Secrecy Performance of Cognitive Cooperative Industrial Radio Networks

Truong Xuan Quach[1,3], Hung Tran[2], Elisabeth Uhlemann[2], and Mai Tran Truc[3]
[1]TNU-University of Information and Communication Technology, Vietnam.
E-mail: qxtruong@ictu.edu.vn.
[2]School of Innovation, Design, and Engineering, Malardalen University, Sweden.
E-mail: {tran.hung, elisabeth.uhlemann}@mdh.se.
[3]VNU University Engineering and Technology, Vietnam.
Email: mai.tran@vnu.edu.vn.

***Abstract*—Although cognitive radio networks (CRNs) were originally intended as a powerful solution to enhance spectrum utilization, it can also be used to improve reliability by avoiding interference in the 2.4 or 5 GHz band. Using multiple relay nodes in CRNs, the outage probability, i.e., the probability that the end-to-end signal-to-noise ratio drops below a predefined threshold, can be reduced significantly. This implies that the probability that a message is not delivered within a specific time frame, can be kept below a required threshold, even when there are constraints on energy efficiency in terms of peak transmit power. This is particularly useful for industrial networks with real-time constraints. However, using CRNs may also reveal secret information to eavesdroppers (EAVs). Therefore, guaranteeing secure and reliable communications in CRNs is still a challenging problem. To this end, the secrecy performance of a proactive decode-and-forward relaying scheme in a cognitive cooperative radio network is investigated. More specifically, analytical as well as approximate expressions for the secrecy outage probability and probability of non-zero secrecy capacity are derived to evaluate the system performance. Numerical results show that the approximation tightly match the analytical results and simulations, and thus it can be used to provide a fast evaluation of the security and reliability of communications using a considered assignment of relay nodes in a cognitive cooperative radio network (CCRN). Consequently, our results enable to secure the communication, and increasing the reliability, availability, robustness, and maintainability of wireless industrial network, subject to various constraints from the CRN.**

***Index Terms*—Physical Layer Security, Cognitive Radio Networks, Cooperative Communication, Relay Selection, Secrecy Capacity, Industrial Wireless Networks.**

I. INTRODUCTION

Recently, cognitive radio networks (CRNs) have been recognized as one of the most powerful solutions to enhance the spectrum utilization [1]. In a CRN, the secondary user (SU), also known as cognitive user, is permitted to access spectrum belonging to the primary user (PU) provided that the SU does not cause harmful interference to the PU. According to this principle, three spectrum accesses have been proposed, known as underlay, overlay, and interweave [1], of which the spectrum underlay access approach has attracted attention from many researchers due to its simple resource management and without using complex sensing mechanisms [2]. More specifically, in the spectrum underlay approach, the SU is allowed to simultaneously access the licensed spectrum of the PU as long as the interference from the SU to the PU is kept below a predefined threshold. However, when the transmit power of the SU is limited due to interference constraints of the PU, this leads to reduced coverage range and communication capacity of the SU. Moreover, the SU communication information may be vulnerable due to the appearance of illegal eavesdroppers and jamming attackers in the spectrum sharing environment.

To overcome the above drawbacks, wireless physical layer security techniques based on information theory has recently attracted much attention as an efficient method to secure wireless communication [3], [4] and [5]. Basically, the communication is considered secure if the capacity of the main channel is better than the one of the wiretap channel, and then the messages can be transmitted confidently from source to destination without being intercepted by illegal receivers [6]. To improve the security capability for conventional wireless communication, recent works have focused on multiple antennas techniques [7]–[11], artificial noise [12], and cooperative communication [13], [14]. Regarding security in the CRN, works reported in [15]–[21] have investigated many aspects of physical layer security. More specifically, in [17], [18], the authors have studied secrecy rates in CRNs with multiple eavesdroppers. In [19], given the quality of service (QoS) constraints of the PU, multiuser communication strategies have been introduced to improve the security for CRN. Multiuser scheduling mechanisms, the achievable secrecy rate and intercept probability have been examined. Taking the advantages of diversity techniques in relaying communication, in [20], characteristics of selective relaying for security improvement in the CRN have been exploited, the proposed scheme have used the best relay selection to assist the SU and to maximize the achievable secrecy rate without interrupting the PU. In [22], different relay selection strategies to enhance secure communication in cognitive decode-and-forward relay networks was examined. The authors have proposed a pair of relayers for security protection against eavesdropping, in which one relay is first selected to transmit the secrecy information to the destination, while the another relay is used as a friendly jammer to transmit an artificial noise to the eavesdropper.

978-1-5090-6505-9/17/$31.00 2017 IEEE

Although there have been several studies using relaying for physical-layer security in the CRN, studies on cognitive cooperative radio network (CCRN) under joint outage probability constraint of the PU and peak transmit power constraint of the SU are still sparse.

In this paper, we study the secrecy performance in a CCRN in the presence of an eavesdropper (EAV), which is using selection combining (SC) to eavesdrop the transmitted signal of the SU over two hops. Proactive decode-and-forward (DF) relaying is used to enhance the end-to-end capacity over the main channel. Accordingly, adaptive transmit power policy for the SU is considered. To this end, two performance metrics are considered, namely the secrecy outage probability and the probability of non-zero secrecy capacity. Approximation expressions for the secrecy outage probability and probability of non-zero secrecy capacity for the selection combining scheme at the eavesdropper are obtained to provide a fast valuation for the secrecy performance of the CCRN.

The rest of this paper is organized as follows. In Section II, the system model, channel assumptions, secrecy and interference constraints are presented. In Section III, derivations for the power allocation policies and the secure performance for the considered CCRN are derived. In Section IV, numerical examples are provided to analyze the secure performance. Finally, the conclusions are presented in Section V.

II. SYSTEM MODEL

Let us consider a CCRN as shown in Fig. 1 where the secondary transmitter (S-Tx) communicates with a secondary receiver (S-Rx) through the help of N decode-and-forward (DF) relay nodes, while an EAV attempts to overhear the SU's transmission. The S-Tx→S-Rx direct link is absent due to the severe shadowing. For mathematical modelling, the channel gains of S-Tx→SR_i, secondary relay (SR)$_i$→S-Rx, and primary transmitter (P-Tx)→primary receiver (P-Rx) communication links are denoted by $h_{1i}, h_{2i}, i = 1, \ldots, N$, and g_1, respectively. The channel gains of S-Tx→EAV and SR$_i$→EAV eavesdrop links are denoted by f_0 and f_i, respectively. Furthermore, the channel gains of S-Tx→P-Rx, SR$_i$→P-Rx, P-Tx→SR$_i$, P-Tx→S-Rx, and P-Tx→EAV interference links are symbolized by α_0, α_i, β_i, β_0, and g_0, $i = 1, \ldots, N$, respectively. All channels are subject to Rayleigh fading, and channel gains are exponential random variables (RVs). Here, the mean channel gains of α_0, α_i, β_0, β_i, h_{1i}, h_{2i}, f_0, f_i are presented as Ω_{α_0}, Ω_{α}, Ω_{β_0}, Ω_{β}, Ω_{h_1}, Ω_{h_2}, Ω_{f_0}, Ω_{f}, Ω_{g_0}, and Ω_{g_1}, respectively.

In the considered system model, we assume that all relays can decode the information from the S-Tx and the proactive DF scheme is selected to assist the communication between the source and destination, i.e., the best relay selection is selected [23]. Accordingly, the communication is executed in the two phases as follows:

In the first phase, the S-Tx regulates its transmit power to broadcast its signal to N SRs, and the capacity of the S-Tx→SR$_i$ communication link is expressed as follows:

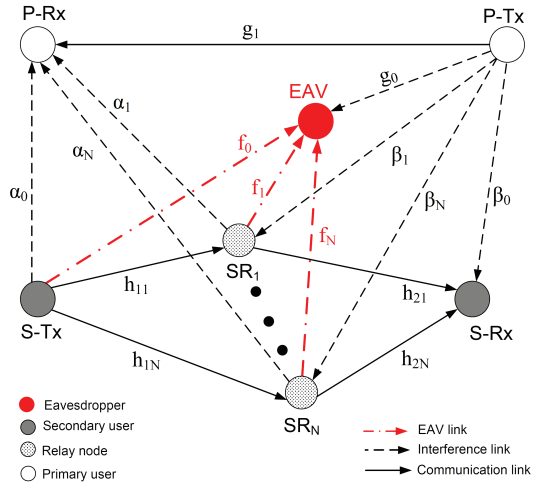

Fig. 1. Model of CCRN where the S-Tx communicates with a S-Rx through the help of N relay nodes. The EAV overhears the information of the S-Tx or SRs.

$$C_{SR_i} = \frac{1}{2} B \log_2(1 + \gamma_{SR_i}) \tag{1}$$

where γ_{SR_i} is signal-to-interference-plus-noise ratio (SINR) at each SR$_i$ and it can be formulated as

$$\gamma_{SR_i} = \frac{P_S h_{1i}}{P_P \beta_i + N_0}, \tag{2}$$

in which P_P, P_S and N_0 are PU transmit power, S-Tx transmit power and noise power, respectively. Note that the transmit power of the S-Tx must be controlled to not degrade the performance of the PU. This can be interpreted into the outage probability constraint of the PU ξ_p and the peak transmit power of the S-Tx P_{pk}^s as follows [24]:

$$\Pr\left\{C_P^{(S-Tx)} < R_p\right\} \leq \xi_p, \tag{3}$$

$$P_S \leq P_{pk}^s, \tag{4}$$

where $C_P^{(S-Tx)}$ is the channel capacity of the P-Tx→P-Rx link under interference from the S-Tx, defined by

$$C_P^{(S-Tx)} = B \log_2\left(1 + \frac{P_P g_1}{P_S \alpha_0 + N_0}\right) \tag{5}$$

When the S-Tx transmits its signal, the EAV manages to overhear, and its capacity in the first phase can be expressed as

$$C_{SE} = \frac{1}{2} B \log_2\left(1 + \gamma_{SE}\right) \tag{6}$$

where γ_{SE} is the SINR at the EAV and it can be defined as

$$\gamma_{SE} = \frac{P_S f_0}{P_P g_0 + N_0} \approx \frac{P_S f_0}{P_P g_0}, \tag{7}$$

in which the EAV is assumed to have a powerful noise filter, thus the noise power is set to zero, i.e. $N_0 = 0$ and the EAV is only subject to the interference from the P-Tx.

In the second phase, one of the SRs is selected, say SR_i, to forward the signal to the S-Rx. Accordingly, the SINRs at the S-Rx and EAV can be formulated, respectively, as

$$\gamma_{RiD} = \frac{P_R h_{2i}}{P_P \beta_0 + N_0}, \tag{8}$$

$$\gamma_{RiE} = \frac{P_R f_i}{P_P g_0 + N_0} \approx \frac{P_R f_i}{P_P g_0}, \tag{9}$$

where P_R is the transmit power of the SR_i. Similar to the first phase, the transmit power of the SR_i in the second phase must satisfy the joint outage probability constraint of the PU and its peak transmit power P_{pk}^r as

$$\Pr\left\{C_P^{(SR_i)} < R_p\right\} \le \xi_p, \tag{10}$$

$$P_R \le P_{pk}^r, \tag{11}$$

where $C_P^{(SR_i)}$ is the channel capacity of the P-Tx$\rightarrow$P-Rx communication link under the interference from the SR_i, and it is formulated as

$$C_P^{(SR_i)} = B\log_2\left(1 + \frac{P_P g_1}{P_R \alpha_i + N_0}\right). \tag{12}$$

In this phase, the EAV listens to the signal from the SR_i, and the capacity of the EAV over illegitimate channels is obtained as

$$C_{RiE} = \frac{1}{2} B\log_2\left(1 + \gamma_{RiE}\right). \tag{13}$$

The end-to-end capacity of the SU communication link is expressed as

$$C_M = \max_{i=1,\ldots,N}\{\min\left\{C_{SR_i}, C_{RiD}\right\}\}. \tag{14}$$

where $C_{RiD} = \frac{1}{2} B\log_2(1+\gamma_{RiD})$. In reality, the EAV can use various advanced processing techniques to decode the overheard signal. Here, the EAV is assumed to use the SC technique, i.e., the EAV compares the received signal in two phases and selects the best one. Accordingly, the end-to-end channel capacity of the EAV over the illegitimate links is obtained as

$$C_E = \max\left\{C_{SE}, C_{R_{i^*}E}\right\} \tag{15}$$

where i^* is index of the selected relay to transmit, i.e.,

$$i^* = \arg\max_{i=\{1,\ldots,N\}}\{\min\left\{C_{SR_i}, C_{RiE}\right\}\}. \tag{16}$$

According to [4], the secrecy capacity of the considered CCRN is defined as the instantaneous secrecy capacity of the secondary network, C_S, is expressed as follows

$$C_S = C_M - C_E, \tag{17}$$

where C_M and C_E are given in (14) and (15), respectively.

To evaluate the system performance, we consider two performance metrics as follows:

- Outage probability of secrecy capacity of the considered CCRN is defined as the probability that secrecy capacity of the CCRN is smaller than a secrecy target rate R, i.e.,

$$\mathcal{O}_{sec} = \Pr\left\{C_S < R\right\}. \tag{18}$$

- Probability of non-zero secrecy capacity is defined as the probability that the secrecy capacity C_S is greater than zero, i.e.,

$$\mathcal{O}_{non-zero} = \Pr\left\{C_S > 0\right\}. \tag{19}$$

III. PERFORMANCE ANALYSIS

In this section, we analyze the secrecy performance of the considered CCRN by using the power allocation policies for the S-Tx and SRs like in [24].

A. Power Allocation Policy for the SU

The secondary network can efficiently utilize the share spectrum at the same time without causing harmful interference to the primary network. To obtained reliable communication of the primary network, we need to consider constraints on the transmit power of the secondary network as follows.

1) The transmit power of S-Tx: From (3), we can calculate power allocation policy for S-Tx as follows

$$\Pr\left\{\frac{P_P g_1}{P_S \alpha_0 + N_0} < \gamma_{th}^p\right\} \le \xi_p, \tag{20}$$

where $\gamma_{th}^p = 2^{\frac{R_p}{B}} - 1$. Applying [24, *Property 1*] for (20), we have

$$1 - \frac{P_P \Omega_{g_1}}{\gamma_{th}^p P_S \Omega_{\alpha_0} + P_P \Omega_{g_1}} \exp\left(-\frac{\gamma_{th}^p N_0}{P_P \Omega_{g_1}}\right) \le \xi_p. \tag{21}$$

After some mathematical manipulations, the transmit power of the S-Tx should satisfy the following constraint

$$P_S \le \frac{P_P \Omega_{g_1}}{\gamma_{th}^p \Omega_{\alpha_0}} \chi, \tag{22}$$

where χ is defined as

$$\chi = \max\left\{0, \frac{1}{1-\gamma_{th}^p} \exp\left(-\frac{\gamma_{th}^p N_0}{P_P \Omega_{g_1}}\right) - 1\right\}^+. \tag{23}$$

By combining (22) with (4), the power allocation policy for the S-Tx is obtained as

$$P_S = \min\left\{P_{pk}^s, \frac{P_P \Omega_{g_1}}{\gamma_{th}^p \Omega_{\alpha_0}} \chi\right\}. \tag{24}$$

2) The transmit power of the SR: Similar in the first phase, the power allocation policy for the SR_{i^*} can be derived from (10) as follows:

$$\Pr\left\{\frac{P_P g_1}{P_R \alpha_i + N_0} < \gamma_{th}^p\right\} \le \xi_p. \tag{25}$$

Applying [24, *Property 1*] for (25), we have

$$1 - \frac{P_P \Omega_{g_1}}{\gamma_{th}^p P_R \Omega_{\alpha} + P_P \Omega_{g_1}} \exp(-\frac{\gamma_{th}^p N_0}{P_P \Omega_{g_1}}) \le \xi_p, \tag{26}$$

After several manipulations, the transmit power of the SR_{i^*} is obtained as

$$P_R \le \frac{P_P \Omega_{g_1}}{\gamma_{th}^p \Omega_{\alpha}} \chi, \tag{27}$$

Combining (27) with (11), a power allocation policy for the SR_{i^*} is obtained as

$$P_R = \min\left(P_{pk}^r, \frac{P_P\Omega_{g_1}}{\gamma_{th}^p\Omega_\alpha}\chi\right). \tag{28}$$

where χ is defined in (23). To derive the secrecy outage probability and the probability of non-zero secrecy capacity, we consider equations (29) and (15) which are equivalent to equations (14) and (15) respectively, as follows:

$$C_M = \frac{1}{2}B\log_2\left(1+\gamma_M\right) \tag{29}$$

$$C_E = \frac{1}{2}B\log_2\left(1+\gamma_E\right) \tag{30}$$

where the SINRs γ_M and γ_E are defined, respectively, as

$$\gamma_M = \max_{i\in\{1,2,\ldots,N\}}\left\{\min\left\{\gamma_{SRi},\gamma_{RiD}\right\}\right\}, \tag{31}$$

$$\gamma_E = \max\left\{\gamma_{SE},\gamma_{R_{i^*}E}\right\}, \tag{32}$$

where $i^* = \arg\max_{i\in\{1,2,\ldots,N\}}\left\{\min\left\{\gamma_{SRi},\gamma_{RiD}\right\}\right\}$.

B. Secrecy Outage Probability

Secrecy Outage probability is defined as the probability that the instantaneous secrecy capacity of the secondary network is less than a target rate R. Thus, we can derive the secrecy outage probability from (29) and (30) as follows:

$$\begin{aligned}\mathcal{O}_{sec} &= \Pr\left\{C_S < R\right\} = \Pr\left\{\log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) < 2^{\frac{2R}{B}}\right\}\\ &= \Pr\left\{\gamma_M \le \delta + (\delta+1)\gamma_E\right\}\end{aligned} \tag{33}$$

where $\delta = 2^{\frac{2R}{B}} - 1$. Accordingly, the outage probability can be obtained by calculating the integral as follows:

$$\mathcal{O}_{sec} = \int_0^\infty \Pr\left\{\gamma_M \le \delta + (\delta+1)x\right\} f_{\gamma_E}(x)dx. \tag{34}$$

To derive $\mathcal{O}_{sec}$ in (34), we need to find the cumulative distribution function (CDF) of γ_M and the probability density function (PDF) of γ_E. Let us commence with derivation for the CDF of γ_M as follows

$$\begin{aligned}F_{\gamma_M}(y) &= \Pr\left\{\max_{i\in\{1,2,\ldots,N\}}\left\{\min\left\{\gamma_{SRi},\gamma_{RiD}\right\}\right\} \le y\right\}\\ &= \int_0^\infty \prod_{i=1}^N \Pr\left\{\min\left\{\frac{P_S h_{1i}}{P_P\beta_i + N_0}, \frac{P_R h_{2i}}{P_P t + N_0}\right\} \le y\right\} f_{\beta_0}(t)dt\\ &= \int_0^\infty \prod_{i=1}^N \left(1 - J_1 J_2\right) f_{\beta_0}(t)dt.\end{aligned} \tag{35}$$

where J_1 and J_2 are defined, respectively, as

$$J_1 = \Pr\left\{\frac{P_S h_{1i}}{P_P\beta_i + N_0} > y\right\}, \tag{36}$$

$$J_2 = \Pr\left\{\frac{P_R h_{2i}}{P_P t + N_0} > y\right\}. \tag{37}$$

Further, the expression J_1 can be obtained as

$$J_1 = 1 - \int_0^\infty \Pr\left\{\frac{P_S h_{1i}}{P_P u + N_0} < y\right\} f_{\beta_i}(u)du. \tag{38}$$

where $f_{\beta_i}(u)du = \frac{1}{\Omega_\beta}\exp(-\frac{u}{\Omega_\beta})$. As a result, the J_1 can be reached as

$$J_1 = \frac{P_S\Omega_{h_1}}{yP_P\Omega_\beta + P_P\Omega_{h_1}}\exp\left(-\frac{yN_0}{P_S\Omega_{h_1}}\right). \tag{39}$$

Further, the closed-form expression for J_2 is easy to obtain as

$$J_2 = 1 - \Pr\left\{\frac{P_R h_{2i}}{P_P t + N_0} < y\right\} = \exp\left(-\frac{y(P_P t + N_0)}{P_R\Omega_{h_2}}\right). \tag{40}$$

Substituting (39) and (40) into (35), the $F_{\gamma_M}(y)$ is rewritten as follows

$$F_{\gamma_M}(y) = \int_0^\infty \prod_{n=1}^N \left[1 - J_1\exp\left(-\frac{y(P_P t + N_0)}{P_R\Omega_{h_2}}\right)\right] f_{\beta_0}(t)dt \tag{41}$$

where $f_{\beta_0}(t) = \frac{1}{\Omega_{\beta_0}}\exp\left(-\frac{t}{\Omega_{\beta_0}}\right)$. Using binomial expression, we have

$$\begin{aligned}F_{\gamma_M}(y) =& \frac{1}{\Omega_{\beta_0}}\sum_{n=0}^N \binom{N}{n}(-J_1)^n \exp\left(-\frac{nN_0 y}{P_R\Omega_{h_2}}\right)\\ &\times \int_0^\infty \exp\left[-\left(\frac{nP_P y}{P_R\Omega_{h_2}} + \frac{1}{\Omega_{\beta_0}}\right)t\right]dt.\end{aligned} \tag{42}$$

By simplifying the integral, the CDF $F_{\gamma_M}(y)$ can be obtained as

$$F_{\gamma_M}(y) = \sum_{n=0}^N \binom{N}{n}\frac{(-1)^n\exp\left(-\frac{y}{D_1(n)}\right)}{(A_1(n)y+1)(B_1 y+1)^n}. \tag{43}$$

where $A_1(n)$, B_1, and $D_1(n)$ are defined, respectively, as

$$A_1(n) = \frac{nP_P\Omega_{\beta_0}}{P_R\Omega_{h_2}},\ B_1 = \frac{P_P\Omega_\beta}{P_S\Omega_{\beta_{h_1}}}, \tag{44}$$

$$\frac{1}{D_1(n)} = \left(\frac{1}{P_S\Omega_{h_1}} + \frac{1}{P_R\Omega_{h_2}}\right)nN_0, \tag{45}$$

Accordingly, the expression $\Pr\left\{\gamma_M \le \delta + (\delta+1)x\right\}$ in (34) can be easily obtained as

$$\Pr\left\{\gamma_M \le \delta + (\delta+1)x\right\} = F_{\gamma_M}(\delta + (\delta+1)x) \tag{46}$$

where $F_{\gamma_M}(\cdot)$ is given in (43).

Now, we derive the PDF of γ_E as follows

$$\begin{aligned}F_{\gamma_E}(y) &= \Pr\left\{\max\left\{\frac{P_S f_0}{P_P g_0}, \frac{P_R f_{i^*}}{P_P g_0}\right\} \le y\right\}\\ &= \int_0^\infty \Pr\left\{\max\left\{\frac{P_S f_0}{P_P u}, \frac{P_R f_{i^*}}{P_P u}\right\} \le y\right\} f_{g_0}(u)du\\ &= 1 - \frac{1}{A_2 y + 1} - \frac{1}{A_3 y + 1} + \frac{1}{(A_2 + A_3)\,y + 1}.\end{aligned} \tag{47}$$

where $A_2 = \frac{P_P \Omega_{g_0}}{P_R \Omega_f}$ and $A_3 = \frac{P_P \Omega_{g_0}}{P_S \Omega_{f_0}}$.

Taking the derivative for the CDF of γ_E, i.e., $f_{\gamma_E}(y) = \frac{dF_{\gamma_E}(y)}{dy}$, yields the PDF of γ_E as follows

$$f_{\gamma_E}(y) = \frac{A_2}{(A_2 y + 1)^2} + \frac{A_3}{(A_3 y + 1)^2} - \frac{A_2 + A_3}{[(A_2 + A_3)\, y + 1]^2}. \tag{48}$$

Substituting (46) and (48) into (41), and setting $t = \delta + (\delta + 1)x$, the secrecy outage probability can be written as

$$\begin{aligned}
\mathcal{O}_{sec} &= \int_{\delta}^{\infty} \frac{F_{\gamma_M}(t)}{\delta + 1} f_{\gamma_E}(\frac{t - \delta}{\delta + 1}) dt \\
&= \sum_{n=0}^{N} \binom{N}{n} \int_{\delta}^{\infty} \frac{(-1)^n exp(-\frac{t}{D_1(n)}) f_{\gamma_E}(\frac{t-\delta}{\delta+1})}{(A_1(n)t + 1)(B_1 t + 1)^n (\delta + 1)} dt, \\
&= I_1(n) + I_2(n) - I_3(n)
\end{aligned} \tag{49}$$

where $I_1(n)$, $I_2(n)$, and $I_3(n)$ are formulated, respectively, as

$$\begin{aligned}
I_1(n) &= \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_2} \\
&\times \int_{\delta}^{\infty} \frac{\exp(-\frac{t}{D_1(n)})}{(B_1 t + 1)^n (t + C_1)^2 (A_1(n)t + 1)} dt,
\end{aligned} \tag{50}$$

$$\begin{aligned}
I_2(n) &= \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_3} \\
&\times \int_{\delta}^{\infty} \frac{\exp(-\frac{t}{D_1(n)})}{(B_1 t + 1)^n (t + C_2)^2 (A_1(n)t + 1)} dt,
\end{aligned} \tag{51}$$

$$\begin{aligned}
I_3(n) &= \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_2 + A_3} \\
&\times \int_{\delta}^{\infty} \frac{\exp(-\frac{t}{D_1(n)})}{(B_1 t + 1)^n (t + C_3)^2 (A_1(n)t + 1)} dt.
\end{aligned} \tag{52}$$

We consider two cases, $n = 0$ and $n >= 1$, as follows:

- Case 1: $n = 0$

$$I_1(0) = \frac{\delta + 1}{A_2} \int_{\delta}^{\infty} \frac{dt}{(t + C_1)^2} = \frac{\delta + 1}{A_2(\delta + C_1)} \tag{53}$$

$$I_2(0) = \frac{\delta + 1}{A_3} \int_{\delta}^{\infty} \frac{dt}{(t + C_2)^2} = \frac{\delta + 1}{A_3(\delta + C_2)} \tag{54}$$

$$I_3(0) = \frac{\delta + 1}{A_2 + A_3} \int_{\delta}^{\infty} \frac{dt}{(t + C_3)^2} = \frac{\delta + 1}{(A_2 + A_3)(\delta + C_3)} \tag{55}$$

- Case 2: $1 \leq n \leq N$, we consider the Lemma as follows To calculate the above integrals, let us consider a lemma as follows:

Lemma 1. *Assuming A, B, C, D, and δ are positive constants, we have*

$$\begin{aligned}
K(A, B, C, D) &= \int_{\delta}^{\infty} \frac{\exp\left(-\frac{x}{D}\right) dx}{(Bx + 1)^n (x + C)^2 (Ax + 1)} \\
&\approx K_{21} + K_{22} + K_{23} + K_{24}
\end{aligned}$$

where K_{21}, K_{22}, K_{23}, and K_{24} are expressed, respectively, as follows:

$$K_{21} = \frac{\mathcal{B}\left[\frac{D_3}{D}, 1 - n, n\right] - \pi \csc(\pi n)}{(D - D_1)(D - D_2)^2 (D - D_3)^n}$$

$$K_{22} = \frac{\pi \csc(\pi n) - \mathcal{B}\left[\frac{D_3}{D_1}, 1 - n, n\right]}{(D - D_1)(D - D_2)^2 (D_1 - D_3)^n}$$

$$\begin{aligned}
K_{23} &= \frac{n - 1 - n\, {}_2F_1\left(1, 1; 2 - n; \frac{D_3}{D_2}\right)}{(n - 1) D_2 (D - D_2)(D_2 - D_1)^2 (D_2 - D_3) D_3^{n-1}} \\
&- \frac{\pi n \csc(\pi n)}{(D - D_2)(D_2 - D_1)^2 (D_2 - D_3)^{n+1}}
\end{aligned}$$

$$K_{24} = \frac{(2D_2 - D - D_1)\left(\pi \csc(\pi n) - \mathcal{B}\left[\frac{D_3}{D}, 1 - n, n\right]\right)}{(D - D_2)^2 (D_2 - D_1)^2 (D_2 - D_3)^n}$$

in which $D_1 = \frac{1 + A\delta}{A}$, $D_2 = \delta + C$, and $D_3 = \frac{B\delta + 1}{B}$. Functions $\csc(x)$, $\mathcal{B}[\cdot, \cdot, \cdot]$, and ${}_2F_1(\cdot, \cdot; \cdot; \cdot)$ are cosecant, incomplete beta function, and hypergeometric functions, respectively.

Proof. Detail proof is presented in Appendix. □

Using the help of $Lemma$ 1, we finally obtain an approximation for secrecy outage probability of the SU as follows:

$$\mathcal{O}_{sec} \approx I_0 + I_1(n) + I_2(n) - I_3(n) \tag{56}$$

where

$$\begin{aligned}
I_0 &= I_1(0) + I_2(0) - I_3(0) \\
I_1(n) &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1) K(A_1(n), B_1, C_1, D_1(n))}{A_2} \\
I_2(n) &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1) K(A_1(n), B_1, C_2, D_1(n))}{A_3} \\
I_3(n) &= \sum_{n=1}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1) K(A_1(n), B_1, C_3, D_1(n))}{A_2 + A_3}
\end{aligned}$$

C. Probability of Non-zero Secrecy Capacity

In security parameters of the system, a probability of non-zero secrecy capacity is given to evaluate whether exists positive security capacity or not. In other words, this parameter expresses probability of the capacity of the main channel is larger than the one of the illegitimate channel. Accordingly, we can obtain the probability of non-zero secrecy capacity by substituting (17) into (19) and set $\delta = 0$ in (33) as follows

$$P_{non-zero}^{sec} = \Pr\{C_{sec} > 0\} \approx 1 - \mathcal{O}_{sec}, \text{ with } \delta = 0. \tag{57}$$

IV. NUMERICAL RESULTS

In this section, we present numerical examples to examine secrecy performance of the CCRN. Without other statements, system parameters are set as follows:

- System bandwidth: $B = 5$ MHz;
- Outage target rate of the PU: $R_p = 64$ Kbps;
- Outage secrecy target rate of the SU: $R = 64$ Kbps;
- Outage probability constraint of the PU: $\xi_p = 0.01$;
- Peak transmit SNR of the S-Tx: $\gamma^s_{pk} = \frac{P^s_{pk}}{N_0} = 20$ (dB);
- Peak transmit SNR of the SR: $\gamma^s_{pk} = \frac{P^r_{pk}}{N_0} = 20$ (dB);
- Number of Relays: $N = 5$;
- Channel mean powers: $\Omega_{g_0} = \Omega_{g_1} = \Omega_{h_1} = \Omega_{h_2} = 10$, $\Omega_\alpha = \Omega_{\alpha_0} = \Omega_\beta = \Omega_{\beta_0} = \Omega_f = \Omega_{f_0} = 0.5$;

Fig. 2 shows the impact of the interference from the P-Tx on the outage secrecy performance by considering three cases as follows:

- Case 1: The channel mean powers of the P-Tx→EAV, S-Tx→P-Rx, P-Tx→S-Rx, and SR→P-Rx interference links are set as a reference case, i.e., $\Omega_{g_0} = 10$, $\Omega_\alpha = \Omega_{\alpha_0} = \Omega_{\beta_0} = 0.5$.
- Case 2: The channel mean power of the P-Tx→EAV is increased, i.e, $\Omega_{g_0} = 14$. This case is used to compare to $Case$ 1.
- Case 3: The channel mean powers of the S-Tx→P-Rx, P-Tx→S-Rx, and SR→P-Rx interference links are increased from $\Omega_\alpha = \Omega_{\alpha_0} = \Omega_{\beta_0} = 0.5$ to $\Omega_\alpha = \Omega_{\alpha_0} = \Omega_{\beta_0} = 2$. This case is used to compare to $Case$ 1.

We can see that the approximate curves match well with analytical curves and simulation results. Also, we can observe that the secrecy performance of $Case$ 2 outperforms $Case$ 1. This can be explained by the fact that the the channel mean power of the P-Tx→EAV in $Case$ 2 is higher than the one in $Case$ 1. This increases interference from the P-Tx to the EAV and then degrades the capacity of the eavesdropper. As a result, the secrecy capacity is improved, i.e., the secrecy

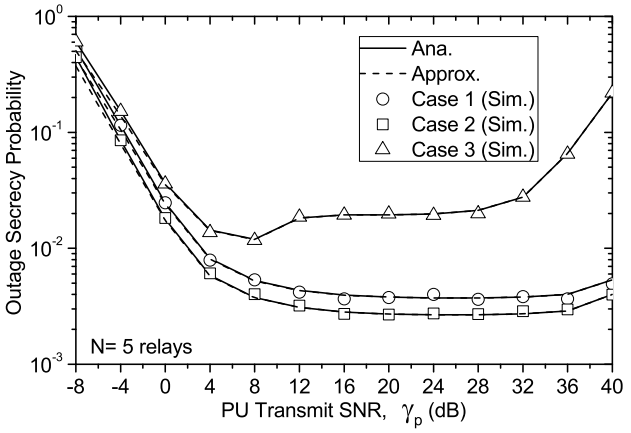

Fig. 2. The outage secrecy probability is a function of the P-Tx transmit SNR with three cases as follows: Case 1: $\Omega_{g0} = 10$, $\Omega_\alpha = \Omega_{\alpha 0} = \Omega_{\beta 0} = 0.5$; Case 2: $\Omega_{g0} = 14$, $\Omega_\alpha = \Omega_{\alpha 0} = \Omega_{\beta 0} = 0.5$; Case 3: $\Omega_{g0} = 10$, $\Omega_\alpha = \Omega_{\alpha 0} = \Omega_{\beta 0} = 2$.

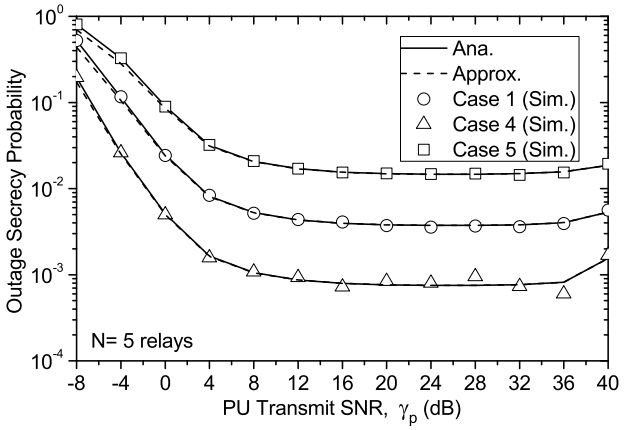

Fig. 3. The Outage probability of Secrecy capacity with: Case 1:$\Omega_{f_0} = \Omega_f = 0.5$; Case 4: $\Omega_{f_0} = \Omega_f = 0.1$; Case 5: $\Omega_{f_0} = \Omega_f = 2$;

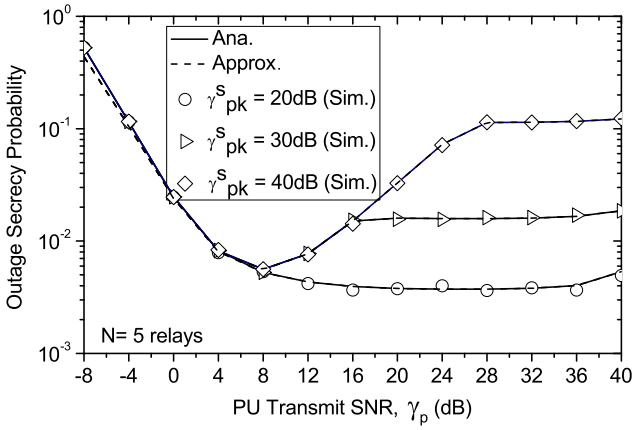

Fig. 4. Secrecy outage probability for different the peak transmit SNR of the S-Tx.

performance is improved. However, when the channel mean powers of interference links between SU and PU are increased in $Case$ 3, the secrecy performance is degraded significantly. This is because that the SUs and PUs cause strong mutual interference to each other. Thus, the S-Tx and SR must reduce its transmit power to not cause harmful interference to the PU. Accordingly, the end-to-end capacity is decreased, i.e., the secrecy capacity is degraded and eventually, the secrecy performance is decreased. Further, we can observe the results from Fig. 3 where the impact of channel mean powers of the S-Tx→EAV and SR→EAV illegitimate links on the secrecy performance of the CCRN are illustrated. Clearly, the higher the channel mean powers of the illegitimate links are, the lower the secrecy performance of CCRN becomes. This is thought due to the fact that the EAV can decode the messages of the SUs more easier as the channel mean powers of the illegitimate links are high.

Fig. 4 illustrates the impact of the peak transmit SNR of the S-Tx on the secrecy outage probability with different values, i.e., $\gamma^s_{pk} = \{20, 30, 40\}$ (dB). Again, we can see that the approximate curves, analytical, and simulation results match

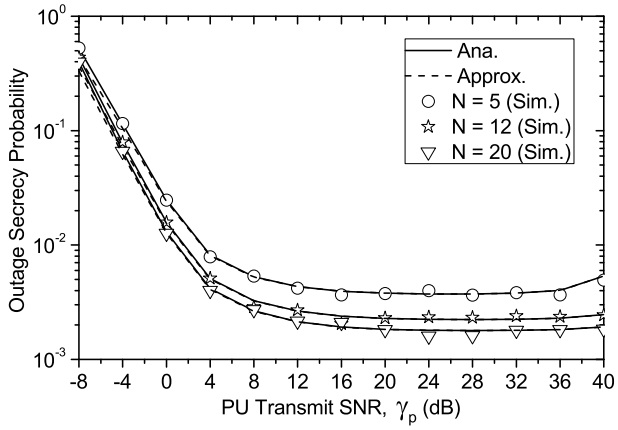

Fig. 5. Secrecy outage probability for different number of SRs.

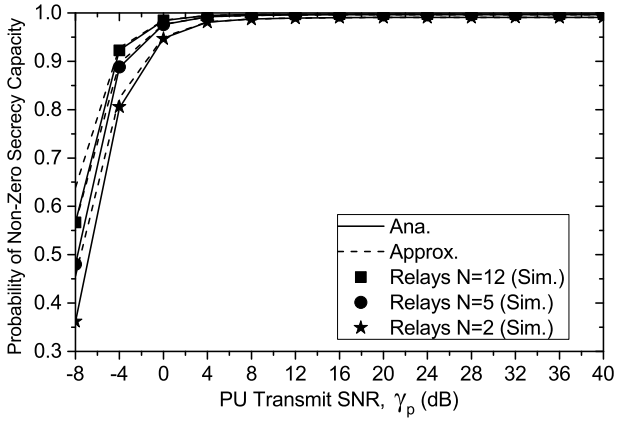

Fig. 6. Probability of the non-zero secrecy capacity for different numbers of relays.

very well. In the low SNR of the P-Tx ($\gamma_p \leq 8$), the outage secrecy probability decreases to an optimal point for all peak transmit SNR of the S-Tx. However, when the transmit SNR of the PU, γ_p, continuously increases, the outage secrecy probability is increased, i.e., the secrecy performance of the SU is degraded. This can be explained that increasing γ_p leads to the performance of the primary network is improved. Accordingly, the S-Tx and SR can increase their transmit SNR with constraint in (24) and (28), and hence the transmit SNR of the S-Tx and SR can approach the its peak values to improve the secrecy performance. However, if the P-Tx transmit SNR increases further, $\gamma_p > 8$ dB, the SUs can not regulate the transmit SNR due to their peak transmit SNR constraint. Therefore, SUs suffer strong interference from the P-Tx, this leads to degrade the secrecy performance of the SU. Moreover, we can see that increase peak transmit SNR of the S-Tx leads to degrade the outage secrecy performance of the SU as $\gamma_p > 8$ dB. This is due to the fact that increasing peak transmit SNR of the S-Tx leads to more messages can arrive at the SRs. However, the SR can not transmit with faster rate due to peak transmit power constraint of the SR. Thus, the SR becomes a bottleneck which degrades the end-to-end secrecy performance. Fig. 5 displays the outage secrecy probability for different number of SRs. It is clear to see that the outage secrecy probability decreases significantly as the number of SRs increases, i.e., $N = 5, 12, 20$. This is thought to be due to the fact that as the number of SRs increases, more available relays assist the S-Tx, and hence the best relay selection is more diverse. As result, the secrecy outage probability of the secondary network is improved.

Finally, we examine the existence of non-zero secrecy capacity for different number of SRs as shown in Fig. 6. It can be seen that in the low transmit SNR of the P-Tx($\gamma_p < 4$ dB), the probability of non-zero secrecy is small, however, in the high regime of the P-Tx transmit SNR, the the probability of non-zero secrecy capacity is approach to 1. We also can see that increasing the number of SR also can improve the probability of non-zero secrecy capacity, however, it is improved not much with high number of SRs, $N = 12$.

V. Conclusions

In this paper, we have examined the secrecy performance of proactive DF relaying scheme in the CCRNs under interferences constraints and an eavesdropper implementing SC technique. More specifically, we have derived approximation expressions for the outage secrecy probability and probability of non-zero secrecy capacity over the Rayleigh fading channels. These expressions can be used to provide a fast valuation for equivalent system models and observe the interaction between different parameters on the secrecy performance. Numerical examples have shown that the approximation results match well with analytical results and simulation. Numerical results have shown that the secrecy performance can be improved by utilizing the channel condition of P-Tx→EAV interference links and when the S-Tx→EAV and SR→EAV illegitimate links are weak.

Appendix

Now, we proof the *Lemma 1* by considering the integral as follows:

$$K = \int_{\delta}^{\infty} \frac{\exp\left(-\frac{x}{D}\right)}{(Bx+1)^n (x+C)^2 (Ax+1)} dx, n \geq 1, \delta > 0 \quad (58)$$

By changing the variable $u = x - \delta$ and using approximation $e^x \approx 1 + x$, we can rewrite the equation (58) as follows

$$K = \int_{0}^{\infty} \frac{\exp(-\frac{u+\delta}{D})}{[B(u+\delta)+1]^n (u+\delta+C)^2 [A(u+\delta)+1]} du$$
$$= \frac{D \exp\left(-\frac{\delta}{D}\right)}{AB^n} \underbrace{\int_{0}^{\infty} \frac{du}{(u+D)(u+D_1)(u+D_2)(u+D_3)^n}}_{K_1},$$

where D_1, D_2, and D_3 are defined, respectively, as

$$D_1 = \frac{1+A\delta}{A},\ D_2 = \delta + C,\ D_3 = \frac{B\delta+1}{B} \quad (59)$$

Further, K_1 can be decomposed into integrals, i.e. $K_1 = K_{21} + K_{22} + K_{23} + K_{24}$, as follows:

$$K_{21} = \frac{-1}{(D-D_1)(D-D_2)^2} \int_0^\infty \frac{du}{(u+D_3)^n (u+D)}$$
$$= \frac{\mathcal{B}\left[\frac{D_3}{D}, 1-n, n\right] - \pi \csc(\pi n)}{(D-D_1)(D-D_2)^2(D-D_3)^n}$$

$$K_{22} = \frac{1}{(D-D_1)(D_1-D_2)^2} \int_0^\infty \frac{du}{(u+D_3)^n (u+D_1)}$$
$$= \frac{\pi \csc(\pi n) - \mathcal{B}\left[\frac{D_3}{D_1}, 1-n, n\right]}{(D-D_1)(D-D_2)^2(D_1-D_3)^n}$$

$$K_{23} = \frac{-1}{(D-D_2)(D_2-D_1)^2} \int_0^\infty \frac{du}{(u+D_3)^n (u+D_2)^2}$$
$$= \frac{n-1-n\,{}_2F_1\left(1,1;2-n;\frac{D_3}{D_2}\right)}{(n-1)D_2(D-D_2)(D_2-D_1)^2(D_2-D_3)D_3^{n-1}}$$
$$- \frac{\pi n \csc(\pi n)}{(D-D_2)(D_2-D_1)^2(D_2-D_3)^{n+1}}$$

$$K_{24} = \frac{2D_2 - D - D_1}{(D-D_2)^2(D_2-D_1)^2} \int_0^\infty \frac{du}{(u+D_3)^n (u+D_2)}$$
$$= \frac{(2D_2 - D - D_1)\left(\pi \csc(\pi n) - \mathcal{B}\left[\frac{D_3}{D}, 1-n, n\right]\right)}{(D-D_2)^2(D_2-D_1)^2(D_2-D_3)^n}$$

where $\csc(x)$, $\mathcal{B}[\cdot,\cdot,\cdot]$, and ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ are cosecant, incomplete beta function, and hypergeometric functions, respectively. Note that K_{21}, K_{22}, K_{23}, and K_{24} can be obtained by using the help of Mathematica software and [25].

ACKNOWLEDGEMENT

The research leading to these results has been performed in the research project of Ministry of Education and Training, Vietnam (No.B2017-TNA-50), and the SafeCOP project which is funded from the ECSEL Joint Undertaking under grant agreement n^0 692529, and from National funding.

REFERENCES

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

[2] H. Yao, Z. Zhou, H. Liu, and L. Zhang, "Optimal power allocation in joint spectrum underlay and overlay cognitive radio networks," in *2009 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, June 2009, pp. 1–5.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[4] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

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

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 356–360.

[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in mimo wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, January 2013.

[8] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "Mimo wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Communications Letters*, vol. 17, no. 9, pp. 1754–1757, September 2013.

[9] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *2007 41st Annual Conference on Information Sciences and Systems*, March 2007, pp. 905–910.

[10] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian mimo wiretap channel," in *2007 IEEE International Symposium on Information Theory*, June 2007, pp. 2471–2475.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

[12] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, Jun 2013.

[13] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, October 2013.

[14] ——, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *2013 IEEE International Conference on Communications (ICC)*, June 2013, pp. 2183–2187.

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

[16] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Communications*, vol. 12, no. 3, pp. 132–150, Mar 2015.

[17] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, May 2008, pp. 1–5.

[18] Y. Pei, Y. c. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over miso cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, April 2010.

[19] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103–5113, December 2013.

[20] H. Sakran, O. Nasr, M. Shokair, E. S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," in *2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug 2012, pp. 1052–1056.

[21] M. Al-jamali, A. Al-nahari, and M. M. AlKhawlani, "Relay selection scheme for improving the physical layer security in cognitive radio networks," in *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, May 2015, pp. 495–498.

[22] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46–49, Feb 2015.

[23] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, Sep. 2007.

[24] H. Tran, H. J. Zepernick, and H. Phan, "Cognitive proactive and reactive df relaying schemes under joint outage and peak transmit power constraints," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1548–1551, August 2013.

[25] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Elsevier, 2007.