

Accepted Manuscript

Cognitive radio network with secrecy and interference constraints

Hung Tran, Georges Kaddoum, François Gagnon, Louis Sibomana

PII: S1874-4907(16)30246-4

DOI: <http://dx.doi.org/10.1016/j.phycom.2016.12.001>

Reference: PHYCOM 350

To appear in: *Physical Communication*

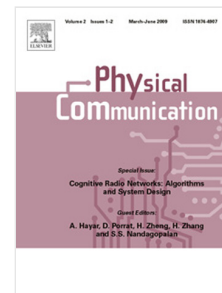
Received date: 28 April 2016

Revised date: 4 October 2016

Accepted date: 6 December 2016

Please cite this article as: H. Tran, G. Kaddoum, F. Gagnon, L. Sibomana, Cognitive radio network with secrecy and interference constraints, *Physical Communication* (2016), <http://dx.doi.org/10.1016/j.phycom.2016.12.001>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Cognitive Radio Network with Secrecy and Interference Constraints

Hung Tran¹, Georges Kaddoum², François Gagnon², Louis Sibomana³

Abstract—In this paper, we investigate the physical-layer security of a secure communication in **single-input multiple-output (SIMO) cognitive radio networks (CRNs)** in the presence of two eavesdroppers. In particular, both primary user (PU) and secondary user (SU) share the same spectrum, but they face with different eavesdroppers who are equipped with multiple antennas. In order to protect the PU communication from the interference of the SU and the risks of eavesdropping, the SU must have a reasonable adaptive transmission power which is set on the basis of channel state information, interference and security constraints of the PU. Accordingly, an upper bound and lower bound for the SU transmission power are derived. Furthermore, a power allocation policy, which is calculated on the convex combination of the upper and lower bound of the SU transmission power, is proposed. On this basis, we investigate the impact of the PU transmission power and channel mean gains on the security and system performance of the SU. Closed-form expressions for the outage probability, probability of non-zero secrecy capacity, and secrecy outage probability are obtained. Interestingly, our results show that the **strong channel mean gain of the PU transmitter to the PU's eavesdropper in the primary network can enhance the SU performance.**

Index Terms—Cognitive Radio Networks, Physical Layer Security, Power Allocation, Security Constraint.

I. INTRODUCTION

Cognitive radio networks (CRNs) have been widely considered as an effective approach to solve the problems of low spectrum utilization for next generation of wireless networks [1]. The key idea behind the CRNs is to let the unlicensed users, known as secondary users (SUs), and licensed users, named as primary users (PUs), share the same frequency band provided that the SUs transmission do not cause harmful interference to the PUs. Based on this concept, two main spectrum access approaches, namely as interweave and underlay, have been proposed [2], [3]. In the interweave approach, the SUs need to find the spectrum holes for their own communication. This approach highly depends on the spectrum detection technique, thus **any missed detection of the SUs may cause severe interference to the PUs.** In addition, in the dense areas, almost spectrum is often occupied by the PUs, and hence this approach is not efficient **due to the lack of spectrum holes.** On the other hands, in the underlay approach, the SUs can concurrently access the licensed spectrum of the PUs as long

as the interference from the SUs to the PUs is maintained below a given threshold. This approach has been obtained a great attention as the SUs can operate in the dense areas where the number of spectrum holes are limited [4]–[10]. Further, the SU can utilize the interference of the PU as an active jamming signal to enhance its security.

There is a fact that the wireless networks face many new security challenges from all aspects of the networking architecture, including the spectrum sensing, spectrum access, and spectrum management due to the natural broadcast property of wireless signals. This becomes more severe in the spectrum underlay approach where the SUs and PUs coexist in the same frequency band, and they may cause mutual interference to each other. To protect the communications confidentiality against the eavesdroppers, the physical layer security has emerged as a promising solution [11]–[17]. Further, to quantify the security of a wireless system, the secrecy capacity metric was formulated as the maximum achievable rate from the transmitter to the legitimate receiver minus the one listening by the eavesdropper over the illegitimate channel. Following this approach, Wyner showed that if the main channel is better than the illegitimate channel, the transmitter can exchange the secure messages with the intended receiver at a non-zero secrecy rate [11]. As an extension of [11], the works in [18]–[23] have studied the physical layer security for various fading models. Face to the same security concerns in the conventional wireless systems, the security policies to against the eavesdroppers becomes **more difficult in the CRN where both SUs and PUs are vulnerable and easy to be eavesdropped due to the mutual interference.** However, in some cases, the secondary transmitter (S-Tx) can take the advantages of fading channel to become an active jammer who can severely degrade the eavesdropper (EAV) capacity in the illegitimate channel, i.e., the PUs secure information may be protected from the EAV by the interference caused by the SUs to the EAV. In the light of this idea, the security concern of the PUs in the CRN has been interpreted into constraints to the SUs, i.e., the SUs are allowed to utilize the licensed spectrum of the PUs as long as the secure criteria and quality of service (QoS) of the PUs are satisfied [24]–[33]. Particularly, in [25] and [29], authors have applied **game theory** cooperation strategies to study the security for a simple CRN scenario where a pair of the SU and a pair of the PU share the same spectrum in the presence of a single EAV. Power allocation and bandwidth assignment strategies have been proposed to enhance the security of the PUs communication.

Regarding to effectiveness of multiple antennas on the security of the CRN, the security problems in the multiple-

¹School of Innovation, Design and Engineering, Malardalen University, Sweden (e-mail: tran.hung@mdh.se).

²University of Québec, ETS engineering school, LACIME Laboratory, Montreal, Canada (e-mail: georges.kaddoum@etsmtl.ca, francois.gagnon@etsmtl.ca).

³School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden (e-mail: lsm@bth.se).

input single-out (MISO) CRNs have been considered in [24], [26], [28]. Authors in [28] have investigated the case where the S-Tx uses the **beamforming technique** to maximize the PU's secrecy capacity under the SU's QoS constraints. In [26] and [24], the SU also uses the beamforming technique to maximize the secrecy rate of the SU while keeping the interference at the PU below a predefined threshold. In [30], the physical layer security with **multiple user scheduling** for CRNs in terms of ergodic secrecy capacity and probability of non-zero secrecy capacity has been examined. More recently, Wang *et al.* have proposed two secure transmission schemes, named as **nonadaptive and adaptive secure transmission strategy**, to maximize the throughput for MISO CRN over slow fading channel [32]. An approximation for the optimal rate parameters of the nonadaptive secure transmission strategy has been obtained at the high signal-to-noise ratio (SNR) regime. However, a power allocation policy for the SU as well as performance analysis of the SU under both the statistical outage and security constraints of the PU have not been studied.

Motivated by all above works, in this paper, we study the performance of a single-input multiple-output (SIMO) CRN under joint constraint of the interference and security of the PU. More specifically, we consider that the two eavesdroppers, named as EAV₁ and EAV₂, equipped with multiple antennas try to overhear the information from the PU and SU in the same spectrum. To guarantee the desired security and performance of the PU, the S-Tx must control its transmission power to meet the peak transmission power of the SU, and both the outage probability constraint and probability of secrecy constraint of the PU. Given these settings, the analysis for the considered secondary network is investigated in two folds, namely as system performance and security performance. Main contributions in this paper are summarized as follows:

- An upper bound and lower bound for the transmission power of the S-Tx are derived. Then, a power allocation policy under the convex combination of the upper and lower transmission power for the S-Tx is proposed.
- To analyse the performance of the SU, a closed-form expression for the outage probability is derived.
- To evaluate the security of the SU, closed-form expressions for the probability of non-zero secrecy capacity and outage secrecy capacity are derived.
- More interestingly, the results show that a strong channel mean gain of the primary transmitter (P-Tx)→EAV₁ wiretap link can enhance the performance of the SU by using our proposed power allocation policy.

The remainder of this paper is presented as follows. In Section II, the system model, assumptions, and problem statement for the SIMO CRN are introduced. In Section III, the upper bound, lower bound of the S-Tx transmission power, and the power allocation policy for the S-Tx are obtained. Further, closed-form expressions for the outage probability, probability of non-zero secrecy capacity, and outage secrecy capacity are derived. In Section IV, the numerical results and discussions are provided. Finally, conclusions are given in Section V.

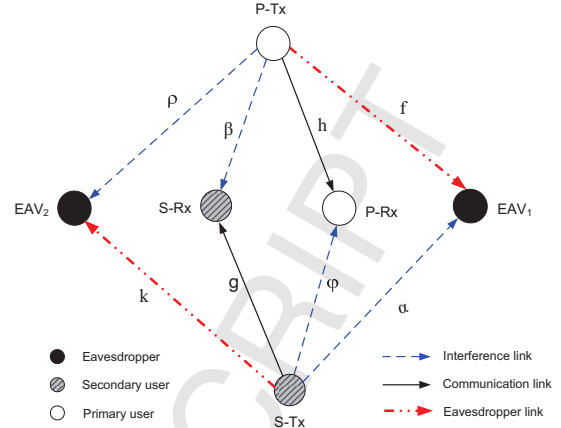


Fig. 1. A system model of underlay CRN in which the SU utilizes the licensed frequency band of the PU. The EAV₁ and EAV₂ illegitimately listen to the information of the P-Tx and S-Tx, respectively. The S-Tx and P-Tx have a single antenna while the S-Rx, P-Rx, EAV₁, and EAV₂ are equipped with N_s , N_p , N_{e1} , and N_{e2} antennas, respectively.

II. SYSTEM MODEL

In this section, we introduce the system model, channel assumptions, and spectrum sharing constraints.

A. System Model

Let us consider a spectrum underlay CRN as shown in Fig. 1 in which SUs (S-Tx and S-Rx) utilize the licensed frequency band of PUs (P-Tx and P-Rx) for their communication. There also exist two EAVs (namely as EAV₁ and EAV₂) who are capable of eavesdropping the messages by observing the channel outputs. In particular, the EAV₁ wants to overhear the message of the P-Tx while the EAV₂ tries to eavesdrop the message of the S-Tx. In this model, the S-Tx and P-Tx have a single antenna while the P-Rx, S-Rx, EAV₁, and EAV₂, are equipped with N_p , N_s , N_{e1} , and N_{e2} antennas, respectively. Note that the considered system model is applicable in practice where the P-Tx and S-Tx may act as mobile users of a primary network and a secondary network, respectively. The P-Rx and S-Rx are base stations or access points, the S-Tx→S-Rx and P-Tx→P-Rx links are uplinks [34]. In fact, the multiple devices can access the spectrum band, and their secure communication may be revealed in an unexpected manner due to **hidden eavesdroppers**. Therefore, the power allocation policy to protect the security communication of the PU become one of the most important problem.

B. Channel Model

As for the radio links between different users, we assume that channels are distributed following **Rayleigh blocked flat fading models**. This fading is widely used to model channels in urban environments where the dominant propagation along a line of sight between the transmitter and receiver is not dominated. Therefore, the channels are considered as constant during the transmission time of one message but they may change independently to different values thereafter.

Symbols	Meaning
N_s, N_p, N_{e1}, N_{e2}	Number of antennas at the secondary receiver (S-Rx), primary receiver (P-Rx), EAV ₁ , EAV ₂
$h = (h_1, h_2, \dots, h_{N_p})$	Channel gain of the P-Tx→P-Rx communication link
$g = (g_1, g_2, \dots, g_{N_s})$	Channel gain of the S-Tx→S-Rx communication link
$f = (f_1, f_2, \dots, f_{N_{e1}})$	Channel gain of the P-Tx→EAV ₁ illegitimate link
$k = (k_1, k_2, \dots, k_{N_{e2}})$	Channel gain of the S-Tx→EAV ₂ illegitimate link
$\beta = (\beta_1, \beta_2, \dots, \beta_{N_s})$	Channel gain of the P-Tx→S-Rx interference link
$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_{N_{e1}})$	Channel gain of the S-Tx→EAV ₁ interference link
$\rho = (\rho_1, \rho_2, \dots, \rho_{N_{e2}})$	Channel gain of the P-Tx→EAV ₂ interference link
$\varphi = (\varphi_1, \varphi_2, \dots, \varphi_{N_p})$	Channel gain of the S-Tx→P-Rx interference link
R_p, R_s	Target rates of the P-Tx and S-Tx
R_δ	Secrecy target rate of the P-Tx under the eavesdropping of EAV ₁
$\gamma_{SU}, \gamma_{PU}, \gamma_{e1}, \gamma_{e2}$	Signal-to-interference-plus-noise ratios (SINRs) of the S-Rx, P-Rx, EAV ₁ , and EAV ₂
θ, ϵ	Outage probability threshold and outage secrecy threshold of the PU
N_0	Noise power (a product of noise power spectral density (\mathcal{N}_0) and system bandwidth (B), i.e., $N_0 = B\mathcal{N}_0$)
P_{S-Tx}, P_{P-Tx}	Transmission power of the S-Tx, P-Tx
P_u, P_l	Upper bound and lower bound of the transmission power of the S-Tx
P_{S-Tx}^{\max}	Peak transmission power of the S-Tx
$\gamma_{P-Tx} = \frac{P_{P-Tx}}{N_0}$	Transmission SNR of the P-Tx
$\gamma_{S-Tx} = \frac{P_{S-Tx}}{N_0}$	Transmission SNR of the S-Tx
$\gamma_u = \frac{P_u}{N_0}$	Upper bound of the transmission SNR of the S-Tx
$\gamma_l = \frac{P_l}{N_0}$	Lower bound of the transmission SNR of the S-Tx

This assumption are inline with previous works [7], [16], [31], [35]–[37]. The channel gains, S-Tx→S-Rx and P-Tx→P-Rx of communication links, are denoted, respectively, by g_t and h_m . The channel gains of S-Tx→P-Rx, P-Tx→S-Rx, S-Tx→EAV₁, and P-Tx→EAV₂, interference links are denoted by φ_m , β_t , α_n , and ρ_ℓ , respectively. Moreover, the channel gains of P-Tx→EAV₁ and S-Tx→EAV₂ illegitimate links are expressed, respectively, by f_n and k_ℓ . Here, the symbols t, m, n, ℓ denote the antenna indexes of the S-Rx, P-Rx, EAV₁, and EAV₂, respectively where $t \in \{1, \dots, N_s\}$, $m \in \{1, \dots, N_p\}$, $n \in \{1, \dots, N_{e1}\}$, and $\ell \in \{1, \dots, N_{e2}\}$. Since the channel coefficients are modeled as Rayleigh blocked flat fading, the channel gains are random variables (RVs) distributed following exponential distribution, and the probability density function (PDF) and cumulative distribution function (CDF) are expressed, respectively, as

$$f_X(x) = \frac{1}{\Omega_X} \exp\left(-\frac{x}{\Omega_X}\right), \quad (1)$$

$$F_X(x) = 1 - \exp\left(-\frac{x}{\Omega_X}\right), \quad (2)$$

where RV $X \in \{g, h, f, \alpha, \varphi, \beta, k, \rho\}$, refers to the channel gain, and $\Omega_X = \mathbf{E}[X]$ is the channel mean gain.

In this paper, the P-Rx, S-Rx, EAV₁, and EAV₂, are assumed to use the **selection combining (SC)** to process the received signal, i.e., the antenna having the maximal SINR will be used to process the received message. This SC scheme is simple for the hardware design, since it would need only a measurement of signal power, while phase shifters or variable gains are not required. According to the Shannon's theorem, the channel capacity of the P-Tx→P-Rx link can be formulated as

$$C_{PU} = B \log_2(1 + \gamma_{PU}), \quad (3)$$

where B is the system bandwidth, and γ_{PU} is defined as

$$\gamma_{PU} = \max_{m \in \{1, 2, \dots, N_p\}} \left\{ \frac{P_{P-Tx} h_m}{P_{S-Tx} \varphi_m + N_0} \right\}, \quad (4)$$

where P_{P-Tx} and P_{S-Tx} are transmission powers of the P-Tx and S-Tx, respectively. Similarly, the channel capacity of the S-Tx→S-Rx link can be given as

$$C_{SU} = B \log_2(1 + \gamma_{SU}), \quad (5)$$

where

$$\gamma_{SU} = \max_{t \in \{1, 2, \dots, N_s\}} \left\{ \frac{P_{S-Tx} g_t}{P_{P-Tx} \beta_t + N_0} \right\}. \quad (6)$$

It is a fact that the SU and PU share the same spectrum, and hence the transmitted messages of the S-Tx and P-Tx for their corresponding S-Rx and P-Rx may be vulnerable due to broadcast nature of radio propagation and mutual interference. On the other hand, the EAVs may know this weakness and then two EAVs have been established to illegally exploit the output messages at the S-Tx and P-Tx over wiretap channels. The channel capacity of the P-Tx→EAV₁ and S-Tx→EAV₂ wiretap links are expressed, respectively, as

$$C_{e1} = B \log_2(1 + \gamma_{e1}), \quad (7)$$

$$C_{e2} = B \log_2(1 + \gamma_{e2}), \quad (8)$$

where SINRs at the EAV₁ and EAV₂ are expressed, respectively, as follows:

$$\gamma_{e1} = \max_{n \in \{1, 2, \dots, N_{e1}\}} \left\{ \frac{P_{P-Tx} f_n}{P_{S-Tx} \alpha_n + N_0} \right\}, \quad (9)$$

$$\gamma_{e2} = \max_{\ell \in \{1, 2, \dots, N_{e2}\}} \left\{ \frac{P_{S-Tx} k_\ell}{P_{P-Tx} \rho_\ell + N_0} \right\}. \quad (10)$$

C. Problem Statement

It is worth to remind that the SU utilizes the spectrum of the PU, and hence the SU should have a power control policy which does not only satisfy the secure and interference constraint of the PU but also can obtain a reasonable transmission power to maintain its own communication. On this basis, we consider the case that both SU and PU uses the Wyner's wiretap code [11] for their own communication. Theoretically,

the perfect security communication of the PU is difficult to achieve when $C_{e1} > R_\delta$, where R_δ is the secrecy target rate which is derived from a bin structure of the wiretap code design to control the leakage of information [38]. Accordingly, the secrecy outage probability of the PU under overhearing of the EAV₁ can be formulated as [35, Eq.(2)]

$$\mathcal{O}_{SEC} = \Pr \{C_{e1} > R_\delta\}, \quad (11)$$

where C_{e1} is the channel capacity of the P-Tx→EAV₁ link given in (7).

Moreover, due to the randomness of wireless channel, the reliable communication of the PU may not be achieved when the rate of code word transmission of the PU is greater than the channel capacity, i.e. $R_p > C_{PU}$. This is known as the communication outage event of the PU, defined by

$$\mathcal{O}_{PU} = \Pr \{R_p > C_{PU}\}. \quad (12)$$

Here, the parameters R_p and R_δ are fixed and chosen offline following [38]–[41].

D. SU Transmission Power Constraint

It is clear to see that if the SU does not have a reasonable transmission power, it may cause the PU information leakage to the EAV₁, or the SU transmission power can become a severe interference to the PU. Therefore, to against the EAV₁ and to protect the PU from the harmful interference, the SU should satisfy both the interference and security constraint of the PU, which can be interpreted into the following constraints:

$$\mathcal{O}_{PU} \leq \theta, \quad (13)$$

$$\mathcal{O}_{SEC} \leq \epsilon, \quad (14)$$

$$P_{S-Tx} \leq P_{S-Tx}^{max}, \quad (15)$$

where θ and ϵ are the communication outage threshold and secrecy outage threshold, respectively. P_{S-Tx}^{max} is maximal transmission power of the S-Tx. In other words, the S-Tx transmission power should keep the outage probability of the PU below a given threshold as in (13). In addition, the S-Tx must control its power to guarantee the security constraint of the PU given in (14). Finally, the S-Tx transmission power is often limited due to its peak transmission power, thus the S-Tx is subject to an additional constraint as given in (15).

Given above settings, optimal transmission power policy for the S-Tx is derived. Accordingly, the outage probability, probability of non-zero secrecy, and secrecy outage probability are investigated to evaluate the performance of the secondary system in the following section.

III. PERFORMANCE ANALYSIS

A. Transmission Power Allocation Policy

In this subsection, we first derive the upper bound and lower bound transmission power of the S-Tx, and then propose a power allocation policy for the S-Tx which is subject to the security constraint and outage probability constraint of the PU. Let us commence by considering a property as follows.

Property 1. Let a , b , and c be positive constants. Further, let X_i and Y_i be independent and exponentially distributed RVs

with mean values Ω_X and Ω_Y , respectively. Then, the RV U defined by

$$U = \max_{i \in \{1,2,\dots,N\}} \left(\frac{aX_i}{bY_i + c} \right) \quad (16)$$

has the CDF given by

$$\begin{aligned} F_U(u) &= \left[1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X}u + 1} \exp\left(-\frac{uc}{a\Omega_X}\right) \right]^N \\ &= \sum_{q=0}^N \binom{N}{q} \frac{(-1)^q}{(Au + 1)^q} \exp\left(-\frac{qu}{D}\right), \end{aligned} \quad (17)$$

where $A = \frac{b\Omega_Y}{a\Omega_X}$ and $\frac{1}{D} = \frac{c}{a\Omega_X}$.

Proof. We derive the CDF of U as follows:

$$\begin{aligned} F_U(u) &= \Pr \{U \leq u\} = \prod_{j=1}^N \Pr \left\{ \frac{aX_j}{bY_j + c} \leq u \right\} \\ &= \prod_{j=1}^N \int_0^\infty \Pr \left\{ X_j \leq \frac{u(by + c)}{a} \right\} f_{Y_j}(y) dy \\ &= \prod_{j=1}^N \int_0^\infty \left[1 - \exp\left(-\frac{u(by + c)}{a\Omega_X}\right) \right] \frac{1}{\Omega_Y} \exp\left(-\frac{y}{\Omega_Y}\right) dy \\ &= \left\{ 1 - \frac{1}{\Omega_Y} \exp\left(-\frac{uc}{a\Omega_X}\right) \right. \\ &\quad \times \left. \int_0^\infty \exp\left[-y \left(\frac{ub}{a\Omega_X} + \frac{1}{\Omega_Y} \right)\right] dy \right\}^N \\ &= \left[1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X}u + 1} \exp\left(-\frac{uc}{a\Omega_X}\right) \right]^N. \end{aligned} \quad (18)$$

By setting $A = \frac{b\Omega_Y}{a\Omega_X}$, $\frac{1}{D} = \frac{c}{a\Omega_X}$, and then using binomial expansion, we obtain the CDF of U as in (17). \square

It is a fact that the S-Tx must select a transmission power level such that it can exploit the licensed spectrum of the PU as much as possible but does not cause harmful interference to the P-Rx. Given the related constraints in (13), (14), and (15), a transmission power policy for the S-Tx is derived as follows.

Firstly, we can calculate the outage probability of the PU from (12), as follows

$$\mathcal{O}_{PU} = \Pr \left\{ \max_{m \in \{1,2,\dots,N_p\}} \left\{ \frac{P_{P-Tx} h_m}{P_{S-Tx} \varphi_m + N_0} \right\} \leq \gamma_{th}^{PU} \right\} \leq \theta, \quad (19)$$

where $\gamma_{th}^{PU} = 2^{\frac{R_p}{B}} - 1$. Using the help of (17) in *Property 1* for (19) by setting $a = P_{P-Tx}$, $b = P_{S-Tx}$, $c = N_0$, $\Omega_X = \Omega_h$, $\Omega_Y = \Omega_\varphi$, and $u = \gamma_{th}^{PU}$, a closed-form expression for the PU outage probability is obtained as

$$\mathcal{O}_{PU} = \left[1 - \frac{1}{\frac{P_{S-Tx} \Omega_\varphi}{P_{P-Tx} \Omega_h} \gamma_{th}^{PU} + 1} \exp\left(-\frac{\gamma_{th}^{PU} N_0}{P_{P-Tx} \Omega_h}\right) \right]^{N_p} \leq \theta. \quad (20)$$

After some manipulations, the transmission power of the S-Tx should satisfy following inequality

$$P_{S-Tx} \leq \frac{P_{P-Tx} \Omega_h}{\gamma_{th}^{PU} \Omega_\varphi} \Xi_1, \quad (21)$$

where Ξ_1 is defined as

$$\Xi_1 = \max \left\{ 0, \frac{1}{1 - N\sqrt{\theta}} \exp \left[-\frac{\gamma_{th}^{PU} N_0}{P_{P-Tx} \Omega_h} \right] - 1 \right\}. \quad (22)$$

Here, Ξ_1 in (22) is to indicate that the mathematical calculation for the second term could be negative in theory, but the S-Tx transmission power must be greater than or equal zero in the practice. Furthermore, the S-Tx transmission power is subject to its maximum transmission power, i.e., $P_{S-Tx} \leq P_{S-Tx}^{\max}$. Thus, the upper bound of the S-Tx transmission power, P_{up} , is calculated as follows:

$$P_{up} = \min \left\{ \frac{P_{P-Tx} \Omega_h}{\gamma_{th}^{PU} \Omega_\varphi} \Xi_1, P_{S-Tx}^{\max} \right\}. \quad (23)$$

Obviously, the S-Tx transmission power must be maintained below the upper bound given in (23) to not cause harmful interference to the PU, i.e., $P_{S-Tx} \leq P_{up}$.

Secondly, the S-Tx transmission power is subject to the secrecy constraint as given in (14), thus the derivations can be given as follows

$$\begin{aligned} \mathcal{O}_{SEC} &= 1 - \Pr \{ C_{e1} < R_\delta \} \leq \epsilon \\ &= \prod_{n=1}^{N_{e1}} \Pr \left\{ \frac{P_{P-Tx} f_n}{P_{S-Tx} \alpha_n + N_0} \leq \gamma_{th}^{e1} \right\} \geq 1 - \epsilon, \end{aligned} \quad (24)$$

where $\gamma_{th}^{e1} = 2^{\frac{R_\delta}{B}} - 1$. Similar to the derivations for the outage probability of the PU, we can obtain the maximum transmission power for the S-Tx under the secrecy constraint by using (17). In particular, by setting $a = P_{P-Tx}$, $b = P_{S-Tx}$, $c = N_0$, $\Omega_X = \Omega_f$, $\Omega_Y = \Omega_\alpha$, and $u = \gamma_{th}^{e1}$ for (24) yields

$$\left[1 - \frac{1}{\frac{P_{S-Tx} \Omega_\alpha}{P_{P-Tx} \Omega_f} \gamma_{th}^{e1} + 1} \exp \left(-\frac{\gamma_{th}^{e1} N_0}{P_{P-Tx} \Omega_f} \right) \right]^{N_{e1}} \geq 1 - \epsilon. \quad (25)$$

After some algebra manipulations, the transmission power for the S-Tx under the secrecy constraint is obtained as

$$P_{S-Tx} \geq P_{lo} = \frac{P_{P-Tx} \Omega_f}{\gamma_{th}^{e1} \Omega_\alpha} \Xi_2, \quad (26)$$

where P_{lo} is a lower bound which the S-Tx transmission power should be satisfied to protect the communication of the PU from the EAV₁. Symbol Ξ_2 is defined as

$$\Xi_2 = \max \left\{ 0, \frac{1}{1 - N\sqrt{1 - \epsilon}} \exp \left[-\frac{\gamma_{th}^{e1} N_0}{P_{P-Tx} \Omega_f} \right] - 1 \right\}. \quad (27)$$

Combining (23) and (26), we can easily see that the S-Tx transmission power should satisfy the following condition

$$P_{lo} \leq P_{S-Tx} \leq P_{up}. \quad (28)$$

It is worth to note that the P_{lo} and P_{up} are calculated on the basis of channel mean gains and other system parameters.

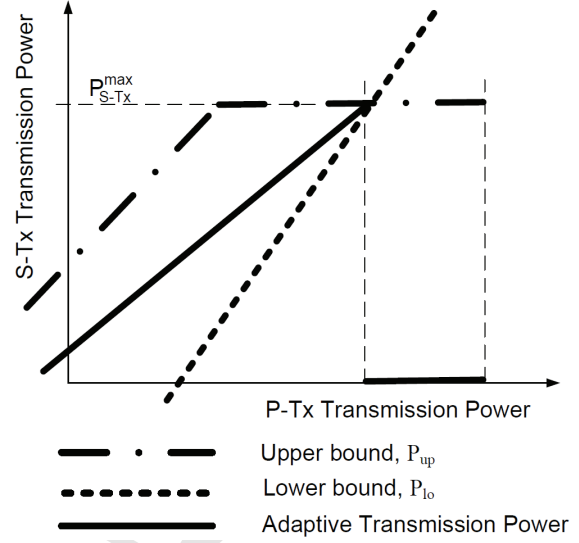


Fig. 2. An example of power allocation policy for the S-Tx versus the P-Tx transmission power.

Thus, depending on the channel state information (CSI) among the SU, PU, and EAVs, the value of P_{lo} may be greater than the one of P_{up} or vice versa. To assure that the S-Tx transmission power does not violate the QoS and security constraint of the PU, we consider the following cases:

- If $P_{lo} \leq P_{up}$, then the transmission power of the S-Tx should be controlled by a convex combination of the upper and lower bounds as $P_s = (1 - a)P_{lo} + aP_{up}$, $0 \leq a \leq 1$. This is because that the wireless channels are often fluctuated due to its natural randomness. Thus, if the transmission power of the S-Tx is too close to the upper bound, the S-Tx may cause seriously interference to the PU when the interference channel gain of the S-Tx→P-Rx link increases outburst. On the other hand, if the S-Tx's transmission power is too close to the lower bound, the S-Tx can not maintain the active noise to the EAV₁ when the interference channel gain of the S-Tx→EAV₁ link suddenly degrades. Thus, the power allocation scheme is adjusted flexibly on the basis value of the upper bound and lower bound, which can make a relative safe gap to guarantee the security communication and QoS of the PU. Note that if $a \rightarrow 1$ then $P_s \rightarrow P_{up}$, when $a \rightarrow 0$, $P_s \rightarrow P_{lo}$.
- If $P_{lo} > P_{up}$, then the S-Tx is not allowed to transmit, i.e., $P_s = 0$. This is due to the fact that the S-Tx transmission power firmly violates both the outage probability and security probability constraint of the PU.

As a result, the power allocation policy for the S-Tx is formulated as

$$P_s = \begin{cases} (1 - a)P_{lo} + aP_{up}, & \text{if } P_{lo} \leq P_{up} \\ 0, & \text{if } P_{lo} > P_{up} \end{cases}, \quad (29)$$

where $0 \leq a \leq 1$, P_{lo} and P_{up} are expressed, respectively, as

$$P_{lo} = \frac{P_{P-Tx} \Omega_f}{\gamma_{th}^{E_1} \Omega_\alpha} \Xi_2, \quad (30)$$

$$P_{up} = \min \left\{ \frac{P_{P-Tx} \Omega_h}{\gamma_{th}^{PU} \Omega_\varphi} \Xi_1, P_{S-Tx}^{\max} \right\}. \quad (31)$$

To make the power allocation policy of the S-Tx more clear, we show an example as in Fig. 2 where the solid line is the S-Tx power allocation policy given in (29).

B. Performance Analysis of Secondary User

In this subsection, we derive the outage probability and symbol error probability (SEP) of the SU to understand how the performance of the SU can be achieved under the interference and secrecy constraint of the PU.

1) *Outage probability*: The outage probability is defined as the probability that the channel capacity is less than or equal the rate of transmission code word.

$$\mathcal{O}_{SU} = \Pr \left\{ \max_{t \in \{1, 2, \dots, N_s\}} \left\{ \frac{P_s g_t}{P_{P-Tx} \beta_t + N_0} \right\} \leq \gamma_{th}^{SU} \right\}, \quad (32)$$

where $\gamma_{th}^{SU} = 2^{\frac{R_s}{B}} - 1$. Applying *Property 1* to (32) by setting $a = P_s$, $b = P_{P-Tx}$, $c = N_0$, $\Omega_X = \Omega_g$, $\Omega_Y = \Omega_\beta$, $u = \gamma_{th}^{SU}$, a closed-form expression for the outage probability of the SU is given as follows

$$\mathcal{O}_{SU} = \sum_{q=0}^{N_s} \binom{N_s}{q} \frac{(-1)^q}{(A_1 \gamma_{th}^{SU} + 1)^q} \exp \left(-\frac{q \gamma_{th}^{SU}}{D_1} \right), \quad (33)$$

where $A_1 = \frac{P_{P-Tx} \Omega_\beta}{P_s \Omega_g}$ and $\frac{1}{D_1} = \frac{N_0}{P_s \Omega_g}$.

C. Secrecy Performance of Secondary User

In this subsection, the secrecy performance of the SU in terms of the probability of non-zero secrecy capacity and outage secrecy capacity of the SU under the overhearing of the EAV₂ are investigated. According to the physical layer security concept [11], the secrecy capacity of the SU is formulated as

$$C_S = C_{SU} - C_{e_2} = B \log_2 \left(\frac{1 + \gamma_{SU}}{1 + \gamma_{e_2}} \right). \quad (34)$$

Here, we assume that the interference caused by the P-Tx to the S-Rx and the EAV₂ is much greater than the additive noise power, i.e., the S-Rx and EAV₂ stay close to the P-Tx. Therefore, the SINR of the SU and EAV₂ in (6) and (10) can be rewritten as

$$\gamma_{SU} \approx \tilde{\gamma}_{SU} = \max_{t \in \{1, 2, \dots, N_s\}} \left\{ \frac{g_t}{\beta_t} \right\} \frac{1}{\mathcal{A}}, \quad (35)$$

$$\gamma_{e_2} \approx \tilde{\gamma}_{e_2} = \max_{\ell \in \{1, 2, \dots, N_{e_2}\}} \left\{ \frac{k_\ell}{\rho_\ell} \right\} \frac{1}{\mathcal{A}}, \quad (36)$$

where $\frac{1}{\mathcal{A}} = \frac{P}{P_{P-Tx}}$. To investigate the secrecy performance of the SU further, we first consider the following random variable

$$Z = \frac{1 + \tilde{\gamma}_{SU}}{1 + \tilde{\gamma}_{e_2}}, \quad (37)$$

The CDF of Z can be derived as follows

$$F_Z(z) = \int_0^\infty \Pr \{ \tilde{\gamma}_{SU} \leq z(1+t) - 1 \} f_{\tilde{\gamma}_{e_2}}(t) dt. \quad (38)$$

Moreover, the CDF of $\tilde{\gamma}_{SU}$ can be calculated as follows

$$\begin{aligned} F_{\tilde{\gamma}_{SU}}(x) &= \Pr \left\{ \tilde{\gamma}_{SU} = \max_{t \in \{1, 2, \dots, N_s\}} \left\{ \frac{g_t}{\beta_t} \right\} \leq x \mathcal{A} \right\} \\ &= \prod_{t=1}^{N_s} \Pr \{ g_t \leq x y \mathcal{A} \} f_{\beta_t}(y) dy \\ &= \prod_{t=1}^{N_s} \left[1 - \frac{1}{\Omega_\beta} \int_0^\infty \exp \left[- \left(\frac{x \mathcal{A}}{\Omega_g} + \frac{1}{\Omega_\beta} \right) y \right] dy \right] \\ &= \left(1 - \frac{1}{x \mathcal{A} \Omega_\beta + 1} \right)^{N_s} = \sum_{n=0}^{N_s} \binom{N_s}{n} \frac{(-1)^n}{(x \mathcal{A} \Omega_\beta + 1)^n}. \end{aligned} \quad (39)$$

where $\Omega_\beta = \frac{\Omega_g}{\Omega_g}$.

Using the same approach for (39), we obtain the PDF and CDF of $\tilde{\gamma}_{e_2}$ as follows:

$$F_{\tilde{\gamma}_{e_2}}(y) = \left(1 - \frac{1}{y \mathcal{A} \Omega_\beta + 1} \right)^{N_{e_2}}, \quad (40)$$

$$\begin{aligned} f_{\tilde{\gamma}_{e_2}}(y) &= \frac{\partial F_{\tilde{\gamma}_{e_2}}(y)}{\partial y} \\ &= N_{e_2} \Omega_\beta \mathcal{A} \sum_{m=0}^{N_{e_2}-1} \binom{N_{e_2}-1}{m} \frac{(-1)^m}{(1 + \Omega_\beta \mathcal{A} y)^{m+2}}, \end{aligned} \quad (41)$$

where $\Omega_\beta = \frac{\Omega_g}{\Omega_g}$.

Substituting (41) and (39) into (38), we have

$$\begin{aligned} F_Z(z) &= \int_0^\infty F_{\tilde{\gamma}_{SU}}(z(1+t) - 1) f_{\tilde{\gamma}_{e_2}}(t) dt \\ &= \sum_{n=0}^{N_s} \sum_{m=0}^{N_{e_2}-1} \binom{N_s}{n} \binom{N_{e_2}-1}{m} \frac{(-1)^{n+m} N_{e_2} I}{\Omega_\beta^{m+1} (\Omega_\beta z)^n \mathcal{A}^{n+m}}, \end{aligned} \quad (42)$$

where I is given by

$$I = \int_0^\infty \frac{dt}{\left[t + \frac{(z-1) \mathcal{A} \Omega_\beta + 1}{z \mathcal{A} \Omega_\beta} \right]^n \left[t + \frac{1}{\mathcal{A} \Omega_\beta} \right]^{m+2}}. \quad (43)$$

Using the help of [42, Eq.(3.197.1)] for (43) yields

$$\begin{aligned} I &= (\mathcal{A} \Omega_\beta)^{m+2} \mathcal{B}(1, m+n+1) \left[\frac{(z-1) \mathcal{A} \Omega_\beta + 1}{z \mathcal{A} \Omega_\beta} \right]^{1-n} \\ &\times {}_2F_1 \left(m+2; 1; m+n+2; 1 - \frac{\Omega_\beta}{\Omega_\beta z} [(z-1) \mathcal{A} \Omega_\beta + 1] \right), \end{aligned} \quad (44)$$

where $\mathcal{B}(\cdot, \cdot)$ is Beta function and ${}_2F_1(\cdot; \cdot; \cdot; \cdot)$ is a Hypergeometric function.

Substituting (44) into (42), we finally obtain the CDF of Z after some manipulations as

$$F_Z(z) = \sum_{n=0}^{N_s} \sum_{m=0}^{N_{e2}-1} \binom{N_s}{n} \binom{N_{e2}-1}{m} \times {}_2F_1 \left(m+2; 1; m+n+2; 1 - \frac{\Omega_V [(z-1)\mathcal{A}\Omega_U + 1]}{\Omega_U z} \right) \times \frac{(-1)^{n+m} N_{e2} \Omega_V \mathcal{B}(1, m+n+1)}{\Omega_U z [(z-1)\mathcal{A}\Omega_U + 1]^{n-1}}. \quad (45)$$

1) *Probability of non-zero secrecy capacity*: According to the secrecy capacity definition, the non-zero secrecy capacity is formulated as

$$C_S = [C_{SU} - C_{e2}]^+ = B \log_2(Z). \quad (46)$$

and the probability of non-zero secrecy capacity of the SU is calculated by

$$\mathcal{O}_{non-zero} = \Pr\{C_S > 0\} = 1 - \Pr\{Z \leq 1\} = 1 - F_Z(1). \quad (47)$$

Using $F_Z(z)$ given in (45), we obtain the probability of non-zero secrecy capacity as follows

$$\mathcal{O}_{non-zero} = 1 - \sum_{n=0}^{N_s} \sum_{m=0}^{N_{e2}-1} \binom{N_s}{n} \binom{N_{e2}-1}{m} \times \frac{(-1)^{n+m} N_{e2} \Omega_V \mathcal{B}(1, m+n+1)}{\Omega_U} \times {}_2F_1 \left(m+2; 1; m+n+2; 1 - \frac{\Omega_V}{\Omega_U} \right). \quad (48)$$

2) *Secrecy outage probability*: Secrecy outage probability is defined as the probability that the secrecy capacity is smaller than a predefined threshold given as

$$\mathcal{O}_{SEC} = \Pr\{C_S < R_{e2}\} = F_Z(\gamma_{th}) = \sum_{n=0}^{N_s} \sum_{m=0}^{N_{e2}-1} \binom{N_s}{n} \binom{N_{e2}-1}{m} \times \frac{(-1)^{n+m} N_{e2} \Omega_V \mathcal{B}(1, m+n+1)}{\Omega_U \gamma_{th} [(\gamma_{th}-1)\mathcal{A}\Omega_U + 1]^{n-1}} \times {}_2F_1 \left(m+2; 1; m+n+2; 1 - \frac{\Omega_V [(\gamma_{th}-1)\mathcal{A}\Omega_U + 1]}{\Omega_U \gamma_{th}} \right), \quad (49)$$

where $\gamma_{th} = 2^{\frac{R_{e2}}{B}}$ and R_{e2} is the secrecy rate of the SU under the eavesdropping of the EAV₂ which can be chosen offline following [39]–[41].

IV. NUMERICAL RESULTS

In this section, analytical and simulation results for our considered system are presented. More specifically, we study the impact of the P-Tx transmission power and channel mean gains on the power allocation policy, outage probability, probability of non-zero secrecy capacity, and outage probability of secrecy capacity for the SU communication. Some channel mean gains are set to high values to indicate that these channels and their signals are much stronger than the others.

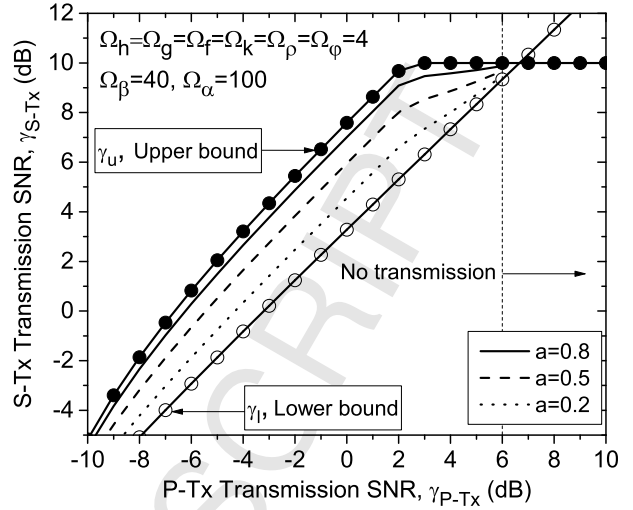


Fig. 3. The S-Tx transmission SNR versus the P-Tx transmission SNR with $N_s = N_p = 3$ and $N_{e1} = N_{e2} = 2$, and $R_{e2} = 1$ kbps;

Unless otherwise stated, the following system parameters are used for both analysis and simulation:

- System bandwidth: $B=1$ MHz;
- SU target rate: $R_s=64$ kbps;
- PU target rate: $R_p=64$ kbps
- The secrecy target rate of the P-Tx: $R_\rho=63$ kbps;
- Outage probability threshold of the PU: $\theta=0.01$;
- Outage secrecy threshold of the PU: $\epsilon=0.5$;
- Maximum the S-Tx transmission SNR: $\gamma_{S-Tx}^{\max} = 10$ dB;

In Fig. 3, we plot the transmission SNR of the S-Tx as a function of the P-Tx transmission SNR with the values of $a = 0.2, 0.5, 0.8$. We can see that the curves of proposed transmission SNR scheme of the S-Tx are always below the upper bound and above the lower bound of the S-Tx. Also, the S-Tx transmission SNR first increases according to the increasing of the P-Tx transmission SNR. However, it starts saturating at $\gamma_{S-Tx} = 10$ dB. This is due to the fact that the S-Tx can adjust its transmission SNR according to the change of the P-Tx transmission SNR. However, the S-Tx transmission SNR is restricted by the peak transmission SNR of the S-Tx, γ_{S-Tx}^{\max} . Thus, when the channel conditions and system parameters are good for the S-Tx communication, the S-Tx transmission SNR can reach the peak value. This is suitable with the expression (23) and arguments for Fig. 2. Most importantly, we can see that the S-Tx stops its transmission when the P-Tx transmission SNR above 6 dB, i.e. $\gamma_{P-Tx} \geq 6$ dB to not degrade the performance of the PU from the SU interference. This observation confirms the predictions for the proposed power allocation policy as shown in Fig. 2.

In Fig. 4, the outage probability is presented as a function of the P-Tx transmission SNR with various values of a . We can see that by adjusting a value from 0.2 to 0.8, the outage performance of the SU is improved significantly, i.e., the outage probability is degraded. Further, the performance of the SU is the best (the worst) when the adjusting parameter

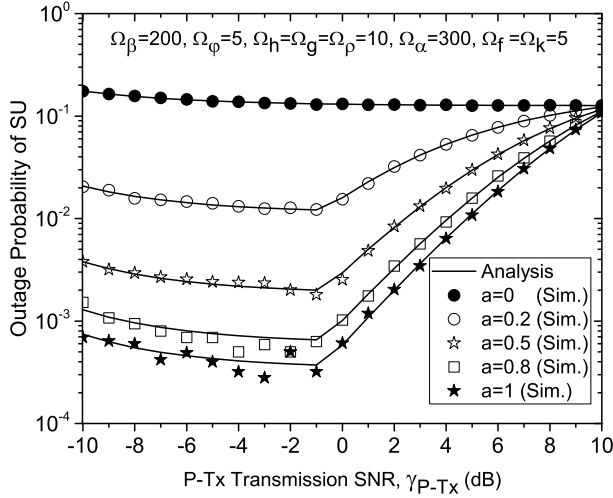


Fig. 4. Outage probability of the SU versus the P-Tx transmission SNR for $a = 0.2, 0.5, 0.8$, and $R_{e2} = 1$ kbps.

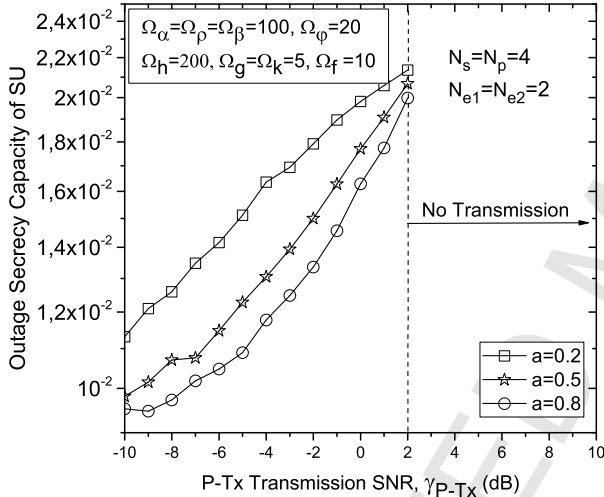


Fig. 5. Outage secrecy capacity of the SU versus the P-Tx transmission SNR for $a = 0.2, 0.5, 0.8$, and $R_{e2} = 64$ kbps.

of the S-Tx is set to $a = 1$ ($a = 0$), i.e. the upper bound (lower bound) of the S-Tx's transmission power. This results are matched well with discussions for the power allocation policy given in Fig. 3. We also observe the outage secrecy capacity of the SU as a function of the P-Tx's transmission SNR as shown in Fig. 5. It can be seen that the outage secrecy capacity increases as the P-Tx's transmission SNR increases. However, the S-Tx must stop its transmission at $\gamma_{P-Tx} = 2$ dB to not cause either harmful interference of the P-Rx or leak the information communication of the PU to the EAV₁. This result is suitable with the predictions given in Fig. 2 and Fig. 3.

Fig. 6 plots the outage probability as a function of the P-Tx's transmission SNR for different channel mean gains and

consider following four cases:

- *Case 1*: It is considered as a reference case where the channel mean gains of the S-Tx→P-Rx P-Tx→S-Rx interference links are set as $\Omega_\beta = 300$ and $\Omega_\varphi = 10$.
- *Case 2*: The channel mean gains of the S-Tx→P-Rx and P-Tx→S-Rx interference links are weaker than the ones of *Case 1*. In other words, the S-Tx and P-Tx stay far away from the P-Rx and S-Rx, respectively.
- *Case 3*: The channel mean gains of the S-Tx→P-Rx and P-Tx→S-Rx interference links are stronger than the ones of *Case 1*.
- *Case 4*: The channel mean gains of the S-Tx→P-Rx and P-Tx→S-Rx interference links are similar to the ones of *Case 3*. However, the number antennas at the P-Rx and S-Rx are greater than the ones of *Case 3*.

As can be clearly seen from the Fig. 6, the simulation and analysis match well for all cases. In all cases, the outage probability is first decreased in the low regime of the P-Tx transmission SNR, ($\gamma_{P-Tx} < -1$ dB) and then increases in the high regime of the P-Tx transmission SNR. In particular, for *Case 2*, the outage probability is slightly decreased to an optimal point $\gamma_{P-Tx} = 2$ dB, and it is increased for $\gamma_{P-Tx} > 2$ dB. These results are because that the P-Tx does not cause much interference to the S-Rx. Thus, the S-Tx can regulate its transmission power in the low regime transmission power of the P-Tx transmission SNR as shown in (29). Nonetheless, in the high regime of the P-Tx transmission SNR, the S-Tx can not control its transmission SNR further since it is subject to its maximum value, i.e. $\gamma_{S-Tx}^{\max} = 10$ dB. Consequently, any increasing the transmission SNR of the P-Tx leads to additional interference to the S-Rx which results in the increasing of the SU outage probability. On the other hand, in *Case 2*, the outage probability is smaller than the *Case 1*. This is due to the fact that the channel mean gains of interference links in *Case 2* are smaller than the one in *Case 1*.

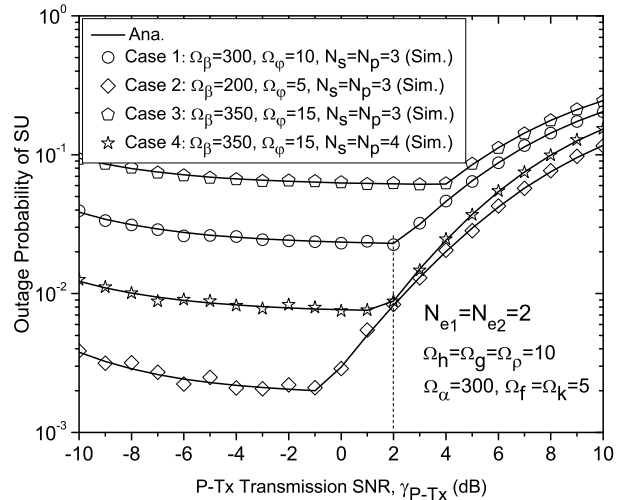


Fig. 6. The SU outage probability versus the P-Tx transmission SNR for $a = 0.5$, $\gamma_{P-Tx}^{\max} = 5$ dB, and $R_{e2} = 1$ kbps.

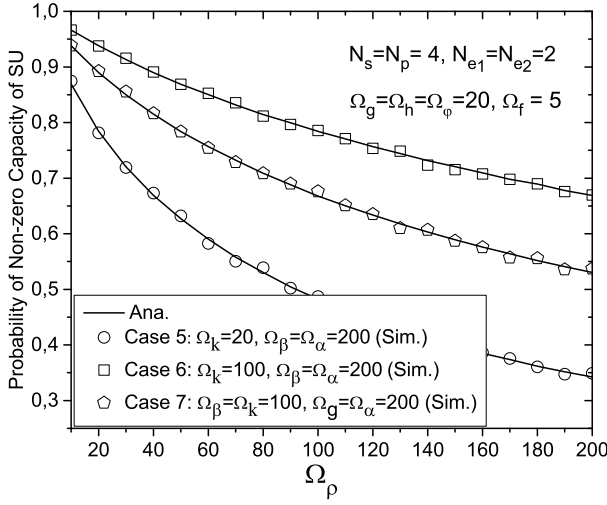


Fig. 7. Probability of non-zero secrecy capacity of the SU versus the channel mean gain of the P-Tx→EAV₂ interference link with $a = 0.5$, and $R_{e2} = 1$ kbps.

1, and then users in primary and secondary network cause low interference to each other, thus the outage performance of the SU in Case 2 is improved. Also, we have similar observations to compare the outage performance between the Case 3 and Case 1. Clearly, the outage probability of Case 3 is worse than the one of Case 1 because the channel mean gains of the interference links between primary and secondary network in Case 3 are stronger than the ones of Case 1. Finally, we observe the impact of antennas on the outage performance of SU by compare Case 4 with Case 3. It is easy to see that the outage probability of Case 4 is better than the Case 3 as the diversity in received signal increases as the number of antennas increases. In other words, if the number of antennas at the S-Rx and P-Rx increases and the mutual interference between the SU and PU is small, then the outage performance is improved significantly.

In Fig. 7, the probability of non-zero secrecy capacity of the SU is plotted as a function of the channel mean gain of the P-Tx→EAV₂ interference link, Ω_p , for different cases as follows:

- Case 5: This is set as a reference case with $\Omega_k = 20$, $\Omega_\beta = \Omega_\alpha = 200$.
- Case 6: The channel mean gain of the S-Tx→EAV₂ illegitimate link is higher than the one in Case 5, i.e., $\Omega_k = 100$.
- Case 7: The channel mean gain of the P-Tx→S-Rx interference link is decreased when it is compared to Case 6, i.e. $\Omega_\beta = 100$ and the channel mean gain of the S-Tx→S-Rx communication link increases when it is compared to Case 6.

It is clear to see that the probability of non-zero secrecy capacity is improved as the channel mean gain of the P-Tx→EAV₂ interference link increases for all cases. It is due to the reason that the EAV₂ suffers more interference from the P-Tx as the channel mean gain of the P-Tx→EAV₂ interference

link increases. Accordingly, the EAV₂ is difficult to overhear the information of the S-Tx, thus the probability of non-zero secrecy capacity is increased. By comparing Case 5 with Case 6, we can see that the probability of non-zero secrecy is degraded significantly when the channel mean gain of the S-Tx→EAV₂ illegitimate link, Ω_k , increases. This is because that the EAV₂ can improve its overhearing information when the illegitimate link is in a good condition for the EAV₂. However, when the channel mean gain of the P-Tx→S-Rx interference link is the bad condition (compare Case 7 with Case 6), the probability of non-zero secrecy capacity is improved significantly. It can be explained by a fact that the lower channel mean gain of the interference link P-Tx→S-Rx lead to the higher SINR at the S-Rx, i.e., the probability of non-zero secrecy capacity is enhanced.

Finally, we examine the impact of channel mean gain on the outage secrecy capacity as shown in Fig. 8. In particular, we consider Case 8 as a reference case and then compare it with other cases as follows. We can observe from figure that the outage secrecy capacity of the SU is increased gradually as the channel mean gain of the S-Tx→EAV₂ illegitimate link increases. It means that the **security of the SU communication is degraded when the illegitimate link is in good condition** for the EAV₂. We now compare Case 9 with Case 8 and see that the secrecy outage probability is improved significantly when the channel mean gain of the S-Tx→S-Rx communication link increases, i.e., $\Omega_g = 20$ to $\Omega_g = 200$. This is reasonable since the capacity of the SU in the main channel is improved significantly, which makes the improvement of the secrecy capacity as shown in (34). In addition, we compare Case 10 with Case 9 by decreasing the $\Omega_p = 200$ to $\Omega_p = 100$ and then observe the impact of channel mean gain of the P-Tx→EAV₂ interference link on the outage secrecy capacity. It is easy to see that low interference from the P-Tx to the EAV₂ leads to

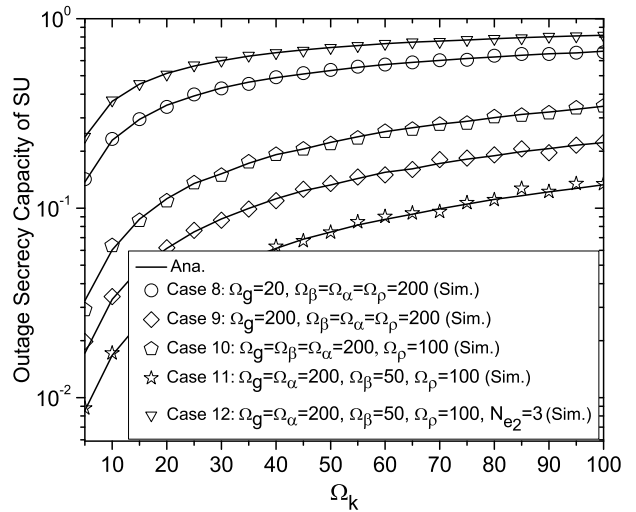


Fig. 8. Outage secrecy of the SU is plotted as a function of the channel mean gain of the S-Tx→EAV₂ illegitimate link with $a = 0.5$, $N_s = N_p = 4$, $N_{e1} = N_{e2} = 2$, $\Omega_h = \Omega_\varphi = 20$, and $\Omega_f = 5$, and $R_{e2} = 1$ kbps.

a high capacity at the EAV_2 , i.e., the outage secrecy capacity in *Case 10* is worse than the one in *Case 9*. Also, we can see that the outage secrecy capacity is improved significantly when the channel mean gain of the P-Tx→S-Rx interference link decreased from $\Omega_\beta = 200$ in *Case 10* to $\Omega_\beta = 200$ in *Case 11*. Especially, *Case 12* becomes the worse cases for the security of the SU when the EAV_2 increases only one antenna ($N_{e_2} = 3$).

V. CONCLUSIONS

In this paper, we have proposed a power allocation policy for the SU in the CRN. The S-Tx is subject to the security constraint and outage probability constraint of the PU, and the peak transmission power constraint of the S-Tx. Moreover, the performance analysis in terms of outage probability, SEP, probability of non-zero secrecy capacity, and outage secrecy capacity for the secondary network has been investigated. Further, the strong channel mean gain of the S-Tx→EAV₂ wiretap link leads to degrade the security of the secondary network. Most interestingly, our results show that the system performance of the SU is not degraded when the channel mean gain of the P-Tx→EAV₁ wiretap link is strong. Oppositely, it can be improved by using our proposed power allocation policy. Finally, the simulations have been provided to validate our analytical results.

ACKNOWLEDGEMENT


The research leading to these results has been performed at University of Québec, ETS engineering school, LACIME Laboratory, Montreal, Canada, and School of Innovation, Design and Engineering, Mälardalen University, Sweden. Dr Hung Tran is partially supported by the SafeCOP-project, with funding from the European Commission and Vinnova under ECSEL Joint Undertaking grant agreement n0692529. Dr Louis Sibomana is supported by the University of Rwanda (UR), Sweden Programme for Research, Higher Education and Institution Advancement under the Swedish International Development Agency (SIDA).

REFERENCES

- [1] FCC, "Promoting more efficient use of spectrum through dynamic spectrum use technologies," Federal Communication Commission (FCC 10-198), Washington DC, Tech. Rep. 10-237, Nov. 2010.
- [2] H. Tran, "Performance analysis of cognitive radio networks with interference constraints," Thesis, Blekinge Institute of Technology, 371-79 Karlskrona, Sweden, Mar. 2013.
- [3] B. Wang and K. Liu, "Advances in cognitive radio networks: A survey," *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 5–23, Feb. 2011.
- [4] R. Zhang, "On active learning and supervised transmission of spectrum sharing based cognitive radios by exploiting hidden primary radio feedback," *IEEE Trans. Commun.*, vol. 58, no. 10, pp. 2960–2970, Oct. 2010.
- [5] S. Stotas and A. Nallanathan, "Optimal sensing time and power allocation in multiband cognitive radio networks," *IEEE Trans. Commun.*, vol. 59, no. 1, pp. 226–235, Jan. 2011.
- [6] R. Tandra, A. Sahai, and S. Mishra, "What is a spectrum hole and what does it take to recognize one?" *Proc. IEEE*, vol. 97, no. 5, pp. 824–848, May 2009.
- [7] H. A. Suraweera, P. J. Smith, and M. Shafi, "Capacity limits and performance analysis of cognitive radio with imperfect channel knowledge," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 1811–1822, May 2010.
- [8] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.
- [9] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 471–487, Feb. 2007.
- [10] H. Tran, M. A. Hagos, M. Mohamed, and H.-J. Zepernick, "Impact of primary networks on the performance of secondary networks," in *Proc. International Conference on Computing, Management and Telecommunications*, Ho Chi Minh City, Vietnam, Jan. 2013, pp. 43–48.
- [11] A. D. Wayner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [12] C. Mitrpan, A. Vinck, and Y. Luo, "An achievable region for the gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.
- [13] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
- [14] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Proc. International Conference on Game Theory for Networks*, Istanbul, Turkey, May 2009, pp. 287–294.
- [15] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, Sep. 2011.
- [16] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.
- [17] J. Yue, C. Ma, H. Yu, Z. Yang, and X. Gan, "Secrecy-based channel assignment for device-to-device communication: An auction approach," in *Proc. International Conference on Wireless Communications Signal Processing*, Hangzhou, China, Oct. 2013, pp. 1–6.
- [18] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *IEEE Proc. International Symposium on Information Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.
- [19] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE Proc. International Symposium on Information Theory*, Jul. 2006, pp. 356–360.
- [20] Y. Liang and H. Poor, "Generalized multiple access channels with confidential messages," in *IEEE Proc. International Symposium on Information Theory*, Seattle, Washington, U.S.A., Jul. 2006, pp. 952–956.
- [21] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
- [22] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [23] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.
- [24] Y. Pei, Y.-C. Liang, L. Zhang, K. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.
- [25] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.
- [26] 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.
- [27] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Comm.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.
- [28] T. Kwon, V. Wong, and R. Schober, "Secure MISO cognitive radio system with perfect and imperfect CSI," in *Proc. IEEE Global Communications Conference*, U.S.A., Dec. 2012.
- [29] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.
- [30] 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.
- [31] 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.

- [32] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.
- [33] L. Sibomana, H. Tran, and Q. A. Tran, "Impact of secondary user communication on security communication of primary user," *Security and Communication Networks*, vol. 10.1002/sec.1333, Aug. 2015.
- [34] S. Al-Rubaye, A. Al-Dulaimi, and J. Cosmas, "Cognitive femtocell," *IEEE Veh. Technol. Mag.*, vol. 6, no. 1, pp. 44–51, Mar. 2011.
- [35] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. PP, no. 99, pp. 1–1, 2015.
- [36] Y. Liu, L. Wang, T. T. Duy, M. ElKashlan, and T. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wirel. Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.
- [37] T. T. Duy, T. Duong, T. L. Thanh, and V. N. Q. Bao, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Comm.*, vol. 9, no. 11, pp. 1427–1435, Jul. 2015.
- [38] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.
- [39] X. Zhou, M. McKay, B. Maham, and A. Hjrungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
- [40] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "On the throughput of secure hybrid-arq protocols for gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.
- [41] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *arXiv preprint arXiv:1412.0349*, 2014.
- [42] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Elsevier, 2007.

No	Author name	Biography	Picture
1	<p>Hung Tran Email: tran.hung@mdh.se</p>	<p>Hung Tran was born in Hanoi Capital, Vietnam, in 1980. He received his BS degree and MS degree in Information Technology from the Vietnam National University, Hanoi, Vietnam, in 2002 and 2006, respectively. He received the Ph.D. degree in March 2013 from the School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden. In 2014, he joined Electrical Engineering Department, ETS, Montreal, Canada. He is currently a postdoctoral researcher at the Mälardalen University, Sweden. His research interests are in the areas of wireless communications, cognitive radio networks, and green cooperative communication systems.</p>	
2	<p>Georges Kaddoum Email: georges.kaddoum@etsmtl.ca</p>	<p>Georges Kaddoum received the B.Sc. degree in electrical engineering from the École Nationale Supérieure de Techniques Avancées de Bretagne, Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne, Brest, in 2005, and the Ph.D. degree (with honors) in signal processing and telecommunications from the University of Toulouse, Toulouse, France, in 2008. He is currently an Assistant Professor of electrical</p>	

		<p>engineering at the École de Technologie Supérieure (ETS), University of Quebec, Montreal, QC, Canada. From September 2009 to October 2012, he served as a Postdoctoral Fellow at the Laboratoire de Communication et d'Intégration de la Microélectronique (LACIME), ETS. He was recognized as an Institutional Researcher in 2012 and then promoted to Assistant Professor in November 2013. He has published over 50 journal and conference papers and held two pending patents. He currently serves on the Editorial Board of the CIP Journal Wireless Communications and Networking. He is also a Scientific Consultant in the field of space telecommunications for Intelcan Technosystems and MDA Corporation. His recent research activities cover wireless communication systems, chaotic modulations, secure transmissions, and space communications and navigation.</p>	
3	<p>Email: Francois.Gagnon@etsmtl.ca</p>	<p>Francois Gagnon (SM'99) received the B.Eng. and Ph.D. degrees in electrical engineering from Ecole Polytechnique de Montréal, Montréal, QC, Canada. Since 1991, he has been a Professor with the Department of Electrical Engineering, École de Technologie Supérieure, Montreal. He Chaired the department from 1999 to 2001 and is currently the holder of</p>	

		<p>the NSERC Ultra Electronics Chair, Wireless Emergency and Tactical Communication, at the same university. His research interests include wireless high-speed communications, modulation, coding, high-speed DSP implementations, and military point-to-point communications.</p> <p>He has been very involved in the creation of the new generation of high-capacity line-of-sight military radios offered by the Canadian Marconi Corporation, which is now ultra electronics tactical communication systems.</p>	
4	<p>Louis Sibomana Email: lsmb@bth.se</p>	<p>Louis Sibomana received the B.S. and M.S. degrees in telecommunication engineering from the National University of Rwanda, Butare, Rwanda, in 2005 and 2008, respectively. He is currently working toward the Ph.D. degree with the Radio Communications Group, Blekinge Institute of Technology, Karlskrona, Sweden. From May 2008 to June 2011, he was a Network Performance Analyst and Optimization and Planning Engineer with</p>	

		<p>Rwandatel: a telecommunication company in Rwanda. Since July 2011, he has been an Assistant Lecturer with the Department of Electrical and Electronic Engineering, National University of Rwanda. His research interests include performance analysis of wireless communication systems, cooperative communications, cognitive radio networks, and physical-layer security in wireless networks.</p>	
--	--	---	--