{aligned}
\Delta_2 &= \int_0^\infty \frac{\log\frac{x}{(1+x)(\beta+x)}}{n-1}\Big(\frac{1}{(1+x)(\frac{1}{n}+x)} - \frac{1}{(1+x)^2}\Big)dx \\
&= \frac{1}{n-1}\int_0^\infty \frac{\log x - \log(1+x) - \log(\beta+x)}{(1+x)(\frac{1}{n}+x)}dx \\
&\quad + \frac{\beta + \beta\log\beta - 1}{(n-1)(\beta-1)}, \quad n \geq 2. \quad (63)
\end{aligned}$$

Using the result in [34, eq. (4.232.2)], the item $\int_0^\infty \frac{\log x}{(1+x)(\frac{1}{n}+x)}dx$ in (63) can be calculated as

$$\int_0^\infty \frac{\log x}{(1+x)(\frac{1}{n}+x)}dx = -\frac{n\log^2 n}{2(n-1)}, \quad n \geq 2. \quad (64)$$

Changing the integral variable $x+1$ to x, the item $\int_0^\infty \frac{\log 1+x}{(1+x)(\frac{1}{n}+x)}dx$ in (63) is rewritten as

$$\begin{aligned}\int_0^\infty \frac{\log 1+x}{(1+x)(\frac{1}{n}+x)}dx &= \int_1^\infty \frac{\log x}{x\big(x-(1-\frac{1}{n})\big)}dx \\ &= -\int_0^1 \frac{\log t}{1-(1-\frac{1}{n})t}dt \\ &= \frac{n}{n-1}\,\mathrm{dilog}\left(\frac{1}{n}\right), \quad n\geq 2. \end{aligned} \tag{65}$$

Similarly, the item $\int_0^\infty \frac{\log \beta+x}{(1+x)(\frac{1}{n}+x)}dx$ in (63) is given as

$$\begin{aligned}&\int_0^\infty \frac{\log \beta+x}{(1+x)(\frac{1}{n}+x)}dx \\ &= \frac{n}{n-1}\Big(\log n\log\beta+\mathrm{dilog}\left(\frac{1}{\beta n}\right)-\mathrm{dilog}\left(\frac{1}{\beta}\right)\Big), \quad n\geq 2. \end{aligned} \tag{66}$$

With the above results, a closed-form expression of $\mathbb{E}[C_{E,s}]$ is presented.

REFERENCES

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[2] L. Lv, J. Chen, and Q. Ni, "Cooperative non-orthogonal multiple access in cognitive radio," *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2059–2062, Oct. 2016.

[3] X. Kang, Y. C. Liang, A. Nallanathan, H. K. Garg, and R. Zhang, "Optimal power allocation for fading channels in cognitive radio networks: Ergodic capacity and outage capacity," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 940–950, Feb. 2009.

[4] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May/Jun. 2013.

[5] V.-D. Nguyen, T. M. Hoang, and O.-S. Shin, "Secrecy capacity of the primary system in a cognitive radio network," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3834–3843, Aug. 2015.

[6] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.

[7] 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. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[8] 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.

[9] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: Low complexity design," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 2192–2198, May 2015.

[10] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[11] S.-H. Tsai and H. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.

[12] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[13] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614–6623, Oct. 2016.

[14] J. S. Hu, F. Shu, and J. Li, "Robust synthesis method for secure directional modulation with imperfect direction angle," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1084–1087, Jun. 2016.

[15] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.

[16] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, Nov. 2013.

[17] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

[18] D. Xu and Q. Li, "Resource allocation for cognitive radio with primary user secrecy outage constraint," *IEEE Syst. J.*, vol. 12, no. 1, pp. 893–904, Mar. 2018.

[19] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

[20] V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2609–2623, Nov. 2016.

[21] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[22] L. Yang, H. Jiang, S. A. Vorobyov, J. Chen, and H. Zhang, "Secure communications in underlay cognitive radio networks: User scheduling and performance analysis," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1191–1194, Jun. 2016.

[23] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[24] Z. Ding *et al.*, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016.

[25] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[26] H. Deng, H.-M. Wang, W. Wang, and M. H. Lee, "Dual user selection for security enhancement in uplink multiuser systems," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1900–1903, Sep. 2016.

[27] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

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

[29] H. Deng, H.-M. Wang, J. Yuan, W. Wang, and Q. Yin, "Secure communication in uplink transmissions: User selection and multiuser secrecy gain," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3492–3506, Aug. 2016.

[30] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Dual antenna selection in secure cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7993–8002, Oct. 2016.

[31] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

[32] T. W. Ban, W. Choi, B. C. Jung, and D. K. Sung, "Multi-user diversity in a spectrum sharing system," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 102–106, Jan. 2009.

[33] J.-P. Hong, B. Hong, T. Ban, and W. Choi, "On the cooperative diversity gain in underlay cognitive radio systems," *IEEE Trans. Commun.*, vol. 60, no. 1, pp. 209–219, Jan. 2012.

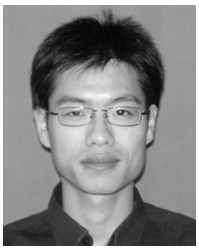
[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 1994.

[35] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*. New York, NY, USA: Dover, 1970.

[36] O. Waqar, M. Ghogho, and D. McLernon, "Tight bounds for ergodic capacity of dual-hop fixed-gain relay networks under Rayleigh fading," *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 413–415, Apr. 2011.

MIAN QIN received the B.S. degree in communication engineering from Wuhan University, China, in 2003. She is currently pursuing the Ph.D. degree in information and communication system with Zhengzhou University, Zhengzhou, China. Her research interests include wireless communications for the next generation, cognitive radio, the key technology of green wireless network, and optimal resource allocation.

SHOUYI YANG received the B.S. degree from Nankai University in 1983, the M.E. degree from Chongqing University in 1990, and the Ph.D. degree from the Beijing Institute of Technology in 2003. From 2003 to 2004, he was a Visiting Researcher with Mie University, Mie, Japan. He is currently a Full Professor with the School of Information Engineering, Zhengzhou University, Zhengzhou, China. His research interests include the broadband wireless communication and cognitive radio technology.



HAO DENG received the Ph.D. degree in information and communication engineering from Xi'an Jiaotong University in 2016. He is currently a Lecturer with the School of Physics and Electronics, Henan University, Kaifeng, China. His research interests include physical-layer security of wireless communications and heterogeneous cellular networks.

MOON HO LEE (S'81–M'85–SM'86–LSM'15) received the Ph.D. degrees in electrical engineering from Chonnam National University, South Korea, in 1984, and from The University of Tokyo, Japan, in 1990. He was the Chief Engineer with Namyang MBC broadcasting from 1970 to 1980. He held a post-doctoral position with the University of Minnesota, Minneapolis, MN, USA, from 1985 to 1986. He was the Chair of the Department of Electronics Engineering, Chonbuk National University, South Korea, where he is currently a Professor. He holds 116 patents. He has made significant original contributions in the areas of mobile communication code design, channel coding, and multidimensional source, and channel coding. He is a member of the National Academy of Engineering, South Korea, and a Foreign Fellow of the Bulgarian Academy of Sciences. He is the Inventor of Jacket Matrix and it in Wikipedia was cited over 95 559 times in 2014.