Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks

Hui Zhao, Youyu Tan, Gaofeng Pan, *Member, IEEE*, Yunfei Chen, *Senior Member, IEEE*, and Nan Yang, *Member, IEEE*

***Abstract*—This paper investigates the secrecy outage performance of transmit antenna selection (TAS)/maximal ratio combining (MRC) in multiple input multiple output (MIMO) cognitive radio networks (CRNs) over Rayleigh fading channels. In the considered system, a secondary user (SU-TX) equipped with N_A ($N_A \geq 1$) antennas uses TAS to transmit confidential messages to another secondary user (SU-RX), which is equipped with N_B ($N_B \geq 1$) antennas and adopts MRC scheme to process multiple received signals. Meanwhile, an eavesdropper equipped with N_E ($N_E \geq 1$) antennas also adopts MRC scheme to overhear the transmitted information between SU-TX and SU-RX. SU-TX adopts the underlay strategy to guarantee the quality of service of the primary user without spectrum sensing. In this paper, we derive the exact and asymptotic closed-form expressions for the secrecy outage probability. Simulations are conducted to validate the accuracy of the analysis.**

***Index Terms*—Cognitive radio networks, maximal ratio combining, multiple input multiple output, secrecy outage probability, transmit antenna selection.**

I. INTRODUCTION

Recently, as a promising solution to the inadequacy of spectrum, cognitive radio (CR) has received great attention [1]. In CR, secondary user (SU) can share the spectrum with the primary user (PU), by using overlay, interweave or underlay methods in order not to affect the quality of service (QoS) of PU. Among them, underlay is easy to realize, as SU only needs to adjust its transmit power within a threshold that PU can tolerate [2]. Thus, underlay has been investigated in several works [3], [4], [5].

On the other hand, due to the broadcast nature of wireless links, it is difficult to prevent eavesdroppers from overhearing wireless communications. To address this concern, physical layer security has been widely considered as an effective technology to prevent information from being intercepted, which was first investigated in [6] and recently in [7]-[11]. Security issues play an important role in wireless networks, especially in cognitive radio networks (CRNs), where the licensed frequency band is shared among the primary and secondary users, leading to an increased possibility of eavesdropping of the transmitted information for both PU and SU [12]-[16].

However, very few research has considered the secrecy performance of multi-antenna diversity, which is one of the most effective technologies to improve the transmission rate in CRNs. Refs. [17]-[18] investigated the secrecy outage performance of single input multiple output (SIMO) system using maximal ratio combining (MRC)/selection combining (SC) in CRNs. However, Ref. [17] only considered an eavesdropper with a single antenna. Ref. [18] only considered SC technique. It is well-known that MRC has better performance than SC.

Motivated by the above observations, in this paper we analyze the secrecy outage performance of MIMO CRN, where a secondary user (SU-TX) equipped with N_A ($N_A \geq 1$) antennas uses TAS[1] to transmit confidential messages to another secondary user (SU-RX), which is equipped with N_B ($N_B \geq 1$) antennas and adopts MRC to process multiple copies of the received signal. Meanwhile, an eavesdropper (Eve), which is equipped with N_E ($N_E \geq 1$) antennas, adopts MRC for successful eavesdropping. SU-TX adopts underlay strategy in order not to degrade the QoS of PU. The main contributions of our work are summarized as follows:

- Compared with [19] and [20] that only considered physical layer security for a conventional non-CR system, our paper considers the physical layer security for an underlay MIMO CRN. Due to the fact that CR system has a shared frequency band and therefore lower security, such an analysis of the secrecy performance for CR system

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. The work of N. Yang was supported by Australian Research Council's Discovery Project DP150103905.

Manuscript received August 31, 2015; revised Nov. 5 and December 29, 2015; accepted Feb. 09, 2016. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. S.-H. Leung. The material of this paper was presented in part at the 7th International Conference on Wireless Communications and Signal Processing (WCSP) in Nanjing, Jiangsu, China in Oct. 2015.

Hui Zhao, Youyu Tan and Gaofeng Pan are with the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China. e-mail: gfpan@swu.edu.cn.

Yunfei Chen is with the School of Engineering, University of Warwick, Coventry, U.K., CV4 7AL. e-mail: Yunfei.Chen@warwick.ac.uk.

Nan Yang is with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia. e-mail: nan.yang@anu.edu.au.

Digital Object Identifier 10.1109/TVT.2016.2529704

[1]TAS is a low cost and complexity method for exploiting spatial diversity in multiple antenna settings [19].

is important. Our proposed analytical model can bring out an insight on the secrecy outage performance of SU systems, which cannot be obtained from [19] and [20] for non-CR systems.
- Compared with [18] that considered physical layer security for CR using SC, this work considers physical layer security for CR using MRC, as MRC can improve the secrecy performance of the desired user but can also increase the eavesdropping capability of the eavesdropper. Thus, it is important to identify the effect of MRC.
- We study the secrecy outage performance of CRNs and derive accurate and asymptotic closed-form expressions for secrecy outage probability (SOP). Our asymptotic results accurately predict the secrecy diversity order and secrecy diversity gain.

II. System model

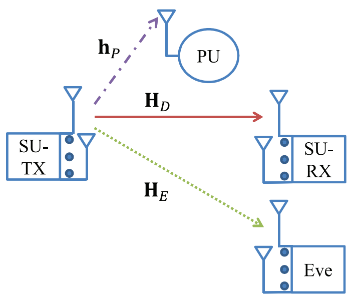

Fig. 1. System model

We consider a MIMO wiretap channel in CRNs, as illustrated in Fig. 1. SU-TX is equipped with N_A ($N_A \geq 1$) antennas and TAS is used to encode the confidential messages into transmitted codeword $x = [x(1), x(2), \cdots, x(n)]$, which is subject to an average power constraint $\frac{1}{n}\sum_{i=1}^{n} \mathrm{E}\left[|x(i)|^2\right] \leq P_S$. SU-TX transmits x to SU-RX, which is equipped with N_B ($N_B \geq 1$) antennas and adopts MRC to improve its received SNR, while Eve, which is equipped with N_E ($N_E \geq 1$) antennas, also adopts MRC to promote successful eavesdropping. $\mathbf{h}_P = [h_{p1}, h_{p2}, \cdots, h_{pN_A}]$ is the channel vector of the SU-TX–PU link. $\mathbf{H}_D$ and $\mathbf{H}_E$ are the channel gain matrixes of SU-TX–SU-RX and SU-TX–Eve links, respectively.

We assume that all channels experience independent Rayleigh fading and additive white Gaussian noise (AWGN) with variance of N_0. We also assume that the channel state information (CSI) of SU-TX–PU and SU-TX–SU-RX links are available at SU-TX, while the CSI of SU-TX–Eve link is unavailable at SU-TX[2]. The CSI from PU to SU-TX can be obtained by using channel reciprocity [5]. For simplification, we denote h_P, h_D and h_E as the average channel power gains of SU-TX–PU, SU-TX–SU-RX and SU-TX–Eve links, respectively.

As the CSI of the SU-TX–Eve link is not available at SU-TX, making use of the CSI among SU-TX–SU-RX, the "best" transmit antenna, which can maximize the total received signal power at SU-RX, is chosen to deliver the information. If such CSI is available, it would also be interesting to consider the selection of the worst antenna for the PU and eavesdropper. This can be a future research topic.

[2]In this scenario, SU-TX has no choice but to encode the confidential data into codewords of a constant rate R_S [18].

In order not to degrade the QoS of PU, when the uth ($u = 1, 2, \cdots, N_A$) antenna of SU-TX is selected to transmit messages, the transmit power (P_t) at SU-TX should be limited at a given threshold (I_P) that PU equipped with a single antenna can tolerate,

$$P_t = \begin{cases} I_P/g_P, & P_S \geq I_P/g_P \Rightarrow g_P \geq I_P/P_S; \\ P_S, & P_S < I_P/g_P \Rightarrow g_P < I_P/P_S, \end{cases} \tag{1}$$

where $g_P = |h_{pu}|^2$ is the channel power gain between the uth antenna of SU-TX and PU, P_S is the maximum transmitting power available at SU-TX.

The received signal vectors of SU-RX and Eve from the uth transmit antenna at time t are

$$\mathbf{y}_D(t) = \sqrt{P_t}\mathbf{h}_{Du}x(t) + \mathbf{n}_D, \tag{2}$$

$$\mathbf{y}_E(t) = \sqrt{P_t}\mathbf{h}_{Eu}x(t) + \mathbf{n}_E, \tag{3}$$

where $\mathbf{h}_{Du}$, $\mathbf{h}_{Eu}$ are the channel vectors between the uth transmit antenna and SU-RX, Eve whose elements are independent and identically distributed (i.i.d.) under Rayleigh fading, and $\mathbf{n}_D$, $\mathbf{n}_E$ are the AWGN vectors at SU-TX and Eve, respectively. This is a reasonable assumption as the channels among SU-TX and each antenna at a terminal, like SU-RX or EVE, are close to each other.

Let $\lambda_P = 1/h_P$, $\lambda_D = 1/h_D$ and $\lambda_E = 1/h_E$. When the uth antenna of SU-TX is selected to transmit information, the probability density functions of the MRC-combined channel power gain of SU-RX and Eve are given by [4]

$$f_{g_{Du}}(g_{Du}) = \frac{g_{Du}^{N_B-1}\exp(-\lambda_D g_{Du})\lambda_D^{N_B}}{(N_B-1)!}, \quad g_{Du} \geq 0, \tag{4}$$

$$f_{g_{Eu}}(g_{Eu}) = \frac{g_{Eu}^{N_E-1}\exp(-\lambda_E g_{Eu})\lambda_E^{N_E}}{(N_E-1)!}, \quad g_{Eu} \geq 0, \tag{5}$$

where $g_{Du} = \|\mathbf{h}_{Du}\|^2$ and $g_{Eu} = \|\mathbf{h}_{Eu}\|^2$, in which $\|\cdot\|$ denotes the Euclidean norm, respectively.

III. Secrecy Performance Analysis

A. Preliminaries

The TAS/MRC-combined channel power gain (g_D) of SU-RX can be given by

$$g_D = \max_{u=1,2,..,N_A} \{g_{Du}\}. \tag{6}$$

According to Ref. [19], the probability density function (PDF) of g_D can be derived as

$$\begin{aligned} f_{g_D}(x) &= N_A[F_{g_{Du}}(x)]^{N_A-1} f_{g_{Du}}(x) \\ &= \frac{N_A\lambda_D^{N_B}}{(N_B-1)!}\sum_{l=0}^{N_A-1}\binom{N_A-1}{l}(-1)^l \\ &\quad \times \exp\left[-\lambda_D(l+1)x\right]\left(\sum_{i=0}^{N_B-1}\frac{\lambda_D^i x^i}{i!}\right)^l x^{N_B-1}, \end{aligned} \tag{7}$$

where $F_{g_{Du}}(\cdot)$ is the cumulative probability density function (CDF) of g_{Du} given by

$$F_{g_{Du}}(x) = 1 - \exp(-\lambda_D x) \sum_{i=0}^{N_B-1} \frac{\lambda_D^i x^i}{i!}. \quad (8)$$

Using Eq. (9) in [21], we can have

$$\begin{aligned} f_{g_D}(x) = {} & \frac{N_A \lambda_D^{N_B}}{(N_B-1)!} \sum_{l=0}^{N_A-1} \binom{N_A-1}{l} (-1)^l \\ & \sum_{n_1=0}^{n_0} \sum_{n_2=0}^{n_1} \cdots \sum_{n_{R-1}=0}^{n_{R-2}} \left[\prod_{i=1}^{R-1} \binom{n_{i-1}}{n_i} \left(\frac{1}{i!}\right)^{n_i - n_{i+1}} \lambda_D^{n_i} \right] \\ & \times x^M \exp\left[-\lambda_D (l+1) x\right], \end{aligned} \quad (9)$$

where $M = N + N_B - 1$, $N = n_1 + n_2 + \cdots + n_{R-1}$, $R = N_B$, $n_0 = l$ and $n_R = 0$. When $R = 1$ and $N = 0$, $\left[\sum_{i=0}^{R-1} (\lambda_D x)^i \frac{1}{i!} \right]^{n_0} = 1$.

As the transmit antenna index is optimum for the SU-TX–SU-RX link, Eve is not able to exploit any additional diversity from the multiple transmit antennas at SU-TX. Thus, the PDF of the combined channel power (g_E) at Eve is given by $f_{g_E}(x) = f_{g_{Eu}}(x)$.

The instantaneous secrecy capacity is given by

$$C_S = \begin{cases} \log_2\left(1 + P_t \frac{g_D}{N_0}\right) - \log_2\left(1 + P_t \frac{g_E}{N_0}\right), & g_D > g_E; \\ 0, & g_D \le g_E. \end{cases} \quad (10)$$

SOP is defined as the probability that the instantaneous secrecy capacity is below a target secrecy rate (C_{th}, $C_{th} \ge 0$). Different from [18], we can calculate SOP under the two cases of P_t suggested by (1) as

$$\begin{aligned} SOP(C_{th}) = {} & \Pr\{g_P \ge I_P/P_S\} SOP_1(C_{th}) \\ & + \Pr\{g_P < I_P/P_S\} SOP_2(C_{th}), \end{aligned} \quad (11)$$

where $SOP_1(C_{th})$ and $SOP_2(C_{th})$ refer to the SOP when $P_t = I_P/g_P$ and $P_t = P_S$, respectively.

As $g_P = |h_{pu}|^2 \sim \exp(1/h_P)$, the items $\Pr\{g_P \ge I_P/P_S\}$ and $\Pr\{g_P \le I_P/P_S\}$ in (11) can be easily obtained as

$$\Pr\{g_P \ge I_P/P_S\} = \exp\left(-\frac{\lambda_P I_P}{P_S}\right) \quad (12)$$

$$\Pr\{g_P \le I_P/P_S\} = 1 - \exp\left(-\frac{\lambda_P I_P}{P_S}\right), \quad (13)$$

respectively. Next, we derive $SOP_1(C_{th})$ and $SOP_2(C_{th})$ to calculate the overall SOP in (11).

B. The derivation of $SOP_1(C_{th})$

When $P_t = I_P/g_P$, we can write $SOP_1(C_{th})$ as [12]

$$\Pr\{C_S \le C_{th}\} = \Pr\left\{\frac{\alpha-1}{\rho} g_P \ge g_D - \alpha g_E\right\}, \quad (14)$$

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

Let $Z_1 = \frac{\alpha-1}{\rho} g_P$, $Z_2 = g_D - \alpha g_E$ and $X = \alpha g_E$. The PDFs of X and Z_1 can be derived as[3]

$$f_X(x) = \frac{x^{N_E-1} \exp(-\lambda_E x/\alpha) \lambda_E^{N_E}}{\alpha^{N_E} (N_E-1)!} \quad (15)$$

$$f_{Z_1}(z_1) = \frac{A\rho\lambda_P}{\alpha-1} \exp\left(-\frac{\rho\lambda_P z_1}{\alpha-1}\right), z_1 \ge \frac{(\alpha-1)N_0}{P_S} = B, \quad (16)$$

respectively, where $A = 1/\exp(-\lambda_P I_P/P_S)$.

Using Eq. (6-55) in [22], when $Z_2 \ge 0$, we can write the PDF of Z_2 as[4]

$$f_{Z_2}(z_2) = \int_0^\infty f_{g_D}(z_2 + x) f_X(x)\, dx. \quad (17)$$

Substituting the PDFs of g_D and X into (17) and after some mathematical manipulations, we can derive $f_{Z_2}(z_2)$ as (18), as shown on the top of next page.

We can rewrite (14) as

$$\begin{aligned} SOP_1(C_{th}) = {} & \underbrace{\int_B^\infty f_{Z_1}(z_1) \int_{-\infty}^0 f_{Z_2}(z_2)\, dz_2 dz_1}_{I_1} \\ & + \underbrace{\int_B^\infty f_{Z_1}(z_1) \int_0^{z_1} f_{Z_2}(z_2)\, dz_2 dz_1}_{I_2}. \end{aligned} \quad (19)$$

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

$$I_3 = \int_0^\infty f_{Z_2}(z_2)\, dz_2. \quad (20)$$

I_3 can be easily calculated as (21), as shown on the top of next page. Therefore, it is easy to observe that

$$I_1 = \int_B^\infty f_{Z_1}(z_1) \cdot (1 - I_3)\, dz_1 = 1 - I_3. \quad (22)$$

We can rewrite I_2 as (23), as shown on the top of next page, where $\Upsilon(n,x) = \int_0^x \exp(-t) t^{n-1} dt$ is the lower incomplete gamma function [23].

Using Eq. (8.352.1) in [23] to expand $\Upsilon(.,.)$ in I_4 into the form of series , the integral in (23) can be derived as (24), as shown on the next page, where $\Lambda = \lambda_D(l+1) + \frac{\rho\lambda_P}{\alpha-1}$ and $\Gamma(n,x) = \int_x^\infty \exp(-t) t^{n-1} dt$ is the upper incomplete gamma function [23].

Finally, we can derive $SOP_1(C_{th})$ as

$$SOP_1(C_{th}) = 1 - I_3 + \sum_\Omega \sum_{k=0}^M \Phi I_4, \quad (25)$$

where I_4 is given in (24), Σ_Ω is given in (18) and Φ is given in (23).

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

[4]To simplify the analysis, we need not calculate the PDF of $Z_2 < 0$, directly.

$$f_{Z_2}\left(z_2\right)=\underbrace{\frac{N_A\lambda_D^{N_B}\lambda_E^{N_E}}{\alpha^{N_E}\left(N_E-1\right)!\left(N_B-1\right)!}\sum_{l=0}^{N_A-1}\begin{pmatrix}N_A-1\\ l\end{pmatrix}(-1)^l\sum_{n_1=0}^{n_0}\sum_{n_2=0}^{n_1}\cdots\sum_{n_{R-1}=0}^{n_{R-2}}\left[\prod_{i=1}^{R-1}\begin{pmatrix}n_{i-1}\\ n_i\end{pmatrix}\left(\frac{1}{i!}\right)^{n_i-n_{i+1}}\lambda_D^{n_i}\right]}_{\Sigma_\Omega}$$
$$\times\sum_{k=0}^{M}\begin{pmatrix}M\\ k\end{pmatrix}\Gamma\left(N_E+k\right)\left(\frac{\lambda_E}{\alpha}+\lambda_D\left(l+1\right)\right)^{-\left(N_E+k\right)}z_2^{M-k}\exp\left(-\lambda_D\left(l+1\right)z_2\right). \tag{18}$$

$$I_3=\sum_{\Omega}\sum_{k=0}^{M}\begin{pmatrix}M\\ k\end{pmatrix}\Gamma\left(N_E+k\right)\left(\frac{\lambda_E}{\alpha}+\lambda_D\left(l+1\right)\right)^{-\left(N_E+k\right)}\Gamma\left(M-k+1\right)\left[\lambda_D\left(l+1\right)\right]^{-\left(M-k+1\right)}. \tag{21}$$

$$I_2=\sum_{\Omega}\sum_{k=0}^{M}\underbrace{\begin{pmatrix}M\\ k\end{pmatrix}\Gamma\left(N_E+k\right)\left(\frac{\lambda_E}{\alpha}+\lambda_D\left(l+1\right)\right)^{-\left(N_E+k\right)}\left[\lambda_D\left(l+1\right)\right]^{-\left(M-k+1\right)}\frac{A\rho\lambda_P}{\alpha-1}}_{\Phi}$$
$$\times\underbrace{\int_B^{\infty}\exp\left(-\frac{\rho\lambda_P z_1}{\alpha-1}\right)\Upsilon\left(M-k+1,\lambda_D\left(l+1\right)z_1\right)dz_1}_{I_4}. \tag{23}$$

$$I_4=\left(M-k\right)!\left\{\frac{\alpha-1}{\rho\lambda_P}\exp\left(-\frac{\rho\lambda_P B}{\alpha-1}\right)-\sum_{m=0}^{M-k}\frac{\left[\lambda_D\left(l+1\right)\right]^m}{m!}\frac{\Gamma\left(m+1,\Lambda B\right)}{\Lambda^{m+1}}\right\}. \tag{24}$$

$$SOP_2\left(C_{th}\right)=1-\frac{1}{\Gamma\left(N_E\right)}\sum_{p=1}^{N_A}\begin{pmatrix}N_A\\ p\end{pmatrix}(-1)^{p-1}\exp\left[-\frac{p\left(\alpha-1\right)}{\overline{\gamma}_B}\right]\prod_{u=1}^{N_B-1}\left[\sum_{i_u=0}^{i_{u-1}}\begin{pmatrix}i_{u-1}\\ i_u\end{pmatrix}\left(\frac{1}{u!}\right)^{i_u-i_{u+1}}\right]\left(\frac{1}{\overline{\gamma}_B}\right)^{\psi_u}$$
$$\times\left(\frac{1}{\overline{\gamma}_E}\right)^{N_E}\sum_{t=0}^{\psi_u}\begin{pmatrix}\psi_u\\ t\end{pmatrix}\alpha^t(\alpha-1)^{\psi_u-t}\Gamma\left(t+N_E\right)\left(\frac{\alpha p}{\overline{\gamma}_B}+\frac{1}{\overline{\gamma}_E}\right)^{-\left(t+N_E\right)}. \tag{26}$$

C. The derivation of $SOP_2\left(C_{th}\right)$

When $g_P < I_P/P_S$, $P_t = P_S$. It means that SU-TX only adopts its maximum transmitting power to deliver information to SU-RX. Obviously, the target system model becomes a non-CR model in this case.

Substituting $\gamma_B = P_S g_D/N_0$, $\overline{\gamma}_B = P_S h_M/N_0$, $\gamma_E = P_S g_E/N_0$ and $\overline{\gamma}_E = P_S h_E/N_0$ into Eq. (25) in [20], where $m_B = m_E = 1$ [5], we can calculate $SOP_2\left(C_{th}\right)$ as (26), as shown on the top of next page, where $\psi_u = \sum_{u=1}^{N_B-1} i_u$, $i_0 = p$ and $i_{N_E} = 0$.

Finally, SOP can be obtained by substituting (12), (13), (25) and (26) into (11).

IV. Asymptotic Secrecy outage probability

In this section, we will present the asymptotic SOP analysis when $\lambda_D \to 0$, namely $\overline{\gamma}_1 = \frac{P_S}{N_0\lambda_D} \to \infty$ in [18], motivated by the fact that the secrecy diversity order and secrecy array gain govern the SOP at high SNR at SU-RX. Another aim of deriving asymptotic SOP is that the asymptotic expression is normally more concise than that of the exact expression.

[5] The closed-form expression for SOP in [20] was derived in Nakagami-m fading scenarios. Then, we can easily obtain the closed-form expression for SOP over Rayleigh fading channels by substituting $m_B = m_E = 1$ into Eq. (25) in [20].

A. The Derivation of Asymptotic SOP_1^{∞}

When $\lambda_D \to 0$, by applying binomial combination and first order Maclaurin series expansion and then keeping the first two terms in the Maclaurin series expansion, we can rewrite (7) as

$$f_{g_D}\left(x\right)=\frac{N_A\lambda_D^{N_A N_B}}{\left(N_B-1\right)!\left(N_B!\right)^{N_A-1}}x^{N_A N_B-1}+o\left(\lambda_D^{N_A N_B}\right), \tag{27}$$

where $o(\cdot)$ denotes higher order terms.

In order to derive the asymptotic analysis, (14) can be rewritten as

$$SOP_1=\Pr\left\{\frac{\alpha-1}{\rho}g_P+\alpha g_E\geq g_D\right\}. \tag{28}$$

Let $Z_3 = \frac{\alpha-1}{\rho} g_P + \alpha g_E$ and $a = \frac{\lambda_E}{\alpha} - \frac{\rho\lambda_P}{\alpha-1}$. Using Eq. (1.111) in [23], we can derive the PDF of Z_3 as

$$f_{Z_3}(z_3) = \frac{A\rho\lambda_P\lambda_E^{N_E}}{(\alpha-1)\alpha^{N_E}(N_E-1)!} \sum_{q=0}^{N_E-1} \begin{pmatrix} N_E-1 \\ q \end{pmatrix} (-1)^{N_E-q-1} \left[Q_1(N_E-q-1,a,z_3) - Q_1(N_E-q-1,a,B)\right] z_3^q \exp\left(-\frac{\lambda_E}{\alpha} z_3\right), \tag{29}$$

where $Q_1(\cdot,\cdot,\cdot)$ is defined as (given by Eq. (1.3.2.6) in [24])

$$Q_1(n,a,x) = \int x^n \exp(ax)\,dx = \exp(ax) \cdot \left[\frac{x^n}{a} + \sum_{p=1}^{n} (-1)^p \frac{n(n-1)\cdots(n-p+1)}{a^{p+1}} x^{n-p}\right]. \tag{30}$$

When $\lambda_D \to 0$, using (27), we can write the asymptotic SOP_1 as

$$SOP_1^\infty = \int_B^\infty f_{Z_3}(z_3) \int_0^{z_3} f_{g_D}(g_D)\,dg_D\,dz_3 = \frac{\lambda_D^{N_A N_B}}{(N_B!)^{N_A}} \int_B^\infty f_{Z_3}(z_3)\, z_3^{N_A N_B}\, dz_3 + o\left(\lambda_D^{N_A N_B}\right). \tag{31}$$

Substituting the PDF of Z_3 into the above equation and using the closed-form expression of Q_2 given in Appendix, we can derive the closed-form expression of the asymptotic SOP_1^∞ as

$$SOP_1^\infty = (G_{a1} \cdot \lambda_D)^{N_A N_B} + o\left(\lambda_D^{N_A N_B}\right), \tag{32}$$

where the achieved secrecy array gain is G_{a1}^{-1} where G_{a1} is defined as (33), as shown on the top of next page, in which $\Theta = \frac{A\rho\lambda_P\lambda_E^{N_E}}{(\alpha-1)\alpha^{N_E}(N_E-1)!(N_B!)^{N_A}}$.

B. The Derivation of Asymptotic SOP_2^∞

When $g_P < I_P/P_S$, the target system model becom CR model in this case. Thus, considering Eqs. (26) a in [20], we can obtain the closed-form expression for

$$SOP_2^\infty = (G_{a2} \cdot \lambda_D)^{N_A N_B} + o\left(\lambda_D^{N_A N_B}\right),$$

where G_{a2} is defined as

$$G_{a2} = \left[\frac{(\alpha-1)^{N_A N_B}}{(N_B!)^{N_A}\Gamma(N_E)} \sum_{p=0}^{N_A N_B} \begin{pmatrix} N_A N_B \\ p \end{pmatrix} \left(\frac{\alpha P_S}{(\alpha-1)\lambda_E N_0}\right)^p \Gamma(N_E+p)\right]^{\frac{1}{N_A N_B}} \frac{N_0}{P_S}.$$

Finally, we can derive the closed-form expression of the asymptotic SOP as

$$SOP^\infty = (G_a \cdot \lambda_D)^{N_A N_B} + o\left(\lambda_D^{N_A N_B}\right), \tag{36}$$

where the achieved secrecy diversity gain is $N_A N_B$, and G_a^{-1} determines the slope of the asymptotic outage probability curve, which is derived as

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

Note that the SOP expressions derived in the previous section allow for the direct determination of the effects of all the important system parameters on the secrecy performance. This eliminates the need for tedious simulations to exhaust all possible values of the system parameters and therefor is useful. Moreover, the asymptotic results in (32) and (36) are only polynomial functions, the simplest possible form, to give the direct insights on the effects of diversity gain and diversity slope. They all represent important contributions.

V. Numerical and Simulation Results

In this section, we run Monte Carlo simulation to validate our analytical expressions of the SOP over Rayleigh fading channels. In each simulation case, SU-TX sends 10^6 bits to SU-RX.

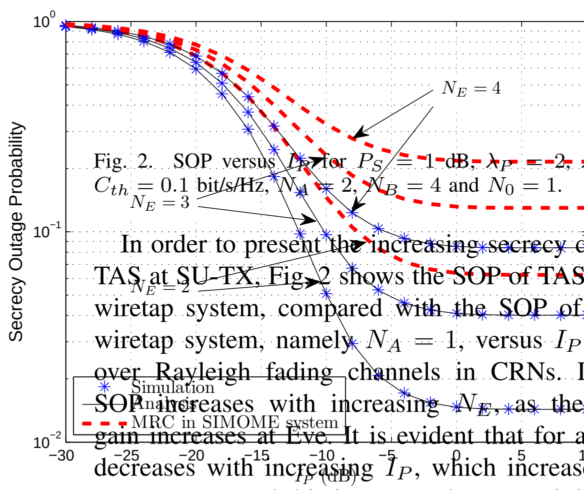

Fig. 2. SOP versus I_P for $P_S = 1$ dB, $\lambda_P = 2$, $\lambda_D = 2$, $\lambda_E = 4$, $C_{th} = 0.1$ bit/s/Hz, $N_A = 2$, $N_B = 4$ and $N_0 = 1$.

In order to present the increasing secrecy diversity of using TAS at SU-TX, Fig. 2 shows the SOP of TAS/MRC in MIMO wiretap system, compared with the SOP of MRC in SIMO wiretap system, namely $N_A = 1$, versus I_P for various N_E over Rayleigh fading channels in CRNs. It is shown that SOP increases with increasing N_E, as the MRC diversity gain increases at Eve. It is evident that for a fixed N_E, SOP decreases with increasing I_P, which increases peak transmit power at PU and this increases the transmitting power at SU-TX. We can also see that, there exists a floor for SOP in the high I_P region. It is because $P_t = P_S$ when $I_P \to \infty$, which means that in this case the transmitting SNR remains constant. Moreover, it can also be seen that the secrecy performance of TAS/MRC scheme greatly outperforms the one of the MRC

$$G_{a1} = \left\{ \Theta \sum_{q=0}^{N_E-1} \left(\begin{array}{c} N_E - 1 \\ q \end{array} \right) (-1)^{N_E-q-1} \left[Q_2 - Q_1 \left(N_E - q - 1, a, B \right) \Gamma \left(N_A N_B + q + 1, \frac{\lambda_E}{\alpha} B \right) \left(\frac{\alpha}{\lambda_E} \right)^{N_A N_B + q + 1} \right] \right\}^{\frac{1}{N_A N_B}}. \tag{33}$$

scheme, because the secrecy diversity order of TAS/MRC is $N_A N_B$, while the secrecy diversity order of MRC is N_B.

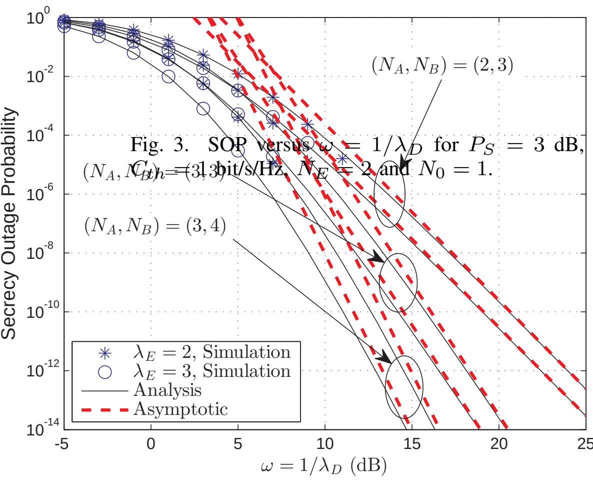

Fig. 3. SOP versus $\omega = 1/\lambda_D$ for $P_S = 3$ dB, $I_P = 1$ dB, $\lambda_P = 2$, $C_{th} = 1$ bit/s/Hz, $N_E = 2$ and $N_0 = 1$.

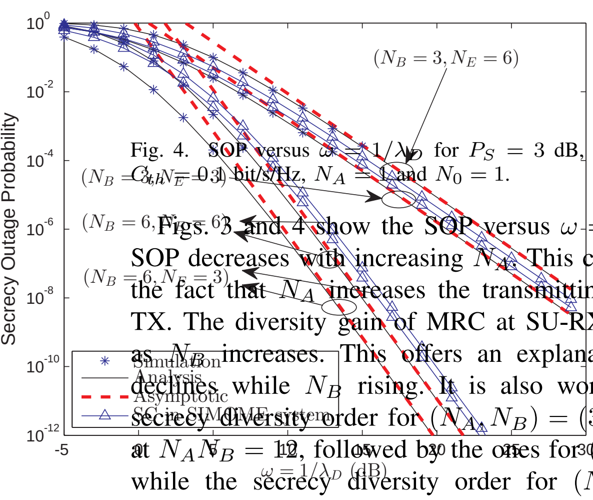

Fig. 4. SOP versus $\omega = 1/\lambda_D$ for $P_S = 3$ dB, $I_P = 1$ dB, $\lambda_P = 3$, $C_{th} = 0.1$ bit/s/Hz, $N_A = 1$ and $N_0 = 1$.

Figs. 3 and 4 show the SOP versus $\omega = 1/\lambda_D$. In Fig. 3, SOP decreases with increasing N_A. This can be explained by the fact that N_A increases the transmitting diversity at SU-TX. The diversity gain of MRC at SU-RX can be improved as N_B increases. This offers an explanation of why SOP declines while N_B rising. It is also worth noting that the secrecy diversity order for $(N_A, N_B) = (3, 4)$ is the highest, at $N_A N_B = 12$, followed by the ones for $(N_A, N_B) = (3, 3)$, while the secrecy diversity order for $(N_A, N_B) = (2, 3)$ is the lowest, at 6, which means that the secrecy outage performance of $(N_A, N_B) = (3, 4)$ is the best among the three (N_A, N_B) combinations. Moreover, the obtained asymptotic results match very well with the exact results, and accurately predict the secrecy diversity order and secrecy array gain in the high ω region, namely, in the high $\overline{\gamma}_1$ region in [18]. Further, we can also observe that the asymptotic SOP presents the upper bound of the exact SOP.

Due to the fact that the secrecy performance of SC scheme in CRNs was only considered in [18], while the secrecy performance of MRC scheme has not yet been investigated in the previous works[6], Fig. 4 compares the secrecy outage performance between MRC and SC schemes, namely, $N_A = 1$. Obviously, apart from the scenario of $(N_B, N_E) = (3, 6)$, the secrecy outage performance of MRC outperforms the one of SC among the other three scenarios, $(N_B, N_E) = (3, 3), (6, 6)$ and $(6, 3)$, respectively, although the secrecy diversity orders of MRC and SC schemes are same.

Further, simulation and analytical results match very well with each other, which verify our proposed analytical models.

VI. Conclusion

In this paper, we have studied the physical layer security in MIMO cognitive wiretap channels and investigated the secrecy outage performance over Rayleigh fading channels by deriving closed-form expressions for the exact and asymptotic SOP.

VII. Appendix

We consider the following integral equation

$$Q_2 = \int_B^\infty Q_1 \left(N_E - q - 1, a, z_3 \right) \cdot z_3^{N_A N_B + q} \exp \left(-\frac{\lambda_E}{\alpha} z_3 \right) dz_3. \tag{38}$$

Substituting $Q_1(\cdot,\cdot,\cdot)$ into the above equation and using Eq. (3.351.2) in [23], we can derive Q_2 as

$$\begin{aligned} Q_2 = &\frac{1}{a} \left(\frac{\alpha - 1}{\rho \lambda_P} \right)^{N_E + N_A N_B} \Gamma \left(N_E + N_A N_B, \frac{\rho \lambda_P}{\alpha - 1} B \right) \\ &+ \sum_{p=1}^{N_E-q-1} (-1)^p \frac{\left(N_E - q - 1 \right) \left(N_E - q - 2 \right) \cdots \left(N_E - q - p \right)}{a^{p+1}} \\ &\cdot \left(\frac{\alpha - 1}{\rho \lambda_P} \right)^{N_E + N_A N_B - p} \Gamma \left(N_E + N_A N_B - p, \frac{\rho \lambda_P}{\alpha - 1} B \right). \end{aligned} \tag{39}$$

[6]Ref. [17] has only considered that Eve is equipped with a single antenna and the transmit power restriction at SU-TX is incomplete, so the contribution of [17] is significantly limited.

REFERENCES

[1] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[2] J. Lee, H. Wang, J. G. Andrews, and D. Hong, “Outage probability of cognitive relay networks with interference constraints,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390-395, Feb. 2011.

[3] T. Q. Duong, V. N. Q. Bao, and H.-J. Zepernick, “Exact outage probability of cognitive AF relaying with underlay spectrum sharing,” *Electron. Lett.*, vol. 47, no. 17, pp. 1001-1002, Aug. 2011.

[4] V. Blagojevic and P. Ivanis, “Ergodic capacity for TAS/MRC spectrum sharing cognitive radio,” *IEEE Commun. Lett.*, vol. 16, no. 3, pp. 321-323, Mar. 2012.

[5] A. Alsharoa, H. Ghazzai, and M. S. Alouini, “Optimal transmit power allocation for MIMO two-way cognitive raley networks with multiple relays using AF strategy,” *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 30-33, Feb. 2014.

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

[7] G. Pan, C. Tang, X. Zhang, et al., “Physical layer security over non-small scale fading channels,” to appear in *IEEE Trans. Veh. Techol.*.

[8] G. Pan, C. Tang, T. Li, and Y. Chen. “Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems,” *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3423-3433, Sept. 2015.

[9] Y. Zhou, G. Pan, T. Li, et al., “Secrecy outage performance for partial relay selection schemes in cooperative systems,” *IET Commun.*, vol. 9, no. 16, pp. 1980-1987, Nov. 2015.

[10] H. Lei, C. Gao, Y. Guo, et al., “On physical layer security over generalized Gamma fading channels,” *IEEE Commun. Lett.*, vol. 19, no. 7, pp. 1257-1260, July 2015.

[11] J. Zhu, Y. Zou, G. Wang, et al., “On secrecy performance of antenna selection aided MIMO systems against eavesdropping,” to appear in *IEEE Trans. Veh. Techol.*.

[12] C. Tang, G. Pan, and T. Li, “Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels,” *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 609-612, Dec. 2014.

[13] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio Systems,” *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215-228, Jan. 2015.

[14] Y. Zou, X. Li, and Y.-C. Liang, “Secrecy outage and diversity analysis of cognitive radio systems,” *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222-2236, Nov. 2014.

[15] H.-Q. Liu, H. Zhao, H. Jiang, C. Tang, G. Pan, T. Li, and Y. Chen, “Physical layer secrecy ouatge of spectrum sharing CR system over fading channels,” to appear in *Sci. China Inf. Sci.*

[16] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, “Securing physical-layer communications for cognitive radio networks,” *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 48-54, Sept. 2015.

[17] H. Zhao, H. Liu, Y. Liu, C. Tang, and G. Pan, “Physical layer security of maximal radio combining in underlay cognitive radio unit over Rayleigh fading channels,” in *Proc. ICCSN 2015*, Chengdu, China, June 6-7 2015, pp. 201-205.

[18] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, “On the security of cognitive radio networks,” *IEEE Trans. Veh. Techol.*, vol. 64, no. 8, pp. 3790-3795, Aug. 2015.

[19] H. Alves, R. D. Souza, M. Debbah, M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” *IEEE Sig. Process. Lett.*, vol. 19, no. 6, pp. 372-375, June 2012.

[20] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, “Transmit antenna selection for security enhancement in MIMO wiretap channels,” *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[21] S. Choi and Y.-C. Ko, “Performance of selection MIMO systems with generalized selection criterion over Nakagami-m fading channels,” *IEICE Trans. Commun.*, vol. E89-B, no. 12, pp. 3467-3470, Dec. 2006.

[22] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*, 4th edition. McGraw Hill Book Company, 2001.

[23] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th edition. Academic Press, 2007.

[24] A. P. Prudnikov, Yu. A. Brychkov, and O. I. Marichev, *Integrals and series, vol. 1, elementary functions*. New York: Gordon & Breach Sci. Publ., 1986.