Secure Transmission in Cognitive Wiretap Networks

Tao Zhang*, Yueming Cai*, Yuzhen Huang*, Caijun Zhong†, Weiwei Yang* and George K. Karagiannidis‡
*College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China
†Institute of Information and Communication Engineering, Zhejiang University, Hangzhou, China
‡Aristotle University of Thessaloniki, Thessaloniki, Greece, and Khalifa University, Abu Dhabi, UAE
Email: ztcool@126.com, caiym@vip.sina.com, yzh_huang@sina.com, caijunzhong@zju.edu.cn, geokarag@ieee.org

***Abstract*—In this paper, we analyze the secrecy performance of multi-antenna cognitive wiretap network, where the secondary transmitter (Alice) communicates with the secondary receiver (Bob) in the presence of an eavesdropper (Eve). Specifically, we investigate the cases of maximal-ratio combining (MRC) with half-duplex (HD) and selection combining/Zero forcing beamforming (SC/ZFB) scheme with full-duplex (FD) operation, respectively. Assuming the Rayleigh fading, closed-form expressions for the secrecy outage probability of cognitive wiretap channels with MRC and SC/ZFB are derived. Furthermore, we provide simple asymptotic approximations for the secrecy outage probability and find that both schemes achieve full diversity. In addition, simulation results reveal that MRC outperforms SC/ZBF in the low interference threshold regime, while the opposite holds in the high interference threshold regime.**

I. Introduction

In the last years, cognitive radios, as an effective means to alleviate the spectrum shortage problem, has received considerable interesting by the research community [1]. In spectrum sharing cognitive radio networks, the secondary users (SUs) are allowed to access the licensed spectrum as long as the interference power inflicted on the primary user (PU) does not exceed the *interference temperature limit*. Extensive research efforts were devoted to investigate the information theoretic performance of spectrum sharing cognitive radio networks, such as transmission rate, outage probability and symbol error rate.

In order to implement cognitive radio networks in practice, a number of challenging issues, including security, need to be addressed. Due to the open and dynamic features, cognitive radio networks are vulnerable to various malicious attacks, making secure communications to be a difficult task. Motivated by this, several works have investigated the security issues of cognitive radio networks from a physical layer perspective. In [2], Y. Pei, *et.al*, designed a robust transmitter for secure transmission in cognitive radio networks. In [3], different relay selection schemes were proposed to enhance the security of cognitive radio networks in the presence of a single eavesdropper. In [4], the authors investigated the secure transmission of cognitive radio networks with the untrusted SUs and derived closed-form expressions for the achievable secrecy rate.

For further secrecy enhancement, various techniques have been proposed, for instance, the use of multi-antenna and full-duplex (FD) transmission. The secrecy performance of multi-antenna assisted wiretap channels has been extensively studied in literature, covering diverse scenarios such as secrecy outage performance of single-input multi-output (SIMO) wiretap channels with maximal ratio combing (MRC) at both the legitimate receiver and the eavesdropper [5], the impact of multiple eavesdroppers [6] and the transmit antenna selection for multiple-input multiple-output (MIMO) wiretap channels with different receiver combining schemes [7]. Similarly, the idea of employing FD operation to improve the secure transmission, by sending a jamming signal to degrade the quality of the eavesdropper channel has been studied in [8]. However, to the best of the authors' knowledge, no works have considered the application of FD in cognitive radio networks with multiple antennas for secrecy improvement.

Motivated by this, we consider a multi-antenna cognitive radio network, where a secondary transmitter (ST) communicates with a secondary destination (SD), equipped with multiple antennas in the presence of a primary receiver (PR) and an eavesdropper. We consider both MRC with half-duplex (HD) and selection combining/Zero forcing beamforming (SC/ZFB) scheme with FD. Exact and simple asymptotic expressions for the secrecy outage probability of cognitive wiretap network are derived. Our results reveal that both schemes achieve full diversity. In addition, MRC outperforms SC/ZBF in the low interference threshold regime, while the opposite holds in the high interference one.

II. System Model

We consider a multi-antenna cognitive wiretap channel, which consists of a secondary transmitter (Alice), a secondary receiver (Bob), a primary receiver (PR) and an eavesdropper (Eve). All nodes are equipped with a single antenna, except Bob, which has N_B antennas. As in [9], we assume that the primary transmitter is far away from the secondary receiver, thus the interference from the primary transmitter can be ignored at the secondary receivers, i.e., Bob and Eve. The corresponding channel coefficient between the nodes K and T is denoted as h_{KT}, which is an exponentially distributed random variable with variance, λ_{KT}. Without loss of generality, the main and eavesdropper channels are assumed to be quasi-static independent and non-identical fading channels, following Rayleigh distribution.

To exploit the advantages of multiple antennas, we consider two different secure transmission schemes, i.e., the MRC with HD, and SC/ZFB with FD.

978-1-5090-1698-3/16/$31.00 ©2016 IEEE

For the MRC with HD operation, Bob adopts the MRC to strengthen the signal detection, thus, the instantaneous SNR between Alice and Bob is given by

$$\gamma_{B_1} = \frac{P_{S_1}}{\sigma^2} \left\| \mathbf{h}_{AB} \right\|^2, \tag{1}$$

where $\mathbf{h}_{AB}$ is an $N_B \times 1$ channel link vector between Alice and Bob, σ^2 denotes the noise variance at each receiver, and P_{S_1} is the transmit power of Alice, which must satisfy $P_{S_1} = \min\left(\frac{Q}{|h_{AP}|^2}, P_t\right)$,where P_t is the maximum transmit power constraint at Alice and Q denotes the interference temperature constraint at the PU.

Similarly, the instantaneous SNR of the eavesdropper channel is given by

$$\gamma_{E_1} = \frac{P_{S_1}}{\sigma^2} \left| h_{AE} \right|^2, \tag{2}$$

where h_{AE} represents the channel coefficient between Alice and Eve.

For theSC/ZFB based on FD operation, Bob first selects the best antenna based on the CSI of the main channel, and utilizes the remaining $N_B - 1$ antennas to send a weighted jamming signal. To satisfy the interference constraint at PR, we adopt the ZF algorithm to avoid the undesirable jamming signals at PR. Thus, the optimal weight vector $\mathbf{w}_{ZF}$ is the solution of the following optimization problem:

$$\begin{aligned} &\max_{\mathbf{w}_{ZF}} \left| \mathbf{h}_{BE}^{\dagger} \mathbf{w}_{ZF} \right| \\ &s.t. \ \left| \mathbf{h}_{BP}^{\dagger} \mathbf{w}_{ZF} \right| = 0 \ \& \ \left\| \mathbf{w}_{ZF} \right\|_F = 1, \end{aligned} \tag{3}$$

where $\mathbf{h}_{BE}$ and $\mathbf{h}_{BP}$ denote the $(N_B - 1) \times 1$ channel vectors between the remaining $N_B - 1$ antennas of the Bob and the Eve, and the remaining $N_B - 1$ antennas of the Bob and the PR, respectively. Now, using the projection matrix theory [10], the optimal weight vector can be derived as

$$\mathbf{w}_{ZF} = \frac{\mathrm{T}^{\perp} \mathbf{h}_{BE}}{\| \mathrm{T}^{\perp} \mathbf{h}_{BE} \|}, \tag{4}$$

where $\mathrm{T}^{\perp} = \left(\mathbf{I} - \mathbf{h}_{BP} \left(\mathbf{h}_{BP}^{\dagger} \mathbf{h}_{BP} \right)^{-1} \mathbf{h}_{BP}^{\dagger} \right)$ is the projection idempotent matrix with rank $N_B - 2$. As a result, the instantaneous SNRs of the main and the eavesdropper channels can be respective expressed as[1]

$$\gamma_{B_2} = \frac{P_{S_2}}{\sigma^2} \max_{i \in N_B} \left(\left| h_{ABi} \right|^2 \right), \tag{5}$$

and

$$\gamma_{E_2} = \frac{P_{S_2} \left| h_{AE} \right|^2}{P_Z \left| \mathbf{h}_{BE}^{\dagger} \mathbf{w}_{ZF} \right|^2 + \sigma^2}, \tag{6}$$

where the transmit power of Alice P_{S_2} is same to P_{S_1}, and P_Z denotes the power of the jamming signal from Bob.

[1]Please note, for the FD operation, we assume that the self-interference can be completely suppressed at Bob as in prior work [11]. The practical self-interference cancelation algorithms are beyond the scope of this paper.

Now, according to [9], the achievable secrecy rate of the multi-antenna cognitive wiretap network is given by

$$C_S = \begin{cases} C_{B_i} - C_{E_i}, & \gamma_{B_i} > \gamma_{E_i} \\ 0, & \gamma_{B_i} \leq \gamma_{E_i} \end{cases} \tag{7}$$

where $i = \{1, 2\}$ represents MRC and SC/ZFB, respectively, $C_{B_i} = \log_2(1 + \gamma_{B_i})$ and $C_{E_i} = \log_2(1 + \gamma_{E_i})$ are the achievable instantaneous rates at Bob and Eve, respectively.

For notational convenience, we define $\rho = \frac{Q}{P_t}$, $\bar{\gamma}_B = \frac{P_t}{\sigma^2} \lambda_{AB} = \frac{Q}{\rho \sigma^2} \lambda_{AB}$, $\bar{\gamma}_E = \frac{P_t}{\sigma^2} \lambda_{AE} = \frac{Q}{\rho \sigma^2} \lambda_{AE}$, and $\bar{\gamma}_Z = \frac{P_Z}{\sigma^2} \lambda_{BE}$.

III. Secrecy Performance Analysis

In this section, we investigate the secrecy outage performance of the cognitive wiretap systems with the proposed secure transmission schemes. The secrecy outage probability is defined as the probability of the secrecy capacity, C_S, being lower than a predetermined threshold R_S. Mathematically, it can be represented as

$$\begin{aligned} P_{\mathrm{out}}(R_S) &= \Pr(C_S < R_S) \\ &= \int_0^{\infty} F_{\gamma_{B_i}} \left(2^{R_S}(1 + x) - 1 \right) f_{\gamma_{E_i}}(x) \, dx. \end{aligned} \tag{8}$$

Next, we present a detail analysis for the secrecy outage probability of multi-antenna cognitive wiretap network with MRC and SC/ZFB, respectively.

A. MRC

The key challenge in the analysis lies in the fact that γ_{B_1} and γ_{E_1} are statistically dependent, due to the presence of the common random variable (RV) $G_1 = |h_{AP}|^2$ in P_{S_1}. Responding to this, we first seek the cumulative distribution function (CDF) of the SNR of the main channel and the probability density function (PDF) of the SNR of the eavesdropper channel, conditioned on the RV G_1.

According to (1), the conditional CDF of γ_{B_1} is given by

$$F_{\gamma_{B_1}}(x|G_1) = 1 - e^{-\frac{x}{P_{S_1} \lambda_{AB}/\sigma^2}} \sum_{k=0}^{N_{\mathrm{B}}-1} \frac{1}{k!} \left(\frac{x}{P_{S_1} \lambda_{AB}/\sigma^2} \right)^k. \tag{9}$$

Similarly, based on (2), the conditional PDF of γ_{E_1} can be expressed as

$$f_{\gamma_{E_1}}(y|G_1) = \frac{1}{P_{S_1} \lambda_{AE}/\sigma^2} \exp\left(-\frac{y}{P_{S_1} \lambda_{AE}/\sigma^2} \right). \tag{10}$$

Now, we are ready to derive the closed-form expression for the secrecy outage probability with MRC in the following Lemma.

Lemma 1. *The secrecy outage probability of multi-antenna cognitive radio systems, employing MRC with HD operation*

is given by

$$P_{\text{out}}^{\text{MRC}}(R_{\text{S}}) = \Bigg[1 - \sum_{k=0}^{N_{\text{B}}-1} \frac{1}{k!} \frac{1}{(\bar{\gamma}_B)^k} \frac{1}{\bar{\gamma}_E} \exp\left(-\frac{2^{R_{\text{S}}}-1}{\bar{\gamma}_B}\right) \times \sum_{i=0}^{k} \binom{k}{i} \left(2^{R_{\text{S}}}-1\right)^{k-i} \left(2^{R_{\text{S}}}\right)^{i} i! \left(\frac{\bar{\gamma}_B\bar{\gamma}_E}{2^{R_{\text{S}}}\bar{\gamma}_E+\bar{\gamma}_B}\right)^{i+1}\Bigg] \times \left(1-\exp\left(-\frac{\rho}{\lambda_{AP}}\right)\right) + \exp\left(-\frac{\rho}{\lambda_{AP}}\right) - \sum_{k=0}^{N_{\text{B}}-1} \frac{1}{k!\left(\rho\bar{\gamma}_B\right)^k \rho\bar{\gamma}_E} \times \sum_{i=0}^{k} \binom{k}{i} \left(2^{R_{\text{S}}}-1\right)^{k-i} \left(2^{R_{\text{S}}}\right)^{i} \left(\frac{\rho\bar{\gamma}_B\bar{\gamma}_E}{2^{R_{\text{S}}}\bar{\gamma}_E+\bar{\gamma}_B}\right)^{i+1} \frac{i!}{\lambda_{AP}} \times \left(\frac{\rho\bar{\gamma}_B\lambda_{AP}}{(2^{R_{\text{S}}}-1)\lambda_{AP}+\rho\bar{\gamma}_B}\right)^{k-i+1} \Gamma\left(k-i+1, \frac{\left(2^{R_{\text{S}}}-1\right)\lambda_{AP}+\rho\bar{\gamma}_B}{\bar{\gamma}_B\lambda_{AP}}\right), \tag{11}$$

where $\Gamma(\cdot,\cdot)$ is the incomplete gamma function [12, Eq. (8.350.2)].

Proof: See Appendix A. ∎

B. SC/ZFB

Similar to the MRC scheme above, in this case, γ_{B_2} and γ_{E_2} are not statistically independent due to the presence of the common RV $G_1 = |h_{AP}|^2$ in P_{S_2}. Hence, we first give the conditional CDF of γ_{B_2} and the conditional PDF of γ_{E_2}, and we have

$$F_{\gamma_{B_2}}(x|G_1) = 1 - \sum_{n=1}^{N_B} \binom{N_B}{n} (-1)^{n-1} \exp\left(-\frac{nx}{\lambda_{AB}P_{S_2}/\sigma^2}\right). \tag{12}$$

Now, we proceed to derive the conditional PDF of γ_{E_2} in the following lemma.

Lemma 2. *The PDF of γ_{E_2} conditioned on the RV G_1 is given by*

$$f_{\gamma_{\text{E}_2}}(y|G_1) = \frac{1}{\lambda_{AE}P_{S_2}/\sigma^2} \exp\left(-\frac{y}{\lambda_{AE}P_{S_2}/\sigma^2}\right) \times \left(\frac{\lambda_{AE}P_{S_2}/\sigma^2}{P_Z/\sigma^2\lambda_{JE}y + \lambda_{AE}P_{S_2}/\sigma^2}\right)^{N_B-2} + \exp\left(-\frac{y}{\lambda_{AE}P_{S_2}/\sigma^2}\right) \times \frac{(N_B-2)\,P_Z/\sigma^2\lambda_{JE}\left(\lambda_{AE}P_{S_2}/\sigma^2\right)^{N_B-2}}{\left(P_Z/\sigma^2\lambda_{JE}y + \lambda_{AE}P_{S_2}/\sigma^2\right)^{N_B-1}}. \tag{13}$$

Proof: The proof will be presented in an extended journal version of this paper [13]. ∎

To this end, according to (12) and (13), we present the secrecy outage probability of multi-antenna cognitive radio networks using SC/ZFB with FD operation in the following key lemma.

Lemma 3. *The secrecy outage probability of multi-antenna cognitive radio systems, using SC/ZBF with FD operation can be given by*

$$P_{\text{out}}^{\text{SC/ZFB}}(R_{\text{S}}) = 1 - \sum_{n=1}^{N_B} \binom{N_B}{n} (-1)^{n-1} \exp\left(-\frac{n\left(2^{R_{\text{S}}}-1\right)}{\bar{\gamma}_B}\right) \times \left[1-\exp\left(-\frac{\rho}{\lambda_{AP}}\right)\right] \left[\frac{1}{\bar{\gamma}_Z}\Psi\left(1, 4-N_B; \frac{n2^{R_{\text{S}}}\bar{\gamma}_E+\bar{\gamma}_B}{\bar{\gamma}_B\bar{\gamma}_Z}\right) + (N_B-2)\,\Psi\left(1, 3-N_B; \frac{n2^{R_{\text{S}}}\bar{\gamma}_E+\bar{\gamma}_B}{\bar{\gamma}_B\bar{\gamma}_Z}\right)\right] - \sum_{n=1}^{N_B} \binom{N_B}{n} (-1)^{n-1} \frac{\rho\bar{\gamma}_B \exp\left(-\frac{n\left(2^{R_{\text{S}}}-1\right)\lambda_{\text{C}}+\rho\bar{\gamma}_B}{\lambda_{AP}\bar{\gamma}_B}\right)}{n\left(2^{R_{\text{S}}}-1\right)\lambda_{AP}+\rho\bar{\gamma}_B} \times \left[\frac{1}{\bar{\gamma}_Z}\Psi\left(1, 4-N_B; \frac{n2^{R_{\text{S}}}\bar{\gamma}_E+\bar{\gamma}_B}{\bar{\gamma}_B\bar{\gamma}_Z}\right) + (N_B-2)\,\Psi\left(1, 3-N_B; \frac{n2^{R_{\text{S}}}\bar{\gamma}_E+\bar{\gamma}_B}{\bar{\gamma}_B\bar{\gamma}_Z}\right)\right], \tag{14}$$

where $\Psi(\cdot,\cdot;\cdot)$ denotes the confluent hypergeometric function of the second kind [12, Eq. (9.211.4)].

Proof: Following similar procedure as in the proof of Lemma 1, the desired result can be obtained. ∎

Remark 1: In Lemmas 1 and 3, closed-form expressions for the secrecy outage probability of multi-antenna cognitive radio networks are presented, which provide an efficient means to evaluate the impact of different system parameters on the system performance. However, the derived expressions are in general complicated to gain more insights. Hence, in the following, we look into the high SNR regime, and analyze the asymptotic secrecy outage probability.

IV. High SNR Analysis

In this section, we focus on the asymptotic high SNR analysis. Specifically, we assume that $\bar{\gamma}_B \to \infty$ and fixed $\bar{\gamma}_E$, a scenario, where the main channel quality is much better than the eavesdropper channel, i.e., when the eavesdropper is located far away from Alice, or the eavesdropper channel is severely blocked due to heavy shadowing.

A. MRC

Corollary 1. *The secrecy outage probability for the MRC scheme when $\bar{\gamma}_B \to \infty$ can be approximated as*

$$P_{\text{out}}^{\text{MRC}}(R_{\text{S}}) \approx \Delta_{\text{MRC}}\bar{\gamma}_B^{-N_B}, \tag{15}$$

where Δ_{MRC} is given by

$$\Delta_{MRC} = \frac{2^{N_B R_{\text{S}}}}{N_B!\bar{\gamma}_E} \sum_{q=0}^{N_B} \binom{N_B}{q} \left(\frac{2^{R_{\text{S}}}-1}{2^{R_{\text{S}}}}\right)^{N_B-q} q!\bar{\gamma}_E^{q+1} \times \left[1-\exp\left(-\frac{\rho}{\lambda_{AP}}\right)\right] + \left(\frac{2^{R_{\text{S}}}}{\rho}\right)^{N_B} \frac{1}{N_B!\bar{\gamma}_E} \sum_{q=0}^{N_B} \binom{N_B}{q} \times \left(\frac{2^{R_{\text{S}}}-1}{2^{R_{\text{S}}}}\right)^{N_B-q} q!\bar{\gamma}_E^{q+1} \left(\frac{1}{\lambda_{AP}}\right)^{-N_B} \Gamma\left(N_B+1, \frac{\rho}{\lambda_{AP}}\right). \tag{16}$$

Proof: The proof will be presented in an extended journal version of this paper [13]. ∎

B. SC/ZFB

Corollary 2. *The secrecy outage probability for the SC/ZBF scheme under $\bar{\gamma}_B \to \infty$ can be approximated as*

$$P_{\text{out}}^{\text{SC/ZFB}}(R_{\text{S}})^{\infty} \approx \Delta_{\text{SC/ZFB}} \bar{\gamma}_B^{-N_B}, \tag{17}$$

where $\Delta_{\text{SC/ZFB}}$ is given by

$$\Delta_{\text{SC/ZFB}} = 2^{N_B R_{\text{S}}} (\Lambda_1 + \Lambda_2) \left[1 - \exp\left(-\frac{\rho}{\lambda_{AP}}\right)\right] + \left(\frac{2^{R_{\text{S}}}}{\rho}\right)^{N_B} (\Lambda_1 + \Lambda_2) \left(\frac{1}{\lambda_{AP}}\right)^{-N_B} \Gamma\left(N_B + 1, \frac{\rho}{\lambda_{AP}}\right), \tag{18}$$

with

$$\Lambda_1 = \sum_{q=0}^{N_B} \binom{N_B}{q} \left(\frac{2^{R_{\text{S}}} - 1}{2^{R_{\text{S}}}}\right)^{N_B - q} \frac{1}{\bar{\gamma}_E} \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_J}\right)^{q+1} \times \Gamma(q+1)\, \Psi\left(q+1, 4+q-N_B; \frac{1}{\bar{\gamma}_J}\right) \tag{19}$$

and

$$\Lambda_2 = \sum_{q=0}^{N_B} \binom{N_B}{q} \left(\frac{2^{R_{\text{S}}} - 1}{2^{R_{\text{S}}}}\right)^{N_B - q} \left(\frac{\bar{\gamma}_E}{\bar{\gamma}_J}\right)^{q} (N_B - 2) \times \Gamma(q+1)\, \Psi\left(q+1, 3+q-N_B; \frac{1}{\bar{\gamma}_J}\right). \tag{20}$$

Proof: The proof will be presented in an extended journal version of this paper [13]. ■

Remark 2: MRC and SC/ZFB achieve the same secrecy diversity, $G_d = N_B$, which is independent from the quality of the eavesdropper channel and the primary networks. However, the parameters of the eavesdropper channel and the primary networks affect the secrecy performance through the coding gain, i.e., $G_c = (\Delta_\star)^{-\frac{1}{N_B}}$, where $\star \in \{\text{MRC}, \text{SC/ZFB}\}$.

V. Numerical Results

In this section, we present representative numerical results to verify the analytical ones. Without loss of generality, we assume that the secrecy rate is $R_s = 2$, the noise variance is $\sigma^2 = 1$, and the SNR is $\frac{P_t}{\sigma^2}$. In addition, the average power of all the channel links is set to one. As shown in these figures, the analytical results are in exact agreement with the Monte Carlo simulations and the asymptotic curves remain sufficiently tight across the entire SNR range of interest, which validates the accuracy of the analytical expressions.

Figs. 1 and 2 illustrate the secrecy outage probability of the cognitive wiretap system with MRC and SC/ZFB schemes for different number of antennas N_B and different interference threshold Q, respectively. It is evident from the both figures that by increasing N_B the secrecy outage probability can be significantly reduced for the two schemes. This is rather intuitive since increasing N_B provides additional the secrecy diversity order or the secrecy coding gain. In addition, as can be seen, when the interference threshold Q at the PR is loose, i.e., for higher Q, the secrecy outage performance of the considered system can be substantially improved.

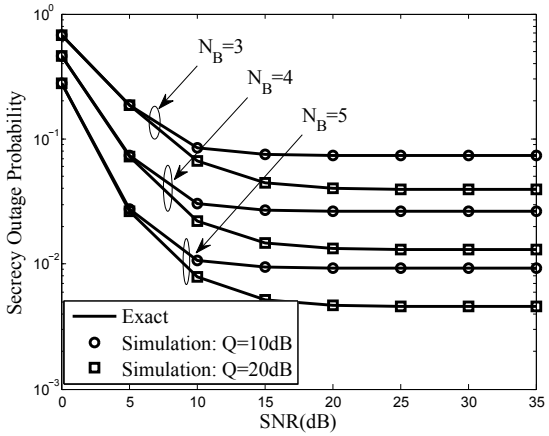

Fig. 1. Secrecy outage probability vs number of antennas for MRC scheme, where the interference threshold $Q = 10\text{dB}$ and $Q = 20\text{dB}$, respectively.

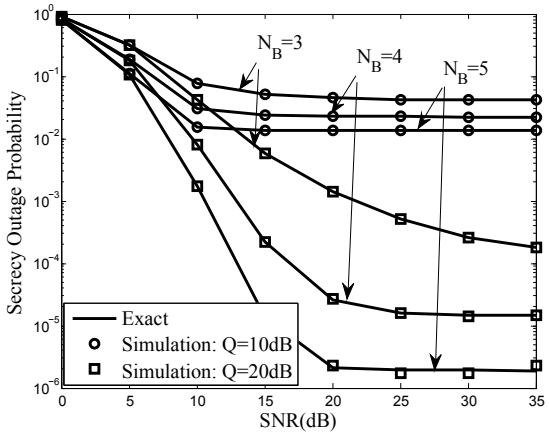

Fig. 2. Secrecy outage probability vs number of antennas for SC/ZFB scheme, where the interference threshold $Q = 10\text{dB}$ and $Q = 20\text{dB}$, respectively.

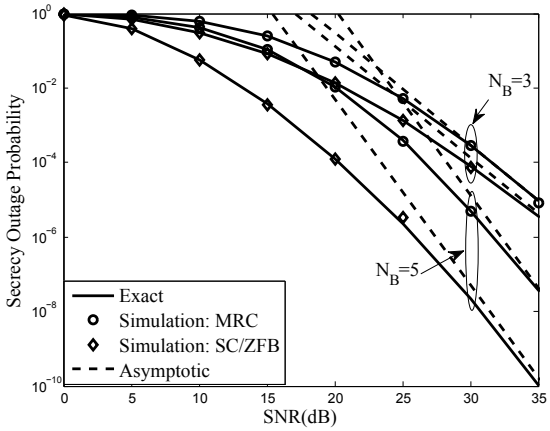

Fig. 3. Exact and asymptotic secrecy outage probabilities for MRC and SC/ZFB schemes, when $\rho = 1$ and $\bar{\gamma}_E = 10\text{dB}$, respectively.

Fig. 3 plots the secrecy outage probability versus SNR for the two proposed schemes when Bob is located close to Alice. It is observed that, both schemes achieve the same secrecy

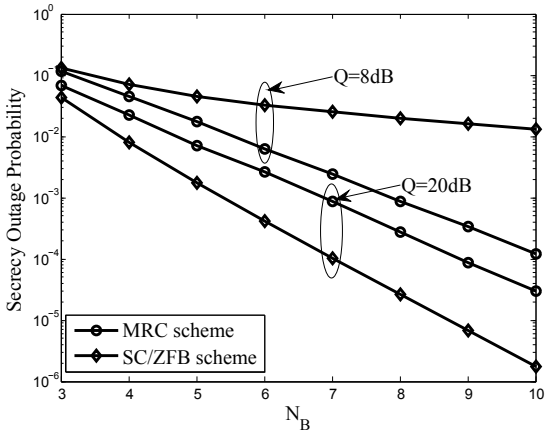

Fig. 4. Secrecy outage probabilities of MRC and SC/ZFB schemes versus the number of antennas of Bob when $P_t = 10$dB.

diversity of N_B. Furthermore, SC/ZFB always attains better performance than MRC, which indicates that the secrecy array gains are different from each other.

Fig. 4 illustrates the impact of antenna, N_B, on the secrecy outage performance of the two proposed schemes, respectively. It can be observed that the secrecy performance of the proposed schemes can be improved by increasing the number of antennas. Moreover, when the interference threshold is large, SC/ZFB achieves better performance than that of MRC. This can be explained by the fact that the higher Q means the loose requirement of PR, thus, the transmit power of jamming signal can be large. In addition, when the interference threshold Q is smaller, MRC with HD operation tends to outperform SC/ZFB with FD operation.

VI. Conclusions

In this paper, we have investigated the secrecy outage performance of multi-antenna cognitive radio systems over Rayleigh fading channels. To exploit the advantages of multiple antennas, we have proposed two secure transmission schemes with both HD and FD operations. Specifically, closed-form expressions for the secrecy outage probability of all the proposed schemes were derived. Moreover, simple and informative high SNR approximations for the secrecy outage probability were derived, which enables us to gain useful insights into the impact of key parameters on the secrecy performance. The findings of this paper suggest that the full diversity, i.e., N_B, can be achieved when quality of the main channel is much better than the eavesdropper channel.

Appendix A
Proof of Lemma 1

Substituting (9) and (10) into (8) and after some simple mathematical manipulations, the conditional secrecy outage probability can be expressed as

$$P_{\text{out}}^{\text{MRC}}(R_{\text{S}}|G_1) = \int_0^{\infty} F_{\gamma_{\text{B}_1}}\left(2^{R_{\text{S}}}(1+y)-1|G_1\right) f_{\gamma_{\text{E}_1}}(y|G_1)\, dy$$
$$= 1 - \sum_{k=0}^{N_{\text{B}}-1} \frac{1}{k!} \frac{1}{\left(P_{S_1}\lambda_{AB}/\sigma^2\right)^k} \frac{1}{P_{S_1}\lambda_{AE}/\sigma^2} \exp\left(-\frac{2^{R_{\text{S}}}-1}{P_{S_1}\lambda_{AB}/\sigma^2}\right)$$
$$\times \sum_{i=0}^{k} \binom{k}{i} \left(2^{R_{\text{S}}}-1\right)^{k-i} \left(2^{R_{\text{S}}}\right)^i i! \left(\frac{P_{S_1}\lambda_{AB}P_{S_1}\lambda_{AE}/\sigma^2}{2^{R_{\text{S}}}P_{S_1}\lambda_{AE}+P_{S_1}\lambda_{AB}}\right)^{i+1}. \tag{21}$$

Then, by averaging over G_1, the unconditional secrecy outage probability can be expressed as

$$P_{\text{out}}^{\text{MRC}}(R_{\text{S}}) = \int_0^{\infty} P_{\text{out}}^{\text{MRC}}(R_{\text{S}}|G_1) f_{G_1}(g)\, dg. \tag{22}$$

To this end, substituting the PDF of G_1 into (22) and utilizing the equality [12, Eq. (3.381.4)], the desired result can be derived after some algebraic manipulations.

Acknowledgment

This work is supported by the Project of Natural Science Foundations of China (No. 61501507, 61471393, 61301162 and 61301163) and the Jiangsu Provincial Natural Science Foundation of China (No. BK20150719 and BK20130067).

References

[1] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," *Ph. D. dissertation,* Royal Inst. Technol. (KTH), Stockholm, Sweden, Dec. 2000.

[2] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[3] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Communications*, vol. 6, no. 16, pp. 2676-2687, 2012.

[4] H. Jeon, S. W. McLaughlin, and J. Ha, "Secure communications with untrusted secondary users in cognitive radio networks," *in Proc. of IEEE GLOBECOM*, pp. 1072-1078, 2012.

[5] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509-511, May 2011.

[6] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and outage secrecy capacity," *IEEE Trans. Inf. Forensics Security,* vol. 6, no. 3, pp. 853-860, Sep. 2011.

[7] 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.

[8] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962-4974, Oct. 2013.

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

[10] A. Basilevsky, *Applied Matrix Algebra in the Statistical Sciences*. New York: North-Holland, 1983.

[11] H. Ju, E. Oh, and D. Hong, "Improving efficiency of resource usage in two-hop full duplex relay systems based on resource sharing and interference cancellation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3933-3938, Aug. 2009.

[12] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.

[13] T. Zhang, Y. Huang, Y. Cai, C. Zhong, W. Yang, and G. K. Karagiannidis, "Secure transmission in multi-antenna cognitive wiretap metworks," submitted for *IEEE Trans. Inf. Forensics Security*.