

On the Security of Cognitive Radio Networks

Maged Elkashlan, *Member, IEEE*, Lifeng Wang, *Student Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, George K. Karagiannidis, *Fellow, IEEE*, and Arumugam Nallanathan, *Senior Member, IEEE*

Abstract—Cognitive radio has emerged as an essential recipe for future high-capacity high-coverage multi-tier hierarchical networks. Securing data transmission in these networks is of utmost importance. In this paper, we consider the cognitive wiretap channel and propose multiple antennas to secure the transmission at the physical layer, where the eavesdropper overhears the transmission from the secondary transmitter to the secondary receiver. The secondary receiver and the eavesdropper are equipped with multiple antennas, and passive eavesdropping is considered where the channel state information of the eavesdropper's channel is not available at the secondary transmitter. We present new closed-form expressions for the exact and asymptotic secrecy outage probability. Our results reveal the impact of the primary network on the secondary network in the presence of a multi-antenna wiretap channel.

Index Terms—Cognitive radio, multiple antennas, physical layer security, wiretap channel.

I. INTRODUCTION

Future multi-tier heterogeneous networks have become more and more vulnerable to serious security attacks and security threats of eavesdropping. Due to the distributed nature of the broadcasting channel, security concerns are further escalated to the forefront and have taken on an increasingly important role in spectrum sharing networks. In underlay cognitive spectrum sharing networks, the primary network and the secondary network are allowed to transmit concurrently in the same spectrum [1, 2]. In such complex environments, securing and protecting the broadcast channel against eavesdropping is arguably a more challenging task. In addition, due to the dynamic nature of these environments, higher layer cryptographic authentication and identification have become expensive and vulnerable to attacks [3, 4].

In light of the aforementioned circumstances, there has been intense interest in physical layer security to secure data transmission without the need for complex cryptographic operations. Physical layer security is also a solution to support and supplement existing cryptographic protocols [5]. The fundamental principle is to strengthen the main channel of the legitimate receiver relative to the eavesdropper's channel for achieving perfect secrecy. Triggered by the rapid advances in multi-antenna techniques for 4G and beyond,

security enhancement in wiretap channels with multiple antennas has attracted widespread attention (e.g., [6–10] and the citations therein), where the transmitter, the receiver, and/or the eavesdropper are equipped with multiple antennas. Previous work in [6] considered the single-input multi-output (SIMO) wiretap channel and derived the secrecy outage probability with maximal ratio combining (MRC) at both the legitimate receiver and the eavesdropper. An extension of [6] to the practical scenario of multiple eavesdroppers was presented in [7]. Transmit antenna selection for security enhancement was introduced in [8, 9] as a low complexity cost-effective approach. More recently in [10], the secrecy outage probability was evaluated in the presence of an untrusted relay.

In particular, cognitive radio is envisioned as a promising technique to alleviate the scarcity of radio frequency spectrum, which is the most important radio resource of wireless networks. This can be done by allowing the unlicensed user to occupy the spectrum without causing harmful interference on the licensed user. Security is an important requirement for future 5G systems, and cognitive radio is no exception. Particularly, security of cognitive radio networks is critical as it is easily exposed to external threats [11–17]. The robust transmitter design via optimization for secure cognitive radio networks with and without perfect channel state information (CSI) was addressed in [11] and [12], respectively. In [13], security for the main channel was guaranteed by performing beamforming from a group of relays. In [14], relay selection was proposed for security constrained cognitive radio with a single eavesdropper. The proposed scheme selects a trusted relay to maximize the achievable secrecy rate subject to interference power constraints at the primary user (PU) under available channel knowledge. In [15], secure communications with untrusted secondary users in cognitive radio networks was proposed and the achievable secrecy rate was derived. In [16, 17], game theory was utilized to exploit the security aspect of cognitive radio networks. While the aforementioned laid a solid foundation to understand the role of physical layer security in cognitive radio networks, the impact of multi-antenna wiretap channels on cognitive spectrum sharing networks for passive eavesdropping is less well understood. In contrast to the aforementioned scenarios, we consider the passive eavesdropping scenario, where knowledge of the eavesdropper's channel is not known at the secondary transmitter. In such a scenario, perfect secrecy cannot be achieved, and as such the secrecy outage probability is an important performance metric used for system evaluation.

In this paper, we take into account the cognitive wiretap channel and determine the necessary conditions to secure the confidential message against eavesdropping. Passive eavesdropping is considered, where the channel state information of the eavesdropper's channel is not available at the secondary

Manuscript received August 11, 2013; revised November 29, 2013 and May 08, 2014; accepted September 01, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. M. Cenk Gursoy.

M. Elkashlan and L. Wang are with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, UK (email: { maged.elkashlan, lifeng.wang }@qmul.ac.uk).

T. Q. Duong is with Queen's University Belfast, UK (e-mail: trung.q.duong@qub.ac.uk).

G. K. Karagiannidis is with Aristotle University of Thessaloniki, Thessaloniki, Greece (e-mail: geokarag@auth.gr).

A. Nallanathan is with King's College London, London, UK (e-mail: arumugam.nallanathan@kcl.ac.uk).

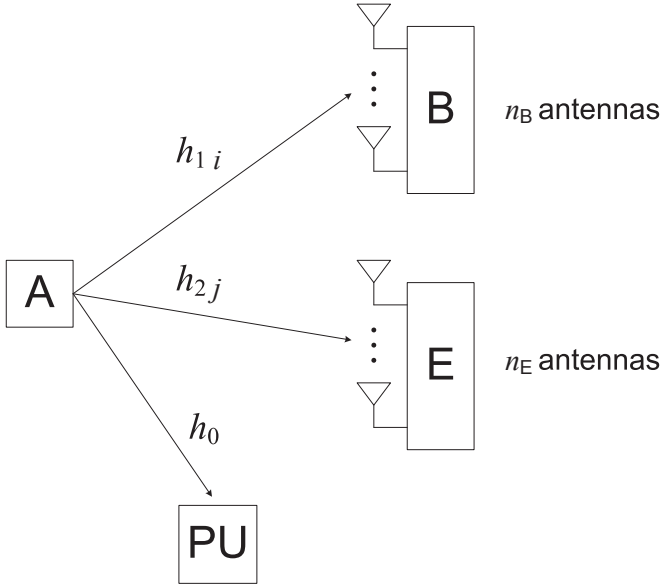


Fig. 1. A cognitive wiretap radio network.

transmitter. In such a cognitive wiretap channel, the secondary transmitter sends confidential messages to the secondary receiver in the presence of an eavesdropper. With this in mind, the secondary receiver is equipped with multiple antennas to promote secure data transmission without the need for a secret key or code. The eavesdropper is equipped with multiple antennas to promote successful eavesdropping. In this network, the interference power at the PU from the secondary transmitter must not exceed a peak interference power threshold. Our aim is to address fundamental questions surrounding the joint impact of two power constraints on the cognitive wiretap channel: 1) the maximum transmit power at the secondary transmitter, and 2) the peak interference power at PU. To address these constraints, we derive new closed-form expressions for the exact and asymptotic secrecy outage probability. Our expressions reveal important design insights into the impact of the primary network on the secondary network in cognitive wiretap radio networks.

II. SYSTEM AND CHANNEL MODELS

Consider a cognitive wiretap radio network, where the secondary transmitter Alice (A) communicates with the secondary receiver Bob (B) under the malicious attempt of the eavesdropper Eve (E) as shown in Fig. 1. We assume a cognitive network with underlay spectrum sharing which allows concurrent transmissions from PU and A in the same spectrum band. For this network, A transmits data to B, where B and E are equipped with multiple antennas n_B and n_E , respectively, whereas A and PU are equipped with a single antenna.

Both the primary channel and the secondary channel are assumed to undergo independent identically distributed (i.i.d.) Rayleigh fading, where the channel gains $\{h_{1i}\}_{i=1}^{n_B}$, $\{h_{2j}\}_{j=1}^{n_E}$, and h_0 are complex Gaussian random variables (RVs) with zero mean and variances Ω_1 , Ω_2 , and Ω_0 , respectively. We also assume that the main channel from A to B and the eavesdropper's channel from A to E are independent of each

other. We consider antenna selection¹ at B and E². Here, B and E select their strongest receive antennas based on perfect CSI estimation via pilot signals transmitted by A. Based on this, the instantaneous signal-to-noise ratio (SNR) in the main and the eavesdropper's channel are given by

$$\gamma_M = \max_{i=1, \dots, n_B} \frac{P_A}{N_0} |h_{1i}|^2, \quad \gamma_E = \max_{j=1, \dots, n_E} \frac{P_A}{N_0} |h_{2j}|^2, \quad (1)$$

respectively, where P_A is the transmit power at A and N_0 is the noise variance.

According to underlay cognitive radio transmission, the transmit power at A must be managed under a peak interference power threshold to guarantee reliable communication at PU. With this in mind, A is power-limited such that the maximum transmit power is P_t . As such, the transmit power at A is strictly constrained by the maximum transmit power P_t at A and the peak interference power I_p at PU according to

$$P_A = \min \left(\frac{I_p}{|h_0|^2}, P_t \right), \quad (2)$$

from which the instantaneous SNR at Bob and Eve in (1) are reexpressed as

$$\gamma_M = \min \left(\frac{\bar{\gamma}_p}{X}, \bar{\gamma}_0 \right) Y_M, \quad \gamma_E = \min \left(\frac{\bar{\gamma}_p}{X}, \bar{\gamma}_0 \right) Y_E, \quad (3)$$

respectively, where $\bar{\gamma}_p = I_p/N_0$, $\bar{\gamma}_0 = P_t/N_0$, $X = |h_0|^2$, $Y_M = \max_{i=1, \dots, n_B} |h_{1i}|^2$, and $Y_E = \max_{j=1, \dots, n_E} |h_{2j}|^2$.

III. SECRECY OUTAGE PROBABILITY

We focus on passive eavesdropping, where knowledge of the eavesdropper's channel is not known at A. In such a scenario, A has no choice but to encode the confidential data into codewords of a constant rate R_s [19]. Following the wiretap channel in [19, 20], A encodes a message block W^k into a codeword X^n , and the eavesdropper receives Y_w^n from the output of its channel. The equivocation rate of Eve is $R_e = H(W^k | Y_w^n)/n$. We assume slow block fading for the main channel and the eavesdropper's channel, where the fading coefficients are constant during a codeword transmission. Taking this into account, we define the secrecy rate as [19]

$$C_s = \begin{cases} C_M - C_E & \text{if } \gamma_M > \gamma_E \\ 0 & \text{if } \gamma_M \leq \gamma_E \end{cases}, \quad (4)$$

where $C_M = \log_2(1 + \gamma_M)$ is the capacity of the main channel and $C_E = \log_2(1 + \gamma_E)$ is the capacity of the eavesdropper's channel. The secrecy rate C_s in (4) is the maximum achievable perfect secrecy rate R such that $R_e = R$ [19, 20]. In passive eavesdropping, if $R_s \leq C_s$, perfect secrecy is guaranteed. Otherwise, if $R_s > C_s$, information-theoretic security is

¹It is well-known that using antenna selection can achieve the full diversity gain with a less number of RF electronics for each branch compared to maximal ratio combining [18].

²In commercial wireless applications, the eavesdropper may be subject to the same resource constraints as the legitimate receiver. Specifically, it may be limited to a single radio frequency (RF) chain due to size and complexity limitations, as was considered in [7] and [9].

compromised. As such, the secrecy outage probability is the probability that C_s falls below R_s

$$P_{\text{out}} = \Pr(C_s < R_s) = \Pr(\gamma_M \leq \gamma_E) + \underbrace{\Pr(\gamma_M > \gamma_E)}_{\mathcal{A}} \underbrace{\Pr(C_s < R_s | \gamma_M > \gamma_E)}_{\mathcal{I}}. \quad (5)$$

In order to evaluate the term \mathcal{I} , we first rewrite C_s in (4) as

$$C_s = \log_2 \left(\frac{1 + \gamma_M}{1 + \gamma_E} \right) < R_s, \quad (6)$$

which is equivalent to

$$\gamma_M < 2^{R_s} (1 + \gamma_E) - 1 = \epsilon(\gamma_E). \quad (7)$$

Then \mathcal{I} can be written as

$$\mathcal{I} = \frac{1}{\mathcal{A}} \int_0^\infty \int_0^\infty \int_{\gamma_E}^{\epsilon(\gamma_E)} f_{\gamma_M | \{X=x\}}(\gamma_M) f_{\gamma_E | \{X=x\}}(\gamma_E) \times f_X(x) d\gamma_M d\gamma_E dx. \quad (8)$$

where $f_X(x)$ is the PDF of X , $f_{\gamma_A | \{X=x\}}(\cdot)$ is the PDF of γ_A conditioned on X , $\gamma_A \in \{\gamma_M, \gamma_E\}$. By exchanging the variable in the limits of inner integral \mathcal{I} , we obtain

$$\mathcal{I} = \frac{\mathcal{I}_1 - \mathcal{I}_2}{\mathcal{A}}, \quad (9)$$

where \mathcal{I}_1 and \mathcal{I}_2 are respectively given as

$$\mathcal{I}_1 = \int_0^\infty \int_0^\infty \int_0^{\epsilon(\gamma_E)} f_{\gamma_M | \{X=x\}}(\gamma_M) f_{\gamma_E | \{X=x\}}(\gamma_E) f_X(x) d\gamma_M d\gamma_E dx \quad (10)$$

and

$$\mathcal{I}_2 = 1 - \mathcal{A}. \quad (11)$$

Putting together (5), (9), (10), and (11), we get

$$P_{\text{out}} = \int_0^\infty \int_0^\infty F_{\gamma_M | \{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E | \{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx. \quad (12)$$

where $F_{\gamma_M | \{X=x\}}(\cdot)$ is the CDF of γ_M conditioned on X .

For ease of exposition and mathematical tractability, we denote $\bar{\gamma}_1 = \bar{\gamma}_0 \Omega_1 = \frac{\bar{\gamma}_p \Omega_1}{\sigma}$ and $\bar{\gamma}_2 = \bar{\gamma}_0 \Omega_2 = \frac{\bar{\gamma}_p \Omega_2}{\sigma}$ with $\sigma = \frac{l_p}{P_t}$. Here, $\bar{\gamma}_1$ represents the maximum possible average SNR of the channel between A and B, and $\bar{\gamma}_2$ represents the maximum possible average SNR of the channel between A and E.

A. Exact Secrecy Outage Probability

In this subsection, we present a novel closed-form expression for the exact secrecy outage probability, as given in the following theorem.

Theorem 1: The exact secrecy outage probability of the proposed cognitive multi-antenna wiretap channel is given by (13) at the top of the next page,

Proof: See Appendix A. ■

It is worth noting that (13) involves only finite summations of exponentials, powers, and exponential integral functions, thus can be calculated in closed-form. This expression

serves as a prerequisite for other secrecy metrics such as the probability of non-zero secrecy capacity, calculated as $\Pr(C_s > 0) = \Pr(\gamma_M > \gamma_E) = 1 - P_{\text{out}}(0)$. In addition, considering the special case of a single antenna transmitter and a single antenna receiver, our secrecy outage probability expression without interference power constraint reduces to [7, eq. (11)]. Our secrecy outage probability expression without interference power constraint also reduces to [9, eq. 34] with a single transmit antenna in Rayleigh fading.

B. Asymptotic Secrecy Outage Probability

We derive a new asymptotic expression for the secrecy outage probability at high SNR operating regions. The main driver is to identify the key players that control network behavior. The aim is to determine the impact of PU on A in the presence of a multi-antenna wiretap channel. In particular, we are interested in the joint impact of the maximum transmit power P_t at A and the peak interference power l_p at PU on the secrecy outage probability. Other key network players of interest are the number of antennas n_B at B and the number of antennas n_E at E. With this in mind, we address the interference power constraint of l_p proportional to P_t according to $l_p = \sigma P_t$, where σ is a positive constant. Based on Appendix A, we first obtain the first order expansion of $F_{\gamma_M | \{X\}}(\gamma)$ conditioned on X as

$$F_{\gamma_M | \{X\}}(\gamma) = \begin{cases} \left(\frac{\gamma}{\bar{\gamma}_1} \right)^{n_B}, & X \leq \frac{\bar{\gamma}_p}{\bar{\gamma}_0} \\ \left(\frac{X}{\bar{\gamma}_1 \sigma} \gamma \right)^{n_B}, & X > \frac{\bar{\gamma}_p}{\bar{\gamma}_0} \end{cases}, \quad (14)$$

Substituting (14) and $f_{\gamma_E | \{X=x\}}(\gamma_E)$ and $f_X(x)$ into (12), and using the binomial expansion, the asymptotic secrecy outage probability is calculated as

$$P_{\text{out}}^\infty = \left(1 - e^{-\frac{\bar{\gamma}_p}{\bar{\gamma}_0 \Omega_0}} \right) \sum_{i=0}^{n_B} \binom{n_B}{i} \left(\frac{2^{R_s} - 1}{\bar{\gamma}_1} \right)^{n_B - i} \left(\frac{2^{R_s}}{\bar{\gamma}_1} \right)^i \sum_{j=0}^{n_E - 1} \binom{n_E - 1}{j} \frac{n_E}{\bar{\gamma}_2} (-1)^j \int_0^\infty (\gamma_E)^i e^{-\frac{(j+1)\gamma_E}{\bar{\gamma}_2}} d\gamma_E + \sum_{i=0}^{n_B} \binom{n_B}{i} \left(\frac{2^{R_s} - 1}{\bar{\gamma}_1 \sigma} \right)^{n_B - i} \left(\frac{2^{R_s}}{\bar{\gamma}_1 \sigma} \right)^i \sum_{j=0}^{n_E - 1} \binom{n_E - 1}{j} \frac{n_E}{\bar{\gamma}_2 \sigma} (-1)^j \frac{1}{\Omega_0} \int_{\frac{\bar{\gamma}_p}{\bar{\gamma}_0}}^\infty e^{-\frac{x}{\bar{\gamma}_0}} \int_0^\infty x^{n_B + 1} (\gamma_E)^i e^{-\frac{(j+1)\gamma_E}{\bar{\gamma}_2 \sigma} x} d\gamma_E dx \quad (15)$$

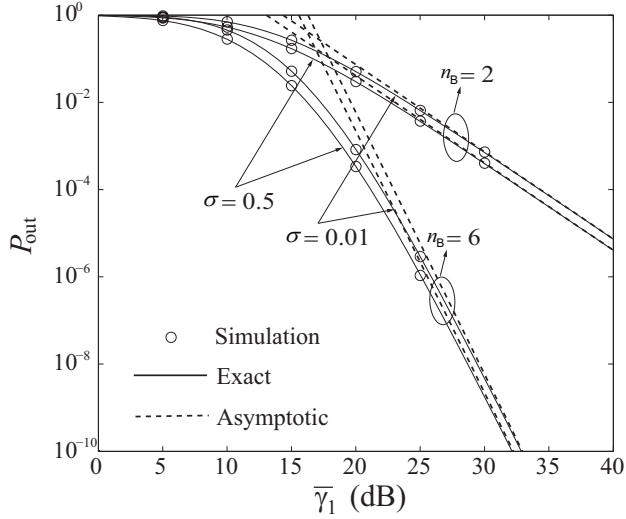
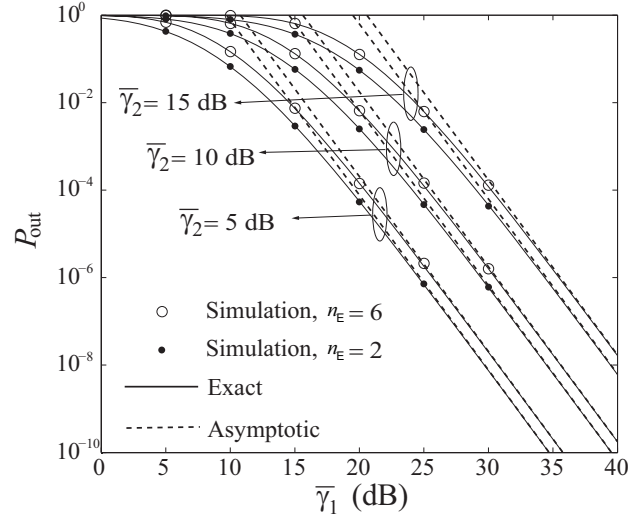
Employing [21, eq. (3.351.3)] given by $\int_0^\infty x^n e^{-\mu x} dx = \frac{\Gamma(n+1)}{\mu^{n+1}}$, we can evaluate the integrals in (15) and derive the secrecy outage probability as

$$P_{\text{out}}^\infty = (G_a \bar{\gamma}_1)^{-G_d} + O\left(\bar{\gamma}_1^{-G_d}\right), \quad (16)$$

where the secrecy diversity order is

$$G_d = n_B \quad (17)$$

$$\begin{aligned}
 P_{\text{out}} = & \left(1 - e^{-\frac{\sigma}{\Omega_0}}\right) \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_2} (-1)^{i+j} e^{-\frac{i(2^{R_s}-1)}{\bar{\gamma}_1}} \left(\frac{i2^{R_s}}{\bar{\gamma}_1} + \frac{j+1}{\bar{\gamma}_2}\right) \\
 & + \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_2 \sigma} (-1)^{i+j} \frac{1}{\Omega_0} \left(\frac{i2^{R_s}}{\bar{\gamma}_1} + \frac{j+1}{\bar{\gamma}_2 \sigma}\right)^{-1} \frac{e^{-\frac{\sigma}{\Omega_0} - \frac{i(2^{R_s}-1)}{\bar{\gamma}_1}}}{\frac{1}{\Omega_0} + \frac{i(2^{R_s}-1)}{\bar{\gamma}_1 \sigma}}, \quad (13)
 \end{aligned}$$


 Fig. 2. Secrecy outage probability with $\bar{\gamma}_2 = 10$ dB and $n_E = 2$.

 Fig. 3. Secrecy outage probability with $\sigma = 0.1$ and $n_B = 4$.

and the secrecy array gain is

$$\begin{aligned}
 G_a = & \left[\left(1 - e^{-\frac{\sigma}{\Omega_0}}\right) \sum_{i=0}^{n_B} \binom{n_B}{i} (2^{R_s} - 1)^{n_B-i} 2^{R_s i} \right. \\
 & \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} n_E \bar{\gamma}_2^i (-1)^j \frac{\Gamma(i+1)}{(j+1)^{i+1}} + \sum_{i=0}^{n_B} \binom{n_B}{i} \\
 & (2^{R_s} - 1)^{n_B-i} \sigma^{-n_B} 2^{R_s i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} n_E (\bar{\gamma}_2 \sigma)^i \\
 & \left. (-1)^j (\Omega_0)^{n_B-i} \frac{\Gamma(i+1)}{(j+1)^{i+1}} \Gamma\left(n_B - i, \frac{\sigma}{\Omega_0}\right) \right]^{-\frac{1}{n_B}}, \quad (18)
 \end{aligned}$$

where $\Gamma(\cdot, \cdot)$ is the incomplete gamma function [21, eq. (8.350.2)].

IV. NUMERICAL RESULTS

Numerical examples are provided to highlight the impact of the primary network on the secondary network in the presence of a multi-antenna wiretap channel. The exact and asymptotic curves are obtained from (13) and (16), respectively. The exact curves are in precise agreement with the Monte Carlo simulations. We also see that the asymptotic curves well approximate the exact curves at high SNR. The asymptotic curves accurately predict the secrecy diversity order and the secrecy array gain. Throughout this section, we assume unity variance $\Omega_0 = 1$ and expected secrecy rate $R_s = 0.1$ bit/s/Hz.

Fig. 2 plots the secrecy outage probability versus $\bar{\gamma}_1$ for different σ and different n_B . According to (17), we see that

the secrecy diversity order increases with n_B , which in turn decreases the secrecy outage probability. We also see that the secrecy outage probability decreases with σ . This is due to relaxing the peak interference power constraint $l_p = \sigma P_t$, which in turn increases transmit power P_A , as indicated by (2). This can also be explained by the fact that the secrecy array gain in (18) increases with increasing σ .

Fig. 3 plots the secrecy outage probability versus $\bar{\gamma}_1$ for different $\bar{\gamma}_2$ and different n_E . The parallel slopes of the asymptotes confirm that the secrecy diversity order is independent of $\bar{\gamma}_2$ and n_E , as indicated in (17). Note the secrecy outage probability increases with increasing $\bar{\gamma}_2$ and n_E . This confirms that the secrecy array gain in (18) is a decreasing function of $\bar{\gamma}_2$ and n_E .

V. CONCLUSIONS

We proposed physical layer security enhancement in cognitive multi-antenna wiretap channels. In an effort to assess the secrecy performance in passive eavesdropping, we adopt the secrecy outage probability as a useful performance measure. We derived new closed-form expressions for the exact and asymptotic secrecy outage probability. Based on these, we revealed important design insights into the interplay between two power constraints, namely the maximum transmit power at the secondary network and the peak interference power at the primary network. The impact of these constraints on the cognitive wiretap channel was showcased.

APPENDIX A: PROOF OF THEOREM 1

We first provide the CDF and PDF of $Y = \max_{n=1, \dots, N} Y_n$, where Y_n is i.i.d. exponential RV with parameter Ω_Y , which can be written as

$$F_Y(y) = \sum_{n=0}^N \binom{N}{n} (-1)^n e^{-\frac{ny}{\Omega_Y}} \quad (19)$$

and

$$f_Y(y) = \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{N}{\Omega_Y} (-1)^n e^{-\frac{(n+1)y}{\Omega_Y}}. \quad (20)$$

In addition, $f_X(x) = \frac{1}{\Omega_0} e^{-\frac{x}{\Omega_0}}$.

Based on (3), we note that when $X \leq \frac{\bar{\gamma}_p}{\bar{\gamma}_0}$, $\gamma_M = \bar{\gamma}_0 Y_M$, $\gamma_E = \bar{\gamma}_0 Y_E$, and when $X > \frac{\bar{\gamma}_p}{\bar{\gamma}_0}$, $\gamma_M = \frac{\bar{\gamma}_p}{X} Y_M$, $\gamma_E = \frac{\bar{\gamma}_p}{X} Y_E$. Hence, the secrecy outage probability in (12) can be calculated as

$$\begin{aligned} P_{\text{out}} = & \underbrace{\int_0^{\frac{\bar{\gamma}_p}{\bar{\gamma}_0}} \int_0^\infty F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx}_{\mathcal{J}_1} \\ & + \underbrace{\int_{\frac{\bar{\gamma}_p}{\bar{\gamma}_0}}^\infty \int_0^\infty F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx}_{\mathcal{J}_2}. \end{aligned} \quad (21)$$

Based on (19), for $X \leq \frac{\bar{\gamma}_p}{\bar{\gamma}_0}$, we have

$$\begin{aligned} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) &= \sum_{i=0}^{n_B} \binom{n_B}{i} (-1)^i e^{-\frac{i\epsilon(\gamma_E)}{\bar{\gamma}_0 \Omega_1}}, \\ f_{\gamma_E|\{X=x\}}(\gamma_E) &= \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_0 \Omega_2} (-1)^j e^{-\frac{(j+1)\gamma_E}{\bar{\gamma}_0 \Omega_2}}. \end{aligned} \quad (22)$$

By substituting (22) into \mathcal{J}_1 of (21), \mathcal{J}_1 can be derived as

$$\begin{aligned} \mathcal{J}_1 &= \int_0^{\frac{\bar{\gamma}_p}{\bar{\gamma}_0}} f_X(x) dx \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_0 \Omega_2} (-1)^{i+j} \\ &\quad \times \int_0^\infty e^{-\frac{i\epsilon(\gamma_E)}{\bar{\gamma}_0 \Omega_1} - \frac{(j+1)\gamma_E}{\bar{\gamma}_0 \Omega_2}} d\gamma_E \\ &= \left(1 - e^{-\frac{\bar{\gamma}_p}{\bar{\gamma}_0 \Omega_0}}\right) \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_0 \Omega_2} (-1)^{i+j} \\ &\quad \times e^{-\frac{i(2^{R_s}-1)}{\bar{\gamma}_0 \Omega_1}} \left(\frac{i2^{R_s}}{\bar{\gamma}_0 \Omega_1} + \frac{j+1}{\bar{\gamma}_0 \Omega_2}\right). \end{aligned} \quad (23)$$

For $X > \frac{\bar{\gamma}_p}{\bar{\gamma}_0}$, we have

$$\begin{aligned} F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) &= \sum_{i=0}^{n_B} \binom{n_B}{i} (-1)^i e^{-\frac{i\epsilon(\gamma_E)}{\bar{\gamma}_p \Omega_1}}, \\ f_{\gamma_E|\{X=x\}}(\gamma_E) &= \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_p \Omega_2} (-1)^j x e^{-\frac{(j+1)\gamma_E}{\bar{\gamma}_p \Omega_2}}. \end{aligned} \quad (24)$$

By substituting (24) into \mathcal{J}_2 of (21), \mathcal{J}_2 can be derived as

$$\begin{aligned} \mathcal{J}_2 &= \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_p \Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \\ &\quad \int_{\frac{\bar{\gamma}_p}{\bar{\gamma}_0}}^\infty e^{-\frac{x}{\Omega_0}} \int_0^\infty x e^{-\frac{i\epsilon(\gamma_E)}{\bar{\gamma}_p \Omega_1} x - \frac{(j+1)\gamma_E}{\bar{\gamma}_p \Omega_2} x} d\gamma_E dx \\ &= \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_p \Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \\ &\quad \int_{\frac{\bar{\gamma}_p}{\bar{\gamma}_0}}^\infty x e^{-\frac{x}{\Omega_0}} e^{-\frac{i(2^{R_s}-1)}{\bar{\gamma}_p \Omega_1} x} \int_0^\infty e^{-\frac{i2^{R_s} x \gamma_E}{\bar{\gamma}_p \Omega_1} - \frac{(j+1)\gamma_E}{\bar{\gamma}_p \Omega_2} x} d\gamma_E dx \\ &= \sum_{i=0}^{n_B} \binom{n_B}{i} \sum_{j=0}^{n_E-1} \binom{n_E-1}{j} \frac{n_E}{\bar{\gamma}_p \Omega_2} (-1)^{i+j} \frac{1}{\Omega_0} \\ &\quad \times \left(\frac{i2^{R_s}}{\bar{\gamma}_p \Omega_1} + \frac{j+1}{\bar{\gamma}_p \Omega_2}\right)^{-1} \frac{e^{-\frac{\bar{\gamma}_p}{\bar{\gamma}_0 \Omega_0} - \frac{i(2^{R_s}-1)}{\bar{\gamma}_0 \Omega_1}}}{\frac{1}{\Omega_0} + \frac{i(2^{R_s}-1)}{\bar{\gamma}_p \Omega_1}}. \end{aligned} \quad (25)$$

Substituting (23) and (25) into (21), we get the desired result (13).

REFERENCES

- [1] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 471–487, Feb. 2007.
- [2] A. Goldsmith, S. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May. 2009.
- [3] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
- [4] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.
- [5] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, pp. 40–47, Feb. 2012.
- [6] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.
- [7] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M -antenna eavesdroppers: Characterization of the outage probability and ϵ -outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.
- [8] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jan. 2012.
- [9] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
- [10] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.
- [11] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, 2010.
- [12] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multi-antenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, 2011.
- [13] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," in *Proc of 45th Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, Mar. 2011, pp. 1–5.
- [14] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Communications*, vol. 6, no. 16, pp. 2676–2687, 2012.
- [15] H. Jeon, S. W. McLaughlin, and J. Ha, "Secure communications with untrusted secondary users in cognitive radio networks," in *Proc of IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, Dec. 2012, pp. 1072–1078.

- [16] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, 2011.
- [17] 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.
- [18] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 4, pp. 1312–1321, July 2005.
- [19] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
- [20] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
- [21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, C.A.: Academic Press, 2007.