SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2015; **8:**4177–4190
Published online 27 August 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1333

RESEARCH ARTICLE

Impact of secondary user communication on security communication of primary user

Louis Sibomana[1,2]*, Hung Tran[3,4] and Quang Anh Tran[5]

[1] Department of Communication Systems (DIKO), Blekinge Institute of Technology, Karlskrona, Sweden
[2] College of Science and Technology, University of Rwanda, Kigali, Rwanda
[3] ETS, University of Québec, Montreal, Canada
[4] Computer Network Department, Faculty of Information Technology, NIEM, Vietnam
[5] Faculty of Information Technology, Hanoi University, Vietnam

ABSTRACT

Cognitive radio network concept has been considered as a promising solution to improve the spectrum utilization. However, it may be vulnerable to security problems as the primary user (PU) and secondary user (SU) access the same resource. In this paper, we consider a system model where an eavesdropper (EAV) illegally listens to the PU communication in the presence of a SU transmitter (SU-Tx) communicating with a SU receiver (SU-Rx). The SU-Tx transmit power is subject to the peak transmit power constraint of the SU and outage probability constraint of the PU. Given this context, the effect of the interference from the SU-Tx to the EAV on the primary system security is investigated. In particular, analytical expressions of the probability of existence of non-zero secrecy capacity and secrecy outage probability of the PU are derived. Moreover, the performance analysis of the secondary network is examined where closed-form expressions of the symbol error probability and achievable rate are presented. Numerical examples are provided to evaluate the impact of the primary system parameters and channel conditions among users on the system performance of secondary and primary networks. Interestingly, our results reveal a fact that the security of the primary network strongly depends on the channel condition of the SU-Tx to the EAV link and the transmit power policy of the SU-Tx. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS
cognitive radio network; symbol error probability; secrecy capacity; secrecy outage probability; achievable rate

***Correspondence**
Louis Sibomana, Department of Communication Systems (DIKO), Blekinge Institute of Technology, SE-371 79 Karlskrona, Sweden.
E-mail: lsm@bth.se, lsibomana@ur.ac.rw

1. INTRODUCTION

During the last decades, cognitive radio network (CRN) has been considered as a feasible solution in improving the spectrum utilization [1–3]. In cognitive radio systems, a secondary user (SU) transmits using the spectrum allocated to the licensed user or primary user (PU). The SU must be aware of its radio environment and dynamically adapts its transmission to the radio operation characteristics in such a way that the PU transmission quality is not violated. Various cognitive radio spectrum access strategies have been proposed in the CRN literature [2–5]. There are two main spectrum access models, namely, opportunistic spectrum access (OSA) and spectrum sharing (SS). For the OSA approach or non-interfering spectrum access model, the SU is allowed to transmit only when the PU is not active. Thus, the OSA model requires robust spectrum sensing techniques to detect the PU's activities. In practice, it is hard to guarantee ideal spectrum sensing, and in case of missed-detection, the SU can cause severe interference to the PU receiver (PU-Rx). In a SS model or interference-tolerant spectrum access, which is also known as an underlay approach, the SU is allowed to transmit simultaneously with the PU as long as the inflicted interference at the PU-Rx is kept below a predefined threshold. Therefore, the SU transmitter (SU-Tx) must control its transmit power to achieve its required transmission quality and to minimize interference to the PU-Rx. In this context, an acceptable level of performance for both primary and secondary networks can be guaranteed, which in turn results in a more efficient overall spectrum utilization. This work focuses on underlay approach, and the SU-Tx transmit power is subject to the PU outage constraint and the SU maximum transmit power limit.

On the other hand, security of wireless information transfer is becoming a critical issue due to the broadcast nature of wireless signals, and is considered as a new quality of service (QoS) constraint in wireless networks design [6,7]. Traditionally, secure communication is commonly achieved by using cryptographic techniques such as encryption, which mainly depend on secret keys above the physical layer. The data encryption protocols assume high computational complexity that prevent the eavesdropper (EAV) to decode the message and consider that an error-free physical layer link has been established. It is noted that the encrypted message (ciphertext) transmission is not perfectly secure, because the ciphertext can still be decrypted by an EAV with exhaustive key search. In contrast to cryptographic techniques, physical layer methods take into account wireless channel characteristics, and hence can be helpful for reliable secure communication without relying on upper layer data encryption. This is the basic principle of information theoretic security that utilizes physical layer techniques such as channel coding [8], artificial noise [9,10], or interference channel [11,12] to secure transmission of confidential information against the eavesdropping.

The problem of secure transmission has been studied in [8–15] from an information theoretic perspective for a wiretap channel. It is shown in [8] that a non-zero secrecy rate can be achieved if the EAV's channel is a degraded version of main channel. In [13–15], a secrecy capacity approach has been introduced to evaluate the security level of transmitted messages in the presence of an EAV. In this respect, the secrecy capacity is defined as the maximum transmission rate at which a message can be reliably received by the legitimate receiver but kept perfectly secret from the EAV. The use of artificial noise to confuse the EAV has been applied in [9,10] where the transmitter was assumed to have multiple antennas or there are cooperative nodes (helpers) who can generate noisy versions of the signal sent by the transmitter. It is important to note that the artificial noise generation and beamforming techniques to combat the eavesdropping attacks consume additional power resources for generating artificial noise and increase the high implementation complexity for beamforming design. Moreover, it is shown in [11,12] that the interferer can increase the secrecy level by generating interference to the EAV (e.g., to degrade the performance of the EAV's channel) and that a secrecy capacity can be achieved even if the main channel is worse than the EAV's channel. In contrast to the traditional wireless communication where interference is treated as harmful factor, such interference becomes a useful resource when secrecy capacity is considered. In addition, interference channel is more beneficial than friendly cooperative nodes or artificial noise because of their power consumption and implementation challenges.

Like any other wireless communication technology, CRN is also subject to security challenges. We refer to [16,17] for more details on several existing security attacks to the physical layer, challenges, and solutions in CRNs. This paper concentrates on one kind of security attacks, that is, a passive EAV who listens to the primary network communication and attempts to decode the transmitted message from wireless channels using eavesdropping intrusion. Following the concerns of security in an underlay CRN, the works in [17–19] investigated the primary network secure communication. In [17], the secrecy capacity and outage probability of secrecy capacity of the PU have been analyzed. Moreover, the authors in [18] considered an information secrecy cooperative game where the PU and SU cooperate and adjust their transmit powers to maximize the secrecy and information rates. In this context, the cooperation is adopted when the PU achieves higher secrecy rate with the help of the SU. Otherwise, the PU does not cooperate with the SU. However, [17,18] did not consider the interference power constraints of the SU. As a result, the QoS of primary network is not guaranteed because of the interference from the SU transmission. In addition, the results in [17] have been obtained from computer simulations, and hence, there is a need to provide an accurate analytic expression of the outage probability of secrecy capacity. In [19], we have investigated the probability of existence of non-zero secrecy capacity for the PU where the SU transmit power is subject to the PU outage constraint and the peak transmit power of the SU. Numerical examples in [19] illustrated that the channel condition between the SU-Tx and EAV has an important impact on the PU secure communication. However, only the probability of existence of non-zero secrecy capacity of the PU has been analyzed. Another security performance metric of interest for limited-delay applications is the outage probability of secrecy capacity of the PU and has not been investigated because of mathematical complexity. Further, in case where the channel state information (CSI) of the EAV is not known at the PU transmitter (PU-Tx), perfect secrecy capacity can not always be achieved, and thus, secrecy outage probability is an appropriate metric.

In this paper, we consider an underlay CRN where a PU-Tx sends important and private message to the PU-Rx, and there exists an EAV who is capable of eavesdropping the PU-Tx's signal by observing the channel output. The objective of this investigation is to study the impact of the SU communication on the primary system security. In particular, we assume that the SU-Tx transmit power is subject to the joint constraint of the PU outage constraint and SU-Tx maximum transmit power limit. Given this system setting, the cumulative distribution function (CDF) and probability density function (PDF) for the signal-to-interference-plus-noise ratio (SINR) are obtained. Accordingly, we derive the probability of existence of non-zero secrecy capacity and outage probability of the secrecy capacity of the PU. Moreover, the performance of secondary network, which is subject to the interference from the PU-Tx, is evaluated where closed-form expressions of the symbol error probability (SEP) and achievable rate are obtained. The numerical results indicate that the probability of existence of non-zero secrecy capacity and outage probability of secrecy capacity of the PU strongly depend

DOI: 10.1002/sec

on the channel conditions of the SU-Tx to the EAV link and SU-Tx transmit power policy. Most interestingly, our results reveal the security of the PU can be improved by the interference from the SU-Tx to the EAV.

The remainder of this paper is organized as follows. Section 2 describes the system and channel model. In Section 3, the SU-Tx transmit power policy, the CDF, and PDF of the received SINR are derived. In Section 4, analytical expressions of the secondary SEP and achievable rate, and the primary probability of existence of non-zero secrecy capacity and outage probability of the secrecy capacity are obtained. Numerical results and discussion are provided in Section 5. Finally, conclusions are presented in Section 6.

2. SYSTEM AND CHANNEL MODEL

2.1. System model

Let us consider a CRN model as shown in Figure 1 in which a trustworthy SU-Tx utilizes the licensed frequency band of the PU to communicate with the SU receiver (SU-Rx). There exists an EAV who attempts to decode the PU's message. The SU transmits on the same channel as the PU as long as the received interference at the PU-Rx remains below a predefined threshold. Note that a related system model has been considered in [17,18], but without interference power constraints of the SU.

On the basis of Shannon theorem, the channel capacity between the PU-Tx and PU-Rx under interference caused by the SU-Tx is given by

$$C_P = B\log_2(1+\gamma_P) \tag{1}$$

where B is the system bandwidth and γ_P is the SINR at the PU-Rx defined by

$$\gamma_P = \frac{P_p h}{P_s \alpha + N_0} \tag{2}$$

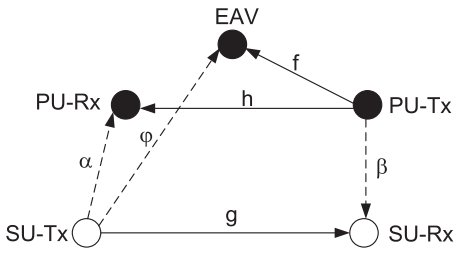

Figure 1. A system model of cognitive radio network in which SU and PU share the same spectrum, while an EAV illegally listens to the PU communication (dashed lines: interference links; solid lines: data information links). PU, primary user; SU, secondary user; EAV, eavesdropper; PU-Tx, PU transmitter; SU-Tx, SU transmitter; PU-Rx, PU receiver; SU-Rx, SU receiver.

while P_p, P_s, and N_0 are the transmit powers of the PU-Tx, SU-Tx, and noise power, respectively. Further, symbols h and α denote the channel power gains of the PU-Tx→PU-Rx communication link and the SU-Tx→PU-Rx interference link, respectively. Similarly, the capacity between the SU-Tx and SU-Rx under interference caused by the PU-Tx can be expressed as

$$C_S = B\log_2(1+\gamma_S) \tag{3}$$

where γ_S is the SINR at the SU-Rx which is formulated as

$$\gamma_S = \frac{P_s g}{P_p \beta + N_0} \tag{4}$$

here, g and β are channel power gains for the SU-Tx→SU-Rx communication link and PU-Tx→SU-Rx interference link, respectively. Due to the nature of broadcast signal in the wireless communication, the EAV may eavesdrop the transmitted information from the PU-Tx to the PU-Rx. However, the received information at the EAV is also subject to the interference caused by the SU-Tx. Thus, the capacity between the PU-Tx and EAV over the wiretap channel is presented as

$$C_E = B\log_2(1+\gamma_E) \tag{5}$$

where γ_E is the SINR at the EAV and defined as

$$\gamma_E = \frac{P_p f}{P_S \varphi + N_0} \tag{6}$$

In (6), f and φ are, respectively, channel power gains of the PU-Tx→EAV and SU-Tx→EAV links.

Based on the random coding approach in [15], we assume that PU-Tx encodes confidential messages $W \in \mathcal{W} = \{1,2,\ldots,M\}$ into a codeword $u^n = \{u(1),u(2),\ldots,u(n)\} \in \mathcal{U}^n$ by using a stochastic encoder $q_n(\cdot) : \mathcal{W} \to \mathcal{U}^n$ and establishes an (M,n) code. The PU-Rx decodes the received signals $v^n = \{v(1),v(2),\ldots,v(n)\} \in \mathcal{V}^n$ using a decoder function $\phi(\cdot) : \mathcal{V}^n \to \mathcal{W}$. In this structure, the PU-Tx should transmit a message to the PU-Rx with an arbitrarily low probability of error, while securing the message against the EAV. The performance of the coding scheme can be measured in terms of average error probability and equivocation rate. The average error probability of an (M,n) code at the PU-Rx is formulated as

$$P_{\text{er}}^n = \sum_{w\in\mathcal{W}} \frac{1}{M} \Pr\{\phi(v^n) \neq w \mid w \quad \text{is sent}\} \tag{7}$$

Note that the average error probability indicates the level of reliable communication between the PU-Tx and PU-Rx. Moreover, the equivocation rate R_e at the EAV measures the secrecy level of confidential message, that is, EAV's uncertainty about w, and is defined as

$$R_e = \frac{1}{n} H(W \mid T^n) \tag{8}$$

where $H(W)$ is the entropy of the amount of information of the transmitted message W and $H(W \mid T^n)$ is the remaining entropy of W given the output information T^n at the EAV. In this work, we only focus on the achievable level of perfect secrecy that requires the equivocation rate R_e to be equal to the message rate [13,15]. The rate R_s is achievable with weak secrecy if there exists a $(2^{nR_s}, n)$ code for a sufficient large n such that $P_{\text{er}}^n \leq \delta$ and $R_e \geq R_s - \delta$ for any given $\delta > 0$. The secrecy capacity is the maximum of the achievable secrecy rate, that is,

$$C_{\text{sec}} \triangleq \sup\{R_s : R_s \quad \text{is achievable with weak secrecy}\} \tag{9}$$

In the rest of the paper, we follow the argument in the literature and consider the secrecy rate that satisfies the definition earlier as perfect secrecy [13,15]. Therefore, the secrecy capacity of the primary communication is given by

$$C_{\text{sec}} = \begin{cases} B\log_2(1+\gamma_P) - B\log_2(1+\gamma_E), & \gamma_P \geq \gamma_E \\ 0, & \gamma_P < \gamma_E \end{cases} \tag{10}$$

2.2. Channel assumptions

The channels are assumed to be block Rayleigh fading, that is, the channel remains constant over one time slot, and may change independently from one slot to the next. This assumption is widely accepted in realistic models for wireless communications and is applicable for severe shadowing environment where the line-of-sight does not exist such as in crowed city with many high buildings. Moreover, we denote Ω_X as the channel mean gain where $X \in \{g, h, f, \alpha, \beta, \varphi\}$, that is, the channel mean gains are non-identical. This is reasonable because users may be located at different positions. Accordingly, the channel power gains are independent but not necessarily identically distributed random variables (RVs) with exponential distribution given as follows:

$$f_X(x) = \frac{1}{\Omega} \exp\left(-\frac{x}{\Omega}\right) \tag{11}$$

$$F_X(x) = 1 - \exp\left(-\frac{x}{\Omega}\right) \tag{12}$$

where $f_X(x)$ and $F_X(x)$ are the PDF and CDF of the RV X, respectively.

In the considered SS model, the PU-Tx can transmit with an arbitrary power level for communication without considering the existence of the SU-Rx because it owns spectrum license. On the other hand, the SU-Tx must have a reasonable transmit power policy to not degrade the performance of the PU-Rx. The transmit power of the SU-Tx is controlled based on the CSI of the SU-Tx→PU-Rx and PU-Tx→PU-Rx links. Here, we note that the secondary network and the primary network have limited collaboration, and the dedicated feedback channel from the primary network to the secondary network may not exist. Thus, the instantaneous CSI of the PU-Tx→PU-Rx and SU-Tx→PU-Rx links may not be available at the SU. However, the average channel gain (not instantaneous channel gain) can be estimated by utilizing relatively stable parameters such as transmission distance and antenna gain. This estimation of the average channel gains at the SU may also save feedback channel resources. The SU-Tx and SU-Rx are assumed to have full CSI of their own communication link as they are in the same system and should have a common feedback channel. Nonetheless, the SU-Tx and PU-Tx do not have CSI of the wiretap channels, that is, SU-Tx→EAV and PU-Tx→EAV links as the EAV is a purely passive node [13].

2.3. Spectrum sharing constraints

In an underlay CRN, the SU-Rx should have an appropriate power allocation policy to keep interference at the PU-Rx below a predefined threshold. To achieve this, the knowledge of CSI of the primary network is needed at the SU-Tx. If perfect CSI of the primary channel is available at the SU-Tx, then a PU peak interference power constraint [20] can be applied to protect the primary network. However, in practice, perfect channel information of h and α links at the SU-Tx may not be guaranteed at all times. In this paper, we assume that the SU-Tx has knowledge of channel mean gains Ω_α and Ω_h (e.g., statistical channel knowledge). In particular, the SU-Tx can estimate the average channel gains of the PU based on the system parameters such as transmission distance and transmit/receive antenna gain, which are considered to be relatively stable [21]. In addition, the mean value reduces the PU feedback burden (from PU to the SU) as it requires infrequent updates [22]. In this respect, we employ a probabilistic constraint to keep an acceptable low probability at the PU-Rx. The probabilistic constraint is expressed in terms of a PU minimum target rate that must be guaranteed with a certain desired outage probability [22,23]. As such, the interference constraint given by the PU can be interpreted into the outage probability constraint as

$$P_{\text{out}}^P = \Pr\{B\log_2(1+\gamma_P) < r_p\} \leq \theta_{th} \tag{13}$$

where r_p and θ_{th} are, respectively, the primary network required target rate and outage threshold. From (13), the SU-Tx is allowed to access the licensed frequency band of the PU and causes limited interference to the primary network as long as the PU-Rx outage probability is kept below θ_{th}.

Furthermore, the SU-Tx transmit power is also subject to the SU maximum transmit power limit denoted by P_{pk} such that

$$P_s \leq P_{\text{pk}} \tag{14}$$

This additional constraint of maximum transmit power limit is considered as in practice, the transmit power can not be infinite or very large.

2.4. Performance metrics

This paper has two main objectives: (1) to investigate the impact of the SU transmission (i.e., presence of the SU) on the primary security communication and (2) to analyze and evaluate the effect of the primary network parameters on the secondary system performance. The performance analysis of the secondary network is evaluated in terms of SEP and achievable rate, while the primary system security is analyzed in terms of probability of existence of a non-zero secrecy capacity and secrecy outage probability.

2.4.1. Secondary system performance metrics.

It is noted that the performance of wireless communication systems over fading channels can be quantified through SEP and ergodic capacity. The SEP is defined as the probability that a transmitted data symbol is received with error. It typically depends on modulation scheme, and is directly related to the received SINR of the user. According to [24], the SEP of the SU is expressed as

$$P_e = \frac{\epsilon\sqrt{\eta}}{2\sqrt{\pi}} \int_0^\infty F_{\gamma_S}(\gamma) \frac{\exp(-\eta\gamma)}{\sqrt{\gamma}} d\gamma \tag{15}$$

where ϵ and η are constants that depend on the particular modulation scheme.

Furthermore, ergodic capacity provides an information-theoretic bound on the maximum achievable average rate that a channel can support. The secondary average rate can be obtained as

$$R_{\text{avg}} = B\mathbb{E}[C_S] = B\int_0^\infty \log_2(1+\gamma) f_{\gamma_S}(\gamma) d\gamma \tag{16}$$

where $\mathbb{E}[\cdot]$ denotes the expectation and C_S is the instantaneous SU capacity given in (3).

2.4.2. Primary secure communication.

In a wiretap channel, secure transmission between PU-Tx and PU-Rx can be achieved when $\gamma_P > \gamma_E$. It is shown in [13] that there exists a positive secrecy capacity in fading channel even when the EAV's channel is statistically better than the legitime channel with probability less than 0.5. In what follows, we will analyze the probability of existence of a non-zero secrecy capacity of the PU, which is expressed as

$$P_{\text{ex}} = \Pr\{C_{\text{sec}} > 0\} = \Pr\{\gamma_P > \gamma_E\} \tag{17}$$

For passive eavesdropping, the PU-Tx does not have CSI about the EAV's channel. Hence, the PU-Tx has to set a fixed code rate R_s. If $C_{\text{sec}} > R_s$, the codewords with transmission rate R_s ensures perfect secrecy. On the other hand, if $C_{\text{sec}} < R_s$, the EAV can eavesdrop the data, and therefore, the information security is compromised. In this regard, we analyze the secrecy outage probability as an important and practical secrecy performance metric [14]. The outage probability of secrecy capacity for the primary network is given by

$$P_{\text{out,sec}} = \Pr\{C_{\text{sec}} < R_s\} \tag{18}$$

According to [25, Equation. (6)], this performance metric can be expanded by using the total probability theorem as

$$\begin{aligned} P_{\text{out,sec}} = {} & \Pr\{C_{\text{sec}} < R_s | \gamma_P > \gamma_E\} \Pr\{\gamma_P > \gamma_E\} \\ & + \Pr\{C_{\text{sec}} < R_s | \gamma_P \le \gamma_E\} \Pr\{\gamma_P \le \gamma_E\} \end{aligned} \tag{19}$$

Here, the outage event occurs in two scenarios: firstly, when the SINR at the PU-Rx exceeds to that of EAV but still PU-Rx fail to decode the message (i.e., conventional outage probability) and secondly, when the SINR at EAV node exceeds to that of PU-Rx and the EAV is able to decode the message (i.e., perfect secrecy is compromised).

3. SU-TX TRANSMIT POWER POLICY AND STATISTICS FUNCTIONS

In this section, we derive the power allocation policy for the SU-Tx. Thereafter, the CDF and PDF for different SINRs are obtained. Let us commence by deriving the CDF and PDF of a function of RV which are important to analyze the system performance in next subsections.

Lemma 1. *Assume that a and b are positive constants while X_1 and X_2 are independent exponentially distributed RV with mean values Ω_1 and Ω_2, respectively. A RV Z is defined by*

$$Z = \frac{aX_1}{bX_2 + 1} \tag{20}$$

The CDF and PDF of Z are formulated, respectively, as follows:

$$F_Z(z) = 1 - \frac{1}{1 + z\frac{b\Omega_2}{a\Omega_1}} \exp\left(-\frac{z}{a\Omega_1}\right) \tag{21}$$

$$f_Z(z) = \frac{b\Omega_2}{a\Omega_1} \frac{\exp\left(-\frac{z}{a\Omega_1}\right)}{\left(1 + z\frac{b\Omega_2}{a\Omega_1}\right)^2} + \frac{\exp\left(-\frac{z}{a\Omega_1}\right)}{a\Omega_1\left(1 + z\frac{b\Omega_2}{a\Omega_1}\right)} \tag{22}$$

Proof. According to the probability definition, the CDF of the RV Z can be derived by using the same approach in [26, Eq. (14)] as

$$\begin{aligned} F_Z(z) &= \Pr\{Z < z\} \\ &= \int_0^\infty \Pr\left\{X_1 < \frac{z(bx+1)}{a}\right\} f_{X_2}(x) dx \end{aligned} \tag{23}$$

As X_1 and X_2 are independent exponentially distributed RV, (23) can be rewritten as

$$F_Z(z) = \int_0^\infty \left\{1 - \exp\left[-\frac{z(bx+1)}{a\Omega_1}\right]\right\} \times \frac{1}{\Omega_2}\exp\left(-\frac{x}{\Omega_2}\right)dx \tag{24}$$

After integration, the CDF of Z is obtained as in (21). Then, by differentiating (21) with respect to z, we obtain the PDF of Z as shown in (22). □

3.1. Power allocation policy of the SU-Tx

As the SU accesses the licensed frequency band of the PU, the SU-Tx must have a flexible transmit power policy to keep the interference of the PU below a predetermined threshold. From (13), we can derive the outage probability of the PU to withdraw the transmit power expression of the SU as

$$P_{\text{out}}^{\text{P}} = \Pr\left\{\frac{P_p h}{P_s \alpha + N_0} < \gamma_{th}\right\} \tag{25}$$

where $\gamma_{th} = 2^{\frac{r_p}{B}} - 1$. Using the Lemma 1, an expression for the PU outage probability is presented as

$$P_{\text{out}}^{\text{P}} = 1 - \frac{P_p \Omega_h}{\gamma_{th} P_s \Omega_\alpha + P_p \Omega_h}\exp\left(-\frac{N_0 \gamma_{th}}{P_p \Omega_h}\right) \tag{26}$$

Substituting (26) into (13) and then combining with (14) yields an adaptive transmit power policy of the SU-Tx as

$$\mathcal{P} = \min\left\{\frac{P_p \Omega_h}{\gamma_{th}\Omega_\alpha}\chi^+, P_{\text{pk}}\right\} \tag{27}$$

where

$$\chi^+ = \max\left\{\frac{1}{1-\theta_{th}}\exp\left(-\frac{N_0\gamma_{th}}{P_p\Omega_h}\right) - 1, 0\right\} \tag{28}$$

In what follows, the SU-Tx uses the power allocation policy given in (27) to transmit the signal to the SU-Rx.

3.2. Statistics for SINR

By looking into the considered performance metrics given in (15), (16) (17), and (19), we can see that the CDF and PDF for the SINRs are important functions to analyze the system performance. Therefore, we derive these functions as follows:

Using the power allocation policy given in (27) and setting $c = \frac{P_p}{N_0}$ and $d = \frac{\mathcal{P}}{N_0}$ as the signal-to-noise ratios (SNRs), the SINR at the PU-Rx, SU-Rx, and EAV given respectively in (2), (4), and (6) are rewritten as

$$\gamma_P = \frac{ch}{d\alpha + 1} \tag{29}$$

$$\gamma_S = \frac{dg}{c\beta + 1} \tag{30}$$

$$\gamma_E = \frac{cf}{d\varphi + 1} \tag{31}$$

3.2.1. CDF and PDF of γ_P.

Using *Lemma 1*, the CDF and PDF of γ_P can be obtained by setting $a = c, b = d, \Omega_1 = \Omega_h$, and $\Omega_2 = \Omega_\alpha$ as follows:

$$F_{\gamma_P}(x) = 1 - \frac{1}{1+xA_0}\exp\left(-\frac{x}{B_0}\right) \tag{32}$$

$$f_{\gamma_P}(x) = \exp\left(-\frac{x}{B_0}\right)\left[\frac{A_0}{(1+A_0x)^2} + \frac{1}{B_0(1+A_0x)}\right] \tag{33}$$

where $A_0 = \frac{d\Omega_\alpha}{c\Omega_h}$ and $\frac{1}{B_0} = \frac{1}{c\Omega_h}$.

3.2.2. CDF and PDF of γ_S.

By setting $a = d, b = c, \Omega_1 = \Omega_g$, and $\Omega_2 = \Omega_\beta$, we also obtain the CDF and PDF of γ_S as

$$F_{\gamma_S}(u) = 1 - \frac{1}{1+uF_0}\exp\left(-\frac{u}{G_0}\right) \tag{34}$$

$$f_{\gamma_S}(u) = \exp\left(-\frac{u}{G_0}\right)\left[\frac{F_0}{(1+F_0u)^2} + \frac{1}{G_0(1+F_0u)}\right] \tag{35}$$

where $F_0 = \frac{c\Omega_\beta}{d\Omega_g}$ and $\frac{1}{G_0} = \frac{1}{d\Omega_g}$.

3.2.3. CDF and PDF of γ_E.

Similarly, the CDF and PDF of γ_E are, respectively, obtained by setting $a = c, b = d, \Omega_1 = \Omega_f$, and $\Omega_2 = \Omega_\varphi$ as

$$F_{\gamma_E}(y) = 1 - \frac{1}{1+yD_0}\exp\left(-\frac{y}{E_0}\right) \tag{36}$$

$$f_{\gamma_E}(y) = \exp\left(-\frac{y}{E_0}\right)\left[\frac{D_0}{(1+D_0y)^2} + \frac{1}{E_0(1+D_0y)}\right] \tag{37}$$

where $D_0 = \frac{d\Omega_\varphi}{c\Omega_f}$ and $\frac{1}{E_0} = \frac{1}{c\Omega_f}$.

4. PERFORMANCE ANALYSIS

In this section, we first derive analytical expressions of the secondary SEP and average rate based on the CDF of γ_S. Moreover, we analyze the primary system security and

DOI: 10.1002/sec

derive closed-form expressions for the probability of existence of non-zero secrecy capacity and outage probability of the secrecy capacity.

4.1. Symbol error probability of the SU

By substituting (34) into (15), an expression of the SU SEP can be presented as

$$P_e = \underbrace{\frac{\epsilon\sqrt{\eta}}{2\sqrt{\pi}}\int_0^\infty \frac{\exp(-\eta\gamma)}{\sqrt{\gamma}}d\gamma}_{H_1} - \underbrace{\frac{\epsilon\sqrt{\eta}}{2\sqrt{\pi}}\int_0^\infty \frac{\exp\left(-\frac{\gamma}{F_1}\right)}{(1+F_0\gamma)\sqrt{\gamma}}d\gamma}_{H_2} \tag{38}$$

where $\frac{1}{F_1} = \frac{1}{G_0} + \eta$. Moreover, using [27, Eq. (3.361.2)], H_1 is given by

$$H_1 = \frac{\epsilon}{2} \tag{39}$$

Furthermore, by changing variable and setting $t = \gamma + \frac{1}{F_0}$, H_2 is obtained as

$$\begin{aligned} H_2 &= \frac{\epsilon\sqrt{\eta}}{2\sqrt{\pi}}\frac{1}{F_0}\exp\left(\frac{1}{F_0F_1}\right)\int_{\frac{1}{F_0}}^\infty \frac{\exp\left(-\frac{t}{F_1}\right)}{t\sqrt{t-\frac{1}{F_0}}}dt \\ &= \frac{\epsilon}{2}\sqrt{\frac{\eta\pi}{F_0}}\exp\left(\frac{1}{F_0F_1}\right)\left[1-\mathcal{Q}\left(\frac{1}{\sqrt{F_0F_1}}\right)\right] \end{aligned} \tag{40}$$

where (40) is solved with the help of [27, Eq. (3.363.2)] and $\mathcal{Q}(\cdot)$ is the error function defined as $\mathcal{Q}(z) = (2/\sqrt{\pi})\int_0^z \exp(-t^2)dt$. As a consequence, the analytical expression of the SU SEP is given by

$$P_e = \frac{\epsilon}{2} - \frac{\epsilon}{2}\sqrt{\frac{\eta\pi}{F_0}}\exp\left(\frac{1}{F_0F_1}\right)\left[1-\mathcal{Q}\left(\frac{1}{\sqrt{F_0F_1}}\right)\right] \tag{41}$$

4.2. Average rate of the SU

Applying the integration by parts technique in (16), the secondary average rate can be rewritten as

$$R_{\text{avg}} = B\log_2(e)\int_0^\infty \frac{1}{1+\gamma}\left[1-F_{\gamma_S}(\gamma)\right]d\gamma \tag{42}$$

Then, substituting (34) into (42), two cases are considered as follows:

- If $F_0 = 1$ and with the help of [27, Eq. (3.353.3)], we obtain

$$R_{\text{avg}} = B\log_2(e)\left[1+\frac{1}{G_0}\exp\left(\frac{1}{G_0}\right)\text{Ei}\left(-\frac{1}{G_0}\right)\right] \tag{43}$$

- If $F_0 \neq 1$, we have

$$\begin{aligned} R_{\text{avg}} &= B\log_2(e)\int_0^\infty \frac{\exp\left(-\frac{u}{G_0}\right)}{(1+u)(1+F_0u)}du \\ &= B\log_2(e)\left[\frac{1}{1-F_0}\exp\left(\frac{1}{G_0}\right)\Gamma\left(0,\frac{1}{G_0}\right)\right. \\ &\quad \left.+\frac{\exp\left(\frac{1}{F_0G_0}\right)}{F_0-1}\Gamma\left(0,\frac{1}{F_0G_0}\right)\right] \end{aligned} \tag{44}$$

where $\text{Ei}(z) = -\int_{-z}^\infty (e^{-t}/t)dt$ is the exponential integral and $\Gamma[0,z] = -\text{Ei}(-z)$ for $z > 0$ is the incomplete gamma function [27]. Note that (44) is solved by using partial function technique and with the help of [27, Eq. (3.352.4)].

4.3. Analysis of secure communication of the PU

4.3.1. Probability of existence of secrecy capacity.

According to the margin probability definition, we can derive the probability of existence of non-zero secrecy capacity for the PU given in (17) as follows:

$$\begin{aligned} P_{\text{ex}} &= 1 - \int_0^\infty \Pr\{\gamma_P < y\} f_{\gamma_E}(y)dy \\ &= D_0\int_0^\infty \frac{\exp\left[-\left(\frac{1}{B_0}+\frac{1}{E_0}\right)y\right]}{(1+yA_0)(1+D_0y)^2}dy \\ &\quad + \frac{1}{E_0}\int_0^\infty \frac{\exp\left[-\left(\frac{1}{B_0}+\frac{1}{E_0}\right)y\right]}{(1+A_0yt)(1+yD_0)}dy \end{aligned} \tag{45}$$

where $f_{\gamma_E}(y)$ is given in (37). By setting $\frac{1}{C_0} = \frac{1}{B_0} + \frac{1}{E_0}$, we can rewrite (45) as

$$P_{\text{ex}} = \underbrace{D_0\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{(1+yA_0)(1+D_0y)^2}dy}_{I_1} + \underbrace{\frac{1}{E_0}\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{(1+A_0y)(1+yD_0)}dy}_{I_2} \tag{46}$$

Moreover, I_1 and I_2 can be solved as follows:

- If $A_0 = D_0$, the integrals I_1 and I_2 can be calculated with the help of [27, Eq. (3.353.2)] and [27, Eq.(3.353.3)], respectively, as

$$\begin{aligned} I_1 &= D_0\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{(1+yD_0)^3}dy = \frac{C_0D_0-1}{2C_0D_0} \\ &\quad + \frac{1}{2C_0^2D_0^2}\exp\left(\frac{1}{C_0D_0}\right)\Gamma\left(0,\frac{1}{C_0D_0}\right) \end{aligned} \tag{47}$$

$$I_2 = \frac{1}{E_0}\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{(1+D_0y)^2}dy = \frac{\exp\left(\frac{1}{C_0D_0}\right)}{C_0D_0^2E_0} \times \mathrm{Ei}\left(-\frac{1}{C_0D_0}\right) + \frac{1}{E_0D_0} \tag{48}$$

- If $A_0 \neq D_0$, I_1 is derived as

$$I_1 = \underbrace{\frac{A_0^2D_0}{(D_0-A_0)^2}\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{1+A_0y}dy}_{I_{11}} + \underbrace{\frac{D_0^2}{D_0-A_0}\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{(1+D_0y)^2}dy}_{I_{12}} - \underbrace{\frac{A_0D_0^2}{(D_0-A_0)^2}\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{1+D_0y}dy}_{I_{13}} \tag{49}$$

where the integrals I_{11} and I_{13} are solved using [27, Eq. (3.352.4)] as

$$I_{11} = \frac{A_0D_0}{(D_0-A_0)^2}\exp\left(\frac{1}{A_0C_0}\right)\Gamma\left(0,\frac{1}{A_0C_0}\right) \tag{50}$$

$$I_{13} = \frac{A_0D_0}{(D_0-A_0)^2}\exp\left(\frac{1}{C_0D_0}\right)\Gamma\left(0,\frac{1}{C_0D_0}\right) \tag{51}$$

Further, with the help of [27, Eq. (3.353.3)], we obtain an expression for I_{12} as

$$I_{12} = \frac{D_0}{D_0-A_0} + \frac{1}{C_0(D_0-A_0)}\exp\left(\frac{1}{C_0D_0}\right)\mathrm{Ei}\left(-\frac{1}{C_0D_0}\right) \tag{52}$$

In addition, when $A_0 \neq D_0$, I_2 is calculated as

$$I_2 = \underbrace{\frac{A_0}{E_0(A_0-D_0)}\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{1+A_0y}dy}_{I_{21}} - \underbrace{\frac{D_0}{E_0(A_0-D_0)}\int_0^\infty \frac{\exp\left(-\frac{y}{C_0}\right)}{1+D_0y}dy}_{I_{22}} \tag{53}$$

The expressions of I_{21} and I_{22} are obtained as

$$I_{21} = \frac{\exp\left(\frac{1}{A_0C_0}\right)}{E_0(A_0-D_0)}\Gamma\left(0,\frac{1}{A_0C_0}\right) \tag{54}$$

$$I_{22} = \frac{\exp\left(\frac{1}{C_0D_0}\right)}{E_0(A_0-D_0)}\Gamma\left(0,\frac{1}{C_0D_0}\right) \tag{55}$$

Finally, the expression of probability of existence of secrecy capacity of the PU is obtained as

For $A_0 = D_0$,

$$P_{\mathrm{ex}} = \frac{C_0D_0-1}{2C_0D_0} + \frac{1}{D_0E_0}\exp\left(\frac{1}{C_0D_0}\right) \times \Gamma\left(0,\frac{1}{C_0D_0}\right)\left[\frac{1}{2C_0^2D_0^2} + \frac{1}{C_0^2D_0^2E_0}\right] \tag{56}$$

For $A_0 \neq D_0$,

$$P_{\mathrm{ex}} = \frac{A_0D_0}{(D_0-A_0)^2}\left[\exp\left(\frac{1}{A_0C_0}\right)\Gamma\left(0,\frac{1}{A_0C_0}\right) - \exp\left(\frac{1}{C_0D_0}\right)\Gamma\left(0,\frac{1}{C_0D_0}\right)\right] + \frac{D_0}{D_0-A_0} + \frac{1}{C_0\,(D_0-A_0)}\exp\left(\frac{1}{C_0D_0}\right)\mathrm{Ei}\left(-\frac{1}{C_0D_0}\right) + \frac{1}{E_0\,(A_0-D_0)}\left[\exp\left(\frac{1}{A_0C_0}\right)\Gamma\left(0,\frac{1}{A_0C_0}\right) - \exp\left(\frac{1}{C_0D_0}\right)\Gamma\left(0,\frac{1}{C_0D_0}\right)\right] \tag{57}$$

4.3.2. Outage probability of secrecy capacity.

The probability of outage of the secrecy capacity of the PU in (19) can be rewritten as

$$P_{\mathrm{out,sec}} = \underbrace{\Pr\{C_{\mathrm{sec}} < R_s|\gamma_P > \gamma_E\}}_{J_1}\Pr\{\gamma_P > \gamma_E\} + \underbrace{\Pr\{C_{\mathrm{sec}} < R_s|\gamma_P \leq \gamma_E\}\Pr\{\gamma_P \leq \gamma_E\}}_{J_2} \tag{58}$$

where $\Pr\{\gamma_P > \gamma_E\} = P_{\mathrm{ex}}$ and $\Pr\{C_{\mathrm{sec}} < R_s|\gamma_P \leq \gamma_E\} = 1$ because $R_s > 0$. Accordingly, J_2 is given by

$$J_2 = \Pr\{\gamma_P \leq \gamma_E\} = 1 - \Pr\{\gamma_P > \gamma_E\} = 1 - P_{\mathrm{ex}} \tag{59}$$

Furthermore, we derive J_1 by using the Bayes's law as follows:

$$J_1 = \Pr\left\{\frac{1+\gamma_P}{1+\gamma_E} < \xi, \gamma_P > \gamma_E\right\} = \int_0^\infty \int_y^{\xi(1+y)-1} f_{\gamma_P}(x)f_{\gamma_E}(y)dxdy = J_{11} - J_{12} \tag{60}$$

where $\xi = 2^{\frac{R_s}{B}}$ and

$$J_{11} = \int_0^\infty F_{\gamma_P}\left[\xi(1+y)-1\right] f_{\gamma_E}(y)dy \tag{61}$$

$$J_{12} = \int_0^\infty F_{\gamma_P}(y) f_{\gamma_E}(y)dy = \Pr\{\gamma_P < \gamma_E\} = 1 - P_{ex} \tag{62}$$

Substituting (32) into (61), we have

$$\begin{aligned} J_{11} &= \int_0^\infty \left\{1 - \frac{\exp\left[-\frac{\xi(1+y)-1}{B_0}\right]}{1+A_0[\xi(1+y)-1]}\right\} f_{\gamma_E}(y)dy \\ &= 1 - \underbrace{\frac{\exp\left(-\frac{\xi-1}{B_0}\right)}{1+A_0(\xi-1)} \int_0^\infty \frac{\exp\left(-\frac{\xi}{B_0}y\right)}{1+\frac{A_0\xi}{1+A_0(\xi-1)}y} f_{\gamma_E}(y)dy}_{J_{111}} \end{aligned} \tag{63}$$

where again $f_{\gamma_E}(y)$ is given in (37). Moreover, by setting $A_1 = \frac{\exp\left(-\frac{\xi-1}{B_0}\right)}{1+A_0(\xi-1)}$ and $D_1 = \frac{A_0\xi}{1+A_0(\xi-1)}$ in (63), we can rewrite J_{111} as

$$\begin{aligned} J_{111} &= A_1 \int_0^\infty \frac{\exp\left(-\frac{\xi}{B_0}y\right)}{1+D_1y} \left[\frac{D_0 \exp\left(-\frac{y}{E_0}\right)}{(1+D_0y)^2} + \frac{\exp\left(-\frac{y}{E_0}\right)}{E_0(1+D_0y)}\right] dy \\ &= \underbrace{A_1D_0 \int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{(1+D_1y)(1+D_0y)^2}dy}_{K_1} \\ &\quad + \underbrace{\frac{A_1}{E_0}\int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{(1+D_1y)(1+D_0y)}dy}_{K_2} \end{aligned} \tag{64}$$

where $\frac{1}{B_1} = \frac{\xi}{B_0} + \frac{1}{E_0}$. Further, K_1 and K_2 can be obtained as follows:

If $D_1 = D_0$, K_1 and K_2 are calculated with the help of [27, Eq.(3.353.2)] and [27, Eq.(3.353.3)], respectively, as

$$\begin{aligned} K_1 = D_0A_1 \int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{(1+D_0y)^3}dy &= A_1\left[\frac{1}{2} - \frac{1}{2D_0B_1} \right. \\ &\left. + \frac{\exp\left(\frac{1}{D_0B_1}\right)}{2D_0^2B_1^2}\Gamma\left(0, \frac{1}{D_0B_1}\right)\right] \end{aligned} \tag{65}$$

$$\begin{aligned} K_2 = \frac{A_1}{E_0}\int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{(1+D_1y)^2}dy &= \frac{A_1}{D_0E_0} + \frac{A_1}{D_0^2E_0B_1} \\ &\times \exp\left(\frac{1}{D_0B_1}\right)\mathrm{Ei}\left(-\frac{1}{D_0B_1}\right) \end{aligned} \tag{66}$$

If $D_1 \neq D_0$, we can obtain K_1 and K_2, respectively, as follows:

$$\begin{aligned} K_1 &= D_0A_1 \int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{(1+D_0y)^2(1+D_1y)}dy \\ &= K_{11} - K_{12} + K_{13} \end{aligned} \tag{67}$$

$$K_2 = \frac{A_1}{E_0}\int_0^\infty \frac{\exp\left(-\frac{1}{B_1}\right)}{(1+D_1y)(1+D_0y)}dy = K_{21} - K_{22} \tag{68}$$

where K_{11}, K_{12}, K_{13}, K_{21}, and K_{22} are calculated as follows:

$$\begin{aligned} K_{11} = \frac{A_1D_0^2}{(D_0-D_1)}\int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{(1+D_0y)^2}dy &= \frac{D_0A_1}{D_0-D_1} \\ &+ \frac{A_1\exp\left(\frac{1}{D_0B_1}\right)}{B_1(D_0-D_1)}\mathrm{Ei}\left(-\frac{1}{D_0B_1}\right) \end{aligned} \tag{69}$$

$$\begin{aligned} K_{12} &= \frac{A_1D_0^2D_1}{(D_0-D_1)^2}\int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{1+D_0y}dy \\ &= \frac{A_1D_0D_1}{(D_0-D_1)^2}\exp\left(\frac{1}{D_0B_1}\right)\Gamma\left(0, \frac{1}{D_0B_1}\right) \end{aligned} \tag{70}$$

$$\begin{aligned} K_{13} &= \frac{A_1D_0D_1^2}{(D_0-D_1)^2}\int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{1+D_1y}dy \\ &= \frac{A_1D_0D_1}{(D_0-D_1)^2}\exp\left(\frac{1}{B_1D_1}\right)\Gamma\left(-\frac{1}{B_1D_1}\right) \end{aligned} \tag{71}$$

$$\begin{aligned} K_{21} &= \frac{D_0A_1}{E_0(D_0-D_1)}\int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{1+D_0y}dy \\ &= \frac{A_1\exp\left(\frac{1}{D_0B_1}\right)}{E_0(D_0-D_1)}\Gamma\left(0, \frac{1}{D_0B_1}\right) \end{aligned} \tag{72}$$

$$\begin{aligned} K_{22} &= \frac{A_1D_1}{E_0(D_0-D_1)}\int_0^\infty \frac{\exp\left(-\frac{y}{B_1}\right)}{1+D_1y}dy \\ &= \frac{A_1\exp\left(\frac{1}{B_1D_1}\right)}{E_0(D_0-D_1)}\Gamma\left(0, \frac{1}{B_1D_1}\right) \end{aligned} \tag{73}$$

It is noted that K_{11} is solved using [27, Eq. (3.353.3)], while K_{12}, K_{13}, K_{21}, and K_{22} are reached with the help of [27, Eq. (3.352.4)]. Then, the final expression of $P_{\text{out,sec}}$ is obtained as

For $D_1 = D_0$,

$$P_{\text{out,sec}} = 1 - \frac{A_1}{2} + \frac{A_2}{2D_0B_1} - \frac{A_1 \exp\left(\frac{1}{D_0B_1}\right)}{2D_0^2B_1^2} \times \Gamma\left(0, \frac{1}{D_0B_1}\right) - \frac{A_1}{D_0E_0} - \frac{A_1}{D_0^2E_0B_1} \times \exp\left(\frac{1}{D_0B_1}\right) \text{Ei}\left(-\frac{1}{D_0B_1}\right) \quad (74)$$

For $D_1 \neq D_0$,

$$P_{\text{out,sec}} = 1 - \frac{D_0A_1}{D_0 - D_1} - \frac{A_1 \exp\left(\frac{1}{D_0B_1}\right)}{B_1(D_0 - D_1)} \times \text{Ei}\left(-\frac{1}{D_0B_1}\right) + \frac{A_1D_0D_1}{(D_0 - D_1)^2}\left[\exp\left(\frac{1}{D_0B_1}\right) \times \Gamma\left(0, \frac{1}{D_0B_1}\right) - \exp\left(\frac{1}{B_1D_1}\right)\Gamma\left(-\frac{1}{B_1D_1}\right)\right] + \frac{A_1}{E_0(D_0 - D_1)}\left[\exp\left(\frac{1}{B_1D_1}\right)\Gamma\left(0, \frac{1}{B_1D_1}\right) - \exp\left(\frac{1}{D_0B_1}\right)\Gamma\left(0, \frac{1}{D_0B_1}\right)\right] \quad (75)$$

5. NUMERICAL RESULTS

In this section, the numerical results are presented to analyze the impact of primary network parameters, SU maximum transmit power limit and channel mean powers among users on the on the secondary system performance. Further, we also study the effect of the presence of the SU on the primary network security. Unless otherwise stated, the following system parameter is used for both simulation and analysis: system bandwidth $B = 5$ MHz, for example, bandwidth of Universal Mobile Telecommunications System (UMTS) or Long Term Evolution (LTE) channel.

5.1. SU SEP

Figure 2 illustrates the SU SEP for binary phase-shift keying modulation with different values of the SU maximum transmit SNR $\gamma_{\max}$, $\gamma_{\max} = P_{\text{pk}}/N_0$ and primary network parameter settings.

- Case 1: It is observed that the SU SEP decreases with respect to the increase of the PU transmit SNR, P_p/N_0. This is because when P_p/N_0 increases, the SU-Tx transmit SNR also increases following (27). However, as P_p/N_0 increases further, for example, $P_p/N_0 > 8$ dB, the SU-Tx transmit SNR cannot increase further as it is bounded by $\gamma_{\max}$. As a result, the PU transmit SNR become a strong interference source to the SU, which leads to the increase of the SU SEP.
- Case 2: We set $\gamma_{\max} = 10$ dB, and then compare the change of the SEP to Case 1 where $\gamma_{\max} = 15$ dB. It is easy to see that the SEP optimal value can be obtained at $P_p/N_0 = 2$ dB and then increases rapidly as PU transmit SNR increases further ($P_p/N_0 > 4$ dB). Clearly, the higher $\gamma_{\max}$ is, the degradation of the SEP is slower.

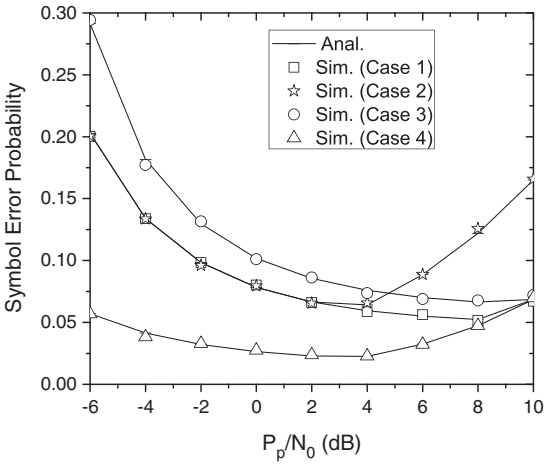

Figure 2. SU SEP versus PU transmit SNR with BPSK modulation scheme, $\Omega_g = \Omega_h = 4$ and $\Omega_\alpha = \Omega_\beta = 2$. Case 1: $\gamma_{\max} = 15$ dB, $r_p = 32$ Kbps, $\theta_{th} = 0.01$; Case 2: $\gamma_{\max} = 10$ dB, $r_p = 32$ Kbps, $\theta_{th} = 0.01$; Case 3: $\gamma_{\max} = 15$ dB, $r_p = 42$ Kbps, $\theta_{th} = 0.01$; Case 4: $\gamma_{\max} = 15$ dB, $r_p = 32$ Kbps, $\theta_{th} = 0.03$. SU SEP, secondary user symbol error probability; PU, primary user; SNR, signal-to-noise ratio; BPSK, binary phase-shift keying.

To observe the impact of the PU target rate r_p and outage threshold θ_{th} on the SEP, we consider the two following cases in Figure 2:

- Case 3: By increasing the PU target rate, for example, $r_p = 32$ Kbps (Case 1) to $r_p = 42$ Kbps, the secondary system performance is degraded (the SU SEP increases). This can be explained by the fact that the increase of r_p leads to higher SINR at the PU-Rx. Accordingly, the SU-Tx must decrease its transmit SNR to satisfy the PU outage constraint, which in turn results in the degradation of the SU SEP.
- Case 4: We can see that the SU SEP is improved when the PU-Rx tolerable error is relaxed, that is, PU outage constraint $\theta_{th} = 0.03$ compared with Case 1 with $\theta_{th} = 0.01$.

Therefore, when the PU QoS requirements are set to high values, the probability of the secondary transmission becomes low, that is, the SU transmit SNR is reduced to satisfy the PU interference power constraint.

Figure 3 illustrates the impact of the channel mean powers of the interference links between primary and

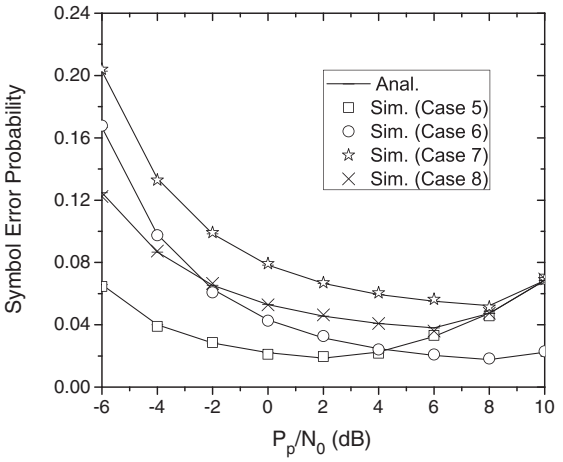

Figure 3. SU SEP versus PU transmit SNR with BPSK modulation scheme, $\gamma_{\max}$ = 15 dB, r_p = 32 Kbps, θ_{th} = 0.01, and Ω_g = 4. Case 5: Ω_h = 4, Ω_α = 0.5, Ω_β = 2; Case 6: Ω_h = 4, Ω_α = 2, Ω_β = 0.5; Case 7: Ω_h = 4, Ω_α = Ω_β = 2; Case 8: Ω_h = 6, Ω_α = 2, Ω_β = 2. SU SEP, secondary user symbol error probability; PU, primary user; SNR, signal-to-noise ratio; BPSK, binary phase-shift keying.

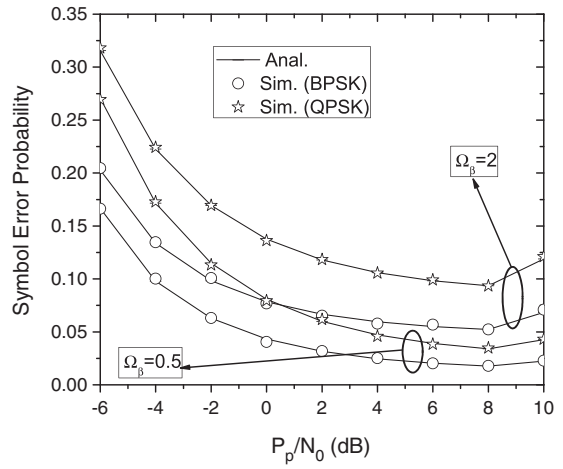

Figure 4. SU SEP versus PU transmit SNR with $\gamma_{\max}$ = 15 dB, r_p = 32 Kbps, θ_{th} = 0.01, Ω_g = Ω_h = 4, and Ω_α = 2. SU SEP, secondary user symbol error probability; PU, primary user; SNR, signal-to-noise ratio; BPSK, binary phase-shift keying; QPSK, quadrature phase-shift keying.

secondary networks, and PU-Tx→PU-Rx link on the SU SEP.

- Cases 5, 6, and 7: It can be observed that the SU SEP becomes high when the channel mean powers of both SU-Tx→PU-Rx and PU-Tx→SU-Rx interference links increase. In particular, when the channel power of the SU-Tx→PU-Rx link increases Ω_α = 0.5 in Case 5 to Ω_α = 2 in Case 7, the SU SEP is high. This is because when Ω_α is high, the PU-Rx suffers strong interference from the SU-Tx. Hence, the SU-Tx must reduce its transmit power to guarantee the PU outage constraint. It is also seen that by increasing the channel mean power of the PU-Tx→SU-Rx from Ω_β = 0.5 (Case 6) to Ω_β = 2 (Case 7), the SU SEP becomes high. In this case, the PU-Tx becomes an interference source to the SU-Rx, which results in the degradation of the secondary network performance.
- Case 8: It is shown that the channel mean power of the PU-Tx→PU-Rx plays an important role on the secondary network performance. For instance, by increasing Ω_h = 4 (Case 7) to Ω_h = 6 (Case 8), the SU SEP decreases significantly. This can be explained by the fact that when Ω_h increases, the PU outage probability decreases resulting in the increase of the the SU-Tx transmit SNR.

In addition, the same impact of the interference from the PU-Tx to SU-Rx is shown in Figure 4 where the SU SEP decreases as Ω_β decreases for different modulation schemes, that is, binary phase-shift keying and quadrature phase shift-keying.

5.2. SU achievable rate

Figure 5 shows the secondary achievable rate as a function of the PU minimum required rate r_p for different values of the PU outage constraint θ_{th}. It is observed that the secondary average rate decreases with the increase of r_p and is low for low value of the PU outage threshold, for example, θ_{th} = 0.01. This is because when the primary network requires high QoS, the SU transmit power is limited to satisfy the interference power constraint at the PU-Rx, which in turn results in degradation of the secondary network performance. The same impact of the primary network parameters on the secondary achievable

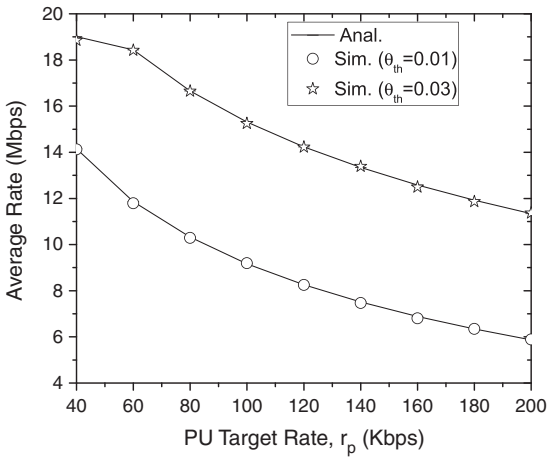

Figure 5. SU average rate versus PU target rate r_p for different values of PU outage constraint where γ_p = 6 dB, $\gamma_{\max}$ = 15 dB, Ω_g = 4, Ω_h = 3, Ω_α = 1.5, and Ω_β = 2. SU, secondary user; PU, primary user.

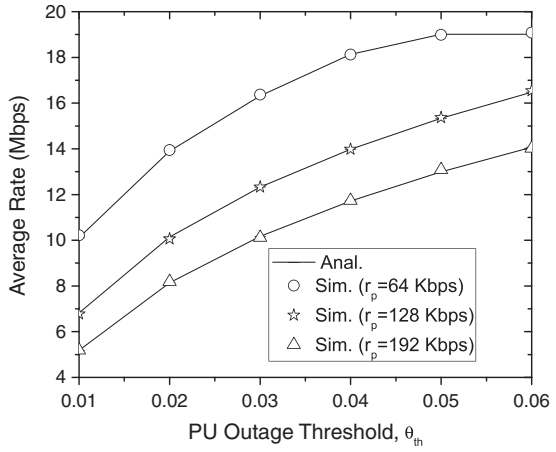

Figure 6. SU average rate versus PU outage constraint for different values of PU target rate r_p where $\gamma_p = 6$ dB, $\gamma_{\max} = 15$ dB, $\Omega_g = 4, \Omega_h = 3$, and $\Omega_\alpha = \Omega_\beta = 2$. SU, secondary user; PU, primary user.

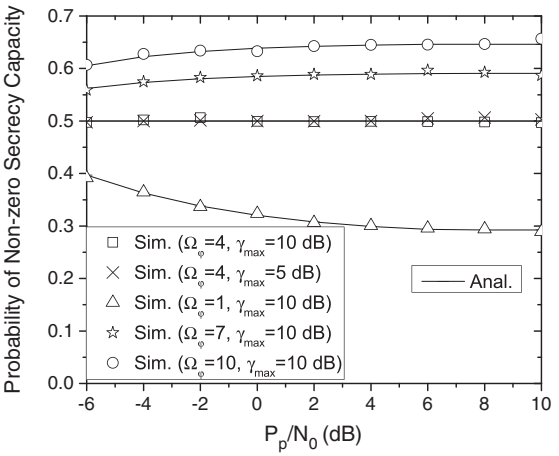

Figure 7. Probability of existence of a non-zero secrecy capacity of the PU versus PU transmit SNR with $r_p = 32$ Kbps, $\theta_{th} = 0.01$, and $\Omega_f = \Omega_g = \Omega_h = \Omega_\alpha = \Omega_\beta = 4$. SU, secondary user; PU, primary user. SNR, signal-to-noise ratio.

rate is also illustrated in Figure 6. Again, we can see that the secondary network performance is improved as the PU-Rx tolerates more error. In addition, the secondary network performance is degraded for high values of r_p, that is, $r_p = 64$ Kbps to $r_p = 192$ Kbps. Note that the aforementioned results in Figures 2, 3, 4, 5, and 6 are in accordance with the SU transmit power policy given in (27).

5.3. Probability of existence of non-zero secrecy capacity of the PU

Figures 7 and 8 illustrate the probability of existence of secrecy capacity of the PU. We can see that this probability does not change with the increase of the PU-Tx transmit SNR for the case of identical channel mean powers and for different values of the SU maximum transmit SNR. In fact, the probability of existence of secrecy capacity strongly depends on the channel condition of the SU-Tx→EAV link. It can be observed that the primary network security is enhanced when the channel mean power of the interference link SU-Tx→EAV Ω_φ increases. For instance, the probability of existence of secrecy capacity increases significantly in Figure 7 by increasing $\Omega_\varphi = 4$ to $\Omega_\varphi = 7, 10$ and from $\Omega_\varphi = 4$ to $\Omega_\varphi = 8$ in Figure 8, respectively. Here, the SU-Tx becomes a strong interference source to the EAV, which degrades the received SINR at the EAV, and hence, the primary network security becomes high. Moreover, we can see from Figure 8 that when Ω_α decreases, the primary network security is also improved. The reason is that decreasing Ω_α results in the increase of the SU-Tx transmit SNR, which results in high interference to the EAV. Thus, curves in Figures 7 and 8 show that the presence of the SU contributes significantly to the primary network security.

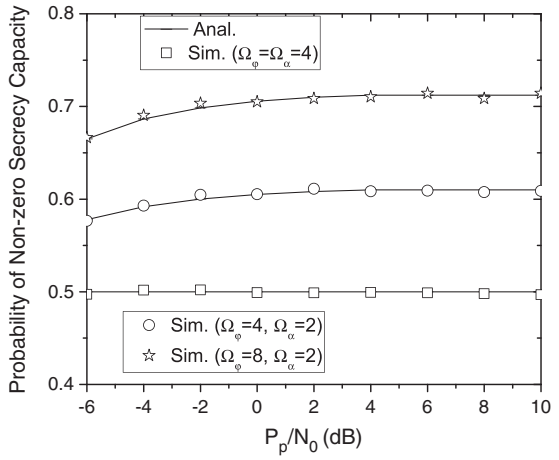

Figure 8. Probability of existence of non-zero secrecy capacity of the PU versus PU transmit SNR with $\gamma_{\max} = 15$ dB, $r_p = 32$ Kbps, $\theta_{th} = 0.01$, and $\Omega_f = \Omega_g = \Omega_h = \Omega_\beta = 4$. PU, primary user; SNR, signal-to-noise ratio.

5.4. Outage probability of secrecy capacity of the PU

Figure 9 illustrates the outage probability of secrecy capacity of the PU.

- Cases 9 and 10: As discussed for the probability of existence of secrecy capacity in Figure 7, it can also be observed that the outage probability of secrecy capacity does not change with the increase of the PU-Tx transmit SNR for the case of identical channels.
- Cases 11 and 12: When the channel mean power of the SU-tx→EAV link increases, for example, $\Omega_\varphi = 8$ in both cases, the primary network security is improved compared with Cases 9 ($\Omega_\varphi = 2$) and 10 ($\Omega_\varphi = 4$).

DOI: 10.1002/sec

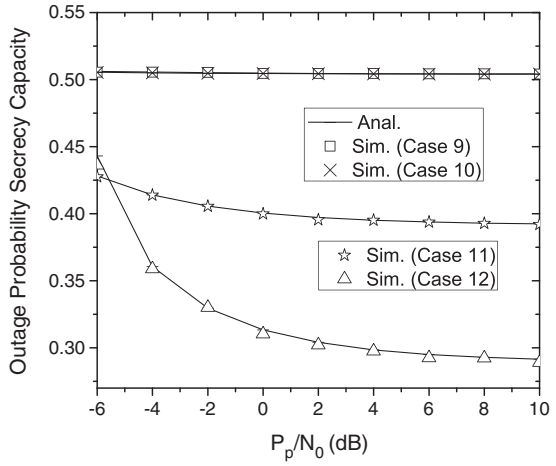

Figure 9. Outage probability of secrecy capacity of the PU versus PU transmit SNR with $R_s = r_p = 32$ Kbps, $\theta_{th} = 0.01$, and $\gamma_{\max} = 15$ dB. Case 9: $\Omega_f = \Omega_h = \Omega_\alpha = \Omega_\varphi = 2$; Case 10: $\Omega_f = \Omega_h = \Omega_\alpha = \Omega_\varphi = 4$; Case 11: $\Omega_f = \Omega_h = \Omega_\alpha = 4$, $\Omega_\varphi = 8$; Case 12: $\Omega_f = \Omega_h = \Omega_\alpha = 2$, $\Omega_\varphi = 8$. PU, primary user; SNR, signal-to-noise ratio.

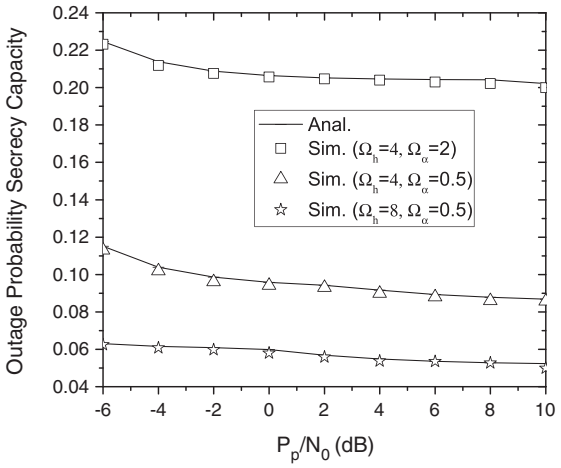

Figure 10. Outage probability of secrecy capacity of the PU versus PU transmit SNR with $R_s = r_p = 32$ Kbps, $\theta_{th} = 0.01$, $\gamma_{\max} = 15$ dB, and $\Omega_f = \Omega_\varphi = 4$. PU, primary user; SNR, signal-to-noise ratio.

Furthermore, Figure 10 shows that the outage probability of secrecy capacity decreases as the channel mean power of the SU-Tx→PU-Rx link decreases, $\Omega_\alpha = 2$ to 0.5. Again, the SU-Tx transmit SNR increases because of the decrease of Ω_α, and hence, the interference from the SU-Tx to EAV becomes high. In addition, the outage probability of secrecy capacity decreases as the channel mean power of the PU-tx→PU-Rx link increases, for example, $\Omega_h = 4$ to 8 with $\Omega_\varphi = 4$ as shown in Figure 10. This is expected because the PU-tx→PU-Rx link becomes better than the PU-tx→EAV link in this scenario.

Moreover, Figure 11 illustrates the outage probability of secrecy capacity of the PU as a function of the SU secrecy rate. It is shown that the secrecy outage probability

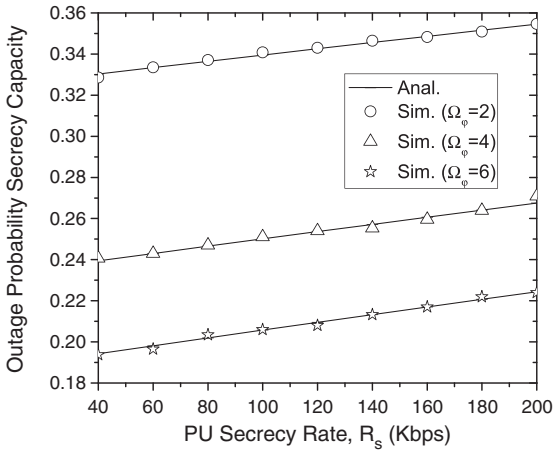

Figure 11. Outage probability of secrecy capacity of the PU versus PU secrecy rate R_s where $\gamma_p = 6$ dB, $\theta_{th} = 0.01$, $r_p = 40$ Kbps, $\gamma_{\max} = 15$ dB, and $\Omega_f = 2$, $\Omega_g = 4$, $\Omega_h = 3$, and $\Omega_\alpha = \Omega_\beta = 1$. PU, primary user; SNR, signal-to-noise ratio.

increases with the increase of R_s. Furthermore, when the EAV moves closer to the SU-tx (e.g., $\Omega_\varphi = 2$ to $\Omega_\varphi = 6$), the primary network is improved significantly. Here, the SU-Tx becomes source interference of the EAV, and thus, the EAV's channel is degraded. The results illustrated in Figures 7, 8, 9, 10, and 11 reveal that the primary network security strongly depends on the channel condition of the SU-tx→EAV and the SU-Tx transmit power policy.

6. CONCLUSIONS

In this paper, we have characterized the role of the SU to enhance primary network security and investigated the secondary system performance. Specifically, the outage probability of secrecy capacity and probability of existence of non-zero secrecy capacity of the PU have been derived under the joint constraint of the PU outage and maximum transmit power limit of the SU. The closed-form expressions of the SEP and achievable rate of the secondary network have been obtained. In addition, the impact of the primary network parameters, channel conditions among users, and SU peak transmit power on the system performance is investigated. Most importantly, our results indicate that the interference from the SU to the EAV significantly contributes to the primary network security enhancement. The obtained results provide valuable insights to system designers in a SS CRN where the interference can be managed to bring more benefit to the heterogeneous wireless networks with secrecy constraints.

ACKNOWLEDGEMENTS

This work is supported by the University of Rwanda (UR), Sweden Programme for Research, Higher Education and Institution Advancement under the Swedish

International Development Agency (SIDA), and Vietnam National Foundation for Science and Technology Development (NAFOSTED, number 102.01-2010.09).

REFERENCES

1. Liang YC, Chen KW, Li GY, Mähönen P. Cognitive radio networking and communications: an overview. *IEEE Transactions Vehicular Technology* 2011; **60**(7): 3386–3407.
2. Haykin S. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications* 2005; **23**(2): 201–220.
3. Akyildiz I, Lee W, Vuran M, Mohanty S. Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Network* 2006; **50**(13): 2127–2159.
4. Goldsmith A, Jafar S, Maric I, Srinivasa S. Breaking spectrum gridlock with cognitive radios: an information theoretic perspective. *IEEE Proceedings* 2009; **97** (5): 894–914.
5. Khoshkholgh MG, Navaie K, Yanikomeroglu H. Access strategies for spectrum sharing in fading environment: overlay, underlay and mixed. *IEEE Transactions on Mobile Computing* 2010; **9** (12): 1780–1793.
6. Schaefer RF, Boche H. Physical layer service integration in wireless networks: signal processing challenges. *IEEE Signal Processing Magazine* 2014; **31** (3): 147–156.
7. Shiu YS, Chang SY, Wu HC, Huang SCH, Chen HH. Physical layer security in wireless networks: a tutorial. *IEEE Wireless Communications* 2011; **18**(2): 66–74.
8. Wyner A. The wire-tap channel. *Bell. System Technical Journal* 1975; **54**(8): 1355–1387.
9. Goel S, Negi R. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications* 2008; **7**(6): 2180–2189.
10. Zhou X, McKay MR. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation,. *IEEE Transactions on Vehicular Technology* 2010; **59**(8): 3831–3842.
11. Tang X, Liu R, Spasojevic P, Poor HV. Interference assisted secret communication. *IEEE Transactions Information Theory* 2011; **57**(5): 3153–3167.
12. Yue J, Ma C, Yu H, Zhou W. Secrecy-based access control for device-to-device communication underlaying cellular networks. *IEEE Communications Letters* 2013; **17**(11): 2068–2071.
13. Barros J, Rodrigues MR. Secrecy capacity of wireless channels, In *Proc. IEEE International Symposium on Information Theory*, Seattle, WA, USA, 2006; 356–360.
14. Bloch M, Barros JO, Rodrigues MR, McLaughlin SW. Wireless information-theoretic securiry. *IEEE Transactions on Information Theory* 2008; **54** (6): 2515–2534.
15. Gopala PK, Lai L, Gamal HE. On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory* 2008; **54**(10): 4687–4698.
16. Esch J. A survey of security challenges in cognitive radio networks: solutions and future research directions. *IEEE Wireless Communications* 2012; **100**(12): 3170–3171.
17. Shu Z, Qian Y, Ci S. On physical layer security for cognitive radio networks. *IEEE Network* 2013; **7**(3): 28–33.
18. Wu Y, Liu K. An information secrecy game in cognitive radio networks. *IEEE Transactions on Information Forensics and Security* 2011; **6**(3): 831–842.
19. Sibomana L, Tran H, Zepernick HJ, Kabiri C. On non-zero secrecy capacity and outage probability of cognitive radio networks, In *Proc. IEEE International Symposium Wireless Personal Multimedia Communications*, Atlantic City, USA, 2013; 1–6.
20. Zhang R. On peak versus average interference power constraints for protecting primary users in cognitive radio networks. *IEEE Transactions on Wireless Communications* 2009; **8**(4): 2112–2120.
21. Zou Y, Zhu J, Zheng B, Yao YD. An adaptive cooperation diversity scheme with best relay selection in cognitive radio networks. *IEEE Transactions on Signal Processing* 2010; **58**(10): 5438–5445.
22. Smith PJ, Domochowski PA, Suraweera HA, Shafi M. The effects of limited channel knowledge on cognitive radio system capacity. *IEEE Transactions on Vehicular Technology* 2013; **62**(2): 927–933.
23. Kang X, Zhang R, Liang YC, Garg HK. Optimal power allocation strategies for fading cognitive radio channels with primary user outage constraint. *IEEE Journal on Selected Areas in Communications* 2011; **2**: 374–383.
24. MacKay M, Grant A, Collings I. Performance analysis of MIMO-MRC in double-correlated Rayleigh environments. *IEEE Transactions on Communications* 2007; **55**(3): 497–507.
25. Alves H, DemoSouza R, Debbah M, Bennis M. Performance of transmit antenna selection physical layer security schemes. *IEEE Signal Processing Letters* 2012; **19**(6): 372–375.
26. Chen Y, Huang H, Lau VKN. Cooperative spectrum access for cognitive radio network employing rateless code, In *Proc. IEEE International Conference on Communications*, Beijing, China, 2008; 1–6.
27. Gradshteyn I, Ryzhik I. *Table of Integrals, Series, and Products*. 7th ed. Elsevier: San Diego, California, USA, 2007.