Physical Layer Security in Underlay CCRNs with Fixed Transmit Power

Songqing Wang[1,2], Xiaoming Xu[1] and Weiwei Yang[1]
[1] PLA University of Science and Technology
Nanjing, 210014 - CHINA
[e-mail: wwyang1981@163.com]
[2] Jinling Hospital, Nanjing University School of Medicine
Nanjing, 210002 - CHINA
[e-mail: songqingwang@126.com]
*Corresponding author: Weiwei Yang

Received July 15, 2014; revised November 10, 201X; accepted November 20, 201X; published December 25, 201X

Abstract

In this paper, we investigate physical layer security for multiple decode-and-forward (DF) relaying underlay cognitive radio networks (CRNs) with fixed transmit power at the secondary network against passive eavesdropping attacks. We propose a simple relay selection scheme to improve wireless transmission security based on the instantaneous channel information of all legitimate users and the statistical information about the eavesdropper channels. The closed-form expressions of the probability of non-zero secrecy capacity and the secrecy outage probability (SOP) are derived over independent and non-identically distributed Rayleigh fading environments. Furthermore, we conduct the asymptotic analysis to evaluate the secrecy diversity order performance and prove that full diversity is achieved by using the proposed relay selection. Finally, numerical results are presented to verify the theoretical analysis and depict that primary interference constrain has a significant impact on the secure performance and a proper transmit power for the second transmitters is preferred to be energy-efficient and improve the secure performance.

Keywords: Cooperative cognitive radio networks, fixed transmit power, physical layer security, relay selection, secrecy outage probability

This research was supported by the National Natural Science Foundation of China (No. 61371122 and No. 61471393) and the China Postdoctoral Science Foundation under a Special Financial Grant (No. 2013T60912).

http://dx.doi.org/10.3837/tiis.2015.01.015 **ISSN : 1976-7277**

1. Introduction

Cognitive radio (CR) has emerged as a promising solution to optimize spectrum resources exploitation [1] [2]. The improvement is achieved by allowing the secondary users (SUs) to exploit the originally spectrum of the licensed primary users (PUs). One of the cognitive modes defining this coexistence between PUs and SUs is the “underlay” approach. In which, the SUs and PUs can exist in the same frequency band simultaneously as long as the SUs strictly satisfies the interference constraint at the primary receiver. To fulfill this constraint limit, SUs generally use relatively low transmit power which eventually limits the reliable and coverage performance of the secondary system.

In order to enhance the performance of secondary systems, cooperative relaying, as a way to achieve the space diversity, has been further exploited in cognitive ratio networks (CRNs). The performance of decode-and-forward (DF) and amplify-and-forward (AF) relaying in underlay cooperative CRNs (CCRNs) has been widely investigated in [3-9]. Different from the non-cooperative CRNs, both the SUs and the relays should maintain the interference constraint to fulfill the requirement of PUs in underlay CCRNs. In general, there are two transmit power control strategies to keep the induced interference always below a given allowable threshold [10]. One is adaptive transmit power (ATP) control, by which the secondary transmitters can adjust their transmit power to satisfy the interference constraint. The other is fixed transmit power (FTP) control, by which the secondary transmitters use their maximum available power when the primary interference constraint is verified, and remain silent otherwise. Although the use of FTP slightly deteriorates the system performance, it significantly alleviates the signaling requirements and implement complexity compared to ATP [10].

On the other hand, due to the broadcasting nature of wireless channel and the openness of cognitive radio architecture, security against overhearing of the eavesdroppers is one of the important issues [11]. Traditionally, the cryptographic techniques relying on secret keys have been employed to protect the communication confidentiality against eavesdropping attacks, however, which increases the computational and communication overheads and introduces additional system complexity for the secret key distribution and management [12]. Recently, physical layer security (PLS) is drawing a lot of attentions as a promising technique to achieve secure communication by exploiting the physical characteristics of wireless channels [13].

More recently, PLS has been considered for underlay CRNs in [14-21]. Different from non-cognitive wireless networks, there are some unique challenges to be addressed for physical layer security in cognitive radio networks, e.g., the PU’s QoS protection issue and the mitigation of mutual interference between PUs and SUs. The first attempt to address the secure transmission for underlay CRNs from the information theoretic perspective has been made in [14] - [16]. In [17], Zou *et al.* investigate the multiuser scheduling issues in CRNs for physical layer security transmission against eavesdropping attacks. Secure resource allocation problems for underlay CRNs are investigated in [18]. The authors in [19] indicated that user cooperation not only improves the reliability and coverage performance of cognitive radio networks, but also has great potential to enhance physical layer security against eavesdropping [19]. In [20], the authors introduce cooperative secure resource allocation to maximize the secondary secrecy rate subject to maintaining a certain level quality of service for PUs via the interference threshed constraint. In [21], the secure transmission issue for a cognitive radio network has investigated over the slow fading channel, which aims to maximize the secrecy throughput of the primary transmission. Recently, the authors attempt to enhance wireless transmission security in underlay CCRNs by relay selection in [22], where the secondary source sends confidential information to a secondary destination with the assist of multiple DF relays, and the adaptive transmit power (ATP) control strategy is used to fulfill the interference power constraints. The proposed relay selection scheme in [22] selects a trusted relay to assist the secondary transmitter and maximize the achievable secrecy rate under the availability of perfect channel state information (CSI) of all channels. However, it is often difficult or impossible for the transmitter to know the accuracy of the eavesdropper's channel, especially for the passive eavesdropping scenario.

Moreover, in underlay CCRNs, PUs and SUs can transmit signals simultaneously by sharing the same spectrum recourses. As a result, the relays and secondary destination inevitable suffer interference from PUs, which comes in the form of co-channel interference (CCI). However, most of previous work have not taken the interference from PUs into consideration or just have translated PUs' interference into the noise term of SUs.

Motivated by the above discussions, in this paper, we investigate physical layer security in underlay CCRNs consisting of one primary transmitter, one primary receiver, one secondary source, multiple secondary relays, and one secondary destination, where one eavesdropper are ready to intercept the transmissions from the secondary relays to the secondary destination. The FTP strategy is adopted at the secondary transmitters, including the secondary source and multiple secondary relays, which significantly depress signal burden and implement complexity. As compared with the existing works, the main contributions of this paper are exhibited as follows:

1) To the best of author's knowledge, this paper is the first attempt to investigate physical layer security for underlay CCRNs employing FTP control strategy under passive eavesdropping attacks. Furthermore, different from previous works, the impact of PU's interference on the relays and secondary destination also is considered.

2) Different from [22], we propose a new relay selection scheme in underlay CCRNs to achieving trade-off between complexity and secure performance, where a secondary relay that satisfies the primary interference constraint and successfully decodes the source message will be selected based on the instantaneous knowledge of all legitimate links and the statistical knowledge of the eavesdropper channels. Thus, our proposed relay selection scheme does not require the estimation of the instantaneous eavesdropper link and thus seems to be an efficient solution with practical interest.

3) We derive the closed-form expressions for the probability of non-zero secrecy capacity and the secrecy outage probability (SOP) over independent and non-identically distributed Rayleigh channels. Moreover, we also conduct the asymptotic analysis for the SOP to provide insights on the impact of some critical parameters, such as the transmit power of the secondary users, the interference constraint, and the number of relays, on the secrecy diversity order performance. Simulation results verify the theoretical analysis, and illustrate that the secure diversity order is same as the number of secondary relays which depicts the fact that full secure diversity is achieved by the proposed relay selection scheme.

4) Furthermore, simulation and theoretical results show that, due to FTP strategy and interference constraint considered, the secure performance in underlay CCRNs is not a monotonically decreasing/increasing function of the transmit signal-to-noise ratio (SNR) anymore. After the SNR approaches a certain level, further increasing SNR may sharply degrade the secrecy performance. Therefore, a proper transmit SNR for secondary transmitter is preferred to be energy-efficient and improve the secure performance.

5) In addition, the interference constraint significantly affects the relay selection process. A strict interference constraint will drop the secondary relays from the active set and thereby reduce the secure performance. As the interference constraint approach infinity, the secure performance is limited by the second hop, and then converges to constant values as the performance floors.

Throughout this paper, the following notations will be used. The channel fading gain of link $x \to y$ is denoted by $\left|h_{xy}\right|^2$, with mean of δ_{xy}^2, $x \in \{s, r_1, \cdots, r_M, u\}$ and $y \in \{r_1, \cdots, r_M, d, e, v\}$. E_x is the transmit power of node x and N_0 is variance of the zero-mean additive white Gaussian (AWGN) at each node. $\gamma_{xy} = E_x \left|h_{xy}\right|^2 / N_0$ and $\bar{\gamma}_{xy}$ stand for the instantaneous SNR and the average SNR of link $x \to y$, respectively. $f_X(\cdot)$ and $F_X(\cdot)$ represent the probability density function (PDF) and the cumulative distribution function (CDF) of random variable (RV) X, respectively.

2. System Model and Relay Selection Scheme

2.1 System Model

We consider a secrecy communication scenario in underlay CCRNs shown as **Fig. 1**. In the primary network, a primary source u sends data to a primary destination v. In the secondary network, a secondary source s sends confidential information to a secondary destination d by employing the assistance of M secondary relays ($r_i, i = 1, 2, \cdots, M$). An eavesdropper e is located around the secondary destination overhearing the transmission from the relays. All the nodes are equipped with single antenna and work in the half-duplexing mode. For notational convenience, M relays are denoted by $\mathrm{R} = \{r_i \mid i = 1, 2, \cdots, M\}$, where the DF relay protocol is employed. Different from [23] and [24], we assume that the direct links from s to d and e are not available, e.g., d and e both are out of the coverage area, which avoids considering the two-hop leakages and simplifies the system model. At each secondary transmitter, including s and $r_i, i = 1, 2, \cdots, M$, the FTP strategy [10] is adapted instead of ATP control to depress the system complexity. Each link in the underlay CCRN is subjected to an AWGN with zero mean and variance N_0. More specially, the mutual interference exists between primary and cognitive transmissions in underlay CCRNs.

The channels between nodes $x \in \{s, r_1, \cdots, r_M, u\}$ and $y \in \{r_1, \cdots, r_M, d, e, v\}$ are modeled as independent and non-identically distributed Rayleigh fading random variable. Thus, the channel fading gains, denoted by $\left|h_{xy}\right|^2$, are independent and exponential random variables with means of δ_{xy}^2.

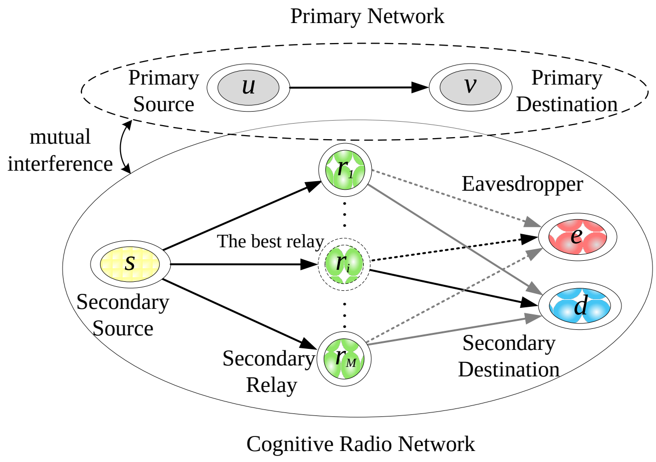

Fig. 1. System model

The interference level at primary destination caused by the secondary transmitters (source and relays) must be below an interference constraint, noted I_0 . Using a FTP E_x ($x \in \{s, r_1, \cdots, r_M\}$), the interference caused by a secondary transmitter x (s or r_i), noted I_x is written as $\mathrm{I}_x = E_x |h_{xv}|^2$. Without loss of generality, we assume that all relays have the same transmit power, e. g., $E_{r_i} = E_r, \forall r_i \in \mathrm{R}$. Thereby, each secondary transmitter may be activated with the probability of $P_{x,\mathrm{I}_0} = \Pr(\mathrm{I}_x < \mathrm{I}_0)$, otherwise, keep silent with the probability of $\bar{P}_{x,\mathrm{I}_0} = 1 - \Pr(\mathrm{I}_x < \mathrm{I}_0)$. It is implied that the whole transmission starts only if s satisfies the interference constraint with the probability of P_{s,I_0} . Meanwhile, some secondary relays in R fall short of the interference constraint and thus they remain silent. The other relays, which meet the interference constraint, are activated and compose a new set A . Given M relays in secondary network, there are 2^M possible combinations from the full set R . Thus, the active relay set is given by

$$\mathrm{A} \in \{\phi, \mathrm{A}_1, \mathrm{A}_2, \cdots, \mathrm{A}_m, \cdots, \mathrm{A}_{2^M - 1}\} \tag{1}$$

where ϕ represents the empty set, while A_m is a non-empty subset from R . If the active set A is empty, the confidential message is unable to reach the destination.

The scenario of $\mathrm{A} = \phi$ is described as

$$E_r |h_{r_i v}|^2 > \mathrm{I}_0, \quad \forall r_i \in \mathrm{R} \tag{2}$$

Similarly, the event $\mathrm{A} = \mathrm{A}_m$ is formulated as

$$\begin{aligned} &E_r |h_{r_i v}|^2 < \mathrm{I}_0, \quad r_i \in \mathrm{A}_m \\ &E_r |h_{r_j v}|^2 > \mathrm{I}_0, \quad r_j \in \mathrm{R}/\mathrm{A}_m \end{aligned} \tag{3}$$

Given a non-empty A_m , the relays in this set will try to decode its received signal. When s broadcasts it's confidential message, the relays in A_m receive both the useful data from s and the interference from u . The instantaneous channel capacity of $s \rightarrow r_i$ link can be given by

$$C_{sr_i} = \frac{1}{2}\log_2\left(1+\frac{\gamma_{sr_i}}{1+\gamma_{ur_i}}\right) \tag{4}$$

where $\gamma_{sr_i} = E_s\left|h_{sr_i}\right|^2 \big/ N_0$, $\gamma_{ur_i} = E_u\left|h_{ur_i}\right|^2 \big/ N_0$, E_u is the transmission power at the primary transmitter. The capacity is halved because two time slots are required for completing the whole transmission.

When the capacity is large than a predetermined transmission rate threshold R_S , i.e., $C_{sr_i} > R_S$, r_i is able to decode x successfully. Those relays that successfully decode the secondary source signal are represented as the decoding set D . Given an active set A_m with the cardinality of $|\mathrm{A}_m|$, the decoding set is given by

$$\mathrm{D} \in \left\{\phi, \mathrm{D}_1, \mathrm{D}_2, \cdots, \mathrm{D}_n, \cdots, \mathrm{D}_{2^{|\mathrm{A}_m|}-1}\right\} \tag{5}$$

If the decoding set D is empty, the confidential message is also unable to reach the destination and the transmission outage occurs; otherwise a best relay will be chosen to forward the decoded signal. The scenario of $\mathrm{D} = \phi$ is described as

$$\frac{1}{2}\log_2\left(1+\frac{\gamma_{sr_i}}{1+\gamma_{ur_i}}\right) < R_S, \quad \forall r_i \in \mathrm{A}_m \tag{6}$$

Similarly, the event $\mathrm{D} = \mathrm{D}_n$ is formulated as

$$\begin{aligned} &\frac{1}{2}\log_2\left(1+\frac{\gamma_{sr_i}}{1+\gamma_{ur_i}}\right) > R_S, \quad r_i \in \mathrm{D}_n \\ &\frac{1}{2}\log_2\left(1+\frac{\gamma_{sr_j}}{1+\gamma_{ur_j}}\right) < R_S, \quad r_j \in \mathrm{A}_m / \mathrm{D}_n \end{aligned} \tag{7}$$

Given that $\mathrm{D} = \mathrm{D}_n$ and the selected relay according to the next subsection is $r_{\mathrm{D}} \in \mathrm{D}$, r_{D} encodes the decoding confidential message by the widely-adopted wiretap code [25]. The corresponding instantaneous channel capacity of link $r_{\mathrm{D}} \to d$ and link $r_{\mathrm{D}} \to e$ are given by respectively

$$C_{r_{\mathrm{D}}d}\left(\mathrm{D}{=}\mathrm{D}_n\right) = \frac{1}{2}\log_2\left(1+\frac{\gamma_{r_{\mathrm{D}}d}}{1+\gamma_{ud}}\right) \tag{8}$$

$$C_{r_{\mathrm{D}}e}\left(\mathrm{D}{=}\mathrm{D}_n\right) = \frac{1}{2}\log_2\left(1+\frac{\gamma_{r_{\mathrm{D}}e}}{1+\gamma_{ue}}\right) \tag{9}$$

where $\gamma_{r_{\mathrm{D}}d} = E_r\left|h_{r_{\mathrm{D}}d}\right|^2 \big/ N_0$, $\gamma_{ud} = E_u\left|h_{ud}\right|^2 / N_0$, $\gamma_{r_{\mathrm{D}}e} = E_r\left|h_{r_{\mathrm{D}}e}\right|^2 \big/ N_0$, and $\gamma_{ue} = E_u\left|h_{ue}\right|^2 / N_0$.

Hence, combining (8) and (9), the instantaneous secrecy capacity condition on $\mathrm{D}{=}\mathrm{D}_n$ and the selected relay r_{D} is given by [26]

$$C_s\left(\mathrm{D}{=}\mathrm{D}_n\right) = \left[C_{r_{\mathrm{D}}d}\left(\mathrm{D}{=}\mathrm{D}_n\right) - C_{r_{\mathrm{D}}e}\left(\mathrm{D}{=}\mathrm{D}_n\right)\right]^+ \tag{10}$$

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

2.2 Proposed Suboptimal Relay Selection Scheme

According to (8), (9), and (10), the relay selection scheme with best secrecy capacity performance condition on $\mathrm{D}{=}\mathrm{D}_n$ should be implemented as

$$r_{\mathrm{D}} = \arg\max_{r_i \in \mathrm{D}_n} \left[C_{r_i d}\left(\mathrm{D}=\mathrm{D}_n\right) - C_{r_i e}\left(\mathrm{D}=\mathrm{D}_n\right) \right]^{+} = \arg\max_{r_i \in \mathrm{D}_n} \left(1+\frac{\gamma_{r_i d}}{1+\gamma_{ud}}\right) \Bigg/ \left(1+\frac{\gamma_{r_i e}}{1+\gamma_{ue}}\right) \tag{11}$$

However, this optimal relay selection has not only to consider the instantaneous CSI of the legitimate link, but also needs to take the instantaneous CSI of eavesdropper link into consideration. Although this is a common assumption in the physical layer security literature, it is not practical in most passive eavesdropping attack scenarios. Furthermore, the instantaneous CSI of $u \rightarrow d$ and $u \rightarrow e$ interference links is not available for cognitive networks.

Although the tacking of the instantaneous $r_i \rightarrow e$ link seems to be impossible for practical applications, knowledge of the average channels can be estimated and obtained by long-term monitoring the eavesdropper's transmission. Thus, we consider a suboptimal relay selection scheme, which selects the relay based on the instantaneous CSI of $r_i \rightarrow d$ link and the statistical CSI of $r_i \rightarrow e$ link. In this paper, the relay selection rule can be formulated as

$$r_{\mathrm{D}} = \arg\max_{r_i \in \mathrm{D}_n} \left\{ \frac{\gamma_{r_i d}}{\bar{\gamma}_{r_i e}} \right\} \tag{12}$$

Specially, if assuming $\bar{\gamma}_{r_i e} = \bar{\gamma}_{re}, \forall r_i \in \mathrm{R}$, which correspond to the scenario where the relays are close to each other and forming a cluster, our proposed relay selection scheme would be totally independent of CSI of the eavesdropper links, and can be implemented as the traditional relay selection scheme in [27], e.g. $r_{\mathrm{D}} = \arg\max_{r_i \in \mathrm{D}_n} \left\{ \gamma_{r_i d} \right\}$.

3. Secrecy Performance for Underlay CCRNs

In this section, we characterize the secrecy performance of our proposed relay selection scheme for underlay CCRNs with FTP in term of probability of non-zero secrecy capacity, exact secrecy outage probability, and asymptotic secrecy outage probability over independent and non-identically distributed Rayleigh fading channels.

3.1 Preliminaries

Firstly, we present the probabilities of the occurrence of active relay set A and the decoding set D , respectively, to facilitate the following secrecy performance analysis.

Since the channel gain $\left|h_{r_i v}\right|^2, \forall r_i \in \mathrm{R}$ of different relays are independent of each other and obey exponential distribution with parameter $\delta_{r_i v}^2$, the probability of the event $\mathrm{A} = \phi$ is obtained from (2) as

$$\Pr\left\{\mathrm{A} = \phi\right\} = \prod_{r_i \in \mathrm{R}} \exp\left(-\frac{\mathrm{I}_0}{E_r \delta_{r_i v}^2}\right) \tag{12}$$

Similarly, the probability of the occurrence $\mathrm{A} = \mathrm{A}_m$ is obtained from (3) as

$$\Pr\left\{\mathrm{A} = \mathrm{A}_m\right\} = \prod_{r_i \in \mathrm{A}_m} \left[1-\exp\left(-\frac{\mathrm{I}_0}{E_r \delta_{r_i v}^2}\right)\right] \prod_{r_j \in \mathrm{R}/\mathrm{A}_m} \exp\left(-\frac{\mathrm{I}_0}{E_r \delta_{r_j v}^2}\right) \tag{13}$$

Meanwhile, given a non-empty A_m , the probability of the event $\mathrm{D} = \phi$ is obtained from (7) as

$$\Pr\left\{\mathrm{D} = \phi \middle| \mathrm{A} = \mathrm{A}_m\right\} = \prod_{r_i \in \mathrm{A}_m} \left[1-\exp\left(-\frac{\theta_1}{\bar{\gamma}_{sr_i}}\right) \frac{\bar{\gamma}_{sr_i}}{\theta_1 \bar{\gamma}_{ur_i} + \bar{\gamma}_{sr_i}}\right] \tag{14}$$

where $\theta_1 = 2^{2R_S} - 1$.

Similarly, the conditional probability of the occurrence $\mathrm{D} = \mathrm{D}_n$ given the non-empty A_m is given by

$$\begin{aligned}\Pr\left\{\mathrm{D} = \mathrm{D}_n \middle| \mathrm{A} = \mathrm{A}_m\right\} &= \prod_{r_i \in \mathrm{D}_n} \exp\left(-\frac{\theta_1}{\overline{\gamma}_{sr_i}}\right) \frac{\overline{\gamma}_{sr_i}}{\theta_1 \overline{\gamma}_{ur_i} + \overline{\gamma}_{sr_i}} \\ &\times \prod_{r_j \in \mathrm{A}_m / \mathrm{D}_n} \left[1 - \exp\left(-\frac{\theta_1}{\overline{\gamma}_{sr_j}}\right) \frac{\overline{\gamma}_{sr_j}}{\theta_1 \overline{\gamma}_{ur_j} + \overline{\gamma}_{sr_j}}\right]\end{aligned} \tag{15}$$

Next, given a non-empty D_n, we will provide the conditional CDF of $\gamma_{r_\mathrm{D} d}$ according to our proposed relay selection scheme in (11).

Lemma 1: Given a non-empty D_n, the conditional CDF of $\gamma_{r_\mathrm{D} d}$ is given by

$$F_{\gamma_{r_\mathrm{D} d} | \mathrm{D}_n}\left(\gamma | \mathrm{D}_n\right) = \sum_{l=0}^{|\mathrm{D}_n|-1} \sum_{\substack{\mathrm{B} \subset \mathrm{D}_n / r_\mathrm{D} \\ |\mathrm{B}| = l}} \frac{(-1)^l}{\Phi_{r_\mathrm{D},\mathrm{B}} + 1} \left[1 - \exp\left(-\mathrm{K}_{r_\mathrm{D},\mathrm{B}} \gamma\right)\right] \tag{16}$$

where $\Phi_{r_\mathrm{D},\mathrm{B}} = \frac{\overline{\gamma}_{r_\mathrm{D} d}}{\overline{\gamma}_{r_\mathrm{D} e}} \sum_{r_j \in \mathrm{B}} \frac{\overline{\gamma}_{r_j e}}{\overline{\gamma}_{r_j d}}$ and $\mathrm{K}_{r_\mathrm{D},\mathrm{B}} = \left(\Phi_{r_\mathrm{D},\mathrm{B}} + 1\right) / \overline{\gamma}_{r_\mathrm{D} d}$. When $|\mathrm{B}| = 0$, we define $\Phi_{r_\mathrm{D},\mathrm{B}} = 0$.

Proof : Given decoding set $\mathrm{D} = \mathrm{D}_n$, if the relay r_D is selected according to (11), it must satisfy the fact that

$$\frac{\gamma_{r_\mathrm{D} d}}{\overline{\gamma}_{r_\mathrm{D} e}} \geq \max_{r_j \in \mathrm{D}_n / r_\mathrm{D}} \left\{\frac{\gamma_{r_j d}}{\overline{\gamma}_{r_j e}}\right\}, \tag{17}$$

from which we derive the probability as

$$\Pr\left\{\frac{\gamma_{r_\mathrm{D} d}}{\overline{\gamma}_{r_\mathrm{D} e}} \geq \max_{r_j \in \mathrm{D}_n / r_\mathrm{D}} \left\{\frac{\gamma_{r_j d}}{\overline{\gamma}_{r_j e}}\right\}\right\} = \prod_{r_j \in \mathrm{D}_n / r_i} \left[1 - \exp\left(-\frac{\gamma_{r_\mathrm{D} d} / \overline{\gamma}_{r_i e}}{\overline{\gamma}_{r_j d} / \overline{\gamma}_{r_j e}}\right)\right].$$

Thus, the conditional CDF of $\gamma_{r_\mathrm{D} d}$ can be derived as

$$\begin{aligned}F_{\gamma_{r_\mathrm{D} d} | \mathrm{D}_n}\left(\gamma | \mathrm{D}_n\right) &= \int_0^\gamma f_{\gamma_{r_\mathrm{D} d}}(x) \prod_{r_j \in \mathrm{D}_n / r_i} \left[1 - \exp\left(-\frac{x / \overline{\gamma}_{r_\mathrm{D} e}}{\overline{\gamma}_{r_j d} / \overline{\gamma}_{r_j e}}\right)\right] dx \\ &= \int_0^\gamma \frac{1}{\overline{\gamma}_{r_\mathrm{D} d}} \exp\left(-\frac{x}{\overline{\gamma}_{r_\mathrm{D} d}}\right) \prod_{r_j \in \mathrm{D}_n / r_\mathrm{D}} \left[1 - \exp\left(-\frac{x / \overline{\gamma}_{r_\mathrm{D} e}}{\overline{\gamma}_{r_j d} / \overline{\gamma}_{r_j e}}\right)\right] dx\end{aligned} \tag{18}$$

Following the multinomial identity and simple integral, we can obtain (16).

3.2 Probability of Non-Zero Secrecy Capacity

In this subsection, we examine the condition for the existence of non-zero secrecy capacity, which depicts the possibility of achievable secure communication.

By imposing the fact that the secrecy capacity is zero when s keep silent, or the active relay set A is empty, or the decoding relay set D is empty, or the signal-to-interference-plus-noise ratio (SINR) from the chosen relay to the destination is lower than that to the eavesdropper. Thus, the probability of non-zero secrecy capacity is given by

$$
\begin{aligned}
\Pr\{C_s > 0\} &= \Pr(\mathrm{I}_s < \mathrm{I}_0)\sum_{m=1}^{2^M-1}\Pr\{\mathrm{A}=\mathrm{A}_m\} \\
&\times \sum_{n=1}^{2^{|\mathrm{A}_m|}-1}\Pr\{\mathrm{D}=\mathrm{D}_n \mid \mathrm{A}=\mathrm{A}_m\}\sum_{r_i\in \mathrm{D}_n}\Pr\{C_s(\mathrm{D}=\mathrm{D}_n)>0, r_{\mathrm{D}}=r_i \mid \mathrm{D}=\mathrm{D}_n\}
\end{aligned}
\tag{19}
$$

where $\Pr(\mathrm{I}_s < \mathrm{I}_0)$=1-$\exp\left(-\mathrm{I}_0/\left(E_s\delta_{sv}^2\right)\right)$. According to (10), the conditional probability $\Pr\{C_s(\mathrm{D}=\mathrm{D}_n)>0, r_{\mathrm{D}}=r_i \mid \mathrm{D}=\mathrm{D}_n\}$ can be further expressed as

$$
\begin{aligned}
&\Pr\{C_s(\mathrm{D}=\mathrm{D}_n)>0, r_{\mathrm{D}}=r_i \mid \mathrm{D}=\mathrm{D}_n\} \\
&= \Pr\{U_{i,1} > U_{i,2}, r_{\mathrm{D}}=r_i \mid \mathrm{D}=\mathrm{D}_n\}
\end{aligned}
\tag{20}
$$

where $U_{i,1}=\frac{\gamma_{r_id}}{1+\gamma_{ud}}$ and $U_{i,2}=\frac{\gamma_{r_ie}}{1+\gamma_{ue}}$ denote the SINR of the link $r_i \to d$ and link $r_i \to e$, respectively. Since γ_{r_id} and γ_{r_ie} can be expressed as $\gamma_{r_id}=E_r\left|h_{r_id}\right|^2/N_0$, and $\gamma_{r_ie}=E_r\left|h_{r_ie}\right|^2/N_0$, respectively, the conditional probability is totally independently with the transmit power E_r of the secondary relays in (20). And the impact of E_r on the probability of non-zero secrecy capacity embodies in limiting the candidates of active relays by (12) and (13).

Since γ_{ud} is an exponential RV, we can obtain the conditional CDF of $U_{1,i}$ using ***Lemma 1*** as

$$
F_{U_{i,1}|\mathrm{D}_n}(x|\mathrm{D}_n) = \sum_{l=0}^{|\mathrm{D}_n|-1}\sum_{\substack{\mathrm{B}\subset \mathrm{D}_n/r_i\\ |\mathrm{B}|=l}}\frac{(-1)^l}{\Phi_{r_i,\mathrm{B}}+1}\left[1-\frac{\exp\left(-\mathrm{K}_{r_i,\mathrm{B}}x\right)}{\left(\mathrm{K}_{r_i,\mathrm{B}}\bar{\gamma}_{ud}x+1\right)}\right]
\tag{21}
$$

From e 's point of view, the optimum relay selection for d is a random relay selection, as the link $r_i \to d$ and link $r_i \to e$ are uncorrelated. Thus, we can obtain the conditional PDF of $U_{2,i}$ as

$$
f_{U_{i,2}|\mathrm{D}_n}(y|\mathrm{D}_n) = \frac{\bar{\gamma}_{r_ie}\bar{\gamma}_{ue}}{\left(\bar{\gamma}_{ue}y+\bar{\gamma}_{r_ie}\right)^2}e^{-\frac{y}{\bar{\gamma}_{r_ie}}} + \frac{1}{\bar{\gamma}_{ue}y+\bar{\gamma}_{r_ie}}e^{-\frac{y}{\bar{\gamma}_{r_ie}}}
\tag{22}
$$

Thereby, using (20), (21) and (22), and applying [28, 3.352.4] and [28, 3.353.3], the conditional probability $\Pr\{C_s(\mathrm{D}=\mathrm{D}_n)>0, r_{\mathrm{D}}=r_i \mid \mathrm{D}=\mathrm{D}_n\}$ can be given by

$$
\begin{aligned}
&\Pr\{C_s(\mathrm{D}=\mathrm{D}_n)>0, r_{\mathrm{D}}=r_i \mid \mathrm{D}=\mathrm{D}_n\} \\
&= \int_0^\infty\left[1-F_{U_1|\mathrm{D}_n}(y|\mathrm{D}_n)\right]f_{U_2|\mathrm{D}_n}(y|\mathrm{D}_n)\,dy \\
&= 1-\sum_{l=0}^{|\mathrm{D}_n|-1}\sum_{\substack{\mathrm{B}\subset \mathrm{D}_n/r_i\\ |\mathrm{B}|=l}}\frac{(-1)^l}{\Phi_{r_i,\mathrm{B}}+1}\left[1-\frac{1}{\mathrm{K}_{r_i,\mathrm{B}}\bar{\gamma}_{ud}\bar{\gamma}_{ue}}\right. \\
&\times\left(\frac{\mathrm{G}_2-\mathrm{G}_1+\bar{\gamma}_{r_ie}+\mathrm{G}_3(\mathrm{G}_1-\mathrm{G}_2)\bar{\gamma}_{r_ie}}{(\mathrm{G}_1-\mathrm{G}_2)^2}e^{\mathrm{G}_2\mathrm{G}_3}\mathrm{Ei}(-\mathrm{G}_2\mathrm{G}_3)\right. \\
&\left.\left.+\frac{\mathrm{G}_1-\mathrm{G}_2-\bar{\gamma}_{r_ie}}{(\mathrm{G}_1-\mathrm{G}_2)^2}e^{\mathrm{G}_1\mathrm{G}_3}\mathrm{Ei}(-\mathrm{G}_1\mathrm{G}_3)+\frac{\bar{\gamma}_{r_ie}}{(\mathrm{G}_1-\mathrm{G}_2)\mathrm{G}_2}\right)\right]
\end{aligned}
\tag{23}
$$

where $\mathrm{G}_1=1/\mathrm{K}_{r_i,\mathrm{B}}\bar{\gamma}_{ud}$, $\mathrm{G}_2=\bar{\gamma}_{r_ie}/\bar{\gamma}_{ue}$, $\mathrm{G}_3=\mathrm{K}_{r_i,\mathrm{B}}+1/\bar{\gamma}_{r_ie}$, and $\mathrm{Ei}(\cdot)$ is the exponential integral function [28].

Finally, the closed-form expression for the probability of non-zero secrecy capacity can be obtained by substituting (13), (15) and (23) into (19).

3.3 Exact Secrecy Outage Probability

The secrecy outage probability is defined as the probability that the achievable secrecy rate is less than a given secrecy transmission rate R_S [29]. Based on the data transmission and our proposed relay selection scheme in previous section, we can find that the secure transmission outage occurs if s keep silent, or the active relay set A is empty, or the decoding relay set D is empty, or the SINR from the chosen relay to the destination is lower than the eavesdropper SINR. Hence, using the law of total probability, the SOP can be formulated as

$$\begin{aligned}
\mathrm{P}_{so}\left(R_s\right) = {} & \Pr\left(\mathrm{I}_s > \mathrm{I}_0\right) + \Pr\left(\mathrm{I}_s \le \mathrm{I}_0\right)\Big[\Pr\left\{\mathrm{A} = \phi\right\} \\
& + \sum_{m=1}^{2^M-1} \Pr\left\{\mathrm{A} = \mathrm{A}_m\right\} \Pr\left\{\mathrm{D} = \phi \middle| \mathrm{A} = \mathrm{A}_m\right\} \\
& + \sum_{m=1}^{2^M-1} \Pr\left\{\mathrm{A} = \mathrm{A}_m\right\} \sum_{n=1}^{2^{|\mathrm{A}_m|}-1} \Pr\left\{\mathrm{D} = \mathrm{D}_n \middle| \mathrm{A} = \mathrm{A}_m\right\} \\
& \times \sum_{r_i \in \mathrm{D}_n} \Pr\left\{C_s\left(\mathrm{D} = \mathrm{D}_n\right) < R_s, r_{\mathrm{D}} = r_i \middle| \mathrm{D} = \mathrm{D}_n\right\}\Big]
\end{aligned} \tag{24}$$

Using (20), (21) and (22), and applying [28, 3.352.4] and [28, 3.353.3], the conditional probability $\Pr\left\{C_s\left(\mathrm{D} = \mathrm{D}_n\right) < R_s, r_{\mathrm{D}} = r_i \middle| \mathrm{D} = \mathrm{D}_n\right\}$ can be given by

$$\begin{aligned}
& \Pr\left\{C_s\left(\mathrm{D} = \mathrm{D}_n\right) < R_s, r_{\mathrm{D}} = r_i \middle| \mathrm{D} = \mathrm{D}_n\right\} \\
& = \Pr\left\{U_{i,1} < \theta_2\left(1 + U_{i,2}\right) - 1 \middle| \mathrm{D} = \mathrm{D}_n\right\} \\
& = \sum_{l=0}^{|\mathrm{D}_n|-1} \sum_{\substack{\mathrm{B} \subset \mathrm{D}_n / r_i \\ |\mathrm{B}| = l}} \frac{(-1)^l}{\Phi_{r_i,\mathrm{B}} + 1} \left[1 - \frac{\exp\left(-\mathrm{K}_{r_i,\mathrm{B}}\left(\theta_2 - 1\right)\right)}{\mathrm{K}_{r_i,\mathrm{B}} \theta_2 \bar{\gamma}_{ud} \bar{\gamma}_{ue}}\right. \\
& \quad \times \left(\frac{\mathrm{E}_2 - \mathrm{E}_1 + \bar{\gamma}_{r_i e} + \mathrm{E}_3\left(\mathrm{E}_1 - \mathrm{E}_2\right)\bar{\gamma}_{r_i e}}{\left(\mathrm{E}_1 - \mathrm{E}_2\right)^2} e^{\mathrm{E}_2 \mathrm{E}_3} \mathrm{Ei}\left(-\mathrm{E}_2 \mathrm{E}_3\right)\right. \\
& \quad \left.\left. + \frac{\mathrm{E}_1 - \mathrm{E}_2 - \bar{\gamma}_{r_i e}}{\left(\mathrm{E}_1 - \mathrm{E}_2\right)^2} e^{\mathrm{E}_1 \mathrm{E}_3} \mathrm{Ei}\left(-\mathrm{E}_1 \mathrm{E}_3\right) + \frac{\bar{\gamma}_{r_i e}}{\left(\mathrm{E}_1 - \mathrm{E}_2\right)\mathrm{E}_2}\right)\right]
\end{aligned} \tag{25}$$

where $\theta_2 = 2^{2R_s}$, $\mathrm{E}_1 = \left(\mathrm{K}_{r_i,\mathrm{B}}\left(\theta_2 - 1\right)\bar{\gamma}_{ud} + 1\right) / \left(\mathrm{K}_{r_i,\mathrm{B}} \theta_2 \bar{\gamma}_{ud}\right)$, $\mathrm{E}_2 = \bar{\gamma}_{r_i e} / \bar{\gamma}_{ue}$, and $\mathrm{E}_3 = \mathrm{K}_{r_i,\mathrm{B}} \theta_2 + 1 / \bar{\gamma}_{r_i e}$.

Thereby, the exact closed-form expression for the SOP is derived by substituting (12), (13), (14), (15) and (25) into (24). It is worth pointing out that the closed-form expression for the SOP in (24) is useful to evaluate the impacts of the transmit power of the secondary users, the interference constraint, and the number of relays on the secure performance of underlay CCRNs with fixed transmit power control.

3.4 Asymptotic Behavior of Secrecy Outage Probability

Since the exact SOP analysis results are too complicated to render insight on the impact of system parameters, we will investigate the asymptotic behavior of the SOP by some special cases in this subsection.

1) Case of $\mathrm{I}_0 \to 0$ or $E_s = E_r \to \infty$: From (24), we directly obtain $\mathrm{P}_{so}\left(R_s\right) \to 1$ as $\mathrm{I}_0 \to 0$ or $E_s = E_r \to \infty$, which illustrates the huge impact of the interference constraint on the underlay

CCRNs with FPT strategy. Given a limited I_0, increase of transmit power will not always lead to the improvement of secure performance, which is significantly different from the traditional wireless communication systems. Therefore, a proper transmit power is preferred for secondary relays to be energy-efficient and improve the secure performance.

2) Case of $\mathrm{I}_0 \to \infty$ and $\delta_{sr_i}^2 \to \infty$, $\forall r_i \in \mathrm{R}$: This case corresponds to the scenario where the primary destination can tolerate an unlimited interference and the relays is close to the secondary source. Notice that when $\delta_{sr_i}^2 \to 0$, the probability of successful decoding will go to one, thus $\mathrm{P}_{so}(R_s) \to 1$. As such, we omit this case in this paper.

When $\mathrm{I}_0 \to \infty$ and $\delta_{sr_i}^2 \to \infty$, $\forall r_i \in \mathrm{R}$, from (13) and (15), we have $\Pr(\mathrm{I}_s \le \mathrm{I}_0) = 1$,

$$\lim_{\mathrm{I}_0 \to \infty} \Pr\{\mathrm{A} = \mathrm{A}_m\} = \begin{cases} 1, & \mathrm{A}_m = \mathrm{R} \\ 0, & \mathrm{A}_m \ne \mathrm{R} \end{cases} \tag{26}$$

and

$$\lim_{\delta_{sr_i}^2 \to \infty,\ \forall r_i \in \mathrm{R}} \Pr\{\mathrm{D} = \mathrm{D}_n | \mathrm{A} = \mathrm{R}\} = \begin{cases} 1, & \mathrm{D}_n = \mathrm{R} \\ 0, & \mathrm{D}_n \ne \mathrm{R} \end{cases} \tag{27}$$

Therefore, the SOP in (24) can be simplified as

$$\mathrm{P}_{so}^{\infty}(R_s) = \sum_{r_i \in \mathrm{R}} \Pr\{C_s(\mathrm{D} = \mathrm{R}) < R_s, r_{\mathrm{D}} = r_i | \mathrm{D} = \mathrm{R}\} \tag{28}$$

where $\Pr\{C_s(\mathrm{D} = \mathrm{R}) < R_s, r_{\mathrm{D}} = r_i | \mathrm{D} = \mathrm{R}\}$ can be derived by substituting $\mathrm{D}_n = \mathrm{R}$ into (25). Thus,

$$\begin{aligned} \mathrm{P}_{so}^{\infty}(R_s) = & \sum_{r_i \in \mathrm{R}} \sum_{l=0}^{2^M - 1} \sum_{\substack{\mathrm{B} \subset \mathrm{R}/r_i \\ |\mathrm{B}| = l}} \frac{(-1)^l}{\Phi_{r_i,\mathrm{B}} + 1} \left[1 - \frac{\exp\left(-\mathrm{K}_{r_i,\mathrm{B}}(\theta_2 - 1)\right)}{\mathrm{K}_{r_i,\mathrm{B}} \theta_2 \bar{\gamma}_{ud} \bar{\gamma}_{ue}} \right. \\ & \times \left(\frac{\mathrm{E}_2 - \mathrm{E}_1 + \bar{\gamma}_{r_i e} + \mathrm{E}_3(\mathrm{E}_1 - \mathrm{E}_2)\bar{\gamma}_{r_i e}}{(\mathrm{E}_1 - \mathrm{E}_2)^2} e^{\mathrm{E}_2 \mathrm{E}_3} \mathrm{Ei}(-\mathrm{E}_2 \mathrm{E}_3) \right. \\ & \left. \left. + \frac{\mathrm{E}_1 - \mathrm{E}_2 - \bar{\gamma}_{r_i e}}{(\mathrm{E}_1 - \mathrm{E}_2)^2} e^{\mathrm{E}_1 \mathrm{E}_3} \mathrm{Ei}(-\mathrm{E}_1 \mathrm{E}_3) + \frac{\bar{\gamma}_{r_i e}}{(\mathrm{E}_1 - \mathrm{E}_2)\mathrm{E}_2} \right) \right] \end{aligned} \tag{29}$$

Remark: Traditionally, the diversity order is used to evaluate the wireless transmission reliability performance in [30], which characterizes the slope of bit error rate (BER) curve as SNR tends to infinity. However, in the presence of eavesdropping attack, the SOP is used to evaluate the secure performance. Moreover, it is observed from (24) the SOP is independent of the transmit power in the high SNR. Thus, the traditional diversity order is not applicable to measure the secure performance. To provide an insight into the impact of the number of the relays on the secrecy performance, we investigate the generalized secure diversity order introduced in [27].

3) **Case of $\mathrm{I}_0 \to \infty$, $\delta_{sr_i}^2 \to \infty$, $\forall r_i \in \mathrm{R}$, and $\lambda_{me} \to \infty$:** where $\delta_{r_i d}^2 = \eta_{r_i d} \delta_m^2$ and $\delta_{r_i e}^2 = \eta_{r_i e} \delta_e^2$ represent the reference channel gains of the legitimate links and the eavesdropper links, respectively, and the main-to-eavesdropper ratio (MER) $\lambda_{me} = \delta_m^2 / \delta_e^2$ [22]. Here, $\lambda_{me} \to \infty$ corresponds to the scenario where the secondary destination is located much closer to the relays than the eavesdropper, which is a practical scenario of interest [29].

In [27], a generalized secure diversity order can be expressed as

$$d_{secure} = -\lim_{\lambda_{me}\to\infty} \frac{\log\left(P_{\text{int}}\right)}{\log\left(\lambda_{me}\right)} \tag{30}$$

where P_{int} denotes the intercept probability, which is the occuring probability of an intercept event when the secrecy capacity becomes negative in [27].

As such, when $\mathrm{I}_0 \to \infty$ and $\delta_{sr_i}^2 \to \infty$, $\forall r_i \in \mathrm{R}$, by setting $R_s = 0$, mathematically, the value of probability $\mathrm{P}_{so}\left(R_s\right)$ is equal to P_{int}, e.g. $P_{\text{int}} = \mathrm{P}_{so}^{\infty}(0)$. To derive the secure diversity order of this case, we first derive the approximate analysis of the SOP as $\lambda_{me} \to \infty$.

Lemma 2: For $\mathrm{I}_0 \to \infty$ and $\delta_{sr_i}^2 \to \infty$, $\forall r_i \in \mathrm{R}$, and $\lambda_{me} \to \infty$, we can obtain $\mathrm{P}_{so}^{\infty}(0)$ as

$$\begin{aligned}\mathrm{P}_{so}^{\infty}(0) \approx{}& \bar{\gamma}_{ue}^{-M} \sum_{p=0}^{M} \frac{\Gamma(M+1)^2}{\Gamma(M-p+1)} \bar{\gamma}_{ud}^{\,p} \prod_{r_j \in \mathrm{R}} \frac{1}{\eta_{r_j d} / \eta_{r_j e}} \\ &\times \left[\Psi\left(M+1, M; \frac{1}{\bar{\gamma}_{ue}}\right) + \frac{1}{\bar{\gamma}_{ue}} \Psi\left(M+1, M+1; \frac{1}{\bar{\gamma}_{ue}}\right)\right] \left(\frac{1}{\lambda_{me}}\right)^{M}\end{aligned} \tag{31}$$

Proof *:* Letting $\lambda_{me} \to \infty$, we have

$$\Pr\left\{\frac{\gamma_{r_\mathrm{D} d}}{\bar{\gamma}_{r_\mathrm{D} e}} \geq \max_{r_j \in \mathrm{D}_n / r_\mathrm{D}} \left\{\frac{\gamma_{r_j d}}{\bar{\gamma}_{r_j e}}\right\}\right\} \approx \prod_{r_j \in \mathrm{R}/r_\mathrm{D}} \frac{x / \bar{\gamma}_{r_\mathrm{D} e}}{\bar{\gamma}_{r_j d} / \bar{\gamma}_{r_j e}} \tag{32}$$

Accordingly, the conditional CDF of $\gamma_{r_\mathrm{D} d}$ in (16) with $\mathrm{D}_n = \mathrm{R}$ can be approximated as

$$\begin{aligned}F_{\gamma_{r_\mathrm{D} d}|\mathrm{R}}^{\infty}\left(\gamma | \mathrm{R}\right) &\approx \int_0^{\gamma} \frac{1}{\bar{\gamma}_{r_\mathrm{D} d}} \exp\left(-\frac{x}{\bar{\gamma}_{r_\mathrm{D} d}}\right) \prod_{r_j \in \mathrm{R}/r_\mathrm{D}} \frac{x / \bar{\gamma}_{r_i e}}{\bar{\gamma}_{r_j d} / \bar{\gamma}_{r_j e}} dx \\ &\overset{(a)}{\approx} \frac{\gamma^M}{M \bar{\gamma}_{r_\mathrm{D} d}^{M}} \prod_{r_j \in \mathrm{R}/r_\mathrm{D}} \frac{\eta_{r_\mathrm{D} d} / \eta_{r_\mathrm{D} e}}{\eta_{r_j d} / \eta_{r_j e}}\end{aligned} \tag{33}$$

where (a) follows from the fact that $\gamma(n,x) \approx x^n / n$ as $x \to 0$.

Then, the conditional CDF of $U_{i,1}$ is approximated as

$$F_{U_{i,1}|\mathrm{R}}^{\infty}\left(x | \mathrm{R}\right) \approx \frac{x^M}{M \bar{\gamma}_{r_i d}^{M}} \prod_{r_j \in \mathrm{R}/r_i} \frac{\eta_{r_i d} / \eta_{r_i e}}{\eta_{r_j d} / \eta_{r_j e}} \sum_{p=0}^{M} \frac{\Gamma(M+1) \gamma_{ud}^{p}}{\Gamma(M-p+1)} \tag{34}$$

Therefore, using (34) and (22), we can derive

$$\begin{aligned}\mathrm{P}_{so}^{\infty}(0) &= \sum_{r_i \in \mathrm{R}} \Pr\left\{U_{i,1} < U_{i,2}\right\} \\ &= \sum_{r_i \in \mathrm{R}} \int_0^{\infty} F_{U_{i,1}|\mathrm{R}}^{\infty}\left(y | \mathrm{R}\right) f_{U_{i,2}|\mathrm{D}_n}\left(y | \mathrm{R}\right) dy \\ &= \frac{1}{\bar{\gamma}_{ue}^{M}} \sum_{p=0}^{M} \frac{\Gamma(M+1) \gamma_{ud}^{p}}{\Gamma(M-p+1)} \prod_{r_j \in \mathrm{R}/r_i} \frac{1}{\eta_{r_j d} / \eta_{r_j e}} \left[\int_0^{\infty} \frac{t^M}{(t+1)^2} \exp\left(-\frac{t}{\bar{\gamma}_{ue}}\right) dt\right. \\ &\quad \left. + \frac{1}{\bar{\gamma}_{ue}} \int_0^{\infty} \frac{t^M}{(t+1)} \exp\left(-\frac{t}{\bar{\gamma}_{ue}}\right) dt\right] \left(\frac{1}{\lambda_{me}}\right)^{M}\end{aligned} \tag{35}$$

Using [28, 3.352.4], the approximated probability $\mathrm{P}_{so}^{\infty}(0)$ can be given by (31).

From (31), we can observe that the SOP $\mathrm{P}_{so}^{\infty}(0)$ behaves as $\left(1/\lambda_{me}\right)^M$ as $\lambda_{me} \to \infty$. Substituting (31) into (30), we can obtain the secure diversity order of our proposed relay selection scheme same as [27]

$$d_{secure} = M \tag{37}$$

which shows the secure diversity order is same as the number of secondary relays, revealing the fact that full secure diversity is achieved by the proposed relay selection scheme. It also indicates that although the PU's interference definitely degrades the SOP, it does not affect the speed at which the SOP decreases as $\lambda_{me} \to \infty$ when $\mathrm{I}_0 \to \infty$, and $\delta^2_{sr_i} \to \infty$, $\forall r_i \in \mathrm{R}$. In contrast, increasing the number of secondary relay, the SOP will decrease at a faster speed. Therefore, exploiting multiple relay with relay selection can effectively improve the secrecy performance.

4. Numerical Results and Discussions

This section presents the numerical results to exam the impacts of the transmit power of the secondary users, the interference constraint, and the number of relays on the secure performance of CCRNs with fixed transmit power control. In all cases, $R_S = 0.5$ bits/s/Hz , $E_u/N_0 = 5\text{dB}$, $\delta^2_{ud} = \delta^2_{ue} = 1$, and $\delta^2_{r_iv}=\delta^2_{ur_i}=1$, $\forall r_i \in \mathrm{R}$. All the nodes are equipped with single antenna and work in the half-duplexing mode. Each link in the underlay CCRN is subjected to an AWGN with zero mean and variance N_0 . All the channels are modeled as independent and non-identically distributed Rayleigh fading random variables. We see from the figures that the exact curves precisely agree with the simulations, which validate the accuracy of our analytical results. We further plot asymptotic curves to predict the secure diversity order. Most importantly, we compare the secrecy performance of our proposed relay selection scheme (PRS) with the traditional relay selection scheme (TRS) in [27] and the optimal relay selection scheme (ORS) in [22].

4.1 Impact of Transmit Power of Secondary Users

The impact of the transmit power of the secondary users on secure performance in term of the probability of non-zero secure capacity and the secrecy outage probability is illustrated in **Fig. 2** and **Fig. 3**, respectively. We consider an equal average energy strategy at the secondary source and relays (i.e. $E_s = E_r = E_T$), and the equal SNR is defined as E_T/N_0 . And we set $M = 3$, $\mathrm{I}_0/N_0 = 15\text{dB}$, $\left[\delta^2_{r_1e},\delta^2_{r_2e},\delta^2_{r_3e}\right]=\left[1,1.5^3,2^3\right]$, and $\delta^2_{sr_i} = \delta^2_{r_id} = 1$, $\forall r_i \in \mathrm{R}$.

Observe that as $E_T/N_0 \to 0$, the probability of non-zero achievable secrecy rate approaches 0 and the secrecy outage probability approaches 1, due to all the $s \to r_i$ links are under outage and no confidential message can be delivered to the destination. We can also see that the secure performance keeps improving as E_T/N_0 increases to about 10dB while an unexpected decrease occures when E_T/N_0 keeps rising. Specially, as $E_T/N_0 \to \infty$, the probability of non-zero achievable secrecy rate approaches 0 and the secrecy outage probability approaches 1. This is because that at the low-to-medium SNR region secure performance is dominated by outage probibility of the $s \to r_i$ links while at the high SNR region the finite interference constraint $(\mathrm{I}_0 = 15\text{dB})$ drops all the relays from the candidate pool. Obviously, due to FTP strategy and interference constraint considered, the secure performance in underlay CCRNs is not a monotonically decreasing/increasing function of the transmit signal-to-noise ratio (SNR) anymore. After the SNR approaches a certain level, further increasing SNR may sharply degrade the secrecy performance. As shown in **Fig. 2** and **Fig. 3**, the best secure performance has been achieved when $E_T/N_0 \approx 7\text{dB}$, and further increasing the transmit power can not improve the secrecy performance. Thus, a fixed and proper E_T/N_0 is preferred for secondary relays to be energy-efficient and significantly improve the secure performance.

As can be seen, TRS is not efficient for configurations with the eavesdropper and perform the worst secure performance. On the other hand, ORS achieves the best secrecy performance owing to the availability of the eavesdropper's instantaneous CSI. However, for most of passive eavesdropping attacks, assuming perfect knowledge of the eavesdropper's CSI is often difficult and impossible. PRS has a complexity overhead similar to TRS as it does not require the estimation of the instantaneous eavesdropper link and thus seems to be an efficient solution with practical interest.

4.2 Impact of Interference Constraint

In **Fig. 4** and **Fig. 5**, the probability of non-zero secure capacity and secrecy outage probability curves for the relay selection schemes versus interference constraint I_0 are plotted respectively. We set that $M=3$, $E_s/N_0 = E_r/N_0 = 10$ dB, $\left[\delta_{r_1e}^2, \delta_{r_2e}^2, \delta_{r_3e}^2\right] = \left[1,1.5^3,2^3\right]$, and $\delta_{sr_i}^2 = \delta_{r_id}^2 = 1$, $\forall r_i \in \mathrm{R}$.

The figures show that as $\mathrm{I}_0 \to 0$, the probability of non-zero secure capacity approaches 0 and the secrecy outage probability approaches 1 since in this case all the relays are dropped from the active selection pool and keep silent during the transmission. Along with the increase of I to about 15dB, the secure performance improves sloely. This improvement lies mainly in the fact that with a rise or an absolute relax of the interference constraint, there are more secondary relays satisfying the interference constrains and participating in the selection during the second time slot, which obviously results in better performance. As $\mathrm{I}_0 \to \infty$, the secure performance is limited by the second hop, and then converges to the constant value as the performance floor.

4.3 Impact of the number of relays M

The impact of M on the secrecy outage probability and the secure diversity order is illustrated in **Fig. 6**. In order to give prominence to the parameter M, we focus on the special case where the primary destination can tolerate an unlimited interference from the secondary transmitters and all the relay nodes successfully decode the source transmission, e.g. $\mathrm{I}_0 \to \infty$, $\delta_{sr_i}^2 \to \infty$, $\forall r_i \in \mathrm{R}$. We set that $E_s/N_0 = E_r/N_0 = 10$ dB, $\delta_{r_id}^2 = \delta_m^2$, and $\delta_{r_ie}^2 = \delta_e^2$, $\forall r_i \in \mathrm{R}$. Fig. 6 plots the exact and asymptotic secrecy outage probability versus MER $\lambda_{me} = \delta_m^2/\delta_e^2$ for various M. We see a pronounced SNR advantage with increasing M. This can be explained by the fact that M exerts an increasing effect on the secure diversity order via its proportional contribution.

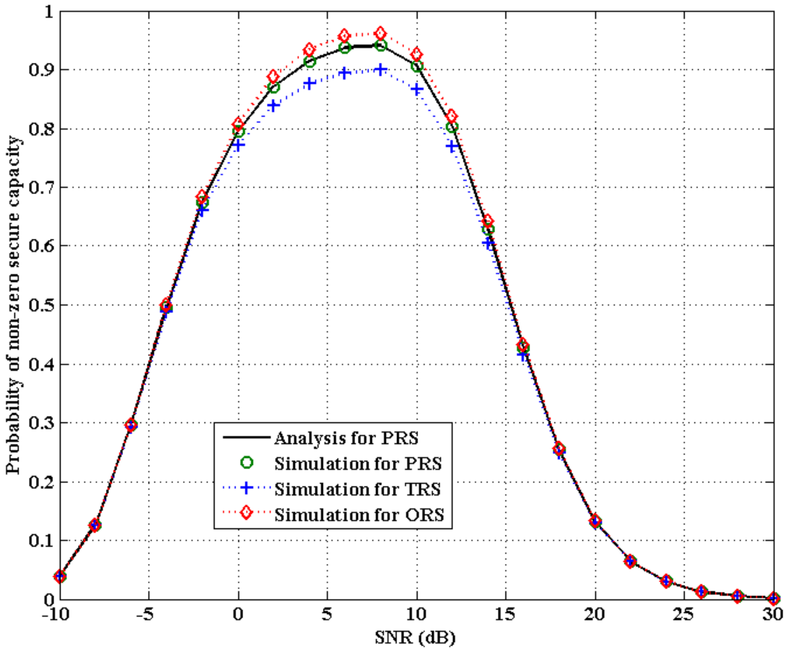

Fig. 2. Probability of non-zero secure capacity versus E_T/N_0.

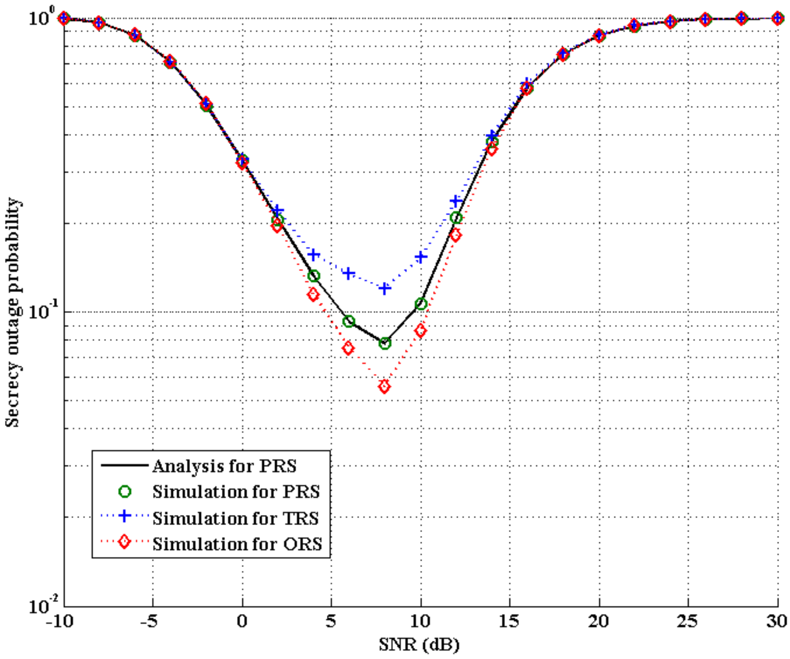

Fig. 3. Secrecy outage probability versus E_T/N_0.

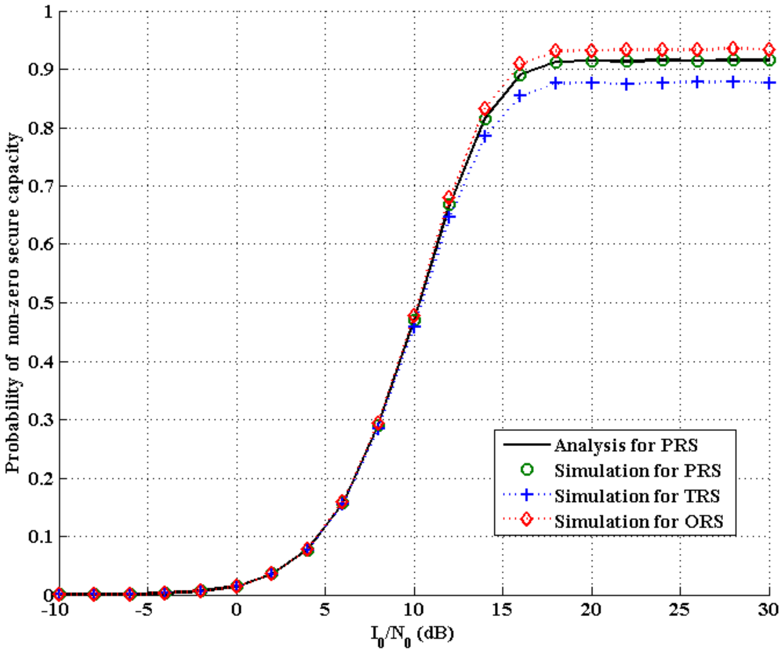

Fig. 4. Probability of non-zero secure capacity versus I_0.

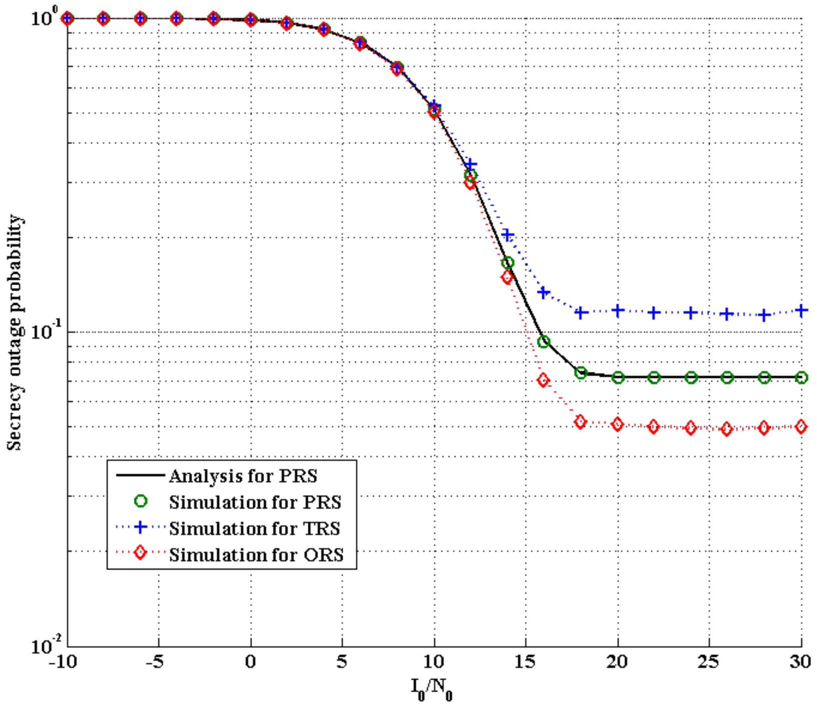

Fig. 5. Secrecy outage probability versus I_0.

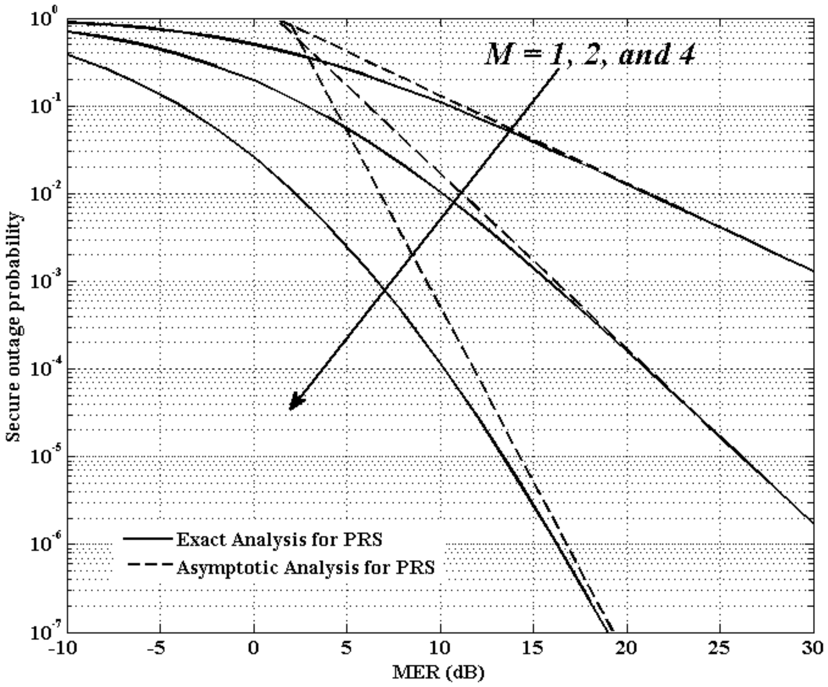

Fig. 6. Secrecy outage probability versus MER λ_{me} with $E_r/N_0 = 10$ dB .

5. Conclusion

In this paper, we have evaluated physical layer security of multiple DF relaying underlay CCRNs with fixed transmit power control in the presence of one eavesdropper. Considered the interference power constraint at PU and modeled CCIs from PU to the secondary system, we proposed a new and simple relay selection scheme, where the relay that satisfies the primary interference constraint and successfully decodes the source message will be selected based on the instantaneous knowledge of all legitimate links and the statistical knowledge of the eavesdropper channels. The exact closed-form expressions for the probability of non-zero secure capacity and the secrecy outage probability have been derived. In order to predict the secure diversity order, moreover, the asymptotic secrecy outage probability analysis is also given. Simulation results are presented to confirm the validity of our theoretical analysis, and illustrate that due to FTP strategy and interference constraint considered, the secure performance in underlay CCRNs is not a monotonically decreasing/increasing function of the transmit signal-to-noise ratio (SNR) anymore. After the SNR approaches a certain level, further increasing SNR may sharply degrade the secrecy performance.

While this paper considered the case when the direct links form the secondary source to the destination and the eavesdropper are ignorable, only one eavesdropper overhear the transmission form the relays, and all nodes are equipped with single antenna, secure communication for the general cases with multiple eavesdroppers, multiple antenna node, and the direct links to the eavesdropper is a challenging problem, which is remained for future work.

References

[1] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb.2005. Article (CrossRef Link)

[2] Z. Xu, W. Qin, Q. Tang, and D. Jiang, “Energy-efficient cognitive access approach to convergence communications,” SCIENCE CHINA Information Sciences, vol. 57, no. 4, pp. 1-12, April. 2014. 2014, 57(4): 1-12. http://www.cnki.com.cn/Article/CJFDTotal-JFXG201404006.htm

[3] K. Tourki, Khalid. A. Qaraqe, and M. -S. Alouini, “Outage analysis for underlay cognitive networks using incremental regenerative relaying,” *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 721–734, Feb. 2013. Article (CrossRef Link)

[4] Y. Zou, J. Zhu, B. Zheng and Y.-D. Yao, “An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks,” *IEEE Trans. Sig. Pross.*, vol. 58, no. 10, pp. 5438–5445, Oct. 2010. Article (CrossRef Link)

[5] T. Q. Duong, V. N. Q. Bao, H. Tran, G. C. Alexandropoulos., and H.-J. Zepernick, “Effect of primary network on performance of spectrum sharing AF relaying,” *Electron, Lett.*, vol. 48, no. 1, pp. 25-27, 2012. Article (CrossRef Link)

[6] W. Xu, J. Zhang, P. Zhang, and C. Tellambure, “Outage probability os denode-and-forword cognitive relay in presence of primary user’s interference,” *IEEE Commun. Lett.*, vol. 16, no. 8, pp. 1252–1255, Aug. 2012. Article (CrossRef Link)

[7] S. I. Hussain, M. M. Abdallah, M.-S. Alouini, M. O. Hasna, K. Qaraqe, “Performance analysis of selective cooperation in underlay cognitive networks over Rayleigh channels,” in *Proc. of IEEE SPAWC*, 2011. Article (CrossRef Link)

[8] S. I. Hussain, M.–S. Alouini, K. Qaraqe, and M. Hasna, “Reactive relay selection in underlay cognitive networks with fixed gain relays,” in *Proc. of IEEE ICC*. 2012. Article (CrossRef Link)

[9] S. I. Hussain, M.–S. Alouini, K. Qaraqe, and M. Hasna, “Outage Analysis of Selective Cooperation in Underlay Cognitive Networks with Fixed Gain Relays and Primary Interference Modeling,” in *Proc. of IEEE PIMRC*, 2012. Article (CrossRef Link)

[10] H. Hakim, H. Boujemmaa, and W. Ajib, “Performance comparison between adaptive and fixed transmit power in underlay cognitive radio networks,” *IEEE Trans. Commun.* vol.61, no. 12, pp. 4836–4846, Dec. 2013. Article (CrossRef Link)

[11] Z. Shu, Y. Qian, and S. Ci, “On physical layer security for cognitive radio networks,” *IEEE Network*, vol. 12, no. 5, pp. 28–33, 2013. Article (CrossRef Link)

[12] H. Delfs, and H. Knebl, *Introduction to cryptography: principles and applications, 2nd edn.* Springer, 2007. Article (CrossRef Link)

[13] A Mukherjee, S. A. Fakoorian, J. Huang and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless network: a survey,” *IEEE Commun. Survey & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014. Article (CrossRef Link)

[14] B. Makki and T. Eriksson, “Secure spectrum sharing via rate adaptation,” in *Proc. of ICNC*, 2013. Article (CrossRef Link)

[15] Y. Pei, Y.-C. Liang, K. C. The, and K. H. Li, “Achieving cognitive and secure transmissions using multiple antennas,” in *Proc. of IEEE PIMRC*, 2009. Article (CrossRef Link)

[16] Y. Pei, Y.-C. Liang, K. C. The, and K. H. Li, “Secure communication over MISO cognitive ratio channels,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010. Article (CrossRef Link)

[17] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitve radio networks,” *IEEE Trans. Commun.* vol.61, no. 12, pp. 5103-5113, Dec. 2013. Article (CrossRef Link)

[18] Y. Wu and K. Liu, “An information secrecy game in cognitive radio networks,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sept. 2011. Article (CrossRef Link)

[19] P. N. Son and H. Y. Kong, “The underlay cooperative cognitive network with secure transmission,” *Communications (QBSC), 27th Biennial Symposium on*, pp. 164 - 167, June 2014. Article (CrossRef Link)

[20] 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. 2013. Article (CrossRef Link)

[21] 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. Article (CrossRef Link)

[22] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive ratio networks," *IET Commun.*, vol. 6, iss. 16, pp. 2676-2687, Jun. 2012. Article (CrossRef Link)

[23] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011. Article (CrossRef Link)

[24] H. –M. Wang, M. Luo, X. –G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE signal process. Lett.*, vol. 20, no. 1, pp. 39-42, Jan. 2013. Article (CrossRef Link)

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

[26] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011. Article (CrossRef Link)

[27] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099 - 2111, Oct. 2013. Article (CrossRef Link)

[28] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products, 7th edition*. Academic Press, San Diego, 2007. http://www.scirp.org/reference/ReferencesPapers.aspx? ReferenceID=697112

[29] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.* vol.61, no. 1, pp. 144-154, Jan. 2013. Article (CrossRef Link)

[30] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no.5, pp. 1073-1096, May 2003. Article (CrossRef Link)

Songqing Wang is currently working toward the Ph. D. degree at PLA University of Science and Technology. His research interests include physical layer security, cooperative communications, and cognitive radio.

Xiaoming Xu is currently studying at PLA University of Science and Technology for his Ph. D. degree. He focuses on researching in physical layer security, simultane ous wireless information and power transfer, and cooperative cognitive networks.

Weiwei Yang received his ph. D. degree in 2011 at PLA University of Science and Technology. He is currently an associate professor in PLA University of Science and Technology. His research focuses on OFDM, channel estimation, in physical layer security, simultaneous wireless information and power transfer, cooperative communications, and cognitive radio.