Frontiers of Information Technology & Electronic Engineering
www.zju.edu.cn/jzus; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Physical layer security of underlay cognitive radio using maximal ratio combining*#

Hui ZHAO[1], Dan-yang WANG[1], Chao-qing TANG[2], Ya-ping LIU[1],
Gao-feng PAN[†‡1], Ting-ting LI[3], Yun-fei CHEN[4]

([1]*School of Electronic and Information Engineering, Southwest University, Chongqing 400715, China*)
([2]*School of Electrical & Electronic Engineering, Newcastle University, Newcastle upon Tyne NE1 7RU, UK*)
([3]*School of Mathematics and Statistics, Southwest University, Chongqing 400715, China*)
([4]*School of Engineering, University of Warwick, Coventry CV4 7AL, UK*)
[†]E-mail: gfpan@swu.edu.cn

Received Oct. 21, 2015; Revision accepted Feb. 16, 2016; Crosschecked Aug. 16, 2016

Abstract: We investigate the secrecy outage performance of maximal ratio combining (MRC) in cognitive radio networks over Rayleigh fading channels. In a single-input multiple-output wiretap system, we consider a secondary user (SU-TX) that transmits confidential messages to another secondary user (SU-RX) equipped with M ($M \geq 1$) antennas where the MRC technique is adopted to improve its received signal-to-noise ratio. Meanwhile, an eavesdropper equipped with N ($N \geq 1$) antennas adopts the MRC scheme to overhear the information between SU-TX and SU-RX. SU-TX adopts the underlay strategy to guarantee the service quality of the primary user without spectrum sensing. We derive the closed-form expressions for an exact and asymptotic secrecy outage probability.

Key words: Cognitive radio networks, Maximal ratio combining, Secrecy outage probability, Single-input multiple-output

http://dx.doi.org/10.1631/FITEE.1500351 **CLC number:** TN929.5

1 Introduction

Cognitive radio (CR) is envisioned as a promising solution to the inadequacy of spectrum, which is one of the most important radio resources of wireless communications. In CR systems, the secondary user (SU) could occupy the spectrum without causing harmful interference on the primary user (PU) by the underlay strategy, which is easier to realize because SU adjusts only its transmitting power within a threshold that PU can tolerate (Lee *et al.*, 2011; Wang QH *et al.*, 2014).

Due to the broadcast nature of wireless links, it is difficult to prevent eavesdroppers (Eves) from overhearing wireless communications. Thus, security issues play an important role in wireless networks. Physical layer security has been widely considered as an effective technology to prevent information from being intercepted (Shiu *et al.*, 2011). In different fading scenarios, Sun *et al.* (2012), Zhang *et al.* (2014), and Pan *et al.* (2015) studied the secrecy performance over independent/correlated Rayleigh/log-normal/Rayleigh-log-normal fading channels. To gain secrecy diversity performance, both the maximal ratio combining (MRC) and selection combining (SC) have been used to improve the secrecy

‡ Corresponding author
* Project supported in part by the National Natural Science Foundation of China (Nos. 61401372 and 61531016), the Research Fund for the Doctoral Program of Higher Education of China (No. 20130182120017), the Natural Science Foundation of CQ CSTC (No. cstc2013jcyjA40040), and the Fundamental Research Funds for the Central Universities, China (No. XDJK2015B023)
# A preliminary version was presented at the 7th IEEE International Conference on Communication Software and Networks, China, June 6–7, 2015
ORCID: Gao-feng PAN, http://orcid.org/0000-0003-1008-5717

performance (He *et al.*, 2011; Alves *et al.*, 2012; Wang LF *et al.*, 2014; Zhao *et al.*, 2016). Moreover, Yang *et al.* (2013a) took both transmit antenna selection (TAS)/MRC and TAS/SC into account in multiple-input multiple-output (MIMO) wiretap channels, and derived exact and asymptotic closed-form expressions for the secrecy outage probability (SOP). Besides, the impact of antenna correlation on SOP in MIMO wiretap channels was analyzed by Yang *et al.* (2013b).

Security issues are especially important in CR networks (CRNs). The secrecy outage performance, over Nakagami-m fading channels, including SOP and the probability of non-zero secrecy capacity, was studied by Tang *et al.* (2014). Liu HQ *et al.* (2016) investigated the secrecy outage performance over log-normal fading channels in CRNs. In addition, a cooperation technique in CRNs was investigated by Zou *et al.* (2015), and both the intercept probability and outage probability of the proposed single-relay and multi-relay selection schemes for the secondary transmission relying on realistic spectrum sensing were analyzed. In cognitive decode-and-forward relay networks, several relay selection schemes were proposed, and two cognitive relays (one relay played a role of relay, while the other acted as a friendly jammer) were used to improve the secrecy outage performance (Liu *et al.*, 2015). Moreover, Liu YW *et al.* (2016) introduced and analyzed a power transfer model and secure information model of device-to-device communications in energy harvesting large-scale cognitive cellular networks to help the legal receiver enhance its received signal-to-noise ratio (SNR).

However, very little research has considered the secrecy performance of the single-input multiple-output (SIMO) system, which is one of the most effective technologies to improve the transmission rate in CRNs. Elkashlan *et al.* (2015) and Zhao *et al.* (2015) investigated the security of SIMO systems using MRC/SC in CRNs. However, Zhao *et al.* (2015) considered only the Eve equipped with a single antenna, while Elkashlan *et al.* (2015) considered only the SC technique. It is well-known that MRC performs better than SC. In addition, although the probability density function (PDF) of MRC is similar to that of Nakagami-m, Tang *et al.* (2014) considered only the imperfect CR scenario and did not deliver the asymptotic analysis in their investigation on secrecy outage performance.

We consider a SIMO spectrum sharing system where an SU transmits confidential messages to another SU equipped with M ($M \geq 1$) antennas, employing an MRC scheme to improve its received SNR. An Eve equipped with N ($N \geq 1$) antennas also adopts the MRC scheme to promote successful eavesdropping. The closed-form expressions of the exact and asymptotic SOP over Rayleigh fading channels are derived. Two main observations can be obtained from the simulation and numerical results:

1. SOP can be improved by increasing the number of the antennas at a secondary legitimate receiver (SU-RX). Meanwhile, increasing the number of the antennas at the Eve will degrade the secrecy outage performance.

2. SOP will remain constant in the high region of the interference threshold at PU, because in this case the secondary user (SU-TX) adopts only its maximum available power as its transmit power.

2 System model

We consider a SIMO wiretap channel in CRNs (Fig. 1). An SU-TX encodes its messages into the codeword $\boldsymbol{x} = [x(1), \cdots, x(l), \cdots, x(L)]$, where L is the number of elements of $\boldsymbol{x}$, and transmits $\boldsymbol{x}$ into an SU-RX equipped with M ($M \geq 1$) antennas and adopting MRC to improve its SNR, while an Eve equipped with N ($N \geq 1$) antennas also adopts MRC to overhear the information between SU-TX and SU-RX. $\boldsymbol{h}_M = [h_{M1}, h_{M2}, \cdots, h_{MM}]^{\mathrm{T}}$ and $\boldsymbol{h}_N = [h_{N1}, h_{N2}, \cdots, h_{NN}]^{\mathrm{T}}$ are the channel vectors of the SU-TX–SU-RX link and the SU-TX–Eve link, respectively.

In order not to degrade the quality of service (QoS) of PU, the transmit power at SU-TX (P_{t}) should be limited at a given threshold (I_P) that the PU can tolerate. Thus, P_{t} can be written as

$$P_{\mathrm{t}} = \begin{cases} I_P/g_P, & P_S \geq /g_P \Rightarrow g_P \geq I_P/P_S, \\ P_S, & P_S < I_P/g_P \Rightarrow g_P < I_P/P_S, \end{cases} \tag{1}$$

where $g_P = |h_p|^2$ is the channel power gain between SU-TX and PU, and P_S is the maximal transmit power at SU-TX.

We assume that all channels experience independent Rayleigh fading and additive white Gaussian noise with a variance of N_0. We also assume that full channel state information (CSI) is

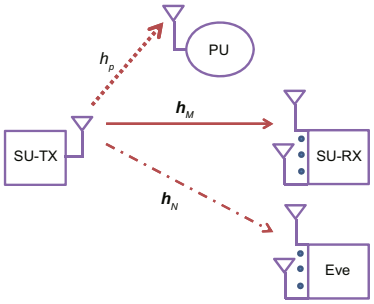

Fig. 1 System model (SU-TX: secondary user; SU-RX: secondary legitimate receiver; PU: primary user; Eve: eavesdropper)

available at SU-TX. If Eve keeps in silence and just listens, the channel gain of SU-TX–Eve ($h_{Nj} \in \boldsymbol{h}_N$, $j \in \{1, 2, \cdots, N\}$) is unavailable at SU-TX. The assumption, also given by Tang *et al.* (2014), that h_{Nj} is available at SU-TX, is to establish theoretical models to investigate the secrecy performance for every realization of h_{Nj}. Similarly, the assumption on the CSI from PU to SU-TX has been widely adopted in cognitive works (Elkashlan *et al.*, 2015) .

Thus, the PDF of the channel power between SU-TX and SU-RX can be given as

$$f_{|h_{Mk}|^2}(x) = \frac{1}{h_M} \exp\left(-\frac{x}{h_M}\right), \tag{2}$$

where h_M is the mean channel power gain for all channels between SU-TX and SU-RX, and $k \in \{1, 2, \cdots, M\}$.

Similarly, we have $|h_{Nj}|^2 \sim \exp(1/h_E)$ and $|h_p|^2 \sim \exp(1/h_P)$, where h_E and h_P are the mean channel power gains of the SU-TX–Eve link and the SU-TX–PU link, respectively.

Let $\lambda_E = 1/h_E$, $\lambda_P = 1/h_P$, and $\lambda_D = 1/h_M$. The PDFs of the combined channel powers of SU-RX and Eve are (He *et al.*, 2011)

$$f(g_q) = \frac{g_q^{i-1} \exp(-\lambda_q g_q) \lambda_q^i}{(i-1)!}, \quad g_q \geq 0, \tag{3}$$

where $(q, i) \in \{(D, M), (E, N)\}$ and $g_q = \|\boldsymbol{h}_i\|^2$.

The cumulative probability density function (CDF) of g_q can be given by

$$\begin{aligned} F(g_q) &= \int_0^{g_q} \frac{u^{i-1} \exp(-\lambda_q u) \lambda_q^i}{(i-1)!} \mathrm{d}u \\ &= 1 - \exp(-\lambda_q g_q) \sum_{v=0}^{i-1} \frac{\lambda_q^v g_q^v}{v!}. \end{aligned} \tag{4}$$

3 Secure outage analysis

The instantaneous secrecy capacity is (Elkashlan *et al.*, 2015)

$$C_S = \max\left\{\log_2\left(1+\frac{P_t g_D}{N_0}\right) - \log_2\left(1+\frac{P_t g_E}{N_0}\right), 0\right\}. \tag{5}$$

SOP is defined as the probability that the instantaneous secrecy capacity is below a target secrecy rate (C_{th}, $C_{\mathrm{th}} \geq 0$). Different from Elkashlan *et al.* (2015), we calculate the SOP under two cases of P_t as suggested by Eq. (1), by

$$\begin{aligned} \mathrm{SOP}(C_{\mathrm{th}}) = &\Pr\{g_P \geq I_P/P_S\} \mathrm{SOP}_1(C_{\mathrm{th}}) \\ &+ \Pr\{g_P < I_P/P_S\} \mathrm{SOP}_2(C_{\mathrm{th}}), \end{aligned} \tag{6}$$

where $\mathrm{SOP}_1(C_{\mathrm{th}})$ and $\mathrm{SOP}_2(C_{\mathrm{th}})$ refer to the SOP when $P_t = I_P/g_P$ and $P_t = P_S$, respectively.

The above method has also been adopted by Liu HQ *et al.* (2016), and it has been verified that this method is easier than that of Elkashlan *et al.* (2015). However, Liu HQ *et al.* (2016) did not perform asymptotic analysis on SOP, which is one of the most important indicators in physical layer security (Wang LF *et al.*, 2014; Elkashlan *et al.*, 2015).

Since $g_P = |h_p|^2 \sim \exp(1/h_P)$, the items $\Pr\{g_P \geq I_P/P_S\}$ and $\Pr\{g_P < I_P/P_S\}$ in Eq. (6) can be easily obtained as

$$\Pr\{g_P \geq I_P/P_S\} = \exp\left(-\frac{\lambda_P I_P}{P_S}\right), \tag{7}$$

$$\Pr\{g_P < I_P/P_S\} = 1 - \exp\left(-\frac{\lambda_P I_P}{P_S}\right). \tag{8}$$

3.1 Derivation of SOP_1

When $P_t = I_P/g_P$, we can write $\mathrm{SOP}_1(C_{\mathrm{th}})$ as (Tang *et al.*, 2014)

$$\begin{aligned} &\Pr\{C_S \leq C_{\mathrm{th}}\} \\ &= \Pr\left\{\log_2\left(1+\rho\frac{g_D}{g_P}\right) - \log_2\left(1+\rho\frac{g_E}{g_P}\right) \leq C_{\mathrm{th}}\right\} \\ &= \Pr\left\{\frac{1+\rho g_D/g_P}{1+\rho g_E/g_P} \leq 2^{C_{\mathrm{th}}}\right\} \\ &= \Pr\left\{\frac{\alpha-1}{\rho} g_P \geq g_D - \alpha g_E\right\}, \end{aligned} \tag{9}$$

where $\alpha = 2^{C_{\mathrm{th}}}$ and $\rho = I_P/N_0$.

Let $Z_1 = \dfrac{\alpha-1}{\rho} g_P$, $Z_2 = g_D - \alpha g_E$, and $X =$

αg_E. The PDFs of X and Z_1 can be derived as

$$f_X(x) = \frac{x^{N-1}\exp(-\lambda_E x/\alpha)\lambda_E^N}{\alpha^N (N-1)!}, \quad (10)$$

$$f_{Z_1}(z_1) = \frac{A\rho\lambda_P}{\alpha-1}\exp\left(-\frac{\rho\lambda_P z_1}{\alpha-1}\right), \quad (11)$$

$$z_1 \geq \frac{(\alpha-1)N_0}{P_S} = B,$$

where $A = 1/\exp(-\lambda_P I_P/P_S)$. In this case, $g_P \geq I_P/P_S$. The PDF of g_P can be obtained by $f_{g_P}(x) = A\lambda_P \exp(-\lambda_P x)$.

We can rewrite Eq. (9) as

$$\begin{aligned}
&\mathrm{SOP}_1(C_{\mathrm{th}}) \\
&= \int_B^{\infty} f_{Z_1}(z_1) \int_{-\infty}^{z_1} f_{Z_2}(z_2)\,\mathrm{d}z_2\mathrm{d}z_1 \\
&= \underbrace{\int_B^{\infty} f_{Z_1}(z_1) \int_{-\infty}^{0} f_{Z_2}(z_2)\,\mathrm{d}z_2\mathrm{d}z_1}_{I_1} \\
&\quad + \underbrace{\int_B^{\infty} f_{Z_1}(z_1) \int_{0}^{z_1} f_{Z_2}(z_2)\,\mathrm{d}z_2\mathrm{d}z_1}_{I_2}. \quad (12)
\end{aligned}$$

3.1.1 Derivation of I_1

By using the distribution function proposed by Papoulis *et al.* (2002), we can derive the PDF of Z_2 as (to simplify the analysis, we do not need to calculate the PDF of $Z_2 < 0$ directly)

$$f_{Z_2}(z_2) = \int_0^{\infty} f_{g_D}(z_2 + x) f_X(x)\,\mathrm{d}x. \quad (13)$$

Considering the derivation presented in Appendix A, we have

$$\begin{aligned}
f_{Z_2}(z_2) =& \Phi \sum_{k=0}^{M-1} \binom{M-1}{k} \frac{\Gamma(N+k)}{(\lambda_D + \lambda_E/\alpha)^{N+k}} \\
&\cdot z_2^{M-k-1} \exp(-\lambda_D z_2), \quad (14)
\end{aligned}$$

where $\Phi = \dfrac{\lambda_D^M \lambda_E^N}{\alpha^N (M-1)!\,(N-1)!}$ and $\Gamma(\cdot)$ is Gamma function (Gradshteyn *et al.*, 2007).

The CDF of Z_2 can be given by

$$\begin{aligned}
F_{Z_2}(z_2) &= \Phi \sum_{k=0}^{M-1} \binom{M-1}{k} \frac{\Gamma(N+k)}{(\lambda_D + \lambda_E/\alpha)^{N+k}} \\
&\quad \cdot \int_0^{z_2} u^{M-k-1} \exp(-\lambda_D u)\,\mathrm{d}u \\
&= \Phi \sum_{k=0}^{M-1} \binom{M-1}{k} \frac{\Gamma(N+k)}{(\lambda_D + \lambda_E/\alpha)^{N+k}} \\
&\quad \cdot \lambda_D^{k-M} \gamma(M-k, \lambda_D z_2), \quad (15)
\end{aligned}$$

where $\gamma(n,x) = \int_0^x \exp(-t)t^{n-1}\mathrm{d}t$ is the lower incomplete Gamma function (Gradshteyn *et al.*, 2007).

To facilitate the analysis, we define an integral, I_3, as follows:

$$\begin{aligned}
I_3 &= \int_0^{\infty} f_{Z_2}(z_2)\,\mathrm{d}z_2 = \Phi \sum_{k=0}^{M-1} \binom{M-1}{k} \\
&\quad \cdot \frac{\Gamma(N+k)}{(\lambda_D + \lambda_E/\alpha)^{N+k}} \frac{\Gamma(M-k)}{\lambda_D^{M-k}}. \quad (16)
\end{aligned}$$

For $Z_1 \in [B, +\infty)$, it is easy to observe that

$$I_1 = \int_B^{\infty} f_{Z_1}(z_1) \cdot (1 - I_3)\,\mathrm{d}z_1 = 1 - I_3. \quad (17)$$

3.1.2 Derivation of I_2

I_2 can be written as

$$\begin{aligned}
I_2 &= \int_B^{\infty} f_{Z_1}(z_1) \cdot F_{Z_2}(z_1)\mathrm{d}z_1 \\
&= \Phi \sum_{k=0}^{M-1} \binom{M-1}{k} \frac{\Gamma(N+k)}{(\lambda_D + \lambda_E/\alpha)^{N+k}} \lambda_D^{k-M} \\
&\quad \cdot \int_B^{\infty} f_{Z_1}(z_1)\,\gamma(M-k, \lambda_D z_1)\,\mathrm{d}z_1. \quad (18)
\end{aligned}$$

Considering the integral equation Q given in Appendix B, we derive I_2 as

$$\begin{aligned}
I_2 &= \Phi \sum_{k=0}^{M-1} \binom{M-1}{k} \\
&\quad \cdot \frac{\Gamma(N+k)}{(\lambda_D + \lambda_E/\alpha)^{N+k}} \cdot (M-k-1)! \\
&\quad \cdot \left\{ 1 - \sum_{n=0}^{M-k-1} \frac{\lambda_D^n}{n!} \frac{A\rho\lambda_P}{\alpha-1} \frac{\Gamma(n+1, \Lambda B)}{\Lambda^{n+1}} \right\}, \quad (19)
\end{aligned}$$

where $\Gamma(n,x) = \int_x^{\infty} \exp(-t)t^{n-1}\mathrm{d}t$ is the upper incomplete Gamma function (Gradshteyn *et al.*, 2007).

Finally, we can obtain SOP_1 as

$$\mathrm{SOP}_1(C_{\mathrm{th}}) = 1 - I_3 + I_2. \quad (20)$$

3.2 Derivation of SOP_2

When $g_P < I_P/P_S$, $P_{\mathrm{t}} = P_S$. It means that SU-TX adopts only its maximal transmitting power to deliver information to SU-RX. Obviously, the target system model falls into a non-CR model in this case.

Substituting $\overline{\gamma}_M = P_S h_M/N_0$ and $\overline{\gamma}_W = P_S h_E/N_0$ into the closed-form expression of SOP presented by He *et al.* (2011), we can calculate $\mathrm{SOP}_2(C_{\mathrm{th}})$ as Eq. (21) (see the next page).

$$\mathrm{SOP}_2\left(C_{\mathrm{th}}\right)=\sum_{k=0}^{N-1}\left(\begin{array}{c}M+k-1\\k\end{array}\right)\frac{\overline{\gamma}_M^k\overline{\gamma}_W^M}{\left(\overline{\gamma}_M+\overline{\gamma}_W\right)^{M+k}}+\sum_{k=0}^{M-1}\left(\begin{array}{c}N+k-1\\k\end{array}\right)\frac{\overline{\gamma}_W^k\overline{\gamma}_M^N}{\left(\overline{\gamma}_M+\overline{\gamma}_W\right)^{N+k}}$$
$$-\frac{\exp\left[-(\alpha-1)/\overline{\gamma}_M\right]}{(N-1)!}\cdot\sum_{k=0}^{M-1}\sum_{n=0}^{k}\frac{\left(\begin{array}{c}k\\n\end{array}\right)\alpha^n(\alpha-1)^{k-n}\left(N+n-1\right)!\,\overline{\gamma}_W^n}{k!\,\overline{\gamma}_M^{k-N-n}\left(\overline{\gamma}_M+\alpha\overline{\gamma}_W\right)^{N+n}}. \tag{21}$$

Finally, SOP can be obtained by substituting Eqs. (7), (8), (20), and (21) into Eq. (6). This expression serves as a prerequisite for other secrecy metrics, such as the probability of non-zero secrecy capacity (PNSC), calculated as

$$\mathrm{PNSC}=\Pr(C_S>0)=1-\mathrm{SOP}(C_{\mathrm{th}}=0). \tag{22}$$

In addition, our SOP expression without the interference power constraint reduces to the SOP expression presented by He *et al.* (2011) in Rayleigh fading.

4 Asymptotic secrecy outage probability

In this section, we derive a new asymptotic expression for the SOP at high SNR operating regions. The aim is to derive two important indicators in physical layer security: the secrecy diversity order and the secrecy array gain (Wang LF *et al.*, 2014; Elkashlan *et al.*, 2015).

By applying the Taylor series expansion truncated to the first order in CDF of g_D, we can derive the first-order expansion as (given by the equation of the first-order expansion of PDF presented by Wang LF *et al.* (2014))

$$\begin{aligned}F_{g_D}\left(g_D\right)&=1-\exp\left(-\lambda_D g_D\right)\sum_{v=0}^{M-1}\frac{\lambda_D^v g_D^v}{v!}\\&=1-\left(1-\lambda_D g_D\right)\\&\quad\cdot\left[\exp\left(\lambda_D g_D\right)-\frac{\left(\lambda_D g_D\right)^M}{M!}-o\left(\lambda_D^M\right)\right]\\&=\frac{\left(\lambda_D g_D\right)^M}{M!}+o\left(\lambda_D^M\right),\\&\lambda_D\to 0,\end{aligned} \tag{23}$$

where $o(\cdot)$ denotes the higher-order terms, and $\lambda_D\to 0$ is namely the $\overline{\gamma}_1=\dfrac{P_S}{N_0\lambda_D}\to\infty$ (Elkashlan *et al.*, 2015).

4.1 Derivation of the asymptotic SOP_1^{∞}

Eq. (9) can be rewritten as

$$\mathrm{SOP}_1=\Pr\left\{\frac{\alpha-1}{\rho}g_P+\alpha g_E\geq g_D\right\}. \tag{24}$$

Let $Z_3=\dfrac{\alpha-1}{\rho}g_P+\alpha g_E$. We can derive the PDF of Z_3 as Eq. (25) (see the next page), where $Q_1(\cdot,\cdot,\cdot)$ is defined as (given by Eq. (1.3.2.6) presented by Prudnikov *et al.* (1986))

$$\begin{aligned}Q_1\left(n,a,x\right)&=\int x^n\exp\left(ax\right)\mathrm{d}x=\exp\left(ax\right)\\&\cdot\left[\frac{x^n}{a}+\sum_{p=1}^{n}(-1)^p\frac{n\left(n-1\right)\cdots\left(n-p+1\right)}{a^{p+1}}x^{n-p}\right].\end{aligned} \tag{26}$$

Considering Eq. (23), we can rewrite the asymptotic SOP_1^{∞} as

$$\begin{aligned}\mathrm{SOP}_1^{\infty}&=\int_B^{\infty}f_{Z_3}\left(z_3\right)\int_0^{z_3}f_{g_D}\left(g_D\right)\mathrm{d}g_D\mathrm{d}z_3\\&=\frac{\lambda_D^M}{M!}\int_B^{\infty}f_{Z_3}\left(z_3\right)z_3^M\mathrm{d}z_3+o\left(\lambda_D^M\right).\end{aligned} \tag{27}$$

Substituting the PDF of Z_3 into Eq. (27), we have Eq. (28) (see the next page).

We consider the integral Eq. (29), as shown on the next page.

Substituting $Q_1(\cdot,\cdot,\cdot)$ into Q_2, we can derive Eq. (30), as shown on the next page, where $a=-\left(\dfrac{\rho\lambda_P}{\alpha-1}-\dfrac{\lambda_E}{\alpha}\right)$.

Using Eq.(3.351.2) presented by Gradshteyn *et al.* (2007), we can derive Q_2 as Eq. (31), as shown on the next page.

Considering the closed-form expression of Q_2, we can derive the closed-form expression of the asymptotic SOP_1^{∞} as

$$\mathrm{SOP}_1^{\infty}=\left(G_{a1}\cdot\lambda_D\right)^M+o\left(\lambda_D^M\right), \tag{32}$$

$$
\begin{aligned}
f_{Z_3}(z_3) &= \int_B^{z_3} f_{Z_1}(x) f_X(z_3 - x)\,\mathrm{d}x \\
&= \frac{A\rho\lambda_P\lambda_E^N}{(\alpha-1)\alpha^N(N-1)!}\exp\left(-\frac{\lambda_E}{\alpha}z_3\right)\int_B^{z_3}(z_3-x)^{N-1}\exp\left[-\left(\frac{\rho\lambda_P}{\alpha-1}-\frac{\lambda_E}{\alpha}\right)x\right]\mathrm{d}x \\
&= \frac{A\rho\lambda_P\lambda_E^N}{(\alpha-1)\alpha^N(N-1)!}\sum_{q=0}^{N-1}\binom{N-1}{q}(-1)^{N-q-1}\left[Q_1\left(N-q-1,-\left(\frac{\rho\lambda_P}{\alpha-1}-\frac{\lambda_E}{\alpha}\right),z_3\right)\right. \\
&\quad \left. - Q_1\left(N-q-1,-\left(\frac{\rho\lambda_P}{\alpha-1}-\frac{\lambda_E}{\alpha}\right),B\right)\right] z_3^q\exp\left(-\frac{\lambda_E}{\alpha}z_3\right). \qquad (25)
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{SOP}_1^{\infty} &= \frac{A\rho\lambda_P\lambda_E^N\lambda_D^M}{(\alpha-1)\alpha^N M!(N-1)!}\sum_{q=0}^{N-1}\binom{N-1}{q}(-1)^{N-q-1}\left\{\int_B^{\infty}Q_1\left(N-q-1,-\left(\frac{\rho\lambda_P}{\alpha-1}-\frac{\lambda_E}{\alpha}\right),z_3\right)\right. \\
&\left.\cdot z_3^{M+q}\exp\left(-\frac{\lambda_E}{\alpha}z_3\right)\mathrm{d}z_3 - Q_1\left(N-q-1,-\left(\frac{\rho\lambda_P}{\alpha-1}-\frac{\lambda_E}{\alpha}\right),B\right)\int_B^{\infty}z_3^{M+q}\exp\left(-\frac{\lambda_E}{\alpha}z_3\right)\mathrm{d}z_3\right\} + o\left(\lambda_D^M\right). \qquad (28)
\end{aligned}
$$

$$
Q_2 = \int_B^{\infty}Q_1\left(N-q-1,-\left(\frac{\rho\lambda_P}{\alpha-1}-\frac{\lambda_E}{\alpha}\right),z_3\right)\cdot z_3^{q+M}\cdot\exp\left(-\frac{\lambda_E}{\alpha}z_3\right)\mathrm{d}z_3. \qquad (29)
$$

$$
\begin{aligned}
Q_2 &= \int_B^{\infty} z_3^{q+M}\exp\left(-\frac{\rho\lambda_P}{\alpha-1}z_3\right) \\
&\quad\cdot\left[\frac{z_3^{N-q-1}}{a}+\sum_{p=1}^{N-q-1}(-1)^p\frac{(N-q-1)(N-q-2)\cdots(N-q-p)}{a^{p+1}}z_3^{N-q-p-1}\right]\mathrm{d}z_3. \qquad (30)
\end{aligned}
$$

$$
\begin{aligned}
Q_2 &= \frac{1}{a}\left(\frac{\alpha-1}{\rho\lambda_P}\right)^{N+M}\Gamma\left(N+M,\frac{\rho\lambda_P}{\alpha-1}B\right)+\sum_{p=1}^{N-q-1}(-1)^p\frac{(N-q-1)(N-q-2)\cdots(N-q-p)}{a^{p+1}} \\
&\quad\cdot\left(\frac{\alpha-1}{\rho\lambda_P}\right)^{N+M-p}\Gamma\left(N+M-p,\frac{\rho\lambda_P}{\alpha-1}B\right). \qquad (31)
\end{aligned}
$$

$$
G_{a1} = \left\{\Theta\sum_{q=0}^{N-1}\binom{N-1}{q}(-1)^{N-q-1}\left[Q_2 - Q_1(N-q-1,a,B)\,\Gamma\left(M+q+1,\frac{\lambda_E}{\alpha}B\right)\left(\frac{\alpha}{\lambda_E}\right)^{M+q+1}\right]\right\}^{1/M}. \qquad (33)
$$

where G_{a1} is defined as Eq. (33), as shown on the previous page, in which $\Theta = \dfrac{A\rho\lambda_P\lambda_E^N}{(\alpha-1)\,\alpha^N M!\,(N-1)!}$.

4.2 Derivation of the asymptotic SOP_2^∞

Using the asymptotic SOP expression presented by Wang LF *et al.* (2014), we have the asymptotic SOP_2^∞ as

$$\mathrm{SOP}_2^\infty = (G_{a2}\cdot\lambda_D)^M + o\left(\lambda_D^M\right), \tag{34}$$

where G_{a2} is defined as

$$G_{a2} = \left[\sum_{i=0}^{M}\binom{M}{i}\frac{\alpha^i(\alpha-1)^{M-i}P_S^i\Gamma(N+i)}{M!\lambda_E^i N_0^i\Gamma(N)}\cdot\left(\frac{N_0}{P_S}\right)^M\right]^{1/M}. \tag{35}$$

Considering the closed-form expressions of SOP_1^∞ and SOP_2^∞, we can rewrite the asymptotic SOP^∞ as

$$\begin{aligned}\mathrm{SOP}^\infty &= \Pr\{g_P \ge I_P/P_S\}\mathrm{SOP}_1^\infty \\ &\quad + \Pr\{g_P < I_P/P_S\}\mathrm{SOP}_2^\infty \\ &= (G_a\cdot\lambda_D)^M + o\left(\lambda_D^M\right),\end{aligned} \tag{36}$$

where G_a is defined as

$$G_a = \left\{G_{a1}^M\cdot\exp\left(-\frac{\lambda_P I_P}{P_S}\right) + G_{a2}^M\cdot\left[1-\exp\left(-\frac{\lambda_P I_P}{P_S}\right)\right]\right\}^{1/M}. \tag{37}$$

It is obvious that the secrecy diversity order is M, and the secrecy array gain is G_a^{-1}. These two indicators determine the slope and characterize the channel power gain advantage of the asymptotic SOP relative to the reference curve λ_D^M.

5 Numerical results and discussion

Fig. 2 plots SOP versus I_P for various λ_E and (M,N) combinations. Obviously, SOP can be improved by increasing M, which also means increasing the MRC diversity gain at SU-RX. Meanwhile, SOP becomes worse as N increases, and as it increases the MRC diversity gain at Eve. The SOP with a higher λ_E outperforms that with a lower λ_E in various (M,N) combinations. It is because that a higher λ_E represents a worse SU-TX–Eve link, which increases the outage probability. We can see that SOP degrades while I_P increases, due to the relaxed peak interference transmit power at the PU, which increases the transmitting power (P_t) at SU-TX in turn. Further, we can find that, there exists a floor for SOP in the high I_P region. It is because $P_\mathrm{t} = P_S$ when $I_P \to \infty$, in which case the transmitting SNR remains constant.

In Fig. 3, it is obvious that our asymptotic curves accurately predict the secrecy diversity order and the secrecy diversity gain at a high ω region, namely at a high $\overline{\gamma}_1 = \dfrac{P_S}{\lambda_D N_0}$ region. SOP can be improved when ω increases, which means that SU-TX–SU-RX links become better compared to SU-TX–Eve links. It is also worth noting that N does not have any impact on the diversity order which is affected only by M, while N can generate an effect on the secrecy array gain.

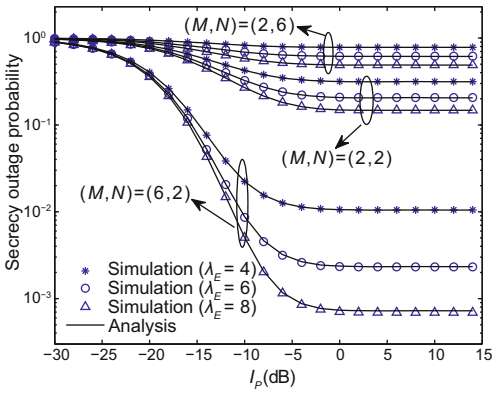

Fig. 2 Secrecy outage probability versus I_P for $\lambda_D=2$, $\lambda_P=3$, $N_0=1$, $P_S=1$ dB, and $C_\mathrm{th}=0.1$ bit/(s·Hz)

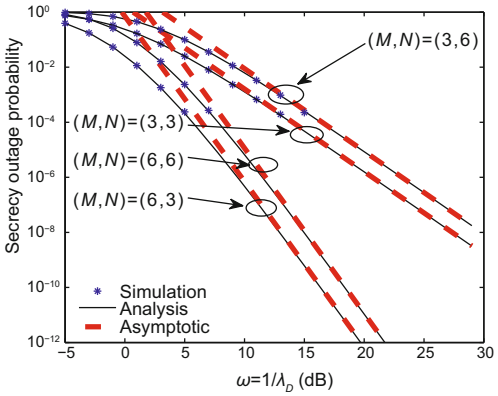

Fig. 3 Secrecy outage probability versus $\omega=1/\lambda_D$ for $\lambda_P=3$, $\lambda_E=2$, $I_P=1$ dB, $P_S=3$ dB, $N_0=1$, and $C_\mathrm{th}=0.1$ bit/(s·Hz)

Moreover, obviously, simulation and analytical results match very well in both figures.

6 Conclusions

In this paper, we have investigated the secrecy outage performance of the SIMO wiretap model in CRNs over independent Rayleigh fading channels. The closed-form expressions for the exact and asymptotic SOP have been derived and verified via simulations.

References

Alves, H., Souza, R.D., Debbah, M., *et al.*, 2012. Performance of transmit antenna selection physical layer security schemes. *IEEE Signal Process. Lett.*, **19**(6):372-375. http://dx.doi.org/10.1109/LSP.2012.2195490

Elkashlan, M., Wang, L., Duong, T.Q., *et al.*, 2015. On the security of cognitive radio networks. *IEEE Trans. Veh. Technol.*, **64**(8):3790-3795. http://dx.doi.org/10.1109/TVT.2014.2358624

Gradshteyn, I.S., Ryzhik, I.M., 2007. Table of Integrals, Series, and Products. Academic Press, New York.

He, F.M., Man, H., Wang, W., 2011. Maximal ratio diversity combining enhanced security. *IEEE Commun. Lett.*, **15**(5):509-511. http://dx.doi.org/10.1109/LCOMM.2011.030911.102343

Lee, J., Wang, H., Andrews, J.G., *et al.*, 2011. Outage probability of cognitive relay networks with interference constraints. *IEEE Trans. Wirel. Commun.*, **10**(2):390-395. http://dx.doi.org/10.1109/TWC.2010.120310.090852

Liu, H.Q., Zhao, H., Jiang, H., *et al.*, 2016. Physical-layer secrecy outage of spectrum sharing CR systems over fading channels. *Sci. China Inform. Sci.*, in press. http://dx.doi.org/10.1007/s11432-015-5451-2

Liu, Y.W., Wang, L.F., Duy, T.T., *et al.*, 2015. Relay selection for security enhancement in cognitive relay networks. *IEEE Wirel. Commun. Lett.*, **4**(1):46-49. http://dx.doi.org/10.1109/LWC.2014.2365808

Liu, Y.W., Wang, L.F., Zaidi, S.A.R., *et al.*, 2016. Secure D2D communication in large-scale cognitive cellular networks: a wireless power transfer model. *IEEE Trans. Commun.*, **64**(1):329-342. http://dx.doi.org/10.1109/TCOMM.2015.2498171

Pan, G.F., Tang, C.Q., Zhang, X., *et al.*, 2015. Physical layer security over non-small scale fading channels. *IEEE Trans. Veh. Techol.*, **65**(3):1326-1339. http://dx.doi.org/10.1109/TVT.2015.2412140

Papoulis, A., Pillai, S.U., 2002. Two Random Variables. *In*: Howell, R.L., Morriss, J.M. (Eds.), Probability, Random Variables and Stochastic Processes. Tata McGraw-Hill Education, Noida, p.124-148.

Prudnikov, A.P., Brychkov, Y.A., Marichev, O.I., 1986. Elementary Functions. *In*: Queen, N.M., translator, Integrals and Series. Gordon and Breach Science Publishers, Philadelphia, p.11-45.

Shiu, Y.S., Chang, S.Y., Wu, H.C., *et al.*, 2011. Physical layer security in wireless networks: a tutorial. *IEEE Wirel. Commun.*, **18**(2):66-74. http://dx.doi.org/10.1109/MWC.2011.5751298

Sun, X.J., Wang, J.H., Xu, W., *et al.*, 2012. Performance of secure communications over correlated fading channels. *IEEE Signal Process. Lett.*, **19**(8):479-482. http://dx.doi.org/10.1109/LSP.2012.2203302

Tang, C.Q., Pan, G.F., Li, T.T., 2014. Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels. *IEEE Wirel. Commun. Lett.*, **3**(6):609-612. http://dx.doi.org/10.1109/LWC.2014.2350501

Wang, L.F., Yang, N., Elkashlan, M., *et al.*, 2014. Physical layer security of maximal ratio combining in two-wave diffuse power fading channels. *IEEE Trans. Inform. Foren. Sec.*, **9**(2):247-258. http://dx.doi.org/10.1109/TIFS.2013.2296991

Wang, Q.H., Wang, H.M., Yin, Q.Y., 2014. Distributed beamforming for multi-relay cognitive radio systems. *Sci. China Inform. Sci.*, **44**(8):980-992 (in Chinese). http://dx.doi.org/10.1360/N112013-00174

Yang, N., Suraweera, H.A., Collings, I.B., *et al.*, 2013a. Physical layer security of TAS/MRC with antenna correlation. *IEEE Trans. Inform. Foren. Sec.*, **8**(1):254-259. http://dx.doi.org/10.1109/TIFS.2012.2223681

Yang, N., Yeoh, P.L., Elkashlan, M., *et al.*, 2013b. Transmit antenna selection for security enhancement in MIMO wiretap channels. *IEEE Trans. Commun.*, **61**(1):144-154. http://dx.doi.org/10.1109/TCOMM.2012.12.110670

Zhang, X., Pan, G.F., Tang, C.Q., *et al.*, 2014. Performance analysis of physical layer security over independent/correlated log-normal fading channels. IEEE Telecommunication Networks and Applications Conf., p.23-27. http://dx.doi.org/10.1109/ATNAC.2014.7020868

Zhao, H., Pan, G.F., 2016. The analysis on secure communications for DF and RF relaying SIMO system with Gauss errors. *Sci. China Inform. Sci.*, **46**(3):350-360 (in Chinese).

Zhao, H., Liu, H.Q., Liu, Y.P., *et al.*, 2015. Physical layer security of maximal ratio combining in underlay cognitive radio unit over Rayleigh fading channels. IEEE Int. Conf. on Communication Software and Networks, p.201-205. http://dx.doi.org/10.1109/ICCSN.2015.7296154

Zou, Y.L., Champagne, B., Zhu, W.P., *et al.*, 2015. Relay-selection improves the security-reliability trade-off in cognitive radio systems. *IEEE Trans. Commun.*, **63**(1):215-228. http://dx.doi.org/10.1109/TCOMM.2014.2377239

Appendix A: Derivation of Eq. (14)

Substituting the PDFs of g_D and X into Eq. (13), we can derive Eq. (A1), as shown on the next page. Expanding $(\cdot)^{M-1}$ in Eq. (A1) by applying the finite sum function of power series presented

$$f_{Z_2}(z_2)=\int_0^{\infty}\frac{(z_2+x)^{M-1}\exp(-\lambda_D(z_2+x))\lambda_D^M}{(M-1)!}\cdot\frac{x^{N-1}\exp(-\lambda_E x/\alpha)\lambda_E^N}{\alpha^N(N-1)!}\mathrm{d}x$$
$$=\frac{\lambda_D^M\lambda_E^N}{\alpha^N(N-1)!(M-1)!}\exp(-\lambda_D z_2)\int_0^{\infty}(z_2+x)^{M-1}x^{N-1}\exp\left[-\left(\lambda_D+\frac{\lambda_E}{\alpha}\right)x\right]\mathrm{d}x. \quad \text{(A1)}$$

$$Q=(M-k-1)!\left\{\int_B^{\infty}f_{Z_1}(z_1)\,\mathrm{d}z_1-\sum_{n=0}^{M-k-1}\frac{\lambda_D^n}{n!}\int_B^{\infty}f_{Z_1}(z_1)\cdot z_1^n\exp(-\lambda_D z_1)\,\mathrm{d}z_1\right\}$$
$$=(M-k-1)!\left\{1-\sum_{n=0}^{M-k-1}\frac{\lambda_D^n}{n!}\frac{A\rho\lambda_P}{\alpha-1}\int_B^{\infty}z_1^n\exp\left[-\left(\lambda_D+\frac{\rho\lambda_P}{\alpha-1}\right)z_1\right]\mathrm{d}z_1\right\}. \quad \text{(B3)}$$

by Gradshteyn *et al.* (2007) for binomial expansion, we have

$$f_{Z_2}(z_2)=\frac{\lambda_D^M\lambda_E^N}{\alpha^N(N-1)!(M-1)!}\exp(-\lambda_D z_2)\cdot\sum_{k=0}^{M-1}\binom{M-1}{k}\cdot z_2^{M-k-1}\cdot\int_0^{\infty}x^{N+k-1}\exp\left[-\left(\lambda_D+\frac{\lambda_E}{\alpha}\right)x\right]\mathrm{d}x. \quad \text{(A2)}$$

By using the Gamma function presented by Gradshteyn *et al.* (2007), we can derive the PDF of Z_2 as Eq. (14).

Appendix B: Derivation of the integral equation Q

We consider the following integral equation:

$$Q=\int_B^{\infty}f_{Z_1}(z_1)\cdot\gamma(M-k,\lambda_D z_1)\,\mathrm{d}z_1. \quad \text{(B1)}$$

Expending $\gamma(\cdot,\cdot)$ in Eq. (18) into the form of series, we have (given by Eq. (8.352.6) presented by Gradshteyn *et al.* (2007))

$$\gamma(M-k,\lambda_D z_1)=(M-k-1)!\cdot\left[1-\exp(-\lambda_D z_1)\sum_{n=0}^{M-k-1}\frac{\lambda_D^n z_1^n}{n!}\right], \quad \text{(B2)}$$

where $M-k=1,2,\cdots,M$.

Substituting Eq. (B2) into Q, we can derive Eq. (B3), as shown on the top of this page.

Using the incomplete Gamma function presented by Gradshteyn *et al.* (2007), we can derive Q as

$$Q=(M-k-1)!\cdot\left\{1-\sum_{n=0}^{M-k-1}\frac{\lambda_D^n}{n!}\frac{A\rho\lambda_P}{\alpha-1}\frac{\Gamma(n+1,\Lambda B)}{\Lambda^{n+1}}\right\}, \quad \text{(B4)}$$

where $\Lambda=\lambda_D+\dfrac{\lambda_P\rho}{\alpha-1}$.