Hindawi
Security and Communication Networks
Volume 2020, Article ID 8842012, 9 pages
https://doi.org/10.1155/2020/8842012

Research Article

Secrecy Analysis of Cognitive Radio Networks over Generalized Fading Channels

Jiangfeng Sun,[1] Zhisong Bie,[1] Hongxia Bie,[1] Pengfei He,[2] and Machao Jin[3]

[1]*The School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100084, China*
[2]*The Institute of Science and Technology for Opto-electronic Information, Yantai University, Yantai Shandong 264005, China*
[3]*Department of Information and Communication, Shanxi Metallurgical Geotechnical Engineering Investigation Co., Ltd., Taiyuan, Shanxi 030002, China*

Correspondence should be addressed to Zhisong Bie; zhisongbie@bupt.edu.cn

Received 24 July 2020; Revised 20 August 2020; Accepted 9 September 2020; Published 22 September 2020

Academic Editor: Lingwei Xu

At present, the fifth generation (5G) communication networks are in the time of large-scale deployment principally because its characteristics consists of large bandwidth, fast response, and high stability. As a partner of 5G, the Internet of Things (IoT) involves billions of devices around the world, which can make the wireless communication environment more intelligent and convenient. However, the problem that cannot be ignored is the physical layer security of 5G-IoT networks. Based on this, we perform a security analysis of cognitive radio networks (CRN) for IoT, where the CRN is the single-input multiple-output (SIMO) model experiencing κ-μ shadowed fading with multiple eavesdroppers. To analyze the confidentiality of the system under consideration, we analyze the security performance for the considered IoT systems with the help of the derived secure outage probability (SOP) and probability of strictly positive secrecy capacity (SPSC). As a verification of the theoretical formula, Monte Carlo simulation is also provided. The results of great interest are the factors that can produce better security performance in high SNRs region which consist of smaller M, smaller k, and larger N, and larger μ, smaller I_P, and smaller R_{th}.

1. Introduction

On the fifth generation (5G) networks, Internet of Things (IoT) technology makes the data exchange between people and things and objects and objects more rapid and intelligent [1]. However, the physical layer security (PLS) problem, that is, the confidential signals between IoT entities are easy to be intercepted and decoded by eavesdroppers [2]. Therefore, how to improve the confidentiality performance of IoT systems is an urgent issue to be solved. There are two methods to deal with this problem; the first is based on the encryption and decryption algorithm of the network layer and above, and the other is to improve the security capacity of the channel by using the characteristics of the fading channel. In recent years, the latter, namely, physical layer security, has gradually become a hot topic in security research. Based on the channel capacity theory [3] and the classic Wyner's eavesdropping model [4], Wei et al. in [5] described the optimal power of artificial noise to ensure the best antieavesdropping ability in the wiretap networks experiencing Rayleigh fading. The PLS of nonorthogonal multiple access (NOMA) networks [6] and relaying 5G networks [7] with Rayleigh channels were developed. The authors in [8] studied the factors that affect the security capability of Wyner's model based on Rician channel, where analytical SOP were deduced and proved. The physical performance and security of nonideal IoT networks over Nakagami-m fading channels were investigated through two important metrics, namely, outage probability (OP) and intercept probability (IP) [9].

Different from the channels described above, the universality of generalized channels, that can be equivalent to other fading channels, has recently received considerable attention. [10–16]. On the premise of fully considering the

actual unfavourable factors of the relaying wireless communication networks (WCNs) over Weibull channels, Li et al. [10] has completed the derivation of the exact formula of OP and the asymptote. The work in [11] developed the approximate expression of probability density function (PDF) and obtained the SOP analysis of the classical Wyner's systems over generalized-K fading channels. Based on the proposed IoT relay networks, the authors of [12] explored the theoretical derivation and simulation analysis of OP and average symbol error probability (ASEP). In [13], when all the links in the wiretap networks suffered from κ-μ fading, Bhargav et al. derived the lower limit of SOP and the closed-form expression of SPSC. Under the condition of imperfect signal transmission, the authors in [14] obtained the theoretical formula of OP in considered model over α-μ fading with two different scenarios. Referring to Wyner's classical wiretap model, Kong et al. derived and analyzed the SOP and the probability of nonzero secrecy capacity (PNZ) of Fox's H-Function [15] channels and Fisher-Snedecor F [16] channels, respectively.

Recently, security issues are very important for popular applications such as Internet of vehicles [17], neural networks [18], and big data [19]. As a developing strategy to solve the obstacles of spectrum scarcity and power allocation in IoT networks, CRN can significantly improve the transmission range and quality have gained great attention in recent literatures [20–26]. With the aid of artificial noise, the IP in the secondary network over Gaussian channel was investigated in [20]. The cooperation of multiple secondary users will further enhance the capacity of CRN; based on this, two different protocols were proposed, and achievable ergodic secrecy rate (ESR) was used to analyze the security performance of the considered system [21]. By employing a CRN network, which suffered from Rayleigh fading and had a legitimate receiver with multiple antennas, the authors of [22] provided the derivation of PNZ and SOP. In [23, 24], Lei et al. studied the security performance of CRNs undergoing Nakagami-m fading and generalized-K fading, respectively. The study of Zhang et al. [25] proposed a method to improve the security capacity of primary networks and secondary networks simultaneously and discussed the strategy of power allocation and band sharing. The authors in [26] studied the secrecy performance of nonorthogonal multiple access (NOMA) CRN over Nakagami-m fading channels, in which connection outage probability (COP), SOP, and effective secrecy throughput (EST) were obtained in a unified form.

More recently, the κ-μ shadowed model was first introduced by Paris in [27], and it is a generalized fading channel, which can be simplified as Rayleigh, Rician shadowed, one-side Gaussian, Nakagami-m, and κ-μ under suitable conditions. Moreover, the κ-μ shadowed fading can be applied to different systems including IoT links [28], satellite channels [29], and underwater links [30]. According to the proposed mobile communication model with κ-μ shadowed fading, the authors of [31] studied the transmission performance by analyzing OP and ergodic channel capacity (ECC). The statistical characteristics of different shadowed κ-μ fading were derived in [32], where the closed-form PDF and cumulative distribution function (CDF) for envelope and signal-to-noise ratio (SNR) were obtained, respectively. The work in [33] investigated the outage performance of hexagonal network affected by κ-μ shadowed fading in term of analyzing the performance benchmark, namely, outage probability and rate. Sun et al. in [34] presented the derivation of SOP and SPSC for the systems over κ-μ shadowed distribution, in which legitimate users and eavesdroppers were both single antenna receivers. As continuations of [34], the security analyses of SIMO networks and decode-and-forward (DF) relaying networks were carried out in [35, 36].

So far, we have not discovered relative research based on CRN over κ-μ shadowed distribution in the open database, let alone the existence of multiple antennas and multi-eavesdroppers. Therefore, combined with the advantages of multiantenna technology [37, 38], this paper is explored. We first present a CRN for IoT, in which the subchannels undergo κ-μ shadowed fading. Then, we derive the mathematical expressions of SOP and SPSC under the condition of multiple eavesdroppers. Finally, Monte Carlo simulations are provided to compare with the mathematical analysis; moreover, some valuable conclusions are obtained. The work can provide theoretical basis for the security performance evaluation of WCNs (5G, Internet of vehicles, etc.).

The paper is arranged as follows; this section mainly introduces the background, related literatures, and motivation. In Section 2, we explain the CRN model for IoT over κ-μ shadowed fading channels, and the PDF and CDF of the channels with multiple eavesdropping terminals are also illustrated. SOP analysis is presented in Section 3. The theoretical derivation of SPSC is made in Section 4. Section 5 provides the numerical results and some interesting results. The conclusions of the paper appear in Section 6.

2. IOT System Model and Properties of Generalized Channels

2.1. IOT System Model. The work considers a four entities CRN model for IoT, as shown in Figure 1, where S is the data source of the secondary networks, while P is the sender of the primary networks, and D is the preset receiver, which uses multiple antennas (N_D) to receive signals. There are many eavesdroppers $(E_1, E_2, \ldots, E_M)$ equipped with multiple antennas (N_E). The secondary network is composed of S, D, and E. Underlay CRN makes spectrum sharing possible, but the cost is that the power of S will not affect the communication of the main networks. h_{SP} is interpreted as the channel coefficient of the link $(S \longrightarrow P)$ and the channel coefficients of main link $(S \longrightarrow D)$ and wiretap link $(S \longrightarrow E)$ are $\mathbf{h}_D$ and $\mathbf{h}_E$, respectively. It should be noted that $\mathbf{h}_D$ and $\mathbf{h}_E$ are vectors because of multiantenna reception at D and E. In our model, we consider passive eavesdropping scenarios, where S does not know the channel state information (CSI) of the wiretap link, but grasps the CSI of the main link.

S will communicate with P, D, and E in the considered IoT networks at the same time. Suppose the secret signal from S is x; then, we have

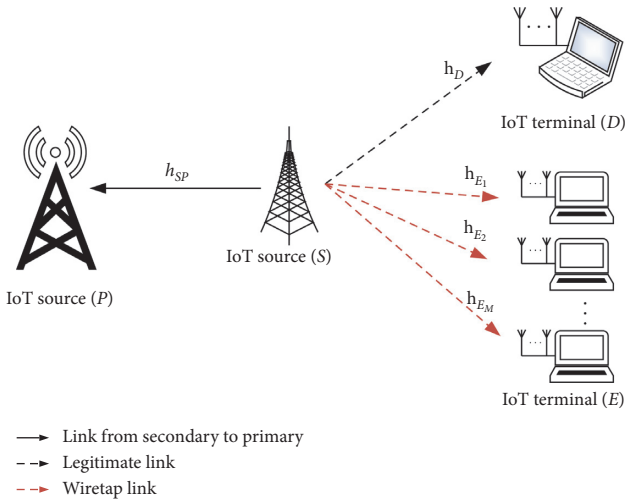

Figure 1: The CRN model for IoT.

$$\begin{aligned} y_{SP} &= \sqrt{P_S} h_{SP} x + z_{SP}, \\ \mathbf{y}_{SD} &= \sqrt{P_S} \mathbf{h}_D x + \mathbf{z}_D, \\ \mathbf{y}_{SE} &= \sqrt{P_S} \mathbf{h}_E x + \mathbf{z}_E, \end{aligned} \tag{1}$$

where P_S is the output power of S, y_{SP} is the signal received by P, z_{SP} is the complex white Gaussian noise on the link from S to P, the statistical expectation of z_{SP} is zero, and the standard deviation is σ. $\mathbf{y}_{SD}$ and $\mathbf{y}_{SE}$ represent the received signal matrices of D and E, while $\mathbf{z}_D$ and $\mathbf{z}_E$ denote noise matrices, and both standard deviations are σ.

2.2. Properties of Generalized Channels. The generalized channels considered in our IoT model is κ-μ shadowed fading channel. This section describes its statistical properties, mainly including the PDFs and CDFs for SNRs in link $(S \longrightarrow P)$, link $(S \longrightarrow D)$, and link $(S \longrightarrow E)$. Relying on [27], the PDF for κ-μ shadowed variable can be expressed as

$$\begin{aligned} f(\gamma) = {} & \frac{\mu^{\mu} m^m (1+k)^{\mu}}{\Gamma(\mu)(\mu k + m)^m \Omega^{\mu}} e^{-\mu(1+k)\gamma/\Omega} \\ & \times \gamma^{\mu-1} {}_1F_1\left(m, \mu; \frac{\mu^2 k(1+k)\gamma}{(\mu k + m)\Omega}\right), \end{aligned} \tag{2}$$

where the parameters used to determine the κ-μ shadowed variable are k, μ, and m. γ and Ω are described as the instantaneous SNR and average SNR on κ-μ shadowed fading channels, $\Gamma(\cdot)$ denotes the Gamma function (equation (8.310.1) in [39]), and ${}_1F_1(\cdot)$ is defined as confluent hypergeometric function (equation (9.14.1) in [39]), respectively.

According to (2) and [34], we can obtain the PDF and CDF for the SNR at the link from $(S \longrightarrow P)$ as

$$f_s(\gamma) = (a_s)^{\mu_s} (b_s)^{m_s} \frac{1}{\Gamma(\mu_s)} \sum_{q=0}^{\infty} \frac{(m_s)_q}{(\mu_s)_q q!} \times \left(\frac{a_s k_s \mu_s}{b_s m_s}\right)^q \gamma^{\mu_s+q-1} e^{-a_s\gamma}, \tag{3}$$

$$\begin{aligned} F_s(\gamma) = {} & b_s^{-m_s} \frac{1}{\Gamma(\mu_s)} \sum_{q=0}^{\infty} \frac{(m_s)_q (k_s\mu_s/b_s m_s)^q}{(\mu_s)_q q!} \\ & \times (\mu_s + q - 1)! \left(1 - e^{-a_s\gamma} \sum_{s=0}^{\mu_s+q-1} \frac{(a_s\gamma)^s}{s!}\right), \end{aligned} \tag{4}$$

where $a_s = \mu_s(1+k_s)/\Omega_s$, $b_s = (\mu_s k_s + m_s)/m_s$. s in the lower right corner indicates that the parameter belongs to the channel $(S \longrightarrow P)$.

Because the expected receiver (D) has N_D antennas and the maximum ratio combining (MRC) merging is adopted, the pdf for random variable (RV) at $(S \longrightarrow D)$ can be formulated as [35]

$$\begin{aligned} f_D(\gamma) = {} & (N_D a_D)^{N_D\mu_D} \frac{b_D^{-N_D m_D}}{\Gamma(N_D\mu_D)} \sum_{q=0}^{\infty} \frac{(N_D m_D)_q}{(N_D\mu_D)_q q!} \\ & \times \left(\frac{N_D a_D k_D \mu_D}{b_D m_D}\right)^q \gamma^{N_D\mu_D+q-1} e^{-N_D a_D \gamma}, \end{aligned} \tag{5}$$

where $(x)_y$ means Pochammer calculation [39]. From (4), we can deduce the CDF of RV at $S \longrightarrow D$ as

$$\begin{aligned} F_D(\gamma) = {} & b_D^{-N_D m_D} \frac{1}{\Gamma(N_D\mu_D)} \sum_{q=0}^{\infty} \frac{(N_D m_D)_q}{(N_D\mu_D)_q q!} \\ & \times \left(\frac{k_D\mu_D}{b_D m_D}\right)^q (N_D\mu_D + q - 1)! \\ & \times \left(1 - e^{-N_D a_D \gamma} \sum_{s=0}^{N_D\mu_D+q-1} \frac{(N_D a_D \gamma)^s}{s!}\right), \end{aligned} \tag{6}$$

for eavesdropping channel $(S \longrightarrow E)$ with multiple eavesdroppers cooperation. Employing [35], we can obtain the PDF of the eavesdropping link as

$$\begin{aligned} f_E(\gamma) = {} & (N_E a_E)^{N_E\mu_E} \frac{b_E^{-N_E m_E}}{\Gamma(N_E\mu_E)} \times \sum_{q=0}^{\infty} \frac{(N_E m_E)_q}{M^{N_E\mu_E+q} (N_E\mu_E)_q q!} \\ & \times \left(\frac{N_E a_E k_E \mu_E}{b_E m_E}\right)^q \gamma^{N_E\mu_E+q-1} e^{-N_E a_E \gamma/M}. \end{aligned} \tag{7}$$

3. SOP Analysis

For the IoT systems, we need clear benchmarks to measure its security performance [40]. For the passive eavesdropping scenario considered in our model, SOPs are very suitable criteria, which can be understood as the probability that the difference value between the instantaneous capacity of the

main link and the capacity of the eavesdropping link is less than a fixed threshold R_{th} [41], and SOP can be written as

$$\text{Sop} = P\{(C_D - C_E) \le R_{\text{th}}\}, \tag{8}$$

where $C_D - C_E$ is the difference value between the instantaneous capacity of $S \longrightarrow D$ and $S \longrightarrow E$.

Two constraints that must be considered in underlay CRN are (i) the power of S cannot exceed the maximum power value (P_{sm}) and (ii) the power of S should not exceed the threshold of anti-interference ability (I_P) to the primary networks. Referring to (9) and [24], SOP in underlay CRN can be expressed as

$$\begin{aligned}\text{Sop} &= P\{(C_D - C_E) \le R_{\text{th}}\} \\ &= P\{(C_D - C_E) \le R_{\text{th}}, P_S = P_{\text{sm}}\} \\ &\quad + P\left\{(C_D - C_E) \le R_{\text{th}}, P_S = \frac{I_P}{X}\right\} = P_1 + P_2,\end{aligned} \tag{9}$$

where X is the instantaneous SNR of the link of $S \longrightarrow P$. Next, we will derive P_1 and P_2 in (9).

3.1. Calculation of P_1. P_1 can be further written as

$$\begin{aligned}P_1 &= P\left\{(C_D - C_E) \le R_{\text{th}}, X \le \frac{I_P}{P_{\text{sm}}}\right\} \\ &= P\left\{\gamma_D \le \theta\gamma_E + \frac{\theta - 1}{\varsigma}\right\} P\left\{X \le \frac{I_P}{P_{\text{sm}}}\right\} = J_1 J_2,\end{aligned} \tag{10}$$

where $\theta = e^{R_{\text{th}}}$ and $\varsigma = P_{\text{sm}}/\sigma^2$, and we obtain

$$J_1 = \int_0^\infty F_D\left(\theta\gamma_E + \frac{\theta - 1}{\varsigma}\right) f_E(\gamma_E)\mathrm{d}\gamma_E. \tag{11}$$

Employing (6) and (7), we have

$$\begin{aligned}J_1 = \Lambda_1 \int_0^\infty \Bigg(1 - e^{-N_D a_D\left(\theta\gamma_E + (\theta - 1/\alpha)\right)} \times \sum_{s=0}^{N_D\mu_D + q - 1} \frac{\left(N_D a_D\left(\theta\gamma_E + (\theta - 1/\varsigma)\right)\right)^s}{s!}\Bigg) \\ \times \gamma^{N_E\mu_E + p - 1} \exp\left(-\frac{N_E a_E \gamma_E}{M}\right)\mathrm{d}\gamma_E,\end{aligned} \tag{12}$$

where

$$\begin{aligned}\Lambda_1 = \frac{b_D^{-N_D m_D}}{\Gamma(N_D\mu_D)} \sum_{q=0}^{\infty} \frac{(N_D m_D)_q \left(k_D\mu_D / b_D m_D\right)^q}{(N_D\mu_D)_q q!} \\ \times (N_D\mu_D + q - 1)! \left(N_E a_E\right)^{N_E\mu_E} \\ \times \frac{b_E^{-N_E m_E}}{\Gamma(N_E\mu_E)} \sum_{p=0}^{\infty} \frac{(N_E m_E)_p \left(N_E a_E k_E \mu_E / b_E m_E\right)^p}{M^{N_E\mu_E + p} (N_E\mu_E)_p p!},\end{aligned} \tag{13}$$

utilizing equation (1.111) in [39],

$$\left(\theta\gamma_E + \frac{\theta - 1}{\varsigma}\right)^s = \sum_{t_1=0}^{s} \left(t_1{}^s\right) \theta^{t_1} \gamma_E^{t_1} \left(\frac{\theta - 1}{\varsigma}\right)^{s - t_1}. \tag{14}$$

Then, making using of equation (3.381.4) in [39], after a more complex integral operation, we have

$$J_1 = \Lambda_1 \left(\Lambda_2 - e^{-N_D a_D(\Theta - 1/\varsigma)} \times \sum_{s=0}^{N_D\mu_D + q - 1} \frac{\left(N_D a_D\right)^s \sum_{t_1=0}^{s} (s/t_1) \theta^{t_1} (\theta - 1/\varsigma)^{s - t_1}}{s!} \times \frac{\Gamma\left(N_E\mu_E + p + t_1\right)}{\left(N_D a_D \theta + N_E a_E / M\right)^{\left(N_E\mu_E + p + t_1\right)}}\right), \tag{15}$$

where

$$\Lambda_2 = \frac{\Gamma\left(N_E\mu_E + p\right)}{\left(N_E a_E / M\right)^{\left(N_E\mu_E + p\right)}}. \tag{16}$$

From (4), J_2 is derived as

$$J_2 = P\left(X \le \frac{I_P}{P_{sm}}\right) = \frac{b_s^{-m_s}}{\Gamma(\mu_s)} \sum_{q=0}^{\infty} \frac{(m_s)_q \left(k_s\mu_s / b_s m_s\right)^q (\mu_s + q - 1)!}{(\mu_s)_q q!} \times \left(1 - e^{-a_s\left(I_P / P_{sm}\right)} \sum_{s=0}^{\mu_s + q - 1} \frac{\left(a_s I_P / P_{sm}\right)^s}{s!}\right). \tag{17}$$

3.2. Calculation of P_2. It can be seen from (9), P_2 is stated as

$$P_2 = P\left\{\left(C_D - C_E\right) \le R_{\text{th}}, P_S = \frac{I_P}{X}\right\}. \tag{18}$$

Referring to [22], we can rewrite P_2 as

$$P_2 = \int_{I_P/P_{sm}}^{\infty} G(x) f_s(x) \mathrm{d}x, \tag{19}$$

where

$$G(x) = \int_0^{\infty} F_D\left(\theta y + \frac{(\theta - 1)x}{\xi}\right) f_E(y) \mathrm{d}y. \tag{20}$$

In (20), $\xi = I_P/\sigma^2$. By means of (6) and (7), $G(x)$ can be derived as

$$G(x) = \Lambda_1\left(\Lambda_2 - e^{-N_D a_D (\theta - 1)x/\xi} \Lambda_3 x^{s - t_2}\right), \tag{21}$$

where

$$\begin{aligned}\Lambda_3 = &\frac{\Gamma\left(N_E\mu_E + p + t_2\right)}{\left(N_D a_D \theta + N_E a_E/M\right)^{\left(N_E\mu_E + p + t_1\right)}} \\ &\times \sum_{s=0}^{N_D\mu_D + q - 1} \frac{\left(N_D a_D\right)^s}{s!} \sum_{t_2=0}^{s} \left(t_2{}^s\right) \theta^{t_2} \left(\frac{\theta - 1}{\xi}\right)^{s - t_2}.\end{aligned} \tag{22}$$

Replacing $G(x)$ in (19) with (21), then, after the integral is completed by using equation (3.351.2) in [39], we obtain the derivation of P_2 as

$$\begin{aligned}P_2 = &\Lambda_1 a_s^{\mu_s} b_s^{m_s} \frac{1}{\Gamma(\mu_s)} \sum_{q=0}^{\infty} \frac{\left(m_s\right)_q \left(a_s k_s \mu_s / b_s m_s\right)^q}{\left(\mu_s\right)_q q!} \times \Lambda_2 a_s^{-\left(\mu_s + q\right)} \Gamma\left(\mu_s + q, a_s \frac{I_P}{P_{\max}}\right) \\ &- \Lambda_3 a_s^{-\left(s - t_2 + \mu_s + q\right)} \Gamma\left(s - t_2 + \mu_s + q, \left(a_s + \frac{N_D a_D (\theta - 1)}{\xi}\right) \frac{I_P}{P_{sm}}\right),\end{aligned} \tag{23}$$

where $\Gamma(a, b)$ is called the incomplete Gamma function (equation (8.350.2) in [39]).

According to (15), (17), (23), and (9), we finally deduce the theoretical analysis formula of SOP.

4. SPSC Analysis

For passive eavesdropping scenarios, SPSC is often used to investigate the confidentiality of WCNs; therefore, we explore the SPSC of IoT networks in this section. According to the definition of SPSC in [41], we know that it can understand the probability that the difference value of instantaneous capacity between main channel and eavesdropping channel is not less than zero, which can be formulated as

$$\begin{aligned}Spsc &= 1 - P\{C_D - C_E \le 0\} \\ &= 1 - \int_0^{\infty} F_D(\gamma_E) f_E(\gamma_E) \mathrm{d}\gamma_E = 1 - \Xi.\end{aligned} \tag{24}$$

For Ξ in (24), after replacing the integral term with (6) and (7), we can obtain

$$\begin{aligned}\Xi = &\int_0^{\infty} \frac{b_D^{-N_D m_D}}{\Gamma\left(N_D\mu_D\right)} \sum_{q=0}^{\infty} \frac{\left(N_D m_D\right)_q}{\left(N_D\mu_D\right)_q q!} \times \left(\frac{k_D\mu_D}{b_D m_D}\right)^q \left(N_D\mu_D + q - 1\right)! \times \left(1 - \sum_{s=0}^{N_D\mu_D + q - 1} \frac{e^{-N_D a_D \gamma} \left(N_D a_D \gamma\right)^s}{s!}\right) \\ &\times \frac{\left(N_E a_E\right)^{N_E\mu_E} b_E^{-N_E m_E}}{\Gamma\left(N_E\mu_E\right)} \sum_{p=0}^{\infty} \frac{\left(N_E m_E\right)_p}{M^{N_E\mu_E + p} \left(N_E\mu_E\right)_p p!} = \Lambda_1 \left(\Lambda_2 - \sum_{s=0}^{N_D\mu_D + q - 1} \frac{\left(N_D a_D\right)^s}{s!} \times \frac{\Gamma\left(N_E\mu_E + p + s\right)}{\left(\left(N_E a_E/M\right) + N_D a_D\right)^{\left(N_E\mu_E + p + s\right)}}\right).\end{aligned} \tag{25}$$

Finally, by employing (24), we can complete the proof of SPSC.

5. Numerical Results

In this part, we perform the theoretical simulations of (9) and (24). As a verification of correctness, Monte Carlo simulations are also obtained for comparison with the analysis results. From all simulation diagrams (Figures 2–9), we can capture the following information. (i) All the analysis curves coincide well with the statistical simulation curves. (ii) All simulation results change with abscissa, namely, Ω_D, and the change trend indicates that a large Ω_D can improve the security of IoT systems. Moreover, matlab simulations show that the convergence condition of the analytical expression including infinite series is that the upper limit of the cycle is 55 times.

Figures 2 and 3 indicate how the SOP and SPSC change with Ω_D when M takes different values. From Figure 2, we can see that when Ω_D is fixed, the value of SOP will rise along with the rise of M. In Figure 3, the increase of M will lead to the decrease of SPSC. Moreover, the distances between

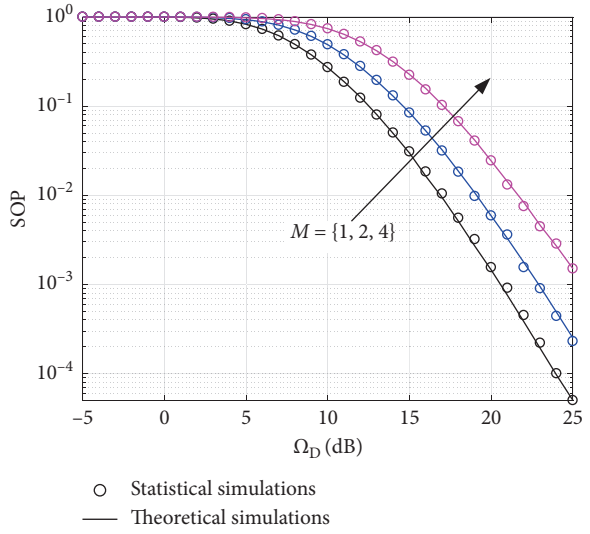

Figure 2: SOP versus Ω_D with various (M), where $k_S = k_D = k_E = 2$, $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $R_{th} = 0.1$, and $I_P = 0.1$.

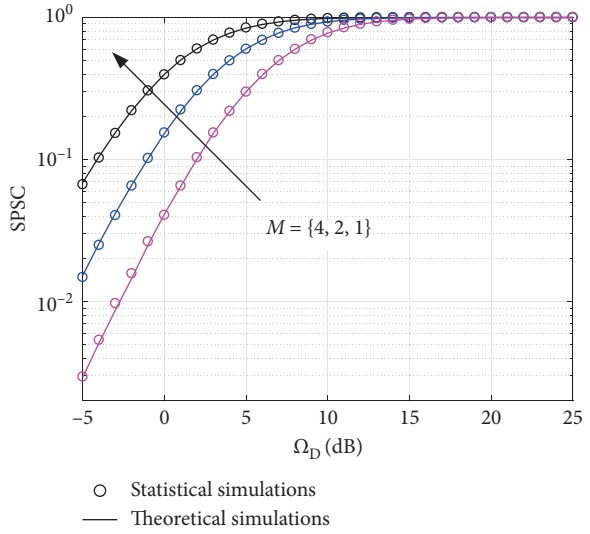

Figure 3: SPSC versus Ω_D with various (M), where $k_S = k_D = k_E = 2$, $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $R_{th} = 0.1$, and $I_P = 0.1$.

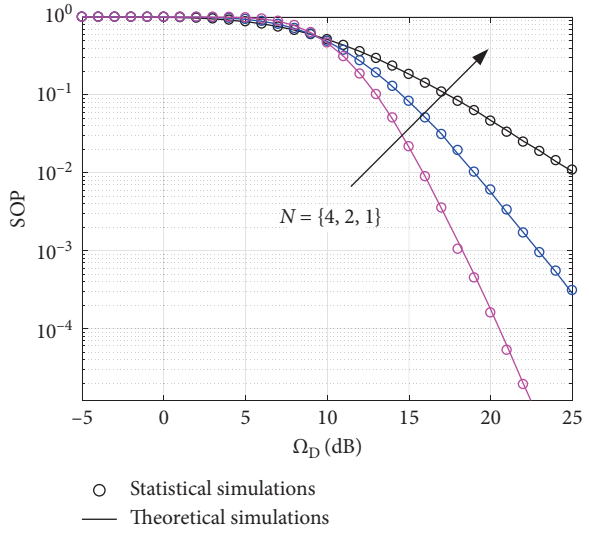

Figure 4: SOP versus Ω_D with various (N), where $k_S = k_D = k_E = 2$, $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $M = 2$, $R_{th} = 0.1$, and $I_P = 0.1$.

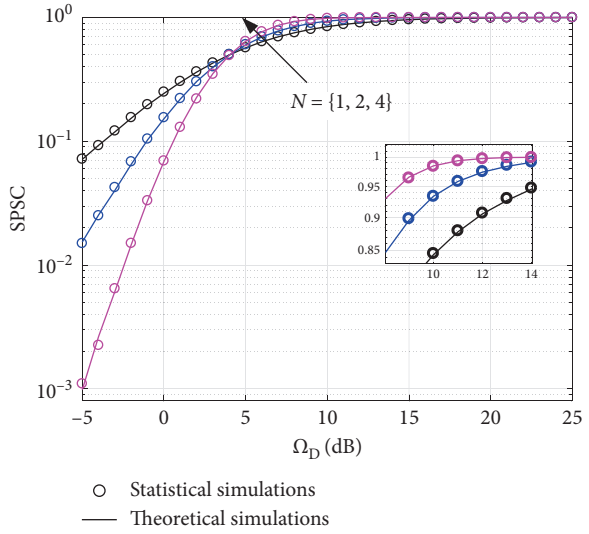

Figure 5: SPSC versus Ω_D with various (N), where $k_S = k_D = k_E = 2$, $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $M = 2$, $R_{th} = 0.1$, and $I_P = 0.1$.

curves represented by different M are larger. Therefore, we conclude that the increase of the number of eavesdroppers will significantly reduce the performance of IoT model.

The influence of the number of antennas on the safety performance is provided in Figures 4 and 5. We assume $N_D = N_E = N$. According to simulation curves, a valuable discovery is that when the value of abscissa is greater than 9 dB; the increase of antenna number, i.e., N, will decrease the SOP and increase the SPSC. This means that, under the mechanism of high SNR, the security can be improved by increasing the number of receiving antennas. On the contrary, in the case of small SNR, the increase of the number of antennas will reduce the ability of security.

When the shape parameters k and μ of the generalized channel change, the security analyses are shown in Figures 6 and 7. We suppose that $k_S = k_D = k_E = k$ and $\mu_S = \mu_D = \mu_E = \mu$, where the subscript S, D, and E indicate that the links are $S \longrightarrow P$, $S \longrightarrow D$, and $S \longrightarrow E$, respectively. Referring to Figures 6(a) and 7(a), we can see that the gradual increase of k causes the increase of SOP and the decrease of SPSC with $\Omega_D \geq 7$ dB. However, the effect of increasing μ on the IoT systems is opposite to that of k based on Figures 6(b) and 7(b).

I_P means the threshold of anti-interference ability to the primary networks. Figure 8 describes its effect on SOP for IoT networks under consideration.R_{in} represents the

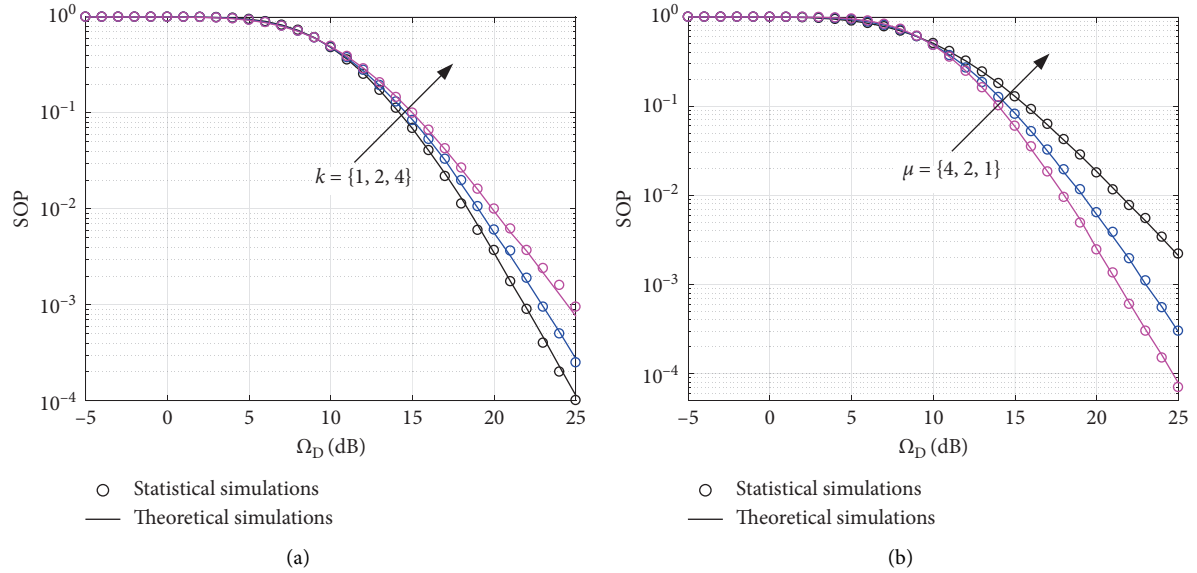

FIGURE 6: (a) SOP versus Ω_D with various k, where $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $M = 2$, $R_{th} = 0.1$, and $I_P = 0.1$. (b) SOP versus Ω_D with various μ, where $k_S = k_D = k_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $M = 2$, $R_{th} = 0.1$, and $I_P = 0.1$.

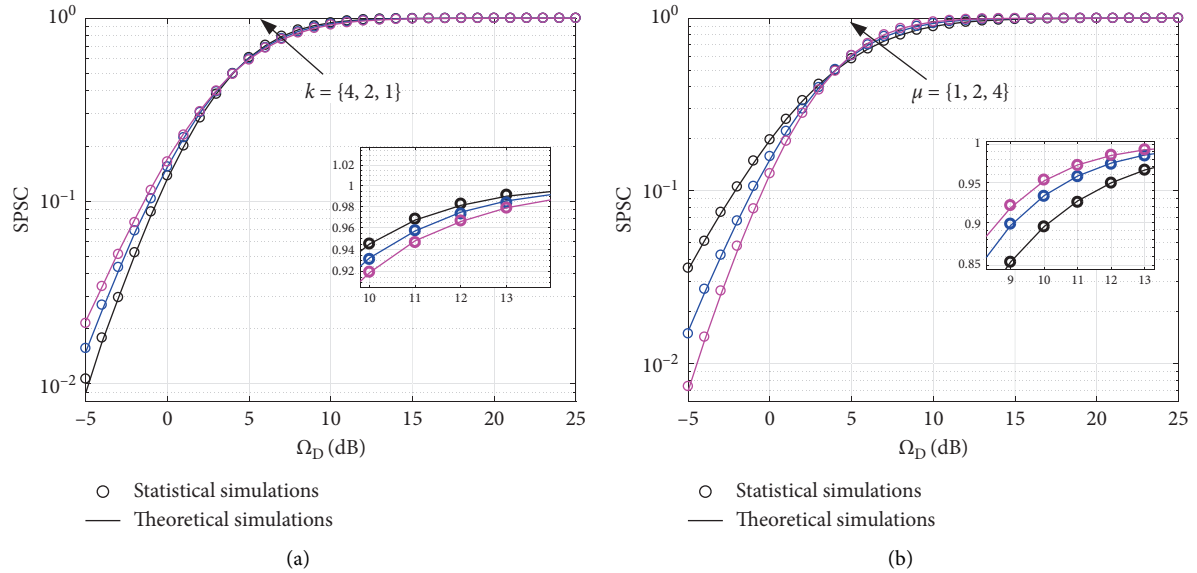

FIGURE 7: (a) SPSC versus Ω_D with various k where $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $M = 2$, $R_{th} = 0.1$, and $I_P = 0.1$. (b) SPSC versus Ω_D with various μ, where $k_S = k_D = k_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $M = 2$, $R_{th} = 0.1$, and $I_P = 0.1$.

threshold value of security capacity interruption, the impact of its change on system performance is illustrated in Figure 9. When I_P changes from 5 dB to −7 dB, then to 15 dB and R_{th} from 0.1 dB to 0.5 dB and then to 1 dB, the change trend of SOP is gradually decreasing. Therefore, we can find that smaller I_P and smaller R_{th} will increase the probability of system security interruption. Moreover, it is interesting that the impact of I_P on security is more significant than that of R_{th}.

m is also an important parameter of κ-μ shadowed distribution, which represents the degree of shadow fading. The simulation results show that when the high SNR is established, the increase of m will improve the SPSC and reduce the SOP, but the difference between the curves is very small. In other words, the impact of m on the security performance is not obvious.

Good security performance requires as small as possible SOP and as large as possible SPSC. Through the above analysis of all simulations, we can obtain that larger M, larger k, and smaller N will worsen the security of the system when the SNR is large. Meanwhile, we also know that larger μ, smaller I_P, and smaller R_{th} will enhance the security performance.

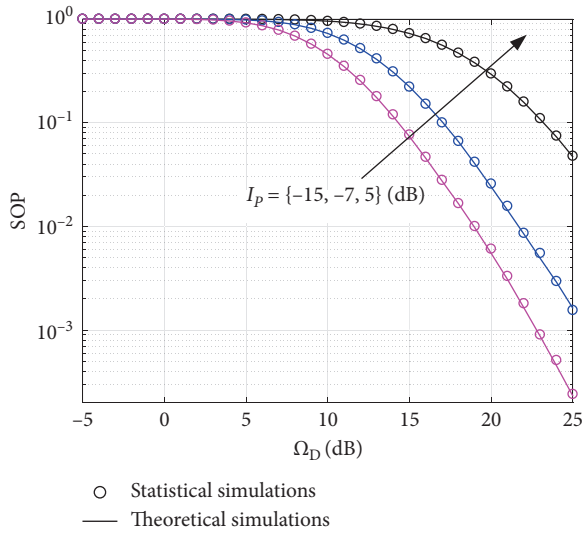

Figure 8: SOP versus Ω_D with various I_P, where $k_S = k_D = k_E = 2$, $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $M = 2$, and $R_{th} = 0.1$.

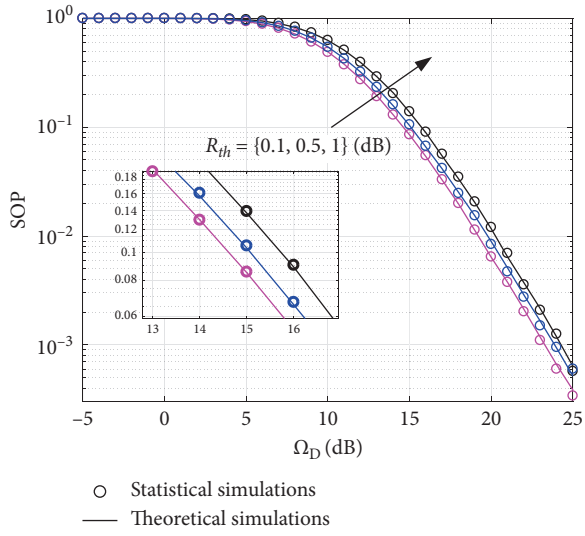

Figure 9: SOP versus Ω_D with various R_{th}, where $k_S = k_D = k_E = 2$, $\mu_S = \mu_D = \mu_E = 2$, $m_S = m_D = m_E = 1$, $N_D = N_E = 2$, $M = 2$, and $I_P = 0.1$.

6. Conclusion

In this paper, we explore PHY layer security of Underlay CRNs for IoT networks over generalized fading channels on the basis of the derived SOP and SPSC. The CRN model with multiple antennas can be used in many different situations. The analytical formulas for SOP and SPSC are derived in a concise form. The accuracy of the analytical formulas is verified by Monte Carlo simulations. Moreover, we discuss the influence of the parameters including M, N, k, μ, I_P, and R_{th} on the security of IoT networks.

Data Availability

The 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 are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 41174158 and Ministry of Land and Resources P.R.C. Special Project in the Public Interest under Grant 201311195-04.

References

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of things: communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[2] M. Seliem, K. Elgazzar, and K. Khalil, "Towards privacy preserving IoT environments: a survey," *Wireless Communications And Mobile Computing*, vol. 2018, Article ID 1032761, 15 pages, 2018.

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

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

[5] H. Wei, X. Hou, Y. Zhu, and D. Wang, "Security analysis for rayleigh fading channel by artificial noise," in *Proceedings of the 2014 Sixth International Conference On Wireless Communications And Signal Processing*, WCSP), Hefei, China, pp. 1–6, 2014.

[6] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding et al., "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Transactions on Vehicular Technology*, p. 1, 2020.

[7] 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*, Article ID 03902, 2006.

[8] Y. Ai, L. Kong, and M. Cheffena, "Secrecy outage analysis of double shadowed Rician channels," *Electronics Letters*, vol. 55, no. 13, pp. 765–767, 2019.

[9] X. Li, M. Huang, J. Li, Q. Yu, K. Rabie et al., "Secure analysis of multi-antenna cooperative networks with residual transceiver HIs and CEEs," *IET Communications*, vol. 13, no. 17, pp. 2649–2659, 2019.

[10] X. Li, J. Li, and L. Li, "Performance analysis of impaired SWIPT NOMA relaying networks over imperfect Weibull channels," *IEEE Systems Journal*, vol. 14, no. 1, pp. 669–672, 2020.

[11] H. Zhao, Y. Liu, A. Sultan-Salem, and M.-S. Alouini, "A simple evaluation for the secrecy outage probability over generalized-K fading channels," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1479–1483, 2019.

[12] A. Dziri, M. Terre, and N. Nasser, "Performance analysis of relay selection for iot networks over generalized k distribution," in *Proceedings of the 2019 15th International Wireless*

Communications And Mobile Computing Conference (IWCMC), pp. 1411–1415, Tangier, Morocco, 2019.

[13] N. Bhargav, 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.

[14] X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, "Residual transceiver hardware impairments on cooperative NOMA networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 680–695, 2020.

[15] 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.

[16] L. Kong and G. Kaddoum, "On physical layer security over the Fisher-snedecor ${\mathcal{F}}$ wiretap fading channels," *IEEE Access*, vol. 6, pp. 39466–39472, 2018.

[17] L. Xu, X. Yu, H. Wang et al., "Physical layer security performance of mobile vehicular networks," *Mobile Networks and Applications*, vol. 25, no. 2, pp. 643–649, 2020.

[18] L. Xu, J. Wang, H. Wang et al., "BP neural network-based ABEP performance prediction for mobile internet of things communication systems," *Neural Computing And Applications*, 2019.

[19] H. Wang, L. Xu, Z. Yan, and T. A. Gulliver, "Low complexity MIMO-FBMC sparse channel parameter estimation for industrial big data communications," *IEEE Transactions on Industrial Informatics*, vol. 2020, Article ID 2995598, 11 pages, 2020.

[20] P. Xie, M. Zhang, G. Zhang, R. Zheng et al., "On physical-layer security for primary system in underlay cognitive radio networks," *IET Networks*, vol. 7, no. 2, pp. 68–73, 2018.

[21] M. Qin, S. Yang, H. Deng, and M. H. Lee, "Enhancing security of primary user in underlay cognitive radio networks with secondary user selection," *IEEE Access*, vol. 6, pp. 32624–32636, 2018.

[22] 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 *Proceedings of the 2015 IEEE International Conference On Communication Software And Networks*, ICCSN), Chengdu, China, pp. 201–205, 2015.

[23] H. Lei, H. Zhang, I. S. Ansari, C. Gao et al., "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10126–10132, 2016.

[24] H. Lei, H. Zhang, I. S. Ansari, G. Pan, and K. A. Qaraqe, "Secrecy outage analysis for SIMO underlay cognitive radio networks over generalized-*K* fading channels," *IEEE Signal Processing Letters*, vol. 23, no. 8, pp. 1106–1110, 2016.

[25] Y. Zhang, R. Lu, B. Cao, and Q. Zhang, "Cooperative jamming-based physical-layer security of cooperative cognitive radio networks: system model and enabling techniques," *IET Communications*, vol. 13, no. 5, pp. 539–544, 2019.

[26] Z. Xiang, W. Yang, G. Pan, Y. Cai et al., "Physical layer security in cognitive radio inspired NOMA network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 700–714, 2019.

[27] J. F. Paris, "Statistical characterization of κ-μ shadowed fading," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 518–526, 2014.

[28] L. Moreno-Pozas, F. J. Lopez-Martinez, S. L. Cotton, J. F. Paris, and E. Martos-Naya, "Comments on human body shadowing in cellular device-to-device communications: channel modelling using the shadowed κ-μ fading model," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 517–520, 2017.

[29] M. K. Arti, "Beamforming and combining based scheme over κ-μ shadowed fading satellite channels," *IET Communications*, vol. 10, no. 15, pp. 2001–2009, 2016.

[30] E. Illi, F. El Bouanani, and F. Ayoub, "Asymptotic analysis of underwater communication system subject to κ-μ shadowed fading channel," in *Proceedings of the 2017 13th International Wireless Communications And Mobile Computing Conference*, IWCMC), Valencia, Spain, pp. 855–860, 2017.

[31] I. Singh and N. P. Singh, "Outage probability and ergodic channel capacity of underlay device-to-device communications over κ-μ shadowed fading channels," *Wireless Networks*, vol. 26, no. 1, pp. 573–582, 2020.

[32] N. Simmons, C. R. N. Da Silva, S. L. Cotton, P. C. Sofotasios et al., "On shadowing the κ-μ fading model," *IEEE Access*, vol. 2020, Article ID 3005527, 9 pages, 2020.

[33] S. Kumar and S. Kalyani, "Outage probability and rate for κ-μ shadowed fading in interference limited scenario," *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 8289–8304, 2017.

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

[35] J. Sun, H. Bie, X. Li, K. M. Rabie, and R. Kharel, "Average secrecy capacity of simo κ-μ shadowed fading channels with multiple eavesdroppers," in *Proceedings of the 2020 IEEE Wireless Communications And Networking Conference (WCNC)*, pp. 1–6, Seoul, Korea, 2020.

[36] J. Sun, H. Bie, and X. Li, "Security performance analysis of SIMO relay systems over Composite Fading Channels," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 6, pp. 2649–2669, 2020.

[37] Z. Chu, Z. Zhu, M. Johnston, and S. Y. Le Goff, "Simultaneous wireless information power transfer for MISO secrecy channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6913–6925, 2016.

[38] Z. Zhu, Z. Chu, F. Zhou, H. Niu, Z. Wang et al., "Secure beamforming designs for secrecy MIMO SWIPT systems," *IEEE Wireless Communications Letters*, vol. 7, no. 3, pp. 424–427, 2018.

[39] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press, Cambridge, MA, USA, 2007.

[40] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[41] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.