Secrecy Performance Analysis of a Cognitive Network for IoT over $k$-$\mu$ Channels

Junxia Li, Hui Zhao, and Michael Johnson

1The College of Information Science and Engineering, Xinjiang University, 830046 Urumqi, China
2Department 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

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 \(\alpha\)-\(\mu\) distribution and the eavesdropping link was modelled as \(k\)-\(\mu\) 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 \(k\)-\(\mu\) 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 \(\eta\)-\(\mu\) fading channels [14] and \(k\)-\(\mu\) 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].
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)). $F(a,b;c;z)$ 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 $P_s$ of ST is written as

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

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 $k$-$\mu$ 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 $v$, $v \in \{d, p, e, i | 1 \leq i \leq L_E\}$; the power gains can be denoted as a $k$-$\mu$ random variable with channel parameters ($k_v$, $\mu_v$), assuming that all channel coefficients are integers; finally, $L_E$ is the number of wiretappers. Therefore, the received signals are

$$ \begin{align*}
  y_p &= h_{sp}x_s + n_p, \\
  y_d &= h_{sd}x_d + n_d, \\
  y_{ei} &= h_{se_i}x_s + n_{ei},
\end{align*} \tag{2} $$

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

$$ \begin{align*}
  y_p &= \frac{|h_{sp}|^2 P_s}{\sigma^2}, \\
  y_d &= \frac{|h_{sd}|^2 P_s}{\sigma^2}, \\
  y_{ei} &= \frac{|h_{se_i}|^2 P_s}{\sigma^2}. \tag{3}
\end{align*} $$

For convenience, we define $x = |h_{sp}|^2$, $y_d = |h_{sd}|^2$, and $y_{ei} = |h_{se_i}|^2$. Taking into account that multiple eavesdroppers...
collaborate with maximal ratio combining (MRC) technology, the total received instantaneous SNR at $E$ is

$$y_e = \sum_{i=1}^{L} y_{e_i} = \frac{P}{\sigma^2} \sum_{i=1}^{L} |h_{e_i}|^2. \quad (4)$$

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

$$y_{e'} = \sum_{i=1}^{L} |h_{e_i}|^2. \quad (5)$$

### 3. Statistical Characteristics of $k$-$\mu$ Fading

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

$$f_u(z) = \frac{\mu_u(1 + k_u)^{(\mu_u+1)/2}}{k_u^{(\mu_u+1)/2}e^{k_u} \Omega_u} \left(\frac{z}{\Omega_u}\right)^{(\mu_u+1)/2} e^{-((\mu_u+1)z)/\Omega_u} \times I_{\mu_u-1} \left(2 \mu_u \frac{k_u(1 + k_u)}{\Omega_u} z \right) \times 1 + \frac{\mu_u(1 + k_u)}{\Omega_u} \frac{e^{-((\mu_u+1)z)/\Omega_u}}{\Omega_u} \sum_{i=0}^{\infty} \frac{(k_u \mu_u)^i}{i!} \left(\frac{\mu_u(1 + k_u)}{\Omega_u} \right)^i z^{i+\mu_u-1},$$

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

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

$$f_u(z) = \frac{(\lambda_u)^{(\mu_u+1)/2} (z)^{\mu_u+1/2} e^{-\lambda_u z}}{(\mu_u \lambda_u)^{1/2} e^{\mu_u \lambda_u}} \times I_{\mu_u-1} \left(2 \sqrt{\mu_u k_u \lambda_u} \frac{z}{\Omega_u} \right) \times \frac{(k_u \mu_u)^i}{i!} \left(\frac{\mu_u(1 + k_u)}{\Omega_u} \right)^i e^{z^{i+\mu_u-1}}.$$

(7)

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

$$F_u(z) = 1 - \frac{1}{e^{\mu_u \lambda_u}} \sum_{j=0}^{\infty} \frac{(k_u \mu_u)^j}{j!} \left(\frac{\mu_u(1 + k_u)}{\Omega_u} \right)^j (z)^j e^{-\lambda_u z} = \frac{1}{e^{\mu_u \lambda_u}} \sum_{j=0}^{\infty} \frac{(k_u \mu_u)^j}{j!} \gamma(\mu_u + 1, \lambda_u z),$$

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 $y_{e'} = \sum_{i=1}^{L} y_{e_i}$, where $y_{e_i}$ 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))

$$f(y_{e'}) = \frac{e^{-(y_{e'})/2}}{(2\beta)^{L} U} \left(\sum_{i=0}^{\infty} \frac{k_{e_i} \lambda_{e_i} L_{k_{e_i}(U-1)} (U y_{e'})}{2\beta^2} \right),$$

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

$$c_0 = \left(\frac{U}{\xi}\right)^{U} \exp \left\{ -\frac{1}{2} \sum_{i=0}^{\infty} \frac{\chi_{a_i}(U - \xi)}{k_{e_i}^2 + a_i^2(U - \xi)} \right\},$$

$$c_k = \frac{1}{k} \sum_{j=0}^{k-1} c_{k-j} \chi_{a_i} \left(\frac{U}{\xi} - 1\right)^{-\mu_u} H_{\mu_u},$$

(10)

$$d_j = \frac{-j\beta U}{2k}, \sum_{i=1}^{k} \chi_{a_i}(\beta - a_i)^{-1} \left(\frac{\xi}{\beta k_{e_i} + a_i(U - \xi)}\right)^{j+1} + \sum_{i=1}^{k} \mu_{e_i}(\beta - a_i)^{-1} \left(\frac{1 - a_i/\beta}{1 + (U/\xi - 1)a_i/\beta}\right)^j, \quad (j \geq 1),$$

where $a_i = \chi_{a_i}([2k_{e_i} - k_{e_i}]/H_{\mu_u}) \chi_{a_i} = 2k_{e_i} H_{\mu_u} / U = \sum_{i=1}^{k} \mu_{e_i} U$ is the number of eavesdroppers; $\Omega_{e_i}$ is the average power gain of the ith wiretap link; and $k_{e_i}, H_{\mu_u}$ are the channel coefficients of the ith wiretap link. The parameters $\xi$ and $\beta$ 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 $\xi \geq U/2 \beta$ must be chosen as $\beta > (2 - U/\xi)\alpha_{a_i}/2$, to make certain the uniform convergence of (9) in any finite interval, where $a_{a_i} = \max \{ a_i \} (i = 1, \ldots, L)$.

### 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
where $\Theta = \frac{C_{\text{in}}}{\alpha}$ and $\alpha = P_{\text{max}}/\sigma^2$. Taking account of the fact that $I_1 > \int_0^\infty F_D(\Theta y_c) f_E(y_c) dy_c$, here, we derive the lower bound of $I_1$ as

$$I_1^L = \int_0^{\infty} F_D(\Theta y_c) f_E(y_c) dy_c.$$ 

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

$$I_1^L = \frac{2(2\Theta \lambda_d) x}{\sigma^2} \sum_{k=0}^{\infty} \frac{k}{q} q! \Gamma(U + q) \left( \frac{U}{\eta} \right)^q$$

Applying (8) to this equation, we get

$$I_2 = F_p \left( \frac{I_p}{P_{\text{max}}} \right) = \frac{1}{\sigma^2} \sum_{l=0}^{\infty} C_l.$$ 

From this, the lower bound of SOP1 can be obtained by applying (20) and (21) as

$$\text{SOP}_1^L = \sum_{k=0}^{\infty} \sum_{l=0}^{\infty} \sum_{q=0}^{\infty} C_i C_l C_q \Gamma \left( \mu_d + i + q + U \right) \right) F_1(\mu_d + i + q + U \mu_d + i + 1 - 2\Theta \lambda_d).$$ 

where

$$C_0 = \frac{1}{\sigma^2}\left( \begin{array}{c}
\frac{2\Theta \lambda_d}{\sigma^2} \\
\frac{2\Theta \lambda_d}{\sigma^2} 
\end{array} \right)$$

$$C_i = \frac{1}{\mu_d + i \Gamma(\mu_d + i)} \left( \begin{array}{c}
\frac{2\Theta \lambda_d}{\sigma^2} \\
\frac{2\Theta \lambda_d}{\sigma^2} 
\end{array} \right)$$

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

$$I_1 = \Pr \left\{ y_d \leq e^{C_{\text{in}}} y_c + e^{C_{\text{th}} - 1}, \right\} \left\{ x \leq \frac{I_p}{P_{\text{max}}} \right\}.$$ 

where $y_d = (P_i/\sigma^2) y_d$, $y_c = (P_c/\sigma^2) y_c$, and $\overline{P}_s = P_{\text{max}}$. Rearranging terms and using mathematical methods, we can obtain

$$I_1 = \int_0^{\infty} F_D(\Theta y_c + \frac{\Theta - 1}{\alpha}) f_E(y_c) dy_c.$$

4.2. SOP2 Analysis. From (15), SOP2 can be expressed as

$$\text{SOP}_2 = \Pr \left\{ C_i \leq C_{\text{th}}, P_s = \frac{I_p}{X} \right\}$$

$$= \Pr \left\{ \frac{1+y_d}{1+y_c} \leq e^{C_{\text{in}}, x > \frac{I_p}{P_{\text{max}}} \right\}$$

$$= \Pr \left\{ y_d \leq e^{C_{\text{in}}} y_c + e^{C_{\text{th}} - 1}, x > \frac{I_p}{P_{\text{max}}} \right\}.$$
Let $\beta_2 = I_p \sigma_2^2$, after some mathematical operations similar to those employed for $I_1$, we obtain the following expression for $SOP_2$:

$$SOP_2 = \Pr \left\{ y_d \leq \Theta y_c + \Theta - 1 \frac{I_p}{\beta_2}, x > \frac{I_p}{P_{\text{max}}} \right\}$$

$$= \int_{\frac{I_p}{P_{\text{max}}}}^{\infty} H(x)f_p(x)dx,$$

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

$$H(x) = 1 - I_{H}(x).$$

Then, substituting (7) into (25), $I_{H}(x)$ can be given by

$$I_{H}(x) = \frac{1}{e^{\lambda_d(\Theta - 1)/\beta_2}} \sum_{n=0}^{\infty} \frac{(k_{dH})^n}{n!} \sum_{m=0}^{n} \lambda_d^m \left( \Theta - 1 - \frac{I_p}{\beta_2} \right)^n e^{-\lambda_d(\Theta - 1)/\beta_2}.$$

where $\varphi = 1/(2\beta_2 \lambda_d + 1)$; substituting (26) into (25), SOP$_2$ becomes

$$SOP_2 = 1 - I_2 - \int_{I_p/P_{\text{max}}}^{\infty} I_{H}(x)f_p(x)dx.$$

From this, we can substitute (28) and (7) into $I_{p_2}$, and with the aid of binomial expansion and [34] (Equation (3.35.2)), $I_{p_2}$ can be shown to be

$$I_{p_2} = \sum_{i=0}^{\infty} \sum_{q=0}^{i} \sum_{k=0}^{q} \sum_{l=0}^{k} \sum_{n=0}^{l} \sum_{m=0}^{n} \sum_{p=0}^{m} D_o D_p D_q D_l D_m C_i C_q^d$$

$$D_0 = \frac{\varphi U^i \varphi^i}{e^{\varphi U} \varphi^i},$$

$$D_2 = \frac{\left(k_{dH}\varphi\right)^i}{i!},$$

$$D_q = \frac{\left(k_{dH}\varphi\right)^q}{q!},$$

$$D_n = \frac{(1 - \varphi)^n}{n!},$$

$$D_d = \frac{(1 - \varphi)^d}{1 - \varphi}.$$

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 ($P_{\text{max}}$) 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

$$SOP_{\text{asym}} = (G_d \Omega_d)^{-G_d} + o(\Omega_d^{-G_d}),$$

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

$$G_a = \frac{1}{1 + k_d \mu_d} \left\{ \frac{1}{(2\beta \Theta)^{U+\mu_d}} \left( \Theta - 1 \right)^{U+\mu_d} \right\}$$

$$\times (q + U - 1 + n - d)!$$

$$\times G \left( \mu_d + i + d, \left( \Theta - 1 \frac{I_p}{P_{\text{max}}} \right) \right).$$

where

$$D_0 = \frac{\varphi U^i \varphi^i}{e^{\varphi U} \varphi^i},$$

$$D_2 = \frac{\left(k_{dH}\varphi\right)^i}{i!},$$

$$D_q = \frac{\left(k_{dH}\varphi\right)^q}{q!},$$

$$D_n = \frac{(1 - \varphi)^n}{n!},$$

$$D_d = \frac{(1 - \varphi)^d}{1 - \varphi}.$$
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

$$\text{SPSC} = \Pr \{ C_s > 0 \} = 1 - \Pr \{ C_s \leq 0 \}. \quad (36)$$

Substituting $C_{\text{in}}$ into (16), we can get

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

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

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

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 $P_{\text{max}} = 1$ 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
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 $\Omega_d$ for different values of $k_d$ and $\mu_d$. 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 $\mu_d$. 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 3 and 4 show the influence of channel parameters $(k_d, \mu_d)$ on SOP. In Figure 6, we plot the different curves of SOP when $k_d$ and $\mu_d$ are varied. The blue curve is the difference between $(k_d, \mu_d) = (1, 1)$ and $(k_d, \mu_d) = (1, 2)$; the red
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 $\Omega_d$ region; when $\Omega_d$ 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 $(k_d, \mu_d)$ 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 $I_p \to \infty$, 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
particular, the red curve of $C_{th} = 0.01$ is almost identical to the blue curve of $C_{th} = 0.1$.

Figure 8 shows the SPSC for different values of $\Omega_p$. From Figure 9, we can see that the SPSC decreases with the increasing values of $(k_e, \mu_e)$. This can be explained by noting that the larger $(k_e, \mu_e)$ 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 $(k_p, \mu_p)$ 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 $\mu_d$, and a smaller $C_{th}$ can improve the confidentiality of the CRN model.
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, $k$-$\mu$ 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 $\alpha$-$\mu$ fading channels,” *IEEE
REFERENCES

[10] H. Zhao, Z. Liu, L. Yang, and M. Alouini, “Secrecy analysis in DF relay over generalized-$\kappa$ 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 $\alpha$–$\mu$ and $\kappa$–$\mu$ shadowed 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 $\kappa$–$\mu$ and $\kappa$–$\mu$ 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. M. Kundu, A. S. Sumona, A. S. M. Badrudduza, and S. Shabab, “Analysis of secrecy performance over correlated $\eta$–$\mu$ 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 BSG 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. Shou, 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 $\kappa$–$\mu$ distribution and the $\eta$–$\mu$ 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 $\kappa$–$\mu$ 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 $\kappa$–$\mu$ fading channels,” IEEE Communications Letters, vol. 21, no. 11, pp. 2544–2547, 2017.

[32] K. P. Peppas, “Sum of nonidentical squared $\kappa$–$\mu$ 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 $\kappa$–$\mu$ 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/.