

# Power allocation policy and performance analysis of secure and reliable communication in cognitive radio networks

Truong Xuan Quach<sup>1,2</sup> · Hung Tran<sup>3</sup> · Elisabeth Uhlemann<sup>3</sup> · George Kaddoum<sup>4</sup> · Quang Anh Tran<sup>5</sup>

Published online: 9 November 2017

© The Author(s) 2017. This article is an open access publication

**Abstract** This paper investigates the problem of secure and reliable communications for cognitive radio networks. More specifically, we consider a single input multiple output cognitive model where the secondary user (SU) faces an eavesdropping attack while being subject to the normal interference constraint imposed by the primary user (PU). Thus, the SU must have a suitable power allocation policy which does not only satisfy the constraints of the PU but also the security constraints such that it obtains a reasonable performance for the SU, without exposing information to the eavesdropper. We derive four power allocation policies for different scenarios corresponding to whether or not the channel state information of the PU and

the eavesdropper are available at the SU. Further, we introduce the concept secure and reliable communication probability (SRCP) as a performance metric to evaluate the considered system, as well as the efficiency of the four power allocation policies. Finally, we present numerical examples to illustrate the power allocation policies, and the impact of these policies on the SRCP of the SU.

**Keywords** Secure and reliable communication · Physical layer security · Power allocation · Cognitive radio networks · Spectrum underlay networks · Performance analysis

---

✉ Hung Tran  
tran.hung@mdh.se

Truong Xuan Quach  
qxtruong@ictu.edu.vn

Elisabeth Uhlemann  
elisabeth.uhlemann@mdh.se

George Kaddoum  
georges.kaddoum@etsmtl.ca

Quang Anh Tran  
tqanh@ptit.edu.vn

- <sup>1</sup> TNU - University of Information and Communication Technology, Thai Nguyen, Vietnam
- <sup>2</sup> VNU University of Engineering and Technology, Hanoi, Vietnam
- <sup>3</sup> School of Innovation, Design, and Engineering, Malardalen University, Västerås, Sweden
- <sup>4</sup> LACIME Laboratory, ETS Engineering School, University of Québec, Montreal, Canada
- <sup>5</sup> Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

## 1 Introduction

A cognitive radio network (CRN) is widely known as a promising solution to enhance spectrum utilization by means of dynamic spectrum access techniques [1–10]. In a CRN, there are two types of users known as primary user (PU) and secondary user (SU), where the (SU) is allowed to access the spectrum licensed to the (PU) as long as it does not degrade the performance of the (PU). Due to this, the (SU) must be equipped with advanced sensing techniques to detect vacant spectrum (known as a spectrum hole) and the channel state information (CSI) of the PU [6, 11]. This, in turn, implies that the  $PU_s$  and  $SU_s$  may be exposed to internal or external attackers who pretend to be sensing devices [12–14]. Furthermore, malicious attackers can abuse the adaptive abilities of the (CRN) causing negative effects to the radio environment, e.g., by generating interference, which may degrade the performance, reveal the secret communication information, or even cause malfunction to the operations of the legitimate users. Clearly, secure and reliable communication between  $SU_s$

can be obtained only if neither the secrecy nor the reliable communication outage events happen. Therefore, solving the security problems from all aspects of the networking architecture becomes one of the most challenging problems with CRN [13, 15].

Recently, physical layer security has emerged as an effective approach to protect the communication of legitimate users from eavesdropping attacks, by e.g., using the characteristics of wireless channels such as multipath fading [16–18]. It has been proven that if the channel from the source to the destination is better than the one from the source to the eavesdropper, the communication of the legitimate users can be secure and reliable at a non-zero data rate [19]. To quantify the security performance more specifically, Wyner has introduced a secrecy capacity concept [16] which is defined as the difference between the capacity of the main channel and the illegitimate channel. Later on, the secrecy capacity concept was extended to include wireless channels, e.g., Gaussian and multipath fading [17, 20]. It revealed that the secrecy capacity may be reduced due to the effect of multipath fading in wireless channels.

Motivated by all the above works and the references therein, in this paper, we evaluate secure and reliable communication for a single-input multiple-output (SIMO) CRN. More specifically, we assume that the secondary transmitter (STx) and the primary transmitter (P-Tx) are equipped with a single antenna, while the primary receiver (P-Rx), secondary receiver (S-Rx), and the eavesdropper (EAV) have multiple antennas. This system model is considered as an instance of a practical scenario where the P-Tx and S-Tx may be wireless sensors or mobile users, while the P-Rx and S-Rx may be access points or base stations. Here, the EAV tries to overhear the information transmitted by the S-Tx. Thus, the S-Tx must have flexible power control policies to protect its secret information, and not cause harmful interference to the PU. Accordingly, a performance metric in terms of secure and reliable communication probability is introduced to evaluate the considered CRN performance. Our major contributions in this paper are summarised as follows:

- Based on the CSI available at the S-Tx, power allocation policies are derived for four scenarios as follows. *Scenario 1* ( $S_1$ ): The S-Tx does not have the CSI of both the P-Tx→P-Rx and the S-Tx→EAV links; *Scenario 2* ( $S_2$ ): The S-Tx has the CSI of the S-Tx→EAV but not the P-Tx→P-Rx link; *Scenario 3* ( $S_3$ ): The S-Tx has the CSI of the P-Tx→P-Rx but not the S-Tx→EAV links; *Scenario 4* ( $S_4$ ): The S-Tx has the CSI of both the P-Tx→P-Rx and the S-Tx→EAV links. Accordingly, a power allocation algorithm corresponding to the four scenarios is introduced.

- Given the four power allocation policies, the the secure and reliable communication probability (SRCP) is introduced to analyse the performance of the considered CRN.
- Our numerical results show that the SRCP of *Scenario 1* and *Scenario 2* (*Scenario 3* and *Scenario 4*) are only different in the low signal-to-noise ratio (SNR) regime of the P-Tx, but they are the same in the high SNR regime of the P-Tx.

To the best of the authors' knowledge, there are no previous publications addressing this problem.

The remainder of this paper is organized as follows. The related work is introduced in Sect. 2, whereas in Sect. 3 the system model, assumptions, constraints corresponding to four scenarios for the CSI at the S-Tx together with problem statement for a SIMO CRN are introduced. In Sect. 4, power allocation policies corresponding to four scenarios are obtained. Further, a closed-form expression for the SRCP is derived. In Sect. 5, the numerical results and discussions are provided. Finally, conclusions are given in Sect. 6.

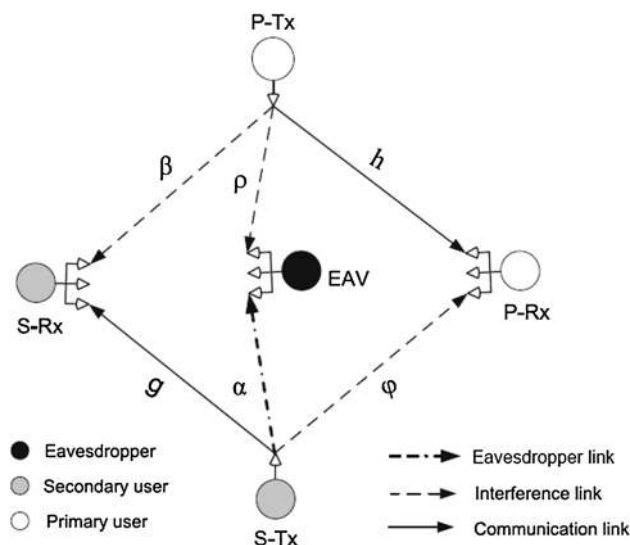
## 2 Related work

The general security performance of the CRN has been studied in [15, 21–23]. More specifically, in [15], the authors studied the primary user emulation (PUE) attack and proposed a solution to reduce the PUE attack in CRN operating in the frequency digital TV (DTV) band. This approach can effectively mitigate PUE attacks with the addition of a plugin AES chip to the system hardware. In [24], a robust Markov decision process for secure power control schemes of cognitive radios was proposed. In [25], the ergodic secrecy capacity for a CRN under the effects of fast fading channels has been analyzed. More recently, communication protocols and signal processing techniques was proposed to enhance the secrecy performance of the CRN in [13, 26–30]. In [30], an optimal relay selection scheme to minimize the secrecy outage probability of the cognitive cooperative radio network (CCRN) with decode-and-forward (DF) relays was investigated. In [31], a performance analysis in terms of average secrecy capacity with a CCRN having multiple reactive DF relays was studied, and the obtained results showed that using relay networks can enhance the secrecy performance. Taking advantage of multi-antenna techniques, beamforming and cooperative jamming techniques for CRNs was studied in [26–28, 32, 33]. Considering the security for multiple users in the CRNs, a scheduling scheme to enhance the security of communication was proposed in [29]. In [34] and [35], game theory cooperation strategies have been applied to

investigate the security for a CRN scenario. Bandwidth assignment strategies and power allocation policies have been proposed to enhance the security of the PU communication. In [27], two secure transmission schemes, termed nonadaptive and adaptive secure transmission strategy, were developed to maximize the throughput for a multiple-input single-out (MISO) CRN over a slow fading channel. An approximation for the optimal rate parameters of the nonadaptive secure transmission strategy was achieved at the high SNR regime. In [36], the impact of secondary user communication on the security of the primary user have been studied. The results showed that the security of the primary network strongly depends on the channel condition of the SU transmitter to the EAV link and the transmit power policy of the S-Tx. Most recently, subject to the maximal tolerable interference threshold of the PU, the secrecy outage probability has been evaluated for various scheduling schemes in [22], in which the S-Tx is overheard by multiple EAV<sub>v</sub>. However, the impact of the P-Tx→P-Rx link on the secure performance has not been considered. In [37], the authors have analyzed the intercept behavior of industrial wireless sensor networks with different scheduling schemes. However, this study is only for conventional wireless sensor networks, and thus the security and reliable criteria have not been considered. Up to now, the performance analysis for the physical layer security of CRN<sub>s</sub>, in terms of non-zero secrecy capacity, probability of outage secrecy capacity, and ergodic secrecy capacity, have obtained great achievements [22, 27, 33, 37–39]. However, not many publications investigate the performance analysis in terms of reliable and security communication, which is considered as one of the most important criteria in the industry and internet of things (IoT) era.

### 3 System model

Let us consider a system model as shown in Fig. 1 in which there are three types of user in the same area, termed the SU, PU, and EAV. The PU allows the SU to re-utilize its licensed spectrum provided that the SU does not cause harmful interference to the PU. On the other hand, the EAV wants to eavesdrop the information of the su’s communication over a wiretap channel. In fact, the EAV can overhear the information of both the S-Tx and P-Tx, but in this system model the EAV wants to utilize the interference from the P-Tx to exploit the exchange of information from the SU. Here, we assume that the S-Tx and P-Tx are equipped with a single antenna while the S-Rx, P-Rx, and EAV have  $N_s$ ,  $N_p$ , and  $N_e$  antennas, respectively. This system model is considered as an instance of practical scenario where the P-Tx and S-Tx may be mobile users



**Fig. 1** A system model of CRN in which the SU utilizes the licensed frequency band of the PU. The EAV overhears the information of the S-Tx. The S-Tx and P-Tx are equipped with a single antenna while the S-Rx, P-Rx, and EAV have  $N_s$ ,  $N_p$ , and  $N_e$  antennas, respectively

while the P-Rx and S-Rx are base stations or access points. Note that the PU can transmit with an optional power level for its communication without caring about the existence of the SU. On the other hand, the SU should keep the interference inflicted onto the PU below a predefined threshold. Hence, the SU should have channel mean gain of the S-Tx→P-Rx link (not instantaneous channel gains) to adjust its transmit power. This is based on the fact that the SU and the PU can collaborate using a localization service where the channel mean gains of the PU and SU such as transmission distance, antenna gain, and so on, can be exchanged [40, 41]. Moreover, the S-Tx and P-Tx are assumed to have full CSI of the S-Tx→S-Rx and P-Tx→P-Rx links, respectively. This is reasonable due to the fact that both SU and PU are in the same systems and they should have dedicated feedback channels. In addition, the channel mean gain of the S-Tx→EAV can be selected offline following [42–44].

Further, all channels are subject to Rayleigh fading and the channel gains are independent random variables distributed following an exponential distribution. Accordingly, the probability density function (PDF) and cumulative distribution function (CDF) of random variables (RV<sub>s</sub>) having exponential distribution are expressed, respectively, as

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

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

where the RV  $X$  refers to the channel gain, and  $\Omega_X = \mathbb{E}[X]$  is the channel mean gain. More specifically, the channel gains, S-Tx→S-Rx and P-Tx→P-Rx of communication links, are denoted, respectively, by  $g_m$ ,  $h_n$ . The channel gains of S-Tx→P-Rx, P-Tx→S-Rx, and P-Tx→EAV interference links are denoted by  $\varphi_m$ ,  $\beta_n$ , and  $\rho_t$ , respectively. The channel gain of the S-Tx→EAV illegitimate links is denoted by  $\alpha_t$ . Here,  $m$ ,  $n$ , and  $t$  ( $m \in \{1, \dots, N_p\}$ ,  $n \in \{1, \dots, N_e\}$ , and  $t \in \{1, \dots, N_s\}$ ), denote the antenna indexes of the S-Rx, EAV, and P-Rx, respectively. In the following, the P-Rx, S-Rx, and EAV are assumed to use SC to process the received signal, i.e., the antenna having the highest signal-to-interference-plus-noise ratio (SINR) will be used to process the received message.

It is a fact that the SU and PU share the same spectrum and thus they may cause mutual interference to each other due to power emission. According to Shannon's theorem, the PU channel capacity subject to interference of the SU can be expressed

$$C_p = B \log_2(1 + \gamma_p), \quad (3)$$

where  $\gamma_p$  is the SINR of the PU defined as

$$\gamma_p = \max_{m \in \{1, 2, \dots, N_p\}} \left\{ \frac{P_p h_m}{P_s \varphi_m + N_0} \right\}, \quad (4)$$

in which  $P_p$  and  $P_s$  are transmit powers of the P-Tx and S-Tx, respectively. Symbol  $N_0$  is the noise power defined by  $N_0 = B \mathcal{N}_0$ ;  $B$  and  $\mathcal{N}_0$  are system bandwidth and noise power spectral density, respectively. Since the SU re-utilizes the PU spectrum band for its communication, the S-Rx suffers from the interference of the P-Tx, and hence the channel capacity of the SU subject to the interference from the P-Tx can be formulated as

$$C_s = B \log_2(1 + \gamma_s), \quad (5)$$

where

$$\gamma_s = \max_{t \in \{1, 2, \dots, N_s\}} \left\{ \frac{P_s g_t}{P_p \beta_t + N_0} \right\}. \quad (6)$$

It should be noted that the EAV overhears the SU information, but it is also subject to interference caused by the P-Tx. Accordingly, the channel capacity of the EAV is given as

$$C_e = B \log_2(1 + \gamma_e), \quad (7)$$

where SINR at the EAVs is expressed as

$$\gamma_e = \max_{n \in \{1, 2, \dots, N_e\}} \left\{ \frac{P_s \alpha_n}{P_p \rho_n + N_0} \right\}. \quad (8)$$

### 3.1 Performance Metric for the SU communication

In the considered system, the transmit power of the SU is subject to its own security constraint and the interference constraint given by the PU. Thus, the SU must have a suitable power allocation policy which does not only satisfy the above constraints but also can obtain a reasonable performance. We assume that the Wyner wiretap code [16] is used for SU communication, and hence a positive rate,  $R_0 > 0$ , should be maintained to provide secure communication for the SU, which can be defined by [42, 45]

$$R_0 = R_s - R_e, \quad (9)$$

where  $R_s$  and  $R_e$  are the code word transmission rate and secret information rate of the SU, respectively.

Accordingly, the perfect secrecy communication of the SU may be obtained if the capacity at the EAV is less than  $R_0$ , i.e.,  $C_e < R_0$ . In other words, the outage secrecy event of the SU occurs when  $C_e > R_0$ , and hence the secrecy outage probability of the SU can be formulated as

$$\mathcal{O}_{sec} = \Pr\{C_e > R_0\}. \quad (10)$$

Moreover, due to the randomness of wireless channels and interference caused by the SU, reliable communication of the PU may not be obtained if the code word transmission rate of the PU is greater than the channel capacity, i.e.  $R_p > C_p$ . It implies that the communication outage event of the PU is expressed as

$$\mathcal{O}_p = \Pr\{C_p < R_p\}. \quad (11)$$

where  $C_p$  is defined in (3).

Clearly, secure and reliable communication of the SU can be obtained if and only if both secrecy and reliable communication outage events do not happen. This can be interpreted into secure and reliable communication probability as

$$\mathcal{O}_{ss} = \Pr\{C_s > R_s, C_e \leq R_0\}, \quad (12)$$

where  $C_s$  and  $C_e$  are formulated in (5) and (7), respectively.

### 3.2 Constraints for transmit power of the SU

In this section, we adopt a common assumption in the literature of the physical security that the CSI is available, together with the S-Tx→EAV wiretap link [46]. This can be obtained when the EAV is active in the network and its behavior may be monitored [47]. In the following, we introduce four communication scenarios in which we study the power allocation policy for the SU.

- 1) *Scenario 1 (S<sub>1</sub>): S-Tx does not have the CSI of neither P-Tx → P-Rx nor the S-Tx → EAV links*

In this scenario, the S-Tx transmits its confidential information without knowing the existence of the EAV. Also the S-Tx does not have the CSI of the P-Tx → P-Rx communication link. Accordingly, the S-Tx only regulates its transmit power on the basis of the interference constraint given by the PU as

$$\mathcal{O}_I = \Pr \left\{ \max_{m \in \{1, 2, \dots, N_p\}} \left\{ \frac{P_s \varphi_m}{N_0} \right\} \geq Q_{pk} \right\} \leq \xi, \quad (13)$$

where  $Q_{pk}$  is peak interference level that the PU can tolerate. This can be interpreted as that the S-Tx is allowed to cause limited interference to the P-Rx, however, the probability of the interference caused by the S-Tx should be kept below a predefined threshold  $\xi$  to not interrupt the PU communication. As a result, the constraints setting on the transmit power of the S-Tx should satisfy two conditions as follows:

$$\mathcal{O}_I \leq \xi, \quad (14)$$

$$0 \leq P_s \leq P_s^{max}, \quad (15)$$

where  $\xi$  and  $P_s^{max}$  are communication outage threshold given by the PU and the maximal transmit power of the S-Tx, respectively.

- 2) *Scenario 2 (S<sub>2</sub>): S-Tx has the CSI of the S-Tx → EAV but not P-Tx → P-Rx*

In this scenario, the S-Tx knows the existence of the EAV in its coverage range and the CSI of the S-Tx → S-Rx link is available at the S-Tx. However, the S-Tx does not have the CSI of the P-Tx → P-Rx link. Consequently, the transmit power of the S-Tx should satisfy three constraints as follows:

$$\mathcal{O}_I \leq \xi, \quad (16)$$

$$\mathcal{O}_{sec} \leq \epsilon, \quad (17)$$

$$0 \leq P_s \leq P_s^{max}, \quad (18)$$

where  $\epsilon$  is the secrecy outage constraint given by the SU and  $\mathcal{O}_I$  and  $\mathcal{O}_{sec}$  are defined in (10) and (13), respectively.

- 3) *Scenario 3 (S<sub>3</sub>): S-Tx has the CSI of the P-Tx → P-Rx but not S-Tx → EAV*

In this scenario, the S-Tx has the CSI of the P-Tx → P-Rx communication link. However, it does not know the existence of the EAV. Accordingly, the constraints for the S-Tx is as follows:

$$\mathcal{O}_p \leq \theta, \quad (19)$$

$$0 \leq P_s \leq P_s^{max}, \quad (20)$$

where  $\mathcal{O}_p$  is defined in (11), and  $\theta$  is the communication outage constraint of the PU. In other words, the transmit power of the S-Tx should keep the outage probability of the PU below a given constraint.

- 4) *Scenario 4 (S<sub>4</sub>): S-Tx has the CSI of both the P-Tx → P-Rx and S-Tx → EAV*

In this scenario, the S-Tx adjust its transmit power to not reveal its confidential information to the EAV and to not cause harmful interference to the P-Rx. Thus, the transmit power of the S-Tx is subject to three constraints as follows:

$$\mathcal{O}_p \leq \theta, \quad (21)$$

$$\mathcal{O}_{sec} \leq \epsilon, \quad (22)$$

$$0 \leq P_s \leq P_s^{max}, \quad (23)$$

where  $\mathcal{O}_p$  and  $\mathcal{O}_{sec}$  are defined in (11) and (10).

### 4 Performance analysis

In this section, we first derive the power allocation policy for the S-Tx, and then use it to calculate the amount of fading, and outage performance of the S-Tx. Let us commence by considering a property as follows.

property 1 Let  $a$ ,  $b$ , and  $c$  be positive constants. Random variables  $X_i$  and  $Y_i$  are independent and exponentially distributed with mean values  $\Omega_X$  and  $\Omega_Y$ , respectively. An RV  $U$  defined by

$$U = \max_{i \in \{1, 2, \dots, N\}} \left( \frac{aX_i}{bY_i + c} \right), \quad (24)$$

and has the CDF and PDF, respectively, given by

$$F_U(u) = \left[ 1 - \frac{1}{\frac{b\Omega_Y}{a\Omega_X}u + 1} \exp\left(-\frac{uc}{a\Omega_X}\right) \right]^N \tag{25}$$

$$= \sum_{q=0}^N \binom{N}{q} \frac{(-1)^q}{(Au + 1)^q} \exp\left(-\frac{qu}{D}\right),$$

$$f_U(u) = N \sum_{q=0}^{N-1} \binom{N-1}{q} (-1)^q \tag{26}$$

$$\times \left[ \frac{A \exp\left(-\frac{(1+q)u}{D}\right)}{(1 + Au)^{q+2}} + \frac{\exp\left(-\frac{(1+q)u}{D}\right)}{D(1 + Au)^{q+1}} \right], \tag{27}$$

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

Proof The proof is given in [48, Lemma 1].  $\square$

### 4.1 Transmission power allocation policies

To derive the power allocation policies for the S-Tx, we need to calculate the secrecy outage probability of the SU given in (10), the outage probability of the PU given in (11), and the outage probability given in (13), respectively.

#### 4.1.1 The transmit power of S-Tx under the interference threshold of the PU

From (14), we can calculate  $\mathcal{O}_I$  as follows

$$\mathcal{O}_I = \Pr\left\{ \max_{m \in \{1, 2, \dots, N_p\}} \left\{ \frac{P_s \varphi_m}{N_0} \right\} \geq Q_{pk} \right\} \leq \zeta$$

$$= 1 - \Pr\left\{ \max_{m \in \{1, 2, \dots, N_p\}} \{ \varphi_m \} < \frac{Q_{pk} N_0}{P_s} \right\} \leq \zeta \tag{28}$$

$$= 1 - \left\{ 1 - \exp\left(-\frac{Q_{pk} N_0}{\Omega_\varphi P_s}\right) \right\}^{N_p} \leq \zeta.$$

After some mathematical manipulations, it can be concluded that the transmit power of the S-Tx should satisfy the following constraint

$$P_s \leq \frac{Q_{pk} N_0}{\Omega_\varphi} \left( \log_e \frac{1}{1 - \frac{N_p}{\sqrt{1 - \zeta}}} \right)^{-1}. \tag{29}$$

#### 4.1.2 The transmit power of the S-Tx under the secrecy outage constraint

Here, we assume that the EAV may have an advanced background noise filter, and the EAV is only interfered by the outburst transmit power from the P-Tx. In other words, we consider the worst case where the background noise is cancelled significantly and the outburst interference from the P-Tx to the EAV is much higher than the background

noise. Therefore, the SINR of the EAV given in (8) can be rewritten as

$$\gamma_e = \max_{n \in \{1, 2, \dots, N_e\}} \left\{ \frac{P_s \alpha_n}{P_p \rho_n + N_0} \right\} \approx \max_{n \in \{1, 2, \dots, N_e\}} \left\{ \frac{P_s \alpha_n}{P_p \rho_n} \right\}. \tag{30}$$

Accordingly, we can derive the secrecy outage probability of the SU as follows

$$\mathcal{O}_{sec} = 1 - \Pr\left\{ \max_{n \in \{1, 2, \dots, N_e\}} \left\{ \frac{\alpha_n}{\rho_n} \right\} \leq \frac{P_p}{P_s} \gamma_{th}^e \right\} \leq \epsilon, \tag{31}$$

where  $\gamma_{th}^e = 2^{\frac{R_0}{B}} - 1$ . Further, we can derive the outage probability by using order statistics theory as follows

$$\mathcal{O}_{sec} = 1 - \prod_{n=1}^{N_e} \int_0^\infty \Pr\left\{ \alpha_n \leq \frac{P_p}{P_s} \gamma_{th}^E x \right\} f_{\rho_n}(x) dx$$

$$= 1 - \left( 1 - \frac{1}{\frac{P_p \Omega_p \gamma_{th}^E}{P_s \Omega_x} + 1} \right)^{N_e} \leq \epsilon. \tag{32}$$

After some manipulation, we obtain the maximum transmission power of the S-Tx under its own secrecy capacity constraint as follows

$$P_s \leq \frac{P_p \Omega_p \gamma_{th}^E}{\Omega_x} \left( \frac{1}{\sqrt[N_e]{1 - \epsilon}} - 1 \right). \tag{33}$$

#### 4.1.3 The transmission power of the S-Tx under the outage probability constraint of the PU

From (11), we can calculate the outage probability of the PU as follows

$$\mathcal{O}_p = \Pr\left\{ \max_{m \in \{1, 2, \dots, N_p\}} \left\{ \frac{P_p h_m}{P_s \varphi_m + N_0} \right\} \leq \gamma_{th}^p \right\} \leq \theta, \tag{34}$$

where  $\gamma_{th}^p = 2^{\frac{R_p}{B}} - 1$ . Using the help of (25) in Property 1 for (34) by setting  $a = P_p$ ,  $b = P_s$ ,  $c = N_0$ ,  $\Omega_X = \Omega_h$ ,  $\Omega_Y = \Omega_\varphi$ , and  $u = \gamma_{th}^p$ , a closed-form expression for PU is obtained as

$$\mathcal{O}_p = \left[ 1 - \frac{1}{\frac{P_s \Omega_\varphi \gamma_{th}^p}{P_p \Omega_h} + 1} \exp\left(-\frac{\gamma_{th}^p N_0}{P_p \Omega_h}\right) \right]^{N_p} \leq \theta. \tag{35}$$

After some manipulations, we obtain the maximal transmission power of the S-Tx as follows

$$P_s \leq \frac{P_p \Omega_h}{\gamma_{th}^p \Omega_\varphi} \Xi, \tag{36}$$

where  $\Xi$  is defined as

$$\Xi = \max \left\{ 0, \frac{1}{1 - \frac{N_p}{\sqrt{\theta}}} \exp \left[ -\frac{\gamma_{th}^p N_0}{P_p \Omega_h} \right] - 1 \right\}. \tag{37}$$

4.1.4 Power allocation policy for the considered scenarios

Now, we can obtain the transmit power allocation policies for four considered scenarios as follows:

- Firstly, the power allocation policy for the scenario  $S_1$  is obtained by combining (15) with (29) as

$$\mathcal{P}_{S_1} = \min \left\{ \frac{Q_{pk} N_0}{\Omega_\varphi} \left( \log_e \frac{1}{1 - \frac{N_p}{\sqrt{1-\xi}}} \right)^{-1}, P_s^{max} \right\}. \tag{38}$$

- Secondly, we obtain the power allocation policy for scenario  $S_2$  by combining (18), (29), with (33) as

$$\mathcal{P}_{S_2} = \min \left\{ \frac{Q_{pk} N_0}{\Omega_\varphi} \left( \log_e \frac{1}{1 - \frac{N_p}{\sqrt{1-\xi}}} \right)^{-1}, \frac{P_p \Omega_\rho \gamma_{th}^e}{\Omega_\alpha} \left( \frac{1}{\sqrt{N_e} \sqrt{1-\epsilon}} - 1 \right), P_s^{max} \right\}. \tag{39}$$

- Thirdly, the transmit power of the S-Tx for scenario  $S_3$  is achieved by combining (20) with (36) as

$$\mathcal{P}_{S_3} = \min \left\{ \frac{P_p \Omega_h}{\gamma_{th}^p \Omega_\varphi} \Xi, P_s^{max} \right\}, \tag{40}$$

where  $\Xi$  is defined in (37) as

$$\Xi = \max \left\{ 0, \frac{1}{1 - \frac{N_p}{\sqrt{\theta}}} \exp \left[ -\frac{\gamma_{th}^p N_0}{P_p \Omega_h} \right] - 1 \right\}. \tag{41}$$

Note that this power allocation is exactly the one reported in [48, Eq. (9)].

- Finally, the transmit power policy of the S-Tx for scenario  $S_4$  is established by combining (20), (36) with (33) as

$$\mathcal{P}_{S_4} = \min \left\{ \frac{P_p \Omega_\rho \gamma_{th}^e}{\Omega_\alpha} \left( \frac{1}{\sqrt{N_e} \sqrt{1-\epsilon}} - 1 \right), \frac{P_p \Omega_h}{\gamma_{th}^p \Omega_\varphi} \Xi, P_s^{max} \right\}. \tag{42}$$

Accordingly, the power allocation algorithm corresponding to four scenarios is given in **Algorithm 1**.

---

**Algorithm 1** Algorithm for Power Allocation Policy.

---

```

1: function PAP()
2:   INITIALIZE(); ▷ Initialize system parameters
3:    $\Xi = \max \left\{ 0, \frac{1}{1 - \frac{N_p}{\sqrt{\theta}}} \exp \left[ -\frac{\gamma_{th}^p N_0}{P_p \Omega_h} \right] - 1 \right\};$ 
4:   /* Scenario  $S_4$  */
5:   if S-Tx has the CSI of both the P-Tx→P-Rx and S-Tx→EAV links then
6:      $\mathcal{P}_S = \min \left\{ \frac{P_p \Omega_\rho \gamma_{th}^e}{\Omega_\alpha} \left( \frac{1}{\sqrt{N_e} \sqrt{1-\epsilon}} - 1 \right), \frac{P_p \Omega_h}{\gamma_{th}^p \Omega_\varphi} \Xi, P_s^{max} \right\};$ 
7:     return  $\mathcal{P}_S$ ;
8:   end if
9:   /* Scenario  $S_3$  */
10:  if S-Tx has the CSI of the P-Tx→P-Rx but not S-Tx→EAV links then
11:     $\mathcal{P}_S = \min \left\{ \frac{P_p \Omega_h}{\gamma_{th}^p \Omega_\varphi} \Xi, P_s^{max} \right\};$ 
12:    return  $\mathcal{P}_S$ ;
13:  end if
14:  /* Scenario  $S_2$  */
15:  if S-Tx has the CSI of the S-Tx→EAV but not P-Tx→P-Rx links then
16:     $\mathcal{P}_S = \min \left\{ \frac{Q_{pk} N_0}{\Omega_\varphi} \left( \log_e \frac{1}{1 - \frac{N_p}{\sqrt{1-\xi}}} \right)^{-1}, \frac{P_p \Omega_\rho \gamma_{th}^e}{\Omega_\alpha} \left( \frac{1}{\sqrt{N_e} \sqrt{1-\epsilon}} - 1 \right), P_s^{max} \right\};$ 
17:    return  $\mathcal{P}_S$ ;
18:  end if
19:  /* Scenario  $S_1$  */
20:  if S-Tx does not have the CSI of both P-Tx→P-Rx and S-Tx→EAV links then
21:     $\mathcal{P}_S = \min \left\{ \frac{Q_{pk} N_0}{\Omega_\varphi} \left( \log_e \frac{1}{1 - \frac{N_p}{\sqrt{1-\xi}}} \right)^{-1}, P_s^{max} \right\};$ 
22:    return  $\mathcal{P}_S$ ;
23:  end if
24: end function

```

---

### 4.2 Secure and reliable communication probability

Recall that the safe and secure communication probability is defined as the probability that the S-Tx can communicate with the S-Rx without exposing the information to the EAV. Given the obtained power allocation policies and mutually independent channels, we can rewrite the safe and secure communication probability in (12) as

$$\mathcal{O}_{ss} = \Pr\{C_s > R_s\} \Pr\{C_e \leq R_0\} = (1 - \mathcal{O}_s)(1 - \mathcal{O}_{sec}), \tag{43}$$

where  $\mathcal{O}_s$  and  $\mathcal{O}_{sec}$  are obtained, respectively, by using the help of *Property 1* according to

$$\mathcal{O}_s = \sum_{i=0}^{N_s} \binom{N_s}{i} \frac{(-1)^i}{(A_s \gamma_{th}^s + 1)^i} \exp\left(-\frac{i \gamma_{th}^s}{D_s}\right) \tag{44}$$

$$\mathcal{O}_{sec} = 1 - \sum_{j=0}^{N_e} \binom{N_e}{j} \frac{(-1)^j}{(A_e \gamma_{th}^e + 1)^j} \tag{45}$$

where  $\gamma_{th}^s = 2^{\frac{R_s}{B}} - 1$ ,  $A_s = \frac{P_p \Omega_B}{P \Omega_g}$ ,  $A_e = \frac{P_p \Omega_p}{P \Omega_z}$ , and  $\frac{1}{D_s} = \frac{N_0}{P \Omega_g}$ .

Finally, a closed-form expression of the safe and secure communication probability is obtained by substituting (44) and (45) into (43), where  $\mathcal{P} \in \{\mathcal{P}_{S_1}, \mathcal{P}_{S_2}, \mathcal{P}_{S_3}, \mathcal{P}_{S_4}\}$  is the transmit power allocation policy of the S-Tx.

### 5 Numerical results

In this section, we present numerical examples to examine the power allocation policies and the SRCP for the considered model. To gain more insights, we make comparisons between the scenario  $S_1$  and the scenario  $S_2$ , the scenario  $S_3$  and the scenario  $S_4$ . In this work, we assume that S-Tx, S-Rx, P-Rx, EAV, and P-Tx are located at (0, 0), (−1, 2), (0.5, 1), (0, 2.5), and (0, 2) on the 2D plane, respectively. Unless otherwise stated, the parameter settings used in the numerical results are derived from existing wireless networks such [49, 50] as follows:

- System bandwidth:  $B=5$  MHz;
- SU target rate:  $R_s=128$  Kbps;
- PU target rate:  $R_p=64$  Kbps;
- SU secrecy information rate:  $R_e=64$  Kbps;
- Pathloss exponent  $\nu = 4$ ;
- Outage probability constraints of the PU and SU:  $\theta = \xi = 0.01$ ;
- Outage probability constraint of the EAV:  $\epsilon = 0.1$ ;
- The maximal transmit SNR of the S-Tx:  $\gamma_s^{\max} = 10$  (dB);
- Peak interference level of the PU:  $Q_{pk} = -5$  (dB)

Without loss generality, we denote  $\bar{\gamma}_s = \frac{P}{N_0}$  and  $\bar{\gamma}_p = \frac{P_p}{N_0}$  as the transmit SNR of the S-Tx and P-Tx, respectively.

Figure 2 shows the transmit SNR of the S-Tx as a function of the P-Tx transmit SNR. Firstly, we observe the behavior of the transmit SNR of the S-Tx in the scenarios  $S_1$  and  $S_2$ , and can see that the transmit SNR of the S-Tx in scenario  $S_1$  is constant for the entire range of the P-Tx SNR. This result matches (38) where the transmit SNR of the S-Tx does not depend on the transmit SNR of the P-Tx. In contrast to scenario  $S_1$ , the S-Tx linearly increases with an increase of the S-Tx transmit SNR in scenario  $S_2$ . However, when the transmit SNR of the P-Tx increases beyond 10 dB ( $A_1$ ), the transmit SNR of the S-Tx is saturated. This can be explained by the fact that the transmit SNR of the S-Tx is allocated using Eq. (39). Thus, in the regime  $[-16, 10]$  dB, the transmit SNR of the S-Tx is controlled by the constraint of the EAV. However, if the transmit SNR of the P-Tx increases further, the transmit SNR of the S-Tx is subject to the minimum value of the first term and third term in Eq. (39), i.e., in the high regime of the transmit SNR of P-Tx, the transmit SNR of the S-Tx is similar to the one in Scenario 1. It is easy to understand that the transmit SNR of the S-Tx in scenario  $S_1$  is always less than or equal to the one in scenario  $S_2$  since the transmit SNR S-Tx in  $S_2$  is subject to a additional constraint, i.e., the outage constraint of the EAV. Secondly, we observe the behavior of the transmit SNR of the S-Tx in scenarios  $S_3$  and  $S_4$ . It can be seen that the transmit SNR of the S-Tx in the scenario  $S_4$  is always less than the one of the scenario  $S_3$ . However, in the high regime of the transmit SNR of the P-Tx, e.g.  $\bar{\gamma}_p \geq 16$  dB, they are equal and saturated at  $A_2$ . This is because the transmit SNR of the S-Tx in scenario  $S_4$  endures more constraints than the one of scenario  $S_3$ , i.e., the constraint of the EAV. Finally, we can conclude that the appearance of the EAV leads to that

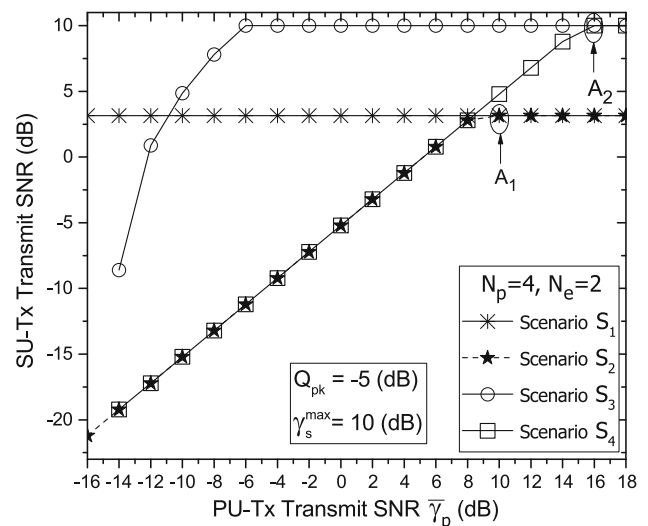


Fig. 2 The S-Tx transmission SNR for four scenarios versus the P-Tx transmission SNR



the power allocation policy for the S-Tx is more complicated and may degrade the performance of the SU.

Figure 3 plots the transmit SNR of the S-Tx as a function of the P-Rx antennas,  $N_p$ . We can see that the transmit SNR of the S-Tx in scenarios  $S_1$  and  $S_3$  is much higher than the one in scenarios  $S_2$  and  $S_4$ . This happens for the same reason as in Fig. 2, i.e., when the S-Tx is subject to the additional constraint of the EAV, the transmit SNR of the S-Tx is degraded. In addition, when the number of antennas of the P-Rx increases, the transmit SNR of the S-Tx in scenario  $S_1$  decreases slightly. It is due to the fact that increasing the number of antennas of the P-Rx leads to increase in the constraints for the S-Tx. Thus, the S-Tx must decrease its transmit SNR to not cause harmful interference to the P-Rx (see Eq.(13)). It is interesting to see that the transmit SNR of scenarios  $S_2$  and  $S_4$  are the same for the whole considered range of  $N_p$ . This is due to the fact that the constraint of the EAV is the strongest one (see Eq. (33)). Accordingly, the transmit SNR of the S-Tx under the constraint of the EAV becomes the minimum value in both (39) and (42) in the considered range of  $N_p$ , i.e.,

$$\mathcal{P}_{S_2} = \mathcal{P}_{S_4} = \frac{P_p \Omega_p \gamma_{th}^E}{\Omega_x} \left( \frac{1}{\sqrt{1-\epsilon}} - 1 \right).$$

Figure 4 shows the impact of the number of antennas on the EAV on the transmit SNR of the S-Tx. Firstly, we observe the behavior of the transmit SNR of the S-Tx in scenarios  $S_1$  and  $S_3$  and see that the transmit SNR of the S-Tx does not change following the change of  $N_e$ . This is because the S-Tx does not know the existence of the EAV. However, when the S-Tx knows the existence of the EAV as in scenarios  $S_2$  and  $S_4$ , the transmit SNR degrades

significantly as the number of antennas of the EAV increases. This is due to the fact that increasing the number of antennas of the EAV leads to an improvement its eavesdropping probability. As a result, the S-Tx in scenarios  $S_2$  and  $S_4$  must reduce its transmit SNR to secure the communication information.

In Fig. 5, we show the impact of the P-Tx transmit SNR on the SRCP of the SU. It can be observed that the SRCP of the scenario  $S_2$  (scenario  $S_4$ ) is always better than the one in scenario  $S_1$  (scenario  $S_3$ ) in the low regime of the P-Tx SNR  $\bar{\gamma}_p \leq -4$  dB ( $\bar{\gamma}_p \leq 2$  dB). However, when the P-Tx SNR is increased further, the SRCP of scenarios  $S_1$  and  $S_2$  (scenarios  $S_3$  and  $S_4$ ) are identical. This is because when the P-Tx transmit SNR is in the low regime, the S-Tx transmit SNR in scenario  $S_1$  (scenario  $S_3$ ) is greater than the one of scenario  $S_2$  (scenario  $S_4$ ). Accordingly, the secure probability of the SU degrades significantly, while the safe communication probabilities are not much different. As a result, the SRCP of scenario  $S_1$  (scenario  $S_3$ ) is smaller than the one of scenario  $S_2$  (scenario  $S_4$ ) (see (43)). When the P-Tx SNR increases further, e.g. 2 (dB)  $\leq \bar{\gamma}_p \leq 14$  (dB), the S-Tx can adjust its transmit power to the maximal value in all scenarios. This leads to the SRCP for scenarios  $S_1$  and  $S_2$  (scenarios  $S_3$  and  $S_4$ ) being identical. Most interestingly, in the high regime of the P-Tx SNR, the SRCP for scenarios  $S_1$  and  $S_2$  (scenarios  $S_3$  and  $S_4$ ), e.g.  $\bar{\gamma}_p \geq 6$  (dB) or  $\bar{\gamma}_p \geq 14$  (dB) are degraded. This is due to the fact that in the low regime of the P-Tx SNR, the S-Tx can regulate its transmit SNR to satisfy the given constraints. However, when the transmit SNR of P-Tx increases further, it becomes a strong interference source to S-Rx, which leads to degrade the SRCP of the SU.

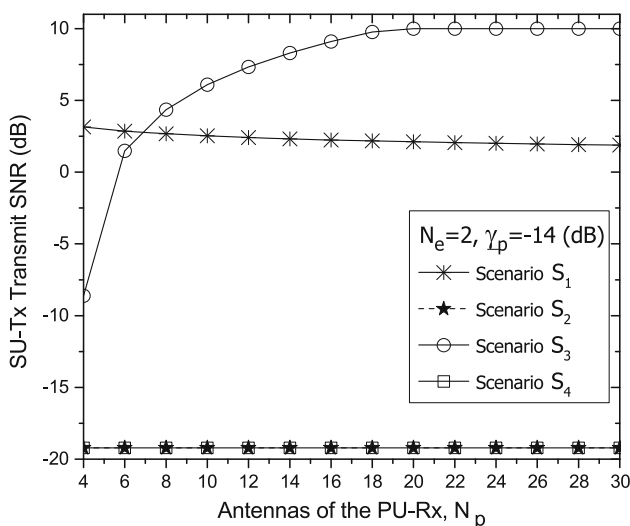


Fig. 3 Impact of the number of antennas of the P-Rx on the transmit SNR of the S-Tx

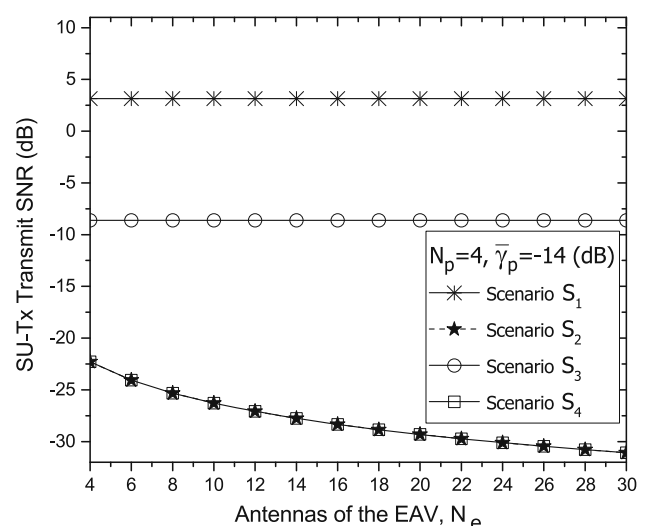
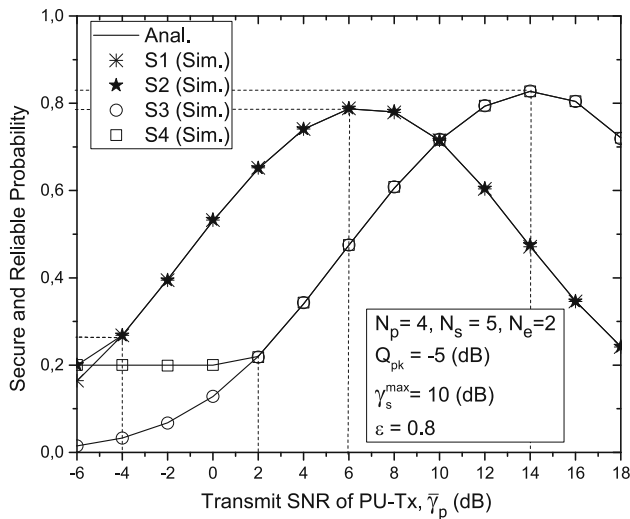
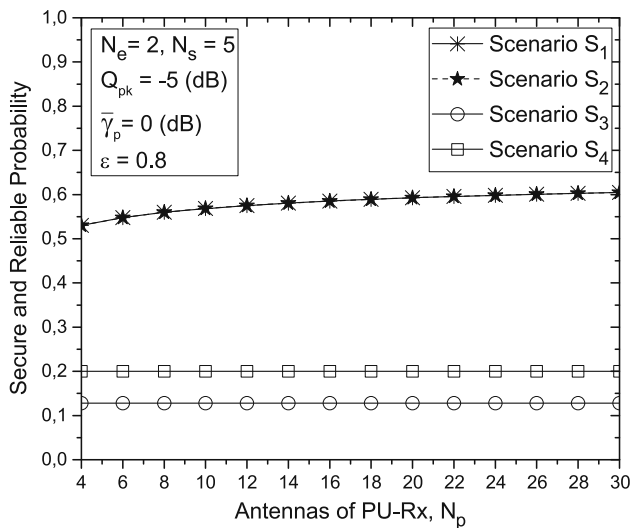


Fig. 4 Impact of the number of antennas of the EAV on the transmit SNR of the S-Tx

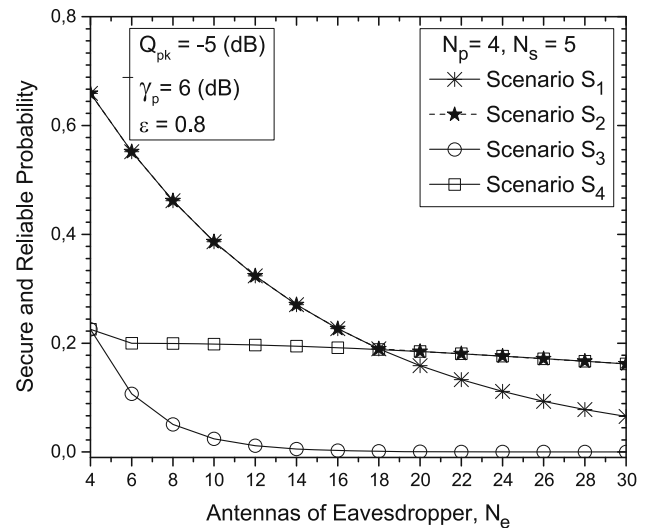


**Fig. 5** SRCP versus the transmit SNR of the P-Tx with  $\epsilon = 0.8$



**Fig. 6** Impact of number of antennas of the P-Rx on the SRCP of the SU

In Fig. 6, we show the impact of number of antennas of the P-Rx on the SRCP of the SU. The  $SRCP_s$  are identical and slight increasing for scenarios  $S_1$  and  $S_2$ . This can be explained as the P-Rx can tolerate more interference from the S-Tx as its number of antennas increases. Consequently, the S-Tx can increase its transmit power to enhance the SRCP. However, under the constraints of peak interference level  $Q_{pk}$ , outage probability constraint  $\xi$ , as well as secrecy outage constraint  $\epsilon$ , the transmit power of the S-Tx is identical for both scenarios  $S_1$  and  $S_2$ . Thus, the SRCP are identical. In contrast to scenarios  $S_1$  and  $S_2$ , the SRCP in scenario  $S_4$  outperforms the one of the scenario  $S_3$ . This is because that the S-Tx in the scenario  $S_3$  does not care about the existence of the EAV, thus it can transmit with maximal transmit power and its information



**Fig. 7** Impact of number of antennas of the EAV on the SRCP of the SU

communication may be revealed to the EAV. Alternatively, in scenario  $S_4$ , the S-Tx knows the existence of the EAV, thus it adjusts its transmit power to not reveal information to the EAV. Accordingly, the SRCP in scenario  $S_4$  outperforms the one in the scenario  $S_3$ .

Finally, we examine the impact of the number of antennas of the EAV on the SRCP of the SU as shown in Fig. 7. It can be seen that the SRCP for scenarios  $S_1$  and  $S_3$ , where the secure constraint are not considered, are degraded rapidly. Alternatively, the SRCP in scenarios  $S_2$  and  $S_4$ , where the secure constraint is integrated, degrade gradually. Clearly, the scenarios with the CSI of the EAV can make the information communication of the SU more secure and reliable.

## 6 Conclusions

In this paper, we have investigated how to obtain secure and reliable communication in a CRN in which the SU transmitter is subject to eavesdropping. Given the constraints of the PU, EAV, and SU, we derive four power allocation policies corresponding to four different scenarios depending on which type of CSI that is available. Accordingly, a performance measure in terms of secure and reliable communication probability is introduced to evaluate the considered system. Our results show that the security constraint only effects the SRCP of the SU in the low regime of the transmit SNR of the P-Tx. Further, the system performance degrades significantly when the security constraints are not considered and the number of antennas of the EAV increases. Finally, simulations validate our analytical results.

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

**Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

## References

- Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 23(2), 201–220.
- Datla, D., Wyglinski, A. M., & Minden, G. J. (2009). A spectrum surveying framework for dynamic spectrum access networks. *IEEE Transactions on Vehicular Technology*, 58(8), 4158–4168.
- Gastpar, M. (2007). On capacity under receive and spatial spectrum-sharing constraints. *IEEE Transactions on Information Theory*, 53(2), 471–487.
- Tran, H. (2013). Performance analysis of cognitive radio networks with interference constraints. *Dissertation*, Blekinge Institute of Technology, Karlskrona.
- Musavian, L., & Aissa, S. (2009). Fundamental capacity limits of cognitive radio in fading environments with imperfect channel information. *IEEE Transactions on Communications*, 57(11), 3472–3480.
- Mitola, J. (Nov. 1999). Cognitive radio for flexible mobile multimedia communications. In *Proceedings of IEEE international workshop mobile multimedia communication*, San Diego (pp. 3–10).
- Jovicic, A., & Viswanath, P. (2006). Cognitive radio: An information-theoretic perspective. In *Proceedings of IEEE ISIT*, Seattle (pp. 2413–2417).
- Akhtar, F., Rehmani, M. H., & Reisslein, M. (2016). White space: Definitional perspectives and their role in exploiting spectrum opportunities. *Telecommunications Policy*, 40(4), 319–331. <http://www.sciencedirect.com/science/article/pii/S0308596116000124>
- Abdelhadi, A., Shajaiah, H., & Clancy, C. (2015). A multitier wireless spectrum sharing system leveraging secure spectrum auctions. *IEEE Transactions on Cognitive Communications and Networking*, 1(2), 217–229.
- Khan, A. A., Rehmani, M. H., & Reisslein, M. (2016). Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols. *IEEE Communications Surveys Tutorials*, 18(1), 860–898.
- Saleem, Y., & Rehmani, M. H. (2014). Primary radio user activity models for cognitive radio networks: A survey. *Journal of Network and Computer Applications*, 43, 1–1. <http://www.sciencedirect.com/science/article/pii/S1084804514000848>
- Fragkiadakis, A. G., Tragos, E. Z., & Askoxylakis, I. G. (2013). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys & Tutorials*, 15(1), 428–445.
- Zou, Y., Zhu, J., Yang, L., Liang, Y. C., & Yao, Y. D. (2015). Securing physical-layer communications for cognitive radio networks. *IEEE Communications Magazine*, 53(9), 48–54.
- Sanyal, S., Bhadauria, R., & Ghosh, C. (2009). Secure communication in cognitive radio networks. In *Proceedings of international conference on computers and devices for communication* (pp. 1–4).
- Alahmadi, A., Abdelhakim, M., Ren, J., & Li, T. (2013). Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard. In *Proceedings of IEEE global communications conference* (pp. 3229–3234).
- Wayner, A. D. (1975). The wire-tap channel. *Bell Systems Technical Journal*, 54(8), 1355–1387.
- Bloch, M., Barros, J., Rodrigues, M., & McLaughlin, S. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6), 2515–2534.
- Mavoungou, S., Kaddoum, G., Taha, M., & Matar, G. (2016). Survey on threats and attacks on mobile networks. *IEEE Access*, 4, 4543–4572.
- Fragkiadakis, A., Tragos, E., & Askoxylakis, I. (2013). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys & Tutorials*, 15(1), 428–445.
- Leung-Yan-Cheong, S. K., & Hellman, M. E. (1978). The gaussian wiretap channel. *IEEE Transactions on Information Theory*, 24(1), 451–456.
- Pei, Y., Liang, Y.-C., Zhang, L., Teh, K., & Li, K. H. (2010). Secure communication over MISO cognitive radio channels. *IEEE Transactions on Wireless Communications*, 9(4), 1494–1502.
- Zou, Y., Li, X., & Liang, Y.-C. (2014). Secrecy outage and diversity analysis of cognitive radio systems. *IEEE Journal on Selected Areas in Communications*, 32(11), 2222–2236.
- Attar, A., Tang, H., Vasilakos, A. V., Yu, F. R., & Leung, V. C. M. (2012). A survey of security challenges in cognitive radio networks: Solutions and future research directions. *IEEE Communications Surveys & Tutorials*, 100(12), 31723186.
- Xiao, H., Yang, K., Wang, X., & Shao, H. (2012). A robust MDP approach to secure power control in cognitive radio networks. In *Proceedings of IEEE international conference on communications*, Ottawa (pp. 4642–4647).
- Pei, Y., Liang, Y.-C., Zhang, L., Teh, K. C., & Li, K. H. (2009). Achieving cognitive and secure transmissions using multiple antennas. In *Proceedings of IEEE personal indoor mobile radio communication*, Singapore (pp. 1–5).
- Pei, Y., Liang, Y.-C., Zhang, L., Teh, K. C., & Li, K. H. (2011). Increasing secrecy capacity via joint design of cooperative beamforming and jamming. In *Proceedings IEEE personal indoor mobile radio communication*, Toronto, ON (p. 12741278).
- Wang, C., & Wang, H.-M. (2014). On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels. *IEEE Transactions on Information Forensics and Security*, 9(11), 1814–1827.
- Gabry, F., Zappone, A., Thobaben, R., Jorswieck, E. A., & Skoglund, M. (2015). A survey of security challenges in cognitive radio networks: Solutions and future research directions. *IEEE Wireless Communications Letters*, 4(4), 437440.
- Zou, Y., Wang, X., & Shen, W. (2013). Physical-layer security with multiuser scheduling in cognitive radio networks. *IEEE Transactions on Communications*, 61(12), 5103–5113.
- Sakran, H., Shokair, M., Nasr, O., El-Rabaie, S., & El-Azm, A. (2012). Proposed relay selection scheme for physical layer security in cognitive radio networks. *IET Communications*, 6(16), 2676–2687.
- Ha, D. B., Vu, T. T., Duy, T. T., & Bao, V. N. Q. (2015). Secure cognitive reactive decode-and-forward relay networks with and without eavesdroppers. *Springer Wireless Personal Communications*, 85(4), 2619–2641.

32. Sibomana, L., Zepernick, H. J., & Tran, H. (2014). On physical layer security for reactive DF cognitive relay networks. In *Proceedings of IEEE GLOBECOM*, Austin, TX (pp. 1290–1295).
33. Nguyen, V. D., Duong, T. Q., Dobre, O., & Shin, O. S. (2016). Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks. *IEEE Transactions on Information Forensics and Security*, 11(99), 1.
34. Wu, Y., & Liu, K. (2011). An information secrecy game in cognitive radio networks. *IEEE Transactions on Information Forensics and Security*, 6(3), 831–842.
35. Stanojev, I., & Yener, A. (2013). Improving secrecy rate via spectrum leasing for friendly jamming. *IEEE Transactions on Wireless Communications*, 12(1), 134–145.
36. Sibomana, L., Tran, H., & Tran, Q. A. (2015). Impact of secondary user communication on security communication of primary user. *Security and Communication Networks, Journal of Wiley*, 41774190(99), 1–1.
37. Zou, Y., & Wang, G. (2016). Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. *IEEE Transactions on Industrial Informatics*, 12(2), 780–787.
38. Ha, D. B., Vu, T. T., Duy, T. T., & Bao, V. N. Q. (2015). Secure cognitive reactive decode-and-forward relay networks: With and without eavesdroppers. *Springer Wireless Personal Communications*, 85(4), 2619–2641.
39. Liu, Y., Wang, L., Duy, T. T., Elkashlan, M., & Duong, T. Q. (2015). Relay selection for security enhancement in cognitive relay networks. *IEEE Wireless Communications Letters*, 4(1), 46–49.
40. Zou, Y., Zhu, J., Zheng, B., & Yao, Y. D. (2010). An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks. *IEEE Transactions on Signal Processing*, 58(10), 5438–5445.
41. Bahrak, B., Bhattarai, S., Ullah, A., Park, J. M. J., Reed, J., & Gurney, D. (2014). Protecting the primary users' operational privacy in spectrum sharing. In *Proceedings of IEEE international symposium on dynamic spectrum access networks*, McLean, VA, pp. 236–247.
42. Zhou, X., McKay, M. R., Maham, B., & Hjørungnes, A. (2011). Rethinking the secrecy outage formulation: A secure transmission design perspective. *IEEE Communications Letters*, 15(3), 302–304.
43. Liu, W., Zhou, X., Durrani, S., & Popovski, P. (2016). Secure communication with a wireless-powered friendly jammer. *IEEE Transactions on Wireless Communications*, 15(1), 401–415.
44. Duy, T. T., Duong, T. Q., Thanh, T. L., & Bao, V. N. Q. (2015). Secrecy performance analysis with relay selection methods under impact of co-channel interference. *IET Communications*, 9(11), 1427–1435.
45. Xu, X., He, B., Yang, W., Zhou, X., & Cai, Y. (2016). Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers. *IEEE Transactions on Information Forensics and Security*, 11(2), 373–387.
46. Zou, Y., & Zhu, J. (2016). *Physical-layer security for cooperative relay networks*. Berlin: Springer.
47. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6), 2515–2534.
48. Tran, H., Hagos, M. A., Mohamed, M., & Zepernick, H.-J. (2013). Impact of primary networks on the performance of secondary networks. In *Proceedings of international conference on computing, management and telecommunications*, Ho Chi Minh City (pp. 43–48).
49. ITU-R (2008). Requirements related to technical performance for IMT-advanced radio interface(s), Technical Report ITU-R M.2134.

50. Garg, V. K. (2011). *LTE-The UMTS long term evolution: From theory to practice*. New York: Wiley.



**Trung Xuan Quach** received a bachelor degree in Information Technology from Vietnam National University, VNU-University of Engineering and Technology (VNU-UET), Vietnam, in 2002, and a Master degree in Computer science from Thai Nguyen University (TNU), Viet Nam, in 2007. He is currently a second year Ph.D. student at VNU-UET, Vietnam. Currently, he is a lecturer and vice-dean of the Faculty of Information Technology, at

Thai Nguyen University of Information and Communication Technology (ICTU), Vietnam. His general research interests include wireless communication, physical-layer security, energy harvesting, and communications theory.



**Hung Tran** was born in Hanoi, Vietnam, in 1980. He received the B.S. degree and M.S. degree in information technology from Vietnam National University, Hanoi, in 2002 and 2006, respectively, and the Ph.D. degree from the School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden, in 2013. In 2014, he joined the Electrical Engineering Department, École de Technologie Supérieure, Montreal, Canada. He is currently a

Post-Doctoral Researcher with Mälardalen University, Sweden. His research interests include cognitive radio networks, cooperative communication systems, millimeter wave communications, energy harvesting and security communications at physical layer.



**Elisabeth Uhlemann** received the Ph.D. degree in Communications Theory from Chalmers, Sweden, in 2004 and worked as Assistant and later Associate Professor at Halmstad University 2005–2012. During this period she also worked with Volvo Technology where she was involved in several EU FP6 projects: CVIS, Safespot and Pre-drive C2X, studying communication requirements for traffic safety applications in vehicular networks. She has

contributed to the European ITS communications architecture produced within COMeSafety and she has served as a technical expert in ETSI TC ITS. She has held visiting positions at Uni. South Australia in 2005, TU Berlin in 2007 and Uni. Canterbury, New Zealand in 2011. She has also worked as a consultant at Ikanos Communications, USA, in 2005 with VDSL protocols and at Free2move, Sweden, during 2009–2010 with wireless audio. She has served in the grading

committee of more than 15 Ph.D. degrees in Sweden, Spain, Germany and Australia and she has organized two post-graduate courses “Communications for Cyber-Physical Systems” in 2014 at MDH and “Block Turbo Codes and Iterative Decoding” at Halmstad University in 2006. She is a Research Grant Reviewer for Vinnova, Sweden’s innovation agency, in the area of vehicular electronics, software and communications and serves as a senior editor for IEEE VT Magazine in the area of Connected Vehicles. She is also co-chair of the Subcommittee on Industrial Communication Systems within the IEEE IES Technical Committee on Factory Automation and vice chair of the Swedish IEEE VT/COM/IT chapter. She has two best paper awards: APCC 2005 and ETFA 2010, is part of the steering group of a large research profile at Karlstad University, and in the Faculty board at Mälardalen University.



**George Kaddoum** received the B.Sc. degree in electrical engineering from the École Nationale Supérieure de Techniques Avancées, 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 (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences, University of Toulouse, Toulouse, France, in 2009. Since 2010, he has been a Scientific Consultant of space and wireless

telecommunications for several U.S. and Canadian companies. He is currently an Associate Professor of Electrical Engineering with the École de Technologie Supérieure, University of Quebec, Montréal, QC, Canada. He has authored over 100 journal and conference papers. He holds two pending patents. His recent research activities cover mobile communication systems, modulations, secure transmissions and space communications & navigation. In 2014, he received the ETS Research Chair in physical layer security for wireless networks. He received the Best Paper Awards at the 2017 IEEE PIMRC and 2014 IEEE WIMOB conferences with three co-authors and the 2015 and 2017 IEEE TRANSACTIONS ON COMMUNICATIONS Top Reviewer Award. He is currently serving as an Editor of the IEEE COMMUNICATIONS LETTERS.



**Quang Anh Tran** is an Associate Professor of Information Technology and the Vice President of Posts and Telecommunications Institute of Technology. In 2003 he finished his Ph.D. at Tsinghua University, from where he also received a Master degree in 2000. He finished his Bachelor at Huazhong University of Science and Technology in 1997. His research interests include Network security, Intrusion detection, Anti-spam, SMS spam filtering, Support vector machines, Evolutionary algorithms, Field-programmable gates array (FPGA).