SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2017, Vol. 60 022307:1–022307:9
doi: 10.1007/s11432-015-0973-8

Secrecy outage analysis for underlay cognitive radio networks over correlated channels

Jiliang ZHANG, Hui ZHAO & Gaofeng PAN*

Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, School of Electronic and Information Engineering, Southwest University, Chongqing 400715*, China*

Received June 27, 2016; accepted August 12, 2016; published online November 17, 2016

Abstract This paper investigates the secrecy outage performance of underlay cognitive radio networks, in which a source in a secondary system transmits its confidential information to a legitimate destination in the presence of an eavesdropper. Specifically, the main (the source-to-destination) and eavesdropping (the source-to-eavesdropper) channels are assumed to be correlated. Moreover, it is also assumed that the main channel and the channel from the source to the primary user's receiver are correlated. Tight closed-form analytical expression for secrecy outage probability and the closed-form analytical expression for the probability of non-zero secrecy capacity are derived and validated by simulation results when the interference temperature limit is comparably large.

Keywords cognitive radio networks, correlated fading channels, probability of non-zero secrecy capacity, secrecy outage probability

Citation Zhang J L, Zhao H, Pan G F. Secrecy outage analysis for underlay cognitive radio networks over correlated channels. Sci China Inf Sci, 2017, 60(2): 022307, doi: 10.1007/s11432-015-0973-8

1 Introduction

Security plays an essential role in wireless communications, as it is inherently vulnerable to eavesdroppers. Traditionally, security is considered in the higher layers of communication protocols by authentication and cryptography. However, in recent years, physical layer security in the information-theoretic sense has attracted considerable interest [1–8], and can be viewed as an alternative or a complement to cryptographic encryption [7]. In [1], Wyner first introduced a wiretap model, and he showed that when the source-to-eavesdropper (S-E) channel was a degraded version of the source-to-destination (S-D) channel, a non-zero secrecy rate could be achieved over the S-D channel. Capacity-equivocation region for discrete and Gaussian memoryless cognitive interference channels with and without secrecy was established in [2]. Liang et al. in [3] obtained the secrecy capacity (SC) region for the collaborative eavesdropping model and inner and outer bounds on the secrecy capacity region for the non-collaborative eavesdropping model over wireless broadcast networks. SC analysis over Rayleigh-fading channels was studied in [4]. Considering heterogeneous cellular networks, physical layer security was studied in [5]. In [6], signal design and optimization were investigated to enhance wireless secrecy in cooperative systems. Later, the wiretap

* Corresponding author (email: gfpan@swu.edu.cn)

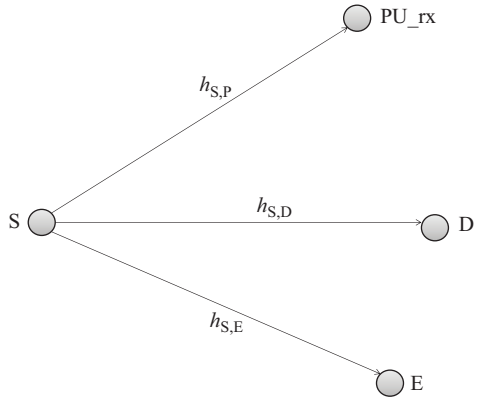

Figure 1 System model.

model has been generalized into multiple-input-single-output (MISO) systems [7, 8]. Li et al. in [7] proposed a random beamforming security scheme for MISO wiretap channels. The effect of finite-alphabet input on the ergodic secrecy of a MISO system was investigated in [8].

On the other hand, cognitive radio networks (CRNs) have also received much attention, as they can solve the problem of spectrum scarcity [9, 10]. Hence, it is interesting and promising to investigate physical layer security issues in CRNs. A thorough literature review of physical layer security in CRNs was presented in [11,12]. Considering a MISO CRN under slow fading channels in the presence of multiple eavesdroppers, the secrecy throughput maximization problems were investigated in [13]. In [14], a new cooperative paradigm for secure communication in CRNs was proposed without degrading the secrecy rate for primary systems. The authors in [15] investigated a secure medium access protocol in CRNs. In [16], the analytical expression for secrecy outage probability (SOP) over Nakagami-m fading channels was derived.

In practical wireless communications, in order to overhear the information as much as possible, passive eavesdroppers or active jammers may be placed close to the destination (i.e., this eavesdropper may be also a legitimate receiver for another system, but it acts as an eavesdropper in our interested secondary system). This close may result in the signals received at D and E experience similar fading to some extent. In other words, the S-D and S-E channels may be correlated with each other with a certain correlation coefficient. Under CRNs systems, since the source in the secondary system transmits information through the same frequency bands as primary system, the S-D and source-primary user's receiver (PU_rx) channels may or may not correlated depending on how close D is placed to PU_rx. Thus, to make it more general, it is reasonable to consider those two channels to be correlated, as uncorrelated case is just a special case of the correlated scenario.

Note that all the aforementioned works about physical layer security issues in CRNs are limited to independent channels only. As stated above, it is also interesting and promising to consider the correlated scenario. Therefore, in this paper, we focus on correlated channels. In particular, the secrecy outage performance of underlay CRNs is studied by assuming the S-D and S-E channels to be correlated, and the S-D and S-PU_rx channels are also assumed to be correlated. Main contributions of this work are as follows.

(1) Under correlated Rayleigh-fading channels, we derive a tight closed-form expression of SOP. From simulation results, we find that this tight approximation is validated when the interference temperature limit is comparably large.

(2) The expression of probability of non-zero secrecy capacity (PNSC) has been also derived over correlated Rayleigh-fading channels.

2 System model

In this work, we consider an underlay wiretap CRNs as shown in Figure 1. It consists of a source, a destination, an eavesdropper in a secondary system and a PU_rx. S transmits confidential information to D, while E wants to overhear it. It is assumed that the S-D and S-E channels are correlated with correlation coefficient ρ_{E}. Moreover, we also assume that the S-D and S-PU_rx links are correlated with correlation coefficient ρ_{P}. The values of those two correlation coefficients are between 0 and 1. When the correlation coefficient is 0, it means those two channels are independent; if the correlation coefficient is 1, it means that they are fully correlated.

The received signal at D can be written as

$$y_{\mathrm{D}} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{S,D}} X_{\mathrm{S}} + n_{\mathrm{D}}, \tag{1}$$

where P_{S} denotes the transmitted power, $h_{\mathrm{S,D}}$ is the channel coefficient modeled as a zero-mean, complex Gaussian random variable with unit variance. To simplify the expression, in the following analysis, we use h_0 to represent $h_{\mathrm{S,D}}$. X_{S} is the transmitted symbol, and n_{D} is the additive white Gaussian noise (AWGN) with a variance of σ_{D}^2.

Thus, the instantaneous signal-to-noise ratio (SNR) at D can be expressed as

$$\gamma_{\mathrm{D}} = \bar{\gamma}_{\mathrm{D}} |h_0|^2, \tag{2}$$

where $\bar{\gamma}_{\mathrm{D}} = P_{\mathrm{S}}/\sigma_{\mathrm{D}}^2$.

The received signal at E can be presented as

$$y_{\mathrm{E}} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{S,E}} X_{\mathrm{S}} + n_{\mathrm{E}}, \tag{3}$$

where n_{E} is the AWGN with a variance of σ_{E}^2.

Since the S-D and S-E channels are correlated, the channel coefficient, $h_{\mathrm{S,E}}$, can be modeled as [17]

$$h_{\mathrm{S,E}} = \rho_{\mathrm{E}} h_0 + \sqrt{1-\rho_{\mathrm{E}}^2} h_1, \tag{4}$$

where h_1 is a zero-mean, complex Gaussian random variable with unit variance.

The instantaneous SNR at E can be given as

$$\gamma_{\mathrm{E}} = \bar{\gamma}_{\mathrm{E}} |h_{\mathrm{S,E}}|^2, \tag{5}$$

where $\bar{\gamma}_{\mathrm{E}} = P_{\mathrm{S}}/\sigma_{\mathrm{E}}^2$.

Substituting (4) into (5), we can have

$$\begin{aligned} \gamma_{\mathrm{E}} &= \bar{\gamma}_{\mathrm{E}} \left| \rho_{\mathrm{E}} h_0 + \sqrt{1-\rho_{\mathrm{E}}^2} h_1 \right|^2 \\ &= \bar{\gamma}_{\mathrm{E}} \left[\rho_{\mathrm{E}}^2 |h_0|^2 + (1-\rho_{\mathrm{E}}^2) |h_1|^2 + 2\rho_{\mathrm{E}} \sqrt{1-\rho_{\mathrm{E}}^2} (\Re[h_0]\Re[h_1] + \Im[h_0]\Im[h_1]) \right], \end{aligned} \tag{6}$$

where $\Re[\cdot]$ and $\Im[\cdot]$ denote the real and imaginary parts, respectively.

The received signal at PU_rx can be given as

$$y_{\mathrm{P}} = \sqrt{P_{\mathrm{S}}} h_{\mathrm{S,P}} X_{\mathrm{S}} + n_{\mathrm{P}}, \tag{7}$$

where n_{P} is the AWGN with a variance of σ_{P}^2.

Similar to (4), $h_{\mathrm{S,P}}$ can be also modeled as

$$h_{\mathrm{S,P}} = \rho_{\mathrm{P}} h_0 + \sqrt{1-\rho_{\mathrm{P}}^2} h_2, \tag{8}$$

where h_2 is a zero-mean, complex Gaussian random variable with unit variance.

The interference power at PU_rx is from source and noise, and it can be written as

$$P_{\mathrm{I}} = P_{\mathrm{S}} \left|h_{\mathrm{S,P}}\right|^2 + \sigma_{\mathrm{P}}^2. \tag{9}$$

Substituting (8) into (9), the interference power is given as

$$\begin{aligned} P_{\mathrm{I}} &= P_{\mathrm{S}} \left| \rho_{\mathrm{P}} h_0 + \sqrt{1-\rho_{\mathrm{P}}^2} h_2 \right|^2 + \sigma_{\mathrm{P}}^2 \\ &= P_{\mathrm{S}} \left[\rho_{\mathrm{P}}^2 \left|h_0\right|^2 + (1-\rho_{\mathrm{P}}^2) \left|h_2\right|^2 + 2\rho_{\mathrm{P}} \sqrt{1-\rho_{\mathrm{P}}^2} (\Re[h_0]\Re[h_2] + \Im[h_0]\Im[h_2]) \right] + \sigma_{\mathrm{P}}^2. \end{aligned} \tag{10}$$

3 Secrecy outage performance

In this section, we will present the derivations of SOP and PNSC. The instantaneous achievable secrecy rate for S-D link can be written as

$$C_s = \begin{cases} \log_2(1+\gamma_{\mathrm{D}}) - \log_2(1+\gamma_{\mathrm{E}}), & \text{if } \gamma_{\mathrm{D}} > \gamma_{\mathrm{E}}, \\ 0, & \text{if } \gamma_{\mathrm{D}} < \gamma_{\mathrm{E}}. \end{cases} \tag{11}$$

The SOP is defined as the probability that the secrecy rate C_s is less than a given target rate R_s, where $R_s > 0$, in non-CRNs systems. However, in CRNs, S in the secondary system can only access and share the frequency bands of primary system to transmit information to D when the interference power P_{I} at PU_rx is smaller than the interference temperature limit Γ. Thus, secrecy outage occurs either when the secrecy rate C_s is less than a given target rate R_s subject to $P_{\mathrm{I}} \leqslant \Gamma$, or when $P_{\mathrm{I}} > \Gamma$. Therefore, the SOP in CRNs can be expressed as

$$P_{\mathrm{sop}} = \Pr(C_s < R_s)\Pr(P_{\mathrm{I}} \leqslant \Gamma) + \Pr(P_{\mathrm{I}} > \Gamma), \tag{12}$$

where

$$\Pr(C_s < R_s) \approx \begin{cases} 1 - \dfrac{\mathrm{e}^{-\frac{\alpha-1}{\bar{\gamma}_{\mathrm{D}} - \alpha\bar{\gamma}_{\mathrm{E}}\rho_{\mathrm{E}}^2}}}{1+\frac{\alpha\bar{\gamma}_{\mathrm{E}}(1-\rho_{\mathrm{E}}^2)}{\bar{\gamma}_{\mathrm{D}} - \alpha\bar{\gamma}_{\mathrm{E}}\rho_{\mathrm{E}}^2}}, & \text{if } \bar{\gamma}_{\mathrm{D}} > \alpha\bar{\gamma}_{\mathrm{E}}\rho_{\mathrm{E}}^2, \\ 1, & \text{if } \bar{\gamma}_{\mathrm{D}} < \alpha\bar{\gamma}_{\mathrm{E}}\rho_{\mathrm{E}}^2, \end{cases} \tag{13}$$

in which $\alpha = 2^{R_s}$,

$$\Pr(P_{\mathrm{I}} \leqslant \Gamma) \approx \begin{cases} 1 - \dfrac{\mathrm{e}^{-\frac{\Gamma-\sigma_{\mathrm{P}}^2}{P_{\mathrm{S}}\rho_{\mathrm{P}}^2}}}{1-\frac{1-\rho_{\mathrm{P}}^2}{\rho_{\mathrm{P}}^2}}, & \text{if } \rho_{\mathrm{P}} \neq 0, \\ 1 - \mathrm{e}^{-\frac{\Gamma-\sigma_{\mathrm{P}}^2}{P_{\mathrm{S}}}}, & \text{if } \rho_{\mathrm{P}} = 0, \end{cases} \tag{14}$$

and

$$\Pr(P_{\mathrm{I}} > \Gamma) = 1 - \Pr(P_{\mathrm{I}} \leqslant \Gamma) \approx \begin{cases} \dfrac{\mathrm{e}^{-\frac{\Gamma-\sigma_{\mathrm{P}}^2}{P_{\mathrm{S}}\rho_{\mathrm{P}}^2}}}{1-\frac{1-\rho_{\mathrm{P}}^2}{\rho_{\mathrm{P}}^2}}, & \text{if } \rho_{\mathrm{P}} \neq 0, \\ \mathrm{e}^{-\frac{\Gamma-\sigma_{\mathrm{P}}^2}{P_{\mathrm{S}}}}, & \text{if } \rho_{\mathrm{P}} = 0. \end{cases} \tag{15}$$

Proof. Assuming $\gamma_{\mathrm{D}} > \gamma_{\mathrm{E}}$, the secrecy rate in (11) can be rewritten as

$$C_s = \log_2\left(\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}}\right). \tag{16}$$

Substituting (2) and (6) into (16), we have

$$C_s = \log_2\left(\frac{1+\bar{\gamma}_{\mathrm{D}}|h_0|^2}{1+\bar{\gamma}_{\mathrm{E}}[\rho_{\mathrm{E}}^2 \left|h_0\right|^2 + (1-\rho_{\mathrm{E}}^2)\left|h_1\right|^2 + 2\rho_{\mathrm{E}}\sqrt{1-\rho_{\mathrm{E}}^2}(\Re[h_0]\Re[h_1] + \Im[h_0]\Im[h_1])]}\right). \tag{17}$$

Due to the two crossing terms of the two independent random variables (i.e., $\Re[h_0]\Re[h_1]$ and $\Im[h_0]\Im[h_1]$) shown in (17), it is very difficult to derive the analytical probability expression subject to $C_s < R_s$ (i.e., $\Pr(C_s < R_s)$). Therefore, to simplify the analysis, a tight approximation is applied by ignoring those two crossing terms to yield

$$C_s \approx \log_2\left(\frac{1+\bar{\gamma}_{\rm D}|h_0|^2}{1+\bar{\gamma}_{\rm E}[\rho_{\rm E}^2\,|h_0|^2+(1-\rho_{\rm E}^2)\,|h_1|^2]}\right), \tag{18}$$

and more discussions on the validation of this approximation will be presented in Section 4.

Using (18), the expression of $\Pr(C_s < R_s)$ is given as

$$\begin{aligned}\Pr(C_s < R_s) &\approx \Pr\left(\log_2\left(\frac{1+\bar{\gamma}_{\rm D}|h_0|^2}{1+\bar{\gamma}_{\rm E}[\rho_{\rm E}^2\,|h_0|^2+(1-\rho_{\rm E}^2)\,|h_1|^2]}\right) < R_s\right)\\ &= \Pr\left(\frac{1+\bar{\gamma}_{\rm D}|h_0|^2}{1+\bar{\gamma}_{\rm E}[\rho_{\rm E}^2\,|h_0|^2+(1-\rho_{\rm E}^2)\,|h_1|^2]} < 2^{R_s}=\alpha\right)\\ &= \Pr((\bar{\gamma}_{\rm D}-\alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2)\,|h_0|^2 < \alpha-1+\alpha\bar{\gamma}_{\rm E}(1-\rho_{\rm E}^2)\,|h_1|^2).\end{aligned} \tag{19}$$

If $\bar{\gamma}_{\rm D} < \alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2$, it always holds for $(\bar{\gamma}_{\rm D}-\alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2)\,|h_0|^2 < \alpha-1+\alpha\bar{\gamma}_{\rm E}(1-\rho_{\rm E}^2)\,|h_1|^2$, as $(\bar{\gamma}_{\rm D}-\alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2)\,|h_0|^2 < 0$ and $\alpha-1+\alpha\bar{\gamma}_{\rm E}(1-\rho_{\rm E}^2)\,|h_1|^2 \geqslant 0$. Therefore, $\Pr(C_s < R_s) \approx 1$. In practice, this scenario occurs when the average SNR at D is smaller than that at E. When $\bar{\gamma}_{\rm D} > \alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2$ (i.e., the average SNR at D is bigger than that at E) holds, we can have

$$\Pr(C_s < R_s) \approx \Pr\left(|h_0|^2 < \frac{\alpha-1+\alpha\bar{\gamma}_{\rm E}(1-\rho_{\rm E}^2)\,|h_1|^2}{\bar{\gamma}_{\rm D}-\alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2}\right). \tag{20}$$

Note that h_i $(i=0,1,2)$ is independent and identically distributed complex Gaussian random variable with zero-mean and unit variance, and $|h_i|^2$ is an exponential random variable with parameter of one. The probability density function (PDF) and cumulative distribution function (CDF) of $|h_i|^2$ can be expressed as [18]

$$f_{|h_i|^2}(x) = {\rm e}^{-x} \tag{21}$$

and

$$F_{|h_i|^2}(x) = 1-{\rm e}^{-x}, \tag{22}$$

respectively.

Using the probability theories in [18], we obtain

$$\Pr(C_s < R_s) \approx \int_0^\infty F_{|h_0|^2}\left(\frac{\alpha-1+\alpha\bar{\gamma}_{\rm E}(1-\rho_{\rm E}^2)x}{\bar{\gamma}_{\rm D}-\alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2}\right) f_{|h_1|^2}(x){\rm d}x. \tag{23}$$

Applying (21) and (22) into (23) and employing the integration, we can have the probability expression of $\Pr(C_s < R_s)$ as shown in (13).

The probability when the interference power is smaller than interference temperature limit is

$$\begin{aligned}\Pr(P_{\rm I} \leqslant \Gamma) &= \Pr\left(P_{\rm S}\left[\rho_{\rm P}^2\,|h_0|^2+2\rho_{\rm P}\sqrt{1-\rho_{\rm P}^2}(\Re[h_0]\Re[h_2]+\Im[h_0]\Im[h_2])+(1-\rho_{\rm P}^2)\,|h_2|^2\right]+\sigma_{\rm P}^2 \leqslant \Gamma\right)\\ &= \Pr\Big(P_{\rm S}[\rho_{\rm P}^2\,|h_0|^2+(1-\rho_{\rm P}^2)\,|h_2|^2]+\sigma_{\rm P}^2 \leqslant \Gamma-\\ &\qquad 2P_{\rm S}\rho_{\rm P}\sqrt{1-\rho_{\rm P}^2}(\Re[h_0]\Re[h_2]+\Im[h_0]\Im[h_2])\Big).\end{aligned} \tag{24}$$

To simplify the analysis, we can ignore the crossing terms of those two random variables when Γ is comparably large in (24) to yield an approximation expression as

$$\begin{aligned}\Pr(P_{\rm I}\leqslant\Gamma)&\approx\Pr\bigg(P_{\rm S}[\rho_{\rm P}^2\left|h_0\right|^2+(1-\rho_{\rm P}^2)\left|h_2\right|^2)]+\sigma_{\rm P}^2\leqslant\Gamma\bigg)\\&=\Pr\bigg(\left|h_0\right|^2\leqslant\frac{\Gamma-\sigma_{\rm P}^2}{P_{\rm S}\rho_{\rm P}^2}-\frac{(1-\rho_{\rm P}^2)\left|h_2\right|^2}{\rho_{\rm P}^2}\bigg)\\&=\int_0^\infty F_{|h_0|^2}\bigg(\frac{\Gamma-\sigma_{\rm P}^2}{P_{\rm S}\rho_{\rm P}^2}-\frac{(1-\rho_{\rm P}^2)x}{\rho_{\rm P}^2}\bigg)\times f_{|h_2|^2}(x){\rm d}x\end{aligned}\tag{25}$$

and more discussions on the validation of this approximation will be presented in Section 4.

Similarly, applying (21) and (22) into (25), the expression as shown in (14) can be obtained.

Finally, using the relationship of $\Pr(P_{\rm I}>\Gamma)=1-\Pr(P_{\rm I}\leqslant\Gamma)$, $\Pr(P_{\rm I}>\Gamma)$ is given as shown in (15). PNSC is defined as the probability that the secrecy rate for S-D link is positive. Thus, we can define PNSC as

$$\text{PNSC}=\Pr(C_s>0)\Pr(P_{\rm I}\leqslant\Gamma)=(1-\Pr(C_s<0))\Pr(P_{\rm I}\leqslant\Gamma).\tag{26}$$

By setting $R_s=0$ in (13), we can obtain

$$\Pr(C_s>0)=\begin{cases}\frac{\bar{\gamma}_{\rm D}-\bar{\gamma}_{\rm E}\rho_{\rm E}^2}{\bar{\gamma}_{\rm D}+\bar{\gamma}_{\rm E}(1-2\rho_{\rm E}^2)}, & \text{if } \bar{\gamma}_{\rm D}>\alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2,\\0, & \text{if } \bar{\gamma}_{\rm D}<\alpha\bar{\gamma}_{\rm E}\rho_{\rm E}^2.\end{cases}\tag{27}$$

4 Numerical results and discussion

In this section, both analytical and simulation results are presented to validate our analysis. The analytical results are obtained from (12), and Monte Carlo simulations are performed with 100000 independent trials to obtain the average results. In the simulation results, the generation of channel coefficients for the S-E and S-PU_rx channels (i.e., $h_{\rm S,E}$ and $h_{\rm S,P}$) are respectively obtained by using (4) and (8) without any approximations.

Figure 2 shows SOP versus the average SNR at D when $\bar{\gamma}_{\rm E}=-10$ dB, -5 dB and 0 dB. Note that the minimum value of Γ (i.e., $\Gamma/P_{\rm S}=8$ dB) used in Figure 2 is obtained through numerical searching by using the analytical expressions, and there will be no any changes for the SOP values if Γ is beyond that value. More details about the effect of Γ on the secrecy performance will be discussed later.

From Figure 2, it is observed that when $\bar{\gamma}_{\rm D}$ is in low-to-medium rigimes (i.e.,$\bar{\gamma}_{\rm D}<18$ dB), analytical results match simulation results quite well. On the other hand, when $\bar{\gamma}_{\rm D}$ increases, those two results mismatch with each other when $\Gamma/P_{\rm S}$ is comparably low. As $\Gamma/P_{\rm S}$ increasing, this mismatch is reduced, and those two results match with each other again when $\Gamma/P_{\rm S}=10$ dB as shown in Figure 2. This is because the two crossing terms, $2P_{\rm S}\rho_{\rm P}\sqrt{1-\rho_{\rm P}^2}(\Re[h_0]\Re[h_2]+\Im[h_0]\Im[h_2])$, are ignored when calculating $\Pr(P_{\rm I}<\Gamma)$ in (24). When $\bar{\gamma}_{\rm D}$ is comparably small, those two terms are insignificant in calculating results. When $\bar{\gamma}_{\rm D}$ increases, ignoring those terms is equivalent to increase the interference temperature limit Γ. Thus, analytical results are better than simulation results at a higher $\bar{\gamma}_{\rm D}$, as the value of equivalent interference temperature limit is different in calculating analytical and simulation results. However, simulation results represent the real SOP values. Therefore, we can conclude that our derived analytical SOP expressions are valid when interference temperature limit Γ is comparably large. In practical communications, low-to-medium SNR regimes are of interest. Therefore, a proper small value of Γ is enough.

Furthermore, we also observe that SOP decreases as $\bar{\gamma}_{\rm D}$ increases. It means that S-D link has a higher probability of successfully transmitting information in higher SNR regimes without being eavesdropped by E under certain $\bar{\gamma}_{\rm E}$ values. Moreover, higher $\bar{\gamma}_{\rm E}$ leads to worse SOP performance as eavesdropper has a higher chance to eavesdrop the information.

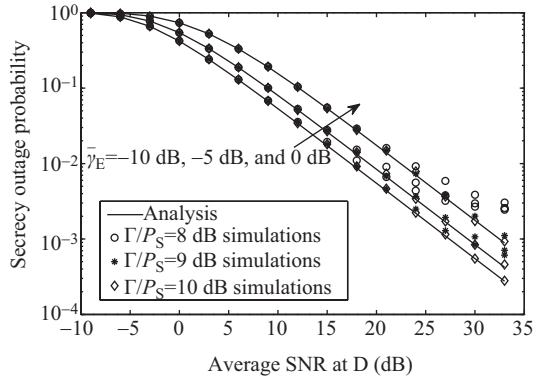

Figure 2 Secrecy outage probability versus average SNR at destination with $R_s = 0.5$ bits $\cdot$ s^{-1} $\cdot$ Hz^{-1}, $\rho_E = 0.2$, $\rho_P = 0.2$, $\bar{\gamma}_P = 20$ dB, and various Γ/P_S.

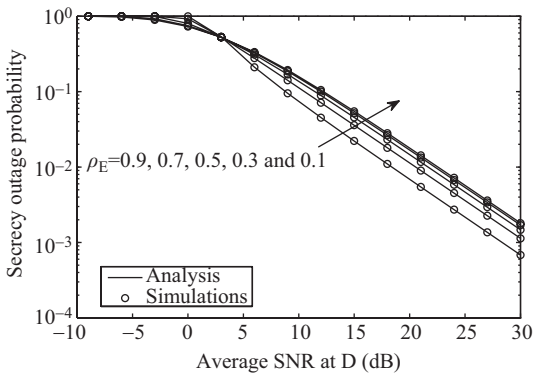

Figure 3 Secrecy outage probability versus average SNR at destination with $R_s = 0.5$ bits $\cdot$ s^{-1} $\cdot$ Hz^{-1}, $\bar{\gamma}_E = 0$ dB, $\rho_P = 0.2$, $\Gamma/P_S = 15$ dB, and $\bar{\gamma}_P = 20$ dB.

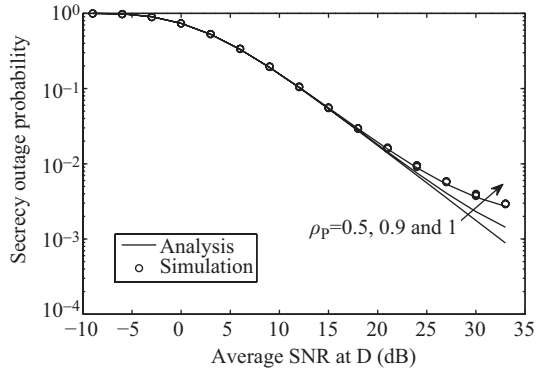

Figure 4 Secrecy outage probability versus average SNR at destination with $R_s = 0.5$ bits $\cdot$ s^{-1} $\cdot$ Hz^{-1}, $\bar{\gamma}_E = 0$ dB, $\rho_E = 0.2$, $\Gamma/P_S = 8$ dB, and $\bar{\gamma}_P = 20$ dB.

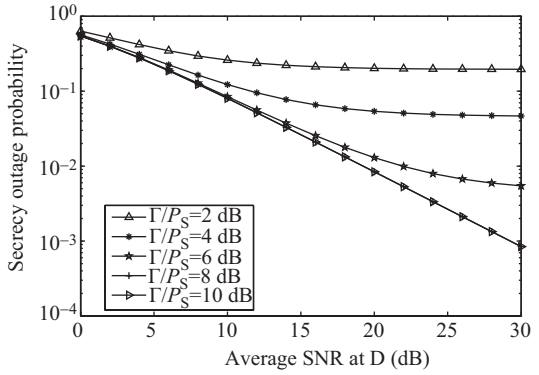

Figure 5 Secrecy outage probability versus average SNR at destination with $R_s = 0.5$ bits $\cdot$ s^{-1} $\cdot$ Hz^{-1}, $\bar{\gamma}_E = -5$ dB, $\rho_E = 0.2$, $\rho_P = 0.8$, and $\bar{\gamma}_P = 20$ dB.

Figure 3 shows SOP against $\bar{\gamma}_D$ from low to medium regimes for various ρ_E. As shown in Figure 3, a crossover of those curves is also observed. In the low $\bar{\gamma}_D$ regimes, i.e., $\bar{\gamma}_D < 3$ dB as shown in Figure 3, SOP degrades as the correlation coefficient ρ_E increases. This is because in this regime, the inequality $\bar{\gamma}_D < \alpha\bar{\gamma}_E\rho_E^2$ in (19) is more likely to hold with the increment of ρ_E. Thus, SOP will degrade and be more close to 1. When $\bar{\gamma}_D$ is in the medium-to-high regimes, the opposite behavior can be observed compared to that in low SNR regimes. This is due to the fact that in the medium-to-high SNR regimes, $\bar{\gamma}_D$ is greater than $\bar{\gamma}_E$, which makes $\bar{\gamma}_D - \alpha\bar{\gamma}_E\rho_E^2 \approx \bar{\gamma}_D$. Thus, $\alpha\bar{\gamma}_E(1-\rho_E^2)\left|h_1\right|^2$ decreases in (20), which leads to lower SOP values, as ρ_E increases.

SOP under various ρ_P is shown in Figure 4. One can easily see that a mismatch occurs when $\bar{\gamma}_D > 24$ dB in Figure 4. This is because when the signal power increases, the term, $2P_S\rho_P\sqrt{1-\rho_P^2}(\Re[h_0]\Re[h_2] + \Im[h_0]\Im[h_2])$, in (24) cannot be ignored compared to Γ, and an approximation error occurs when calculating the analytical results using that approximation. Furthermore, we also observe from simulation results that ρ_P has little effect on SOP.

Figure 5 shows SOP for various interference temperature limits, Γ. It is observed that SOP with a higher Γ outperforms the one with a lower Γ. This is because in CRNs, when Γ is high, P_I cannot easily exceed Γ. S can successfully use the same frequency bands of PU_rx to transmit its information with a higher probability. However, as depicted in Figure 5, there is an error floor for SOP. There exists a particular value of Γ under certain channel conditions, and SOP will not decrease when Γ is beyond that value. This particular value is equal to the maximum interference power at PU_rx under that conditions.

PNSC against $\bar{\gamma}_D$ for various $\bar{\gamma}_E$ is shown in Figure 6. It is noted that PNSC is improved when $\bar{\gamma}_D$

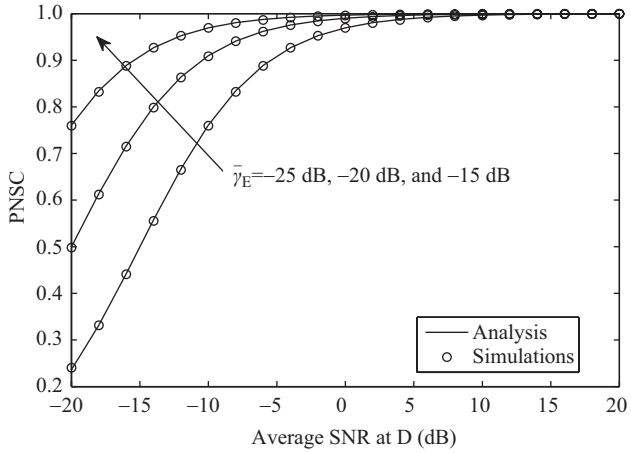

Figure 6 PNSC versus average SNR at destination with $\rho_E = 0.1$, $\rho_P = 0.2$, Γ/P_S, and $\bar{\gamma}_P = 10$ dB.

increases. This behavior is due to the fact that S-D link outperforms S-E link.

5 Conclusion

In this paper, the secrecy outage performance of underlay cognitive radio networks over correlated Rayleigh-fading channels has been studied. Tight closed-form expressions of secrecy outage probability and probability of non-zero secrecy capacity, which are valid when the interference temperature limit Γ is comparably large, have been derived. The derived SOP expressions can help designers to gain some insights from information-theoretic sense when designing secure systems. Our results shows that the correlation between the S-D and S-E channels acts as advantageous effect in the medium-to-high SNR regimes; while the correlation between the S-D and S-PU_rx channels has little effect on the secrecy outage performance. Our proposed analytical model can reveal the effects of system parameters on secrecy outage performance. In practical networks, our model can help the designers to design proper parameters in order to meet the criterion of secrecy performance. Moreover, our proposed model can also be applied to practical secrecy system design such as power control and transmission scheme.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grants Nos. 61401372, 61531016), Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20130182120017), Natural Science Foundation of CQ CSTC (Grant No. cstc2013jcyjA40040), and Fundamental Research Funds for the Central Universities (Grant Nos. XDJK2015B023, XDJK2016A011).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Wyner A. The wire-tap channel. Bell Syst Tech J, 1975, 5: 1355–1367
2 Liang Y B, Somekh-Baruch A, Poor H V, et al. Capacity of cognitive interference channels with and without secrecy. IEEE Trans Inf Theory, 2009, 55: 604–619
3 Liang Y B, Poor H V, Ying L. Secure communications over wireless broadcast networks: stability and utility maximization. IEEE Trans Inf Foren Secur, 2011, 6: 682–692
4 Bloch M, Barros J, Rodrigues M R D, et al. Wireless information-theoretic security. IEEE Trans Inf Theory, 2008, 54: 2515–2534
5 Wang H-M, Zheng T-X, Yuan J, et al. Physical layer security in heterogeneous cellular networks. IEEE Trans Commun, 2016, 64: 1204–1219
6 Wang H-M, Xia X-G. Enhancing wireless secrecy via cooperation: signal design and optimization. IEEE Commun Mag, 2015, 53: 47–53
7 Li Q, Song H, Huang K. Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels. IEEE Commun Lett, 2013, 17: 892–895

8 Bashar S, Ding Z, Xiao C. On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input. IEEE Commun Lett, 2011, 15: 527–529
9 Haykin S. Cognitive radio: brain-empowered wireless communications. IEEE J Sel Areas Commun, 2005, 23: 201–220
10 Hossain E, Bhargava V. Cognitive Wireless Communication Networks. New York: Springer, 2007
11 Sharma R K, Rawat D B. Advances on security thrats and countermeasures for cognitive radio networks: a survey. IEEE Commun Surv Tut, 2015, 57: 1023–1043
12 Zou Y, Zhu J, Yang L, et al. Securing physical-layer communications for cognitive radio networks. IEEE Commun Mag, 2015, 53: 48–54
13 Wang C, Wang H-M. On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels. IEEE Trans Inf Foren Secur, 2014, 9: 1814–1827
14 Mokari N, Parsaeefard S, Saeedi H, et al. Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users. IEEE Trans Wirel Commun, 2014, 13: 1058–1073
15 Alhakami W, Mansour A, Safdar G A, et al. A secure MAC protocol for cognitive radio networks (SMCRN). In: Proceedings of Science and Information Conference (SAI), London, 2013. 796–803
16 Tang C, Pan G, Li T. Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels. IEEE Wirel Commun Lett, 2014, 3: 609–612
17 Chen Y X, Tellambura C. Distribution functions of selection combiner output in equally correlated Rayleigh, Rician, and Nakagami-m fading channels. IEEE Trans Commun, 2004, 52: 1948–1956
18 Papoulis A, Pillai S U. Probability, Random Variables and Stochastic Processes. 4th ed. New York: McGraw-Hill, 2001