Wireless Netw (2018) 24:911–923
https://doi.org/10.1007/s11276-016-1378-9

Relay selection schemes for secure transmission in cognitive radio networks

Mukarram Al-jamali[1] · **Azzam Al-nahari**[2] · **Mohammed AlKhawlani**[1]

Published online: 13 October 2016

Abstract The security in cognitive radio networks (CRNs) has been attracting continuously growing attention due to the open and dynamic nature of cognitive radio architecture. In this paper, we propose new relay selection schemes to improve the physical layer security in CRNs. A trusted decode-and-forward relay is selected to help the secondary user (SU) transmission and improve the secrecy rate in the presence of multiple eavesdroppers and multiple primary users (PUs). The secrecy rate of the SU is characterized under both its own transmit power constraint as well as a set of interference power constraints imposed at each PU, in order to preserve its quality of service. The performance of the proposed schemes is analyzed in terms of the achievable secrecy rate and the intercept probability. Closed form expressions for the asymptotic intercept probability at high source-relays channel variances are also derived. Moreover, new derivations of some existing traditional schemes are presented and compared. The performance comparison of the proposed schemes with the schemes proposed in the literature reveals the superior of the proposed schemes.

✉ Azzam Al-nahari
azzamyn@gmail.com

Mukarram Al-jamali
mukarramja@gmail.com

Mohammed AlKhawlani
m.alshadadi@ust.edu

[1] Department of Electronics Engineering, University of Science and Technology, Sanaa, Yemen

[2] Department of Electrical Engineering, Ibb University, Ibb, Yemen

Keywords Cognitive radio · Relay selection · Physical layer security · Secrecy rate · Intercept probability

1 Introduction

Cognitive radio (CR) is a technology that allows the unlicensed user to access the licensed channels dedicated to a primary user (PU) without causing interference to the PU. There are two main characteristics of cognitive radios. The first is cognitive capability, which refers to the ability of the radio technology to sense information from its radio environment. The second is re-configurability, which enables a user to change the transmitting channel quickly and adaptively according to the radio environment [1]. There are three main different approaches by which secondary user (SU) access spectrum without interfering with the PU. These approaches include underlay, overlay and interweave paradigms [2]. In the underlay paradigm, SUs are allowed to operate only if their interference to the PUs is below a certain threshold. While operating in the overlay paradigm, the SUs transmit their data simultaneously with the PUs but employ sophisticated techniques that maintain (or even improve) the performance of PUs. In the interweave, the SUs sense unused frequency bands called spectrum holes to communicate without disrupting primary transmissions.

Since CR system is open and dynamic in nature, where various unknown wireless devices are allowed to opportunistically access the licensed spectrum, this make them more vulnerable to attack. The traditional security is based on cryptographic approaches; these techniques rely on secret keys and introduce additional complexities due to the dynamic distribution and management of secret key. Physical layer security paradigm is used to prevent the

eavesdropper attack and assure the secure communication by exploiting the physical characteristic of wireless channel. This work was first studied by Shannon in [3] and extended by Wyner in [4], where a so-called secrecy rate is defined as the rate at which information can be transmitted confidently from a source to its intended destination. The maximum achievable secrecy rate is named the secrecy capacity [5]. To improve the physical-layer security of wireless transmissions, some recent work was proposed by exploiting the multiple-input multiple-output (MIMO) techniques [6–8], and cooperative relays [9–11].

Although physical layer security in classic wireless networks has been studied for many years, security in the physical layer of CRNs has not been investigated until recently [12–19]. Many types of attacks have been addressed in the physical layer of CRNs; namely, PU emulation (PUE), spectrum sensing data falsification (SSDF), objective function attack (OFA), jamming attack and eavesdropping attack [12]. In [13] and [14], the two classes of attacks, PUE attack and OFA were studied. The achievable secrecy rates in CRNs with external eavesdroppers have been studied in [15] and [16]. In [17], the physical layer security against eavesdropping in the CRN was investigated by introducing the multiuser scheduling scheme to achieve multiuser diversity for improving the security level of cognitive transmissions with a PU quality of service (QoS) constraint. A relay selection scheme for secrecy-constrained CRNs was proposed in [18], which studied the maximization of the achievable secrecy rate that is subjected to the interference power constraints at the PUs for different numbers of eavesdroppers and PUs, under available channel state information (CSI) assumption. For relay selection schemes in [18], the source and relay nodes transmit at maximum power and the selection process depends on the QoS requirements of the PUs. This will affect the secrecy performance especially at high transmitted power values. Moreover, a unified manner with more general system model is required to improve the secrecy performance. Particularly, relay selection schemes with power scaling at the transmission side is required to compromise the achievable secrecy rate and at the same time satisfy the required QoS at the PU, which will be investigated in this paper.

In this paper, we study secure transmission in cooperative CRNs in the presence of multiple PUs, and multiple eavesdroppers, which attempt to intercept the signal transmitted from the SU to the legitimate receiver in the CRN. The contributions of the paper are summarized as follows. Firstly, we propose new relay selection schemes to improve the physical layer security of underlay cognitive transmission in presence of multiple eavesdroppers. The effect of the presence of multiple PUs is also investigated. The proposed selection schemes consider two power constraints; transmit power constraint at both the SU and the selected relay, and received interference power constraints at the PUs. The QoS at the PUs is considered by limiting the transmitted power of the SU and the selected relay such that the interference received at each PU does not exceed a predefined interference threshold. Decode and forward (DF) relying is assumed, where one relay is selected to help forward the decoded signal to the intended receiver. Two performance metrics are considered; the achievable secrecy rate and the intercept probability. We derive closed form expressions for the asymptotic intercept probability under the assumption of high source-relays channel variances at which all relays decode the transmitted message correctly. Secondly, we investigate the traditional relay selection schemes and the scheme proposed in [18] for the comparison purpose, and new expressions of the asymptotic intercept probability for some traditional schemes that are related to the proposed scheme are derived. The performance of the proposed schemes is compared with the conventional relay selection schemes and the relay selection scheme proposed in [18].

The remainder of this paper is organized as follows. In Sect. 2, the system and channel models are introduced. In Sect. 3, the performance analysis of the proposed relay selection schemes in terms of the achievable secrecy rate and intercept probability is presented; the asymptotic intercept probabilities are also derived. The conventional relay selection schemes and their performance analysis are presented in Sect. 4. Simulation and numerical results are presented and discussed in Sect. 5. Section 6 gives the concluding remarks.

Throughout the paper, the following notations are used. For the set $\mathcal{A}$, $|\mathcal{A}|$ denotes the cardinality of this set. $[x]^+ = \max(0, x)$. Furthermore, $\underline{X}$ denotes a lower bound for X, and $\triangleq$ denotes equals by definition. Finally, we use $x \sim \mathcal{CN}(0, \sigma^2)$ to denote a circularly symmetric complex Gaussian random variable with zero-mean and varianceσ^2.

2 System and channel models

We consider a CRN model as shown in Fig. 1, where a single-antenna SU transmitter (SU-TX) sends confidential information to a legitimate SU receiver (SU-RX), in the presence of K single-antenna PUs, L eavesdroppers, and a set of N relay nodes. For notational convenience, N relays, L eavesdroppers, and K PUs are denoted by the sets $\mathcal{R} = \{R_i | i = 1, 2, \ldots, N\}$, $\mathcal{E} = \{E_j | j = 1, 2, \ldots, L\}$, and $\mathcal{P} = \{p_k | i = 1, 2, \ldots, K\}$, respectively. We also define the decoding set $\mathcal{D}$, which contains the relay nodes that have decoded correctly the received message from the source in the first phase. A cognitive network with underlay

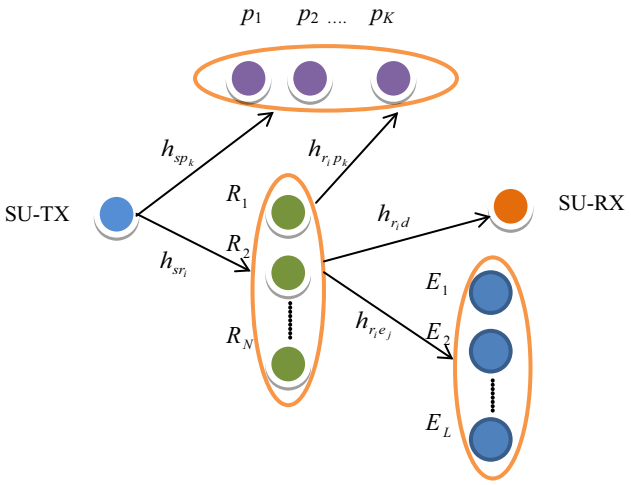

Fig. 1 System model

spectrum sharing which allows concurrent transmission from the PU and the SU simultaneously in the same spectrum band is assumed. We assume that the source has no direct link with the destination and eavesdroppers, i.e., the direct links are in deep shadowing, and the communication is carried out through a reactive DF relays [20, 21]. Moreover, considering the direct link from the source to the destination and eavesdroppers is straightforward extension of this system model, but our main concern here is to investigate the effect of relay selection in enhancing the secrecy performance. In addition, we consider the CSI of the main, primary, and eavesdropper links are available; this is a common assumption in the literature of information-theoretic physical layer security [9, 20]. A slow, flat, block Rayleigh fading is assumed, where the channel remains static for one coherence interval (one slot) and changes independently in different coherence intervals with a variance $\sigma_{ij}^2 = d_{ij}^{-\alpha}$ where $d_{i,j}^{-\alpha}$ is the Euclidean distance between the nodes i and j, and α is the path loss exponent. The fading coefficienth_{ij}between the nodes i and j is distributed as circularly symmetric complex Gaussian random variable with zero-mean and a variance σ_{ij}^2.

Based on the DF protocol, there are two phases in the transmission from the SU-TX to the SU-RX. In the first phase, the source broadcasts its message to the trusted relays. The received signal at the ith relay is given by

$$y_{r_i} = \sqrt{P_s} h_{sr_i} x + z_{r_i} \tag{1}$$

where P_s is the transmitted power at the SU-TX and h_{sr_i} is the fading coefficient of the channel from the source to the ith relay. $x$denotes the transmitted symbol from the source and $z_{r_i} \sim \mathcal{CN}(0, N_{r_i})$ represents the additive white Gaussian noise (AWGN) at the ith relay. The received signal at the kth PU in the first phase is given by

$$y_{p_k}^1 = \sqrt{P_s} h_{sp_k} x + z_{p_k} \tag{2}$$

where h_{sp_k} represents the fading coefficient of the channel from the source to the kth PU and $z_{p_k} \sim \mathcal{CN}(0, N_{p_k})$ represents AWGN. In order to protect the PU, the interference received at the PU shall be guaranteed not to exceed the maximum threshold limit denoted by I. Therefore, the transmitted power P_s should be varied according to the source-primary channel as will be described later.

In the second phase, one of the trusted relays that successfully decoded the message in the first phase is selected to retransmit the signal to the destination. The transmitted signal is also overheard by the eavesdropper due to wireless broadcasting. Considering that the ith relay is selected, the received signals at the destination and eavesdroppers are given by

$$y_d = \sqrt{P_{r_i}} h_{r_i d} x + z_d \tag{3}$$

$$y_{e_j} = \sqrt{P_{r_i}} h_{r_i e_j} x + z_{e_j} \tag{4}$$

where P_{r_i} denotes the transmitted power of the selected relay. $h_{r_i d}$ and $h_{r_i e_j}$ are the fading coefficients of the channels from selected relay to the destination (the main channel), and from selected relay to the jth eavesdropper (the wiretap channel), respectively. $z_d \sim \mathcal{CN}(0, N_d)$ and $z_{e_j} \sim \mathcal{CN}(0, N_{e_j})$ are AWGN at the destination and the jth eavesdroppers, respectively. The received signal at the kth PU is given by

$$y_{p_k}^2 = \sqrt{P_{r_i}} h_{r_i p_k} x + z_{p_k} \tag{5}$$

where $h_{r_i p_k}$ is the fading coefficient of the channel from the selected relay to the kth PU, and $z_{p_k} \sim \mathcal{CN}(0, N_{p_k})$. It should be noted that in (1)–(5), both P_s, and P_{r_i} should be adjusted in every transmitted block according to the channel condition between the SU and the PU.

3 The proposed relay selection schemes

In this section, we present the proposed relay selection schemes to improve the physical-layer security of CRNs and analyze their performance in terms of the achievable secrecy rate and intercept probability with single and multi-eavesdroppers. Furthermore, we analyze their performance considering the presence of one and multiple PUs.

3.1 Proposed relay selection scheme with single eavesdropper (SE)

In this case, we consider single eavesdropper and single PU. The objective of the proposed selection scheme is to select the relay node that maximizes the achievable secrecy rate

and at the same time keep the received interference power at the PU below a threshold level I. Therefore, we propose to limit the transmitted power at the source node in accordance to this allowed interference threshold as follows

$$P_s = \min\left(P, \frac{I}{|h_{sp}|^2}\right) \tag{6}$$

where P is the maximum power budget at the SU-TX and h_{sp} is the fading coefficient from the source to the PU. Note that the transmitted power is a random variable but is limited by the maximum transmitted power P. Using (6), the received interference at the PU can be ensured not to exceed I. Without loss of generality, we assume that the maximum transmitted power at any relay node is P. Therefore, the transmitted power of the relay R_i is given by

$$P_{r_i} = \min\left(P, \frac{I}{|h_{r_iP}|^2}\right) \tag{7}$$

The instantaneous achievable secrecy rate when the ith relay is selected is defined as [20]

$$C_{S,SE}(R_i) = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{r_id}}{1+\gamma_{r_ie}}\right)\right]^+ \tag{8}$$

where, $\gamma_{r_id} \triangleq \frac{P_{r_i}|h_{r_id}|^2}{N_d}$ and $\gamma_{r_ie} \triangleq \frac{P_{r_i}|h_{r_ie}|^2}{N_e}$ represent the signal to noise ratios (SNRs) at the SU-RX and eavesdropper, respectively. The objective is to select a relay from the decoding set $\mathcal{D}$ that maximizes the secrecy rate given in (8) as follows

$$\text{BestRelay} = \arg\max_{R_i \in \mathcal{D}} C_{S,SE}(R_i) \tag{9}$$

Hence, the achievable secrecy rate of the proposed scheme is given as

$$\begin{aligned} C_{S,SE}^{prop} &= \max_{R_i \in \mathcal{D}} C_{S,SE}(R_i) \\ &= \max_{R_i \in \mathcal{D}} \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\min\left(\mathrm{P},\mathrm{I}/|\mathrm{h_{r_iP}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d}}{1+\frac{\min\left(\mathrm{P},\mathrm{I}/|\mathrm{h_{r_iP}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_e}}\right)\right]^+ \end{aligned} \tag{10}$$

Finding closed form expression of the ergodic achievable secrecy rate for (10) requires solving high dimensional integrals, which is cumbersome. However, the ergodic achievable secrecy rate can be solved easily using computer simulation.

3.1.1 Asymptotic intercept probability analysis

We introduce the intercept probability as another performance metric for the proposed schemes. The intercept probability is defined as the probability that the secrecy rate is less than zero [10, 17]. In other words, the intercept event occurs when the wiretap link is better than that the main link (i.e. when the achievable secrecy rate becomes negative). Therefore, the intercept probability in this case is given as [20]

$$P_{\text{int,SE}}^{prop} = \sum_{n=1}^{N} \Pr\{|\mathcal{D}| = n\}\left[\Pr\{C_{S,SE}^{prop} < 0\} \,|\, |\mathcal{D}| = n\right] \tag{11}$$

where $C_{S,SE}^{prop}$ is the rate given in (10). For simplicity of analysis, we drive an asymptotic intercept probability under the assumption that all relay nodes decode the received signals correctly in the first phase.[1] As the transmit power is a random variable, we assume high source-relays channel variances to ensure correct decoding of all relays. In this case, all relays are assumed to decode the signal that is transmitted from SU-TX correctly so that $\Pr\{|\mathcal{D}| = N\} = 1$, and hence, the intercept probability in (11) becomes $P_{\text{int,SE}}^{prop} = \Pr\{C_{S,SE}^{prop} < 0\}$. Considering (9) and (10) and assuming that $N_d = N_e$, the asymptotic intercept probability of the proposed scheme for one realization of the rate $C_{S,SE}(R_i)$ given in (8), which correspond to the ith relay is given as

$$\begin{aligned} P_{\text{int,SE}} &= \Pr\{C_{S,SE}(R_i) < 0\} \\ &= \Pr\left\{1 + \frac{\min\left(\mathrm{P},\mathrm{I}/|\mathrm{h_{r_iP}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d} < 1 \right. \\ &\quad \left. + \frac{\min\left(\mathrm{P},\mathrm{I}/|\mathrm{h_{r_iP}}|^2\right)|\mathrm{h_{r_ie}}|^2}{N_e}\right\} \\ &= \Pr\left\{|h_{r_id}|^2 < |h_{r_ie}|^2\right\} \end{aligned} \tag{12}$$

Note that the intercept probability does not depend on the transmitted power. Define $X_1 \triangleq |h_{r_id}|^2$, and $X_2 \triangleq |h_{r_ie}|^2$. Note that both $X_1$and X_2 are independent exponentially distributed random variables, with means $\sigma_{r_id}^2$, and $\sigma_{r_ie}^2$, respectively. Therefore, (12) is given as

$$\begin{aligned} P_{\text{int,SE}} &= \int_0^\infty F_{X_1}(x_2) f_{X_2}(x_2) dx_2 \\ &= \frac{1}{\sigma_{r_ie}^2}\int_0^\infty (1 - e^{-\frac{x_2}{\sigma_{r_id}^2}}) e^{-\frac{x_2}{\sigma_{r_ie}^2}} dx_2 \\ &= \frac{\sigma_{r_ie}^2}{\sigma_{r_id}^2 + \sigma_{r_ie}^2} \end{aligned} \tag{13}$$

Using the order statistics [22], for the N independent realizations of the random variables $C_{S,SE}(R_i)$, $i = 1, 2, \ldots, N$, the asymptotic intercept probability is given as

[1] It should be noted that in [9] and [10] all relays are assumed to decode correctly , and the derived expressions of the intercept probability are considered exact . Our case is more general as we consider $|\mathcal{D}| = N$ an asymptotic case. So, the derived expressions are considered asymptotic according to this assumption.

$$P_{\text{int,SE}}^{prop} = \Pr\left\{\max_{R_i\in\mathcal{D}} C_{S,SE}(R_i)\right\} = \prod_{i=1}^{N}\frac{\sigma_{r_ie}^2}{\sigma_{r_id}^2+\sigma_{r_ie}^2} \tag{14}$$

3.2 Proposed relay selection with multiple eavesdroppers (ME)

In this case, we consider L eavesdroppers that try to decode the information intended for the SU independently, without cooperation between them. The worst case, which represents choosing the eavesdropper that can achieve the maximum rate, is considered. Therefore, the overall rate of the wiretap links is the maximum of individual rates achieved at Leavesdroppers. Hence, the instantaneous achievable secrecy rate when selecting the relay R_i is given as

$$C_{S,ME}(R_i) = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{r_id}}{1+\max\limits_{E_j\in\mathcal{E}}\gamma_{r_ie_j}}\right)\right]^+ \tag{15}$$

where $\gamma_{r_ie_j}$ is the SNR at the jth eavesdropper. The objective is to select the relay that maximizes the rate given in (15) as follows

$$\text{BestRelay} = \arg\max_{R_i\in\mathcal{D}} C_{S,ME}(R_i) \tag{16}$$

Hence, the achievable secrecy rate of the proposed scheme with multiple eavesdroppers is given by

$$C_{S,ME}^{prop} = \max_{R_i\in\mathcal{D}}\left[\frac{1}{2}\log_2\left[\frac{1+\frac{\min\left(\mathrm{P},\mathrm{I}/|\mathrm{h_{r_ip}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d}}{1+\frac{\min\left(\mathrm{P},\mathrm{I}/|\mathrm{h_{r_ip}}|^2\right)\max\limits_{\mathrm{E_j}\in\mathcal{E}}|\mathrm{h_{r_ie_j}}|^2}{N_e}}\right]\right]^+ \tag{17}$$

The achievable ergodic secrecy rate of (17) can be obtained through computer simulations.

3.2.1 Asymptotic intercept probability analysis

We drive an asymptotic intercept probability when multiple eavesdroppers try to decode the message. Following similar assumptions in the previous subsection, the intercept probability of the rate given in (15) is given by

$$\begin{aligned} P_{\text{int,ME}} &= \Pr\left\{1+\frac{\min\left(\mathrm{P},\mathrm{I}\Big/|\mathrm{h_{r_ip}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d} < 1 + \frac{\min\left(\mathrm{P},\mathrm{I}\Big/|\mathrm{h_{r_ip}}|^2\right)\max\limits_{\mathrm{E_j}\in\mathcal{E}}|\mathrm{h_{r_ie_j}}|^2}{N_e}\right\} \\ &= \Pr\left\{|h_{r_id}|^2 < \max_{E_j\in\mathcal{E}}|h_{r_ie_j}|^2\right\} \end{aligned} \tag{18}$$

The random variable $|h_{r_id}|^2$ is exponential distributed with mean $\sigma_{r_id}^2$. Define $X \triangleq \max\limits_{E_j\in\mathcal{E}}|h_{r_ie_j}|^2$; the cumulative distribution function (CDF) and the probability density function (PDF) of the random variable X, considering order statistics, are given as

$$F_X(x) = \prod_{j=1}^{L}\left(1-\exp\left(-\frac{x}{\sigma_{r_ie_j}^2}\right)\right) \tag{19}$$

$$f_X(x) = \sum_{j=1}^{L}\frac{1}{\sigma_{r_ie_j}^2}\exp\left(-\frac{x}{\sigma_{r_ie_j}^2}\right)\prod_{n=1,n\neq j}^{L}\left(1-\exp\left(-\frac{x}{\sigma_{r_ie_n}^2}\right)\right) \tag{20}$$

So, the intercept probability in (18) is calculated by averaging the CDF of $|h_{r_id}|^2$ over the PDF of X, given in (20), as follows

$$P_{\text{int,ME}} = \int_0^\infty\left(1-\exp\left(-\frac{x}{\sigma_{r_id}^2}\right)\right)\sum_{j=1}^{L}\frac{1}{\sigma_{r_ie_j}^2}\exp\left(-\frac{x}{\sigma_{r_ie_j}^2}\right)\prod_{n=1,n\neq j}^{L}\left(1-\exp\left(-\frac{x}{\sigma_{r_ie_n}^2}\right)\right)dx \tag{21}$$

The product term in (21) can be expanded using the binomial theorem as

$$\prod_{n=1,n\neq j}^{L}\left(1-\exp\left(-\frac{x}{\sigma_{r_ie_n}^2}\right)\right) = 1+\sum_{k=1,k\neq j}^{2^L-2}(-1)^{|\mathcal{E}_k|}\exp\left(-\sum_{E_n\in\mathcal{E}_k}\frac{x}{\sigma_{r_ie_n}^2}\right) \tag{22}$$

where, $\mathcal{E}_k$ is the kth nonempty subset of L eavesdroppers, excluding the subset when $k=j$, and $|\mathcal{E}_k|$ represents the cardinality of set $\mathcal{E}_k$. Substituting (22) into (21) and performing the integration by changing the order of summations and integration, it can easily be shown that

$$P_{\text{int,ME}} = 1-\sum_{j=1}^{L}\left(\frac{\sigma_{r_id}^2}{\sigma_{r_id}^2+\sigma_{r_ie_j}^2}\right) - \sum_{j=1}^{L}\sum_{k=1,k\neq j}^{2^L-2}\frac{(-1)^{|\mathcal{E}_k|}}{\left(1+\frac{\sigma_{r_ie_j}^2}{\sigma_{r_id}^2}+\sum_{E_n\in\mathcal{E}_k}\frac{\sigma_{r_ie_j}^2}{\sigma_{r_ie_n}^2}\right)} \tag{23}$$

The intercept probability of the rate given in (17) can be obtained using the order of statistics as

$$P_{\text{int,ME}}^{prop} = \prod_{i=1}^{N}\left(1-\sum_{j=1}^{L}\left(\frac{\sigma_{r_id}^2}{\sigma_{r_id}^2+\sigma_{r_ie_j}^2}\right) - \sum_{j=1}^{L}\sum_{k=1,k\neq j}^{2^L-2}\frac{(-1)^{|\mathcal{E}_k|}}{\left(1+\frac{\sigma_{r_ie_j}^2}{\sigma_{r_id}^2}+\sum_{E_n\in\mathcal{E}_k}\frac{\sigma_{r_ie_j}^2}{\sigma_{r_ie_n}^2}\right)}\right) \tag{24}$$

Note that for $L = 1$, (24) reduces to (14) for the case of single eavesdropper.

3.3 Proposed relay selection with multiple primary users (MP)

In this case, K PUs and one eavesdropper are considered. The objective is to investigate the effect of the presence of multiple PUs on the achievable secrecy rate and the intercept probability. Presence of multiple PUs will certainly add more constraints on the transmitted power at the SU-TX and the selected relay. Therefore, in order to limit the transmitted power at SU-TX in accordance to the allowed interference threshold I at each PU, the transmitted power at SU-X, and the ith selected relay will be

$$P_{s,MP} = \min\left(P, \min_{p_k \in \mathcal{P}} \frac{I}{|h_{sp_k}|^2}\right), \tag{25}$$

$$P_{r,MP} = \min\left(P, \min_{p_k \in \mathcal{P}} \frac{I}{|h_{r_i p_k}|^2}\right), \tag{26}$$

respectively. The instantaneous achievable secrecy rate with the relay R_i is given as

$$C_{S,MP}(R_i) = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{r_i d}}{1+\gamma_{r_i e}}\right)\right]^+ \tag{27}$$

where $\gamma_{r_i d} = \frac{P_{r_i,MP}|h_{r_i d}|^2}{N_d}$, and $\gamma_{r_i e} = \frac{P_{r_i,MP}|h_{r_i e}|^2}{N_e}$ represent the SNRs at the destination and eavesdropper, respectively. The objective is to select the relay that maximizes the rate given in (27) as follows

$$\text{BestRelay} = \arg\max_{R_i \in \mathcal{D}} C_{S,MP}(R_i) \tag{28}$$

Hence, the achievable secrecy rate of the proposed scheme with multiple PUs is given as

$$C^{prop}_{S,MP} = \max_{R_i \in \mathcal{D}} \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\min\left(\mathrm{P}, \min\limits_{\mathrm{p_k}\in\mathcal{P}} \mathrm{I}/|\mathrm{h_{r_i p_k}}|^2\right)|\mathrm{h_{r_i d}}|^2}{N_d}}{1+\frac{\min\left(\mathrm{P}, \min\limits_{\mathrm{p_k}\in\mathcal{P}} \mathrm{I}/|\mathrm{h_{r_i p_k}}|^2\right)|\mathrm{h_{r_i e}}|^2}{N_e}}\right)\right]^+ \tag{29}$$

3.3.1 Asymptotic intercept probability analysis

We derive an asymptotic approximation of the intercept probability when multiple PUs are considered. The PUs are protected from the interference through limiting the transmitted power at the SU-TX and relays as in (25) and (26). Considering the same assumptions mentioned before, the intercept probability of one realization of the achievable secrecy rate corresponding to the ith relay is given by

$$\begin{aligned} P_{\text{int,MP}} &= \Pr\left\{1 + \frac{\min\left(\mathrm{P}, \min\limits_{\mathrm{p_k}\in\mathcal{P}} \mathrm{I}/|\mathrm{h_{r_i p_k}}|^2\right)|\mathrm{h_{r_i d}}|^2}{N_d} < 1 \right. \\ &\qquad \left. + \frac{\min\left(\mathrm{P}, \min\limits_{\mathrm{P_k}\in\mathcal{P}} \mathrm{I}/|\mathrm{h_{r_i p_k}}|^2\right)|\mathrm{h_{r_i e}}|^2}{N_e}\right\} \\ &= \Pr\left\{|h_{r_i d}|^2 < |h_{r_i e}|^2\right\} \end{aligned} \tag{30}$$

which is the same as (12). So, the intercept probability of the multiple PUs case is given as

$$P^{prop}_{\text{int,MP}} = \prod_{i=1}^{N} \frac{\sigma^2_{r_i e}}{\sigma^2_{r_i d} + \sigma^2_{r_i e}} \tag{31}$$

Interestingly, the asymptotic intercept probabilities of the proposed scheme with single and multi PUs are the same. This can be interpreted as follows. In our system model, the performance enhancement is due to the selection process. In the asymptotic case, all relays decode the received signals correctly and hence belong to the decoding set, and the performance start to saturates either for the secrecy rate or the intercept probability as will be shown in Sect. 5. Therefore, the presence of multiple PUs will only limit the transmitted power. As the asymptotic intercept probability does not depend on the transmitted power, its performance with single and multiple PUs is the same. This will also be confirmed in Sect. 5 via simulations.

4 The conventional relay selection schemes

In this section, for the comparison purpose, we analyze the performance of the conventional relay selection schemes. However, we drive new closed-form expressions for the asymptotic intercept probability of these schemes.

4.1 Conventional selection (CS1) with single eavesdropper (SE)

In this scheme, the objective is to select the relay R_i that maximizes the achievable rate of the main link without considering the existence of the eavesdropper as follows

$$\text{BestRelay} = \arg\max_{R_i \in \mathcal{D}} \{\gamma_{r_i d}\} \tag{32}$$

In this case, the achievable secrecy rate of this scheme, which is denoted as CS1, is given as

$$C_{S,SE}^{CS1} = \left[\frac{1}{2}\log_2\left(\frac{1+\max\limits_{R_i\in\mathcal{D}}\gamma_{r_id}}{1+\gamma_{r_ie}}\right)\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\max\limits_{R_i\in\mathcal{D}}\frac{\min\left(\mathrm{P},\mathrm{I}\middle/|\mathrm{h_{r_ip}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d}}{1+\frac{\min\left(\mathrm{P},\mathrm{I}\middle/|\mathrm{h_{r_ip}}|^2\right)|\mathrm{h_{r_ie}}|^2}{N_e}}\right)\right]^+ \tag{33}$$

As before, we assume that $N_d = N_e$. Also, all relays are assumed to decode the signal that is transmitted from source correctly so that $\Pr\{|\mathcal{D}| = n\} = 1$. Therefore, the asymptotic intercept probability is given by

$$\begin{aligned} P_{\text{int,SE}}^{CS1} &= \Pr\left\{1+\max_{R_i\in\mathcal{D}}\frac{\min\left(\mathrm{P},\mathrm{I}\middle/|\mathrm{h_{r_ip}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d} < 1 + \frac{\min\left(\mathrm{P},\mathrm{I}\middle/|\mathrm{h_{r_ip}}|^2\right)|\mathrm{h_{r_ie}}|^2}{N_e}\right\} \\ &= \Pr\left\{\max_{R_i\in\mathcal{D}}\left\{\min\left(P,I\middle/|h_{r_ip}|^2\right)|h_{r_id}|^2\right\} < \min\left(P,I\middle/|h_{r_ip}|^2\right)|h_{r_ie}|^2\right\} \end{aligned} \tag{34}$$

A closed form solution for the intercept probability in (34) is difficult. Therefore, a numerical intercept probability is done through computer simulation. However, a lower bound on the intercept probability can be obtained by performing the maximization in the left-hand side of the inequality in (34) only over the random variables $|h_{r_id}|^2$,$i = 1, 2, \ldots, N$. In this way, we obtain a lower bound on the asymptotic intercept probability as follows

$$\begin{aligned} \underline{P}_{\text{int,SE}}^{CS1} &= \Pr\left\{\max_{R_i\in\mathcal{D}}|h_{r_id}|^2 < |h_{r_ie}|^2\right\} \\ &= \int_0^\infty \prod_{i=1}^{N}\left(1-\exp\left(-\frac{x}{\sigma_{r_id}^2}\right)\right)\frac{1}{\sigma_{r_ie}^2}\exp\left(-\frac{x}{\sigma_{r_ie}^2}\right)dx \end{aligned} \tag{35}$$

Using the binomial expansion theorem, the product term in (35) is expressed as

$$\prod_{i=1}^{N}\left(1-\exp\left(-\frac{x}{\sigma_{r_id}^2}\right)\right) = 1+\sum_{n=1}^{2^N-1}(-1)^{|\mathcal{R}_n|}\exp\left(-\sum_{R_i\in\mathcal{R}_n}\frac{x}{\sigma_{r_id}^2}\right) \tag{36}$$

where $\mathcal{R}_n$ is the nth non-empty subset of N relays. Substituting (36) into (35) and performing the integration yield

$$\underline{P}_{\text{int,SE}}^{CS1} = 1+\sum_{n=1}^{2^N-1}\frac{(-1)^{|\mathcal{R}_n|}}{1+\sum_{R_i\in\mathcal{R}_n}\frac{\sigma_{r_ie}^2}{\sigma_{r_nd}^2}} \tag{37}$$

4.2 Conventional selection (CS1) with multi eavesdroppers (ME)

With multiple eavesdroppers, the conventional scheme selects the relay that maximize the SNR at SU-RX regardless of the presence of the eavesdroppers as in (32). Regarding the wiretap link, the eavesdropper that achieves the maximum rate is considered. As a result, the achievable secrecy rate is given as

$$C_{S,ME}^{CS1} = \left[\frac{1}{2}\log_2\left(\frac{1+\max\limits_{R_i\in\mathcal{D}}\gamma_{r_id}}{1+\max\limits_{E_j\in\mathcal{E}}\gamma_{r_ie_j}}\right)\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\max\limits_{R_i\in\mathcal{D}}\frac{\min\left(\mathrm{P},\mathrm{I}\middle/|\mathrm{h_{r_ip}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d}}{1+\frac{\min\left(\mathrm{P},\mathrm{I}\middle/|\mathrm{h_{r_ip}}|^2\right)\max\limits_{\mathrm{E_j}\in\mathcal{E}}|\mathrm{h_{r_ie_j}}|^2}{N_e}}\right)\right]^+ \tag{38}$$

Note that the maximization over the SNRs of the wiretap links in (38) is reduced to the maximization over the channel coefficients $|h_{r_ie_j}|^2$, $j = 1, 2, \ldots, L$, because a relay is already selected to maximize the main link and the maximization here is over the eavesdroppers that achieve the maximum rate from the selected relay. As in the case of single eavesdropper, a lower bound on the asymptotic intercept probability in this case can be obtained as

$$\underline{P}_{\text{int,ME}}^{CS1} = \Pr\left\{\max_{R_i\in\mathcal{D}}|h_{r_id}|^2 < \max_{E_j\in\mathcal{E}}|h_{r_ie_j}|^2\right\} \tag{39}$$

Define $X \triangleq \max\limits_{E_j\in\mathcal{E}}|h_{r_ie_j}|^2$, and $Y \triangleq \max\limits_{R_i\in\mathcal{D}}|h_{r_id}|^2$; The CDF and PDF of both the random variables X and Y are given in (19), and (20), respectively. Therefore, the lower bound of the asymptotic intercept probability given in (39) is calculated as

$$\begin{aligned} \underline{P}_{\text{int,ME}}^{\text{CS1}} &= \int_0^\infty F_Y(x)f_X(x)dx \\ &= \int_0^\infty \prod_{i=1}^{N}\left(1-\exp\left(-\frac{x}{\sigma_{r_id}^2}\right)\right) \\ &\quad \sum_{j=1}^{L}\frac{1}{\sigma_{r_ie_j}^2}\exp\left(-\frac{x}{\sigma_{r_ie_j}^2}\right)\prod_{n=1,n\neq j}^{L}\left(1-\exp\left(-\frac{x}{\sigma_{r_ie_n}^2}\right)\right)dx \end{aligned} \tag{40}$$

Substituting the binomial expansions, given in (22) and (36), instead of the product terms in (40), and changing the orders of integrations and summations, it can be shown that

$$\begin{aligned} \underline{P}_{\text{int,ME}}^{\text{CS1}} &= 1+\sum_{j=1}^{L}\sum_{n=1}^{2^N-1}\frac{(-1)^{|\mathcal{R}_n|}}{1+\sum_{R_i\in\mathcal{R}_n}\frac{\sigma_{r_ie_j}^2}{\sigma_{r_id}^2}} \\ &\quad +\sum_{j=1}^{L}\sum_{n=1}^{2^N-1}\sum_{\substack{k=1,\\k\neq j}}^{2^L-2}\frac{(-1)^{|\mathcal{R}_n|}(-1)^{|\mathcal{E}_k|}}{1+\sum_{R_i\in\mathcal{R}_n}\frac{\sigma_{r_ie_j}^2}{\sigma_{r_id}^2}+\sum_{E_n\in\mathcal{E}_k}\frac{\sigma_{r_ie_j}^2}{\sigma_{r_ie_n}^2}} \end{aligned} \tag{41}$$

4.3 Conventional selection scheme (CS1) with multi primary users(MP)

In this case, we consider K PUs and one eavesdropper. The transmitted power at SU-TX and the ith relay are given in (25) and (26). Hence, the achievable secrecy rate in this case is given as

$$C_{S,MP}^{CS1} = \left[\frac{1}{2}\log_2\left(\frac{1+\max\limits_{R_i\in\mathcal{D}}\gamma_{r_id}}{1+\gamma_{r_ie}}\right)\right]^+ = \left[\frac{1}{2}\log_2\left(\frac{1+\max\limits_{R_i\in\mathcal{D}}\frac{\min\left(\mathrm{P},\min\limits_{\mathrm{p_k}\in\mathcal{P}}\mathrm{I}/|\mathrm{h_{r_ip_k}}|^2\right)|\mathrm{h_{r_id}}|^2}{N_d}}{1+\frac{\min\left(\mathrm{P},\min\limits_{\mathrm{p_k}\in\mathcal{P}}\mathrm{I}/|\mathrm{h_{r_ip_k}}|^2\right)|\mathrm{h_{r_ie}}|^2}{N_e}}\right)\right]^+ \tag{42}$$

Following the same assumptions as in the previous subsections, the asymptotic intercept probability in this case is given by

$$P_{\mathrm{int,MP}}^{CS1} = \Pr\left\{\max_{R_i\in\mathcal{D}}\left\{\min\left(P,\min_{p_k\in\mathcal{P}} I\Big/|h_{r_ip_k}|^2\right)|h_{r_id}|^2\right\} < \min\left(P,\min_{p_k\in\mathcal{P}} I\Big/|h_{r_ip_k}|^2\right)|h_{r_ie}|^2\right\} \tag{43}$$

A closed form solution for the intercept probability in (43) is cumbersome. However, a lower bound on the intercept probability can be obtained by maximizing over the relay-eavesdroppers channels, i. e, $\max\limits_{R_i\in\mathcal{D}}|h_{r_id}|^2$, as

$$\underline{P}_{\mathrm{int,MP}}^{CS1} = \Pr\left\{\max_{R_i\in\mathcal{D}}|h_{r_id}|^2 < |h_{r_ie}|^2\right\} \tag{44}$$

which is reduced to the problem in (35) with the case of single PU. So, the asymptotic intercept probability is given by

$$\underline{P}_{\mathrm{int,MP}}^{CS1} = 1 + \sum_{n=1}^{2^N-1}\frac{(-1)^{|\mathcal{R}_n|}}{1+\sum_{R_n\in\mathcal{R}_n}\sigma_{r_ie}^2\Big/\sigma_{r_nd}^2} \tag{45}$$

4.4 The selection scheme proposed in [18]

For the comparison purpose, we briefly introduce the selection scheme proposed in [18] which we denote as Scheme2. The achievable secrecy rate of this scheme with single eavesdropper and single PU is given as

$$C_{S,SE}^{Scheme2} = \max_{R_i\in\mathcal{D}}\left[\frac{1}{2}\log_2\left(\frac{1+\frac{P|h_{r_id}|^2}{N_d}}{1+\frac{P|h_{r_ie}|^2}{N_e}}\right)\right]^+ \quad \text{subject to} \quad INT \le I \tag{46}$$

where, INT is the interference received at the PU and expressed as $INT = N_p + P|h_{sp}|^2 + P|h_{r_ip}|^2$. Note that this scheme transmits with the maximum power P that is available at the SU-TX and the relay. The relay is selected subject to the constraint $INT \le I$; in the proposed scheme, a relay is always selected and the transmitted power is controlled according to the channel characteristics to the PU so that the interference received at the PU is always less than I. When L eavesdroppers is considered, the selection criteria (46) is used after replacing $|h_{r_ie}|^2$ with $\max\limits_{E_j\in\mathcal{E}}|h_{r_ie_j}|^2$. In the case of multiple PUs and one eavesdropper, the selection criteria for this scheme is given as in (46) but with the constraint $\max\limits_{p_k\in\mathcal{P}} INT_{p_k} \le I$; where $INT_{p_k} = N_{p_k} + P|h_{sp_k}|^2 + P|h_{r_ip_k}|^2$. The intercept probability for this scheme is defined as [18]

$$P_{\mathrm{int,SE}}^{Scheme2} = \sum_{n=1}^{N}\Big[\Pr\left\{\tilde{C}_{S,SE}^{Scheme2} < 0 \,||\mathcal{D}| = n\right\}\Pr\{|\mathcal{D}| = n\} \Pr\{INT \le I\} + \Pr\{INT \ge I\}\Big] \tag{47}$$

where $\tilde{C}_{S,SE}^{Scheme2}$ is the rate given in (46) without enforcing the rate to be more or equal to zero. When multiple eavesdroppers or multiple PUs are considered, (47) is modified according to the constrains discussed above.

5 Simulation results

In this section, we investigate the effectiveness of the proposed relay selection schemes via computer simulations that also validate the analytical results. We follow the system model shown in Fig. 1, and perform Monte Carlo simulation consisting of 40,000 independent trials to obtain the average result. The system parameters are as follows:

The SU-TX, $N = 4$relays, SU-RX, and $L = \{1, 2\}$ eavesdroppers are deployed in a two-dimensional unit-square area. The locations of SU-TX, and SU-RX are $\{X, Y\} = \{0, 0.5\}$ and $\{1, 0.5\}$, respectively. The locations of the eavesdroppers are $\{1, 0\}$ in case of single eavesdropper, and $\{1, 0\}$, $\{1, 1\}$ in case of two eavesdroppers. The relays are located at $\{0.5, 0.2\}$, $\{0.5, 0.4\}$, $\{0.5, 0.6\}$, $\{0.5, 0.8\}$. Moreover, the PU is located at $\{1, 3\}$ in case of single PU. In the case of two PUs, i.e. $K = 2$, we distinguish between two cases: (1) the second PU is farther than the first, located at $\{1, 4\}$ and (2) the second PU is closer than the first, located at $\{1, 2\}$.

The total interference temperature limit $I = -3$ dB. The path loss exponent $\alpha = 3$. The transmission rate

$R_0 = 2$bits/s/Hz, which represent the transmission rate of the SU-TX. A relay $R_i \in \mathcal{D}$ if its channel capacity with the SU-TX is larger than R_0. In all simulations, the maximum transmitted power at each relay is set at 10 dB.

Figure 2 shows the achievable ergodic secrecy rate versus the transmitted power budget Pat the SU-TX for the proposed scheme, the conventional scheme CS1, the scheme proposed in [18] which we denote as Scheme2, and the conventional scheme CS2, which also presented in [18] for the comparison purpose with Scheme2. It can be seen from the figure that the proposed scheme gives the best performance over the range of P. The case of multi-eavesdroppers is also shown on the figure. The achievable ergodic secrecy rate of the proposed scheme and CS1 scheme gradually increases with P before it saturates. Saturation occurs at high Pdue to one of the following reasoning: (1) at high transmitted power, all the relays may decode the signal correctly and more power will not further enhance the performance. (2) As the actual transmitted power are given in (6), (7), small values of the interference threshold I will restrict he transmitted power by the average value of the random variable $I/|h_{sp}|^2$ and the achievable rate saturate, although some of the relays do not belong to the decoding set. Note that with Scheme2, which transmit at the maximum power, the achievable ergodic secrecy rate starts to increase with Pbut further increase in the transmitted power will affect the selection process because the interference power at the PU increases. Therefore, the secrecy rate starts to decrease until it reaches zero at $P = 30$ dB. We also note that with $L = 2$, the achievable ergodic secrecy rate is degraded compared with one eavesdropper.

Figure 3 shows the intercept probability for the different schemes versus P. As shown, the proposed scheme gives the minimum intercept probability over all values of P. For Scheme2 and CS2, the intercept probability starts to decrease at low transmit power; however, further power increase will affect the selection process due to high interference at the PU. Therefore, the intercept probability starts to increase until it reaches 1 at $P = 30$ dB.

In order to investigate the asymptotic secrecy performance, where all the relays decodes the signal correctly, we plot the intercept probability against source-relays variances in Fig. 4 with $P = 10$ dB. The exact expressions of the asymptotic intercept probabilities for the different schemes are also shown in the figure . It can be seen that the analytical results matches well the simulation results. Note that the performance of Scheme2 and CS2 saturates at high source-relays channel variances with fixed transmit power, but at lower values compared to the proposed schemes.

Figure 5 shows the effect of the presence of two PUs located at {1, 3}, and {1, 4} on the achievable secrecy rate. The dotted lines represent the case of one PU located at {1, 3}. In this case, where the second PU is father than the first one, we note that the secrecy rate with one PU is slightly smaller than the case of two PUs. This is because

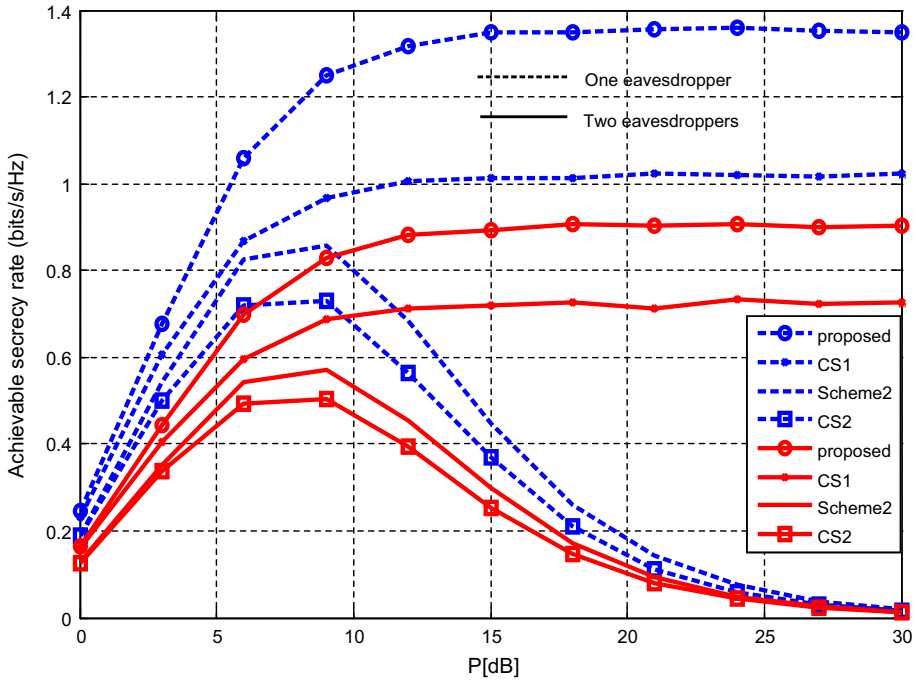

Fig. 2 Achievable ergodic secrecy rate versus power P, with single and multi-eavesdroppers. $N = 4$, $L = \{1, 2\}$, $K = 1$

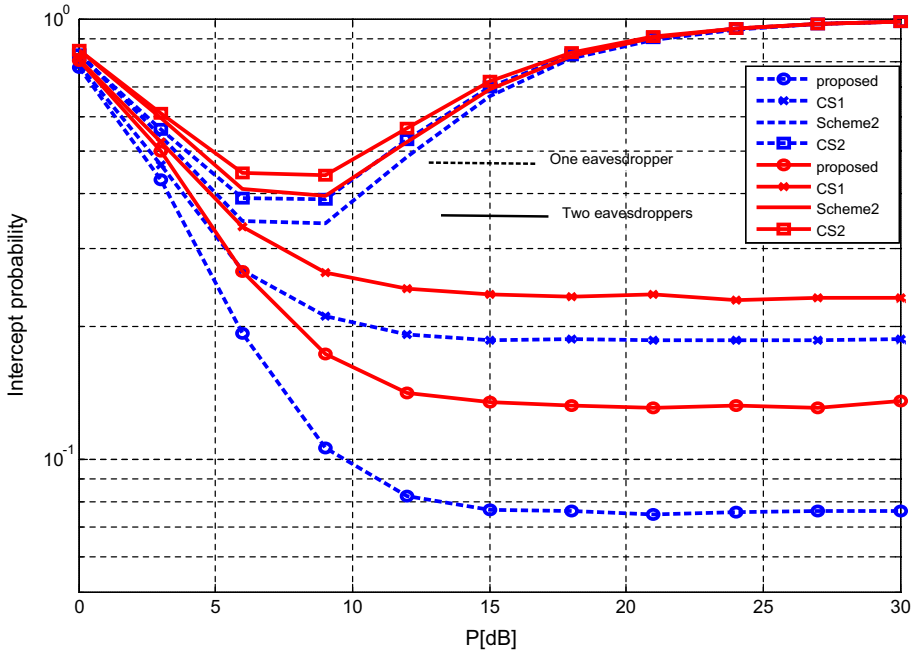

Fig. 3 The intercept probability versus power, with single and multi-eavesdroppers. $N = 4$, $L = \{1, 2\}$, $K = 1$

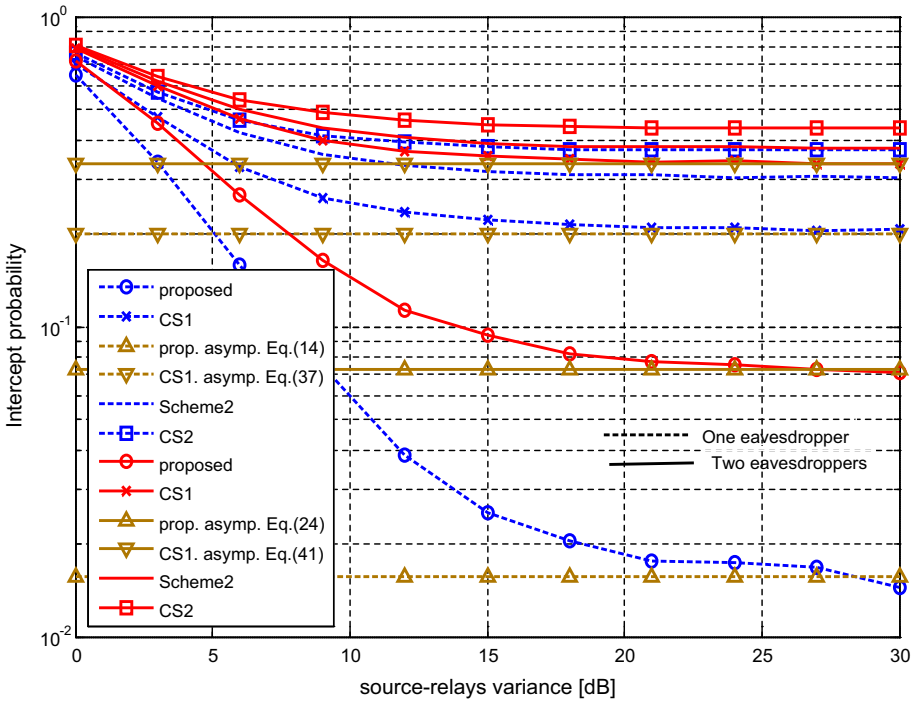

Fig. 4 The intercept probability versus source-relays variances, with single and multi-eavesdroppers, with $N = 4$, $L = \{1, 2\}$, $K = 1$

the power that causes the maximum allowed interference at the PUs is given according to (25) and (26). As the first PU is nearer to the SU-TX and the selected relay, it is more likely to be the dominant factor in selecting the transmitted power. In Fig. 6, the second PU is located at {1, 2}, closer to the SU-TX and the selected relay than the first PU located at {1, 3}. The achievable secrecy rate is lower than that with one PU as shown on the figure. The minimum transmitted power is selected to protect both PUs from interference and because the second is located closer than the first, It will be dominant PU and therefore, the secrecy rate decreases.

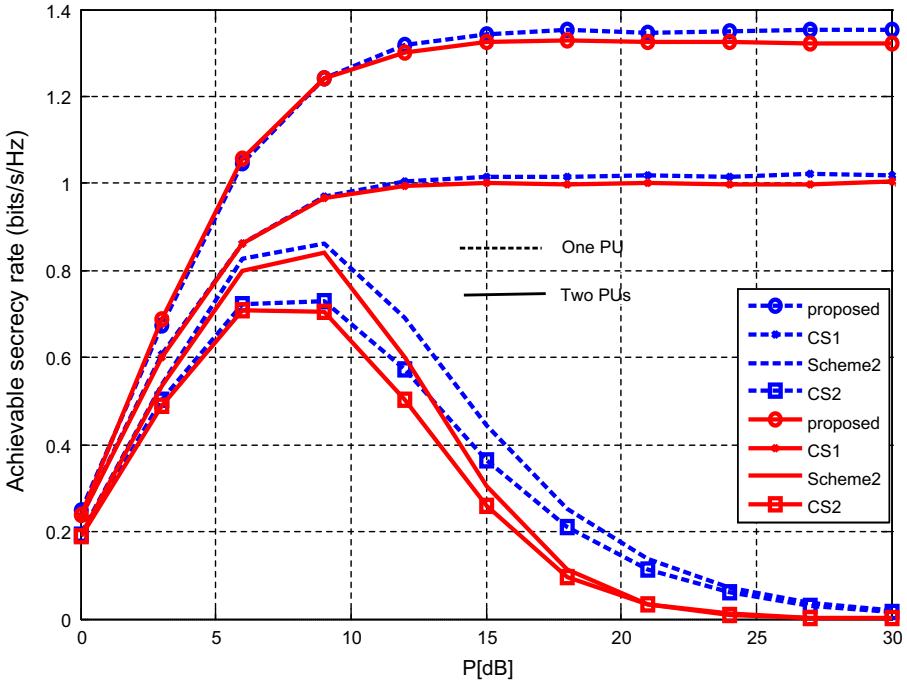

Fig. 5 Achievable ergodic secrecy rate versus power P, with single and two PUs. The two PUs are located at $\{1, 3\}$ and $\{1, 4\}$. $N = 4$, $L = 1$, $K = \{1, 2\}$

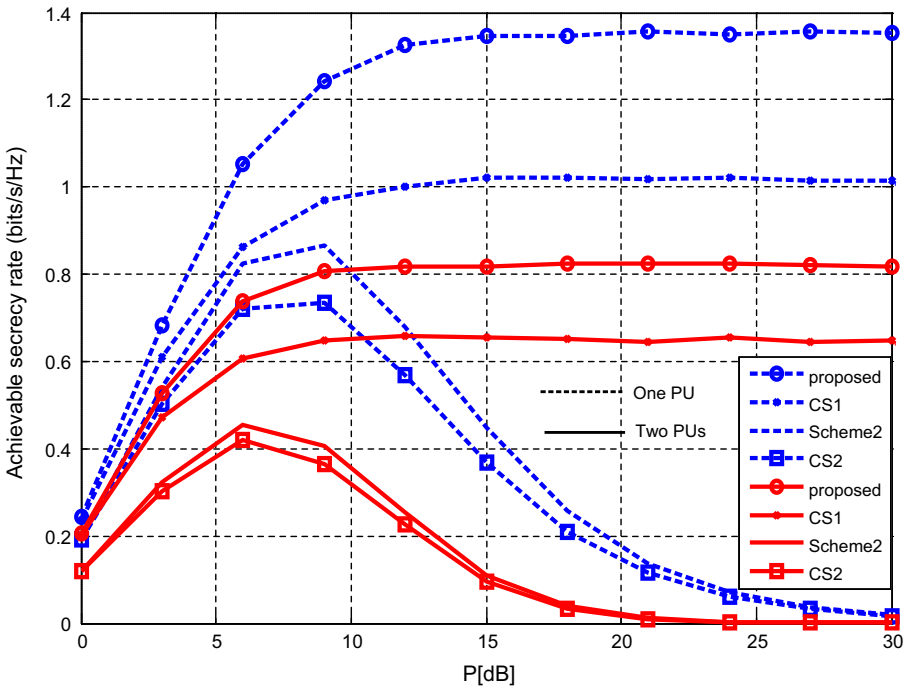

Fig. 6 Achievable ergodic secrecy rate versus power P, with single and two PUs. The two PUs are located at $\{1, 3\}$ and $\{1, 2\}$. $N = 4$, $L = 1$, $K = \{1, 2\}$

Finally, we plot the intercept probability for the different schemes versus the source-relays variances in cases of one and two PUs as shown in Fig. 7. The two PUs are located at $\{1, 3\}$, $\{1, 2\}$ and the transmitted power is set at $P = 10$ dB. It can be seen that at high source-relays variances, meaning that the SU-TX is very close to the relays and hence all relays are assumed to belong to the decoding set, the intercept probability with one and two PUs are the same. This confirms the analytical results derived in Sect. 3, which also shown on the figure.

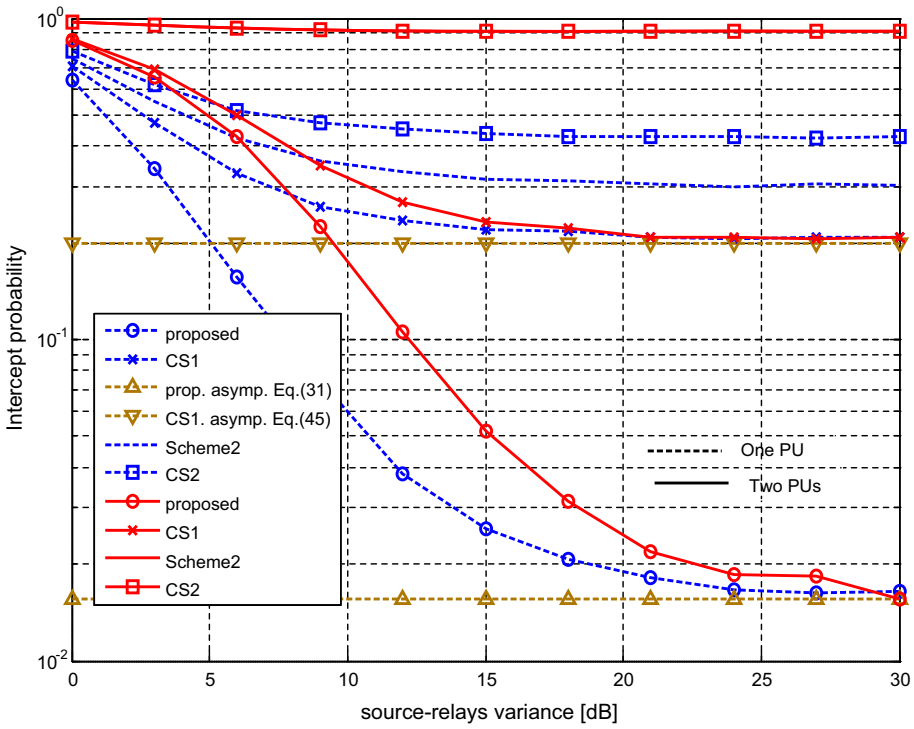

Fig. 7 The intercept probability versus source-relays channel, with $N = 4$, $L = 1$, $K = \{1, 2\}$

6 Conclusions

In this paper, we have studied the physical layer security in cooperative CRNs. We have proposed relay selection schemes to improve the physical layer security in CRNs against the presence of multiple eavesdroppers, and at the same time taking into account the QoS constraints of the PUs in the network. The DF relaying is used, where a relay is selected from the decoding set to help the source transmission and also maximize the secrecy rate. Two performance metrics are considered; namely, achievable ergodic secrecy rate and intercept probability. We have shown that the proposed selection schemes outperform the conventional and other schemes proposed in the literature over all the range of the transmitted power in terms of both the achievable ergodic secrecy rate and the intercept probability. Also, it has be shown that presence of multiple eavesdroppers or PUs in the network degrade both the achievable secrecy rate and the intercept probability. However, in the asymptotic case, the intercept probability with multiple PUs is the same as that with single PU. Furthermore, we have derived closed form expressions of the asymptotic intercept probability of the proposed schemes, and tight lower bounds for the asymptotic intercept probability of the conventional schemes.

References

1. Akyildiz, I. F., Lee, W. Y., Vuran, M. C., & Mohanty, S. (2006). Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks, 50*(13), 2127–2159.
2. Biglieri, E., Goldsmith, A. J., Greenstein, L. J., Mandayam, N. B., & Poor, H. V. (2013) *Principles of cognitive radio*. Cambridge: Cambridge University Press.
3. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal, 28*(4), 656–715.
4. Wyner, A. D. (1975). The wire-tap channel. *Bell System Technical Journal, 54*(8), 1355–1387.
5. Barros, J., & Rodrigues, M. R. D. (2006, July). Secrecy capacity of wireless channels. In *Proceedings of IEEE international symposium information theory* (pp. 356–360).
6. Li, Z., Trappe, W., & Yates, R. (2007, March). Secret communication via multi-antenna transmission. In *Proceedings of 41st conference on information sciences systems*, Baltimore, MD.
7. Khisti, A., Womell, G., Wiesel, A., & Eldar, Y. (2007, June). On the Gaussian MIMO wiretap channel. In *Proceedings of IEEE international symposium on information theory*, Nice, France.
8. Oggier, F., & Hassibi, B. (2007). The secrecy capacity of the MIMO wiretap channel. *IEEE Transactions on Information Theory, 57*(8), 4961–4972.
9. Zou, Y., Wang, X., & Shen, W. (2013). Optimal relay selection for physical layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications, 31*(10), 2099–2111.
10. Zou, Y., Wang, X., & Shen, W. (2013, June). Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack. In *Proceedings of IEEE international conference on communicaitons (ICC 2013)* (pp. 1–5).

11. Al-nahari, A., Krikidis, I., Ibrahim, A. S., Dessouky, M. I., & El-Samie, F. A. (2012). Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers. *Transactions on Emerging Telecommunications Technologies (ETT), 25*(4), 445–460.
12. Shu, Z., Qian, Y., & Ci, S. (2013). On physical layer security for cognitive radio networks. *IEEE Networks, 27*(3), 28–32.
13. Leon, O., Serrano, J. H., & Soriano, M. (2010). Securing cognitive radio networks. *International Journal of Communications Systems, 23*(5), 633–652.
14. El-Hajj, W., Safa, H., & Guizani, M. (2011). Survey of security issues in cognitive radio networks. *Journal of Internet Technology, 12*(2), 25–37.
15. Anand, S., & Chandramouli, R. (2008, May). On the secrecy capacity of fading cognitive wireless networks. In *Proceedings IEEE CrownCom*.
16. Pei, Y., Liang, Y., Zhang, L., Teh, K. C., & Li, K. H. (2010). Secure communication over MISO cognitive radio channels. *IEEE Transactions on Wireless Communications, 9*(4), 1494–1592.
17. Zou, Y., Wang, X., & Shen, W. (2013). Physical layer security with multiuser scheduling in cognitive radio networks. In *IEEE Transactions on Communications, 61*(12), 5103–5113.
18. Sakran, H., Nasr, O., Shokair, M., El-Rabaie, E., & El-Azm, A. (2012). Proposed relay selection scheme for physical layer security in cognitive radio networks. *IET Communications, 6*(16), 2676–2687.
19. Al-Jamali, M., Al-nahari, A., & Al-Khawlani, M. (2015). Relay selection scheme for improving the physical layer security in cognitive radio networks. In *Proceedings of 23rd IEEE signal processing and communications applications*, Malatya, 16–19 May 2015.
20. Krikidis, I. (2010). Opportunistic relay selection for cooperative networks with secrecy constraints. *IET Communications, 4*(15), 1787–1791.
21. Zou, Y., Wang, X., & Shen, W. (2013). Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE Journal on Selected Areas in Communications, 31*(10), 1787–1791.
22. Miller, S., & Childers, D. (2004). *Probability and random processes with applications to signal processing and communications*. San Diego: Elsevier Academic Press.

Mukarram Al-jamali received the B.Sc. degree in Electronics and Telecommunications Engineering from Zagazig University, Egypt, in 2005. He received an M.Sc. degree in Communications Engineering from University of Science and Technology, Yemen. He is also working as a lecturer at the Electronics Engineering Department, University of Science and Technology, Yemen. His research interests are wireless communications, cooperative communications, cognitive radio, and physical layer security.

Azzam Al-nahari received the B.Sc. degree in electronic and communications engineering from the University of Technology, Baghdad, Iraq. He received M.Sc. and Ph.D. degrees in electrical communication from the Faculty of Electronic Engineering, Menoufia University, Egypt in 2008, and 2011, respectively. He is currently an Assistant Professor at the Department of Electrical Engineering, Ibb University, Ibb, Yemen. His current research interests include MIMO, OFDM, cooperative communications, physical layer security, cognitive radio, massive MIMO and signal processing for wireless Communications.

Mohammed AlKhawlani is a Senior Lecturer at the University of Science and Technology (UST), Sana'a, Yemen. He received his Ph.D. in Data Communication and Networking Engineering from De Montfort University, UK, in July 2008. He received his M.Sc. in Data Communication Systems from Brunel University, UK, in December 2003. He received his B.Sc. in Computer Engineering from Cairo University, Egypt, in July 2001. His research interest is radio resource management in the next generation of wireless networks with the aid of artificial intelligence tools.