Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6785754, 9 pages
https://doi.org/10.1155/2022/6785754

Research Article

Physical Layer Security for CRNs over Beaulieu-Xie Fading Channels

Yanyang Zeng,[1] **Yang Hua**,[1] **Yiwei Fang**,[2] **and Xiaohong Wang**[3]

[1] *The College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454003, China*
[2] *The Wuhan Maritime Communication Research Institute, Wuhan 430079, China*
[3] *The College of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 454003, China*

Correspondence should be addressed to Yanyang Zeng; zengyy@hpu.edu.cn

Received 6 May 2022; Revised 6 July 2022; Accepted 27 July 2022; Published 8 August 2022

Academic Editor: Enrico M. Vitucci

In recent years, the access of massive communication devices leads to the insufficient spectrum resources of wireless networks. One of the practical means to resolve the problem is to build cognitive radio networks (CRNs), which can realize the sharing of spectrum resources between primary and secondary users, thereby improving the utilization rate of wireless spectrum resources. To this end, the CRNs are utilized to establish the Wyner's eavesdropping model over the Beaulieu-Xie fading channels. We mainly deduce the accurate expressions of secrecy outage probability and strictly positive secrecy capacity to explore the performance of physical layer security. Moreover, the better overlap between the statistical simulation and the theoretical results indicates the correctness of the theoretical analysis equation. The interesting results are that both increasing the $P_{\max}$ and decreasing the C_{th} can improve the security performance. This work is a good reference and guidance for modeling CRNs (Internet of Things, fifth generation, cell phone networks, etc.) and security performance evaluation.

1. Introduction

With the wide application of wireless transmission, the useful information will face the risk of disclosure in the process of transmission, so it is particularly important to find measures to avoid and reduce the eavesdropping of signals. Recently, the issue has become a research hotspot in academia. Different from traditional encryption and decryption methods, physical layer security (PLS) utilizes the characteristics of the transmission channels and noise to ensure the secure transmission of information. It was first proposed in [1] and applied to many practical communication scenarios, such as Beyond-5G low-latency communication networks [2], multihop amplify-and-forward (AF) relay systems [3], and cognitive radio networks (CRNs) [4]. Furthermore, the authors of [5] proposed a scheme combining deep learning with transmit antenna selection to enhance the PLS of cellular networks. In [6], the authors outlined some low complexity PLS schemes appropriate for the Internet of Things (IoTs). A cooperative beamforming scheme was designed in [7] to enhance the PLS in CRNs. For exploring the PLS properties of $\kappa-\mu$ shadowed fading, Sun et al. in [8] deduced closed-form expressions for the lower bounds of strictly positive secrecy capacity (SPSC) and secure outage probability (SOP).

Radio waves are utilized to transmit information in wireless communication networks (WCNs), but the actual communication environment is complex and variable so that there is a difference between the received and the transmitted signal, which lead to the distorted transmission of information. To better evaluate the transmission performance of WCNs, it is necessary to build and analyze system models of different fading channels [9–16]. Zhu et al. in [9] studied the performance of a full-duplex decode-and-forward (DF) system over the Rician distribution by analyzing the exact analytical expression of the outage probability (OP). The authors in [10] proposed the $\eta-\mu$ fading model and derived precise expressions of level crossing rate (LCR) and average fading duration (AFD). Badarneh et al. in [11] obtained precise expressions for the average bit error rate (ABER) and average channel capacity (ACC) of dual $\alpha - \mu$ distribution to explored the performance of selective combining receivers. In [12], the outage performance of relay-assisted vehicular communication under double-Rayleigh fading was investigated. The exact expressions of probability density function (PDF), LCR, and AFD of double Hoyt channel were derived in [13]. Ata in [14] analyzed the PLS of cascaded Rayleigh fading channels by solving the exact precise expressions of SOP. The authors of [15] studied the security performance of the DF relay system under the $\kappa - \mu$ shadowed fading by deducing the exact accurate expressions of SOP and SPSC. In [16], the security performance of single-input multiple-output (SIMO) system under composite distribution was studied by deriving the closed expression of ACC.

The access of a large number of wireless devices will lead to a sharp shortage of spectrum resources, and the emergence of CRNs can effectively solve the problem. The CRNs improve the utilization of wireless spectrum resources mainly by using spectrum sensing technology [17] [18]. The combination of CRNs and other technologies has been extensively studied by scholars [19–27]. Goldsmith et al. in [19] reviewed the basic capacity constraints of different wireless network design patterns based on cognitive radios. In [20], the performance of CRNs was discussed when there are multiple groups of cognitive radio relays. The authors of [21] proposed a new scheme for power allocation in CRNs with limited cross-layer interference. Zhang et al. in [22] investigated the effect of the relay selection scheme on the outage performance of CRNs by studying the exact expression of OP. Tashman and Hamouda in [23] analyzed the security performance of SIMO cognitive networks over $\kappa - \mu$ distribution by deriving the closed expression of SOP. In [24], the transmission performance of SIMO underlay CRNs over generalized K channels was studied. The authors in [25] explored the PLS of CRNs under cascaded Rayleigh channels. By analyzing the accurate expression of SOP, the authors of [26] studied the security performance when there are multiple master control units and eavesdroppers in the network. The optimal PLS scheme for users in underlay multiple-input multiple-output (MIMO) CRN was studied in [27].

Exact modeling based on wireless fading channels is important for simulating specific practical scenarios and analyzing their security performance. Different fading channels have their respective characteristics, so the channels can simulate different scenarios. For instance, the Nakagami-m distribution can vary m to control the number of clusters [28]. And the Rician distribution can simulate scenarios when line-of-sight (LOS) or deterministic components are present in the received signal [29]. Combining the advantages of the above two distributions, Beaulieu and Xie proposed a new Beaulieu-Xie (BX) fading channels [30], which can represent both specular and diffuse scattering components, that is, it can simulate both LOS and non-LOS (NLOS) scenarios [31]. Therefore, the BX fading is very suitable for modeling and researching femtocells [32] and high-speed trains [33]. The accurate formulas of the LCR and AFD for BX distribution were deduced in [34]. In [35], the closed expressions for the asymptotic upper and lower bounds of the OP and the error probability of the BX fading were deduced. The theoretical expression of the OP for two BX random variables was investigated in [36]. The authors of [37] explored precise and progressive expressions for the effective rate of MIMO networks over BX distribution. Singh and Joshi in [38] derived exact expressions for the ABER of SIMO and MIMO orthogonal frequency division multiplexing systems under BX fading.

As far as the author's knowledge, there are no relevant literatures to study the security analysis based on CRNs under BX fading channels in the published database. Therefore, this work focuses on deriving the exact closed expressions of SOP and SPSC based on CRNs over the BX fading channels. On this basis, the PLS of CRN is analyzed emphatically. Moreover, the influences of the channel parameters and the maximum interference power on the security of the considering model are both studied. Finally, the correctness of the derivations in this paper is verified by simulation analysis.

The organization of this paper is as follows: In this section, we mainly introduced the research background, current situation and contributions. In Section 2, the system model based on the underlay CRN and the accurate expression of the PDF and cumulative distribution function (CDF) of the signal-to-noise ratio (SNR) of the BX distribution were described. Section 6 obtained the precise expression of SOP. The exact expression of SPSC was derived in Section 4. Section 5 analyzed the numerical simulation results. Section 6 summarized the paper.

2. System Model and Channel Characteristics

2.1. System Model. As shown in Figure 1. The underlay CRN model includes the primary network and the secondary network, which can share frequency band resources, but the premise is that the normal communication of the primary network is not disturbed. We assume that the primary network has one transmission source (P) and N users. The secondary network consists of a signal transmitting source (S), a target receiver (D), and an eavesdropper (E), and all nodes are equipped with an antenna. The channel coefficients of $S \longrightarrow P$, $S \longrightarrow D$, and $S \longrightarrow E$ are represented as h_{SP}, h_D, and h_E, respectively. S can transmit information to P, D, and E, and the transmitted signal at S is x; then the information received at P, D, and E can be written as

$$y_{SP} = \sqrt{P_S} h_{sp} x + n_{SP}, \tag{1}$$

$$y_{SD} = \sqrt{P_S} h_D x + n_D, \tag{2}$$

$$y_{SE} = \sqrt{P_S} h_E x + n_E, \tag{3}$$

where P_S represents the transmit power of S. y_{SP}, y_{SD}, and y_{SE} are the signals received at P, D, and E, respectively. $n_i \sim CN\left(0, \sigma^2\right)$ $(i = S, P, D, E)$ are represented as additive white Gaussian noise.

2.2. Statistical Properties of the BX Distribution. In this section, the expressions of the PDF and CDF for the BX distribution are given, and to make the calculation easier and

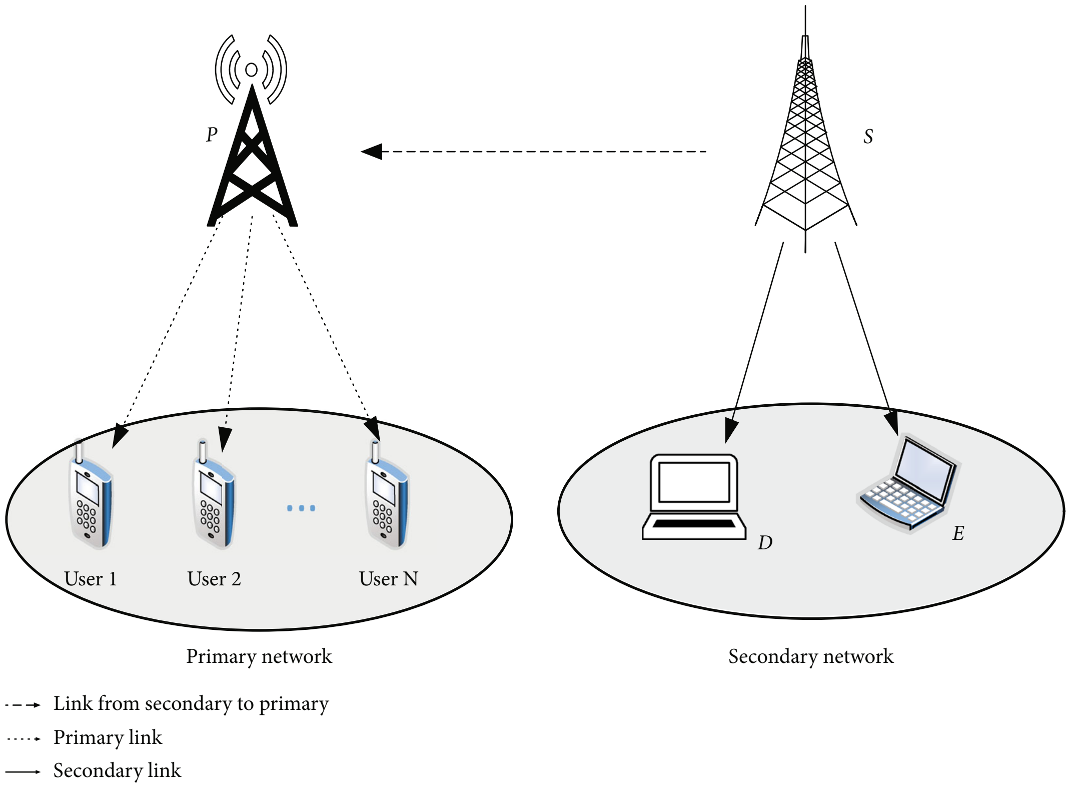

Figure 1: The system model.

more convenient, we have performed some mathematical operations on them. In [38] (eq. (3)), the PDF of the SNR for the BX channels is written as

$$f(\gamma) = \left(\frac{\sqrt{2}}{\lambda}\right)^{m-1} \left(\sqrt{\frac{m}{\Omega}}\right)^{m+1} \gamma^{m/2-1/2} e^{-\lambda^2/2} e^{-m\gamma/\Omega} I_{m-1} \cdot \left(\sqrt{\frac{2m\gamma}{\Omega}}\lambda\right), \tag{4}$$

where m and λ reflect the shape and extension, respectively, and Ω is the average SNR. $I_x(\cdot)$ is the Bessel function [39] (eq. (8.401)).

According to the formula in [39] (eq. (8.445)) of

$$I_\alpha(z) = \sum_{j=0}^{\infty} \frac{1}{j!\Gamma(\alpha+j+1)} \left(\frac{z}{2}\right)^{\alpha+2j}, \tag{5}$$

(4) can be rewritten as

$$\begin{aligned} f(\gamma) &= \left(\frac{\sqrt{2}}{\lambda}\right)^{m-1} \left(\sqrt{\frac{m}{\Omega}}\right)^{m+1} \gamma^{m/2-1/2} e^{-\lambda^2/2} e^{-m\gamma/\Omega} \\ &\quad \cdot \sum_{k=0}^{\infty} \frac{1}{k!\Gamma(m+k)} \left(\frac{((2/m)/\Omega)^{1/2}\gamma^{1/2}\lambda}{2}\right)^{m+2k-1} \\ &= \left(\frac{\sqrt{2}}{\lambda}\right)^{m-1} \left(\sqrt{\frac{m}{\Omega}}\right)^{m+1} e^{-\left(\lambda^2/2\right)} \sum_{k=0}^{\infty} \frac{1}{k!\Gamma(m+k)} \\ &\quad \cdot \left(\frac{((2/m)/\Omega)^{1/2}\lambda}{2}\right)^{m+2k-1} \gamma^{m+k-1} e^{-m\gamma/\Omega} \\ &= e^{-\left(\lambda^2/2\right)} \sum_{k=0}^{\infty} \frac{2^{-k} m^{m+k} \Omega^{-(m+k)} \lambda^{2k}}{k!\Gamma(m+k)} \gamma^{m+k-1} e^{-(m/\Omega)\gamma}. \end{aligned} \tag{6}$$

Utilizing [39] (eq. (3.351.3)), the CDF of SNR is expressed as

$$\begin{aligned} F(\gamma) &= \int_0^{\gamma} f(x)dx = e^{-\left(\lambda^2/2\right)} \sum_{l=0}^{\infty} \frac{\left(\lambda/\sqrt{2}\right)^{2l}}{l!\Gamma(l+m)} (l+m-1)! \\ &\quad \cdot \left(1 - e^{-(m\gamma/\Omega)} \sum_{l_1=0}^{l+m-1} \frac{(m/\Omega)^{l_1} \gamma^{l_1}}{l_1!}\right). \end{aligned} \tag{7}$$

3. SOP Analysis

We utilize SOP as a performance evaluation metric to explore the security. SOP is defined as the probability that the value of secrecy capacity is less than the specified threshold value [40], which can be expressed as

$$SOP = \Pr\{C_S \le C_{th}\}, \tag{8}$$

where $C_S = C_D - C_E$, C_D, and C_E denote the instantaneous channel capacity of link ($S \longrightarrow D$) and the link ($S \longrightarrow E$), respectively, and C_{th} represents the specified threshold. The primary and the secondary network in the underlay CRNs must satisfy the following conditions [41]: (i) The maximum transmission power ($P_{\max}$) cannot be less than the transmission power of S. (ii) The maximum interference power (Ip) allowed by the main network cannot be less than the power from S to P. Therefore, the SOP in underlay CRNs is written as

$$\begin{aligned} SOP = \Pr\{Cs \le C_{th}\} &= \Pr\left\{C_s \le C_{th}, X \le \frac{I_p}{P_{\max}}\right\} \\ &+ \Pr\left\{C_s \le C_{th}, X \ge \frac{I_p}{P_{\max}}\right\} = \Phi_1 + \Phi_2, \end{aligned} \tag{9}$$

where X represents the instantaneous SNR of $S \longrightarrow P$. In the next subsection, we will evaluate the closed-form expressions of Φ_1 and Φ_2 in (9).

3.1. Representation of Φ_1. According to the above analysis, Φ_1 can be converted to

$$\begin{aligned} \Phi_1 &= \Pr\left\{Cs \le C_{th}, X \le \frac{Ip}{P_{\max}}\right\} \\ &= P\left\{\gamma_D \le \theta\gamma_E + \frac{\theta - 1}{\upsilon}\right\} P\left\{X \le \frac{Ip}{P_{\max}}\right\} = I_1 I_2, \end{aligned} \tag{10}$$

where $I_1 = P\{\gamma_D \le \theta\gamma_E + (\theta - 1/\upsilon)\}$, $I_2 = P\{X \le Ip/P_{\max}\}$, $\theta = e^{Cth}$, and $\upsilon = P_{\max}/\sigma^2$.

Using (6) and (7), I_1 can be obtained as

$$\begin{aligned} I_1 &= \int_0^\infty F_D\left(\theta\gamma_E + \frac{\theta - 1}{\upsilon}\right) f_E(\gamma_E)\, d\gamma_E \\ &= \int_0^\infty e^{-\left(\lambda_D{}^2/2\right)} \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{l!\Gamma(l + m_D)} (l + m_D - 1)! \\ &\cdot \left(1 - e^{-m_D(\theta\gamma_E + ((\theta-1)/\upsilon))/\Omega_D} \sum_{l_1=0}^{l+m_D-1} \right. \\ &\left. \cdot \frac{(m_D/\Omega_D)^{l_1} (\theta\gamma_E + ((\theta - 1)/\upsilon))^{l_1}}{l_1!} \right) \\ &\times e^{-\left(\lambda_E{}^2/2\right)} \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E + k)} \\ &\cdot \gamma_E{}^{m_E+k-1} e^{-(m_E/\Omega_E)\gamma_E} d\gamma_E. \end{aligned} \tag{11}$$

Utilizing an equation in [39] (eq. (1.111)), the exact analytical solution for I_1 can be represented as

$$\begin{aligned} I_1 &= e^{-\left(\lambda_E{}^2/2\right)} e^{-\left(\lambda_D{}^2/2\right)} \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E + k)} \\ &\cdot \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{l!\Gamma(l + m_D)} (l + m_D - 1)! \\ &\times \left(\int_0^\infty \gamma_E{}^{m_E+k-1} e^{-(m_E/\Omega_E)\gamma_E} d\gamma_E - e^{-((m_D((\theta-1)/\upsilon))/\Omega_D)} \right. \\ &\cdot \sum_{l_1=0}^{l+m_D-1} \frac{(m_D/\Omega_D)^{l_1}}{l_1!} \times \sum_{t_1=0}^{l_1} \binom{l_1}{t_1} \theta^{t_1} \left(\frac{\theta - 1}{\upsilon}\right)^{l_1 - t_1} \\ &\left. \cdot \int_0^\infty e^{-((m_D\theta/\Omega_D) + (m_E/\Omega_E))\gamma_E} \gamma_E{}^{m_E+k+t_1-1} d\gamma_E \right) \\ &= e^{-\left(\lambda_E{}^2/2\right)} e^{-\left(\lambda_D{}^2/2\right)} \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E + k)} \\ &\cdot \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{l!\Gamma(l + m_D)} (l + m_D - 1)! \\ &\times \left(\frac{\Gamma(m_E + k)}{(m_E/\Omega_E)^{m_E+k}} - e^{-((m_D((\theta-1)/\upsilon))/\Omega_D)} \right. \\ &\cdot \sum_{l_1=0}^{l+m_D-1} \frac{(m_D/\Omega_D)^{l_1} \sum_{t_1=0}^{l_1} \binom{l_1}{t_1} \theta^{t_1} ((\theta - 1)/\upsilon)^{l_1 - t_1}}{l_1!} \\ &\left. \cdot \frac{\Gamma(m_E + k + t_1)}{((m_D\theta/\Omega_D) + (m_E/\Omega_E))^{m_E+k+t_1}} \right). \end{aligned} \tag{12}$$

Using the similar method as solving I_1, I_2 is obtained as

$$\begin{aligned} I_2 &= \Pr\left\{X \le \frac{Ip}{P_{\max}}\right\} = F_p\left(\frac{Ip}{P_{\max}}\right) \\ &= e^{-\lambda_p{}^2/2} \sum_{l=0}^{\infty} \frac{\left(\lambda_p/\sqrt{2}\right)^{2l}}{l!\Gamma(l + m_p)} (l + m_p - 1)! \\ &\cdot \left(1 - e^{-m_p(Ip/P_{\max})/\Omega_p} \sum_{l_1=0}^{l+m_p-1} \frac{(m_p/\Omega_p)^{l_1} (Ip/P_{\max})^{l_1}}{l_1!}\right). \end{aligned} \tag{13}$$

3.2. Representation of Φ_2. According to (9) and [42] (eq. (13)), the expressions for Φ_2 can be rewritten as

$$\Phi_2 = \Pr\left\{C_s \le C_{th}, X \ge \frac{I_p}{P_{\max}}\right\} = \int_{Ip/P_{\max}}^{\infty} G(x) f_s(x)\, dx, \tag{14}$$

where $G(x) = \int_0^\infty F_D(\theta y + ((\theta - 1)x/\varphi)) f_E(y)\, dy$, $\varphi = Ip/\sigma^2$.

Using (6) and (7) and an equation in [39] (eq. (3.381.4)), the exact $G(x)$ is expressed as

$$
\begin{aligned}
G(x) &= \int_0^\infty F_D\left(\theta y + \frac{(\theta-1)x}{\varphi}\right) f_E(y)dy \\
&= \int_0^\infty e^{-\lambda_D{}^2/2} \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{l!\Gamma(l+m_D)} (l+m_D-1)! \\
&\quad \times \left(1 - e^{-(m_D(((\theta-1)x)/\varphi))/\Omega_D} \sum_{l_1=0}^{l+m_D-1} \right. \\
&\quad \left. \cdot \frac{(m_D/\Omega_D)^{l_1} \sum_{t_1=0}^{l_1} \binom{l_1}{t_1} \theta^{t_1} ((\theta-1)/\varphi)^{l_1-t_1} x^{l_1-t_1}}{l_1!} y^{t_1} e^{-(\theta m_D y/\Omega_D)} \right) \\
&\quad \times e^{-\left(\lambda_E{}^2/2\right)} \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E+k)} y^{m_E+k-1} e^{-(m_E/\Omega_E)y} dy \\
&= e^{-\left(\lambda_D{}^2/2\right)} \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{l!\Gamma(l+m_D)} (l+m_D-1)! e^{-\left(\lambda_E{}^2/2\right)} \\
&\quad \cdot \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E+k)} \\
&\quad \times \int_0^\infty \left(y^{m_E+k-1} e^{-m_E/\Omega_E y} - e^{-m_D((\theta-1)x/\varphi)/\Omega_D} \sum_{l_1=0}^{l+m_D-1} \frac{(m_D/\Omega_D)^{l_1}}{l_1!} \right. \\
&\quad \left. \cdot \times \sum_{t_1=0}^{l_1} \binom{l_1}{t_1} \theta^{t_1} \left(\frac{(\theta-1)}{\varphi}\right)^{l_1-t_1} x^{l_1-t_1} y^{m_E+k+t_1-1} e^{-(m_E/\Omega_E+\theta m_D/\Omega_D)y} \right) dy \\
&= B_1 B_2 \left(B_3 - B_4 x^{l_1-t_1} e^{-m_D(((\theta-1)x)/\varphi)/\Omega_D} \right),
\end{aligned}
\tag{15}
$$

where

$$
B_1 = e^{-\left(\lambda_D{}^2/2\right)} \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{l!\Gamma(l+m_D)} (l+m_D-1)!, \tag{16}
$$

$$
B_2 = e^{-\lambda_E{}^2/2} \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E+k)}, \tag{17}
$$

$$
B_3 = \frac{\Gamma(m_E+k)}{(m_E/\Omega_E)^{(m_E+k)}}, \tag{18}
$$

$$
\begin{aligned}
B_4 = &\sum_{l_1=0}^{l+m_D-1} \frac{(m_D/\Omega_D)^{l_1} \sum_{t_1=0}^{l_1} \binom{l_1}{t_1} \theta^{t_1} ((\theta-1)/\varphi)^{l_1-t_1}}{l_1!} \\
&\cdot \frac{\Gamma(m_E+k+t_1)}{((m_E/\Omega_E) + (\theta m_D/\Omega_D))^{(m_E+k+t_1)}}.
\end{aligned}
\tag{19}
$$

Substituting (15) into (14) and using [39] (eq. (3.351.2)), Φ_2 can be represented as

$$
\begin{aligned}
\Phi_2 &= \int_{Ip/P_{\max}}^{\infty} G(x) f_s(x) dx = \int_{Ip/P_{\max}}^{\infty} B_1 B_2 \left(B_3 B_5 x^{m_E+k-1} e^{-m_E/\Omega_E x} \right. \\
&\quad \left. - B_4 B_5 x^{l_1-t_1+m_E+k-1} e^{-\left(\frac{m_D((\theta-1)/\varphi)}{\Omega_D} + \frac{m_E}{\Omega_E}\right)x} \right) dx \\
&= B_1 B_2 \left(B_3 B_5 \left(\frac{m_E}{\Omega_E}\right)^{-(m_E+k)} \Gamma\left(m_E+k, \frac{Ip}{P_{\max}} \frac{m_E}{\Omega_E}\right) \right. \\
&\quad - B_4 B_5 \left(\frac{m_D((\theta-1)/\varphi)}{\Omega_D} + \frac{m_E}{\Omega_E} \right)^{-(l_1-t_1+m_E+k)} \Gamma \\
&\quad \left. \cdot \left(l_1 - t_1 + m_E + k, \left(\frac{m_D((\theta-1)/\varphi)}{\Omega_D} + \frac{m_E}{\Omega_E} \right) \frac{Ip}{P_{\max}} \right) \right),
\end{aligned}
\tag{20}
$$

where

$$
B_5 = e^{-\lambda_E{}^2/2} \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E+k)}. \tag{21}
$$

4. SPSC Analysis

For the communication network security, SPSC is also one of the important evaluation indicators. SPSC is described as the probability that the secrecy capacity is greater than zero, which can be expressed as [40]

$$
SPSC = P\{C_D - C_E > 0\} = 1 - \int_0^\infty F_D(\gamma_E) f_E(\gamma_E) d\gamma_E = 1 - \Psi. \tag{22}
$$

Substituting (6) and (7) into Equation (22), we can get the expression of Ψ as

$$
\begin{aligned}
\Psi &= \mathrm{P}\{\gamma_D \le \gamma_E\} = \int_0^\infty F_D(\gamma_E) f_E(\gamma_E) d\gamma_E \\
&= \int_0^\infty e^{-\lambda_D{}^2/2} \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{\Gamma(l+1)\Gamma(l+m_D)} (l+m_D-1)! \\
&\quad \cdot \left(1 - e^{-m_D \gamma_E/\Omega_D} \sum_{l_1=0}^{l+m_D-1} \frac{(m_D/\Omega_D)^{l_1} \gamma_E{}^{l_1}}{l_1!} \right) \times e^{-\lambda_E{}^2/2} \\
&\quad \cdot \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E+k)} \gamma_E{}^{m_E+k-1} e^{-m_E/\Omega_E \gamma_E} d\gamma_E \\
&= e^{-\lambda_E{}^2/2} \sum_{k=0}^{\infty} \frac{2^{-k} m_E{}^{m_E+k} \Omega_E{}^{-(m_E+k)} \lambda_E{}^{2k}}{k!\Gamma(m_E+k)} e^{-\lambda_D{}^2/2} \\
&\quad \cdot \sum_{l=0}^{\infty} \frac{\left(\lambda_D/\sqrt{2}\right)^{2l}}{\Gamma(l+1)\Gamma(l+m_D)} (l+m_D-1)! \times \left(\frac{\Gamma(m_E+k)}{(m_E/\Omega_E)^{m_E+k}} \right. \\
&\quad \left. - \sum_{l_1=0}^{l+m_D-1} \frac{(m_D/\Omega_D)^{l_1}}{l_1!} \frac{\Gamma(m_E+k+l_1)}{((m_E/\Omega_E) + (m_D/\Omega_D))^{m_E+k+l_1}} \right).
\end{aligned}
\tag{23}
$$

Combined with (22) and (23), the exact accurate analytical formula of SPSC can be obtained. In (23), with the increase of λ, λ^{2k} and $(\lambda/\sqrt{2})^{2l}$ will increase and lead to

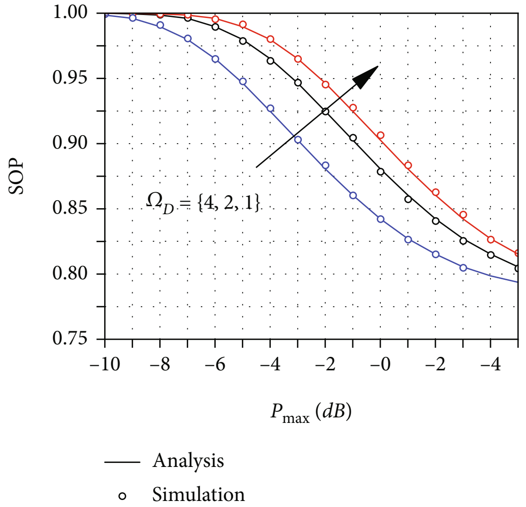

Figure 2: SOP versus $P_{\max}$ for different Ω_D.

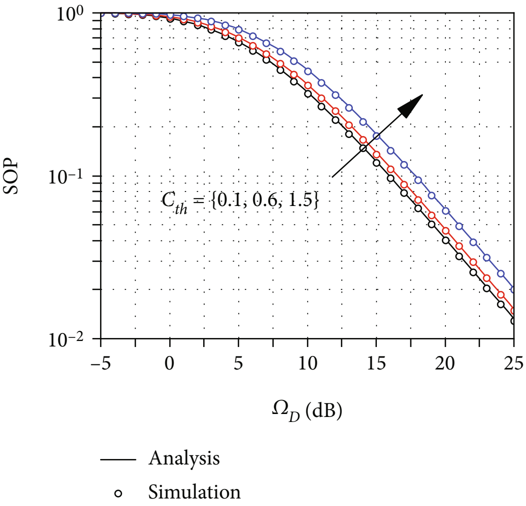

Figure 3: SOP versus Ω_D for different C_{th}.

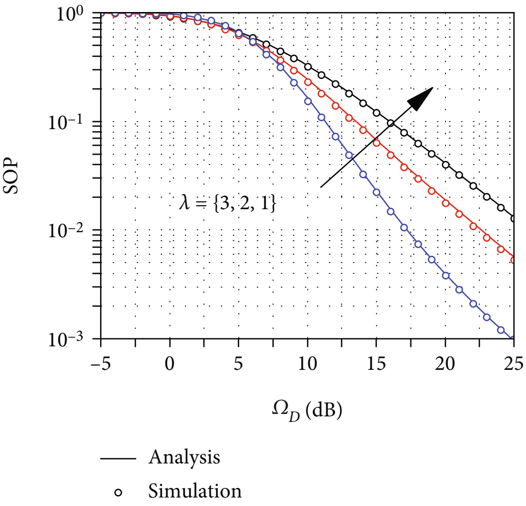

Figure 4: SOP versus Ω_D for different λ.

the improvement of SPSC; however, $e^{-\lambda^2/2}$ will increase and lead to the decline of SPSC.

5. Numerical Analysis

In this section, the simulation results of the inferences are given, and their correctness will be verified by statistical simulations. Furthermore, we analyze the performance through the simulation curves. We implement the random number generator of BX distribution by using the acceptance rejection method. It is worth noting that the SOP and SPSC contain infinite series; however, when the number of loops reaches more than 40 times, the derived formulas for SOP and SPSC will converge to a fixed value.

Figure 2 presents the variation of SOP under the conditions of different $\Omega\{\Omega_D = \Omega_E = (4, 2, 1)\}$. In all simulations, we set $\lambda_D = \lambda_E = 1$, $m_D = m_E = 1$, $Ip = 10$ dB, and $C_{th} = 0.1$ dB . The theoretical curves overlap well with the Monte Carlo simulations. Ω_D is the average SNR of the main channel, the larger Ω_D means that the better transmission quality of the signal. In this situation, the SOP should be smaller. In addition, the value of SOP decreases as $P_{\max}$ rises, which shows that increasing the value of $P_{\max}$ can enhance the confidentiality. And by increasing the Ω_D, the SOP decreases and the security is improved.

Figure 3 illustrates the change of SOP with the average SNR under different C_{th}. The parameter settings are as follows: $\lambda_D = \lambda_E = 1$, $m_D = m_E = 1$, $Ip = 10$ dB, $P_{\max} = 1$ dB, and $\Omega_E = 1$ dB. Figure 3 shows that as Ω_D rises, SOP gradually decreases, indicating that increasing the average SNR of the main channel when the SNR of the eavesdropping channel is constant can enhance security. And with the rise of the set threshold C_{th}, the security will be weakened.

Figure 4 describes the variation of SOP with the average SNR and $\lambda_D = \lambda_E = \{3, 2, 1\}$. Its parameters are set to $m_D = m_E = 1$, $Ip = 5$ dB, $P_{\max} = 1$ dB, $\Omega_E = 1$ dB, and $C_{th} = 0.1$ dB. This figure depicts the effect of the parameter λ of the BX fading on the security, Figure 4 is based on the Equations (9), (10), (12), (13), and (20). We can see that the value of λ has a large transformation on the system performance at $\Omega_D > 5$ dB. In other words, the rise of λ will greatly enhance the security under the condition of high SNR.

Figure 5 plots the change of SPSC with Ω_D and λ. The parameters are $m_D = m_E = 2$, $C_{th} = 0.1$ dB, $Ip = 0.1$ dB, $P_{\max} = 1$ dB, and $\Omega_E = 2$ dB. It can be seen that the change of λ has different effects on security under high and low SNR. When $\Omega_D < 2$ dB, the value of SPSC reduces as λ increases. That is, at low SNR, the increase of λ weakens the security. Analysis of Figures 4 and 5 shows that under high SNR, with the rise of λ, the value of SOP decreases rapidly, and the value of SPSC gradually increases. These conclusions collectively demonstrate that the increase of λ will enhance confidentiality.

Figure 6 depicts the variation of SOP with m and Ω_D. The remaining parameters are set as follows: $\lambda_D = \lambda_E = 1$, $\Omega_E = 1$ dB, $Ip = 5$ dB, $P_{\max} = 1$ dB, and $C_{th} = 0.1$ dB. From Figure 6, the value of SOP reduces rapidly as the m rises for $\Omega_D > 6$ dB, which indicates that increasing m can greatly

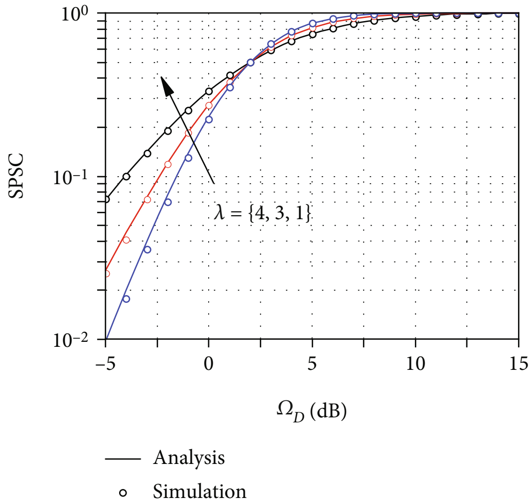

FIGURE 5: SPSC versus Ω_D for different λ.

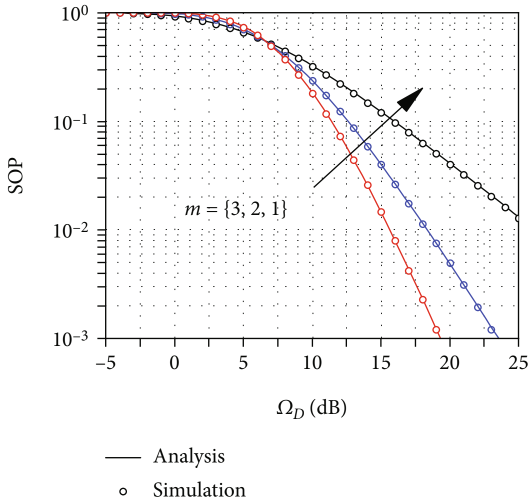

FIGURE 6: SOP versus Ω_D for different m.

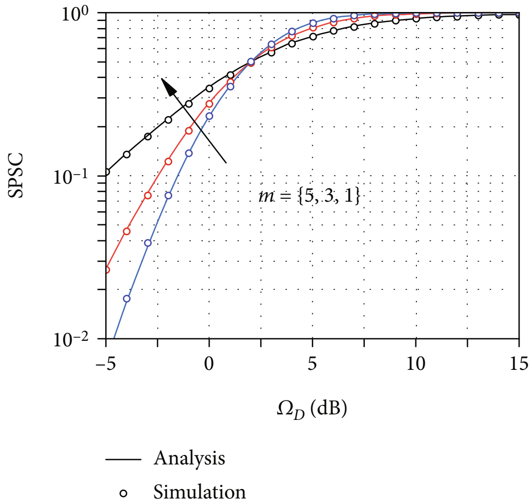

FIGURE 7: SPSC versus Ω_D for different m.

enhance the security, and when $\Omega_D < 6$ dB, the change of m has little effect on the confidentiality.

Figure 7 shows the variation of SPSC under different m with the average SNR. In Figure 7 we set $\lambda_D = \lambda_E = 2$, $C_{th} = 0.1$ dB, $\Omega_E = 2$ dB, $Ip = 0.1$ dB, and $P_{\max} = 1$ dB. The simulation curves are drawn based on (22) and (23). Furthermore, it can be observed that at low SNR, as m increases, the value of SPSC reduces, which proved that the confidentiality is weakened. When $\Omega_E > 3$ dB, as m adds, the security of the system is improved. This is consistent with the results obtained in Figure 6.

6. Conclusion

In this paper, we investigate the PLS of the CRNs over BX fading channels. The accurate expressions of SOP and SPSC are obtained. Then the impact of the parameters for the BX fading channels which inherits the advantages of both Nakagami-m and Rician fading channels on the security of the CRN is analyzed. Finally, we compared the theoretical derivation with Monte Carlo simulation; the coincidence of simulation curves proves the correctness of the theoretical formulas. And interestingly, rising $P_{\max}$, increasing Ω_D, decreasing C_{th}, and increasing the values of λ and m under high SNR all promote the confidentiality.

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 is no conflict of interest about the publication of this paper.

Acknowledgments

This work was supported in part by the Key Scientific Research Projects of Higher Education Institutions in Henan Province under grant 20A510007 and in part by the Doctoral Fund of Henan Polytechnic University under grant B2022-13.

References

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

[2] A. K. Yerrapragada, T. Eisman, and B. Kelley, "Physical layer security for beyond 5G: ultra secure low latency communications," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2232–2242, 2021.

[3] L. Qing, H. Guangyao, and F. Xiaomei, "Physical layer security in multi-hop AF relay network based on compressed sensing," *IEEE Communications Letters*, vol. 22, no. 9, pp. 1882–1885, 2018.

[4] Z. Lianbing, "Research on physical layer security of cognitive radio based on cooperative communication," in *Sixth International Conference on Intelligent Systems Design and*

Engineering Applications (ISDEA), vol. 2015, pp. 661–664, IEEE, Guiyang, China, 2015.

[5] L. Li, Y. Hu, H. Zhang, W. Liang, and A. Gao, "Deep learning based physical layer security of D2D underlay cellular network," *China Communications*, vol. 17, no. 2, pp. 93–106, 2020.

[6] A. Mukherjee, "Physical-Layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[7] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1835–1841, 2016.

[8] J. Sun, X. Li, M. Huang, D. Yuan, and J. Jin, "Performance analysis of physical layer security over shadowed fading channels," *IET Communications*, vol. 12, no. 8, pp. 970–975, 2018.

[9] Y. Zhu, Y. Xin, and P. Kam, "Outage probability of Rician fading relay channels," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2648–2652, 2008.

[10] M. Yacoub, "The η-μ distribution: a general fading distribution," in *In Vehicular Technology Conference Fall 2000. IEEE VTS Fall VTC2000*, vol. 2, pp. 872–877, 52nd Vehicular Technology Conference, Boston, MA, USA, 2000.

[11] O. S. Badarneh, D. B. da Costa, M. Benjillali, and M. Alouini, "Selection combining over double α-μ fading channels," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 3444–3448, 2020.

[12] Z. Li, L. Jia, F. Li, and H. Hu, "Outage performance analysis in relay-assisted inter-vehicular communications over double-Rayleigh fading channels," in *International Conference on Communications and Mobile Computing,*, vol. 2010, pp. 266–270, IEEE, Shenzhen, China, 2010.

[13] N. Hajri, N. Youssef, and M. Patzold, "A study on the statistical properties of double Hoyt fading channels," in *In 2009 6th International Symposium on Wireless Communication Systems*, pp. 201–205, IEEE, Siena, Italy, 2009.

[14] S. Ö. Ata, "Physical layer security over cascaded Rayleigh fading channels," in *In 2018 26th Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4, IEEE, Izmir, Turkey, 2018.

[15] 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. 1–6, 2020.

[16] 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 *IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 2020, pp. 1–6, IEEE, Seoul, Korea (South), 2020.

[17] L. Singh and N. Dutta, "Various optimization algorithm used in CRN," in *In 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, pp. 95–100, IEEE, Dubai, United Arab Emirates, 2020.

[18] D. H. Tashman and W. Hamouda, "An overview and future directions on physical-layer security for cognitive radio networks," *IEEE Network*, vol. 35, no. 3, pp. 205–211, 2021.

[19] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: an information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, 2009.

[20] S. Mishra and A. Trivedi, "Relay selection with channel allocation for cognitive radio relay channels in CRN," in *Eleventh International Conference on Wireless and Optical Communications Networks (WOCN)*, vol. 2014, pp. 1–4, IEEE, Vijayawada, India, 2014.

[21] T. Zhang, D. Zhang, J. Qiu, X. Zhang, P. Zhao, and C. Gong, "A kind of novel method of power allocation with limited cross-tier interference for CRN," *IEEE Access*, vol. 7, pp. 82571–82583, 2019.

[22] X. Zhang, Z. Yan, Y. Gao, and W. Wang, "On the study of outage performance for cognitive relay networks (CRN) with the nth best-relay selection in Rayleigh-fading channels," *IEEE Wireless Communications Letters*, vol. 2, no. 1, pp. 110–113, 2013.

[23] D. H. Tashman and W. Hamouda, "Physical-layer security on maximal ratio combining for SIMO cognitive radio networks over cascaded κ-μ fading channels," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 4, pp. 1244–1252, 2021.

[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] D. H. Tashman and W. Hamouda, "Physical-layer security for cognitive radio networks over cascaded Rayleigh fading channels," in *In GLOBECOM 2020–2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, Taipei, Taiwan, 2020.

[26] S. Chetry and A. Singh, "Physical layer security of outdated CSI based CRN," in *In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–5, IEEE, Bengaluru, India, 2018.

[27] N. Nandan, S. Majhi, and H. -C. Wu, "Maximizing secrecy capacity of underlay MIMO-CRN through bi-directional zero-forcing beamforming," *IEEE Transactions on Wireless Communications*, vol. 17, no. 8, pp. 5327–5337, 2018.

[28] S. O. Rice, "Statistical properties of a sine wave plus random noise," *The Bell System Technical Journal*, vol. 27, no. 1, pp. 109–157, 1948.

[29] A. Glavieux, P. Y. Cochet, and A. Picart, "Orthogonal frequency division multiplexing with BFSK modulation in frequency selective Rayleigh and Rician fading channels," *IEEE Transactions on Communications*, vol. 42, no. 234, pp. 1919–1928, 1994.

[30] N. C. Beaulieu and X. Jiandong, "A novel fading model for channels with multiple dominant specular components," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 54–57, 2015.

[31] P. S. Chauhan, S. Kumar, and S. K. Soni, "On the physical layer security over Beaulieu-Xie fading channel," *AEU–International Journal of Electronics and Communications*, vol. 113, article 152940, 2019.

[32] M. Mirahmadi, A. Al-Dweik, and A. Shami, "Interference modeling and performance evaluation of heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2132–2144, 2014.

[33] H. S. Silva, D. B. T. Almeida, W. J. L. Queiroz, I. E. Fonseca, A. S. R. Oliveira, and F. Madeiro, "Cascaded double beaulieu-xie fading channels," *IEEE Communications Letters*, vol. 24, no. 10, pp. 2133–2136, 2020.

[34] A. Olutayo, H. Ma, J. Cheng, and J. F. Holzman, "Level crossing rate and average fade duration for the Beaulieu-Xie fading

model," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 326–329, 2017.

[35] A. Olutayo, J. Cheng, and J. Holzman, "Asymptotically tight performance bounds for selection diversity over Beaulieu-Xie fading channels with arbitrary correlation," in *IEEE International Conference on Communications (ICC)*, vol. 2017, pp. 1–6, IEEE, Paris, France, 2017.

[36] H. S. Silva, D. B. T. Almeida, W. J. L. Queiroz, I. E. Fonseca, A. S. R. Oliveira, and F. Madeiro, "Outage probability of the product of two Beaulieu–Xie, η-μ, κ-μ, or α-μ random variables," *IEEE Antennas and Wireless Propagation Letters*, vol. 19, no. 12, pp. 2182–2186, 2020.

[37] V. Kansal and S. Singh, "Effective rate analysis of MISO over Beaulieu-Xie fading channel," *AEU-International Journal of Electronics and Communications*, vol. 138, article 153886, 2021.

[38] D. Singh and H. D. Joshi, "Generalized MGF based analysis of line-of-sight plus scatter fading model and its applications to MIMO-OFDM systems," *AEU - International Journal of Electronics and Communications*, vol. 91, pp. 110–117, 2018.

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

[40] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE International Symposium on Information Theory*, pp. 356–360, IEEE, Seattle, WA, USA, 2006.

[41] J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Communications*, vol. 12, no. 3, pp. 132–150, 2015.

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