OPEN ACCESS

KING'S College LONDON

King's Research Portal

DOI:
10.1016/j.phycom.2016.05.003

Document Version
Peer reviewed version

Link to publication record in King's Research Portal

Citation for published version (APA):
Nguyen, N-P., Thanh, T. L., Duong, T. Q., & Nallanathan, A. (2017). Secure Communications in Cognitive Underlay Networks over Nakagami-m Channel. PHYCOM: Physical Communication, 25(2), 610-618. https://doi.org/10.1016/j.phycom.2016.05.003

Citing this paper
Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights
Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

•Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
•You may not further distribute the material or use it for any profit-making activity or commercial gain
•You may freely distribute the URL identifying the publication in the Research Portal

Take down policy
If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 23. May. 2019

Secure Communications in Cognitive Underlay Networks over Nakagami-m Channel

Nam-Phong Nguyen, Tu Lam Thanh, Trung Q. Duong, and A. Nallanathan

Abstract

In this paper, the secure communication of a cognitive radio network (CRN) over Nakagami-m fading channel is investigated. An underlay protocol is used in the considered network, where the unlicensed users or secondary users (SUs) can operate simultaneously with the primary users (PUs) in the same spectrum bands providing that the transmit power of the SUs is constrained by not only the maximum tolerance interference at the PU's receiver but also the maximum transmit power at the SU's transmitter. The exact closed-form expressions of important secure performance metrics, i.e., secrecy outage probability (SOP) and secrecy capacity (SC), are derived. In addition, to give a deep insight into the secure performance trends, the asymptotic expression of the SOP is also obtained when the average signal-to-noise ratio (SNR) of the legitimate channel is high. It is proven that the considered system achieves full diversity gain regardless of the number of antennas at the eavesdropper. Finally, the correctness of our mathematical framework is verified by Monte Carlo simulations.

Index Terms

Physical layer security, cognitive radio networks, secrecy outage probability, wiretap channel, multiple antennas.

I. Introduction

Nowadays, the scarcity of spectrum resources has become more and more severe owing to the exponential growth in the number of wireless devices and services such as tablets, smart phones, wearable devices or video conferences. Meanwhile, according to Federal Communications Commission (FCC), most of the licensed spectrum bands are underutilized [1]. As a consequence,

N.-P. Nguyen and T. Q. Duong are with Queen's University Belfast, UK (email: {pnguyen04, trung.q.duong}@qub.ac.uk).

T. L. Thanh is with Posts and Telecommunications Institute of Technology, Vietnam (e-mail: thanhtl@ptithcm.edu.vn).

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

it is essential to find out a new technology that can not only overcome the inefficiency of the current radio frequency usage but also be compatible with the current spectrum management policies and legacy wireless systems. Fortunately, cognitive radio (CR), which was introduced by Mitola [2], holds tremendous potential for coping with these challenges by allowing unlicensed users or secondary users (SUs) to access licensed spectrums of primary users (PUs) under the condition that no harmful interference is inflicted on the PUs. The spectrum underlay scheme is one of the possible ways to enable CR networks, in which the SUs and the PUs are allowed transmitting concurrently as long as the interference temperature at the PUs is not exceeded a threshold. Therefore, this scheme can provide the reliable communications in the primary networks regardless of the secondary networks operation [3]. Nevertheless, it also contains some drawbacks such as the short coverage area or the difficulties in ensuring reliable transmission at the secondary networks due to the transmit power constraint. Moreover, it is worth noting that the network is vulnerable to malicious attacks from both other SUs and PUs as a result of the concurrent usage of the same frequency bands and the broadcasting nature of wireless channels.

To overcome the challenge of unreliable communications, space diversity such as multiple-input multiple-output (MIMO) associated with diversity combining, i.e., maximal ratio combining or selection combining, is used in practice to deal with small transmit power. Besides, in the conventional wireless communications, to protect the confidential messages against eavesdropping, upper layer cryptographic approaches are typically adopted. However, it has been proven in [4], [5] that these upper layer cryptographic scheme are more expensive and unreliable. Physical layer security, which exploits the characteristics of wireless channels to improve transmission security [6], has recently become an interesting solution to support the existing cryptography protocols [7]. As a result, the secure performance of physical layer security combined with diversity combining in multi-antenna wiretap channels, where the transmitters, the receivers and/or the eavesdroppers deploy multiple antennas, has attracted widespread attention in the research community (e.g., [8]–[12] and the citations therein).

In [8], the authors derived the secrecy outage probability (SOP) using the MRC technique at both the legitimate receiver and the eavesdropper in the single-input multiple-output (SIMO) wiretap channel. The results showed that the SOP can be significantly improved once the main channel gain goes to infinity. An extension of [8] with multiple eavesdroppers was presented in [9]. In [10] and [11], transmit antenna selection was presented as a cost-effective method to enhance information security. Recently, the SOP was studied in [12] under the assumption that the

relay is untrusted. In [13], the authors proposed a relay selection scheme for security constrained in the CRNs with an eavesdropper. In [14], the authors proposed four different relay selection schemes to enhance the security in the CRNs, i.e., random relay and random jammer, random jammer and best relay, best relay and best jammer, and best relay and no jammer. The authors in [15] compared the security performance in the CRNs of different channel state information based relay selection schemes, i.e., optimal relay selection, sub-optimal relay selection, and partial relay selection. While all of the above-mentioned works focused on understanding the role of physical layer security in either the conventional wireless networks or single-antenna at the eavesdropper and/or the legitimate receiver, the effect of multi-antenna wiretap channels on passive eavesdropping cognitive underlay networks is still not well understood.

Recently, in [16], a cognitive wiretap radio network over Rayleigh fading channels, where the channel state information (CSI) of the eavesdropper was not available at the secondary transmitter, was investigated under the joint constraint of the maximal transmit power at the SU and the maximal interference at the PU. However, Rayleigh fading may not be useful in a wide range of fading scenarios. Taking this into consideration, our work aims to study a comprehensive secure performance inspired by [16] over independent and identically distributed (i.i.d.) Nakagami-m fading channels. The choice of Nakagami-m fading, which is a general case of Rayleigh fading, makes our analysis more adaptable to different fading scenarios. Moreover, in this work, the most important secure performance metric in physical layer security, i.e., secrecy capacity, is investigated along with the SOP. In particular, the exact closed-form expressions of both SOP and SC are derived. Our work shows that the secrecy capacity can be enhanced significantly by increasing either the number of antennas at the legitimate receiver or the severity parameter of the main channel.

The rest of this paper is organized as follows. System and channel models are presented in section II. An exact closed-form expression of the system SOP is described in section III while the asymptotic SOP is studied in section IV. Section V introduces the expression of the system secrecy capacity. Numerical results based on Monte-Carlo methods are presented to confirm the correctness of our analysis in section VI. Finally, we conclude this paper in section VII.

II. System and Channel Models

Let us consider a cognitive underlay wiretap network consisting of a secondary transmitter $\mathbf{A}$, a secondary receiver $\mathbf{B}$, an eavesdropper $\mathbf{E}$ co-allocated with one primary user $\mathbf{P}$, as shown

in Fig. 1. In particular, $\mathbf{A}$ acts as a transmitter and tries to send information to $\mathbf{B}$ under the malicious attempt of the eavesdropper $\mathbf{E}$. It is assumed that both $\mathbf{B}$ and $\mathbf{E}$ are equipped with multiple antennas, while $\mathbf{A}$ and $\mathbf{P}$ use single antenna. The number of antennas at $\mathbf{B}$ and $\mathbf{E}$ are denoted as N_{B} and N_{E}, respectively. We further define $\{h_{\mathsf{B}_t}\}_{t=1}^{N_{\mathsf{B}}}, \{h_{\mathsf{E}_w}\}_{w=1}^{N_{\mathsf{E}}}$,and h_{P} as the channel gains from $\mathbf{A}$ to $\mathbf{B}$, $\mathbf{A}$ to $\mathbf{E}$, and $\mathbf{A}$ to $\mathbf{P}$, respectively. In this cognitive underlay network, the transmit power of the secondary transmitter $\mathbf{A}$ is constrained by not only its maximum transmit power $\mathcal{P}_{\mathsf{m}}$ but also the maximum tolerance interference power at the primary receiver $\mathcal{I}_{\mathsf{p}}$. Mathematically, we have [17]

$$\mathcal{P}_{\mathsf{A}} = \min\left(\frac{\mathcal{I}_{\mathsf{p}}}{|h_{\mathsf{P}}|^2}, \mathcal{P}_{\mathsf{m}}\right). \tag{1}$$

The secondary receiver $\mathbf{B}$ as well as the eavesdropper $\mathbf{E}$ uses selection combining technique to combine incoming signals due to low complexity and high performance. As a result, the instantaneous SNRs at $\mathbf{B}$ γ_{B} and $\mathbf{E}$ γ_{E} are given as

$$\begin{aligned}\gamma_{\mathsf{B}} &= \max_{t\in\{1,N_{\mathsf{B}}\}} \frac{\mathcal{P}_{\mathsf{A}}}{N_0}|h_{\mathsf{B}_t}|^2,\\ \gamma_{\mathsf{E}} &= \max_{w\in\{1,N_{\mathsf{E}}\}} \frac{\mathcal{P}_{\mathsf{A}}}{N_0}|h_{\mathsf{E}_w}|^2,\end{aligned} \tag{2}$$

where N_0 is the noise variance. To facilitate the notation, let us denote $\gamma_p = \frac{\mathcal{I}_{\mathsf{p}}}{N_0}$ and $\gamma_0 = \frac{\mathcal{P}_{\mathsf{m}}}{N_0}$, where γ_0 is the average SNR of the main channel. Without loss of generality, we assume that $\gamma_p = \sigma\gamma_0$, where σ is a positive constant [17]. As such, we can rewrite γ_{B} and γ_{E} as

$$\begin{aligned}\gamma_{\mathsf{B}} &= \gamma_0 \min\left(\frac{\sigma}{|h_{\mathsf{P}}|^2}, 1\right) \times \max_{t\in\{1,N_{\mathsf{B}}\}} |h_{\mathsf{B}_t}|^2,\\ \gamma_{\mathsf{E}} &= \gamma_0 \min\left(\frac{\sigma}{|h_{\mathsf{P}}|^2}, 1\right) \times \max_{w\in\{1,N_{\mathsf{E}}\}} |h_{\mathsf{E}_w}|^2.\end{aligned} \tag{3}$$

In this paper, all the channels are characterized by i.i.d. Nakagami-m flat fading. Therefore, the power gains $|h_{\mathsf{B}_t}|^2$, $|h_{\mathsf{E}_w}|^2$, and $|h_{\mathsf{P}}|^2$ follow the gamma distribution with mean power λ_{B}, λ_{E}, λ_{P} and severity parameters m_{B}, m_{E}, m_{P}, respectively. Without loss of generality, we assume that m_{B}, m_{E}, m_{P} are integers. The cumulative distribution function (CDF) and the probability density function (PDF) of the random variable (RV) Y, where Y=$\{|h_{\mathsf{B}_t}|^2, |h_{\mathsf{E}_w}|^2, |h_{\mathsf{P}}|^2\}$, are shown respectively as follows:

$$F_Y(y) = 1 - \frac{\Gamma\left(m_Y, \frac{y}{\Omega_Y}\right)}{\Gamma(m_Y)}, \tag{4}$$

$$f_Y(y) = \frac{y^{m_Y-1}}{\Gamma(m_Y)(\Omega_Y)^{m_Y}} \exp\left(-\frac{y}{\Omega_Y}\right), \tag{5}$$

where $\Omega_Y = \frac{\lambda_y}{m_Y}$ and $\Gamma(\cdot,\cdot)$ is the incomplete gamma function [18, Eq. (8.352.6)].

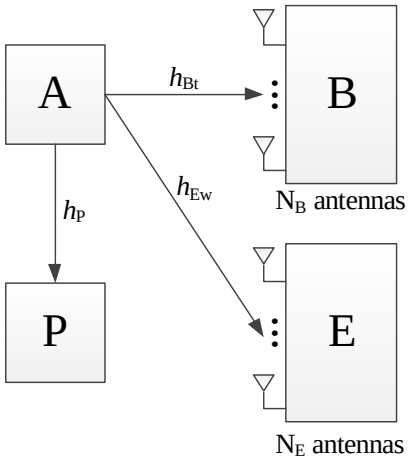

Fig. 1: Cognitive spectrum sharing system model.

III. Exact Secrecy Outage Probability

In this paper, we focus on the case of passive eavesdropping. Therefore, the eavesdropper's CSI is unknown at **A**. In this situation, the confidential data at **A** just can be encoded into code words with constant rate of R_{S}. We assume slow fading for both the main channel and the eavesdropping channel, which makes fading coefficients remain the same during one transmission block and independently change in another. Taking this into account, we define the secrecy rate as [19]

$$C_{\mathsf{S}} = \begin{cases} C_{\mathsf{B}} - C_{\mathsf{E}} & \text{if } \gamma_{\mathsf{B}} > \gamma_{\mathsf{E}} \\ 0 & \text{if } \gamma_{\mathsf{B}} \leq \gamma_{\mathsf{E}} \end{cases}, \tag{6}$$

where the capacity of the main channel and the eavesdropping channel are respectively defined as

$$\begin{aligned} C_{\mathsf{B}} &= \log_2(1+\gamma_{\mathsf{B}}), \\ C_{\mathsf{E}} &= \log_2(1+\gamma_{\mathsf{E}}). \end{aligned} \tag{7}$$

In passive eavesdropping, if $R_{\mathsf{S}} \leq C_{\mathsf{S}}$, perfect secrecy is guaranteed. In the other case, if $R_{\mathsf{S}} > C_{\mathsf{S}}$, information-theoretic security is compromised. Therefore, the secrecy outage probability

(SOP) is the probability that C_{S} falls below R_{S}. As such, the SOP of the system can be given as [19]

$$P_{\text{out}} = \Pr\left(C_{\mathsf{S}} < R_{\mathsf{S}}\right). \tag{8}$$

From (6) and (7), C_{S} can be rewritten as

$$C_{\mathsf{S}} = \log_2\left(\frac{1+\gamma_{\mathsf{B}}}{1+\gamma_{\mathsf{E}}}\right). \tag{9}$$

By substituting (9) into (8), the SOP can be written as

$$\begin{aligned} P_{\text{out}} =& \Pr\left(C_{\mathsf{S}} < R_{\mathsf{S}}\right) \\ =& \Pr\left(\log_2\left(\frac{1+\gamma_{\mathsf{B}}}{1+\gamma_{\mathsf{E}}}\right) < R_{\mathsf{S}}\right) \\ =& \Pr\left(\frac{1+\gamma_{\mathsf{B}}}{1+\gamma_{\mathsf{E}}} < 2^{R_{\mathsf{S}}}\right) \\ =& F_{\hat{\gamma}}\left(\gamma_{\text{th}}\right), \end{aligned} \tag{10}$$

where $\gamma_{\text{th}} = 2^{R_{\mathsf{S}}}$ and $\hat{\gamma} = \frac{1+\gamma_{\mathsf{B}}}{1+\gamma_{\mathsf{E}}}$.

From (10), we see that to obtain the SOP of the considered system, we need to find out the CDF of $\hat{\gamma}$ which is given in the following Lemma.

Lemma 1: The CDF of $\hat{\gamma}$ is given as follows:

$$\begin{aligned} F_{\hat{\gamma}}\left(\gamma\right) = 1 + \sum_{t=1}^{N_{\mathsf{B}}} \sum_{l_b=0}^{t(m_b-1)} \sum_{w=1}^{N_{\mathsf{E}}} \sum_{l_e=0}^{w(m_e-1)} \sum_{k_b=0}^{l_b} \binom{l_b}{k_b} \mathcal{A}_t \mathcal{A}_w c_{l_b} c_{l_e} (\gamma-1)^{l_b-k_b} \gamma^{k_b} (\beta_{\mathsf{E}} + \beta_{\mathsf{B}}\gamma)^{-(k_b+l_e)} \\ \times \left[\mathcal{C} \exp\left(-\frac{\beta_{\mathsf{B}}\left(\gamma-1\right)}{\gamma_0}\right) + \mathcal{D}\right] \Theta_1, \end{aligned} \tag{11}$$

$$\mathcal{A}_{n_x} = (-1)^{n_x}\binom{N_x}{n_x},$$

$$c_k = \begin{cases} b_0 = a_0^n & k = 0 \\ \frac{1}{k a_0}\sum_{i=1}^{k}(iN_{\mathsf{B}} - k + i)a_i b_{k-i} & k \geq 1 \end{cases},$$

$$a_k = \frac{1}{k!}\left(\frac{1}{\Omega_x}\right)^k, \beta_{\mathsf{B}} = \frac{t}{\Omega_{\mathsf{B}}}, \beta_{\mathsf{E}} = \frac{w}{\Omega_{\mathsf{E}}}, \phi = \frac{\beta_{\mathsf{B}}}{\beta_{\mathsf{E}}},$$

$$\mathcal{C} = \left(\frac{1}{\gamma_0}\right)^{l_b - k_b}\left(1 - \frac{\Gamma(m_{\mathsf{P}}, \frac{\sigma}{\Omega_{\mathsf{P}}})}{\Gamma(m_{\mathsf{P}})}\right),$$

$$\mathcal{B} = \left(\frac{1}{\Omega_{\mathsf{P}}} + \frac{\beta_{\mathsf{B}}\sigma\left(\gamma - 1\right)}{\gamma_0}\right),$$

$$\mathcal{D} = \frac{1}{\Gamma\left(m_{\mathsf{P}}\right)\left(\Omega_{\mathsf{P}}\right)^{m_{\mathsf{P}}}}\left(\frac{\sigma}{\gamma_0}\right)^{l_b - k_b}\frac{\Gamma\left(m_{\mathsf{P}} + l_b - k_b, \sigma\mathcal{B}\right)}{\mathcal{B}^{m_{\mathsf{P}} + l_b - k_b}},$$

$$\Theta_1 = \begin{cases} \frac{-\beta_{\mathsf{E}}}{\beta_{\mathsf{E}} + \beta_{\mathsf{B}}\gamma}\Gamma(k_b + l_e + 1) & l_e = 0 \\ \frac{-\beta_{\mathsf{E}}}{\beta_{\mathsf{E}} + \beta_{\mathsf{B}}\gamma}\Gamma(k_b + l_e + 1) + l_e\Gamma(k_b + l_e) & l_e \geq 0 \end{cases}.$$

Proof: The proof is given in Appendix A. ■

IV. Asymptotic Performance Analysis

Although the exact closed-form expression can enable us to numerically evaluate the secrecy performance of our considered network, it does not provide further insight into the system performance such as diversity order. Therefore, in this section, we study the performance of the considered system in the high SNR regime by deriving the asymptotic SOP. The main motivation behind this is to study the impact of the maximum transmit power $\mathcal{P}_{\mathsf{m}}$ and the maximum interference power $\mathcal{I}_{\mathsf{p}}$ on the secrecy communication of the considered multiple antenna Nakagami-m channel. As we can see that the SOP of the considered system attains full diversity gain, which is proven in the following Lemma.

Lemma 2: In the high SNR regime, the asymptotic of the SOP can be written as

$$P_{\text{out}}^{\infty} \approx (G_a\gamma_0)^{-G_d} + O({\gamma_0}^{-G_d}) \tag{12}$$

where the secrecy diversity order is

$$G_d = m_{\mathsf{B}}N_{\mathsf{B}}, \tag{13}$$

the secrecy array gain is

$$G_a = \left\{ \sum_{w=1}^{N_{\mathsf{E}}} \sum_{l_e=0}^{w(m_{\mathsf{E}}-1)} \sum_{q=0}^{m_{\mathsf{B}}N_{\mathsf{B}}} \binom{m_{\mathsf{B}}N_{\mathsf{B}}}{q} \mathcal{A}_{wc_{l_e}} \frac{(\gamma_{\text{th}}-1)^{m_{\mathsf{B}}N_{\mathsf{B}}-q}\gamma_{\text{th}}^{q}{\gamma_p}^{q}}{(m_{\mathsf{B}}!)_{\mathsf{B}}^{N}\Gamma\left(m_{\mathsf{P}}\right)\left(\Omega_{\mathsf{B}}\right)^{m_{\mathsf{B}}N_{\mathsf{B}}}} \Theta_2 \right.$$
$$\left. \times \left[\sigma^{-q} \left(\Gamma(m_{\mathsf{P}}) - \Gamma\left(m_{\mathsf{P}}, \frac{\sigma}{\Omega_{\mathsf{P}}}\right)\right) + \sigma^{-m_{\mathsf{B}}N_{\mathsf{B}}}(\Omega_{\mathsf{P}})^{-m_{\mathsf{B}}N_{\mathsf{B}}-q}\Gamma(m_{\mathsf{P}}+m_{\mathsf{B}}N_{\mathsf{B}}-q, \frac{\sigma}{\Omega_{\mathsf{P}}}) \right] \right\}^{\frac{-1}{m_{\mathsf{B}}N_{\mathsf{B}}}}, \tag{14}$$

and $\Theta_2 = \begin{cases} -\frac{(q+l_e)!}{(\beta_{\mathsf{E}})^{q+l_e}} & \text{if } l_e = 0 \\ -\frac{(q+l_e)!}{(\beta_{\mathsf{E}})^{q+l_e}} + l_e \frac{(q+l_e-1)!}{\beta_{\mathsf{E}}^{q+l_e}} & \text{if } l_e > 0 \end{cases}$.

Proof: The proof is given in Appendix B. ■

V. Secrecy Capacity

In this section, we concentrate on deriving the secrecy capacity of the considered system, which is given in the following Lemma.

Lemma 3: The secrecy capacity of the cognitive underlay multiple antennas network over Nakagami-m channel is given as

$$\overline{C} = \frac{-1}{\log(2)} \sum_{t=1}^{N_{\mathsf{B}}} \sum_{l_b=0}^{t(m_{\mathsf{B}}-1)} \sum_{w=1}^{N_{\mathsf{E}}} \sum_{l_e=0}^{w(m_{\mathsf{E}}-1)} \sum_{k_b=0}^{l_b} \sum_{d_b=0}^{l_b-k_b} \binom{l_b}{k_b} \binom{l_b-k_b}{d_b} \mathcal{A}_t \mathcal{A}_w c_{l_b} c_{l_e} (-1)^{l_b-k_b-d_y} (\beta_{\mathsf{B}})^{-(k_b+l_e)} \Theta_3, \tag{15}$$

where

$$\Theta_3 = \begin{cases} \psi & \text{if } l_e = 0 \\ \psi + \alpha & \text{if } l_e > 0 \end{cases}, \tag{16}$$

and ψ and α are defined as follows:

$$\psi = -\frac{\Gamma(k_b+l_e+1)}{\phi} \times \left[\mathcal{C} I_1 \left(1+\frac{1}{\phi}, k_b+l_e+1, k_b+d_b-1, \frac{\beta_{\mathsf{B}}}{\gamma_0} \right) \right.$$
$$+ \mathcal{H} \sum_{p=0}^{m_{\mathsf{P}}+l_b-k_b-1} \left(\frac{\sigma^p}{p!} \right) \left(\frac{\beta_{\mathsf{B}}}{\gamma_p} \right)^{p-(m_{\mathsf{P}}+l_b-k_b)}$$
$$\left. \times I_2(1+\frac{1}{\phi}, \frac{\gamma_p}{\Omega_{\mathsf{P}}\beta_{\mathsf{B}}}, k_b+l_e+1, m_{\mathsf{P}}+l_b-k_b-p, k_b+d_b-1, \sigma\frac{\beta_{\mathsf{B}}}{\gamma_p}) \right], \tag{17}$$

$$\alpha = l_e\Gamma\left(k_b+l_e\right)\times\Bigg[\mathcal{C}I_1\left(1+\frac{1}{\phi},k_b+l_e,k_b+d_b-1,\frac{\beta_{\mathsf{B}}}{\gamma_0}\right) + \mathcal{H}\sum_{p=0}^{m_{\mathsf{P}}+l_b-k_b-1}\left(\frac{\sigma^p}{p!}\right)\left(\frac{\beta_{\mathsf{B}}}{\gamma_p}\right)^{p-(m_{\mathsf{P}}+l_b-k_b)} \times I_2(1+\frac{1}{\phi},\frac{\gamma_p}{\Omega_{\mathsf{P}}\beta_{\mathsf{B}}},k_b+l_e,m_{\mathsf{P}}+l_b-k_b-p,k_b+d_b-1,\sigma\frac{\beta_{\mathsf{B}}}{\gamma_p})\Bigg], \tag{18}$$

where $\mathcal{H}$, $I_1(\cdot)$, and $I_2(\cdot)$ are written as

$$\mathcal{H} = \frac{\Gamma\left(m_{\mathsf{P}}+l_b-k_b\right)}{\left(\gamma_p\right)^{l_b-k_b}\Gamma\left(m_{\mathsf{P}}\right)\left(\Omega_{\mathsf{P}}\right)^{m_{\mathsf{P}}}}\exp\left(-\frac{\sigma}{\Omega_{\mathsf{P}}}\right), \tag{19}$$

$$I_1\left(a,m,n,v\right) = \int_0^\infty \frac{\left(x+1\right)^n}{\left(x+a\right)^m}\exp\left(-vx\right)dx = \begin{cases}\sum_{k=0}^{n} C_n^k J\left(a,m,k,v\right) & \text{if } n\geq 0\\ S_1\left(a,1,m,-n,0,v\right) & \text{if } n<0\end{cases}, \tag{20}$$

$$I_2\left(a,b,m,n,k,v\right) = \begin{cases}\sum_{j=0}^{k} C_k^j S_1\left(a,b,m,n,j,v\right) & \text{if } k\geq 0\\ S_2\left(a,b,1,m,n,-k,0,v\right) & \text{if } k<0\end{cases}. \tag{21}$$

The terms $J(\cdot)$, $S_1(\cdot)$, and $S_2(\cdot)$ are respectively given by

$$J\left(a,m,n,v\right) = \int_0^\infty \frac{x^n\exp\left(-vx\right)}{\left(x+a\right)^m}dx = \frac{n!}{v^{n+1-m}}U\left(m,m-n,av\right), \tag{22}$$

$$S_1\left(a,b,m,n,k,v\right) = \int_0^\infty \frac{x^k\exp\left(-vx\right)dx}{\left(x+a\right)^m\left(x+b\right)^n} = \sum_{i=1}^{m} A_i J\left(a,i,k,v\right) + \sum_{j=1}^{n} B_j J\left(b,j,k,v\right), \tag{23}$$

$$S_2\left(a,b,c,m,n,q,k,v\right) = \sum_{i=1}^{m} C_i J\left(a,i,k,v\right) + \sum_{j=1}^{n} D_j J\left(b,j,k,v\right) + \sum_{o=1}^{q} E_o J\left(c,o,k,v\right), \tag{24}$$

where (22) is obtained with the help of the definition of Tricomi's confluent hypergeometric function, i.e., $U\left(a,b,z\right)$, which is defined in [18, Eq. (9.211.4)]. The terms A_i, B_j, C_i, D_j, and

E_o are partial fraction coefficients and are defined as follows:

$$\begin{aligned}
A_i &= \frac{1}{(m-i)!}\frac{d^{(m-i)}}{dx}\left[\frac{x^k}{(x+b)^n}\right]\Bigg|_{x=-a}, \\
B_j &= \frac{1}{(n-j)!}\frac{d^{(n-j)}}{dx}\left[\frac{x^k}{(x+a)^m}\right]\Bigg|_{x=-b}, \\
C_i &= \frac{1}{(m-i)!}\frac{d^{(m-i)}}{dx}\left[\frac{1}{(x+b)^n(x+c)^q}\right]\Bigg|_{x=-a}, \\
D_j &= \frac{1}{(n-j)!}\frac{d^{(n-j)}}{dx}\left[\frac{1}{(x+a)^m(x+c)^q}\right]\Bigg|_{x=-b}, \\
E_o &= \frac{1}{(q-o)!}\frac{d^{(q-o)}}{dx}\left[\frac{1}{(x+b)^n(x+a)^m}\right]\Bigg|_{x=-c}.
\end{aligned} \tag{25}$$

Proof: The proof is given in Appendix C. ■

VI. Numerical Results and Discussions

In this section, simulation results based on Monte Carlo method are provided to verify the accuracy of the above performance analysis. More specifically, the exact and asymptotic curves of the SOP in (11), (12), and (15) are compared with the ones obtained using numerical result. Without loss of generality, the following parameters are fixed throughout this section: the expected rate $R_{\mathsf{S}} = 0.5$ bps/Hz, $\lambda_{\mathsf{P}} = 3$, $\lambda_{\mathsf{B}} = 6$, $m_{\mathsf{P}} = 2$, $m_{\mathsf{B}} = 1$, and $m_{\mathsf{E}} = 2$.

In Fig. 2, the exact and asymptotic SOP, and their numerical results versus γ_0 are plotted with fixed value of N_{E} and different values of N_{B} and σ. We can see that the analysis results match the simulation results well. As can be clearly seen from this figure, when the number of antennas at the secondary receiver increases the SOP decreases, which is in agreement with the result obtained in (12). These results point out that the secrecy diversity order of the considered system depends on the number of antennas at the secondary receiver, i.e., the larger the number of antennas at the secondary receiver is, the better the security performance is. Fig. 2 also shows that relaxing the ratio between $\mathcal{I}_{\mathsf{p}}$ and $\mathcal{P}_{\mathsf{m}}$ witnesses an increase in the SOP of the system. When σ decreases $\mathcal{I}_{\mathsf{p}}$ also decreases. In this situation, the transmitter has to reduce its transmit power to protect the PU. As a result, the SNR at the receiver reduces followed by an increase in the SOP. In addition, the variations in the value of σ in Fig. 2 and N_{E} in Fig. 3 lead to different parallel curves of the SOP. This results prove that the secrecy diversity order is independent of σ and N_{E}.

The secrecy capacity of the system versus N_{B}, N_{E}, and σ is verified in Fig. 4, Fig. 5, and Fig. 6, respectively. Fig. 4 points out that the secrecy capacity increases with the number of antennas

at the secondary receiver while Fig. 5 shows that the increase in the number of antennas at the eavesdropper has bad effect on the system's secrecy capacity. In Fig. 6, we can see how the secrecy capacity of the system is affected by $\mathcal{I}_{\mathsf{p}}$ and $\mathcal{P}_{\mathsf{m}}$. By decreasing the σ parameter, the peak interference constraint at the PU is decreased followed by an increase in the system's secrecy capacity.

VII. Conclusions

In this paper, secure performance of the cognitive underlay network with multiple antennas at the receiver and the eavesdropper over Nakagami-m channel has been studied. In particular, the exact closed-form and the asymptotic expressions of the SOP have been derived. The results showed that the secrecy diversity order of the considered system merely depends on the number of antennas at the intended receiver and the fading parameter of the main channel. Hence, to enhance the secure communication we solely need to increase the number of antennas in the secondary receiver. In addition, the secrecy capacity of the considered system is also investigated. Finally, the numerical results are provided to validate our correctness.

Appendix A
Proof of Lemma 1

The CDF of $\hat{\gamma}$ is given as

$$\begin{aligned} F_{\hat{\gamma}}\left(\gamma\right) &= \Pr\left(\hat{\gamma} < \gamma\right) = \Pr\left(\gamma_{\mathsf{B}} < \gamma\left(1+\gamma_{\mathsf{E}}\right) - 1\right) \\ &= \int_{0}^{\infty} \int_{0}^{\gamma(1+\gamma_{\mathsf{E}})-1} f_{\gamma_{\mathsf{B}},\gamma_{\mathsf{E}}}\left(\gamma_{\mathsf{B}},\gamma_{\mathsf{E}}\right) d\gamma_{\mathsf{B}} d\gamma_{\mathsf{E}}. \end{aligned} \tag{A.1}$$

To compute the integral in (A.1), we need to find out the joint CDF of main and eavesdropping channel. However, the joint CDF can not be obtained easily due to the dependence between the two RVs, i.e., $\gamma_{\mathsf{B}}, \gamma_{\mathsf{E}}$. More specifically, these RVs contain the common variable $|h_{\mathsf{P}}|^2$ as presented in (3). To overcome this, we firstly compute the joint CDF conditioned on $|h_{\mathsf{P}}|^2 = X$. Mathematically, we have

$$f_{\gamma_{\mathsf{B}},\gamma_{\mathsf{E}}|X}\left(\gamma_{\mathsf{B}},\gamma_{\mathsf{E}}\right) = f_{\gamma_{\mathsf{B}}|X}\left(\gamma_{\mathsf{B}}\right) f_{\gamma_{\mathsf{E}}|X}\left(\gamma_{\mathsf{E}}\right). \tag{A.2}$$

We obtain (A.2) because $\gamma_{\mathsf{B}}|X, \gamma_{\mathsf{E}}|X$ are independent of each other. To this end, the integral in (A.1) is re-written as

$$F_{\hat{\gamma}}(\gamma) = \int_0^{\infty}\int_0^{\infty}\int_0^{\gamma(1+\gamma_{\mathsf{E}})-1} f_{\gamma_{\mathsf{B}}|X}(\gamma_{\mathsf{B}}) f_{\gamma_{\mathsf{E}}|X}(\gamma_{\mathsf{E}}) f_X(x)\, d\gamma_{\mathsf{B}} d\gamma_{\mathsf{E}} dx$$
$$= \int_0^{\infty}\int_0^{\infty} F_{\gamma_{\mathsf{B}}|X}(\gamma(1+\gamma_{\mathsf{E}})-1) f_{\gamma_{\mathsf{E}}|X}(\gamma_{\mathsf{E}}) f_X(x)\, d\gamma_{\mathsf{E}} dx. \quad \text{(A.3)}$$

From (A.3), we need to achieve the CDF of $\gamma_{\mathsf{B}}|\,X$, PDF of $\gamma_{\mathsf{E}}|\,X$, and PDF of X before computing the CDF of $\hat{\gamma}$.

In this paper, we assume that all channel coefficients, e.g., h_{T} are impaired by Nakagami-m channel, with $\mathsf{T} = \{\mathsf{P}, \mathsf{B}, \mathsf{E}\}$. As a result, $|h_{\mathsf{T}}|^2$ follows Gamma distribution with CDF, PDF are given as:

$$F_{Y=|h_{\mathsf{T}}|^2}(y) = 1 - \frac{\Gamma\left(m_{\mathsf{T}}, \frac{y}{\Omega_{\mathsf{T}}}\right)}{\Gamma(m_{\mathsf{T}})}$$
$$= 1 - \exp\left(-\frac{y}{\Omega_{\mathsf{T}}}\right)\sum_{l_t=0}^{m_{\mathsf{T}}-1}\frac{1}{l_t!}\left(\frac{1}{\Omega_{\mathsf{T}}}\right)^{l_t} y^{l_t}$$
$$= 1 - \exp\left(-\frac{y}{\Omega_{\mathsf{T}}}\right)\sum_{l_t=0}^{m_{\mathsf{T}}-1} a_{l_t} y^{l_t}, \quad \text{(A.4)}$$

$$f_{Y=|h_{\mathsf{T}}|^2}(y) = \frac{y^{m_{\mathsf{T}}-1}}{\Gamma(m_{\mathsf{T}})(\Omega_{\mathsf{T}})^{m_{\mathsf{T}}}}\exp\left(-\frac{y}{\Omega_{\mathsf{T}}}\right), \quad \text{(A.5)}$$

where

$$a_{l_t} = \frac{1}{l_t!}\left(\frac{1}{\Omega_{\mathsf{T}}}\right)^{l_t}, \Omega_{\mathsf{T}} = \frac{\lambda_{\mathsf{T}}}{m_{\mathsf{T}}}.$$

We obtain (A.4) with the help of [18, Eq. (8.352.6)].

Besides, from (3), we have

$$\gamma_{\mathsf{B}}|X = \gamma_0 \min\left(\frac{\sigma}{X}, 1\right) \times \max_{n\in(1,N_{\mathsf{B}})}\left(|h_{B_n}|^2\right)$$
$$= u \times \max_{n\in(1,N_{\mathsf{B}})}\left(|h_{B_n}|^2\right), \quad \text{(A.6)}$$

where $u = \gamma_0 \min\left(\frac{\sigma}{X}, 1\right)$.

From (A.6), the CDF of SNR at $\mathbf{B}$ conditioned on X is given as

$$\begin{aligned}
F_{\gamma_{\mathsf{B}}|X}(\gamma) &= \Pr(\gamma_{B|X} < \gamma) \\
&= \Pr\left(u \times \max_{t\in(1,N_{\mathsf{B}})}\left(|h_{\mathsf{B}_t}|^2\right) < \gamma\right) \\
&= \Pr\left(\max_{t\in(1,N_{\mathsf{B}})}\left(|h_{\mathsf{B}_t}|^2\right) < \frac{\gamma}{u}\right) \\
&= F_{\max\limits_{t\in(1,N_{\mathsf{B}})}\left(|h_{\mathsf{B}_t}|^2\right)}\left(\frac{\gamma}{u}\right) \\
&= \left[F_{|h_{\mathsf{B}}|^2}\left(\frac{\gamma}{u}\right)\right]^{N_{\mathsf{B}}} \\
&= \left[1-\exp\left(-\frac{\gamma}{u\Omega_{\mathsf{B}}}\right)\sum_{l_b=0}^{m_{\mathsf{B}}-1} a_{l_b}\left(\frac{\gamma}{u}\right)^{l}\right]^{N_{\mathsf{B}}} \\
&= 1+\exp\left(-\frac{t\gamma}{u\Omega_{\mathsf{B}}}\right)\sum_{t=1}^{N_{\mathsf{B}}}\sum_{l_b=0}^{t(m_{\mathsf{B}}-1)} A_t c_{l_b}\left(\frac{\gamma}{u}\right)^{l_b}, \qquad \text{(A.7)}
\end{aligned}$$

where $\mathcal{A}_{n_y} = (-1)^{n_y} C_{N_y}^{n_y}$ and $c_k = \begin{cases} b_0 = a_0^n & \text{if } k = 0 \\ \frac{1}{ka_0}\sum\limits_{i=1}^{k}\left(iN_y - k + i\right)a_i b_{k-i} & \text{if } k \geq 1 \end{cases}$.

We obtain (A.7) with the assistance of binomial expansion and [18, Eq. (0.314)]. Similarly, CDF of $\gamma_{\mathsf{E}}|X$ is calculated as

$$F_{\gamma_{\mathsf{E}}|X}(x) = 1+\exp\left(-\frac{wx}{u\Omega_{\mathsf{E}}}\right)\sum_{w=1}^{N_{\mathsf{E}}}\sum_{l_e=0}^{w(m_{\mathsf{E}}-1)} A_w c_{l_e}\left(\frac{x}{u}\right)^{l_e}. \qquad \text{(A.8)}$$

The PDF of $\gamma_{\mathsf{E}}|X$ can be calculated by deriving the CDF of $\gamma_{\mathsf{E}}|X$. Mathematically, we have

$$f_{\gamma_{\mathsf{E}}|X}(x) = \frac{1}{u}\exp\left(-\frac{wx}{u\Omega_{\mathsf{E}}}\right)\sum_{w=1}^{N_{\mathsf{E}}}\sum_{l_e=0}^{w(m_{\mathsf{E}}-1)} A_w c_{l_e}\Theta_0, \qquad \text{(A.9)}$$

where $\Theta_0 = \begin{cases} -\beta_{\mathsf{E}}\left(\frac{x}{u}\right)^{l_e} & \text{if } l_e = 0 \\ -\beta_{\mathsf{E}}\left(\frac{x}{u}\right)^{l_e} + l_e\left(\frac{x}{u}\right)^{l_e-1} & \text{if } l_e > 0 \end{cases}$.

Substituting (A.5), (A.7), and (A.9) into (A.3), the CDF of $\hat{\gamma}$ is given as follows:

$$F_{\hat{\gamma}}(\gamma) = \int_0^\infty \int_0^\infty \left(1 + \exp\left(-\frac{t\left(\gamma\left(1+y\right)-1\right)}{u\Omega_{\mathsf{B}}}\right) \sum_{t=1}^{N_{\mathsf{B}}} \sum_{l_b=0}^{t(m_{\mathsf{B}}-1)} A_t c_{l_b} \left(\frac{\left(\gamma\left(1+y\right)-1\right)}{u}\right)^{l_b}\right)$$
$$\times \left[\frac{1}{u}\exp\left(-\frac{wy}{u\Omega_{\mathsf{E}}}\right) \sum_{w=1}^{N_{\mathsf{E}}} \sum_{l_e=0}^{w(m_{\mathsf{E}}-1)} A_w c_{l_e} \Theta_0\right] \frac{x^{m_{\mathsf{P}}-1}}{\Gamma\left(m_{\mathsf{P}}\right)\left(\Omega_{\mathsf{P}}\right)^{m_{\mathsf{P}}}} \exp\left(-\frac{x}{\Omega_{\mathsf{P}}}\right) dydx$$
$$\overset{(a)}{=} 1 + \sum_{t=1}^{N_{\mathsf{B}}} \sum_{l_b=0}^{t(m_{\mathsf{B}}-1)} \sum_{w=1}^{N_{\mathsf{E}}} \sum_{l_e=0}^{w(m_{\mathsf{E}}-1)} \sum_{k_b=0}^{l_b} \binom{l_b}{k_b} (\gamma-1)^{l_b-k_b} \gamma^{k_b} \mathcal{A}_t \mathcal{A}_w c_{l_b} c_{l_e} \Theta_1 (\beta_{\mathsf{B}}\gamma + \beta_{\mathsf{E}})^{-(k_b+l_e)}$$
$$\times \int_0^\infty \left(\frac{1}{\gamma_0 \min\left(\frac{\sigma}{x}, 1\right)}\right)^{l_b-k_b} \exp\left(-\frac{\beta_{\mathsf{B}}\left(\gamma-1\right)}{\gamma_0 \min\left(\frac{\sigma}{x}, 1\right)}\right) \frac{x^{m_{\mathsf{P}}-1}}{\Gamma\left(m_{\mathsf{P}}\right)\left(\Omega_{\mathsf{P}}\right)^{m_{\mathsf{P}}}} \exp\left(-\frac{x}{\Omega_{\mathsf{P}}}\right) dx$$
$$\overset{(b)}{=} 1 + \sum_{t=1}^{N_{\mathsf{B}}} \sum_{l_b=0}^{t(m_{\mathsf{B}}-1)} \sum_{w=1}^{N_{\mathsf{E}}} \sum_{l_e=0}^{w(m_e-1)} \sum_{k_b=0}^{l_b} \binom{l_b}{k_b} \mathcal{A}_t \mathcal{A}_w c_{l_b} c_{l_e} (\gamma-1)^{l_b-k_b} \gamma^{k_b}$$
$$\times (\beta_{\mathsf{E}} + \beta_{\mathsf{B}}\gamma)^{-(k_b+l_e)} \left[\mathcal{C}\exp\left(-\frac{\beta_{\mathsf{B}}\left(\gamma-1\right)}{\gamma_0}\right) + \mathcal{D}\right] \Theta_1, \tag{A.10}$$

where $\beta_{\mathsf{B}} = \frac{t}{\Omega_{\mathsf{B}}}, \beta_{\mathsf{E}} = \frac{w}{\Omega_{\mathsf{E}}}, \phi = \frac{\beta_{\mathsf{B}}}{\beta_{\mathsf{E}}}, \mathcal{C} = \left(\frac{1}{\gamma_0}\right)^{l_b-k_b}\left(1 - \frac{\Gamma\left(m_{\mathsf{P}}, \frac{\sigma}{\Omega_{\mathsf{P}}}\right)}{\Gamma(m_{\mathsf{P}})}\right), \mathcal{B} = \left(\frac{1}{\Omega_{\mathsf{P}}} + \frac{\beta_{\mathsf{B}}(\gamma-1)}{\gamma_p}\right), \mathcal{D} = \frac{1}{\Gamma(m_{\mathsf{P}})(\Omega_{\mathsf{P}})^{m_{\mathsf{P}}}}\left(\frac{1}{\gamma_p}\right)^{l_b-k_b} \frac{\Gamma(m_{\mathsf{P}}+l_b-k_b, \sigma\mathcal{B})}{\mathcal{B}^{m_{\mathsf{P}}+l_b-k_b}}$, and $\Theta_1 = \begin{cases} -\left(\frac{\beta_e}{\beta_e+\beta_y\gamma}\right)\Gamma(k_b+l_e+1) & \text{if } l_e = 0 \\ -\left(\frac{\beta_e}{\beta_e+\beta_y\gamma}\right)\Gamma(k_b+l_e+1) + l_e\Gamma(k_b+l_e) & \text{if } l_e > 0 \end{cases}$.

The manipulation in (a) and (b) are achieved with the support of binomial expansion and [18, Eq. (3.351)].

APPENDIX B
PROOF OF LEMMA 2

To prove the Lemma 2, we firstly expand the first order of CDF of Gamma RV $Y = |h_t|^2$ as

$$F_Y(y) \overset{y\to 0}{\approx} \frac{1}{m_t!}\left(\frac{y}{\Omega_t}\right)^{m_t}. \tag{B.1}$$

By applying (B.1) into the CDF of $\gamma_{B|X}$, we have

$$F_{\gamma_{B|X}}(x) \approx \left[\frac{1}{m_{\mathsf{B}}!}\left(\frac{x}{\Omega_{\mathsf{B}}}\right)^{m_{\mathsf{B}}}\right]^{N_{\mathsf{B}}} = \frac{1}{(m_{\mathsf{B}}!)^{N_{\mathsf{B}}}}\left(\frac{x}{\Omega_{\mathsf{B}}}\right)^{m_{\mathsf{B}}N_{\mathsf{B}}}. \tag{B.2}$$

To this end, the asymptotic of SOP is computed by substituting (B.2) into (A.9) and (A.5). After some manipulations, we reach (12), which concludes our proof.

APPENDIX C
PROOF OF LEMMA 3

The secrecy capacity is computed by solving following integral

$$\begin{aligned}
\overline{C} &= \frac{1}{\log(2)} \int_1^{\infty} \log(\gamma) f_{\hat{\gamma}}(\gamma) d\gamma \\
&\overset{(a)}{=} \frac{1}{\log(2)} \left[\underbrace{\log(\gamma) F_{\hat{\gamma}}(\gamma)|_1^{\infty}}_{\to 0} - \int_1^{\infty} \frac{1}{\gamma} F_{\hat{\gamma}}(\gamma) d\gamma \right] \\
&\overset{(b)}{=} \frac{-1}{\log(2)} \int_0^{\infty} \frac{1}{x+1} F_{\hat{\gamma}}(x+1) dx \\
&= \frac{-1}{\log(2)} \sum_{t=1}^{N_{\mathsf{B}}} \sum_{l_b=0}^{t(m_{\mathsf{B}}-1)} \sum_{w=1}^{N_{\mathsf{E}}} \sum_{l_e=0}^{w(m_e-1)} \sum_{k_b=0}^{l_b} \sum_{d_y=0}^{l_b-k_b} \binom{l_b-k_b}{d_y} \binom{l_b}{k_b} (-1)^{l_b-k_b-d_y} (\beta_{\mathsf{B}})^{-(k_b+l_e)} A_t A_w c_{l_b} c_{l_e} \\
&\times \int_0^{\infty} (x+1)^{d_y+k_b-1} \left(\phi^{-1}+1+x\right)^{-(k_b+l_e)} \\
&\times \left[\mathcal{C} \exp\left(-\frac{\beta_{\mathsf{B}}}{\gamma_0} x\right) + \mathcal{H} \exp\left(-\frac{\sigma \beta_{\mathsf{B}}}{\gamma_p} x\right) \sum_{p=0}^{m_{\mathsf{P}}+l_b-k_b-1} \frac{\sigma^p}{p!} \frac{\left(\frac{\beta_y}{\gamma_p}\right)^{p-(m_{\mathsf{P}}+l_b-k_b)}}{\left(x+\frac{\gamma_p}{\beta_y \Omega_x}\right)^{m_{\mathsf{P}}+l_b-k_b-p}} \right] \Delta dx \\
&\overset{(c)}{=} \frac{-1}{\log(2)} \sum_{t=1}^{N_{\mathsf{B}}} \sum_{l_b=0}^{t(m_{\mathsf{B}}-1)} \sum_{w=1}^{Ne} \sum_{l_e=0}^{w(m_e-1)} \sum_{k_b=0}^{l_b} \sum_{d_y=0}^{l_b-k_b} \binom{l_b}{k_b} \binom{l_b-k_b}{d_y} \mathcal{A}_t \mathcal{A}_w c_{l_b} c_{l_e} (-1)^{l_b-k_b-d_y} (\beta_{\mathsf{B}})^{-(k_b+l_e)} \Theta_3,
\end{aligned} \tag{C.1}$$

where

$$\Delta = \begin{cases} \underbrace{-\phi^{-1}\left(\phi^{-1}+1+x\right)^{-1} \Gamma(k_b+l_e+1)}_{\hat{A}} & \text{if } l_e = 0 \\ \hat{A} + l_e \Gamma(k_b+l_e) & \text{if } l_e > 0 \end{cases}.$$

The step (a) is obtained by using integral by part and the term $\log(\gamma) F_{\hat{\gamma}}(\gamma)$ goes to zero while $\gamma \to \infty$ with the help of L' Hospital rule. The step (b) is computed by changing variable $x = \gamma - 1$. After some manipulations, (c) is computed by using partial fraction method combined with the definition of Tricomi's confluent hyper-geometric function, i.e., $U(a,b,z)$, which is defined in of [18, Eq. (9.211.4)]. Θ_3 is provided in (15). Finally, we can complete our proof.

REFERENCES

[1] Federal Communications Commission, *Spectrum Policy Task Force Report*. ET Docket No. 02-155, 2002.

[2] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[3] A. Goldsmith, S. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 95, no. 5, pp. 894–914, May 2009.

[4] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Trans. Comput.*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[5] M. Debbah, "Mobile felexible networks: The challenges ahead," in *Proc. IEEE ATC*, Hanoi, Vietnam, Oct. 2008, pp. 3–7.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[7] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, pp. 40–47, Feb. 2012.

[8] 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.

[9] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with m-antenna eavesdroppers: Characterization of the outage probability and outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

[10] H. Alves, R. D. Souza, and M. Debbah, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jan. 2012.

[11] 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. 6, no. 10, pp. 144–154, Jan. 2013.

[12] 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.

[13] 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, Nov. 2012.

[14] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[15] T. Q. Duong, T. T. Duy, M. Elkashlan, N. H. Tran, and O. A. Dobre, "Secured cooperative cognitive radio networks with relay selection," in *Proc. IEEE GLOBECOM*, Austin, TX, Dec. 2014, pp. 3074–3079.

[16] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[17] T. Q. Duong, D. B. da Costa, M. Elkashlan, and V. N. Q. Bao, "Cognitive amplify-and-forward relay networks over Nakagami-m fading," *IEEE Trans. Veh. Technol.*, vol. 61, no. 5, pp. 2368–2374, May 2012.

[18] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. San Diego, CA: Academic press, 2007.

[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.

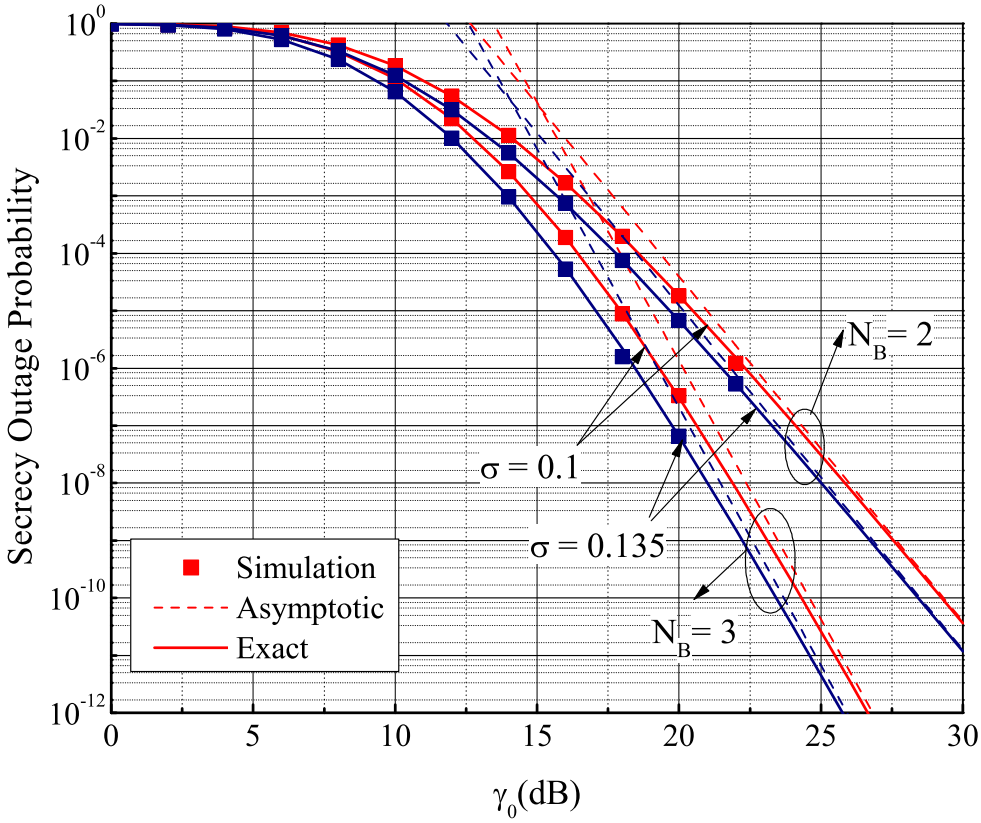

Fig. 2: Secrecy outage probability with different N_{B} and σ values.

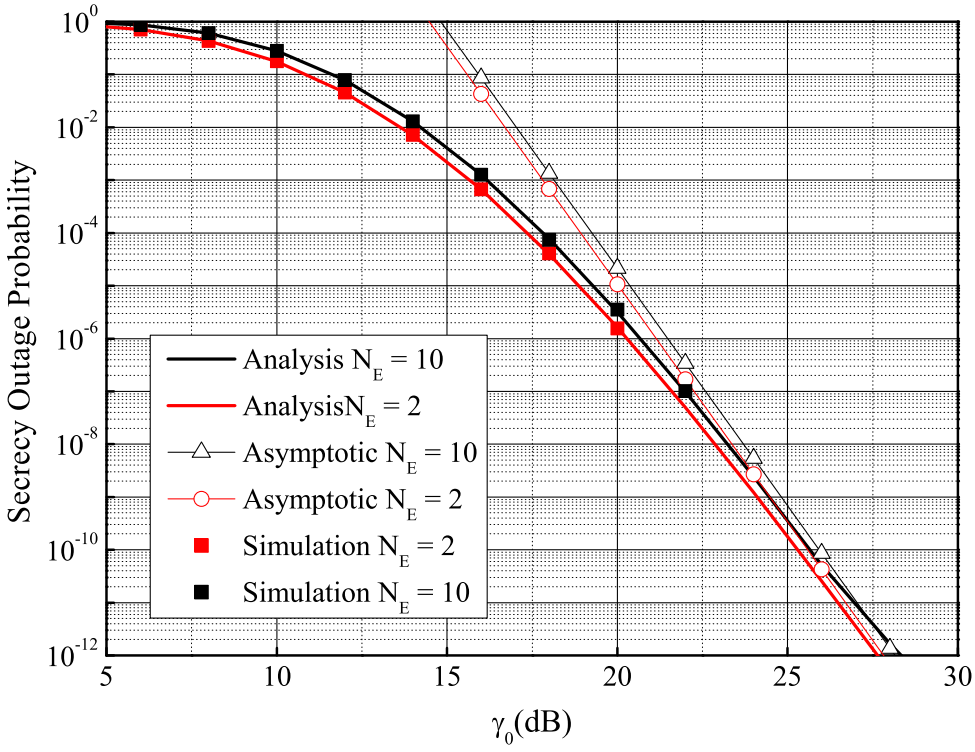

Fig. 3: Secrecy outage probability with different N_{E} values.

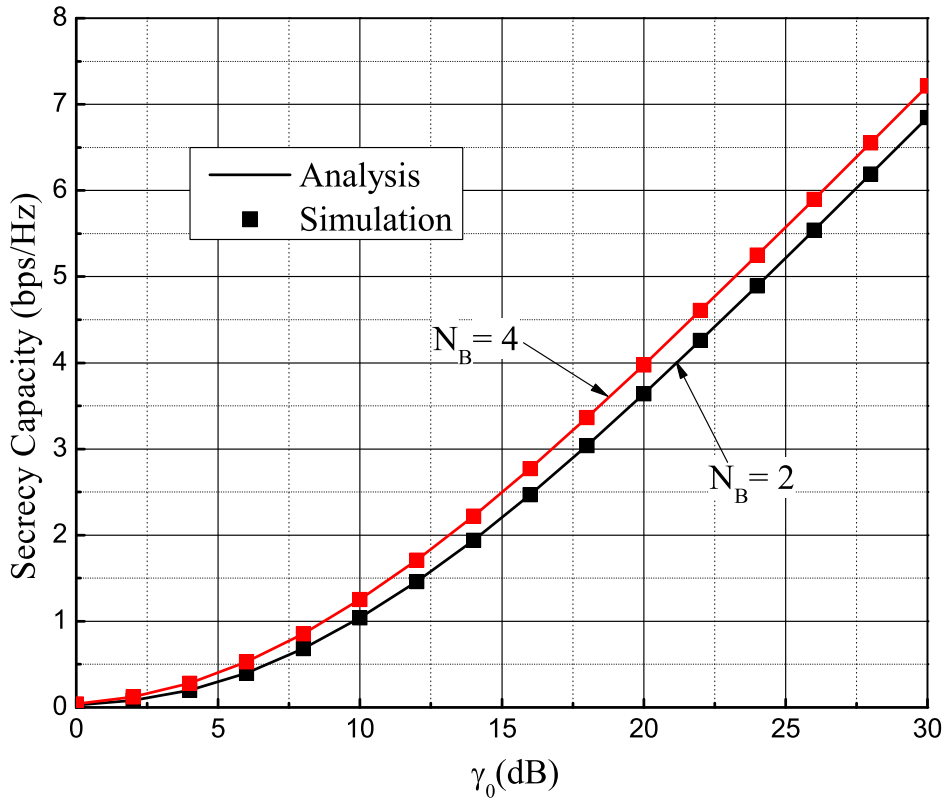

Fig. 4: Secrecy capacity with different N_{B} values.

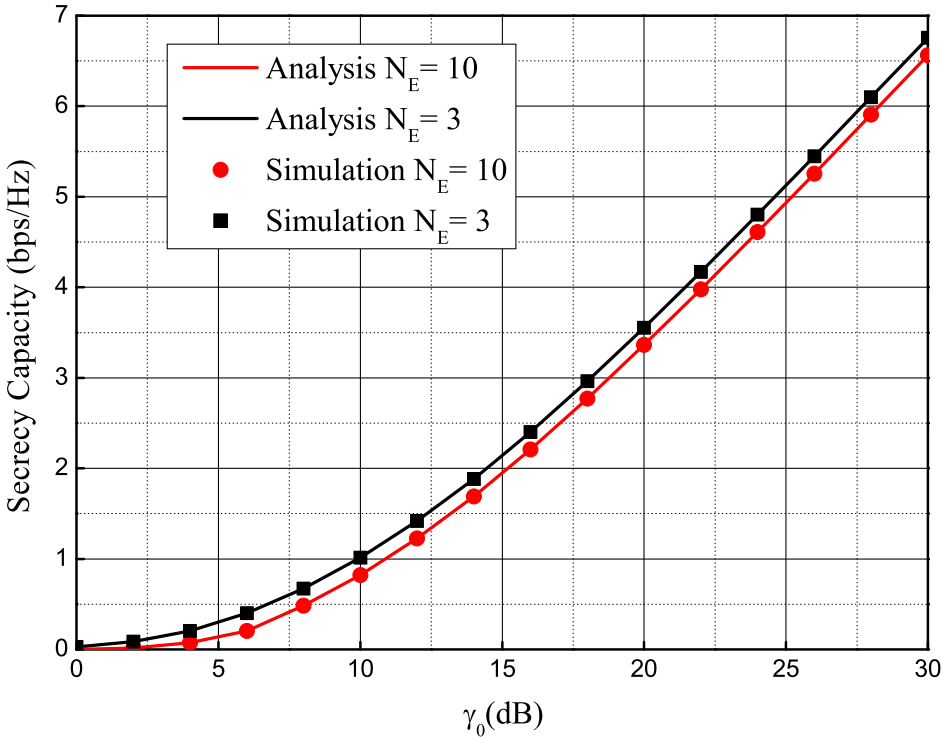

Fig. 5: Secrecy capacity with different N_{E} values.

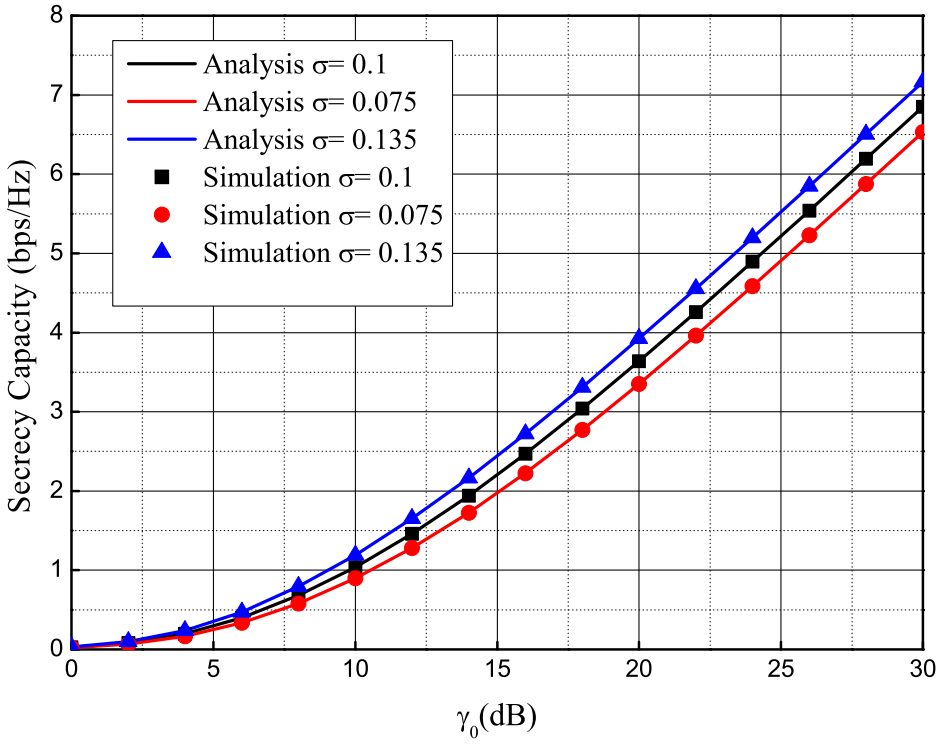

Fig. 6: Secrecy capacity with different σ values.