INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2016, VOL. 62, NO. 2, PP. 153–158
Manuscript received May 18, 2015; revised June, 2016. DOI: 10.1515/eletel-2016-0021

Probability of Secrecy Outage in Cognitive Radio Networks over Rician-Fading Channels

Jiliang Zhang, Hong Jiang, and Gaofeng Pan

Abstract—**In Rician-fading scenario, cognitive radio networks (CRNs) with a source in a secondary system transmitting its confidential information to a legitimate destination in the presence of an eavesdropper, are considered in this paper. Under CRNs, the interference power reaching at primary user (PU) is limited by some pre-defined threshold. Secrecy outage not only occurs when the achievable secrecy capacity for source-destination link is smaller than a target rate, but also occurs in the case that the interference power at PU is greater than that threshold. Analytical expression for secrecy outage probability has been derived and verified with simulation results. In addition, we have also derived the analytical expression for probability of non-zero secrecy capacity.**

Keywords—**Cognitive radio networks, wiretap, Rician-fading, secrecy outage probability, probability of non-zero secrecy capacity.**

I. Introduction

RECENTLY, cognitive radio has attracted many researchers' attention as it is a promising technology to support as many services and applications as possible in wireless networks with limited frequency spectrum [1]. In cognitive radio networks (CRNs), a secondary user (SU) is allowed to access and use the frequency spectrum of a licensed primary user (PU) to transmit its confidential information to a legitimate receiver subject to the constraint of promising PU system performance, and this condition can be satisfied if the interference power at PU is smaller than a pre-defined threshold.

Moreover, security is also an very important issue in wireless communications, as it is inherently vulnerable to eavesdroppers [2]. Traditionally, wireless security is considered in the higher layers of communication systems by authentication and cryptography [3]. However, recent works show that security can also be achieved in physical layer based on an information-theoretic sense [1]-[5], and it can be viewed as an alternative or a complement to cryptographic encryption [4]. In the analysis of physical-layer security, three nodes are normally involved: a legitimate transmitter, a legitimate receiver, and an eavesdropper. Wyner [5] first introduced a wiretap channel. It showed that if the source-destination channel is better than the source-eavesdropper channel, a non-zero secrecy rate could be guaranteed in the source-destination channel. Later, Wyner's wiretap model has been generated to non-degraded discrete memoryless broadcast channels [6], Gaussian channels [7], and fading channels [8]-[14].

Secrecy capacity (SC) under Rayleigh-fading scenario is considered in [8] and [9]. In [10], the effects of Nakagami-*m* fading on SC and probability of non-zero secrecy capacity (PNSC) were investigated. Under two different assumptions on the transmitter channel state information, the definition of SC was extended to account for the secrecy constraint over Rayleigh-fading channels in [11]. In order to increase SC, the authors in [12] proposed a novel artificial noise based method to impair the source-eavesdropper channel. Liu [13] derived analytical expressions for secrecy outage probability (SOP) over correlated log-normal fading channels. SC and SOP expressions in the form of infinite series have been shown in [14] when the source-destination and the source-eavesdropper channels are experienced correlated Rayleigh-fading.

In this paper, we consider the physical-layer security in CRNs. In CRNs, secrecy outage occurs either the achievable secrecy rate is smaller than a target rate if SU can successfully use the frequency spectrum of PU to transmit information, or the interference power at PU is greater than a pre-defined threshold. Moreover, another commonly used fading channel model is the Rician distribution, which is used when there is a line-of-sight (LOS) component existing in the transmission [15]. Thus, it is interesting to study the impacts of Rician-fading on the physical-layer security in CRNs. Keeping this in mind, analytical expression for SOP in CRNs over Rician-fading channels has been derived. In addition, the expression of PNSC have been derived.

This paper is organized as follows. Section 2 presents the system and channel model. Analytical expressions for SOP and PNSC are given in Section 3. Section 4 reports numerical results and discussions. Finally, concluding remarks are presented in Section 5.

II. System Model

In this paper, a wiretap channel model as shown in Fig. 1 is considered in CRNs. Specifically, four nodes are considered: a source (S), a destination (D), an eavesdropper (E) and a PU. S is allowed to access and use the frequency bands of PU to transmit its information to D while E is trying to overhear it.

As shown in Fig. 1, the received signals at D and E can be expressed as

$$y_D = \sqrt{P_s} h_{S,D} X_s + n_D \tag{1}$$

This research was supported in part by the National Science Foundation under Grants 61401372 and 61531016, Research Fund for the Doctoral Program of Higher Education of China under Grant 20130182120017, Natural Science Foundation of CQ CSTC under Grant cstc2013jcyjA40040, the Fundamental Research Funds for the Central Universities under Grant XDJK2015B023 and XDJK2016A011.).

The authors are with the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, P. R. China (e-mail: gfpan@swu.edu.cn).

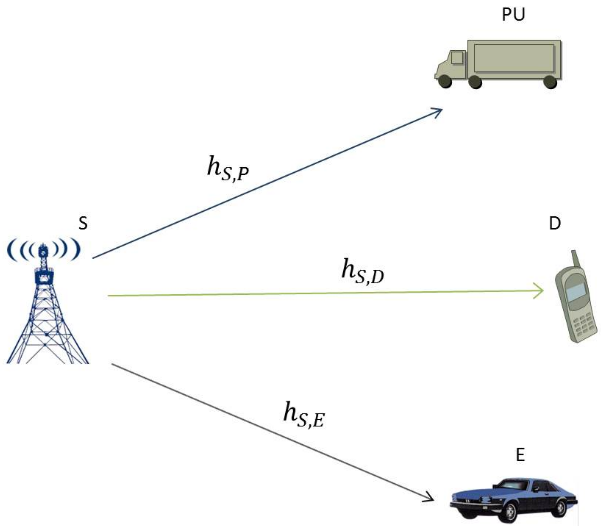

Fig. 1. System Model

and

$$y_E = \sqrt{P_s} h_{S,E} X_s + n_E \tag{2}$$

respectively, where P_s denotes the transmitted power at S, $h_{S,D}$ and $h_{S,E}$ are the channel coefficients, X_s is the transmitted symbol at S, and n_D and n_E are the additive white Gaussian noise (AWGN) with variances of σ_D^2 and σ_E^2, respectively. The instantaneous signal-to-noise ratios (SNRs) of the received signal at D and E are

$$\gamma_D = \bar{\gamma}_D |h_{S,D}|^2 \tag{3}$$

and

$$\gamma_E = \bar{\gamma}_E |h_{S,E}|^2 \tag{4}$$

where $\bar{\gamma}_D = P_s/\sigma_D^2$ and $\bar{\gamma}_E = P_s/\sigma_E^2$.

The received signal at PU is

$$y_P = \sqrt{P_s} h_{S,P} X_s + n_P \tag{5}$$

where $h_{S,P}$ is the channel coefficient and n_P is the AWGN with a variance of σ_P^2. The instantaneous interference power at PU is

$$P_I = P_s \left|h_{S,P}\right|^2 + \sigma_P^2. \tag{6}$$

For simplicity, we use h_0, h_1 and h_2 to represent $h_{S,D}$, $h_{S,E}$ and $h_{S,P}$, respectively. Moreover, we also assume that all the channels undergo identical and independent Rician-fading. Thus, h_i, where $i = 0, 1, 2$, are independent and identical Rician-distributed random variables. The channel state information h_i is assumed to be available at S. From [15], the probability density function (PDF) of $|h_i|^2$ is given by

$$f_{|h_i|^2}(x) = (1+K_i) e^{-[-K_i+(1+K_i)x]} I_0\left(2\sqrt{K_i(1+K_i)x}\right) \tag{7}$$

where $I_0(\cdot)$ is the zero-order modified Bessel function of the first kind, and K_i are the specular-to-total diffused power ratios of the Rician-fading channels, defined as

$$K_i = \frac{A_i^2}{2\sigma_i^2} \tag{8}$$

where A_i^2 is the power level of LOS component, and $2\sigma_i^2$ is the power level of the scattered components of the channels. The cumulative distribution function (CDF) of $|h_i|^2$ can be expressed as [15]

$$F_{|h_i|^2}(x) = 1 - Q_1\left(\sqrt{2K_i}, \sqrt{2(1+K_i)x}\right) \tag{9}$$

where $Q_1(\cdot,\cdot)$ is the first-order Marcum Q function.

III. Probability of Secrecy Outage

In this section, the analytical expressions for SOP and PNSC will be presented. The achievable rates at D and E are

$$R_D = \log_2(1+\gamma_D) \tag{10}$$

and

$$R_E = \log_2(1+\gamma_E) \tag{11}$$

respectively. Thus, the instantaneous achievable secrecy rate for S-D link is

$$C_s = \max\{R_D - R_E, 0\}. \tag{12}$$

Assuming $\gamma_D > \gamma_E$, the secrecy rate in (12) can be re-expressed as

$$C_s = \log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right). \tag{13}$$

In non-CRNs systems, the SOP is defined as the probability of the secrecy rate C_s is less than a given target rate R_s, where $R_s > 0$ [13]. While in CRNs systems, S can only use the frequency spectrum of PU to transmit information to D when $P_I \le \Gamma$, where Γ is the interference temperature limit. Hence, SOP can be defined as the probability that the secrecy rate C_s is less than R_s subject to the interference power constraint at PU, or the probability that the interference power at PU is greater than the interference temperature limit. Thus, the SOP in CRNs systems is

$$P_{sop} = Pr(C_s < R_s) Pr(P_I \le \Gamma) + Pr(P_I > \Gamma). \tag{14}$$

Substituting (3) and (4) into (13), we have

$$C_s = \log_2\left(\frac{1+\bar{\gamma}_D|h_0|^2}{1+\bar{\gamma}_E|h_1|^2}\right). \tag{15}$$

After some calculations, the probability expression of $Pr(C_s < R_s)$ can be written as

$$Pr(C_s < R_s) = Pr\left(|h_0|^2 < A + B\,|h_1|^2\right) \tag{16}$$

where

$$A = \frac{2^{R_s} - 1}{\bar{\gamma}_D} \tag{17}$$

and

$$B = \frac{\bar{\gamma}_E}{\bar{\gamma}_D} \times 2^{R_s}. \tag{18}$$

Since $|h_0|^2$ and $|h_1|^2$ are independent random variables with PDF and CDF respectively shown in (7) and (9), we substitute (7) and (9) into (16) and obtain the expression of $Pr(C_s < R_s)$ as shown in (19).

$$\begin{aligned} Pr(C_s < R_s) =& \int_0^\infty F_{|h_0|^2}(A+Bx) \times f_{|h_1|^2}(x)dx \\ =&1-(1+K_1)e^{-K_1}\int_0^\infty Q_1\Big(\sqrt{2K_0}, \sqrt{2(1+K_0)(A+Bx)}\Big)e^{-(1+K_1)x}I_0\Big(2\sqrt{K_1(1+K_1)x}\Big)dx. \end{aligned} \tag{19}$$

$$\begin{aligned} Pr(C_s < R_s) = 1 - \sqrt{\frac{1+K_1}{K_1}}e^{-\left[K_0+K_1+A(1+K_0)-\frac{K_1(1+K_1)}{2[1+K_1+B(1+K_0)]}\right]}\sum_{n=0}^{\infty}\sum_{p=0}^{n}\frac{{K_0}^n(1+K_0)^p}{\Gamma(n+1)\Gamma(p+1)}\sum_{m=0}^{p}\binom{p}{m}A^m B^{p-m} \\ \times \frac{\Gamma(p-m+1)}{[1+K_1+B(1+K_0)]^{p-m+\frac{1}{2}}}M_{m-p-\frac{1}{2},0}\left(\frac{K_1(1+K_1)}{1+K_1+B(1+K_0)}\right) \end{aligned} \tag{20}$$

Next, after some manipulations, we have a simpler expression of $Pr(C_s < R_s)$ as shown in (20), in which $\Gamma(n+1) = n!$ is the Gamma function, $\binom{p}{m} = \frac{p!}{m!(p-m)!}$, and $M_{\cdot,\cdot}(\cdot)$ represents the Whittaker function defined in [16]. The detailed derivations of (20) is shown in Appendix.

In what follows, the truncation error of the infinite series of (20) will be analysed. Assuming that only the first $N+1$ terms (i.e., n takes from 0 to N) in (20) are used to calculate $Pr(C_s < R_s)$, and substituting (A.6) into (19), the truncation error can be expressed as

$$\begin{aligned} E = &(1+K_1)e^{-(K_0+K_1)}\int_0^\infty \sum_{n=N+1}^{\infty}\frac{{K_0}^n}{(n!)^2} \\ &\times \Gamma\Big(1+n, (1+K_0)(A+Bx)\Big)e^{-(1+K_1)x} \\ &\times I_0\Big(2\sqrt{K_1(1+K_1)x}\Big)dx. \end{aligned} \tag{21}$$

Note that the incomplete Gamma function shown in (21) is bounded by

$$\begin{aligned} &\Gamma\Big(1+n, (1+K_0)(A+Bx)\Big) \\ &= n!e^{-(1+K_0)(A+Bx)}\sum_{p=0}^{n}\frac{[(1+K_0)(A+Bx)]^p}{p!} \\ &< n!. \end{aligned} \tag{22}$$

Thus, the truncation error E is upper bounded as

$$\begin{aligned} E < &(1+K_1)e^{-(K_0+K_1)}\sum_{n=N+1}^{\infty}\frac{{K_0}^n}{n!} \\ &\times \int_0^\infty e^{-(1+K_1)x}I_0\Big(2\sqrt{K_1(1+K_1)x}\Big)dx. \end{aligned} \tag{23}$$

From Eq. 6.614.3 of [16] and after some calculations, we have

$$\begin{aligned} E <& \frac{1}{\sqrt{K_1}}e^{-(K_0+\frac{K_1}{2})}\sum_{n=N+1}^{\infty}\frac{{K_0}^n}{n!}M_{-\frac{1}{2},0}(K_1) \\ =&\frac{1}{\sqrt{K_1}}e^{-(K_0+\frac{K_1}{2})}\left(e^{K_0}-\sum_{n=0}^{N}\frac{{K_0}^n}{n!}\right)M_{-\frac{1}{2},0}(K_1). \end{aligned} \tag{24}$$

Obviously, it has $\lim\limits_{N\to\infty}\sum_{n=0}^{N}\frac{{K_0}^n}{n!} = e^{K_0}$, which means the truncation error E converges to zero as n goes to infinity.

Next, as the interference power is $P_I = P_s|h_2|^2 + \sigma_P^2$, the probability when $P_I \le \Gamma$, i.e., $Pr(P_I \le \Gamma)$, is given as

$$\begin{aligned} Pr(P_I \le \Gamma) =& Pr(P_s|h_2|^2 + \sigma_P^2 \le \Gamma) \\ =&Pr\left(|h_2|^2 \le \frac{\Gamma-\sigma_P^2}{P_s}\right) \\ =&1-Q_1\left(\sqrt{2K_2}, \sqrt{\frac{2(1+K_2)(\Gamma-\sigma_P^2)}{P_s}}\right). \end{aligned} \tag{25}$$

Finally, the probability expression of $Pr(P_I > \Gamma)$ as shown in (14) can be obtained using the relationship of $Pr(P_I > \Gamma) = 1 - Pr(P_I \le \Gamma)$.

PNSC is another important characterization of the physical-layer security and is defined as the probability that the secrecy rate for S-D link is positive, which can be computed as [8]

$$\begin{aligned} PNSC =& 1 - P_{sop} \\ =&Pr(C_s > R_s)Pr(P_I \le \Gamma) \\ &\text{s.t.}\quad R_s = 0. \end{aligned} \tag{26}$$

By setting $R_s = 0$ in (20) and using the relationship of $Pr(C_s > 0) = 1 - Pr(C_s < 0)$, we have the final expression of $Pr(C_s > 0)$ denoted as (27) shown on the top of the next page.

IV. Numerical Results and Discussions

In this section, numerical results and discussions are presented. In Fig. 2, we present the analytical SOP versus $\bar{\gamma}_D/\bar{\gamma}_E$, and those analytical results are obtained from SOP expression by truncating the infinite series with different values of N. As depicted in Fig. 2, it is observed that larger value of N results in better SOP performance when $N < 30$ under certain conditions, as truncation error is still large and more terms are needed to calculate the analytical results. However, this increment of N does not improve the SOP performance when $N > 30$. This is because truncation error is very small when $N > 30$ and it is insignificant in calculating the analytical results. Hence, in what follows, we choose $N = 30$ to calculate the analytical results.

$$Pr(C_s > 0) = \sqrt{\frac{1+K_1}{K_1}} e^{-\left[K_0+K_1-\frac{K_1(1+K_1)}{2[1+K_1+\frac{\bar{\gamma}_E}{\bar{\gamma}_D}(1+K_0)]}\right]} \sum_{n=0}^{\infty}\sum_{p=0}^{n} \frac{{K_0}^n(1+K_0)^p(\frac{\bar{\gamma}_E}{\bar{\gamma}_D})^p}{\Gamma(n+1)\Gamma(p+1)} \times \frac{\Gamma(p+1)}{[1+K_1+\frac{\bar{\gamma}_E}{\bar{\gamma}_D}(1+K_0)]^{p+\frac{1}{2}}} M_{-p-\frac{1}{2},0}\left(\frac{K_1(1+K_1)}{1+K_1+\frac{\bar{\gamma}_E}{\bar{\gamma}_D}(1+K_0)}\right). \tag{27}$$

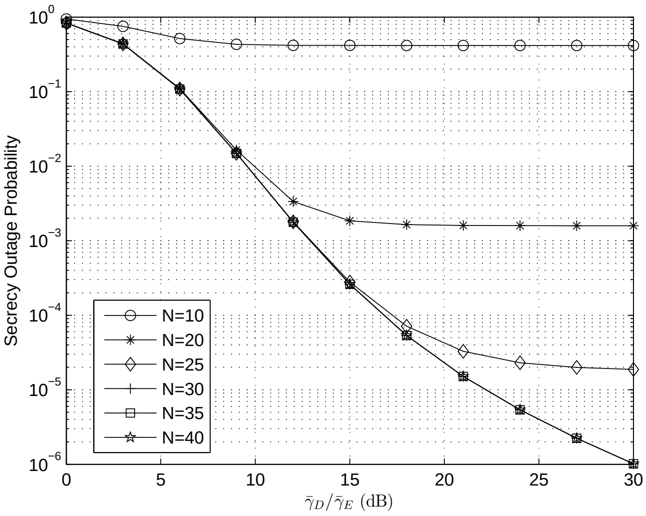

Fig. 2. Secrecy outage probability versus $\bar{\gamma}_D/\bar{\gamma}_E$ with $R_s = 0.5$ bits/s/Hz, $K_1 = 5$, $K_0 = K_2 = 10$, $\Gamma/P_s = 9$ dB, and $\bar{\gamma}_P = 20$ dB.

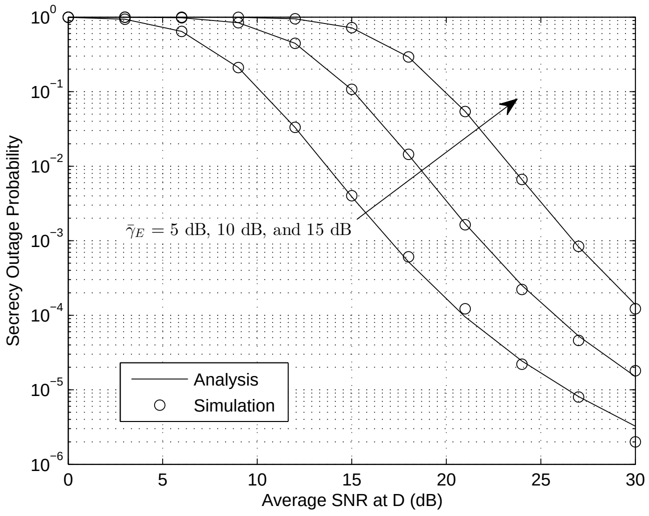

Fig. 3. Secrecy outage probability versus average SNR at destination with $R_s = 0.5$ bits/s/Hz, $K_0 = K_1 = K_2 = 10$, $\Gamma/P_s = 9$ dB, and $\bar{\gamma}_P = 20$ dB.

Fig. 3 shows the SOP versus average SNR $\bar{\gamma}_D$ with $\bar{\gamma}_E = 5$ dB, 10 dB and 15 dB, respectively. In Fig. 3, simulation results are obtained by performing 500000 independent trials at each $\bar{\gamma}_D$ point. It is seen that simulation curves match well with the analytical results. This match verifies the analytical expression derived. Moreover, we also observe that a lower SOP value could be obtained when $\bar{\gamma}_D$ is comparably higher with respective to $\bar{\gamma}_E$. It means that S has a higher probability of successfully transmitting information to D without being overheard by E when S-D link is better than S-E link.

SOP versus $\bar{\gamma}_D/\bar{\gamma}_E$ under various specular-to-total diffused power ratios of S-D link, K_0, is shown in Fig. 4. Comparing SOP performance with different K_0 values, we find that SOP performance with a higher value of K_0 is superior to that with a lower one, as S-D link is better when K_0 is higher.

Fig. 5 shows SOP performance under different values of Γ/P_s. As depicted in Fig. 5, we can see that a higher Γ leads to better SOP performance. This is because under CRNs, S can only use the PU frequency bands to transmit its confidential information when the interference power, P_I, at PU is less than Γ. Therefore, SOP performance is better with a higher value of Γ, as P_I has less chance to exceed it. However, we can also see from Fig. 5, this is not always hold with the increment of Γ. There exits a particular value of Γ under certain conditions, and SOP performance can not be improved when Γ is beyond that value. This particular value is equal to the maximum interference power at PU.

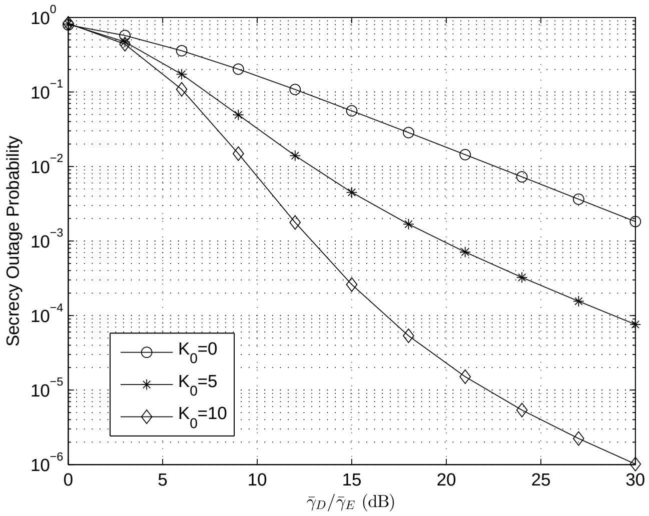

Fig. 4. Secrecy outage probability versus $\bar{\gamma}_D/\bar{\gamma}_E$ with $R_s = 0.5$ bits/s/Hz, $K_1 = 5$, $K_2 = 10$, $\Gamma/P_s = 9$ dB, and $\bar{\gamma}_P = 20$ dB.

PNSC performance with $\bar{\gamma}_E = -15$ dB, -10 dB and -5 dB is shown in Fig. 6. It is noted that PNSC performance can be improved when $\bar{\gamma}_D$ increases or $\bar{\gamma}_E$ decreases. This is due to the fact that S-D link is better than S-E link.

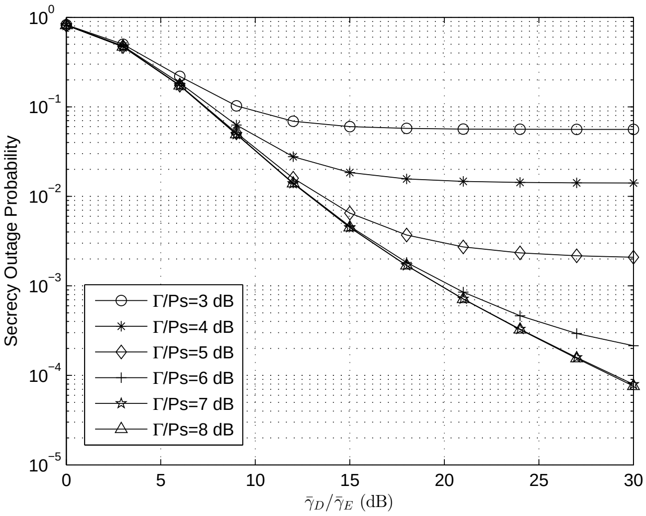

Fig. 5. Secrecy outage probability versus $\bar{\gamma}_D/\bar{\gamma}_E$ with $R_s = 0.5$ bits/s/Hz, $K_0 = K_1 = K_2 = 5$, and $\bar{\gamma}_P = 20$ dB.

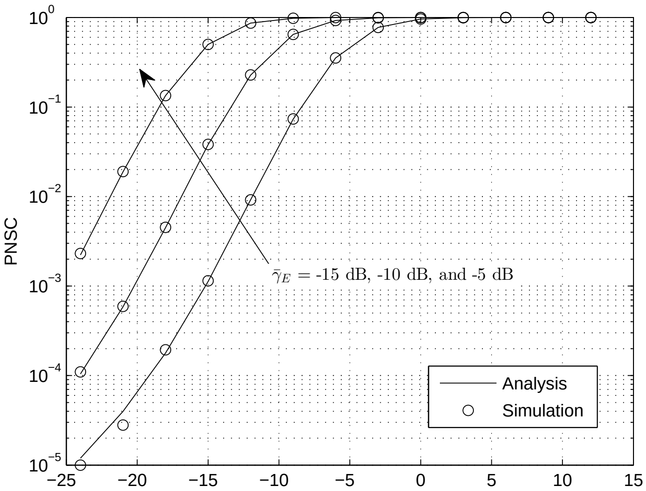

Fig. 6. PNSC versus average SNR at destination with $R_s = 0.5$ bits/s/Hz, $K_0 = K_1 = K_2 = 10$, $\Gamma/P_s = 9$ dB, and $\bar{\gamma}_P = 20$ dB.

V. Conclusion

In this paper, we focus on the secrecy outage performance in cognitive radio networks, in which all the fading channels are assumed to be Rician-faded. Analytical expressions with infinite-series representations of secrecy outage probability and probability of non-zero secrecy capacity have been derived. It has been shown that summing up finite series is enough to obtain the analytical results, as truncation error would converge to zero. Simulation results verify the derived analytical expressions.

Appendix

It is noted that the first-order Marcum Q function, $Q_1(\cdot,\cdot)$, inside of (19) is defined as [15]

$$Q_1(a,b) = \int_b^\infty x e^{-(\frac{x^2+a^2}{2})} I_0(ax)dx \qquad (A.1)$$

and the zero-order modified Bessel function of the first kind, $I_0(\cdot)$, can be also represented by the infinite series

$$I_0(x) = \sum_{n=0}^{\infty} \frac{(x/2)^{2n}}{(n!)^2}. \qquad (A.2)$$

Substituting (A.2) into (A.1), and after some manipulations, we have

$$Q_1(a,b) = e^{-a^2/2} \sum_{n=0}^{\infty} \frac{a^{2n}}{2^n (n!)^2} \int_{b^2/2}^{\infty} e^{-u} u^n du. \qquad (A.3)$$

Note that the incomplete gamma function is defined as [16]

$$\Gamma(a,x) = \int_x^\infty e^{-t} t^{a-1} dt. \qquad (A.4)$$

with its special case shown as

$$\Gamma(1+n,x) = n! e^{-x} \sum_{p=0}^{n} \frac{x^p}{p!}. \qquad (A.5)$$

Thus, the integration part of (A.3) can be replaced by (A.5), and letting $a = \sqrt{2K_0}$ and $b = \sqrt{2(1+K_0)(A+Bx)}$, we obtain

$$\begin{aligned} &Q_1\Bigg(\sqrt{2K_0}, \sqrt{2(1+K_0)(A+Bx)}\Bigg) \\ &= e^{-K_0} \sum_{n=0}^{\infty} \frac{{K_0}^n}{(n!)^2} \Gamma\Bigg(1+n, (1+K_0)(A+Bx)\Bigg) \\ &= e^{-K_0+(1+K_0)(A+Bx)} \sum_{n=0}^{\infty} \sum_{p=0}^{n} \frac{{K_0}^n [(1+K_0)(A+Bx)]^p}{n! p!}. \end{aligned} \qquad (A.6)$$

Next, substituting (A.6) into (19), we have

$$\begin{aligned} Pr(C_s < R_s) = 1 - (1+K_1) & e^{-[K_0+K_1+A(1+K_0)]} \\ & \times \sum_{n=0}^{\infty} \sum_{p=0}^{n} \frac{{K_0}^n (1+K_0)^p}{\Gamma(n+1)\Gamma(p+1)} \\ & \times \int_0^\infty e^{-[(1+K_1)+B(1+K_0)]x} \Bigg(A+Bx\Bigg)^p \\ & \times I_0\Bigg(2\sqrt{K_1(1+K_1)x}\Bigg) dx. \end{aligned} \qquad (A.7)$$

Furthermore, the expression of $\Bigg(A+Bx\Bigg)^p$ in (A.7) can be expanded using power series defined in Eq. 1.111 of [16] as

$$\Bigg(A+Bx\Bigg)^p = \sum_{m=0}^{p} \binom{p}{m} A^m (Bx)^{p-m}. \qquad (A.8)$$

From Eq. 6.643.2 of [16] and substituting (A.8) into (A.7), we obtain the final expression of $Pr(C_s < R_s)$ as shown in (20),

References

[1] E. Hossain and V. Bhargava, *Cognitive Wireless Communication Networks*, Springer, 2007.

[2] N. S. Ferdinand, D. B. da Costa, A. F. de Almeida, and M. Latva-aho, “Physical layer secrecy performance of TAS wiretap channels with correlated main and eavesdropper channels,” *IEEE Commun. Lett.*, vol. 3, no. 1, pp. 86-89, Feb. 2014.

[3] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733-742, May 1993.

[4] Q. Li, H. Song, and K. Huang, “Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels,” *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892-895, May 2013.

[5] A. Wyner, “The wire-tap channel,” *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355-1367, Oct. 1975.

[6] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[7] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008.

[9] P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[10] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, “Secrecy capacity of Nakagami-*m* fading wireless channels in the presence of multiple eavesdroppers,” in *Asilomar Conference on Signals, Systems, and Coputers*, California, 2009; 829-833.

[11] O. Gungor, J. Tan, C. E. Koksal, H. El Gamal, “Secrecy outage capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379-5397, Aug. 2013.

[12] W. Li, M. Ghogho, B. Chen, and C. Xiong, “Secure communications via sending artificial noise by the receiver: Outage secrecy capacity/Region analysis,” *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628-1631, Oct. 2012.

[13] X. Liu, “Outage probability of secrecy capacity over correlated log-normal fading channels,” *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 289-292, Feb. 2013.

[14] X. Sun, J. Wang, W. Xu, and C. Zhao, “Performance of secure communications over correlated fading channels,” *IEEE Sig. Process. Lett.*, vol. 19, no. 8, pp. 479-482, Aug. 2012.

[15] J. G. Proakis and M. Salehi, *Digital Communications*, 5th Ed., McGraw-Hill, 2007.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products.*, 7th Ed., Elsevier, 2007.