Secrecy performance of threshold-based decode-and-forward cooperative cognitive radio network

Khyati Chopra[1,*], Ranjan Bose[2], Anupam Joshi[3]

[1]Dept. of Electrical Engineering, Indian Institute of Technology, Delhi, New Delhi-110016, India
[2]Dept. of Electrical Engineering, Indian Institute of Technology, Delhi, New Delhi-110016, India
[3]Dept. of Computer Science, University of Maryland, Baltimore County, Baltimore, MD 21250, United States
[*]eez148071@ee.iitd.ac.in

Abstract: This paper evaluates the intercept and outage probability of a decode-and-forward (DF) underlay cognitive radio network. The secondary users are subject to interference limitations from the primary network, with an eavesdropper tapping the second hop of cognitive network, when all the links undergo Rayleigh fading. For this threshold-based system, without assuming that the DF relays can always decode the message correctly, here we consider that only a set of relays whose SNR satisfies a predetermined threshold can decode the message successfully. We have obtained asymptotic analysis for both cases, when average SNRs of secondary source-relay and relay-destination links are balanced or unbalanced. We have shown that the desired secrecy rate, predetermined threshold, eavesdropper channel quality and interference power limitations significantly affects the secrecy performance of the cognitive radio system. We have investigated the outage and intercept probability of relay selection scheme, when either full instantaneous channel state information (ICSI) or statistical channel state information (SCSI) of all the links is available. We have shown that the optimal relay selection improves the performance of the multi-relay cognitive system, when the number of relays is increased.

1. Introduction

Cognitive radio has emerged as a dynamic spectrum access technique, where an unlicensed (secondary) user is allowed to simultaneously access the licensed channels. These channels are dedicated to a primary user (PU), as long as the quality of service (QoS) of PU is not affected [1–3]. In this underlay cognitive radio [4], the transmitting power of the secondary users (SUs) is optimally controlled, such that the interference caused due to the secondary transmission does not exceed the maximum tolerable interference level, which is defined by the primary receiver [5]. Due to the open and dynamic nature of the cognitive radio network (CRN) architecture, the licensed spectrum is opportunistically accessed by the various unknown wireless devices. This makes it extremely vulnerable to potential eavesdropping attacks [1, 5].
Physical layer security (PLS) or information theoretic security has been developed as an effective secure wireless communications paradigm, to prevent the eavesdropper from intercepting transmission messages on the wireless links [1, 2]. Thus, the security performance is improved by exploiting the physical characteristics of wireless channels, without the need for traditional complex cryptographic protocols [4, 5]. The wiretap channel model was introduced by Wyner, where

it was shown that the perfectly secure messages with a non-zero rate can be delivered, if the eavesdropper channel is the degraded version of the legitimate main channel [6].

Cooperative communication plays a promising role to improve the PLS in CRN [1, 7–10]. It is worthwhile to note that secrecy rate and secrecy outage probability are the two frequently used measures of secrecy performance in these cooperative networks. Secrecy outage and intercept probability of the single and multi-relay system has been investigated in [7] for the CRN. However in [8], secure performance analysis of cognitive two-way relay system is derived over Rayleigh fading channels, only in terms of the intercept probability. Both DF and amplify-and-forward (AF) relays are used in multi-relay dual-hop cooperative networks as given in [11]. In [4], authors have investigated the secrecy outage probability for underlay cognitive DF relay network. While in [10], intercept outage probability analysis of AF relaying networks under a spectrum sharing mechanism in presence of eavesdropping attack is discussed.

Secrecy performance of cooperative CRN has been discussed in literature for both known and unknown CSI [12–14]. Achievable secrecy capacity for underlay CRN is investigated in [13] for both cases of known and unknown channel information. Secrecy outage probability performance for cooperative DF underlay CRNs, with outdated channel state information (CSI) has been discussed in [12]. Asymptotic analysis of cooperative diversity systems, both with perfect and imperfect CSI in a spectrum-sharing scenario has been investigated in [14].

The outage performance of the underlay CRN, where secondary network is subjected to interference constrains from the primary network is investigated in [15–17]. However, the effect of the interference from the primary network to the secondary network can be ignored [15–17], if the primary transmitter is located far away from the secondary users. Also, the interference can be ignored when it is represented by the noise term, under an assumption that the primary transmitter's signal is generated by random Gaussian code-book [15–17]. Authors in [3, 14] have ignored the detailed protocol between the primary source and the primary destination, and have translated the interference from the primary source into the noise term of the secondary system. In [18, 19] authors have shown that the system performance decreases, with increase of primary user's transmit power and larger pathloss exponent. The outage performance of the secondary system deteriorates, when the primary transmitter is located closer to the secondary receiver.

Optimal and sub-optimal relay selection schemes have been extensively discussed in [20] for the cooperative relay networks, and it is shown that the performance of the optimal selection scheme is the best as compared to sub-optimal and traditional relay selection schemes. In [9], authors have presented the relay selection scheme for the CRN that is subjected to the interference power constraints. Similarly, the relay selection scheme, where a trusted DF relay is selected to assist the source transmission and improve the secrecy rate, subject to QoS constraints of PU is presented in [1]. The performance of this system is analyzed in terms of the intercept probability and the achievable secrecy rate. In [21, 22] authors have explored relay selection schemes for security enhancement in CRN for AF and DF protocols, without taking into account the direct transmissions from source to eavesdropper.

In the existing literature, typically it is assumed that a relay can correctly decode the message due to high SNR scenario [23]. However, this is not always a practical assumption as fading might degrade the signal strength, such that the relay is not able to correctly decode the message [24]. Correct decoding over a particular threshold SNR is thus a better assumption and is considered in this paper. Opportunistic relay selection scheme can be used to exploit the channel fluctuation among relays for DF relay networks to enhance the secure transmission [23–25]. Motivated by this, we have considered threshold-based decoding, where the relays can correctly decode the message,

only if their SNR satisfies the predetermined threshold. Our work is significantly different from the others discussed in literature [1, 20–24], as both intercept and outage probability are investigated for threshold-based cooperative CRN, subject to interference constraints from the primary user. The secrecy performance is analyzed for both with and without the direct link between secondary source and eavesdropper.

The key contributions of our work are summarized as follows:

- We have investigated the intercept and outage performance of threshold-based underlay cognitive radio system, under interference constraints from the primary network. We have not assumed perfect decoding at secondary relays and have shown that the link quality of both secondary source-relay and relay-destination affects the secrecy performance of this cognitive system.
- Without assuming that the direct links are in deep shadow fading or the nodes may be far apart, the expression for intercept and outage probability of threshold-based CRN is derived, both with and without the direct link between secondary source-eavesdropper.
- We have shown that the improvement in desired secrecy rate, predetermined threshold, eavesdropper channel quality and interference constraints affect the secrecy performance of the cognitive radio system. The outage probability of cognitive transmissions decreases accordingly with an increase in the maximum tolerable interference level at primary destination.
- We have obtained asymptotic analysis for both the cases, when average SNRs of secondary source-relay and relay-destination links are balanced or unbalanced.
- We have also evaluated the outage and intercept probability for secondary relay selection scheme, when either full ICSI or SCSI of all the links is available. We have shown that the optimal relay selection improves the performance of the multi-relay cognitive system, when the number of relays is increased.

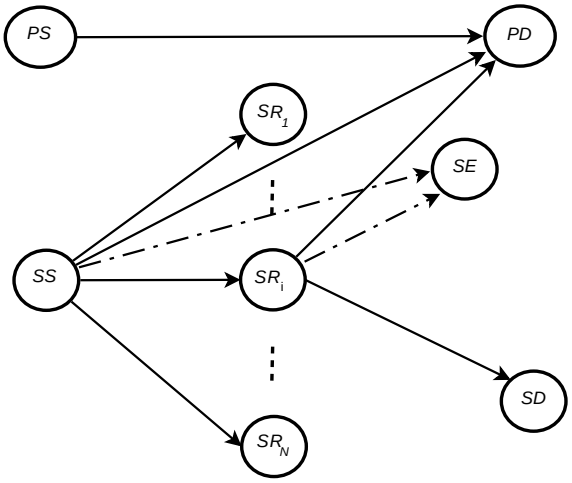

Fig. 1. *Dual-hop DF cooperative cognitive threshold-based multi-relay system*

The remainder of the paper is organized as follows. Section 2 presents the cognitive radio system model. In Section 3, secrecy outage and intercept probability expressions are evaluated for threshold-based cognitive radio system, subject to interference limitations from primary user, both

with and without secondary direct transmission. The outage and intercept probability of optimal relay selection scheme is investigated in Section 4. In Section 5, asymptotic analysis for balanced and unbalanced case is examined. Simulation and numerical results are discussed in Section 6 and finally, Section 7 gives the concluding remarks.

Notation: $\mathcal{E}(x)$ defines exponential distribution with parameter x, $\mathbb{P}[\cdot]$ is the probability of an event, $\mathbb{E}_X[\cdot]$ is the expectation of its argument over random variable X. $\max\{\cdot\}$ and $\min\{\cdot\}$ denote the maximum and minimum of its arguments respectively and $(x)^+ \triangleq \max(0, x)$. Generally $F_X(\cdot)$, in capital letter, denotes the cumulative distribution function (CDF) of a RV X. $f_X(\cdot)$, in small letter, denotes the corresponding probability density function (PDF).

2. System Model

The system model consists of a secondary source SS, a secondary destination SD, a secondary eavesdropper SE, a primary source PS , a primary destination PD and N number of DF secondary relays SR_i , $i \in [1, 2.., N]$ as depicted in the Fig.1. The underlay spectrum sharing is considered throughout this paper where, a secondary unlicensed user and a primary user are allowed to transmit simultaneously over the same spectrum band, as long as the interference caused by the SUs is tolerable at PD, such that the quality of service (QoS) of $PS-PD$ transmission is not degraded [3]. We have assumed a maximum tolerable interference power level I_m at PD without affecting its QoS. This constrains the transmit power of secondary users, such that the interference received at PD from SUs is less than I_m [4, 21, 26]. We have assumed that the primary transmitter is located far away from the secondary users and also the transmit power of primary source is very small [15–17]. Thus, we have ignored the effect of interference from the primary network to the secondary network, in order to obtain the closed-form results for intercept and outage probability of this threshold-based cognitive relay system.

Due to the broadcast nature of wireless medium, we also consider a direct link from secondary source to secondary eavesdropper $SS - SE$ and assume that SE is located closer as compared to SD [8, 9]. The communication between SS and SD takes place with the aid of only a single cooperative DF secondary relay [1, 21]. We have evaluated the expression for intercept and outage probability of this threshold-based dual-hop cooperative CRN, subject to interference constraints from PD. The secrecy performance analysis is done for both with and without the direct link between secondary source and eavesdropper. We have modeled the links between various nodes as mutually independent Rayleigh flat fading channels, which work in half-duplex mode and are not identical. In addition, we consider that the ICSI of all the links is available [20, 21].

The SNR Γ_{ab} between any two random nodes a and b, is given as [20]

$$\Gamma_{ab} = \frac{P_a |h_{ab}|^2}{N_{0_b}}, \tag{1}$$

where the transmitted power at node a is given as P_a , the noise variance of the additive white Gaussian noise (AWGN) at y is given as N_{0_b}. Γ_{ab} is exponentially distributed, as h_{ab} is Rayleigh distributed, and the mean value is $1/\beta_{ab}$ [27] , denoted as $\Gamma_{ab} \sim \mathcal{E}(\beta_{ab})$, where β_{ab} is the parameter of exponentially distribution. For the random variable A, which is exponentially distributed with parameter β_{ab}, the CDF is given as

$$F_A(z) = 1 - e^{-z\beta_{ab}}, \tag{2}$$

and the corresponding PDF is obtained by differentiating (2) with respect to z as

$$f_A(z) = \beta_{ab} e^{-z\beta_{ab}}. \tag{3}$$

For the random variable A, where A is the sum of two random variables X and Y, which are exponentially distributed with parameters β_{ab} and $\beta_{a'b'}$, the CDF is given as

$$\begin{aligned} F_A(z) &= \mathbb{P}[X + Y \leq z] \\ &= \mathbb{P}[X \leq z - Y] \\ &= 1 - \frac{\beta_{a'b'} e^{-z\beta_{ab}}}{\beta_{a'b'} - \beta_{ab}} - \frac{\beta_{ab} e^{-z\beta_{a'b'}}}{\beta_{ab} - \beta_{a'b'}}, \end{aligned} \tag{4}$$

and the corresponding PDF is obtained by differentiating (4) with respect to z as

$$f_A(z) = \frac{\beta_{a'b'}\beta_{ab} e^{-z\beta_{ab}}}{\beta_{a'b'} - \beta_{ab}} + \frac{\beta_{ab}\beta_{a'b'} e^{-z\beta_{a'b'}}}{\beta_{ab} - \beta_{a'b'}}. \tag{5}$$

The $SS - SR_i$ channels h_{sr_i}, $SR_i - SD$ channels $h_{r_i d}$, $SR_i - SE$ channels $h_{r_i e}$, $SS - SE$ channels h_{se} , $SS - PD$ channels h_{sp} and $SR_i - PD$ channels $h_{r_i p}$, $\forall i \in [1, 2.., N]$, are slowly varying Rayleigh flat fading channels [28]. The transmit powers used at secondary source SS and secondary relay SR_i are denoted as P_s and P_{r_i} respectively. As the secondary user transmits to SD over the same spectrum band as the PS, there is a maximum tolerable interference power level I_m at PD. This constrains the transmit power of secondary users, such that the interference received at PD from secondary users is less than I_m. In addition, we also consider the maximum transmit power constraint, such that the power of the secondary users is less than $\bar{P}$, where $\bar{P}$ is the maximum transmit power of secondary users [3,15,17,29]. Using both interference and maximum transmit power constraints, the power of the secondary users is limited as

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

$$P_{r_i} \leq \min\left(\frac{I_m}{|h_{r_i p}|^2}, \bar{P}\right) \tag{7}$$

For extremely large values of $\bar{P}$, the transmit powers P_s and P_{r_i} of secondary source and relay respectively are modeled as

$$P_s = \frac{I_m}{|h_{sp}|^2} \tag{8}$$

$$P_{r_i} = \frac{I_m}{|h_{r_i p}|^2} \tag{9}$$

It is shown in [15] that for high values of $\bar{P}$, due to the maximum transmit power constraint, the transmitting power of the secondary users is modeled as (8) and (9) with high probability. Contrary to [15], the interference temperature constraint is also taken into consideration in [16]. They have investigated that when $\bar{P}$ tends to infinity, the transmit power of secondary source and relay is modeled as (8) and (9) with probability equal to one. The interference temperature constraint becomes the dominant factor to determine the maximum allowed transmit power at secondary

source and relay and outage saturation would appear [16]. The excessive use of power at secondary source and relay will be limited by a fixed I_m. The distributed transmit power allocation for the multi-hop CRN is discussed in [30]. This power control modeling for characterizing the underlay CRN given by (8) and (9), is widely used in literature [3–5, 15, 21, 29]. We have considered the use of (8) and (9) throughout this paper, to model the transmit power of secondary users for the sake of simplicity and in order to obtain the closed-form results [4, 21].

Without loss of generality, let N_{sr_i}, N_{r_id}, N_{r_ie}, N_{se}, N_{sp} and N_{r_ip} denote the variances of additive white Gaussian noise of $SS-SR_i$, SR_i-SD, SR_i-SE, $SS-SE$, $SS-PD$ and SR_i-PD links respectively. The SNRs Γ_{sr_i} , Γ_{r_id} , Γ_{r_ie}, Γ_{se}, Γ_{sp} and Γ_{r_ip} are exponentially distributed given as $\Gamma_{sr_i} = \frac{P_s|h_{sr_i}|^2}{N_{sr_i}}$, $\Gamma_{r_id} = \frac{P_{r_i}|h_{r_id}|^2}{N_{r_id}}$, $\Gamma_{r_ie} = \frac{P_{r_i}|h_{r_ie}|^2}{N_{r_ie}}$, $\Gamma_{se} = \frac{P_s|h_{se}|^2}{N_{se}}$, $\Gamma_{sp} = \frac{P_s|h_{sp}|^2}{N_{sp}}$ and $\Gamma_{r_ip} = \frac{P_{r_i}|h_{r_ip}|^2}{N_{r_ip}}$, with link quality taken as $\gamma_{sr_i} = \frac{|h_{sr_i}|^2}{N_{sr_i}}$, $\gamma_{r_id} = \frac{|h_{r_id}|^2}{N_{r_id}}$, $\gamma_{r_ie} = \frac{|h_{r_ie}|^2}{N_{r_ie}}$, $\gamma_{se} = \frac{|h_{se}|^2}{N_{se}}$, $\gamma_{sp} = |h_{sp}|^2$ and $\gamma_{r_ip} = |h_{r_ip}|^2$, whose mean values are $1/\beta_{sr_i}$, $1/\beta_{r_id}$, $1/\alpha_{r_ie}$, $1/\alpha_{se}$, $1/\theta_{sp}$ and $1/\theta_{r_ip}$ respectively, where β_{sr_i}, β_{r_id}, α_{r_ie}, α_{se}, θ_{sp} and θ_{r_ip} are the parameters of the exponential distribution. When the secrecy capacity of the cognitive relay system is less than the desired secrecy rate , given as R_s where, $R_s > 0$ and $\rho = 2^{2R_s}$, an outage event is occurred [11, 20]. Here, we have used ρ for directly mapping desired secrecy rate R_s. We use both the terms as desired secrecy rate throughout the paper interchangeably. The secrecy outage probability P_o is defined as the probability of successful occurrence of this outage event. An intercept event occurs when the secrecy capacity is negative (i.e. strictly less than zero), and the intercept probability P_{int} is defined as the probability of successful occurrence of this event. It can be observed that P_{int} is nothing but a special case of the secrecy outage probability P_o with desired secrecy rate $R_s = 0$ [5]. Both P_o and P_{int} are the key metrics in evaluating the performance of PLS [28].

We have investigated two scenarios in our study, subject to the primary user's QoS constraint i.e. the maximum allowable interference level I_m at PD during cognitive radio transmissions. The first scenario is when the direct link between $SS-SE$ exists. The second scenario is when no direct link between $SS-SE$ is considered, assuming that the direct link between $SS-SE$ is in deep shadow fading or the secondary eavesdropper is far apart from the secondary source [1, 21–23]. Assuming that the optimal Gaussian code-book is used at the source, the secrecy capacity of the system in the first scenario is given as [6, 11, 20, 28]

$$C_s^e \triangleq \frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_M^e}{1+\Gamma_E^e}\right)\right]^+ \tag{10}$$

where C_s^e is the secrecy capacity when the predetermined threshold is satisfied by the secondary relay, such that $\Gamma_M^e = \Gamma_{r_id}$ is the SNR of the secondary main link at SD and $\Gamma_E^e = \Gamma_{r_ie} + \Gamma_{se}$ is the combined SNR of the secondary eavesdropper link at SE. The capacity of the main link at secondary destination SD given in (10), is determined by the SNR of the second hop Γ_{r_id}, but is not influenced by the SNR of the first hop Γ_{sr_i}, as we have considered very high threshold regime for the first hop of main link. Without assuming perfect decoding at the secondary relays, here we consider that among all the secondary relays, only those relays can successfully decode the message, whose SNR satisfies the predetermined threshold, taken as γ_{th} for $SS-SR_i$ link [22, 23, 25]. The threshold γ_{th} , is assumed to be very high for the first hop of main link. The message can be correctly decoded by relays only if the SNR of $SS-SR_i$ link, Γ_{sr_i} is greater than γ_{th} else, only direct transmission between $SS-SE$ takes place in the secondary network. The term 1/2 here denotes that we require two time slots in order to complete this dual-hop secondary transmission process. In the first time slot, the SS broadcasts the message to the secondary relay, who correctly

decodes the message if the predetermined threshold is satisfied. In the second time slot, one relay node which is selected among the relays that successfully decoded the source message, re-encodes and forwards the message to SD. From (10), when the secondary relay node does not satisfy the predetermined threshold due to shadow fading [31], only direct communication link $SS - SE$ exists and the achievable secrecy rate is given as $C_s^{e'}$ where $\Gamma_E^{e'} = \Gamma_{se}$ is the SNR of the secondary eavesdropper link at SE.
In the second scenario, when the predetermined threshold is satisfied by the secondary relay, the secrecy capacity from (10) is given as C_s^{ne} where, C_s^{ne} is the secrecy capacity when secondary eavesdropper direct link $SS-SE$ does not exists, such that $\Gamma_M^{ne} = \Gamma_{r_id}$ is the SNR of the secondary main link at SD and $\Gamma_E^{ne} = \Gamma_{r_ie}$ is the SNR of the secondary eavesdropper link at SE. When the predetermined threshold is not satisfied by the secondary relay due to shadow fading [31], it is not selected for secondary cooperative communication.

3. Outage and Intercept Probability of Single Relay Cognitive System

This section deals with the evaluation of the expression for secrecy outage probability and intercept probability of a threshold-based dual-hop DF underlay cognitive relay network, in the two scenarios discussed in our study. We have divided each scenario into two cases. In the first case, the SNR at the relay node meets the predetermined threshold, and thus the relay is selected and decodes the message correctly. In the second case, the SNR at the relay node does not satisfy the predetermined threshold, and thus the relay is not selected to forward source data [23, 25].
Using (1)-(10), we have evaluated the secrecy outage probability for single i^{th} relay in the first scenario where, the direct link between $SS - SE$ exists. The expectation is taken over random variable $\gamma_{sp}, \gamma_{r_ip}$ for obtaining closed-form solution. The outage probability is given as

$$
\begin{aligned}
P_o^i(R_s) &= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\mathbb{P}\left[C_s^e < R_s | \Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\mathbb{P}[\Gamma_{sr_i} \geq \gamma_{th} | \gamma_{sp}, \gamma_{r_ip}] \\
&\quad + \mathbb{P}\left[C_s^{e'} < R_s | \Gamma_{sr_i} < \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\mathbb{P}\Big[\Gamma_{sr_i} < \gamma_{th} | \gamma_{sp}, \gamma_{r_ip}\Big]\Bigg]\Bigg] \\
&= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_{r_id}}{1+\Gamma_{r_ie}+\Gamma_{se}}\right)\right] < R_s \Big| \Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\mathbb{P}\Big[\Gamma_{sr_i} \geq \gamma_{th} | \gamma_{sp}, \gamma_{r_ip}\Big] \\
&\quad + \mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1}{1+\Gamma_{se}}\right)\right] < R_s \Big| \Gamma_{sr_i} < \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\mathbb{P}\Big[\Gamma_{sr_i} < \gamma_{th} | \gamma_{sp}, \gamma_{r_ip}\Big]\Bigg]\Bigg] \\
&= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\mathbb{P}\left[\frac{1+\frac{I_m\gamma_{r_id}}{\gamma_{r_ip}}}{1+\frac{I_m\gamma_{r_ie}}{\gamma_{r_ip}}+\frac{I_m\gamma_{se}}{\gamma_{sp}}} < \rho \Big| \Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\left[1 - \mathbb{P}\left[\frac{I_m\gamma_{sr_i}}{\gamma_{sp}} < \gamma_{th} \Big| \gamma_{sp}, \gamma_{r_ip}\right]\right] \\
&\quad + \mathbb{P}\left[\frac{1}{1+\frac{I_m\gamma_{se}}{\gamma_{sp}}} < \rho \Big| \Gamma_{sr_i} < \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\mathbb{P}\left[\frac{I_m\gamma_{sr_i}}{\gamma_{sp}} < \gamma_{th} \Big| \gamma_{sp}, \gamma_{r_ip}\right]\Bigg]\Bigg] \\
&= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\Bigg(1 - \frac{\alpha_{r_ie}\gamma_{r_ip}\alpha_{se}\gamma_{sp}e^{-\frac{(\rho-1)\beta_{r_id}\gamma_{r_ip}}{I_m}}}{\alpha_{se}\gamma_{sp} - \alpha_{r_ie}\gamma_{r_ip}} \times
\end{aligned}
$$

$$
\left(\frac{1}{\rho\beta_{r_id}\gamma_{r_ip}+\alpha_{r_ie}\gamma_{r_ip}}-\frac{1}{\rho\beta_{r_id}\gamma_{r_ip}+\alpha_{se}\gamma_{sp}}\right)e^{-\frac{\gamma_{th}\beta_{sr_i}\gamma_{sp}}{I_m}}
+\left(1-e^{-\frac{\gamma_{th}\beta_{sr_i}\gamma_{sp}}{I_m}}\right)\Bigg]\Bigg]
$$

$$
=\int_0^{+\infty}\int_0^{+\infty}\Bigg[\Bigg(1-\frac{x\alpha_{r_ie}\alpha_{se}e^{-\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}y}}{(\alpha_{se}x-\alpha_{r_ie}y)(\rho\beta_{r_id}+\alpha_{r_ie})}
+\frac{xy\alpha_{r_ie}\alpha_{se}e^{-\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}y}}{(\alpha_{se}x-\alpha_{r_ie}y)(\rho\beta_{r_id}y+\alpha_{se}x)}\Bigg)e^{-\frac{\gamma_{th}\beta_{sr_i}x}{I_m}}
+\left(1-e^{-\frac{\gamma_{th}\beta_{sr_i}x}{I_m}}\right)\Bigg]\theta_{sp}e^{-\theta_{sp}x}\theta_{r_ip}e^{-\theta_{r_ip}y}dxdy \tag{11}
$$

where $\rho = 2^{2R_s}$. The secrecy outage probability expression for single i^{th} relay from (11) is obtained as

$$
\begin{aligned}
P_o^i(R_s) = \Bigg[& \left(\frac{\theta_{sp}}{\theta_{sp}+\frac{\gamma_{th}\beta_{sr_i}}{I_m}}\right)+\left(\frac{\alpha_{se}\theta_{sp}\theta_{r_ip}}{(\rho\beta_{r_id}+\alpha_{r_ie})}\right)\\
&\times\left(\frac{1}{a_1^2}\left(\log_e\left(\frac{a_1}{b_1}-1\right)-\left(\frac{a_1}{a_1-b_1}\right)\right)\right)\\
&+\left(\frac{\alpha_{r_ie}^2\theta_{sp}\theta_{r_ip}}{\alpha_{se}(\rho\beta_{r_id}+\alpha_{r_ie})}\right)\\
&\times\left(\frac{1}{a_2^2}\left(\log_e\left(\frac{a_2}{b_2}-1\right)-\left(\frac{a_2}{a_2-b_2}\right)\right)\right)\\
&+\left(\frac{\rho\beta_{r_id}\alpha_{r_ie}\theta_{sp}\theta_{r_ip}}{\alpha_{se}(\alpha_{r_ie}+\rho\beta_{r_id})}\right)\\
&\times\left(\frac{1}{a_3^2}\left(\log_e\left(\frac{a_3}{b_3}+1\right)-\left(\frac{a_3}{a_3+b_3}\right)\right)\right)\Bigg]\\
&+\left(\frac{\frac{\gamma_{th}\beta_{sr_i}}{I_m}}{\theta_{sp}+\frac{\gamma_{th}\beta_{sr_i}}{I_m}}\right)
\end{aligned} \tag{12}
$$

where

$$
a_1=\left(\theta_{sp}+\frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)+\frac{\left(\theta_{r_ip}+\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right)\alpha_{se}}{\alpha_{r_ie}} \tag{13}
$$

$$
b_1=\frac{\left(\theta_{r_ip}+\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right)\alpha_{se}}{\alpha_{r_ie}} \tag{14}
$$

$$
a_2=\left(\theta_{r_ip}+\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right)+\frac{\left(\theta_{sp}+\frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)\alpha_{r_ie}}{\alpha_{se}} \tag{15}
$$

$$b_2 = \frac{\left(\theta_{sp} + \frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)\alpha_{r_ie}}{\alpha_{se}} \tag{16}$$

$$a_3 = \left(\theta_{r_ip} + \left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right) - \frac{\rho\left(\theta_{sp} + \frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)\beta_{r_id}}{\alpha_{se}} \tag{17}$$

$$b_3 = \frac{\rho\left(\theta_{sp} + \frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)\beta_{r_id}}{\alpha_{se}} \tag{18}$$

The intercept probability expression for single i^{th} relay with direct $SS-SE$ link is obtained from (12) by substituting $\rho = 1$.

Using (1)-(10), we now evaluate outage probability for single i^{th} relay in the second scenario where, no direct link between $SS-SE$ exists. For this scenario also, we have presented the probabilistic analysis of both cases, where either the relay is selected, or the relay is not selected for communicating source data. The second case is significantly taken into account, when due to low SNR of the first hop of main link, the relay is not selected. When $\Gamma_{sr_i} < \gamma_{th}$, secrecy outage probability becomes unity [24], irrespective of direct link $SS-SE$ exists or not. The expectation is taken over random variable $\gamma_{sp}, \gamma_{r_ip}$ for obtaining closed-form solution. The outage probability is given as

$$\begin{aligned}
P_o^i(R_s) &= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\mathbb{P}\left[C_s^{ne} < R_s|\Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\mathbb{P}[\Gamma_{sr_i} \geq \gamma_{th}|\gamma_{sp}, \gamma_{r_ip}] \\
&\quad + \mathbb{P}[\Gamma_{sr_i} < \gamma_{th}|\gamma_{sp}, \gamma_{r_ip}]\Bigg]\Bigg] \\
&= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\mathbb{P}\left[\frac{1}{2}\left[\log_2\left(\frac{1+\Gamma_{r_id}}{1+\Gamma_{r_ie}}\right)\right] < R_s\Big|\Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\mathbb{P}\Big[\Gamma_{sr_i} \geq \gamma_{th}|\gamma_{sp}, \gamma_{r_ip}\Big] \\
&\quad + \mathbb{P}\Big[\Gamma_{sr_i} < \gamma_{th}|\gamma_{sp}, \gamma_{r_ip}\Big]\Bigg]\Bigg] \\
&= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\mathbb{P}\left[\frac{1+\frac{I_m\gamma_{r_id}}{\gamma_{r_ip}}}{1+\frac{I_m\gamma_{r_ie}}{\gamma_{r_ip}}} < \rho\Big|\Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_ip}\right]\left[1 - \mathbb{P}\left[\frac{I_m\gamma_{sr_i}}{\gamma_{sp}} < \gamma_{th}\Big|\gamma_{sp}, \gamma_{r_ip}\right]\right] \\
&\quad + \left[\mathbb{P}\left[\frac{I_m\gamma_{sr_i}}{\gamma_{sp}} < \gamma_{th}\Big|\gamma_{sp}, \gamma_{r_ip}\right]\right]\Bigg]\Bigg] \\
&= \mathbb{E}_{\gamma_{r_ip}}\Bigg[\mathbb{E}_{\gamma_{sp}}\Bigg[\left(1 - \frac{\alpha_{r_ie}e^{-\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\gamma_{r_ip}}}{\rho\beta_{r_id} + \alpha_{r_ie}}\right)e^{-\frac{\gamma_{th}\beta_{sr_i}\gamma_{sp}}{I_m}} \\
&\quad + \left(1 - e^{-\frac{\gamma_{th}\beta_{sr_i}\gamma_{sp}}{I_m}}\right)\Bigg]\Bigg] \\
&= \int_0^{+\infty}\int_0^{+\infty}\Bigg[\left(1 - \frac{\alpha_{r_ie}e^{-\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}y}}{\rho\beta_{r_id} + \alpha_{r_ie}}\right)e^{-\frac{\gamma_{th}\beta_{sr_i}x}{I_m}}
\end{aligned}$$

$$+\left(1-e^{-\frac{\gamma_{th}\beta_{sr_i}x}{I_m}}\right)\Bigg]\theta_{sp}e^{-\theta_{sp}x}\theta_{r_ip}e^{-\theta_{r_ip}y}dxdy \tag{19}$$

where $\rho = 2^{2R_s}$. The secrecy outage probability expression for single i^{th} relay from (19) is obtained as

$$P_o^i(R_s) = \left(1 - \frac{\alpha_{r_ie}\theta_{r_ip}\theta_{sp}}{\left(\rho\beta_{r_id}+\alpha_{r_ie}\right)\left(\theta_{r_ip}+\left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right)\left(\theta_{sp}+\frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)}\right) \tag{20}$$

The intercept probability for single i^{th} relay without direct $SS-SE$ link is obtained from (19) by substituting $\rho = 1$ and by taking second term in (19) as zero. For $\Gamma_{sr_i} < \gamma_{th}$, the relay node does not transmit and there is no link between $SS-SE$, thus there is no signal present that can be intercepted. The intercept probability expression is given as

$$P_{int}^i = \frac{\beta_{r_id}\theta_{sp}}{\left(\theta_{sp}+\frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)\left(\beta_{r_id}+\alpha_{r_ie}\right)} \tag{21}$$

In contrast to the prior literature, where the direct link between the secondary source and secondary eavesdropper is not considered [1, 21–23], we have derived the expression for secrecy outage probability and intercept probability of a threshold-based dual-hop DF cooperative cognitive relay network, both with and without the direct link between $SS-SE$ as discussed in our study.

4. Outage and Intercept Probability of Multi-Relay Cognitive System

This section evaluates the outage and intercept probability of optimal relay selection scheme for threshold-based dual-hop cognitive relay network. The outage and intercept probability in this section is obtained under the scenario, when there is no direct link between $SS-SE$ and without assuming perfect decoding at relays [11,23,32]. Relay selection has been investigated when either full ICSI of the system, including that of eavesdropper is available or when the eavesdropper's ICSI is unknown, but the SCSI of the system, including that of eavesdropper is available.

4.1. Optimal Selection: ICSI of All the Links is Known

In the optimal relay selection scheme (OS) for cognitive relay network [11,20,23,32], the relay that maximizes the secrecy capacity of system is selected to forward the source data, but at the same time also keeps received interference power at the PD below a maximum allowable interference level I_m [1]. In this case, ICSI of all the primary and secondary links is available. The relay is taken to be selected if predetermined threshold is satisfied, and P is taken as the number of relays which are selected. When the predetermined threshold is not satisfied, the relay is not selected and Q is taken as the number of relays which are not selected. As the random variable h_{sp} is present in every CDF, the CDFs are not treated independently and the averaging is done over complete selected and not selected set of relays. The probability that the maximum of some independent random variable is less than some quantity, is the probability that all the independent random variables are less than that quantity. The final summation is done over the set S, where S is the set of all possible

combinations of relay $i \in [1, 2.., N]$. The expectation is taken over random variable $\gamma_{sp}, \gamma_{r_i p}$ for obtaining closed-form solution. Considering the fact that an outage event occurs when the secrecy capacity becomes less than the desired secrecy rate R_s, we can evaluate the outage probability of this optimal relay selection scheme as

$$
\begin{aligned}
P_o^{OS}(R_s) = \sum_S \Bigg[\mathbb{E}_{\gamma_{r_i p}} \Bigg[\mathbb{E}_{\gamma_{sp}} \Bigg[\Bigg(\prod_{\substack{\forall i \in [1,P] \\ \text{selected}}} \mathbb{P}[\Gamma_{sr_i} \geq \gamma_{th} | \gamma_{sp}, \gamma_{r_i p}] \Bigg) \Bigg(\prod_{\substack{\forall j \in [1,Q] \\ \text{not selected}}} \mathbb{P}[\Gamma_{sr_j} < \gamma_{th} | \gamma_{sp}, \gamma_{r_i p}] \Bigg) \times \\
\mathbb{P}\Bigg[\max_{\substack{\forall i \in [1,P] \\ \text{selected}}} \{C_s^{ne}\} < R_s | \Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_i p} \Bigg] \Bigg] \Bigg] \Bigg] \\
= \sum_S \Bigg[\mathbb{E}_{\gamma_{r_i p}} \Bigg[\mathbb{E}_{\gamma_{sp}} \Bigg[\Bigg(\prod_{i=1}^{P} \Big(e^{-\frac{\gamma_{th} \beta_{sr_i} \gamma_{sp}}{I_m}} \Big) \Bigg) \Bigg(\prod_{j=1}^{Q} \Big(1 - e^{-\frac{\gamma_{th} \beta_{sr_j} \gamma_{sp}}{I_m}} \Big) \Bigg) \times \\
\prod_{i=1}^{P} \mathbb{P}\left[C_s^{ne} < R_s | \Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_i p} \right] \Bigg] \Bigg] \Bigg] \\
= \sum_S \int_0^{+\infty} \int_0^{+\infty} \Bigg[\Bigg(\prod_{i=1}^{P} \Big(e^{-\frac{\gamma_{th} \beta_{sr_i} x}{I_m}} \Big) \Bigg) \Bigg(\prod_{j=1}^{Q} \Big(1 - e^{-\frac{\gamma_{th} \beta_{sr_j} x}{I_m}} \Big) \Bigg) \times \\
\prod_{i=1}^{P} \mathbb{P}\left[C_s^{ne} < R_s | \Gamma_{sr_i} \geq \gamma_{th}, \gamma_{sp}, \gamma_{r_i p} \right] \Bigg] \theta_{sp} e^{-\theta_{sp} x} \theta_{r_i p} e^{-\theta_{r_i p} y} dx dy \\
= \sum_S \int_0^{+\infty} \int_0^{+\infty} \Bigg[\Big(e^{-\sum_{i=1}^{P} \frac{\gamma_{th} \beta_{sr_i} x}{I_m}} \Big) \Bigg(\prod_{j=1}^{Q} \big(1 - e^{-\beta_j x} \big) \Bigg) \times \\
\prod_{i=1}^{P} \left(1 - \frac{\alpha_{r_i e} e^{-\left(\frac{\rho - 1}{I_m} \right) \beta_{r_i d} y}}{\rho \beta_{r_i d} + \alpha_{r_i e}} \right) \Bigg] \theta_{sp} e^{-\theta_{sp} x} \theta_{r_i p} e^{-\theta_{r_i p} y} dx dy
\end{aligned} \tag{22}
$$

where $\rho = 2^{2R_s}$ and $\beta_j = \frac{\gamma_{th} \beta_{sr_j}}{I_m}$. The middle term $\prod_{j=1}^{Q} \left(1 - e^{-\beta_j x} \right)$ in (22), is further expanded as

$$
\begin{aligned}
\prod_{j=1}^{Q} \left(1 - e^{-\beta_j x} \right) = 1 - \sum_{k_1=1}^{Q} e^{-x \beta_{k_1}} + \sum_{k_1=1}^{Q-1} \sum_{k_2=k_1+1}^{Q} e^{-x \left(\beta_{k_1} + \beta_{k_2} \right)} \\
- \cdots + (-1)^Q \sum_{k_1=1}^{Q-(Q-1)} \sum_{k_2=k_1+1}^{Q-(Q-2)} \\
\cdots \sum_{k_Q = k_{Q-1}+1}^{Q} e^{-x \left(\beta_{k_1} + \beta_{k_2} + \cdots + \beta_{k_Q} \right)} \\
= 1 + \sum_{j=1}^{Q} (-1)^j \sum\nolimits_j e^{-x \beta'_j},
\end{aligned} \tag{23}
$$

where

$$\sum\nolimits_j = \sum_{k_1=1}^{Q-(j-1)} \sum_{k_2=k_1+1}^{Q-(j-2)} \cdots \sum_{k_{j-1}=k_{j-2}+1}^{Q-1} \sum_{k_j=k_{j-1}+1}^{Q}, \tag{24}$$

and $\beta'_j = \sum_{l=1}^{j} \beta_{k_l}$.

Using the results of (23), $P_o^{OS}(R_s)$ for optimal relay selection scheme in closed-form is evaluated as

$$\begin{aligned}
P_o^{OS}(R_s) = \sum_S \int_0^{+\infty} \Bigg[\Bigg(& e^{-\sum_{i=1}^{P} \frac{\gamma_{th}\beta_{sr_i}x}{I_m}} \Bigg) \times \\
& \left(1 + \sum_{j=1}^{Q} (-1)^j \sum\nolimits_j e^{-x\beta'_j}\right) \times \\
& \prod_{i=1}^{P} \left(1 - \frac{\alpha_{r_ie}\theta_{r_ip}}{(\rho\beta_{r_id} + \alpha_{r_ie})\left(\theta_{r_ip} + \left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right)}\right) \Bigg] \theta_{sp} e^{-\theta_{sp}x} dx \\
= \sum_S \int_0^{+\infty} \Bigg[\Bigg(& e^{-\sum_{i=1}^{P} \frac{\gamma_{th}\beta_{sr_i}x}{I_m}} \\
& + \sum_{j=1}^{Q} (-1)^j \sum\nolimits_j e^{-x\left(\beta'_j + \sum_{i=1}^{P} \frac{\gamma_{th}\beta_{sr_i}}{I_m}\right)} \Bigg) \times \\
& \prod_{i=1}^{P} \left(1 - \frac{\alpha_{r_ie}\theta_{r_ip}}{(\rho\beta_{r_id} + \alpha_{r_ie})\left(\theta_{r_ip} + \left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right)}\right) \Bigg] \theta_{sp} e^{-\theta_{sp}x} dx
\end{aligned} \tag{25}$$

The outage probability expression of optimal relay selection scheme for cooperative CRN is obtained from (25) as

$$\begin{aligned}
P_o^{OS}(R_s) = \sum_S \Bigg[\Bigg(& \frac{\theta_{sp}}{\theta_{sp} + \sum_{i=1}^{P} \frac{\gamma_{th}\beta_{sr_i}}{I_m}} \\
& + \sum_{j=1}^{Q} (-1)^j \sum\nolimits_j \frac{\theta_{sp}}{\theta_{sp} + \beta'_j + \sum_{i=1}^{P} \frac{\gamma_{th}\beta_{sr_i}}{I_m}} \Bigg) \times \\
& \prod_{i=1}^{P} \left(1 - \frac{\alpha_{r_ie}\theta_{r_ip}}{(\rho\beta_{r_id} + \alpha_{r_ie})\left(\theta_{r_ip} + \left(\frac{\rho-1}{I_m}\right)\beta_{r_id}\right)}\right) \Bigg]
\end{aligned} \tag{26}$$

The intercept probability of optimal relay selection scheme for cooperative CRN is obtained from (26) by substituting $\rho = 1$ and by excluding the case when none of the relay is selected. The intercept probability expression is given as

$$P_{int}^{OS} = \sum_{S \neq \emptyset} \Bigg[\left(\frac{\theta_{sp}}{\theta_{sp} + \sum_{i=1}^{P} \frac{\gamma_{th}\beta_{sr_i}}{I_m}} + \sum_{j=1}^{Q} (-1)^j \sum\nolimits_j \frac{\theta_{sp}}{\theta_{sp} + \beta'_j + \sum_{i=1}^{P} \frac{\gamma_{th}\beta_{sr_i}}{I_m}} \right) \times$$

$$\prod_{i=1}^{P}\left(\frac{\beta_{r_id}}{\beta_{r_id}+\alpha_{r_ie}}\right)\Bigg] \tag{27}$$

Optimal relay selection requires global monitoring of ICSI [20]. We can reduce the complexity and power consumption of system, by locally monitoring partial ICSI among the nodes, as opposed to globally, and thus can prolong the lifetime of the network [20].

4.2. Optimal Selection: SCSI of All the Links is Known

We have examined another relay selection scheme where, no knowledge of instantaneous channel state information is required [20]. This relay selection method has been proposed in [20], and it requires only the statistical information of all the links for secrecy outage probability measurement. This relay selection method is the optimal one, only when no knowledge of ICSI is available except statistical information. In this scheme, the relay for which the secrecy outage probability of system becomes minimum is selected [20]. The secrecy outage probabilities, $P_o^i(R_s)$ of all the individual single relay systems as obtained in (20) can be first measured, and then we can find the optimal relay i^* [20].
It can be expressed mathematically as

$$i^* = \arg \min_{i\in[1,\cdots,N]} \left(P_o^i(R_s)\right). \tag{28}$$

Since ICSI is not required, power consumption is reduced as no complex channel measurements are necessary. Compared to the ICSI, channel statistics does not considerably change over time and thus, this is a one-time process. Under severe resource constraint like power and computational complexity, this selection scheme can improve the secrecy performance [20]. The performance of optimal relay selection scheme will be better, as improvement is achieved by utilizing the knowledge of ICSI of the system in OS scheme [20], while only SCSI of the system is available for this scheme. This scheme can be useful in the networks, where there is no availability of CSI of the eavesdropper at all the time instants and due to power limitations, the ICSI of other nodes cannot be fed back at all instants to the decision making node.

5. Asymptotic Analysis

In this section, asymptotic analysis of threshold-based dual-hop DF cognitive relay network is presented, under the scenario when there is no direct link between $SS-SE$, subject to interference constraints from the primary user. When we asymptotically increase $SS-SR_i$ and or SR_i-SD link SNRs, as compared to secondary eavesdropper's link, the behavior of the secrecy outage probability becomes significant for the system design. We have considered two cases [20], which are of main importance, 1) balanced case, when average SNRs of $SS-SR_i$ and SR_i-SD link are equal, for all i, and they together tends to infinity, i.e. $1/\beta_{sr_i}=1/\beta_{r_id}=1/\beta\to\infty$, 2) unbalanced case, when either of the $SS-SR_i$ or SR_i-SD for all i, link average SNR tends to infinity, i.e. $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id}=1/\beta\to\infty$, or $1/\beta_{r_id}$ is fixed and $1/\beta_{sr_i}=1/\beta\to\infty$.

5.1. Single Secondary Relay with Balanced Case

In the balanced case, when $1/\beta_{sr_i} = 1/\beta_{r_id} = 1/\beta \to \infty$, the secrecy outage probability for single relay cognitive radio system in (20) is expressed as

$$\begin{aligned} P_o^i(R_s) &= \frac{\beta_{r_id}\left(\rho\theta_{r_ip} + \frac{\alpha_{r_ie}(\rho-1)}{I_m}\right)}{\alpha_{r_ie}\theta_{r_ip}} + \frac{\gamma_{th}\beta_{sr_i}}{I_m\theta_{sp}} \\ &= \beta\left[\frac{\rho\theta_{r_ip} + \frac{\alpha_{r_ie}(\rho-1)}{I_m}}{\alpha_{r_ie}\theta_{r_ip}} + \frac{\gamma_{th}}{I_m\theta_{sp}}\right] \\ &= \frac{1}{\frac{1}{\beta}}\left[\frac{\rho}{\alpha_{r_ie}} + \frac{(\rho-1)}{I_m\theta_{r_ip}} + \frac{\gamma_{th}}{I_m\theta_{sp}}\right] \end{aligned} \tag{29}$$

It can be observed from (29) that at a very high main channel SNR ($1/\beta$), secrecy outage probability is inversely proportional to $1/\beta$ and it tends to zero. It is directly proportional to the secondary eavesdropper channel SNR $1/\alpha_{r_ie}$, required threshold γ_{th} and desired secrecy rate ρ. The secrecy outage probability of this cooperative cognitive system also decreases accordingly, with an increase of maximum allowable interference level I_m at primary destination.
Diversity order is a critical metric to examine how fast the secrecy outage probability decreases, when SNR tends to infinity. Thus, the impact of increase in the number of secondary relays on the outage probability can also be intuitively comprehended. We can define diversity order [11] of system as

$$D = -\lim_{\text{SNR}\to\infty} \frac{\log P_o(\text{SNR})}{\log(\text{SNR})}, \tag{30}$$

where $P_o(\text{SNR})$ is the secrecy outage probability given as function of SNR $= 1/\beta$ in cognitive relay system. With this definition, we can observe that the diversity order of (29) can be computed as one. The power of SNR $= 1/\beta$ in the denominator of (29), is equal to the diversity order, D. As no relay selection is considered, it is intuitive that diversity order of one is obtained by this single relay cognitive system.

5.2. Single Secondary Relay with Unbalanced Case

In the unbalanced case, the behavior of secrecy outage probability in cognitive relay system is studied by asymptotically increasing the average SNR of the $SR_i - SD$ link and keeping the average SNR of the $SS - SR_i$ link fixed, i.e. when $1/\beta_{sr_i}$ is fixed and $1/\beta_{r_id} = 1/\beta \to \infty$.

$$\begin{aligned} P_o^i(R_s) = &\left[1 - \frac{\theta_{sp}}{\theta_{sp} + \frac{\gamma_{th}\beta_{sr_i}}{I_m}}\right] + \\ &\frac{1}{\frac{1}{\beta}}\left[\left(\frac{\theta_{sp}}{\theta_{sp} + \frac{\gamma_{th}\beta_{sr_i}}{I_m}}\right)\left(\frac{\rho\theta_{r_ip} + \frac{\alpha_{r_ie}(\rho-1)}{I_m}}{\alpha_{r_ie}\theta_{r_ip}}\right)\right] \end{aligned} \tag{31}$$

Also, the behavior of secrecy outage probability in cognitive relay system is studied by asymptotically increasing the average SNR of the $SS - SR_i$ link and keeping the average SNR of the

$SR_i - SD$ link fixed, i.e. when $1/\beta_{r_i d}$ is fixed and $1/\beta_{sr_i} = 1/\beta \to \infty$.

$$P_o^i(R_s) = \left[1 - \frac{\alpha_{r_i e}\theta_{r_i p}}{\left(\rho\beta_{r_i d} + \alpha_{r_i e}\right)\left(\frac{\beta_{r_i d(\rho-1)}}{I_m} + \theta_{r_i p}\right)}\right] + \frac{1}{\frac{1}{\beta}}\left[\frac{\gamma_{th}}{I_m\theta_{sp}}\right] \tag{32}$$

The asymptotic secrecy outage probability can be expressed as a summation of an asymptotically varying term with SNR $= 1/\beta$ and a constant quantity. Asymptotically varying term dominates at low SNR, but it vanishes at high SNR. It can be interpreted from (31) and (32) that unbalance is caused due to fixing average SNR of any hop for this dual-hop cognitive relay system. Hence, secrecy outage probability of the cognitive relay system is limited to a constant, even if the average SNR of other secondary hop is increased infinitely [20].

From the above analysis, we can conclude that the outage performance is affected by either of the $SS - SR_i$ or $SR_i - SD$ link quality. The effect of $SS - SR_i$ link quality is neglected in literature by assuming perfect decoding at the DF secondary relays. In our study, for the complete performance analysis of cooperative CRN under interference limitations from the primary user, we have considered the affect of both the $SS - SR_i$ or $SR_i - SD$ link quality [11, 23, 32].

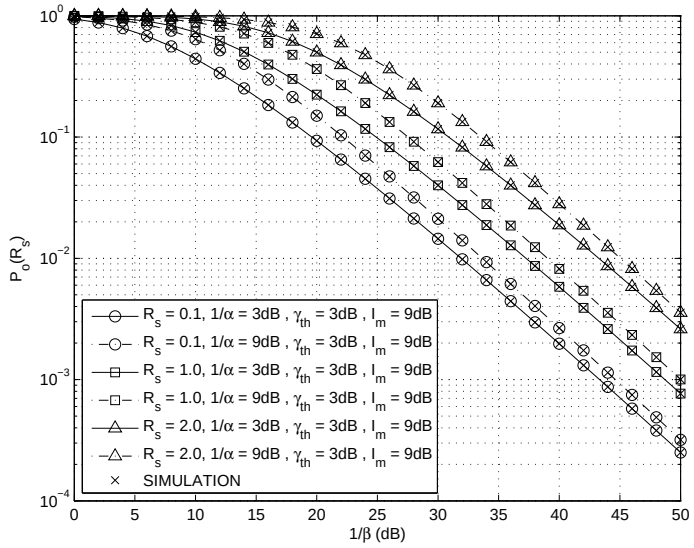

Fig. 2. *Outage probability of single balanced secondary relay system with* $1/\beta$ *in direct* $SS - SE$ *link scenario for* $1/\alpha = 3, 9$ *dB ,* $R_s = 0.1, 1.0, 2.0$ *,* $\gamma_{th} = 3$ *dB and* $I_m = 9$ *dB*

6. Numerical Analysis

In this section, we present and evaluate the analytical results with simulations for a dual-hop threshold-based DF cognitive relay network, under interference limitations from primary user. Noise power is assumed to be same at all the primary and secondary nodes. We have covered

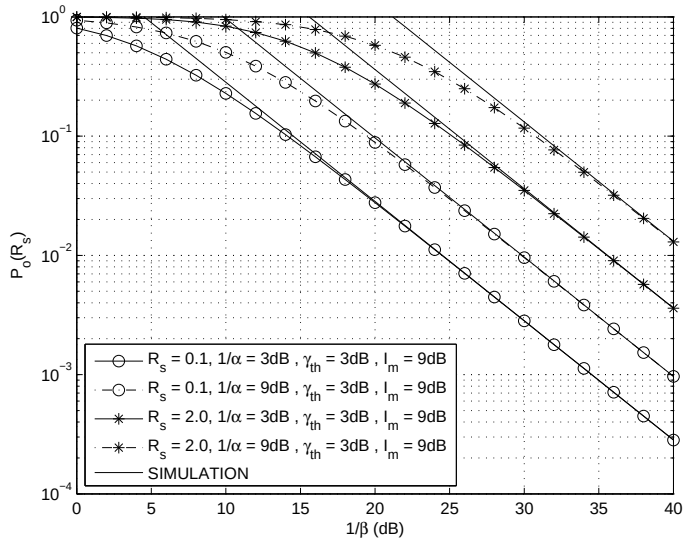

Fig. 3. *Secrecy outage probability of single balanced secondary relay system with* $1/\beta$ *in no direct link scenario for* $1/\alpha = 3, 9$ *dB* , $R_s = 0.1, 2.0$, $\gamma_{th} = 3$ *dB and* $I_m = 9$ *dB*

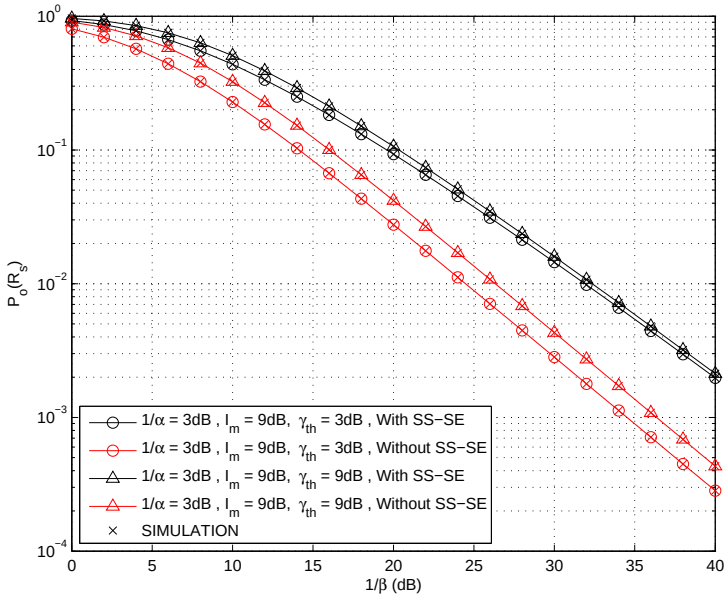

Fig. 4. *Comparison of outage probability of single balanced secondary relay system with* $1/\beta$ *under two scenarios, 1) with direct link between* $SS - SE$ *and 2) with no direct link between* $SS - SE$ *for* $\gamma_{th} = 3, 9$ *dB* , $R_s = 0.1$, $1/\alpha = 3$ *dB and* $I_m = 9$ *dB*

reasonable range of desired secrecy rate, by considering both high and low desired secrecy rate of $R_s = 2.0$ and $R_s = 0.1$.

Fig. 2 shows the outage probability $P_o(R_s)$ of single i^{th} secondary relay in cognitive network , as expressed in (12) for the balanced case under the scenario when direct link is present between

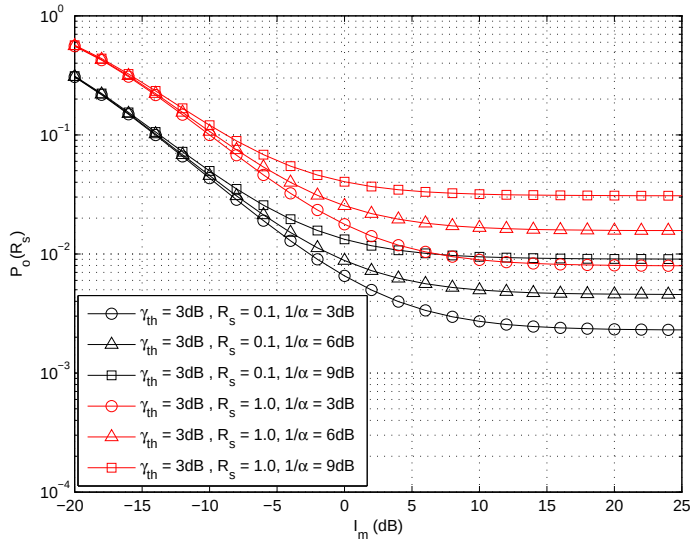

Fig. 5. *Secrecy outage probability of single balanced secondary relay system with I_m in no direct link scenario for $1/\alpha = 3, 6, 9$ dB , $R_s = 0.1, 1.0$ and $\gamma_{th} = 3$ dB*

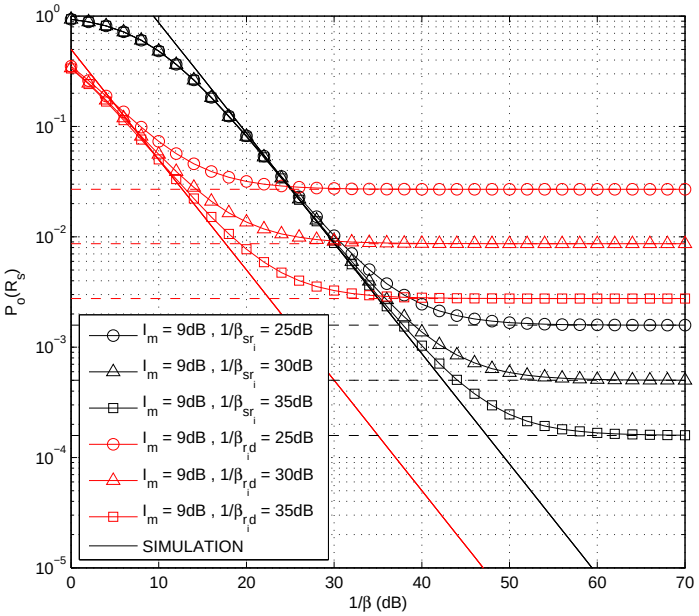

Fig. 6. *Secrecy outage probability of single unbalanced secondary relay system with $1/\beta$ in no direct link scenario for $1/\alpha = 3$ dB , $\gamma_{th} = 3$ dB , $R_s = 1.0$ and $I_m = 9$ dB with $1/\beta_{sr_i} = 25, 30, 35$ dB and $1/\beta_{r_id} = 25, 30, 35$ dB*

secondary source and secondary eavesdropper, with total SNR $1/\beta$. We have plotted the figure with different secondary relay to secondary eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 3, 9$ dB , desired secrecy rate $R_s = 0.1, 1.0, 2.0$ and fixed predetermined threshold $\gamma_{th} = 3$ dB , maximum

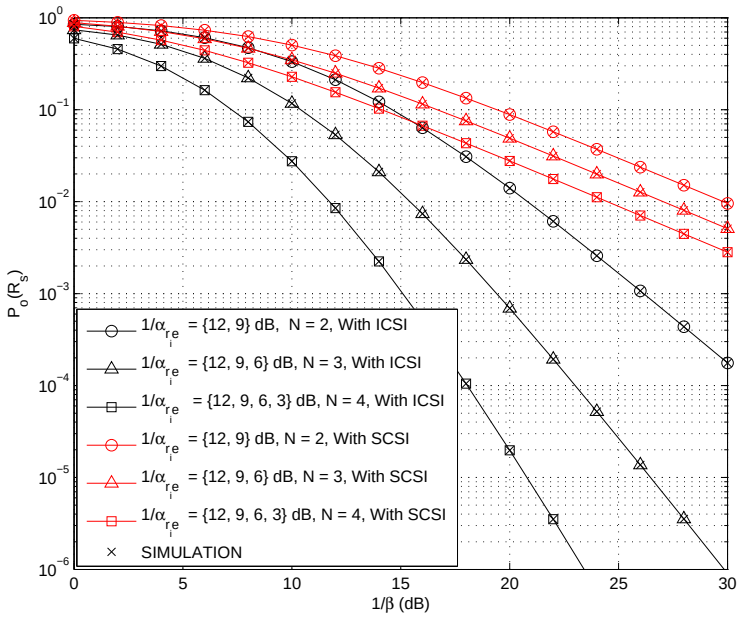

Fig. 7. *Secrecy outage probability of optimal relay selection scheme, when either ICSI or SCSI is known with* $1/\beta$ *in no direct link scenario for* $N = 2, 3, 4$*,* $1/\alpha_{r_ie} = 12, 9, 6, 3$ *dB ,* $R_s = 0.1$*,* $\gamma_{th} = 3$ *dB and* $I_m = 9$ *dB*

tolerable interference level $I_m = 9$ dB, $1/\alpha_{se} = 3$ dB , $1/\theta_{sp} = 3$ dB, $1/\theta_{r_ip} = 3$ dB . It is observed from the figure that the improvement in channel quality of secondary eavesdropper, degrades the $P_o(R_s)$ of the cognitive system. Also, $P_o(R_s)$ increases in function of the desired secrecy rate R_s. Fig. 3 shows the secrecy outage probability $P_o(R_s)$ of single i^{th} secondary relay in cognitive network , as expressed in (20) for the balanced case under the scenario when direct link is not present between both $SS - SD$ and $SS - SE$, with total SNR $1/\beta$. The figure is plotted with different secondary relay to secondary eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 3, 9$ dB, desired secrecy rate $R_s = 0.1, 2.0$ and fixed predetermined threshold $\gamma_{th} = 3$ dB , maximum allowable interference level $I_m = 9$ dB , $1/\theta_{sp} = 3$ dB, $1/\theta_{r_ip} = 3$ dB. It is observed from the figure that the improvement in secondary eavesdropper channel quality degrades the $P_o(R_s)$ of the cognitive system. Also, $P_o(R_s)$ increases in function of the desired secrecy rate R_s. Corresponding asymptotic analysis as expressed in (29) is also shown by solid straight lines passing through the curves.
Fig. 4 shows the comparison of outage probability $P_o(R_s)$ of single i^{th} secondary relay in cognitive network, for the balanced case under two scenarios, 1) when direct link is present between secondary source and secondary eavesdropper and 2) when direct link is not present between secondary source and secondary eavesdropper , with total SNR $1/\beta$. We have plotted the figure with different predetermined threshold $\gamma_{th} = 3, 9$ dB and fixed maximum allowable interference level $I_m = 9$ dB, desired secrecy rate $R_s = 0.1$, secondary relay to secondary eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 3$ dB, $1/\alpha_{se} = 3$ dB, $1/\theta_{sp} = 3$ dB, $1/\theta_{r_ip} = 3$ dB . It is observed from the figure that the $P_o(R_s)$ is more when $SS - SE$ link is present which is intuitive, as compared to when there is no direct link between $SS - SE$. Also, $P_o(R_s)$ increases in function of the predetermined threshold γ_{th} in both the scenarios. This is because with increase in threshold γ_{th}, the probability of the relay to get selected for forwarding source data decreases, thus outage probabil-

ity increases.

Fig. 5 shows the secrecy outage probability $P_o(R_s)$ of single i^{th} secondary relay in cognitive network , as expressed in (20) for the balanced case under the scenario when direct link is not present between both $SS - SD$ and $SS - SE$, with maximum allowable interference level I_m. The figure is plotted with different secondary relay to secondary eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 3, 6, 9$ dB , desired secrecy rate $R_s = 0.1, 1.0$ and fixed predetermined threshold $\gamma_{th} = 3$ dB , $1/\beta_{sr_i} = 30$ dB, $1/\beta_{r_id} = 30$ dB, $1/\theta_{sp} = 3$ dB, $1/\theta_{r_ip} = 3$ dB . It is observed from the figure that with the increase in the maximum allowable interference level I_m , the secrecy outage probability decreases [3]. This can be explained that with an increasing I_m , the secondary users are allowed to transmit with higher power, leading to a decrease of $P_o(R_s)$. One can see from the plot that as I_m increases beyond a certain value, it converges to the respective secrecy outage probability floor. This observation holds true for the other scenario also. It is also observed from the figure that the improvement in secondary eavesdropper channel quality degrades the $P_o(R_s)$ of the cognitive system. Also, $P_o(R_s)$ increases in function of the desired secrecy rate R_s.

Fig. 6 shows the secrecy outage probability $P_o(R_s)$ of single i^{th} secondary relay in cognitive network, as expressed in (20) for the unbalanced case under the scenario when direct link is not present between both $SS - SD$ and $SS - SE$, with average SNR of $1/\beta_{sr_i} = 1/\beta$ at different $1/\beta_{r_id} = 25, 30, 35$ dB with fixed $1/\alpha_{r_ie} = 1/\alpha = 3$ dB , $\gamma_{th} = 3$ dB, desired secrecy rate $R_s = 1.0$, maximum allowable interference level $I_m = 9$ dB, $1/\theta_{sp} = 3$ dB, $1/\theta_{r_ip} = 3$ dB. Also, it is plotted for the unbalanced case with average SNR of $1/\beta_{r_id} = 1/\beta$ at different $1/\beta_{sr_i} = 25, 30, 35$ dB with fixed $1/\alpha_{r_ie} = 1/\alpha = 3$ dB, $\gamma_{th} = 3$ dB, desired secrecy rate $R_s = 1.0$, maximum allowable interference level $I_m = 9$ dB, $1/\theta_{sp} = 3$ dB, $1/\theta_{r_ip} = 3$ dB. It is observed that $P_o(R_s)$ tends to a fixed constant, shown by horizontal dashed line, which is derived in (31) and (32) for a given $1/\beta_{r_id}$ or $1/\beta_{sr_i}$, even if $1/\beta$ increases . From this flooring of curves, we can interpret that the $P_o(R_s)$ is constrained by either of the $SS - SR_i$ or $SR_i - SD$ link quality. It is also interesting to observe from the figure that the asymptotically varying term of (31) and (32) depicted as straight solid line, crosses dashed lines specifically at the point after which average SNR of the hop exceeds average SNR of the other hop [20].

Fig. 7 shows the secrecy outage probability $P_o(R_s)$ of optimal relay selection scheme, when either ICSI or SCSI is known for the cognitive relay system. The figure is plotted with different number of secondary relays $N = 2, 3, 4$ as expressed in (26) and (28), under the scenario when direct link is not present between both $SS - SD$ and $SS - SE$, with total SNR $1/\beta$. This figure is plotted with different secondary relay to secondary eavesdropper average SNR $1/\alpha_{r_ie} = 1/\alpha = 12, 9, 6, 3$ dB, with fixed desired secrecy rate $R_s = 0.1$, $\gamma_{th} = 3$ dB, maximum allowable interference level $I_m = 9$ dB , $1/\theta_{sp} = 3$ dB, $1/\theta_{r_ip} = 3$ dB. It is clearly observed from the figure that $P_o(R_s)$ decreases with the increase in number of secondary relays N. The relay selection will improve the performance of multi-relay cognitive system, when the number of relays is increased, for the case when ICSI of the system is known. Whereas, when ICSI of the system is not available, while only SCSI of the system is known, the secrecy performance can either remain same or increase, when the number of relays is increased, depending on the channel characteristics. Particularly for this numerical analysis, we have shown that when only SCSI of the system is known, the secrecy performance is increasing with the increase in the number of relays. Here, out of N relays, we select the relay for which the secrecy outage probability of the system becomes minimum. The secrecy performance with only SCSI of the system will be less, as compared to the one with ICSI of the system, which is also intuitive as improvement is achieved by utilizing the knowledge of instantaneous channel information of the system.

7. Conclusion

In this paper, we have investigated the intercept and outage probability performance of a threshold-based underlay CRN, under interference constraints from the primary network. The closed-form expressions are evaluated for both with and without the direct link between secondary source and eavesdropper. Asymptotic analysis for both cases is obtained, when average SNRs of secondary source-relay and relay-destination links are equal or unequal. We have shown that the desired secrecy rate, predetermined threshold, eavesdropper channel quality and interference power limitations significantly affects the secrecy performance of the CRN. We have also evaluated the outage and intercept probability for optimal secondary relay selection scheme, when either full ICSI or SCSI of all the links is known. We have shown that the relay selection improves the performance of the multi-relay cognitive system, when the number of relays is increased.

8. References

[1] Al-jamali, M., Al-Nahari, A., AlKhawlani, M. M.: 'Relay selection scheme for improving the physical layer security in cognitive radio networks'. Proc. IEEE 23th Signal Processing and Communications Applications Conference (SIU), 2015, pp. 495-498

[2] Shu, Z., Yang, Y., Qian, Y., Hu, R. Q.: 'Impact of interference on secrecy capacity in a cognitive radio network'. Proc. IEEE Global Telecommunications Conference (GLOBECOM), 2011, pp. 1-6

[3] Zou, Y., Li, X., Liang, Y.-C.: 'Secrecy outage and diversity analysis of cognitive radio systems', *IEEE Journal on Selected Areas in Communications*, 2014, **32**, (11), pp. 2222-2236

[4] Do, N. T., An, B.: 'Secure transmission using decode-and-forward protocol for underlay cognitive radio networks'. Proc. IEEE Seventh International Conference on Ubiquitous and Future Networks (ICUFN), 2015, pp. 914-918

[5] Zou, Y., Wang, X., Shen, W.: 'Physical-layer security with multiuser scheduling in cognitive radio networks', *IEEE Transactions on Communications*, 2013, **61**, (12), pp. 5103-5113

[6] Wyner, A. D.: 'The wire-tap channel', *The Bell System Technical Journal*, 1975, **54**, (8), pp. 1355-1387

[7] Zou, Y., Champagne, B., Zhu, W.-P., Hanzo, L.: 'Relay-selection improves the security-reliability trade-off in cognitive radio systems', *IEEE Transactions on Communications*, 2015, **63**, (1), pp. 215-228

[8] Gu, Q., Wang, G., Fan, R., Zhong, Z.: 'Secure performance analysis of cognitive two-way relay system with an eavesdropper'. Proc. IEEE/CIC International Conference on Communications in China (ICCC), 2014, pp. 176-180

[9] Sakran, H., Shokair, M., Nasr, O., El-Rabaie, S., El-Azm, A. A.: 'Proposed relay selection scheme for physical layer security in cognitive radio networks', *IET Communications*, 2012, **6**, (16), pp. 2676-2687

[10] Yang, J., Chen, L., Ding, J., Hu, X., Mathiopoulos, P. T.: 'Intercept outage probability analysis of cognitive relay networks in presence of eavesdropping attack'. Proc. IEEE 21st Asia-Pacific Conference on Communications (APCC), 2015, pp. 304-308

[11] Zou, Y., Wang, X., Shen, W.: 'Optimal relay selection for physical layer security in cooperative wireless networks', *IEEE Journal on Selected Areas in Communications*, 2013, **31**, (10), pp. 2099-2111

[12] Yang, W., Xu, X., Cai, Y., Zheng, B.: 'Secrecy outage analysis for cooperative DF underlay CRNs with outdated CSI'. Proc. IEEE Wireless Communications and Networking Conference (WCNC), 2014, pp. 416-421

[13] Sibomana, L., Zepernick, H.-J., Tran, H.: 'Achievable secrecy capacity in an underlay cognitive radio network'. Proc.IEEE Conference on Communications and Network Security (CNS), 2014, pp. 1-6

[14] Ding, H., Ge, J., da Costa, D. B., Jiang, Z.: 'Asymptotic analysis of cooperative diversity systems with relay selection in a spectrum-sharing scenario', *IEEE Transactions on Vehicular Technology*, 2011, **60**, (2), pp. 457-472

[15] Lee, J., Wang, H., Andrews, J. G., Hong, D.: 'Outage probability of cognitive relay networks with interference constraints', *IEEE Transactions on Wireless Communications*, 2011, **10**, (2), pp. 390-395

[16] Zhong, C., Ratnarajah, T., Wong, K.-K.: 'Outage analysis of decode-and-forward cognitive dual-hop systems with the interference constraint in Nakagami-*m* fading channels', *IEEE Transactions on Vehicular Technology*, 2011, **60**, (6), pp. 2875-2879

[17] Sagong, S., Lee, J., Hong, D.: 'Capacity of reactive DF scheme in cognitive relay networks', *IEEE Transactions on Wireless Communications*, 2011, **10**, (10), pp. 3133-3138

[18] Xu, W., Zhang, J., Zhang, P., Tellambura, C.: 'Outage probability of decode-and-forward cognitive relay in presence of primary users interference', *IEEE Communications Letters*, 2012, **16**, (8), pp. 1252-1255

[19] Pan, L., Si, J., Li, Z., Huang, H., Chen, J.: 'Optimal relay selection and power allocation for cognitive two-way relay transmission with primary user's interference'. Proc. IEEE Wireless Communications and Networking Conference (WCNC), 2013, pp. 1797-1801

[20] Kundu, C., Ghose, S., Bose, R.: 'Secrecy outage of dual-hop regenerative multi-relay system with relay selection', *IEEE Transactions on Wireless Communications*, 2015, **14**, (8), pp. 4614-4625

[21] Li, D.-J.: 'Outage probability of cognitive radio networks with relay selection', *IET Communications*, 2011, **5**, (18), pp. 2730-2735

[22] Wang, L., Kim, K. J., Duong, T. Q., Elkashlan, M., Poor, H. V.: 'Security enhancement of cooperative single carrier systems', *IEEE Transactions on Information Forensics and Security*, 2015, **10**, (1), pp. 90-103

[23] Krikidis, I.: 'Opportunistic relay selection for cooperative networks with secrecy constraints', *IET Communications*, 2010, **4**, (15), pp. 1787-1791

[24] Ghose, S., Kundu, C., Bose, R.: 'Secrecy performance of dual-hop decode-and-forward relay system with diversity combining at the eavesdropper', *IET Communications*, 2016, **10**, (8), pp. 904-914

[25] Al-Qahtani, F. S., Zhong, C., Alnuweiri, H. M.: 'Opportunistic relay selection for secrecy enhancement in cooperative networks', *IEEE Transactions on Communications*, 2015, **63**, (5), pp. 1756-1770

[26] Son, P. N., Kong, H. Y.: 'The underlay cooperative cognitive network with secure transmission'. Proc. IEEE 27th Biennial Symposium on Communications (QBSC), 2014, pp. 164-167

[27] Proakis, J.: 'Digital Communications' (McGraw-Hill, New York, 2001, 4th edn.)

[28] Barros, J., Rodrigues, M. R.: 'Secrecy capacity of wireless channels'. Proc. IEEE International Symposium on Information Theory, 2006, pp. 356-360

[29] Tourki, K., Qaraqe, K. A., Alouini, M.-S.: 'Outage analysis for underlay cognitive networks using incremental regenerative relaying', *IEEE Transactions on Vehicular Technology*, 2013, **62**, (2), pp. 721-734

[30] Mietzner, J., Lampe, L., Schober, R.: 'Distributed transmit power allocation for multihop cognitive-radio systems', *IEEE Transactions on Wireless Communications*, 2009, **8**, (10), pp. 5187-5201

[31] Lu, T., Liu, P., Panwar, S.: 'Shining a light into the darkness: How cooperative relay communication mitigates correlated shadow fading'. Proc. IEEE 81st Vehicular Technology Conference (VTC Spring), 2015, pp. 1-7

[32] Liu, Y., Wang, L., Duy, T. T., Elkashlan, M., Duong, T. Q.: 'Relay selection for security enhancement in cognitive relay networks', *IEEE Wireless Communications Letters*, 2015, **4**, (1), pp. 46-49