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 Jin3

1The School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100084, China
2The Institute of Science and Technology for Opto-electronic Information, Yantai University, Yantai Shandong 264005, China
3Department 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

Copyright © 2020 Jiangfeng Sun et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 $\kappa-\mu$ 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 $\mu$, 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 anti-eavesdropping 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 $\kappa-\mu$ 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 $\alpha-\mu$ 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 $\kappa-\mu$ 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 $\kappa-\mu$ under suitable conditions. Moreover, the $\kappa-\mu$ 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 $\kappa-\mu$ shadowed fading, the authors of [31] studied the transmission performance by analyzing OP and ergodic channel capacity (ECC). The statistical characteristics of different shadowed $\kappa-\mu$ 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 $\kappa-\mu$ 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 $\kappa-\mu$ 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 $\kappa-\mu$ shadowed distribution in the open database, let alone the existence of multiple antennas and multiple 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 $\kappa-\mu$ 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 $\kappa-\mu$ 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 ($E_1, E_2, . . . , E_M$) 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 ($S \rightarrow P$) and the channel coefficients of main link ($S \rightarrow D$) and wiretap link ($S \rightarrow E$) are $h_D$ and $h_E$, respectively. It should be noted that $h_D$ and $h_E$ 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
\[ f_s(y) = (a_s)^{m_s} (b_s)^{m_s} \frac{1}{\Gamma(m_s)} \sum_{q=0}^{\infty} \frac{(m_s)_q}{(m_s)_q^q} \left( \frac{a_s k_s \mu_s}{b_s m_s} \right)^q y^{m_s-q-1} e^{-a_s y}, \]

\[ F_s(y) = b_s^{-m_s} \frac{1}{\Gamma(m_s)} \sum_{q=0}^{\infty} \frac{(m_s)_q (k_s \mu_s/b_s m_s)^q}{(m_s)_q^q} (\mu_s)^q \times (\mu_s + q - 1)! \left( 1 - e^{-a_s y} \sum_{s=0}^{\infty} \frac{(a_s y)^s}{s!} \right), \]

where \( a_s = \mu_s/(1 + k_s) \Omega_s \), \( b_s = (\mu_s k_s + m_s)/m_s \), and \( \mu_s \) is the lower right corner indicates that the parameter belongs to the channel \((S \rightarrow D)\).

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 \((S \rightarrow D)\) can be formulated as [35]

\[ f_D(y) = (N_D \Omega_D)^{N_D m_D} b_D^{-N_D m_D} \frac{1}{\Gamma(N_D \mu_D)} \sum_{q=0}^{\infty} \frac{(N_D m_D)_q}{(N_D \mu_D)_q^q} \times \left( \frac{k_D \mu_D}{b_D m_D} \right)^q (N_D \mu_D + q - 1)! \left( 1 - e^{-N_D \mu_D y} \sum_{s=0}^{\infty} \frac{(N_D \mu_D y)^s}{s!} \right), \]

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

\[ f_E(y) = (N_E \Omega_E)^{N_E m_E} b_E^{-N_E m_E} \frac{1}{\Gamma(N_E \mu_E)} \sum_{q=0}^{\infty} \frac{(N_E m_E)_q}{(N_E \mu_E)_q^q} \times \left( \frac{k_E \mu_E}{b_E m_E} \right)^q (N_E \mu_E + q - 1)! \left( 1 - e^{-N_E \mu_E y} \sum_{s=0}^{\infty} \frac{(N_E \mu_E y)^s}{s!} \right). \]

### 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

$$\text{Sop} = P\{C_D - C_E \leq R_{th}\},$$

(8)

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

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

$$\text{Sop} = P\{C_D - C_E \leq R_{th}\}
= P\{C_D - C_E \leq R_{th}, P_S = P_{sm}\}
+ P\{C_D - C_E \leq R_{th}, P_S = \frac{I_P}{X}\} = P_1 + P_2,$$

(9)

where $X$ is the instantaneous SNR of the link of $S \rightarrow P$.

Next, we will derive $P_1$ and $P_2$ in (9).

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

$$P_1 = P\{C_D - C_E \leq R_{th}, X \leq \frac{I_P}{P_{sm}}\}
= P\{\gamma_D \leq \frac{\theta_{YE}}{\zeta} + \frac{\theta - 1}{\zeta}\} P\{X \leq \frac{I_P}{P_{sm}}\} = J_1 J_2,$$

where $\theta = e^R$ and $\zeta = P_{sm}/\gamma_D$, and we obtain

$$J_1 = \int_0^\infty F_D\left(\frac{\theta_{YE}}{\zeta} + \frac{\theta - 1}{\zeta}\right) f_E(\gamma_E) d\gamma_E.$$

(11)

Employing (6) and (7), we have

$$J_1 = A_1 \int_0^\infty \left(1 - e^{-N_e\mu_E} \binom{\theta_{YE}}{\theta - 1}/s!\right) \times \sum_{s=0}^{N_e\mu_E - q - 1} \binom{N_e\mu_E}{s} \frac{(N_D a_D (\theta_{YE} + (\theta - 1)/\zeta))}{\theta_{YE}^{s-t_1}} d\gamma_E,$$

(12)

utilizing equation (1.111) in [39],

$$\left(\frac{\theta_{YE}}{\zeta} + \theta - 1\right)^s = \sum_{t_1=0}^s (t_1!)^{\theta_{YE}} \binom{\theta - 1}{\zeta}^{s-t_1}.$$

(14)

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

$$J_1 = A_1 \left(A_2 - e^{-N_e\mu_E} (\theta - 1)/s! \times \sum_{s=0}^{N_e\mu_E - q - 1} \binom{N_D a_D}{s} \sum_{t_1=0}^s (s/t_1!)^{\theta_{YE}} (\theta - 1)/\zeta)^{s-t_1} \times \frac{\Gamma(N_e\mu_E + p + t_1)}{(N_D a_D \theta + N_e a_E/M)^{(N_e\mu_E + p + t_1)}}\right),$$

(15)

where

$$A_2 = \frac{\Gamma(N_e\mu_E + p)}{(N_e a_E/M)^{(N_e\mu_E + p)}}$$

(16)

From (4), $J_2$ is derived as

$$J_2 = \left(1 - e^{-a_s(I_s/P_{sm})}\sum_{s=0}^{\mu_E - q - 1} \binom{a_s}{s!}\right) \times \left(1 - e^{-a_s(I_s/P_{sm})}\sum_{s=0}^{\mu_E - q - 1} \binom{a_s}{s!}\right).$$

(17)
3.2. Calculation of $P_2$. It can be seen from (9), $P_2$ is stated as

$$P_2 = P\left\{ (C_D - C_E) \leq R_{th}, P_S = \frac{I_p}{X} \right\}. \quad (18)$$

Referring to [22], we can rewrite $P_2$ as

$$P_2 = \int_{I_p/R_{th}}^{\infty} G(x) f_s(x)dx, \quad (19)$$

where

$$G(x) = \int_{0}^{\infty} F_D\left( \theta y + \left( \frac{\theta - 1}{\xi} \right) \right) f_E(y)dy. \quad (20)$$

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

$$G(x) = \Lambda \left( \frac{e^{-\frac{1}{\sigma^2}} / \mu + q} {1 - e^{-\frac{1}{\sigma^2}} / \mu + q} \right). \quad (21)$$

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

$$Spsc = 1 - P\left\{ C_D - C_E \leq 0 \right\} \quad (24)$$

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

$$\Xi = \int_{0}^{\infty} b_D^{-N_D \mu_D} \sum_{q=0}^{\infty} (N_D^{-\mu_D} \mu_D)^q \times \Gamma(N_D \mu_D + q - 1) \times \left( 1 - \sum_{s=0}^{\infty} e^{-N_D \mu_D / s} \right) \times \frac{\left( \frac{I_p}{P_{max}} \right)}{x D \mu_D + q + \sum_{s=0}^{\infty} \frac{\left( N_D^{-\mu_D} \mu_D \right)^s}{s!} \times \Gamma(N_D \mu_D + \mu_D + q)} \left( N_D \mu_D \right)^{t_s} \times \left( N_D \mu_D \right)^{t_d} \times \left( \frac{I_p}{P_{max}} \right). \quad (25)$$

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 analysis curves coincide well with the statistical simulation curves.

(ii) All simulation results change with abscissa, namely, $\Omega_D$, and the change trend indicates that a large $\Omega_D$ 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 $\Omega_D$ when $M$ takes different values. From Figure 2, we can see that when $\Omega_D$ 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
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 $9\, \text{dB}$, 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 $\mu$ 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 $S \rightarrow P$, $S \rightarrow D$, and $S \rightarrow E$, 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 $\Omega_D \geq 7\, \text{dB}$. However, the effect of increasing $\mu$ 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. $R_{\text{th}}$ represents the
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 $\kappa-\mu$ 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 $\mu$, smaller $I_p$, and smaller $R_{th}$ will enhance the security performance.
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. Moreover, we discuss the influence of the parameters including $M$, $N$, $k$, $\mu$, $I_p$, and $R_{th}$ on the security of IoT networks.

**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. Moreover, we discuss the influence of the parameters including $M$, $N$, $k$, $\mu$, $I_p$, 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 61771458 and Ministry of Land and Resources P.R.C. Special Project in the Public Interest under Grant 201311195-04.

**References**


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


