IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 26, 2019, accepted January 13, 2020, date of publication January 21, 2020, date of current version January 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968325

Secrecy Performance of Cooperative Cognitive Radio Networks Under Joint Secrecy Outage and Primary User Interference Constraints

TRUONG XUAN QUACH[1,3], HUNG TRAN[2], ELISABETH UHLEMANN[2], AND MAI TRAN TRUC[3]

[1]TNU–University of Information and Communication Technology, Thai Nguyen 0208, Vietnam
[2]School of Innovation, Design, and Engineering, Mälardalen University, 724 80 Västerås, Sweden
[3]VNU University of Engineering and Technology, Ha Noi 100000, Vietnam

Corresponding author: Hung Tran (tran.hung@mdh.se)

This work was supported in part by the SSF Framework Grant Serendipity.

ABSTRACT In this paper, we investigate the secrecy performance of a Cooperative Cognitive Radio Network (CCRN) in the presence of an eavesdropper (EAV). The secondary users (SUs) are subject to three constraints which include peak transmit power level and interference limitation with respect to the primary user (PU) as well as secrecy outage constraints due to the EAV. Secrecy outage is achieved when the EAV cannot decode the targeted signal, but communications in the secondary network is still possible (non-zero capacity exists). Approximation expressions of the secrecy outage probability and the probability of non-zero secrecy capacity are derived to evaluate the secrecy performance. Monte Carlo simulations are provided to examine the accuracy of the derived approximation expressions. Based on this, power allocation policies for the SUs are derived, satisfying all the constraints while maximizing the secrecy performance as well as the quality of service performance of the secondary network. It can be concluded that with knowledge of the channel state information (CSI) of the EAV it is possible to calculate the optimal value for the secrecy outage threshold of the secondary user (SU) which in turn allows maximizing the secrecy performance. Most interestingly, our numerical results illustrate that the secrecy performance of the system is much improved when the parameters obtained using the CSI of the EAV are calculated optimally. Thence, the system can adjust the power allocation so that no eavesdropping occurs even without reducing quality of service (QoS) performance compared to a network without any EAV.

INDEX TERMS Physical layer security, cooperative cognitive radio networks, power allocation, secrecy outage probability, secrecy capacity.

I. INTRODUCTION

The explosive growth of new wireless communication systems in the recent years has lead to spectrum shortage. Due to the tradition of governmental agencies auctioning off fixed frequency bands to different service providers, the radio frequency bands have been used inefficiently during certain periods of times. To solve the problem of spectrum shortage, cognitive radio networks (CRN) was proposed as a promising solution to exploit temporary unused spectrum, termed spectrum holes [1]. More specifically, all users in CRN are classified into two types, named primary user (PU) and secondary user (SU), where the SU utilizes the licensed spectrum belonging to the PU as long as it does not cause harmful interference. To this end, two major spectrum access approaches, termed opportunistic spectrum access and spectrum underlay, have been proposed. In opportunistic spectrum access, the SU takes advantage of spectrum sensing to identify the spectrum holes and use them for their own communication. The disadvantage is that any missed detection made by the SU may cause serious interference to the PU. In spectrum underlay access, the SU is permitted to access the licensed frequency band of the PU simultaneously provided that the interference from the PU to the SU should be kept below a given threshold, e.g. outage constraint, peak interference power or average interference

The associate editor coordinating the review of this manuscript and approving it for publication was Ivan Wang-Hei Ho.

power constraints [2], [3]. This is to ensure that the performance of the PU is not collapsed. Recently, the spectrum underlay approach has received significant attention from the research community due to its simplified control functions and due to not requiring complex sensing mechanisms [4]. However, the interference constraints of the spectrum underlay approach not only narrow the transmission coverage, but also limits the transmit power of the SU. In order to combat channel impairments such as fading or shadowing, improve quality of service (QoS), and expand the coverage range for the SU transmissions. There are several network technologies that are exploited to solve this problem such as D2D Networks, Mobile Opportunistic Networks [5], [6], and cooperative relaying networks [7]–[10]. In particular, the cooperative relaying network is a possible solution to tailored for the cognitive radio network (CRN). With cooperative relaying, the secondary transmitter can transmit its signal to the secondary receiver either through the direct link or via the help of one or more relay nodes. Using proactive decode-and-forward, only the single best relay node is selected for assisting the SU communication [11].

Due to the broadcast nature of wireless signals, security is one of the most challenging issues encountered in wireless networks. This becomes even more serious in CRN as the spectrum band is shared by a secondary network and even more so when cooperative communications is introduced. This problem was addressed in [12] where the secrecy outage performance of cooperative cognitive radio networks (CCRN) was derived under interference constraints from the PU. Secrecy outage is achieved when an eavesdropper (EAV) cannot decode the targeted signal, but communications between nodes in the secondary network is still possible. The solution in [12] indicates that it requires careful power allocation policies to achieve secrecy outage towards the EAV, while also maintaining the interference constraints set by the PU.

As an extension of the work in [12], we study here power allocation policies capable of fulling the secrecy outage constraint as well as the PU interference constraints of the CRN. Considering the above constraints and the channel conditions, the major contributions in this paper are summarised as follows:

- Given the interference limitations from the PU and the secrecy constraints from the EAV, power allocation policies for the secondary network are obtained.
- Based on the obtained power allocation policies, we calculate the minimal value required to achieve secrecy outage, which allows to improve the secrecy performance of the secondary network in the system.
- Approximate expressions for the secrecy outage probability and the probability of non-zero secrecy capacity are calculated to analyze the secrecy performance of the considered system.
- Numerical results illustrate that the secrecy performance when using the optimized secure outage threshold is much improved, to the point where the QoS in the secondary network is just as good as if there was no EAV in the network. In addition, the interference links in the considered system model are useful in preventing eavesdropping.

The remainder of this paper is structured as follows. In Section II, we briefly describe the related works whereas Section III presents the CCRN system model. In Section IV, the secrecy performance measures are outlined, and in Section IV-B, the transmit power, interference and secrecy constraints are detailed. Next, in Section V, the power allocation policies for the SU and secondary relay (SR) are derived. Further, approximate expressions of the secrecy outage probability and probability of non-zero secrecy capacity are derived. In Section VI, the simulations and numerical results are presented and discussed. Finally, conclusions are given in Section VII.

II. RELATED WORK

Traditional security is based on different cryptographic approaches which are set up at higher layers through authentication. These are often complex algorithms and requires high running cost to generate and manage secret keys. Recently, physical layer security has been proposed as a promising approach to achieving secure communications by exploiting the natural physical characteristics of the wireless channel [13]–[18]. According to [19], a message can be transmitted confidently from the source to the destination without being decrypted by an eavesdropper if the capacity of the legitimate channel, i.e., the channel between the transmitter and its intended receiver, is higher than the capacity of the channel between the transmitter and the eavesdropper. Accordingly, many investigations are focused in this direction, namely analyzing and improving this channel capacity difference, aiming to improve the overall security performance for future wireless networks.

Taking advantage of multi-antenna techniques to enhance the capacity of the legitimate channel while reducing the capacity of the eavesdropper channel, the use of multiple antennas for enhanced security has also attracted a lot of attention [20]–[27]. More specifically, in [22]–[24], transmit antenna selections have been used to enhance security for data transmissions. In [25], transmit antenna selection along with maximal ratio combining techniques have been proposed to reduce the probability of overhearing in the secondary network. Similarly, in [13], [28], [29], the authors have proposed multi-user scheduling mechanisms to improve the security of secondary users. In [17], the authors used probability theory to calculate the impact the interference has on the secrecy capacity. In [26], the results show that the transmit power of the SU can be utilized to interfere with the eavesdroppers to enhance the secrecy capacity of the PU. Further, the secrecy capacity of a multiple-input single-out (MISO) channel with and without perfect channel state information (CSI) has been analyzed in [20], [21]. Subject to the constraints emerging from the primary receiver, outage considerations and the peak transmit power of the SU,

the authors in [30] have studied the impact of the interference from the primary transmitter on the security of the secondary network but for point-to-point communication. In [31], power allocation policies for a MISO CRN were studied, when both the SU and the PU are overheard by eavesdroppers. A convex combination of the power control was proposed to reduce the probability of eavesdropping. Considering the interference mitigation via power control policy, Femtocell Network, a kind of high density cognitive radio networks with interference constraints has been investigated as an efficient and cost-effective approach to improve network capacity and coverage [32]. In [27], we investigated a single-input multiple-output (SIMO) CRN which is subject to overhearing of EAV. We derived an optimal power allocation policy for the secondary transmitter, but for point-to-point communication only.

Cooperative communication is known as a virtual multiple-input multiple-output (MIMO) system which can be used to expand the coverage range or improve the reliability of wireless communications. Recently, it has been studied for use also in physical layer security and considered as a promising solution to enhance both the security and the reliability of the communication in CRN [18], [33]–[40]. Specifically, in [39], [40], relay selection strategies have been investigated to enhance the secrecy performance for the CCRNs. In [33], the trade-off between the security and the reliability of the secondary transmissions in CRNs with multi-relayers in the presence of an eavesdropper was studied. In [41], the authors employed maximal ratio combining (MRC) techniques both for decode-and-forward (DF) and amplify and forward (AF) for multi-relayers to analyze the secrecy performance.

In [42], the authors investigated the secrecy outage for DF cooperative CRNs. Also, the intercept outage probability of cognitive AF relaying networks in the presence of eavesdroppers over Rayleigh fading channels is discussed in [36]. Further, the secrecy performance of CCRN has been investigated for both known and unknown CSI. In [43], the authors have studied secrecy outage probability for DF relay CCRN with outdated CSI, whereas an asymptotic analysis for the outage performance of cooperative diversity systems with the assumption of perfect or imperfect CSI has been investigated in [44].

In the existing literature, the security problems of the secondary network in CCRN have been addressed. However, very few studies have investigated the existence of the direct link between the secondary users, and it is often ignored for mathematical simplicity. The random nature of wireless communication also means that direct channel signals at the destination are not always weak. The authors in [45], [46] assume that there exits direct links between the secondary transmitter and the secondary receiver. In [45], the secondary receiver and the EAV use MRC to combine the direct and the relayed signals. Further, a power back-off scheme is proposed to improve the secrecy performance, and finally a closed-form expression for the secrecy outage probability is derived taking into account the PU interference constraints.

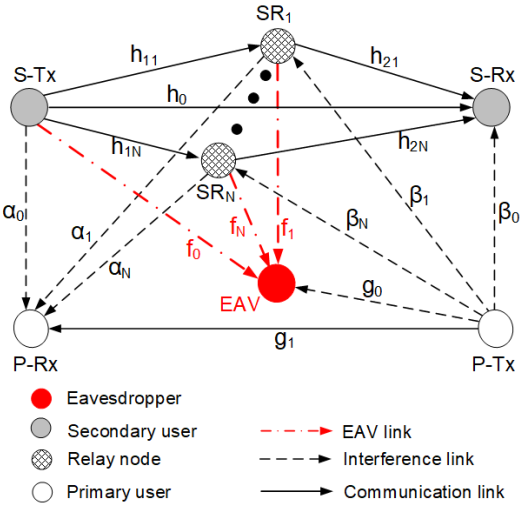


FIGURE 1. A system model of CCRN in which the S-Tx communicates with the S-Rx via a direct link or the help of N SRs, the transmission information can be intercepted by an eavesdropper (EAV).

In [46], a multi-relay DF cognitive relay network with channels which experience Rayleigh fading is studied. The probabilities of nonzero secrecy capacity and the secrecy outage probabilities with the accurate and asymptotic expressions are derived to evaluate the secrecy performance. However, the impact of the interference from the PU to the secondary network and the EAV have not been investigated in the above works. To the best of our knowledge, there is no published research on the use of knowledge about the CSI to calculate the optimal value for the power constraints in order to improve the secrecy performance of the system.

III. SYSTEM MODEL

Let us consider a system model of a CCRN in the presence of an eavesdropper as shown in Figure 1. We assume that the S-Rx) is still within the coverage range of the S-Tx, and therefore, a direct link between S-Tx and S-Rx co-exists with multiple links from S-Tx to N secondary relay (SR). Here, S-Tx can transmit its signal to S-Rx through the direct link or via the help of N DF relay nodes. If the signal over the direct link is week, then the communication takes place via a relay node, using two consecutive time-slots. In the first time slot, S-Tx broadcasts its signal to both S-Rx and all SRs. In the second time-slot, one of the SRs is selected to relay the message to the S-Rx. We use a proactive DF scheme to select the relay node, where only one single relay node is selected for assisting the SU communication [11].

The channel gain of the communication links from the primary transmitter to the primary receiver (P-Tx→P-Rx), as well as the S-Tx→SR$_i$, the SR$_i$ →S-Rx and the S-Tx→S-Rx channel gains are denoted g_1, h_{1i}, h_{2i}, and h_0, $i \in \{1, \ldots, N\}$, respectively. Furthermore, the channel gains of the interference links (i.e., S-Tx→primary receiver (P-Rx), SR$_i$ →P-Rx, primary transmitter (P-Tx)→SR$_i$, P-Tx→S-Rx, and P-Tx→EAV), are denoted $\alpha_0, \alpha_i, \beta_i, \beta_0$ and g_0, for $i = 1, \ldots, N$, respectively. Additionally,

the channel gains of the eavesdropping links S-Tx→EAV, SR_i →EAV are expressed by f_0 and f_i, respectively. All channels are subjected Rayleigh fading and the channel gains are random variables distributed following an exponential distribution. Here, channel mean gains are denoted by $\Omega_{g_1}, \Omega_{h_1}, \Omega_{h_2}, \Omega_{h_0}, \Omega_{\alpha_0}, \Omega_{\alpha_i}, \Omega_{\beta_0}, \Omega_{\beta_i}, \Omega_{g_0}, \Omega_{f_0}$, and Ω_f.

In the first time slot, S-Tx broadcasts its signal to both N SRs and S-Rx. Following Shannon's capacity formula, the capacity of S-Tx→SR_i link is expressed as

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

where γ_{SR_i} represents the signal-to-interference-plus-noise ratio (SINR) at SR_i and is defined as follows

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

in which P_P, P_S are the PU and SU transmit powers, and N_0 is the additive noise power. In the direct link, S-Tx transmits its signal directly to S-Rx without relaying. Thus, the capacity of the S-Tx→S-Rx link is given as

$$C_{SD} = B \log_2(1 + \gamma_{SD}), \tag{3}$$

where γ_{SD} is the SINR of the S-Tx→S-Rx link and is formulated as

$$\gamma_{SD} = \frac{P_S h_0}{P_P \beta_0 + N_0}. \tag{4}$$

According to the broadcast nature of the radio signal, the SU'transmission may be overheard by the EAV. Thus, the channel capacity at the EAV when S-Tx transmits is

$$C_{SE} = \frac{1}{2} B \log_2(1 + \gamma_{SE}), \tag{5}$$

where γ_{SE} is the SINR of the S-Tx→EAV link given by

$$\gamma_{SE} = \frac{P_S f_0}{P_P g_0 + N_0} \approx \frac{P_S f_0}{P_P g_0}. \tag{6}$$

Here, we assume that the EAV is only affected by the interference from the PU, i.e., $P_P g_0 \gg N_0$.

In the second time slot, one of the SRs is selected to forward the source signal to S-Rx. Accordingly, we obtain the capacity of the SR_i →S-Rx channel as follows

$$C_{R_iD} = \frac{1}{2} B \log_2(1 + \gamma_{R_iD}), \tag{7}$$

where γ_{R_iD} is the SINR of the SR_i →S-Rx link and is written as

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

where, P_R is the transmit power of the SR. In this time slot, the transmitted signal of the SR_i can be overheard by the EAV, and the channel capacity is

$$C_{R_iE} = \frac{1}{2} B \log_2(1 + \gamma_{R_iE}), \tag{9}$$

where γ_{R_iE} is the SINR of the SR_i →EAV link and it is expressed as

$$\gamma_{R_iE} = \frac{P_R f_i}{P_P g_0 + N_0} \approx \frac{P_R f_i}{P_P g_0}. \tag{10}$$

This model uses the proactive DF scheme to select the relay node, where the end-to-end capacity of the SU'communication is expressed as

$$C_{E2E} = \max_{i \in \{1,2,\ldots,N\}} \{C_{SD}, \min\{C_{SR_i}, C_{R_iD}\}\}. \tag{11}$$

On the other hand, the EAV's overhearing occurs during two time slots, both S-Tx→EAV and SR_i →EAV. It can therefore use selection combining (SC) to processing the signal. Accordingly, the achievable capacity at the EAV is obtained as

$$C_E = \max\left\{C_{SE}, C_{R_{i^*}E}\right\} \tag{12}$$

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

$$i^* = \arg \max_{i \in \{1,\ldots,N\}} \{\min\left\{C_{SR_i}, C_{RiD}\right\}\}. \tag{13}$$

IV. CONSTRAINTS AND PERFORMANCE METRICS

A. SECRECY PERFORMANCE MEASURES

The secrecy capacity (C_S) is defined as the difference between the capacity of the main channel and the capacity of the eavesdropper's channel, a.k.a. the wiretap link [19]. Consequently, the secrecy capacity of SU is expressed as follows

$$C_S = [C_{E2E} - C_E]^+, \tag{14}$$

where C_{E2E} and C_E are defined in (11) and (12), respectively.

The system fail when the information is not secure and/or reliable. Thus, to assess the security performance of the system, we need to consider the following performance metrics:

- Secrecy outage probability: For a given secrecy target rate R, the secrecy outage probability of a CCRN is defined as the probability that the secrecy capacity is smaller than R, i.e.,

$$\mathcal{O}_{SEC} = \Pr\{C_S < R\}. \tag{15}$$

- Probability of non-zero secrecy capacity: According to [19], the secrecy capacity is zero when the signal-to-noise ratio (SNR) in the EAV's channel is larger than the SINR of the legitimate channels and it is positive when the SINR of the EAV's channel is smaller than the SNR of the legitimate channels. Based on (14), the probability of the existence of non-zero secrecy capacity (possibility to eavesdrop exists) is defined as follows

$$\mathcal{O}_{nonZero} = \Pr\{C_S > 0\}. \tag{16}$$

B. TRANSMIT POWER, INTERFERENCE AND SECRECY CONSTRAINTS

In this section, we study the power allocation policies of the SU on the basis of the CSI from wireless channels in the system model [47]–[49].

Firstly, the S-Tx and SR must control their transmit power so that their interference power impact to the PU is not greater than the interference threshold allowed by the PU. Accordingly, their transmit power must satisfy the interference constraint given by the PU [30] as follows:

- Constraint on the power of P-Tx→P-Rx link when the S-Tx transmits its signals,

$$\mathcal{O}_{I_1} = \Pr\left\{\frac{P_S\alpha_0}{N_0} \geq I_{th}\right\} \leq \xi_P, \tag{17}$$

$$0 \leq P_S \leq P_{pk}^S, \tag{18}$$

  where I_{th} is the interference power threshold of the P-Rx, P_{pk}^S is the peak transmit power of the S-Tx, and ξ_P is the outage probability constraint to not degrade the performance of the PU.
- Constraint on the power of the P-Tx→P-Rx link when the SR_{i^*} is selected to transmit its signals,

$$\mathcal{O}_{I_2} = \Pr\left\{\frac{P_R\alpha_{i^*}}{N_0} \geq I_{th}\right\} \leq \xi_P, \tag{19}$$

$$0 \leq P_R \leq P_{pk}^R, \tag{20}$$

  where P_{pk}^R is the peak transmit power of SR.

On the other hand, based on the CSI of the EAV being available, S-Tx and SR_i must adjust their transmit power so as to not reveal their confidential information to the EAV. Consequently, the transmit powers of S-Tx and SR_i should satisfy two secrecy constraints as follows

$$\mathcal{O}_{SE} = \Pr\{C_{SE} > R\} \leq \epsilon, \tag{21}$$

$$\mathcal{O}_{R_{i^*}E} = \Pr\left\{C_{R_{i^*}E} > R\right\} \leq \epsilon. \tag{22}$$

where ϵ is the secrecy outage constraint given by the SU.

V. POWER ALLOCATION POLICIES

In this section, the power allocation policy for the secondary network is derived on the basis of the constraints on power and interference from the primary network and the constraints on secrecy due to the presences of an eavesdropper. Next, we analyze the secrecy performance of the CCRN based on these power allocation policies.

A. TRANSMISSION POWER ALLOCATION POLICIES

To obtain the power allocation policies for the secondary network, we need to analyze the outage probabilities given in (17) and (19), and the secrecy outage probabilities given in (21) and (22).

1) THE TRANSMIT POWER OF S-Tx GIVEN THE INTERFERENCE THRESHOLD OF PU

From (17), we analyze $\mathcal{O}_{I_1}$ as follows

$$\begin{aligned}\mathcal{O}_{I_1} &= \Pr\left\{\frac{P_S\alpha_0}{N_0} \geq I_{th}\right\} \leq \xi_P \\ &= \Pr\left\{\alpha_0 \geq \frac{I_{th}N_0}{P_S}\right\} \leq \xi_P \\ &= 1 - \Pr\left\{\alpha_0 < \frac{I_{th}N_0}{P_S}\right\} \leq \xi_P \\ &= \exp\left(-\frac{I_{th}N_0}{P_S\Omega_{\alpha_0}}\right) \leq \xi_P.\end{aligned} \tag{23}$$

After some mathematical calculations, it can be concluded that the transmit power of S-Tx is subject to the following constraint

$$P_S \leq \frac{I_{th}N_0}{\Omega_{\alpha_0}\ln(\frac{1}{\xi_P})}. \tag{24}$$

2) THE TRANSMIT POWER OF THE SELECTED RELAY NODE SR_i GIVEN THE INTERFERENCE THRESHOLD OF PU

Similar, from (19) we have

$$\begin{aligned}\mathcal{O}_{I_2} &= \Pr\left\{\frac{P_R\alpha_{i^*}}{N_0} \geq I_{th}\right\} \leq \xi_P \\ &= \Pr\left\{\alpha_{i^*} \geq \frac{I_{th}N_0}{N_0P_R}\right\} \leq \xi_P \\ &= 1 - \Pr\left\{\alpha_{i^*} < \frac{I_{th}N_0}{P_R}\right\} \leq \xi_P \\ &= \exp\left(-\frac{I_{th}N_0}{P_R\Omega_{\alpha_i}}\right) \leq \xi_P.\end{aligned} \tag{25}$$

After some mathematical calculations, it can be concluded that the transmit power of SR_i should be bound as follows

$$P_R \leq \frac{I_{th}N_0}{\Omega_{\alpha_{i^*}}\ln(\frac{1}{\xi_P})}. \tag{26}$$

3) THE TRANSMIT POWER OF THE S-Tx GIVEN THE SECRECY OUTAGE CONSTRAINT DUE TO EAV

Under the assumption that S-Tx has information of the EAV's CSI, it must control its transmit power according to the constraint given in (21), i.e.,

$$\begin{aligned}\mathcal{O}_{SE} &= \Pr\{C_{SE} > R\} \leq \epsilon \\ &= \Pr\left\{\frac{1}{2}B\log_2\left(1 + \frac{P_Sf_0}{P_Pg_0}\right) > R\right\} \leq \epsilon \\ &= 1 - \Pr\left\{\frac{1}{2}B\log_2\left(1 + \frac{P_Sf_0}{P_Pg_0}\right) < R\right\} \leq \epsilon \\ &= 1 - \epsilon \leq \Pr\left\{\frac{f_0}{g_0} < \frac{P_P\gamma_{th}^e}{P_S}\right\},\end{aligned} \tag{27}$$

where $\gamma_{th}^e = 2^{\frac{2R}{B}} - 1$. Using probability formula in (27), we obtain the maximal transmission power of S-Tx as follows

$$1 - \epsilon \leq \int_0^\infty \Pr\left\{f_0 < \frac{P_P\gamma_{th}^e u}{P_S}\right\} f_{g_0}(u)du,$$

$$1-\epsilon \le \int_0^\infty \left[1-\exp\left(-\frac{P_P\gamma_{th}^e u}{P_S\Omega_{f_0}}\right)\right] \times \left[\frac{1}{\Omega_{g_0}}\exp\left(-\frac{u}{\Omega_{g_0}}\right)\right] du,$$

$$\frac{1}{\Omega_{g_0}}\int_0^\infty \exp\left[-\left(\frac{P_P\gamma_{th}^e}{P_S\Omega_{f_0}}+\frac{1}{\Omega_{g_0}}\right)u\right] du \le \epsilon,$$

$$P_S \le \frac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)}. \tag{28}$$

4) THE TRANSMIT POWER OF THE SELECTED RELAY NODE SR$_i$ UNDER THE SECRECY OUTAGE CONSTRAINT DUE TO THE EAV

we can derive the secrecy outage probability of SR$_i$ based on (22) as follows

$$\begin{aligned}\mathcal{O}_{R_{i^*}E} &= \Pr\left\{C_{R_{i^*}E} > R\right\} \le \epsilon \\ &= \Pr\left\{\frac{1}{2}B\log_2\left(1+\frac{P_R f_{i^*}}{P_P g_0}\right) > R\right\} \le \epsilon \\ &= 1-\Pr\left\{\frac{1}{2}B\log_2\left(1+\frac{P_R f_{i^*}}{P_P g_0}\right) < R\right\} \le \epsilon \\ &= 1-\epsilon \le \Pr\left\{\frac{f_{i^*}}{g_0} < \frac{P_P\gamma_{th}^e}{P_R}\right\},\end{aligned} \tag{29}$$

where $\gamma_{th}^e = 2^{\frac{2R}{B}} - 1$. Similarly, we calculate the probability formula in (29) as follows

$$P_R \le \frac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_{i^*}}\left(\frac{1}{\epsilon}-1\right)}. \tag{30}$$

5) POWER ALLOCATION POLICY FOR THE SU AND THE SR$_i$

From the analysis in the previous sections, we obtain the transmit power allocation polices for S-Tx by combining the constraints (18), (24), and (28) together as

$$P_S = \min\left\{P_{pk}^S, \frac{I_{th}N_0}{\Omega_{\alpha_0}\ln(\frac{1}{\xi_P})}, \frac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)}\right\}, \tag{31}$$

whereas the power allocation policy for SR$_i$ is derived from (20), (26), and (30) according to

$$P_R = \min\left\{P_{pk}^R, \frac{I_{th}N_0}{\Omega_{\alpha_{i^*}}\ln(\frac{1}{\xi_P})}, \frac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_{i^*}}\left(\frac{1}{\epsilon}-1\right)}\right\}. \tag{32}$$

From (31) and (32), we can see that the system is subject to the secure outage constraint ϵ. If the secure outage constraint is not optimally selected, the secure performance will be degraded significantly. To guarantee that the value of the selected secure outage constraint will not degrade the system performance, we need to find the optimal value for ϵ on the basis of the available parameters as follows:

We can rewrite (31) as follows

$$P_S = \min\left\{P_I^S, \frac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)}\right\}, \tag{33}$$

where $P_I^S = \min\left\{P_{pk}^S, \frac{I_{th}N_0}{\Omega_{\alpha_0}\ln(\frac{1}{\xi_P})}\right\}$.

In other words, we have

$$P_S = \begin{cases} P_I^S, & P_I^S < \dfrac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)} \\ \dfrac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)}, & P_I^S \ge \dfrac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)}. \end{cases} \tag{34}$$

From the transmit power equations given in (34), it is expected that the secrecy performance of the system will improve when P_S equals P_I^S. The secondary network depends only on the internal constraints of the system. And thus, the SU can control its transmit power close to the threshold given by the QoS constraint of the system without violating the secrecy constraint, i.e., the secure outage threshold (ϵ) should satisfy the condition as follows:

$$\epsilon \le \frac{\Omega_{f_0}P_I^S}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_0}P_I^S}. \tag{35}$$

Similarly, the (32) can be rewritten as

$$P_R = \begin{cases} P_I^R, & P_I^R < \dfrac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)} \\ \dfrac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)}, & P_I^R \ge \dfrac{P_P\gamma_{th}^e\Omega_{g_0}}{\Omega_{f_0}\left(\frac{1}{\epsilon}-1\right)} \end{cases} \tag{36}$$

where $P_I^R = \min\left\{P_{pk}^R, \frac{I_{th}N_0}{\Omega_{\alpha_{i^*}}\ln(\frac{1}{\xi_P})}\right\}$.

As a result, the secure outage constraint ϵ at the SR should satisfy the following condition

$$\epsilon \le \frac{\Omega_{f_{i^*}}P_I^R}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_{i^*}}P_I^R}. \tag{37}$$

Combining (35) and (37), the secure outage threshold (ϵ) should satisfy the following condition

$$\epsilon \le \min\left\{\frac{\Omega_{f_0}P_I^S}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_0}P_I^S}, \frac{\Omega_{f_{i^*}}P_I^R}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_{i^*}}P_I^R}\right\}. \tag{38}$$

Clearly, the maximum value of the secure outage constraint can be calculated by the available parameters as follows:

$$\epsilon_{\max} = \min\left\{\frac{\Omega_{f_0}P_I^S}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_0}P_I^S}, \frac{\Omega_{f_{i^*}}P_I^R}{P_P\gamma_{th}^e\Omega_{g_0}+\Omega_{f_{i^*}}P_I^R}\right\}. \tag{39}$$

B. SECURE COMMUNICATION PROBABILITY OF THE CCRN

To evaluate the secrecy performance of the consider system, we need to analyze the two performance metrics in (15) and (16) based on the obtained power allocation policies of S-Tx and SR.

1) SECRECY OUTAGE PROBABILITY

From (15), we can rewrite $\mathcal{O}_{SEC}$ as follows

$$\begin{aligned}\mathcal{O}_{SEC} &= \Pr\{C_S < R\} = \Pr\left\{\frac{1+\gamma_{E2E}}{1+\gamma_E} < 2^{\frac{2R}{B}}\right\} \\ &= \Pr\{\gamma_{E2E} \le \delta + (\delta+1)\gamma_E\}, \end{aligned} \tag{40}$$

where $\delta = 2^{\frac{2R}{B}} - 1$, the end-to-end SINR of the γ_E and γ_{E2E} are defined, respectively, as

$$\gamma_E = \max\left\{\gamma_{SE}, \gamma_{R_{i^*}E}\right\}, \tag{41}$$

$$\gamma_{E2E} = \max\{\gamma_{SD}, \gamma_M\}, \tag{42}$$

where γ_M is obtained by the relaying selection strategy as

$$\gamma_M = \max_{i\in\{1,2,\ldots,N\}} \{\min\{\gamma_{SRi}, \gamma_{RiD}\}\}. \tag{43}$$

To derive this secrecy outage probability, we need to calculate the integral as follows

$$\mathcal{O}_{SEC} = \int_0^\infty \Pr\{\gamma_{E2E} \le \delta + (\delta+1)x\} f_{\gamma_E}(x)dx. \tag{44}$$

To calculate the formula in (44), we derive the cumulative distribution function (CDF) of γ_{E2E} and the probability density function (PDF) of γ_E. The CDF of γ_{E2E} can be computed as follows:

$$\begin{aligned} F_{\gamma_{E2E}}(t) &= \Pr\{\max\{\gamma_{SD}, \gamma_M\} \le t\} \\ &= \int_0^\infty \Pr\left\{\max\left\{\frac{P_S h_0}{P_P x + N_0}, \gamma_M\right\} \le t\right\} f_{\beta_0}(x)dx, \\ &= \int_0^\infty \Pr\left\{\frac{P_S h_0}{P_P x + N_0} \le t\right\} \Pr\{\gamma_M \le t\} f_{\beta_0}(x)dx, \\ &= \int_0^\infty P_1 P_2 f_{\beta_0}(x)dx, \end{aligned} \tag{45}$$

where P_1 and P_2 are represented, respectively, as

$$P_1 = \Pr\left\{\frac{P_S h_0}{P_P x + N_0} \le t\right\}, \tag{46}$$

$$P_2 = \Pr\{\gamma_M \le t\}. \tag{47}$$

Next, P_1 is easily obtained as

$$\begin{aligned} P_1 &= \Pr\left\{\frac{P_S h_0}{P_P x + N_0} \le t\right\} = \Pr\left\{h_0 \le \frac{(P_P x + N_0)t}{P_S}\right\} \\ &= 1 - \exp\left\{-\frac{(P_P x + N_0)t}{P_S \Omega_{h_0}}\right\} \\ &= 1 - \exp\left\{-\frac{P_P x t}{P_S \Omega_{h_0}}\right\} \exp\left\{-\frac{N_0 t}{P_S \Omega_{h_0}}\right\}. \end{aligned} \tag{48}$$

Further, P_2 is calculated as

$$\begin{aligned} P_2 &= \Pr\{\gamma_M \le t\} \\ &= \prod_{i=1}^N \Pr\left\{\min\left\{\frac{P_S h_{1i}}{P_P \beta_i + N_0}, \frac{P_R h_{2i}}{P_P x + N_0}\right\} \le t\right\} \\ &= \prod_{i=1}^N \left[1 - \Pr\left\{\min\left\{\frac{P_S h_{1i}}{P_P \beta_i + N_0}, \frac{P_R h_{2i}}{P_P x + N_0}\right\} > t\right\}\right] \\ &= \prod_{i=1}^N \left[1 - \Pr\left\{\frac{P_S h_{1i}}{P_P \beta_i + N_0} > t\right\} \Pr\left\{\frac{P_R h_{2i}}{P_P x + N_0} > t\right\}\right] \\ &= \prod_{i=1}^N \left[1 - \left(1 - \Pr\left\{\frac{P_S h_{1i}}{P_P \beta_i + N_0} \le t\right\}\right)\right. \\ &\quad \left. \times \left(1 - \Pr\left\{\frac{P_R h_{2i}}{P_P x + N_0} \le t\right\}\right)\right] \\ &= \prod_{i=1}^N [1 - Q_1 Q_2], \end{aligned} \tag{49}$$

where Q_1 and Q_2 are given, respectively, by

$$Q_1 = 1 - \Pr\left\{\frac{P_S h_{1i}}{P_P \beta_i + N_0} \le t\right\}, \tag{50}$$

$$Q_2 = 1 - \Pr\left\{\frac{P_R h_{2i}}{P_P x + N_0} \le t\right\}. \tag{51}$$

Next, Q_1 is calculated as

$$Q_1 = 1 - \int_0^\infty \Pr\left\{\frac{P_S h_{1i}}{P_P u + N_0} \le t\right\} f_{\beta_i}(u)du, \tag{52}$$

where $f_{\beta_i}(u) = \frac{1}{\Omega_\beta} \exp\left(-\frac{u}{\Omega_\beta}\right)$, and Q_1 can be derived as

$$\begin{aligned} &Q_1 \\ &= 1 - \int_0^\infty \Pr\left\{\frac{P_S h_{1i}}{P_P u + N_0} \le t\right\} \frac{1}{\Omega_\beta} \exp\left(-\frac{u}{\Omega_\beta}\right) du \\ &= \frac{1}{\Omega_\beta} \exp\left(-\frac{N_0 t}{P_S \Omega_{h_1}}\right) \int_0^\infty \exp\left[-\left(\frac{P_P t}{P_S \Omega_{h_1}} + \frac{1}{\Omega_\beta}\right) u\right] du \\ &= \frac{P_S \Omega_{h_1}}{P_P \Omega_\beta t + P_S \Omega_{h_1}} \exp\left(-\frac{N_0 t}{P_S \Omega_{h_1}}\right). \end{aligned} \tag{53}$$

Similarly, we obtain Q_2 as

$$\begin{aligned} Q_2 &= 1 - \Pr\left\{h_{2i} \le \frac{(P_P x + N_0)t}{P_R}\right\} \\ &= \exp\left(-\frac{(P_P x + N_0)t}{P_R \Omega_{h_2}}\right). \end{aligned} \tag{54}$$

Substituting (53) and (54) into (49), yields P_2 as follows

$$\begin{aligned} P_2 &= \prod_{n=1}^N \left[1 - \frac{P_S \Omega_{h_1}}{P_P \Omega_\beta t + P_S \Omega_{h_1}} \exp\left(-\frac{N_0 t}{P_S \Omega_{h_1}}\right)\right. \\ &\quad \left. \times \exp\left(-\frac{(P_P x + N_0)t}{P_R \Omega_{h_2}}\right)\right] \\ &= \prod_{n=1}^N \left\{1 - \frac{1}{\frac{P_P \Omega_\beta}{P_S \Omega_{h_1}} t + 1} \exp\left(-\frac{P_P x t n}{P_R \Omega_{h_2}}\right)\right. \\ &\quad \left. \times \exp\left[-\left(\frac{1}{P_S \Omega_{h_1}} + \frac{1}{P_R \Omega_{h_2}}\right) N_0 t\right]\right\}. \end{aligned} \tag{55}$$

Setting $B_0 = \frac{P_P\Omega_\beta}{P_S\Omega_{h_1}}$, substituting B_0 into (55), and using the binomial theorem, we have

$$P_2 = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n}{(B_0t+1)^n}\exp\left(-\frac{P_Pxtn}{P_R\Omega_{h_2}}\right) \times \exp\left[-\left(\frac{1}{P_S\Omega_{h_1}}+\frac{1}{P_R\Omega_{h_2}}\right)N_0tn\right]. \quad (56)$$

Accordingly, substituting (48) and (56) into (45), $F_{\gamma_{E2E}}(t)$ can be rewriten as follows

$$F_{\gamma_{E2E}}(t) = \underbrace{\int_0^\infty P_2 f_{\beta_0}(x)dx}_{F_1} - \underbrace{\int_0^\infty Q_3 f_{\beta_0}(x)dx}_{F_2} \quad (57)$$

where Q_3 is obtained as

$$Q_3 = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n\exp\left[-\left(\frac{1}{P_S\Omega_{h_0}}+\frac{1}{P_R\Omega_{h_2}}\right)P_Ptx\right]}{(B_0t+1)^n} \exp\left[-\left(\frac{1}{P_S\Omega_{h_0}}+\frac{n}{P_S\Omega_{h_1}}+\frac{n}{P_R\Omega_{h_2}}\right)N_0t\right]. \quad (58)$$

To derive $F_{\gamma_{E2E}}(t)$ in (45), we need to compute the expression F_1 and F_2 in (57). For F_1, substituting (56) into F_1 we have

$$F_1 = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n}{(B_0t+1)^n} \times \exp\left[-\left(\frac{1}{P_S\Omega_{h_1}}+\frac{1}{P_R\Omega_{h_2}}\right)N_0tn\right] \times \underbrace{\int_0^\infty \exp\left(-\frac{P_Pxtn}{P_R\Omega_{h_2}}\right)\frac{1}{\Omega_{\beta_0}}\exp\left(-\frac{x}{\Omega_{\beta_0}}\right)dx}_{F_{11}}. \quad (59)$$

The result of the integral expression F_{11} is obtained as

$$F_{11} = \frac{1}{\Omega_{\beta_0}}\frac{1}{\frac{P_Ptn}{P_R\Omega_{h_2}}+\frac{1}{\Omega_{\beta_0}}} = \frac{1}{B_nt+1}, \quad (60)$$

where $B_n = \frac{P_P\Omega_{\beta_0}n}{P_R\Omega_{h_2}}$. Substituting (60) into (59), F_1 is expressed as

$$F_1 = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n}{(B_0t+1)^n(B_nt+1)}\exp\left(-\frac{t}{C_n}\right), \quad (61)$$

where $\frac{1}{C_n} = \left(\frac{1}{P_P\Omega_{h_1}}+\frac{1}{P_R\Omega_{h_2}}\right)N_0n$. Similar, substituting (58) into the integral expression F_2 in (57), we have

$$F_2 = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n}{(B_0t+1)^n}\exp\left(-\frac{1}{D_n}\right) \times \int_0^\infty \exp\left(-\left(\frac{1}{P_S\Omega_{h_0}}+\frac{n}{P_R\Omega_{h_2}}\right)P_Ptx\right) \times\frac{1}{\Omega_{\beta_0}}\exp\left(-\frac{x}{\Omega_{\beta_0}}\right)dx,$$

$$= \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n}{(B_0t+1)^n}\exp\left(-\frac{1}{D_n}\right)F_{21}, \quad (62)$$

where $\frac{1}{D_n} = \left(\frac{1}{P_S\Omega_{h_0}}+\frac{n}{P_S\Omega_{h_1}}+\frac{n}{P_R\Omega_{h_2}}\right)N_0$ and F_{21} is integral expression and can be calculated as

$$F_{21} = \frac{1}{\Omega_\beta}\int_0^\infty \exp\left\{-\left[\left(\frac{1}{P_S\Omega_{h_0}}+\frac{n}{P_R\Omega_{h_2}}\right)P_Pt+\frac{1}{\Omega_{\beta_0}}\right]x\right\}dx, = \frac{1}{\Omega_{\beta_0}}\frac{1}{\left(\frac{1}{P_S\Omega_{h_0}}+\frac{n}{P_R\Omega_{h_2}}\right)P_Pt+\frac{1}{\Omega_{\beta_0}}} = \frac{1}{E_nt+1}, \quad (63)$$

where $E_n = \left(\frac{1}{P_S\Omega_{h_0}}+\frac{n}{P_R\Omega_{h_2}}\right)P_P\Omega_{\beta_0}$, Substituting (63) into (62), F_2 can be obtained as

$$F_2 = \sum_{n=0}^{N}\binom{N}{n}\frac{(-1)^n}{(B_0t+1)^n(E_nt+1)}.\exp\left(-\frac{t}{D_n}\right). \quad (64)$$

Accordingly, $F_{\gamma_{E2E}}(t)$ can be obtained as

$$F_{\gamma_{E2E}}(t) = F_1 - F_2, \quad (65)$$

where F_1 and F_2 are given by in (61) and (64), respectively. Now, we can compute the CDF of γ_E as

$$\begin{aligned} F_{\gamma_E}(y) &= \Pr\left\{\max\left\{\frac{P_Sf_0}{P_Pg_0},\frac{P_Rf_{i^*}}{P_Pg_0}\right\}\le y\right\} \\ &= \int_0^\infty \Pr\left\{\max\left\{\frac{P_Sf_0}{P_Pu},\frac{P_Rf_{i^*}}{P_Pu}\right\}\le y\right\}f_{g_0}(u)du \\ &= \int_0^\infty\left[\Pr\left\{f_0\le\frac{yP_Pu}{P_S}\right\}\Pr\left\{f_{i^*}\le\frac{yP_Pu}{P_R}\right\}\right]f_{g_0}(u)du \\ &= \int_0^\infty\left[1-\exp\left(-\frac{yP_Pu}{P_S\Omega_{f_0}}\right)\right]\left[1-\exp\left(-\frac{yP_Pu}{P_R\Omega_f}\right)\right]f_{g_0}(u)du \\ &= 1-T_1-T_2+T_3, \end{aligned} \quad (66)$$

where T_1, T_2 and T_3 are integrals and are calculated as follows

$$\begin{aligned} T_1 &= \int_0^\infty \exp\left(-\frac{yP_Pu}{P_R\Omega_f}\right)f_{g_0}(u)du, \\ &= \frac{1}{\Omega_{g_0}}\int_0^\infty \exp\left(-\frac{yP_Pu}{P_R\Omega_f}\right)\exp\left(-\frac{u}{\Omega_{g_0}}\right)du, \\ &= \frac{1}{A_2y+1}, \quad \text{with } A_2 = \frac{P_P\Omega_{g_0}}{P_R\Omega_f}; \\ T_2 &= \int_0^\infty \exp\left(-\frac{yP_Pu}{P_S\Omega_{f_0}}\right)f_{g_0}(u)du, \\ &= \frac{1}{\Omega_{g_0}}\int_0^\infty \exp\left(-\frac{yP_Pu}{P_S\Omega_{f_0}}\right)\exp\left(-\frac{u}{\Omega_{g_0}}\right)du, \end{aligned} \quad (67)$$

$$= \frac{1}{A_3 y + 1}, \quad \text{with } A_3 = \frac{P_P \Omega_{g_0}}{P_S \Omega_{f_0}}; \tag{68}$$

$$T_3 = \int_0^\infty \exp\left[-\left(\frac{1}{P_R \Omega_f} + \frac{1}{P_S \Omega_{f_0}}\right) P_P u y\right] f_{g_0}(u) du,$$

$$= \frac{1}{\Omega_{g_0}} \int_0^\infty \exp\left\{-\left[\left(\frac{1}{P_R \Omega_f} + \frac{1}{P_S \Omega_{f_0}}\right) P_P y + \frac{u}{\Omega_{g_0}}\right] u\right\} du,$$

$$= \frac{1}{(A_2 + A_3) y + 1}. \tag{69}$$

From (67), (68) and (69), the CDF of γ_E in (66) is rewritten as

$$F_{\gamma_E}(y) = 1 - \frac{1}{A_2 y + 1} - \frac{1}{A_3 y + 1} + \frac{1}{(A_2 + A_3) y + 1}. \tag{70}$$

From (70), the PDF of γ_E can be derived as

$$f_{\gamma_E}(y) = \frac{dF_{\gamma_E}(y)}{dy},$$

$$= \frac{A_2}{(A_2 y + 1)^2} + \frac{A_3}{(A_3 y + 1)^2} - \frac{A_2 + A_3}{[(A_2 + A_3) y + 1]^2}. \tag{71}$$

Consider $\mathcal{O}_{SEC}$ in (44), we can see that

$$\Pr\{\gamma_{E2E} \le \delta + (\delta + 1)x\} = F_{\gamma_{E2E}}(\delta + (\delta + 1)x), \tag{72}$$

where $F_{\gamma_{E2E}}(\cdot)$ is given in (65). Setting $t = \delta + (\delta + 1)x$, and substituting (71) and (72) into (44), we can formulate the secrecy outage probability as follows

$$\mathcal{O}_{SEC} = \int_\delta^\infty \frac{F_{\gamma_{E2E}}(t)}{\delta + 1} f_{\gamma_E}\left(\frac{t - \delta}{\delta + 1}\right) dt$$

$$= \underbrace{\int_\delta^\infty \frac{F_1}{\delta + 1} f_{\gamma_E}\left(\frac{t - \delta}{\delta + 1}\right) dt}_{O_1} - \underbrace{\int_\delta^\infty \frac{F_2}{\delta + 1} f_{\gamma_E}\left(\frac{t - \delta}{\delta + 1}\right) dt}_{O_2}, \tag{73}$$

wherein $f_{\gamma_E}(.)$ is rewritten as

$$f_{\gamma_E}\left(\frac{t - \delta}{\delta + 1}\right) = \frac{A_2}{\left(A_2 \frac{t - \delta}{\delta + 1} + 1\right)^2} + \frac{A_3}{\left(A_3 \frac{t - \delta}{\delta + 1} + 1\right)^2} - \frac{A_2 + A_3}{\left[(A_2 + A_3) \frac{t - \delta}{\delta + 1} + 1\right]^2},$$

$$= \frac{(\delta + 1)^2}{A_2 (t + C_1)^2} + \frac{(\delta + 1)^2}{A_3 (t + C_2)^2} - \frac{(\delta + 1)^2}{(A_2 + A_3)(t + C_3)^2}, \tag{74}$$

where $C_1 = \frac{1 + \delta - A_2 \delta}{A_2}$, $C_2 = \frac{1 + \delta - A_3 \delta}{A_3}$ and $C_3 = \frac{1 + \delta - (A_2 + A_3)\delta}{A_2 + A_3}$.

From (73), the O_1 can be computed as

$$O_1 = \frac{1}{\delta + 1} \sum_{n=0}^{N} \binom{N}{n} \int_\delta^\infty \frac{(-1)^n}{(B_0 t + 1)^n (B_n t + 1)} \times \exp\left(-\frac{1}{C_n}\right) f_{\gamma_E}\left(\frac{t - \delta}{\delta + 1}\right) dt,$$

$$= I_1(n) + I_2(n) - I_3(n), \tag{75}$$

where $I_1(n)$, $I_2(n)$ and $I_3(n)$ are the following integral expressions, respectively

$$I_1(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_2} \times \int_\delta^\infty \frac{\exp\left(-\frac{1}{C_n}\right)}{(B_0 t + 1)^n (B_n t + 1)(t + C_1)^2} dt; \tag{76}$$

$$I_2(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_3} \times \int_\delta^\infty \frac{\exp\left(-\frac{1}{C_n}\right)}{(B_0 t + 1)^n (B_n t + 1)(t + C_2)^2} dt; \tag{77}$$

$$I_3(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_2 + A_3} \times \int_\delta^\infty \frac{\exp\left(-\frac{1}{C_n}\right)}{(B_0 t + 1)^n (B_n t + 1)(t + C_3)^2} dt. \tag{78}$$

Similarly, O_2 can be expressed as

$$O_2 = \frac{1}{\delta + 1} \sum_{n=0}^{N} \binom{N}{n} \int_\delta^\infty \frac{(-1)^n}{(B_0 t + 1)^n (E_n t + 1)} \times \exp\left(-\frac{1}{D_n}\right) f_{\gamma_E}\left(\frac{t - \delta}{\delta + 1}\right) dt,$$

$$= J_1(n) + J_2(n) - J_3(n), \tag{79}$$

where the integrals $J_1(n)$, $J_2(n)$ and $J_3(n)$ are given, respectively, as follows:

$$J_1(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_2} \times \int_\delta^\infty \frac{\exp\left(-\frac{1}{D_n}\right)}{(B_0 t + 1)^n (E_n t + 1)(t + C_1)^2} dt; \tag{80}$$

$$J_2(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_3} \times \int_\delta^\infty \frac{\exp\left(-\frac{1}{D_n}\right)}{(B_0 t + 1)^n (E_n t + 1)(t + C_2)^2} dt; \tag{81}$$

$$J_3(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta + 1)}{A_2 + A_3}$$

$$\times \int_{\delta}^{\infty} \frac{\exp\left(-\frac{1}{D_n}\right)}{(B_0 t+1)^n (E_n t+1)(t+C_3)^2} dt. \quad (82)$$

In here, to calculate the integrals in O_1 and O_2, we use the help of a lemma which has been proved in the our previous study [12, Lemma 1]. The lemma is presented as follows:

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

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

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

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

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

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

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

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 the cosecant, the incomplete beta function, and the hypergeometric function, respectively. *Proof:* The proof is detailed in the Appendix of [12]. □

Finally, the secrecy outage probability of CCRN is rewritten as

$$\mathcal{O}_{SEC} \approx [I_1(n) + I_2(n) - I_3(n)] - [J_1(n) + J_2(n) - J_3(n)], \quad (83)$$

wherein

$$I_1(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(B_n, B_0, C_1, C_n)}{A_2},$$

$$I_2(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(B_n, B_0, C_2, C_n)}{A_3},$$

$$I_3(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(B_n, B_0, C_3, C_n)}{A_2 + A_3},$$

$$J_1(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(E_n, B_0, C_1, D_n)}{A_2},$$

$$J_2(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(E_n, B_0, C_2, D_n)}{A_3},$$

$$J_3(n) = \sum_{n=0}^{N} \binom{N}{n} \frac{(-1)^n (\delta+1) K(E_n, B_0, C_3, D_n)}{A_2 + A_3},$$

2) PROBABILITY OF NON-ZERO SECRECY CAPACITY

Recalling that a non-zero secrecy capacity exists when the capacity of the legitimate channel is larger than the one of the wiretap channel. From (16), the probability of existence of non-zero secrecy capacity of the system can be evaluated by setting $\delta = 0$ in (40) as follows

$$\begin{aligned} \mathcal{O}_{nonZero} &= \Pr\{C_S > 0\}, \\ &= 1 - \Pr\{C_S < 0\}, \\ &\approx 1 - \mathcal{O}_{SEC}, \quad \text{with } \delta = 0. \end{aligned} \quad (84)$$

VI. NUMERICAL RESULTS

In this section, illustrative examples are presented to highlight the impact of the power allocation policies on the secrecy outage probability for the considered. In the numerical evaluation, system parameters are initially given as follows, unless otherwise stated.

- System bandwidth: $B = 5$ MHz;
- PU target rate: $R_p = 64$ Kbps;
- Secrecy target rate of SU: $R = 64$ Kbps;
- Outage probability constraints of the PU: $\xi_P = 0.01$;
- Transmit SNR of the P-Tx: $\gamma^p = \frac{P^p}{N_0} = 10$ (dB);
- Peak transmit SNR of the S-Tx: $\gamma^s_{pk} = \frac{P^s_{pk}}{N_0} = 20$ (dB);
- Peak transmit SNR of the *SR*: $\gamma^r_{pk} = \frac{P^r_{pk}}{N_0} = 20$ (dB);
- Number of relays: $N = 5$;
- Channel mean gains: $\Omega_{g_1} = 15$, $\Omega_{h_1} = \Omega_{h_2} = 10$, $\Omega_{h_0} = 5$, $\Omega_{g_0} = 5$, $\Omega_\alpha = \Omega_{\alpha_0} = \Omega_\beta = \Omega_{\beta_0} = 1$, $\Omega_f = \Omega_{f_0} = 1$;

In our numerical results, the approximate curves match very well with the analytical curves and simulation results in all cases. Thus, we only plot all three curves (i.e. analytical, simulation, and approximate curves) once in Figure 2. The other figures only contains the simulation and approximate curves.

We can observe from Figure 2 that the secrecy outage probability in all cases is reduced when the peak interference level I_{th} of the PU increases. This is because the SU can transmit with high power level to improve QoS as PU tolerates more interference. However, the secrecy outage probability with $\epsilon = 0.1$ is saturated as $\frac{I_{th}}{N_0} > -4$, while the one with ϵ is given by formula (39) continues to be significantly reduced and then saturate. This can be explained when ϵ is fixed, the peak interference level of the PU can be increased further but the SU could still not increase its transmit power further because it is limited by the secrecy outage constraint. In contrast, when ϵ is optimized by the formula in (39), the values of ϵ can be changed according to the instantaneous parameters of the system. Therefore, the secrecy outage probability, in this case, is better. However, the SU is subject to constraints on peak transmit power, and thus increasing the interference tolerate level does not change the secrecy performance.

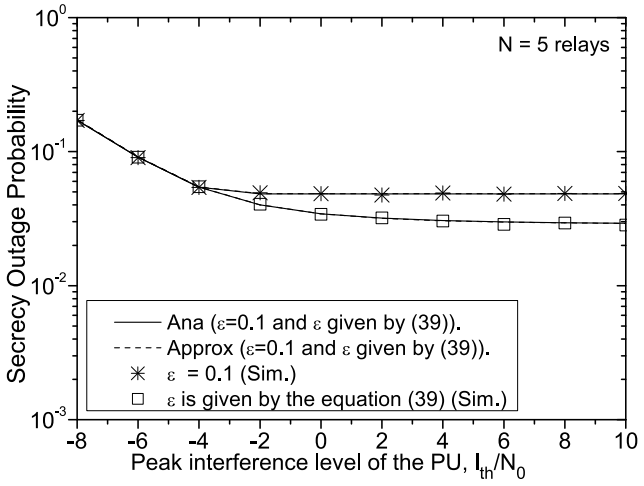


FIGURE 2. Impact of ϵ on the secure outage probability according to the value range of $\frac{I_{th}}{N_0}$.

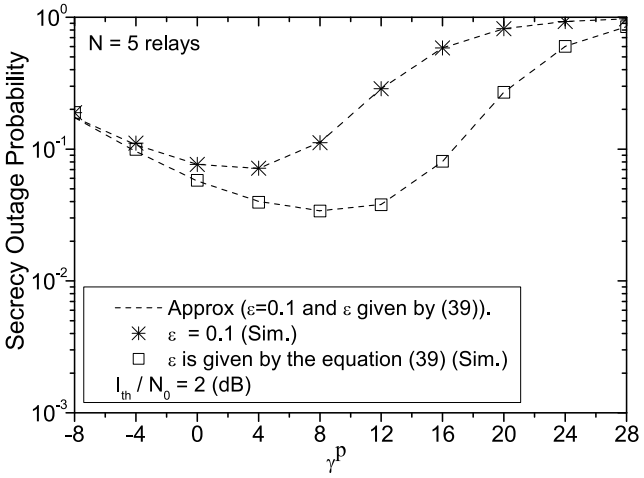


FIGURE 3. Impact of ϵ on the secure outage probability according to the value range of γ_P.

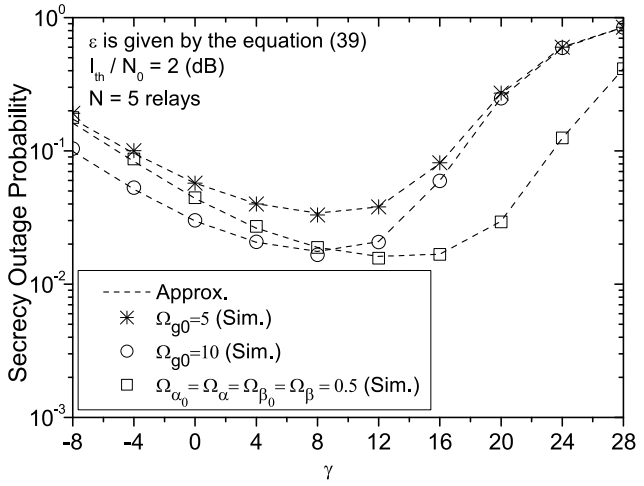


FIGURE 4. Impact of the interference links on the secrecy outage probability.

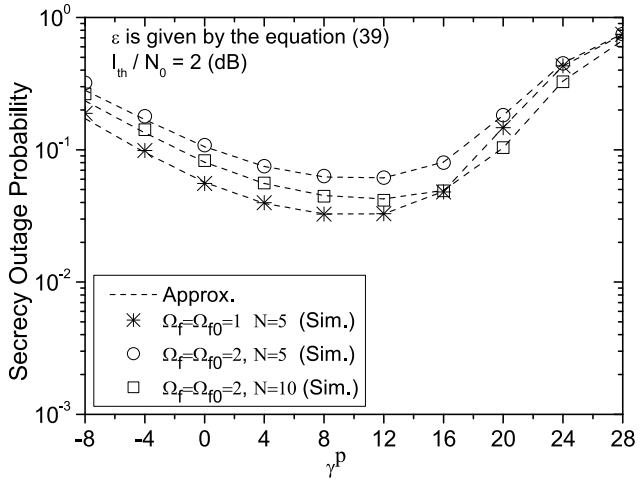


FIGURE 5. Impact of the channel mean gain of the wiretap links and number of SRs on the secrecy outage probability.

Figure 3 shows the secrecy outage probability by γ_p. It is interesting to see that the secrecy outage probability with ϵ calculated using equation (39) is always smaller than or equal to the one with fixed ϵ. In addition, we see that the secrecy outage probability decreases to an optimal value and then it increases as the transmit SNR of PU increases further. It is because the SU can regulate their transmit powers following proposed power polices as the transmit SNR of the PU is small enough. However, if the transmit SNR of the PU is large the SU can not adjust its transmit power according to the corresponding change of the PU due to its peak transmit power constraint. As a result, the transmit SNR of the PU becomes a very strong limitation to SU which degrades the secrecy performance for the considered system. Clearly, the secrecy performance in the optimized ϵ case is better than the one in the fixed ϵ case.

In Figure 4, we show the impact of the interference links on the secrecy outage probability. We see that when Ω_{g0} increases from 5 to 10, the secrecy performance of the system is significantly improved in the low SNR regime of the PU. The reason is that increasing the channel mean gain of the P-Tx→EAV link makes the interference from the PU to the EAV increase, and the transmit power of the PU becomes a strong interference source for the EAV, i.e, the channel capacity of EAV will be reduced. In addition, it can be observed that the secrecy outage probability is degraded as the channel mean gains of interference links between the SU and the PU decrease, e.g, Ω_{α_0}, Ω_{α}, Ω_{β}, Ω_{β_0} from 1 to 0.5. This means that the SU and the PU cause less interference to each other as the channel mean gains between them are low. Thus, the secondary network can increase its transmit power and still not cause harmful interference to the PU. Accordingly, the capacity of the secondary network is enhanced. Also, as the transmit SNR of the PU increases to a high value (beyond 12 dB), the secrecy outage probability increases very fast, because the PU can generate very strong interference to the SU. From Figure 4, we can determine how to make use of the interference of PUs in the network to prevent eavesdropping.

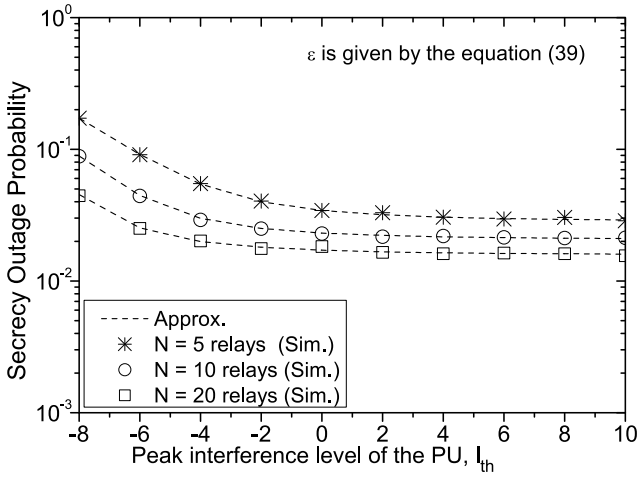


FIGURE 6. Impact of the different number of SR the secrecy outage probability according to the value range of $\frac{I_{th}}{N_0}$.

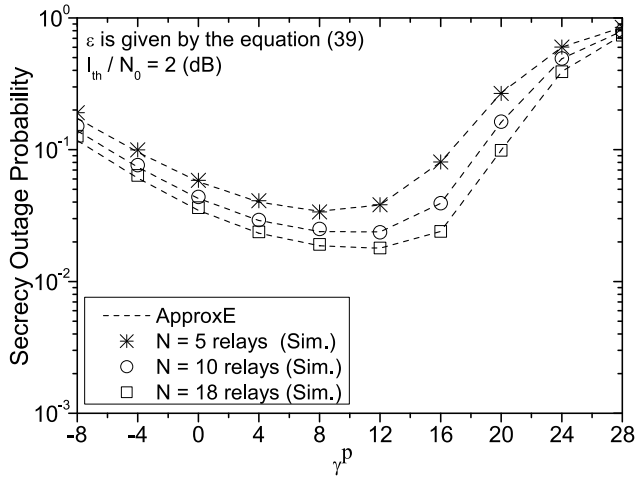


FIGURE 7. Impact of the different number of SR the secrecy outage probability according to the value range of γ_p.

On the other hand, Figure 5 shows the impact of channel mean gain of the S-Tx→EAV and SR→EAV wiretap links on the secrecy performance of the CCRN (e.g, $\Omega_{f_0} = \Omega_f = 1$ and $\Omega_{f_0} = \Omega_f = 2$). Clearly, the higher the channel mean gains of the wiretap links are, the higher value of the secrecy outage probability is. That means the secrecy performance of the CCRN is degraded. This is due to the fact the EAV can decode the messages of the secondary network more easier as the channel mean gains of the wiretap links are high. However, when the number of SR, N, increases from $N = 5$ to $N = 10$, the secrecy outage probability decreases significantly, i.e., the secrecy performance of the secondary network is improved. Similarly, in Figure 6 and Figure 7, the secrecy outage probability has been plotted using different number of SRs. It is clear that the secrecy performance of the system is improved significantly as the number of SRs increases, i.e., $N = 5; 10; 18; 20$. This means that as the number of SRs increases, there are more relays support the S-Tx forward information, and thus the ability to select the best relay is more diverse and efficient. As result, the secrecy performance of the system is improved.

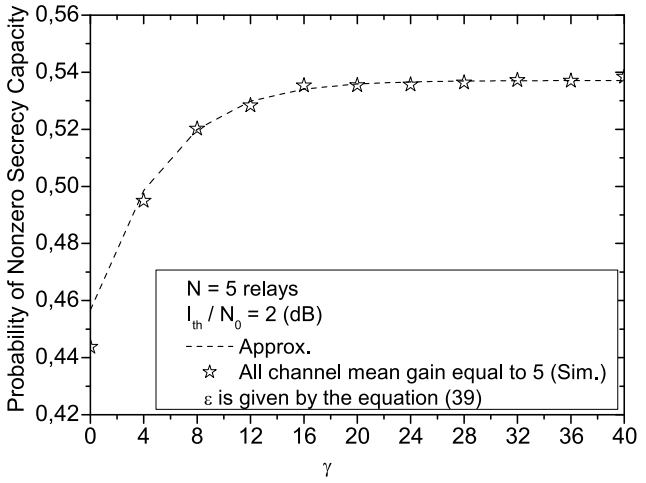


FIGURE 8. Probability of the non-zero secrecy capacity of CCRN with identical channel mean gain equals to 5.

In Figure 8, we plot the probability of the nonzero secrecy capacity with identical channel mean gains equals to 5. It can be seen that the probability of non-zero secrecy capacity is improve significantly as the transmit SNR of PU increases. This is because the transmit SNR of the PU will become an active jamming source to degrade the decoding capability of the eavesdropper. In other words, the interference of the PU is in this case a useful noise source to enhance the security of the secondary network.

VII. CONCLUSION

In this paper, we have studied cooperative relays for enhancing the secrecy performance of CCRN under interference and power level constraints from the primary network and secrecy constraints to prevent eavesdropping. Given the considered constraints, we derived the maximal secrecy capacity and optimized power allocation policies for the considered system model. Moreover, we have obtained approximate expressions for the secrecy outage probability and the probability of non-zero secrecy capacity over Rayleigh fading channels. Our analysis shows that the P-Tx→EAV, the S-Tx→EAV and the SR→EAV as well as the transmit SNR of the PU all have a strong impact on the security performance of the considered CCRN. Most importantly, our numerical results show that the secrecy performance of the system is clearly improved when the parameters obtained using the CSI of the wiretap channel are calculated optimally. Thence, the system can adjust the power allocation so that no eavesdropping occurs even without reducing QoS performance. In the future, we will investigate the impact of imperfect channel state information on the power allocation policy and secrecy performance.

REFERENCES

[1] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Proc. IEEE Int. Workshop Mobile Multimedia Commun.*, Jan. 2003, pp. 3–10.

[2] A. Ghasemi and E. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.
[3] R. Zhang, "On peak versus average interference power constraints for protecting primary users in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 2112–2120, Apr. 2009.
[4] M. El Tanab and W. Hamouda, "Resource allocation for underlay cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1249–1276, Nov. 2017.
[5] Y. Liu, H. Wu, Y. Xia, Y. Wang, F. Li, and P. Yang, "Optimal online data dissemination for resource constrained mobile opportunistic networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5301–5315, Jun. 2017.
[6] Y. Liu, W. Quan, T. Wang, and Y. Wang, "Delay-constrained utility maximization for video Ads push in mobile opportunistic D2D networks," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 4088–4099, Oct. 2018.
[7] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.
[8] B. Cao, J. W. Mark, Q. Zhang, R. Lu, X. Lin, and X. S. Shen, "On optimal communication strategies for cooperative cognitive radio networking," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 1726–1734.
[9] X. Chen, H. H. Chen, and W. Meng, "Cooperative communications for cognitive radio networks: From theory to applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1180–1192, 3rd Quart., 2014.
[10] M. E. Bayrakdar and S. Bayrakdar, "A cooperative communication approach for voluntary secondary users in cognitive radio networks," in *Proc. 23nd Signal Process. Commun. Appl. Conf. (SIU)*, May 2015, pp. 604–607.
[11] A. Bletsas, H. Shin, and M. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, Sep. 2007.
[12] T. X. Quach, H. Tran, E. Uhlemann, and M. T. Truc, "Secrecy performance of cognitive cooperative industrial radio networks," in *Proc. 22nd IEEE Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2017, pp. 1–8.
[13] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.
[14] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[15] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[16] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.
[17] Z. Shu, Y. Yang, Y. Qian, and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–6.
[18] M. Al-Jamali, A. Al-Nahari, and M. M. Alkhawlani, "Relay selection scheme for improving the physical layer security in cognitive radio networks," in *Proc. 23nd Signal Process. Commun. Appl. Conf. (SIU)*, May 2015, pp. 495–498.
[19] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.
[20] Y. Pei, Y.-C. Liang, L. Zhang, K. Teh, and K. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.
[21] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.
[22] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.
[23] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.
[24] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
[25] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10236–10242, Dec. 2016.
[26] H. Zhang, T. Wang, L. Song, and Z. Han, "Interference improves PHY security for cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 609–620, Mar. 2016.
[27] T. X. Quach, H. Tran, E. Uhlemann, G. Kaddoum, and Q. A. Tran, "Power allocation policy and performance analysis of secure and reliable communication in cognitive radio networks," *Wireless Netw.*, vol. 25, no. 4, pp. 1477–1489, May 2019, doi: 10.1007/s11276-017-1605-z.
[28] P. Yan, Y. Zou, and J. Zhu, "Secrecy diversity analysis with multi-user scheduling for overlay cognitive radio systems," in *Proc. IEEE Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Nov. 2016, pp. 482–486.
[29] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.
[30] L. Sibomana, H. Tran, and H.-J. Zepernick, "On physical layer security for cognitive radio networks with primary user interference," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2015, pp. 281–286.
[31] H. Tran, G. Kaddoum, F. Gagnon, and L. Sibomana, "Cognitive radio network with secrecy and interference constraints," *Phys. Commun.*, vol. 22, pp. 32–41, Mar. 2017.
[32] Y. Liu, L. Hao, Z. Liu, K. Sharif, Y. Wang, and S. K. Das, "Mitigating interference via power control for two-tier femtocell networks: A hierarchical game approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7194–7198, Jul. 2019.
[33] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.
[34] Q. Gu, G. Wang, R. Fan, and Z. Zhong, "Secure performance analysis of cognitive two-way relay system with an eavesdropper," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Oct. 2014, pp. 176–180.
[35] H. Sakran, O. Nasr, S. El-Rabaie, A. El-Azm, and M. Shokair, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.
[36] J. Yang, L. Chen, J. Ding, X. Hu, and P. T. Mathiopoulos, "Intercept outage probability analysis of cognitive relay networks in presence of eavesdropping attack," in *Proc. 21st Asia–Pacific Conf. Commun. (APCC)*, Oct. 2015, pp. 304–308.
[37] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Cooperative relaying and jamming for primary secure communication in cognitive two-way networks," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.
[38] X. Xu, W. Yang, and Y. Cai, "Opportunistic relay selection improves reliability–reliability tradeoff and security–reliability tradeoff in random cognitive radio networks," *IET Commun.*, vol. 11, no. 3, pp. 335–343, Feb. 2017.
[39] L. Sibomana, H.-J. Zepernick, and H. Tran, "On physical layer security for reactive DF cognitive relay networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 1290–1295.
[40] T. Q. Duong, T. T. Duy, M. Elkashlan, N. H. Tran, and O. A. Dobre, "Secured cooperative cognitive radio networks with relay selection," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 3074–3079.
[41] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[42] N. T. Do and B. An, "Secure transmission using decode-and-forward protocol for underlay cognitive radio networks," in *Proc. IEEE Int. Conf. Ubiquitous Future Netw.*, Jul. 2015, pp. 914–918.
[43] W. Yang, X. Xu, Y. Cai, and B. Zheng, "Secrecy outage analysis for cooperative DF underlay CRNs with outdated CSI," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 416–421.
[44] H. Ding, J. Ge, D. B. Da Costa, and Z. Jiang, "Asymptotic analysis of cooperative diversity systems with relay selection in a spectrum-sharing scenario," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 457–472, Feb. 2011.
[45] P. Chakraborty and S. Prakriya, "Secrecy outage performance of a cooperative cognitive relay network," *IEEE Commun. Lett.*, vol. 21, no. 2, pp. 326–329, Feb. 2017.
[46] J. Ding, Q. Yang, and J. Yang, "Secrecy performance analysis in multi-relay DF cognitive relay networks under interference constraints," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Dec. 2016, pp. 1–6.
[47] X. Zhou, M. R. Mckay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[48] T. T. Duy, T. L. Thanh, V. N. Q. Bao, and T. Q. Duong, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Commun.*, vol. 9, no. 11, pp. 1427–1435, Jul. 2015.
[49] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

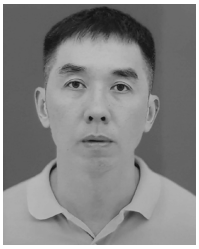
TRUONG XUAN QUACH received the bachelor's degree in information technology from Vietnam National University–VNU University of Engineering and Technology (VNU-UET), Vietnam, in 2002, and the master's degree in computer science from Thai Nguyen University (TNU), Viet Nam, in 2007. He is currently pursuing the Ph.D. degree with VNU-UET.

He is also a Lecturer and the Vice Dean of the Faculty of Information Technology, TNU–University of Information and Communication Technology (ICTU), Vietnam. His general research interests include wireless communication, communications theory, physical-layer security, wireless power transfer, and machine learning.

HUNG TRAN received the B.S. and M.S. degrees in information technology from Vietnam National University, Vietnam, in 2002 and 2006, respectively, and the Ph.D. degree from the Blekinge Institute of Technology, Sweden, in March 2013.

In 2014, he was with the Electrical Engineering Department, ETS, Montreal, QC, Canada. Since October 2015, he has been a Postdoctoral Researcher with Mälardalen University, Sweden. His research interests are in the areas of cognitive radio networks, cooperative communication, physical layer security for wireless communication, and wireless power transfer.

ELISABETH UHLEMANN received the Ph.D. degree in communications theory from the Chalmers University of Technology, Sweden, in 2004. She worked as an Assistant and later an Associate Professor with Halmstad University, from 2005 to 2012. During this period, she also worked with Volvo Technology, where she was involved in several EU FP6 projects: CVIS, Safespot, and Predrive C2X, studying communication requirements for traffic safety applications in vehicular networks. She has contributed to the European ITS communications architecture produced within COMeSafety. She has served as a Technical Expert with ETSI TC ITS. She has held visiting positions at the University of South Australia, in 2005, TU Berlin, in 2007, and the University of Canterbury, New Zealand, in 2011. She has also worked as a Consultant with Ikanos Communications, USA, in 2005, with VDSL protocols and at Free2move, Sweden, from 2009 to 2010, with wireless audio. She has served in the grading committee for more than 15 Ph.D. degrees in Sweden, Spain, Germany, and Australia, and organized two postgraduate courses Block Turbo Codes and Iterative Decoding at Halmstad University, in 2006, and Communications for Cyber-Physical Systemsat MDH, in 2014. She is currently a Research Grant Reviewer of Vinnova, Sweden's Innovation Agency, in the area of vehicular electronics, software, and communications. She has served as a Senior Editor for the *IEEE VT Magazine* in the area of connected vehicles. She is also the Co-Chair of the Subcommittee on Industrial Communication Systems within the IEEE IES Technical Committee on Factory Automation and the Vice Chair of the Swedish IEEE VT/COM/IT Chapter. She has two best paper awards: APCC 2005 and ETFA 2010, is a part of the steering group of a large research profile at Karlstad University, and in the Faculty board at Mälardalen University.



MAI TRAN TRUC received the B.S. degree from the Hanoi University of Technology, and the M.S. and Ph.D. degrees in wireless communication from Bristol University, U.K., in 2003 and 2010, respectively.

His research interests include 4G, 5G wireless technology, power line communication, and MIMO communication.