Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5548428, 12 pages
https://doi.org/10.1155/2021/5548428

Research Article

Secrecy Performance Analysis of a Cognitive Network for IoT over k-μ Channels

Junxia Li[1], **Hui Zhao**[1] **and Michael Johnson**[2]

[1]*The College of Information Science and Engineering, Xinjiang University, 830046 Urumqi, China*
[2]*Department of Electronic and Computer Engineering, University of Limerick, Limerick, Ireland*

Correspondence should be addressed to Hui Zhao; zhmerryxjdx@163.com

Received 2 March 2021; Revised 14 May 2021; Accepted 1 June 2021; Published 28 June 2021

Academic Editor: Xingwang Li

With the development of Internet of Things (IoTs), devices are now connecting and communicating together on a heretofore unheard-of scale, forming huge heterogeneous networks of mobile IoT-enabled devices. For beyond 5G- (B5G-) enabled networks, this raises concerns in terms of spectral resource allocation and associated security. Cognitive radio is one effective solution to such a spectrum sharing issue which can be adopted to these B5G networks, which works on the principle of sharing spectrum between primary and secondary users. In this paper, we develop the confidentiality of cognitive radio network (CRNs) for IoT over k-μ fading channels, with the information transmitted between secondary networks with multiple cooperative eavesdroppers, under the constraint of the maximum interference that the primary users can tolerate. All considered facilities use a single-antenna receiver. Of particular interest, the minimum limit values of secure outage probability (SOP) and the probability of strictly positive secrecy capacity (SPSC) are developed for this model in a concise form. Finally, the Monte Carlo simulations for the system are provided to support the theoretical analysis presented.

1. Introduction

With the recent roll-out of 5G technology globally, an ever-increasing number of intelligent devices are now joining the Internet including mobile IoT devices in social, industrial, healthcare, and smart-grid nature [1]. With this rapid rise in connectivity between such devices, associated security threats and challenges are also on the increase, becoming more pressing, and need to be resolved urgently.

Traditional network encryption mechanisms can resolve security problem through various encryption algorithms at the network layer and above. However, such encryption mechanisms can no longer provide perfect security for wireless communication networks due to the complexity and time-consuming nature of the problem. Fortunately, the influence of fading channel and noise actually provides the possibility for implementing physical layer security (PLS), which has been the subject of extensive research in the literature. On the basis of [2], Wyner first proposed a model to estimate the security of communication systems [3]. For the scenarios of active eavesdropping, Ai et al. provided another evaluation benchmark, namely, average secrecy capacity (ASC), over double-Rayleigh fading channels [4]. Referring to the classical Wyner eavesdropping model, SOP was given to study the security of the correlated Rician fading channels [5]. To minimize information leakage, a precoding scheme and the security of Rician fading channels were investigated by analyzing the SOP in [6]. Elsewhere, [7] studied the security capability of large-scale fading channels according to the probability of nonzero secrecy capacity (PNSC) and SOP.

The generalized fading channel can model the real transmission environment. By changing its parameters, it can represent many channel models. To account for this, a large section of the literature has studied the transmission performance and security of the generalized fading channels [8–15]. In [8], Lei et al. employed two mathematical forms to complete the derivation of the lower limit of SOP and strictly positive secrecy capacity (SPSC). Elsewhere, the ability of such a channel to resist active eavesdropping was investigated by deriving the ASC in [9]. Using a system model of decode-and-forward (DF) relay cooperation

over generalized-K channels, the exact and approximate theoretical expressions of SOP and ESC were evaluated in [10]. Using channels with the premise that the main link follows α-μ distribution and the eavesdropping link was modelled as k-μ distribution, the analytical expressions of ASC, SOP, and SPSC were derived in [11]. Sun et al. described the closed form of SOP and SPSC over other k-μ shadowed fading channels in a concise form [12] and gave an approximate analysis through the method of moment matching. The authors of [13] analyzed the security of Fox's H-function fading channels by simulating the SOP and probability of nonzero secrecy capacity (PNZ). In real-world wireless communication networks (WCNs), the correlation between antennas cannot be ignored. Based on this, the security performance analysis of correlated systems over η-μ fading channels [14] and k-μ shadowed fading channels [15] has also been investigated.

More recently, nonorthogonal multiple access (NOMA) and ambient backscatter communication technology have attracted more and more attention due to the high spectral and energy efficiency for the Internet of Things. In order to investigate the reliability and security of the ambient backscatter NOMA systems considering hardware damage, the outage probability (OP) and the intercept probability (IP) were studied [16]. More practically, the ambient backscatter NOMA system under in-phase and quadrature-phase imbalance (IQI) was taken into account in [17], where the expressions for the OP and the IP are derived in closed exact analytical form [18] and the secure performance for the future beyond 5G (B5G) networks in the presence of nonlinear energy harvesters and imperfect CSI and IQI in terms of the closed form of OP and IP was studied.

Most recently, many scholars are interested in CRNs because they can make use of scarce spectrum resources without causing decoding errors to the primary user's communication. Considering a multirelay network over Nakagami- m fading channels, the authors of [19] studied the effect of three different relay schemes on the security capacity of the channel. In [20], the SOP of the single-input multiple-output (SIMO) underlay CRNs over Rayleigh fading channels with imperfect CSI were derived and analyzed. Park et al. [21] proposed a CRN model composed of a multirelay primary network and a direct link secondary network, where the outage performance of the two networks was analyzed. The secrecy outage performance of DF-based multihop relay CRN under different parameters was investigated in the presence of imperfect CSI in [22]. The authors in [23] studied the energy distribution of CRN by analyzing spectrum sharing. Based on an underlying CRN, the derivation and analysis of SOP and SPSC are described in [24]. Combined with machine learning, a resource allocation protocol for CRN has also been proposed, and the influence of channel parameters on spectrum efficiency is presented in [25]. For conditions where the secondary network cannot interfere with the communication of the primary network, the authors in [26] took PNSC and SOP as the benchmark for studying CRN over Rayleigh fading channels. Recently, security issues are studied for popular applications such as relaying system a direct connection [27] and NOMA system [28].

As a generalized channel, k-μ fading can be equated with Rayleigh, one-sided Gaussian, Nakagami- m, and Rician fading channel [29], which can be used to simulate many wireless communication scenarios, so it is of great value to explore transmission performance. Bhargav et al. [30] analyzed the security of the wiretap system over fading channels by deriving the SOP and SPSC of the considered system. The SOP was derived based on classical Wyner's model over k-μ distribution [31]. The authors in [32] studied the statistical properties of k-μ distribution and obtained the probability density function (PDF) and cumulative distribution function (CDF) for multiple independent k-μ variables. Utilizing DF relay scheme, the SOP and SPSC in a relay system over k-μ channels were provided [33]. As an extension to [32], the authors of analyzed the secrecy outage performance of a SIMO wiretap system over k-μ channels.

1.1. Motivation and Contribution. To date, there is negligible work presented in the literature on the CRN security assessment of multiple eavesdroppers over k-μ fading channels. Motivated by the aforementioned discussions, this paper presents such an investigation into the secrecy outage performance of CRN under multiple eavesdroppers by deriving the SOP and SPSC.

The main contributions of this paper are summarized as follows:

(i) The work presents a CRN security assessment of multiple eavesdroppers over k-μ fading channels, considering multiple eavesdroppers in the cognitive radio network. It provides theoretical analysis of SOP and studies the influence of channel parameters and other parameters on the secrecy outage performance

(ii) The paper also presents a derivation of SPSC for such a setup, from which it can be seen that SPSC is independent of the primary channel, and this conclusion is confirmed by simulation

(iii) To further evaluate the security for the considered system, the asymptotic analysis of SOP in the high signal-to-noise ratios (SNRs) is derived in this paper. The simulation results indicate that the secrecy diversity order is equal to the main channel parameters and is not influenced by the other parameters

1.2. Organization. The rest of this paper is organized as follows. Section 2 illustrates the proposed system model. Section 3 presents the premise, including the PDFs and CDFs of the main, primary, and wiretap channel. The SOP is derived in Section 4, the asymptotic SOP is then considered in Section 5. Section 6 introduces the associated evaluation of the SPSC. In Section 7, numerical results are presented based on the Monte Carlo method to verify the theoretical analysis presented in the preceding sections. Finally, Section 8 provides the conclusion for this paper.

1.3. Notations. In this paper, $I_m(\cdot)$ is the modified Bessel function with order m and we present $\Gamma(\cdot)$ as the Gamma

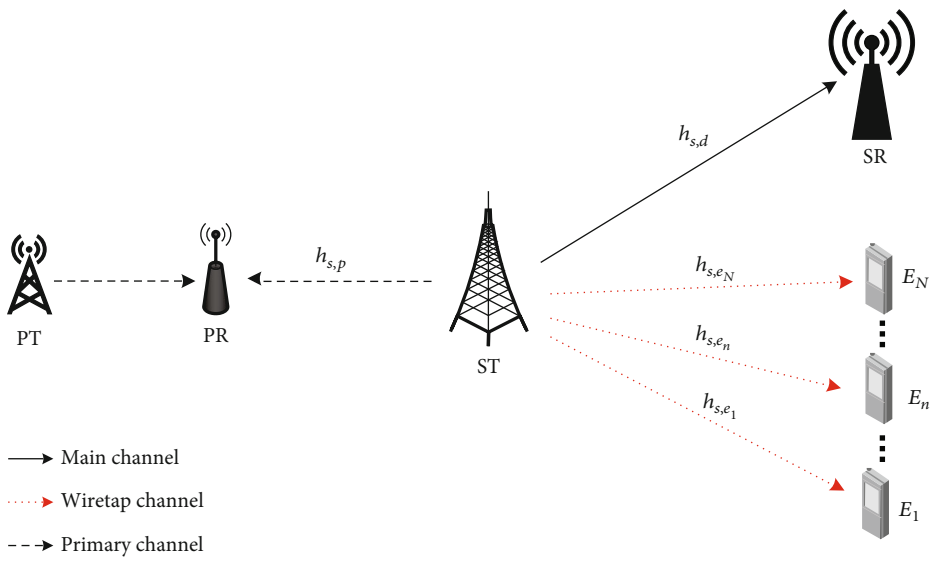

Figure 1: System model.

function. $\gamma(a, z)$ denotes the Pochhammer symbol. $(U)_k$ is the denotation of the generalized Laguerre polynomial. ${L_k}^m(\cdot)$ presents upper incomplete Gamma function. $\Psi(a, b; z)$ is the Tricomi confluent hypergeometric function defined in [33] (Equation (9.211.4)). ${}_2F_1(a, b; c; z)$ is the Gauss hypergeometric function of variable z with parameters of a, b, and c. In this paper, we represent the probability density function (PDF) in $f(\cdot)$ and the cumulative distribution function (CDF) in $F(\cdot)$.

2. System Model

The system model is presented in Figure 1. It consists of one primary transmitter (PT), one primary receiver (PR), one secondary transmitter (ST), one secondary receiver (SR), and multiple eavesdroppers $(E_i, i = 1, 2, \cdots, L_E)$. An effective way to realize spectrum sharing is to use cognitive radio networks (CRN). There are three types of CRN: interweave, underlay, and overlay. The model in this paper adopts the underlying CRN. The system model and analysis method can also be applied to other wireless fading channels.

In this paper, we assume that the considered network functions in underlay mode, i.e., the secondary users (SUs), concurrently are entitled to use the resources of the primary network. In underlay mode, communication among the secondary networks of the CRN can be implemented, but it must be carried out under the limitation of guaranteeing the quantity of service (QoS) of the primary network. ST tries to transmit information to SR in the presence of multiple cooperative wiretappers, without reducing the communication quality of the primary network. Hence, the transmitter power $\overline{P_s}$ of ST is written as

$$\overline{P_s} = \min\left(\frac{I_p}{|h_{sp}|^2}, P_{\max}\right), \tag{1}$$

where I_p is the maximum interference power at PR and $P_{\max}$ represents the peak transmit power of S restricted by designed hardware. It is assumed that there are no direct links between PT and SR and that E_i $(i = 1, 2, \cdots, L_E)$ can only eavesdrop on the signal from ST. All links of the considered system are independent, nonidentity, frequency flat, and subject to k-μ fading, with the coefficients of the channel unchanging during a transmission block.

Based on these assumptions, $h_{s,v}$ is the channel gain from S to v, $v \in (d, p, e_i, i \in (1, 2, \cdots, L_E))$; the power gains can be denoted as a k-μ random variable with channel parameters (k_v, μ_v), assuming that all channel coefficients are integers; finally, L_E is the number of wiretappers. Therefore, the received signals are

$$\begin{cases} y_{sp} = h_{sp}x_s + n_p, \\ y_{sd} = h_{sd}x_s + n_d, \\ y_{se_i} = h_{se_i}x_s + n_{e_i}, \end{cases} \tag{2}$$

where n_p, n_d, n_{ei} are the additive white Gaussian noise with zero mean value and variance of σ^2 on PR, SR, and E_i. From (2), the received instantaneous SNRs are

$$\begin{cases} \gamma_p = \dfrac{|h_{sp}|^2\overline{P_s}}{\sigma^2}, \\ \gamma_d = \dfrac{|h_{sd}|^2\overline{P_s}}{\sigma^2}, \\ \gamma_{e_i} = \dfrac{|h_{se_i}|^2\overline{P_s}}{\sigma^2}. \end{cases} \tag{3}$$

For convenience, we define $x = |h_{sp}|^2, y_d = |h_{sd}|^2$, and $y_{e_i} = |h_{se_i}|^2$. Taking into account that multiple eavesdroppers

collaborate with maximal ratio combining (MRC) technology, the total received instantaneous SNR at E is

$$\gamma_e = \sum_{i=1}^{L_E} \gamma_{e_i} = \frac{\overline{P}_s}{\sigma^2} \sum_{i=1}^{L_E} \left| h_{se_i} \right|^2. \tag{4}$$

From this, one can get the total wiretapped channel power gain as

$$y_e = \sum_{i=1}^{L_E} \left| h_{se_i} \right|^2. \tag{5}$$

3. Statistical Characteristics of k-μ Fading

Since all channels of the considered system experience the independent, nonidentity k-μ fading, from [26] (Equation (10)), the k-μ power probability density function (PDF) of the link from ST to SR or E_i can be expressed as

$$\begin{aligned} f_u(z) &= \frac{\mu_u (1+k_u)^{(\mu_u+1)/2}}{k_u^{(\mu_u-1)/2} e^{\mu_u k_u} \Omega_u} \left(\frac{z}{\Omega_u} \right)^{(\mu_u-1)/2} e^{\left(-((\mu_u(1+k_u))/\Omega_u)z\right)} \\ &\quad \times I_{\mu_u-1} \left(2\mu_u \sqrt{\frac{k_u(1+k_u)}{\Omega_u} z} \right) \\ &= \frac{1}{e^{\mu_u k_u}} \left(\frac{\mu_u(1+k_u)}{\Omega_u} \right)^{\mu_u} e^{\left(-((\mu_u(1+k_u))/\Omega_u)z\right)} \\ &\quad \times \sum_{i=0}^{\infty} \frac{(k_u \mu_u)^i}{i! \Gamma(\mu_u + i)} \left(\frac{\mu_u(1+k_u)}{\Omega_u} \right)^i z^{i+\mu_u-1}, \end{aligned} \tag{6}$$

where $z \in (y_d, x)$, $u \in (p, d)$, and p, and d denote the subscripts of the channel coefficient from ST to PR or SR, respectively; y_d,x is the channel power gain of the link from ST to SR or PR, respectively; $I_m(\cdot)$ is the modified Bessel function; and $\Gamma(\cdot)$ is the Gamma function.

Utilizing ([34] Equation (8.445)), we substitute $\lambda_u = ((1+k_u)\mu_u)/\Omega_u$ into (6), and after some algebraic manipulations, (6) can be rewritten as

$$\begin{aligned} f_u(z) &= \frac{(\lambda_u)^{(\mu_u+1)/2} (z)^{(\mu_u-1)/2} e^{-\lambda_u z}}{(\mu_u k_u)^{\mu_u - 1/2} e^{\mu_u k_u}} I_{\mu_u-1} \left(2\sqrt{\mu_u k_u} \sqrt{\lambda_u z} \right) \\ &= \frac{(\lambda_u)^{\mu_u}}{e^{\mu_u k_u}} \sum_{i=0}^{\infty} \frac{(k_u \mu_u \lambda_u)^i}{i! \Gamma(\mu_u + i)} z^{i+\mu_u-1} e^{-\lambda_u z}. \end{aligned} \tag{7}$$

According to the relation between the CDF and PDF, the CDF of the channel gain can now be derived as

$$\begin{aligned} F_u(z) &= 1 - \frac{1}{e^{\mu_u k_u}} \sum_{l=0}^{\infty} \frac{(k_u \mu_u)^l}{l!} \sum_{n=0}^{\mu_u+l-1} \frac{\lambda_u^n}{n!} (z)^n e^{-\lambda_u z} \\ &= \frac{1}{e^{\mu_u k_u}} \sum_{l=0}^{\infty} \frac{(k_u \mu_u)^l}{l! \Gamma(\mu_u + l)} \gamma(\mu_u + l, \lambda_u z), \end{aligned} \tag{8}$$

where $\gamma(\mu_u + l, \lambda_u z)$ denotes the lower incomplete Gamma function from ([34] Equation (8.350.1)).

In the considered system, all eavesdropping links, though independent, are not necessarily identical, and the cooperative eavesdroppers all apply MRC techniques, such that the total channel gain of all of the wiretap links is written as $y_e = \sum_{l=1}^{L} y_{ei}$, where y_{ei} is the channel gain of the link from the transmitter to E_i and L is the number of eavesdroppers. Therefore, the PDF of y_e is given by [33] (Equation (3))

$$\begin{aligned} f(y_e) &= \frac{e^{-(y/2\beta)} {y_e}^{U-1}}{(2\beta)^U \Gamma(U)} \sum_{k=0}^{\infty} \frac{k! c_k}{(U)_k} L_k^{(U-1)} \left(\frac{U y_e}{2\beta\xi} \right) \\ &= \frac{e^{-(y_e/2\beta)}}{(2\beta)^U} \sum_{k=0}^{\infty} c_k \sum_{q=0}^{k} \frac{(-k)_q {y_e}^{q+U-1}}{q! \Gamma(U+q)} \left(\frac{U}{2\beta\xi} \right)^q, \end{aligned} \tag{9}$$

where $(U)_k = \Gamma(U+k)/\Gamma(U)$ denotes the Pochhammer symbol [32], the series representation of the generalized Laguerre polynomial $L_k^{(U-1)}$ ([35] Equation (05.08.02.0001.01)). The efficient c_k in $f(y_e)$ can be calculated as

$$\begin{aligned} c_0 &= \left(\frac{U}{\xi} \right)^U \exp \left\{ -\frac{1}{2} \sum_{i=1}^{L} \frac{\chi_i a_i (U-\xi)}{\beta\xi + a_i(U-\xi)} \right\} \\ &\quad \times \prod_{i=1}^{L} \left(1 + \frac{a_i}{\beta} \left(\frac{U}{\xi} - 1 \right) \right)^{-\mu_{ei}}, \end{aligned} \tag{10}$$

$$c_k = \frac{1}{k} \sum_{j=0}^{k-1} c_j d_{k-j}, \quad k \geq 1, \tag{11}$$

$$\begin{aligned} d_j &= -\frac{j\beta U}{2\xi} \sum_{i=1}^{L} \chi_i a_i (\beta - a_i)^{j-1} \left(\frac{\xi}{\beta\xi + a_i(U-\xi)} \right)^{j+1} \\ &\quad + \sum_{i=1}^{L} \mu_{ei} \left(\frac{1 - a_i/\beta}{1 + (U/\xi - 1)a_i/\beta} \right)^j (j \geq 1), \end{aligned} \tag{12}$$

where $a_i = \Omega_{ei}/[2\mu_{ei}(1+k_{ei})]$; $\chi_{ei} = 2k_{ei}\mu_{ei}$; $U = \sum_{i=0}^{L} \mu_i$; L is the number of eavesdroppers; Ω_{ei} is the average power gain of the ith wiretap link; and k_{ei}, μ_{ei} are the channel coefficients of the ith wiretap link. The parameters ξ and β must be carefully selected to guarantee the convergence of the series in (9). Specifically, when $\xi < U/2$ and $\beta > 0$, (9) will converge in any finite interval; if $\xi \geq U/2$,β must be chosen as $\beta > (2 - U/\xi)a_{(n)}/2$, to make certain the uniform convergence of (9) in any finite interval, where $a_{(n)} = \max\{a_i\}$ $(i = 1, \cdots, L)$.

4. Analysis of Secrecy Outage Probability

According to information security theory, perfect secrecy connection can be guaranteed if the rate of encoding of the confidential data into code words is lower or equal to the secrecy capacity. Otherwise, the security of the information will be compromised. In this section, we focus on analyzing the SOP, which is an important performance metric of

describing the security of the considered system; it denotes the maximum achievable rate. The secrecy capacity of CRN is

$$C_s = \begin{cases} C_D - C_E \gamma_d > \gamma_e, \\ 0 \gamma_d \le \gamma_e, \end{cases} \tag{13}$$

where $C_D = \log_2(1 + \gamma_D)$ and $C_E = \log_2(1 + \gamma_e)$ are the instantaneous channel capacity of main and wiretap link (s), respectively.

For a CRN working in underlay mode, in order to guarantee the quality of the service for the primary network, the transmitter power of ST must be constrained by the maximum interference threshold, I_p, that the primary user can tolerate and its maximum transmitter power, $P_{\max}$, as

$$\overline{P_s} = \min\left\{\frac{I_p}{x}, P_{\max}\right\}. \tag{14}$$

From the definition of SOP, it can be denoted as

$$\begin{aligned} \mathrm{SOP} &= \Pr\{C_s \le C_{\mathrm{th}}\} \\ &= \Pr\left\{C_s \le C_{\mathrm{th}}, x < \frac{I_p}{P_{\max}}\right\} + \Pr\left\{C_s \le C_{\mathrm{th}}, x \ge \frac{I_p}{P_{\max}}\right\} \\ &= \underbrace{\Pr\{C_s \le C_{\mathrm{th}}, P_s = P_{\max}\}}_{\mathrm{SOP}_1} + \underbrace{\Pr\left\{C_s \le C_{\mathrm{th}}, P_s = \frac{I_p}{x}\right\}}_{\mathrm{SOP}_2}. \end{aligned} \tag{15}$$

From expression (15), we can see that the SOP is composed of two components, with reference to SOP_1 and SOP_2. The remainder of this section will consider these 2 terms in greater detail.

4.1. SOP$_1$ Analysis. When $\overline{P_s} = P_{\max}$, the work mode is the same as for a normal communication system. According to probability theory, SOP_1 can be calculated as

$$\begin{aligned} \mathrm{SOP}_1 &= \Pr\{C_s \le C_{\mathrm{th}}, \overline{P_s} = P_{\max}\} \\ &= \underbrace{\Pr\{\gamma_d \le e^{C_{\mathrm{th}}}\gamma_e + e^{C_{\mathrm{th}}} - 1\}}_{I_1} \underbrace{\Pr\left\{x \le \frac{I_p}{P_{\max}}\right\}}_{I_2}. \end{aligned} \tag{16}$$

Next, we derive an expression for I_1, from (16):

$$I_1 = \Pr\{\gamma_d \le e^{C_{th}}\gamma_e + e^{C_{\mathrm{th}}} - 1\}, \tag{17}$$

where $\gamma_d = (P_s/\sigma^2)y_d$, $\gamma_e = (\overline{P_s}/\sigma^2)y_e$, and $\overline{P_s} = P_{\max}$. Rearranging terms and using mathematical methods, we can obtain

$$\begin{aligned} I_1 &= \Pr\left\{y_d \le \Theta y_e + \frac{\Theta - 1}{\alpha}\right\} \\ &= \int_0^{\infty} F_D\left(\Theta y_e + \frac{\Theta - 1}{\alpha}\right) f_E(y_e) dy_e, \end{aligned} \tag{18}$$

where $\Theta = e^{C_{\mathrm{th}}}$ and $\alpha = P_{\max}/\sigma^2$. Taking account of the fact that $I_1 > \int_0^{\infty} F_D(\Theta y_e) f_E(y_e) dy_e$, here, we derive the lower bound of I_1 as

$$I_1^L = \int_0^{\infty} F_D(\Theta y_e) f_E(y_e) dy_e. \tag{19}$$

Substituting (8) and (9) into (19) and utilizing [38] (Equation (3.10.1.2)), we derived the expression of I_1^L as

$$\begin{aligned} I_1^L = {} & \frac{(2\beta\Theta\lambda_d)^{\mu_d}}{e^{\mu_d k_d}} \sum_{k=0}^{\infty} c_k \times \sum_{q=0}^{k} \frac{(-k)_q}{q!\Gamma(U+q)} \left(\frac{U}{\xi}\right)^q \\ & \times \sum_{i=0}^{\infty} \frac{(2\beta\Theta\lambda_d k_d \mu_d)^i}{i!\Gamma(\mu_d + i)} \frac{\Gamma(\mu_d + i + q + U)}{(\mu_d + i)} \\ & \times {}_2F_1(\mu_d + i, \mu_d + i + q + U; \mu_d + i + 1; -2\beta\Theta\lambda_d). \end{aligned} \tag{20}$$

Applying (8) to this equation, we get

$$I_2 = F_P\left(\frac{I_p}{P_{\max}}\right) = \frac{1}{e^{\mu_p k_p}} \sum_{l=0}^{\infty} C_l. \tag{21}$$

From this, the lower bound of SOP_1 can be obtained by applying (20) and (21) as

$$\begin{aligned} {\mathrm{SOP}_1}^L = {} & C_0 \sum_{k=0}^{\infty} \sum_{l=0}^{\infty} \sum_{q=0}^{k} \sum_{i=0}^{\infty} c_k C_i C_l C_q \Gamma(\mu_d + i + q + U) {}_2F_1(\mu_d \\ & + i, \mu_d + i + q + U; \mu_d + i + 1; -2\beta\Theta\lambda_d), \end{aligned} \tag{22}$$

where

$$\begin{aligned} C_0 &= \frac{1}{e^{\mu_p k_p}} \frac{(2\beta\Theta\lambda_d)^{\mu_d}}{e^{\mu_d k_d}}, \\ C_i &= \frac{(2\beta\Theta\lambda_d k_d \mu_d)^i}{i!(\mu_d + i)\Gamma(\mu_d + i)}, \\ C_l &= \frac{\left(k_p \mu_p\right)^l}{l!\Gamma\left(\mu_p + l\right)} \gamma\left(\mu_p + l, \lambda_p \frac{\mathrm{I}_p}{P_{\max}}\right), \\ C_q &= \frac{(-k)_q}{q!\Gamma(U+q)} \left(\frac{U}{\xi}\right)^q. \end{aligned} \tag{23}$$

4.2. SOP$_2$ Analysis. From (15), SOP_2 can be expressed as

$$\begin{aligned} \mathrm{SOP}_2 &= \Pr\left\{C_s \le C_{\mathrm{th}}, P_s = \frac{I_p}{x}\right\} \\ &= \Pr\left\{\frac{1 + \gamma_d}{1 + \gamma_e} \le e^{C_{th}}, x > \frac{I_p}{P_{\max}}\right\} \\ &= \Pr\left\{\gamma_d \le e^{C_{th}}\gamma_e + e^{C_{th}} - 1, x > \frac{I_p}{P_{\max}}\right\}. \end{aligned} \tag{24}$$

Let $\beta_2 = I_p/\sigma^2$, after some mathematical operations similar to those employed for I_1, we obtain the following expression for SOP_2:

$$\begin{aligned}\mathrm{SOP}_2 &= \Pr\left\{y_d \le \Theta y_e + \frac{\Theta-1}{\beta_2}x, x > \frac{I_p}{P_{\max}}\right\} \\ &= \int_{I_p/P_{\max}}^{\infty} H(x) f_P(x) dx,\end{aligned} \tag{25}$$

where $H(x) = \int_0^{\infty} F_D(\Theta y_e + ((\Theta-1)/\beta_2)x) f_E(y_e) dy_e$. Substituting (8) into this equation, after some mathematical derivation, we can obtain $H(x)$ as

$$H(x) = 1 - I_H(x), \tag{26}$$

where

$$\begin{aligned}I_H(x) = &\frac{1}{e^{\mu_d k_d}} \sum_{i=0}^{\infty} \frac{(k_d\mu_d)^i}{i!} \sum_{n=0}^{\mu_d+i-1} \frac{\lambda_d{}^n}{n!} \\ &\cdot \int_0^{\infty} e^{-\lambda_d(\Theta y_e + ((\Theta-1)/\beta_2)x)} \left(\Theta y_e + \frac{\Theta-1}{\beta_2}x\right)^n f_E(y_e) dy_e.\end{aligned} \tag{27}$$

Then, substituting (7) into (25), $I_H(x)$ can be given by

$$\begin{aligned}I_H(x) = &\frac{(\varphi)^U}{e^{k_d\mu_d}} \sum_{g=0}^{\infty} \frac{(k_d\mu_d)^g}{g!} \sum_{n=0}^{\mu_d+g-1} \frac{(1-\varphi)^n}{n!} \\ &\cdot \sum_{k=0}^{\infty} c_k \sum_{q=0}^{k} \frac{(-k)_q}{q!\Gamma(U+q)} \left(\frac{\varphi U}{\xi}\right)^q \\ &\times \sum_{d=0}^{n} C_n^d \left(\frac{\Theta-1}{\beta_2}\right)^d (q+U-1+n-d)! \\ &\cdot \left(\frac{\lambda_d}{1-\varphi}\right)^d x^d e^{-\lambda_d(((\Theta-1)/\beta_2)x)},\end{aligned} \tag{28}$$

where $\varphi = 1/(2\beta\lambda_d\Theta + 1)$; substituting (26) into (25), SOP_2 becomes

$$\mathrm{SOP}_2 = 1 - I_2 - \underbrace{\int_{I_p/P_{\max}}^{\infty} I_H(x) f_P(x) dx}_{I_{p2}}. \tag{29}$$

From this, we can substitute (28) and (7) into I_{P_2}, and with the aid of binomial expansion and [34] (Equation (3.351.3)), I_{P_2} can be shown to be

$$\begin{aligned}I_{p2} = &D_0 \sum_{i=0}^{\infty}\sum_{g=0}^{\infty} \sum_{n=0}^{\mu_d+g-1} \sum_{k=0}^{\infty}\sum_{q=0}^{k}\sum_{d=0}^{n} D_i D_g D_n c_k D_q D_d C_n^d \\ &\cdot (q+U-1+n-d)! \\ &\times \Gamma\left(\mu_p + i + d, \left(\lambda_d \frac{\Theta-1}{\beta_2} + \lambda_p\right)\frac{I_p}{P_{\max}}\right),\end{aligned} \tag{30}$$

where

$$\begin{aligned}D_0 &= \frac{\varphi^U \psi^{\mu_p}}{e^{k_d\mu_d + \mu_p k_p}}, \\ D_i &= \frac{\left(k_p\mu_p\psi\right)^i}{i!\Gamma\left(\mu_p + i\right)}, \\ D_g &= \frac{(k_d\mu_d)^g}{g!}, \\ D_n &= \frac{(1-\varphi)^n}{n!}, \\ D_d &= \left(\frac{1-\psi}{1-\varphi}\right)^d,\end{aligned} \tag{31}$$

$D_q = ((-k)_q/q!\Gamma(U+q))(\varphi U/\xi)^q$,
$\psi = \lambda_p/\lambda_d((\Theta-1)/\beta_2) + \lambda_p$.

$\Gamma(x,y)$ is the upper incomplete Gamma function ([34] Equation (8.350.2)). Making use of the derivation result, the lower SOP can be obtained as

$$\mathrm{SOP}^L = 1 - I_2 - I_{p2} + \mathrm{SOP}_1^L. \tag{32}$$

5. Analysis of Secrecy Outage Probability Asymptotic Secure Outage Probability

Although the expressions of SOP can help us perform numerical analysis on the secrecy outage performance of the considered system, asymptotic analysis can also be used to further evaluate the system performance. Therefore, we focus on the derivation of an asymptotic expression of SOP in this section and study the impact of the maximum transmit power $(P_{\max})$ of ST and the maximum interference (I_p) that PU can tolerate on the secrecy communication with multiple eavesdroppers.

In the high-SNR region, the asymptotic SOP can be defined as

$$\mathrm{SOP}^{\infty} = (G_a\Omega_d)^{-G_d} + o\left(\Omega_d{}^{-G_d}\right), \tag{33}$$

where $G_d = \mu_d$ denotes the secrecy diversity order and $o(\cdot)$ represents higher order terms. The secrecy array gain is

$$\begin{aligned}G_a = &\frac{1}{(1+k_d)\mu_d} \left\{\frac{1}{(2\beta\Theta)^U(\mu_d)e^{\mu_p k_p}} \left(\frac{\Theta-1}{\alpha}\right)^{U+\mu_d} \right. \\ &\cdot \sum_{l=0}^{\infty}\sum_{k=0}^{\infty}\sum_{q=0}^{k} A_0 C_l c_k A_q \times \left(\frac{\Theta-1}{\Theta\alpha}\right)^q \Gamma(q+U)\Psi \\ &\cdot \left(q+U, q+U+\mu_d+1; \frac{\Theta-1}{2\beta\Theta\alpha}\right) \\ &+ \frac{(2\beta\Theta)^{\mu_d}}{(\mu_d)e^{\mu_p k_p}} \sum_{k=0}^{\infty}\sum_{q=0}^{k}\sum_{d=0}^{\mu_d}\sum_{i=0}^{\infty} A_0 c_k A_q A_d A_i \Gamma \\ &\left.\cdot \left(\mu_p + i + d, \lambda_p \frac{I_p}{P_{\max}}\right)\right\}^{-(1/\mu_d)},\end{aligned} \tag{34}$$

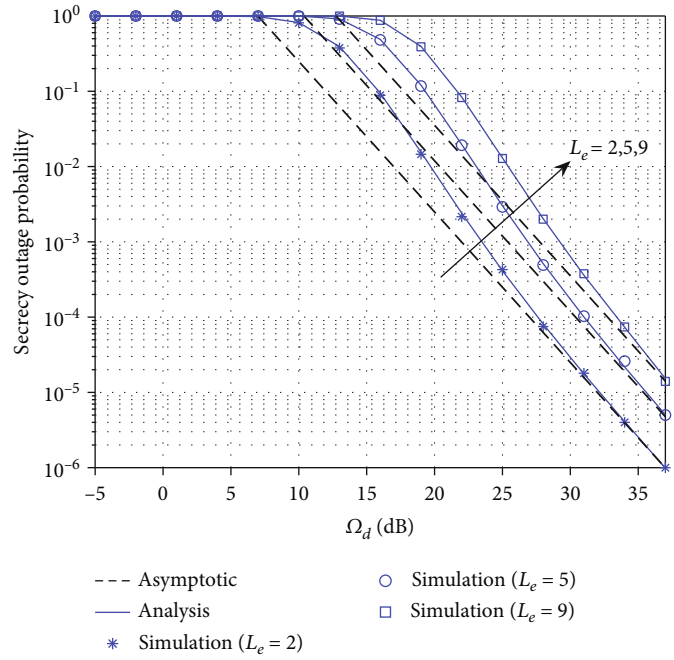

Figure 2: SOP with different L_e values, $\Omega_p = 2$, $\Omega_e = 4$,$I_p = 0.1$, $C_{\text{th}} = 0.1$; $(k_p, \mu_p) = (2, 2)$; $(k_d, \mu_d) = (3, 2)$; $(k_e, \mu_e) = (2, 2)$.

where

$$A_0 = \frac{1}{e^{\mu_d k_d}},$$

$$A_q = \frac{(-k)_q}{q!\Gamma(U+q)}\left(\frac{U}{\xi}\right)^q,$$

$$A_d = C_{\mu_d}^d \left(\frac{\Theta - 1}{\beta_2}\right)^d \left(\frac{1}{\lambda_p 2\beta\Theta}\right)^d (\mu_d - d + q + U - 1)!,$$

$$A_l = \frac{\left(k_p \mu_p \lambda_p\right)^l}{l!\Gamma\left(\mu_p + l\right)}. \tag{35}$$

6. Probability of Strictly Positive Secrecy Capacity

In information theory, the absolute security of communication can be guaranteed only when the instantaneous secrecy capacity exceeds zero. Thus, SPSC is considered to be an important indicator for measuring the secure communication system, which is given by the formula

$$\text{SPSC} = \Pr\{Cs > 0\} = 1 - \Pr\{Cs \le 0\}. \tag{36}$$

Substituting C_{th} into (16), we can get

$$\text{SOP}\Big|_{C_{\text{th}}=0} = \sum_{k=0}^{\infty}\sum_{q=0}^{k}\sum_{i=0}^{\infty} B_0 c_k A_q A_i (2\beta)^{i+q+\mu_d}\Gamma(\mu_d + i + q + U) \times {}_2F_1(\mu_d + i, \mu_d + i + q + U ; \mu_d + i + 1; -2\lambda_d\beta), \tag{37}$$

where $\lambda_d = (\mu_d(1 + k_d))/\Omega_d$; $U = \sum_{i=0}^{L}\mu_{ei}$; $B_0 = {\lambda_d}^{\mu_d}/e^{\mu_d k_d}$; $A_i = (k_d\mu_d\lambda_d)^i/i!(\mu_d + i)!$; and A_q and A_0 are the same as mentioned above. Then, SPSC can be obtained as

$$\text{SPSC} = 1 - \sum_{k=0}^{\infty}\sum_{q=0}^{k}\sum_{i=0}^{\infty} A_0 c_k A_q A_i (2\beta)^{i+q+\mu_d}\Gamma(\mu_d + i + q + U) \times {}_2F_1(\mu_d + i, \mu_d + i + q + U ; \mu_d + i + 1; -2\lambda_d\beta). \tag{38}$$

From this expression of SPSC, we can see that it does not rely on the primary channel gain but is only dependent on the gain of eavesdropping channel and main channel.

7. Numerical Results

In this section, the curves obtained by Monte Carlo simulation of SOP for the considered system are compared with the above mathematical analysis in order to consider the impact which the different related parameters have on the security of the cognitive networks. After verification, when the value of the variable reaches 50 times, it converges to a constant value. Infinite series does not affect the simulation results. The parameters utilised in this paper are set to $P_{\max} = 1$ and $\sigma = 1$, and the other parameter settings are as shown in the relevant figure.

Figure 2 shows the curves of the SOP for different numbers of eavesdroppers. It can be seen that the analysis results are in agreement with the simulation curves across the entire range of SNRs. In addition, the approximate curve is the tangent line of the exact theoretical results. Moreover, we can also see that the SOP will increase as the number of eavesdroppers increases. This is due to the fact that all of

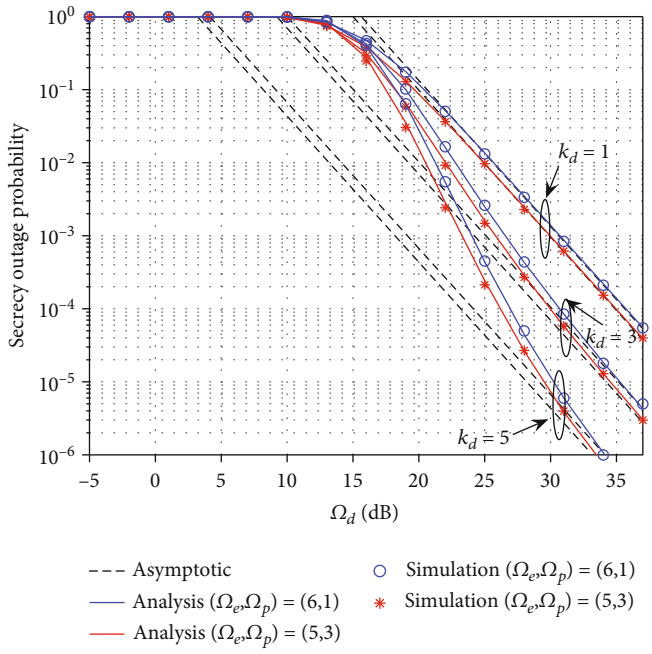

FIGURE 3: SOP with $(k_p, \mu_p) = (2,2)$, $\mu_d = 2$; $(k_{ei}, \mu_{ei})_{i=1,2,3} = (3,2)(5,2)(4,1)$; red traces $\Omega_p = 1, \Omega_e = 6$; blue traces $\Omega_p = 3, \Omega_e = 5$.

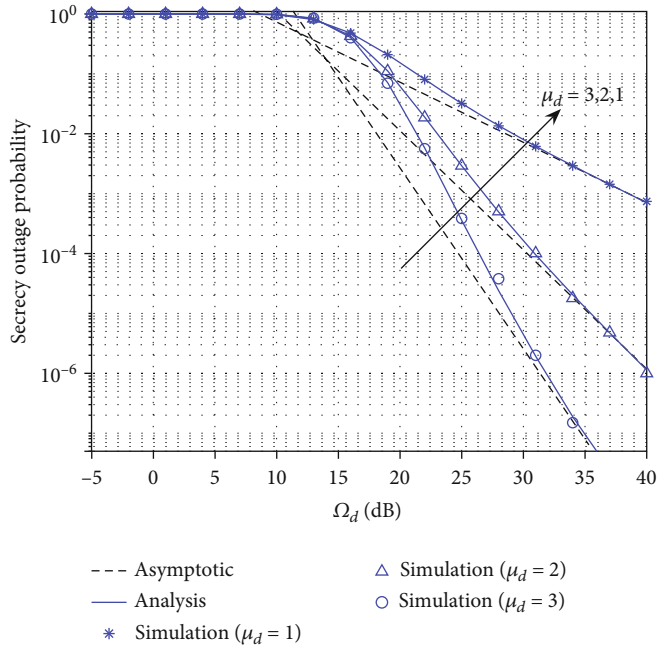

FIGURE 4: SOP with different μ_d values $\Omega_p = 2$, $\Omega_e = 6$; $I_p = 0.1$; $C_{\text{th}} = 0.01$; $(k_p, \mu_p) = (1,1)$; $k_d = 3$; $(k_{ei}, \mu_{ei})_{i=1,2,3} = (2,2)(3,1)(2,1)$.

the eavesdroppers cooperate with each other. The more eavesdroppers there are, the stronger the wiretapped signal strength, which means that the eavesdropper SNR increases, followed by an increase in the SOP.

Figures 3 and 4 provide the curves of SOP versus Ω_d for different values of k_d and μ_d. In order to observe the variation of SOP with k_d more clearly, two groups of experiments with different parameters were carried out and the results are shown in Figure 3. It can be seen that SOP decreases with the increase of either k_d or μ_d. Moreover, we can see that with this increase in the value of$k_d$or$\mu_d$which means the SNR at the receiver increases, the secrecy performance will improve.

Figures 5 and 6 show the influence of channel parameters (k_d, μ_d) on SOP. In Figure 6, we plot the different curves of SOP when k_d and μ_d are varied. The blue curve is the difference between $(k_d, \mu_d) = (1,1)$ and $(k_d, \mu_d) = (1,2)$; the red

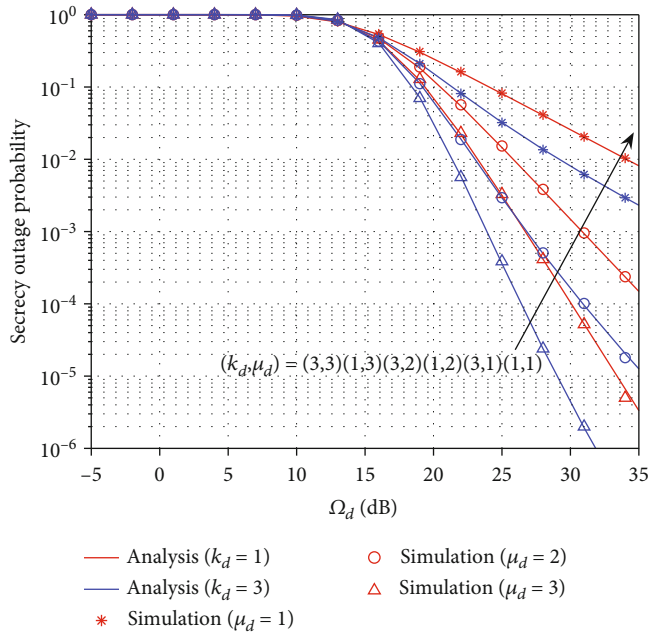

Figure 5: SOP with different μ_d and k_d values and $\Omega_p = 2, \Omega_e = 6$; $I_p = 0.1$, $C_{\text{th}} = 0.01$; $(k_p, \mu_p) = (1, 1)$; $(k_{ei}, \mu_{ei})_{i=1,2,3} = (2, 2)(3, 1)(2, 1)$.

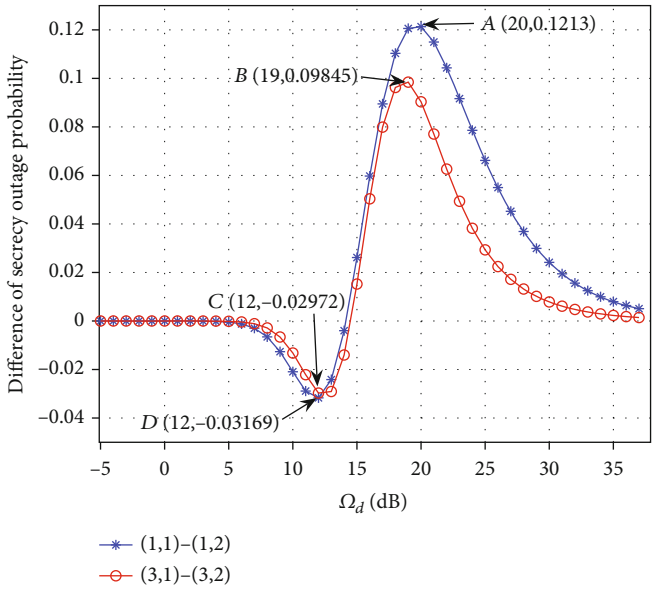

Figure 6: The difference of SOP between $(k_d, \mu_d) = (1, 1)$, $(k_d, \mu_d) = (1, 2)$ and $(k_d, \mu_d) = (3, 1)$, $(k_d, \mu_d) = (3, 2)$.

curve shows the difference of SOP at $(k_d, \mu_d) = (3, 1)$ and $(k_d, \mu_d) = (3, 2)$. It is worth noting that the two curves coincide together in the low Ω_d region; when Ω_d is very high, the difference is very small. When $\Omega_d = 12$, the difference of SOP is a negative peak; the corresponding positive maximum appears at $\Omega_d = 19, 20$. In other words, at these two points, the channel parameters (k_d, μ_d) have the greatest impact on the channel security performance.

From Figure 7, it can be seen that the higher the value of I_p, the better the security of the system, since ST can transmit more high power information. We can also see that there is a limitation for the SOP in the high I_p. This is attributed to the fact that the maximum transmit power of ST($P_{\max}$) is equal to 1, while $I_p \longrightarrow \infty$, as suggested in the above sections.

Next, without loss of generality, we plot a set of curves with different parameters to observe the effect of C_{th} on SOP. As we can see from Figure 8, the SOP for lower C_{th} outperforms the ones for the higher C_{th}. This is due to the fact that SOP is the probability that secrecy capacity C_s remains below the output threshold C_{th}. The lower the threshold C_{th} is, the smaller the corresponding probability obtained. In

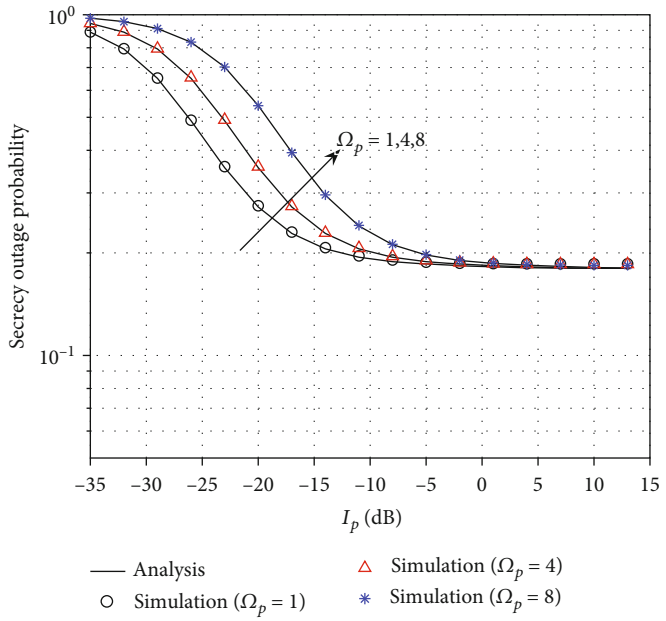

FIGURE 7: SOP versus I_p with $\Omega_d = 15$, $\Omega_e = 1$; $C_{\text{th}} = 0.1$; $(k_p, \mu_p) = (1, 1)$; $(k_d, \mu_d) = (2, 1)$; $(k_{ei}, \mu_{ei})_{i=1,2,3} = (4, 1)(5, 2)(3, 1)$.

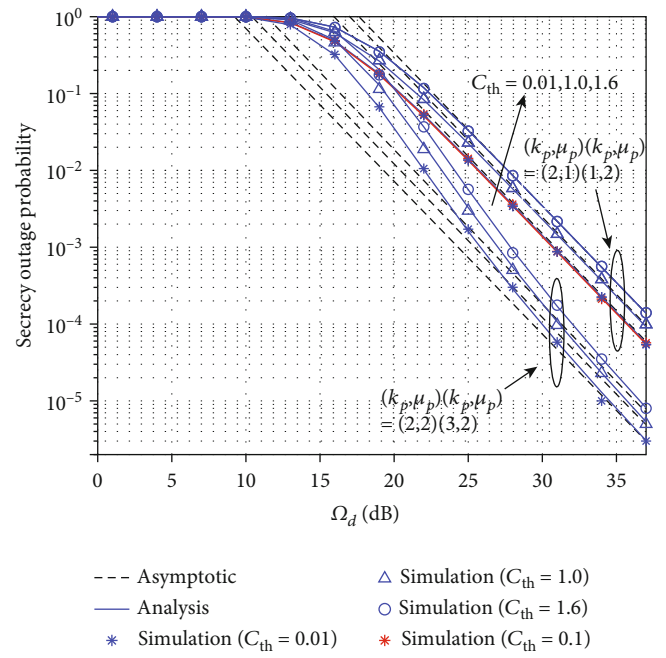

FIGURE 8: SOP versus Ω_d with $I_p = 0.1$; $(k_{ei}, \mu_{ei})_{i=1,2,3} = (4, 1)(5, 2)(3, 2)$; up ones $\Omega_p = 1, \Omega_e = 6$; $(k_p, \mu_p)(k_d, \mu_d) = (2,1)(1,2)$; down ones $\Omega_p = 3, \Omega_e = 5$; $(k_p, \mu_p)(k_d, \mu_d) = (2,2)(3,2)$.

particular, the red curve of $C_{\text{th}} = 0.01$ is almost identical to the blue curve of $C_{\text{th}} = 0.1$.

Figure 9 shows the SPSC for different values of Ω_p. From Figure 9, we can see that the SPSC decreases with the increasing values of (k_e, μ_e). This can be explained by noting that the larger (k_e, μ_e) implies a stronger signal obtained by eavesdroppers; hence, the eavesdropper SNR increases which decreases the secrecy capacity and thereby increases the SOP. In addition, we can also observe that the SPSC does not change with the variation of (k_p, μ_p) as discussed in (38).

To sum up, the interesting conclusion can be obtained that the improvement of the confidentiality is manifested by a larger value of SPSC and a smaller value of SOP. Therefore, a smaller number of eavesdropping antennas, a larger k_d, a larger μ_d, and a smaller C_{th} can improve the confidentiality of the CRN model.

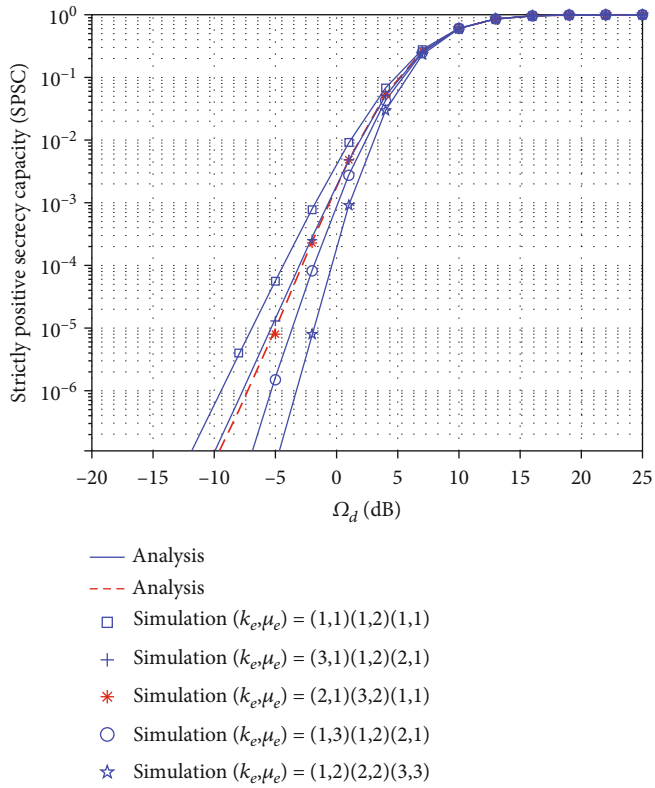

FIGURE 9: SPSC with $\Omega_p = 2, \Omega_e = 4$; $I_p = 0.1$; $\sigma = 1$, $P_{\max} = 1$; $(k_p, \mu_p) = (2, 2)$; $(k_d, \mu_d) = (1, 2)$.

8. Conclusions

In this paper, we have investigated the security performance for CRNs which operate in underlay mode with 5G, beyond 5G, and Internet of Things (IoT) technologies, where all channels experience independent, but not necessarily identically, k-μ fading. The exact and asymptotic theoretical expressions of SOP are derived for the considered system in the presence of multiple eavesdroppers. We also derive an equivalent expression for the SPSC of such a system. These resulting formulae show that the secrecy diversity order relies on the main channel parameter. This is corroborated with simulation results, which also prove this conclusion. Finally, Monte Carlo simulation results are presented to verify these analytical expressions and illustrate the influence which factors have on the secrecy performance versus the SNR ratio (s) of the channel (s).

Data Availability

Data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest about the publication of this paper.

References

[1] L. Xu, X. Yu, and T. A. Gulliver, "Intelligent outage probability prediction for mobile IoT networks based on an IGWO-Elman neural network," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1365–1375, 2021.

[2] C. E. Shannon, "Communication theory of secrecy systems∗," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] A. Mathur and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Communications Letters*, vol. 7, no. 6, pp. 1038–1041, 2018.

[5] K. N. Le, "SOP under dual correlated Rician fading," in *2018 24th Asia-Pacific Conference on Communications (APCC)*, pp. 68–72, Ningbo, China, 2018.

[6] C. Liu and R. Malaney, "Location-based beamforming and physical layer security in Rician wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7847–7857, 2016.

[7] M. Ahmed and L. Bai, "Secrecy capacity of artificial noise aided secure communication in MIMO Rician channels," *IEEE Access*, vol. 6, pp. 7921–7929, 2018.

[8] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical layer security over generalized gamma fading channels," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1257–1260, 2015.

[9] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M. Alouini, "Secrecy capacity analysis over α-μ fading channels," *IEEE*

Communications Letters, vol. 21, no. 6, pp. 1445–1448, 2017.

[10] H. Zhao, Z. Liu, L. Yang, and M. Alouini, "Secrecy analysis in DF relay over generalized-*K* fading channels," *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 7168–7182, 2019.

[11] J. M. Moualeu and W. Hamouda, "Secrecy performance analysis over mixed α-μ and κ-μ fading channels," in *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Barcelona, 2018.

[12] J. Sun, X. Li, M. Huang, Y. Ding, J. Jin, and G. Pan, "Performance analysis of physical layer security over k-μ and k-μ shadowed fading channels," *IET Communications*, vol. 12, no. 8, pp. 970–975, 2018.

[13] L. Kong, G. Kaddoum, and H. Chergui, "On physical layer security over Fox's H-function wiretap fading channels," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6608–6621, 2019.

[14] M. K. Kundu, A. S. Sumona, A. S. M. Badrudduza, and S. Shabab, "Analysis of secrecy performance over correlated η-μ fading channels," in *IEEE International Conference on Signal Processing, Information, Communication & Systems (SPICSCON)*, pp. 100–103, Dhaka, Bangladesh, 2019.

[15] J. Sun, H. Bie, X. Li, J. Zhang, G. Pan, and K. M. Rabie, "Secrecy performance analysis of SIMO systems over correlated kappa–mu shadowed fading channels," *IEEE Access*, vol. 7, pp. 86090–86101, 2019.

[16] X. Li, M. Zhao, M. Zeng et al., "Hardware impaired ambient backscatter NOMA systems: reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, 2021.

[17] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12286–12290, 2020.

[18] X. Li, H. Mengyan, Y. Liu, V. G. Menon, A. Paul, and Z. Ding, "I/Q imbalance aware nonlinear wireless-powered relaying of B5G networks: security and reliability analysis," *IEEE Transactions on Network Science and Engineering*, 2020.

[19] H. Lei, H. Zhang, I. S. Ansari et al., "On secrecy outage of relay selection in underlay cognitive radio networks over *Nakagami-m* fading channels," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 614–627, 2017.

[20] H. Lei, J. Zhang, K. Park, I. S. Ansari, G. Pan, and M. Alouini, "Secrecy performance analysis of SIMO underlay cognitive radio systems with outdated CSI," *IET Communications*, vol. 11, no. 12, pp. 1961–1969, 2017.

[21] J. Park, C. Jang, and J. H. Lee, "Outage analysis of underlay cognitive radio networks with multihop primary transmission," *IEEE Communications Letters*, vol. 20, no. 4, pp. 800–803, 2016.

[22] K. Shim, N. T. Do, B. An, and S. Nam, "Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information," in *International Conference on Electronics, Information, and Communications (ICEIC)*, pp. 1–4, Da Nang, 2016.

[23] L. Sboui, Z. Rezki, and M. Alouini, "Energy-efficient power allocation for underlay cognitive radio systems," *IEEE Transactions on Cognitive Communications and Networking*, vol. 1, no. 3, pp. 273–283, 2015.

[24] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over *Nakagami- m* fading channels," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 609–612, 2014.

[25] W. Lee, "Resource allocation for multi-channel underlay cognitive radio network based on deep neural network," *IEEE Communications Letters*, vol. 22, no. 9, pp. 1942–1945, 2018.

[26] H. Zhao, H. Liu, Y. Liu, C. Tang, and G. Pan, "Physical layer security of maximal ratio combining in underlay cognitive radio unit over Rayleigh fading channels," in *IEEE International Conference on Communication Software and Networks (ICCSN)*, pp. 201–205, Chengdu, 2015.

[27] A. Pandey, S. Yadav, D. T. Do, and R. Kharel, "Secrecy performance of cooperative cognitive AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15095–15112, 2020.

[28] M. V. Nguyen and D. Do, "Evaluating secrecy performance of cooperative NOMA networks under existence of relay link and direct link," *International Journal of Communication Systems*, vol. 33, no. 6, article e4284, 2019.

[29] M D, "The κ–μ distribution and the η–μ distribution," *IEEE Antennas & Propagation Magazine*, vol. 49, no. 1, pp. 68–81, 2007.

[30] S. L. Cotton and D. E. Simmons, "Secrecy capacity analysis over κ–μ fading channels: theory and applications," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3011–3024, 2016.

[31] J. M. Moualeu and W. Hamouda, "On the secrecy performance analysis of SIMO systems over κ–μ fading channels," *IEEE Communications Letters*, vol. 21, no. 11, pp. 2544–2547, 2017.

[32] K. P. Peppas, "Sum of nonidentical squared k-μ variates and applications in the performance analysis of diversity receivers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 413–419, 2012, Dhaka, Bangladesh, 2019, pp. 100-103.

[33] A. Roy, P. Maji, G. Cherukuri, and S. Kundu, "PHY layer security for IOT in κ-μ fading channel," in *9th International Conference on Communication Systems and Networks (COMSNETS)*, pp. 472–475, Bangalore, 2017.

[34] I. Gradshteyn and I. Ryzik, *Table of Integrals, Series, and Products*, Academic, San Diego, CA, USA, 7th edition, 2007.

[35] Eq. (05.08.02.0001.01), https://functions.wolfram.com/.