Secure Multiantenna Cognitive Wiretap Networks

Tao Zhang, *Student Member, IEEE*, Yuzhen Huang, *Member, IEEE*, Yueming Cai, *Senior Member, IEEE*, Caijun Zhong, *Senior Member, IEEE*, Weiwei Yang, *Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—In this paper, we investigate the secrecy performance of a multiantenna cognitive wiretap network, where the secondary transmitter (Alice) communicates with the secondary receiver (Bob) in the presence of an eavesdropper (Eve). Specifically, we consider both half-duplex (HD) and full-duplex (FD) operations. For the HD, maximal-ratio combining (MRC) is adopted at Bob, while for the FD, we propose two jamming schemes to deteriorate the quality of the eavesdropper's channel, i.e., selection combining/selection jammer (SC/SJ) and SC/zero forcing beamforming (SC/ZFB). Assuming Rayleigh fading, exact closed-form expressions for the secrecy outage probability of the cognitive wiretap network are derived. In addition, we also provide simple asymptotic approximations for the secrecy outage probability under two distinct scenarios, depending on the quality of the main and wiretap channels. From the analytical results and numerical simulations, it is concluded that all the proposed schemes outperform the SC scheme; all the proposed schemes achieve full diversity when the main channel is much better than the eavesdropper's channel; MRC outperforms SC/SJ and SC/ZBF in the low interference threshold regime, while the opposite holds in the high interference one; and SC/ZFB always achieves better performance than SC/SJ, albeit with higher complexity.**

***Index Terms*—Cognitive radio, full duplex (FD), multiple antennas, physical layer security.**

Manuscript received March 24, 2016; revised June 12, 2016 and July 31, 2016; accepted September 11, 2016. Date of publication September 14, 2016; date of current version May 12, 2017. This work was supported in part by the National Science Foundations of China under Grant 61471393, Grant 61501507, Grant 61371122, Grant 61671406, and Grant 61501512 and in part by the Jiangsu Provincial Natural Science Foundation of China under Grant BK20150719 and Grant BK20150718. The work of G. K. Karagiannidis was supported in part by the European Social Fund-ESF and in part by the Greek National Funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework Research Funding Program: THALESNTUA MIMOSA. This paper was presented in part at the IEEE 83rd Vehicular Technology Conference (VTC2016-Spring), Nanjing, China, May 2016. The review of this paper was coordinated by Dr. S. Sun.

T. Zhang is with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China, and also with Nanjing Telecommunication Technology Institute, Nanjing 210007, China (e-mail: ztcool@126.com).

Y. Cai, and W. Yang are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail: caiym@vip.sina.com; wwyang1981@163.com).

Y. Huang is with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 21007, China, and also with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: yzh_huang@sina.com).

C. Zhong is with the Institute of Information and Communication Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: caijunzhong@zju.edu.cn).

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54 124, Thessaloniki, Greece (e-mail: geokarag@auth.gr).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2016.2609396

I. Introduction

COGNITIVE radio, which is an effective framework to alleviate the spectrum shortage problem, has received considerable interests from the research community in recent years [1]–[3]. In spectrum sharing cognitive radio networks (CRNs), secondary users (SUs) are allowed to access the licensed spectrum as long as the interference on the primary user (PU) does not exceed the *interference temperature limit*. Extensive research efforts were made to investigate the information theoretic performance of spectrum sharing CRNs, such as outage probability [3], symbol error rate [4], and ergodic capacity [5]. To implement CRNs in practice, a number of challenging issues, including security, need to be addressed. Due to the open and dynamic features, CRNs are vulnerable to various malicious attacks, making secure communications to be a difficult task. In parallel, a physical layer security technique has emerged as a promising solution to provide perfect secrecy for data transmission [6]. Motivated by this, several works have investigated the security issues of CRNs from a physical layer perspective. In [7], Pei *et.al* designed a robust transmitter for secure transmission in CRNs. In [8], different relay selection schemes were proposed to enhance the security of CRNs, where the best relay was selected taking into account both the peak interference power constraint at PU and the maximal transmit power constraint at SU. In [9], the secure transmission of CRNs with the untrusted SUs was investigated and closed-form expressions for the achievable secrecy rate were presented.

For further secrecy enhancement, various techniques have been proposed, for instance, the multiantenna and full-duplex (FD) transmission. The secrecy performance of multiantenna 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 selection combining (SC) scheme at the legitimate receiver [10], the impact of multiple eavesdroppers [11], the transmit antenna selection for multiple-input multiple-output (MIMO) wiretap channels with different receiver combining schemes [12]–[14] and the effect of antenna correlation on the secrecy outage performance [15]. In addition, the idea of employing the FD technique to improve the security by sending a jamming signal to degrade the quality of eavesdropper's channel was analyzed in [16]. Later, in [17], a cooperative secrecy transmission scheme in noncognitive wiretap network has been investigated, where a FD Bob not only receives the signal from Alice but sends a jamming signal at the same time as well. However, to the best of the authors' knowledge, no works have considered the application of FD operation in CRNs with multiple antennas for secrecy improvement.

Motivated by the above, we consider a multiantenna CRNs, where a secondary transmitter (Alice) communicates with a secondary destination (Bob), equipped with multiple antennas in the presence of a primary receiver (PR) and an eavesdropper (Eve). Both half-duplex (HD) and FD operations are assumed at Bob, respectively. Specifically, for the HD operation, the Bob employs maximal-ratio combining (MRC) to strengthen the signal detection, while for the FD operation, two different secure transmission schemes are proposed: 1) SC/selection jammer (SC/SJ) scheme, where the Bob first selects the best antenna to recover the data from the Alice, and then utilizes one of the remaining antennas to transmit the jamming signal at the same time, 2) SC/zero-forcing beamforming (SC/ZFB) scheme, where the Bob also selects the best antenna to recover the data from the Alice and use all the remaining antennas to send the jamming signal according to the principle of ZFB. It is worth noting that, in [10], the secrecy outage performance of multiantenna CRNs with an SC scheme has been investigated. However, it neglected the effect of correlation due to the interference link between Alice and PR on the secrecy performance. In addition, only HD operation was considered. Different from [10], this paper considers a more general system model taking into account this correlation. The main contributions of this paper are summarized as follows.

1) We first derive a closed-form expression for the secrecy outage probability of multiantenna cognitive radio HD networks with MRC, which provides an efficient means to evaluate the impact of key system parameters on the secrecy performance of cognitive wiretap channels. To gain more insights, we present an asymptotic secrecy diversity analysis in the high signal-to-noise ratio (SNR) regime under two scenarios: Scenario I–The legitimate receiver is located close to the transmitter. Scenario II–The legitimate receiver and the eavesdropper are both located close to the transmitter. Based on the analytical results, we find that the secrecy diversity order is significantly affected by the distance between the Alice and the eavesdropper.
2) We derive new closed-form expressions for the secrecy outage probability of multiantenna cognitive radio FD networks with the operation of FD at Bob, under two different transmission schemes, i.e., SC/SJ and SC/ZFB. Moreover, for both schemes, the asymptotic secrecy diversity gain is investigated, which reveals that both SC/SJ and SC/ZFB can achieve full secrecy diversity under Scenario I and zero secrecy diversity under Scenario II.
3) The results demonstrate the intuition that increasing the number of antennas improves the secrecy performance of all the proposed schemes. Moreover, MRC tends to outperform SC/SJ and SC/ZFB when the constraint of the interference threshold at PR is stringent. However, when the interference temperature constraint becomes loose, both SC/SJ and SC/ZFB achieve better performance than MRC, and they gradually approach the performance of conventional noncognitive wiretap networks, i.e., no interference temperature constraint scenario. In addition, the secrecy performance of SC/ZFB is superior to that of SC/SJ, and the performance gap becomes large with the increase of antenna numbers at Bob.

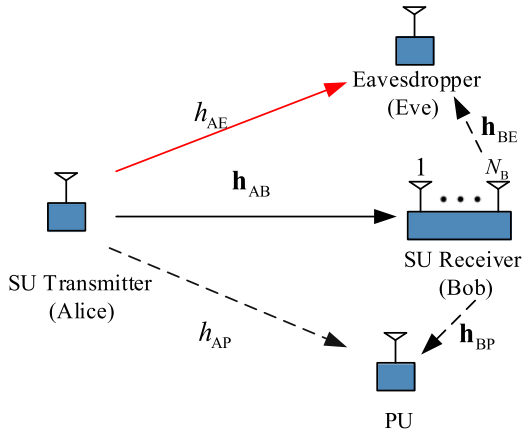


Fig. 1. System model.

The rest of the paper is organized as follows. The system model is introduced in Section II. Section III formulates the problem and presents a set of new analytical expressions for the secrecy outage performance. In Section IV, we provide a high SNR analysis for the secrecy outage probability. Section V presents the numerical results and discussions. Finally, Section VI concludes the paper and summarizes the key findings.

II. System Model

Let us consider a multiantenna cognitive wiretap channel, as shown in Fig. 1, which consists of a secondary transmitter (Alice), a secondary receiver (Bob), a primary receiver (PR), and an eavesdropper (Eve). Similar to [10] and [18], the considered scenario can be regarded as a uplink network, where all users are equipped with a single antenna, except that base station (BS), i.e., Bob, has N_{B} antennas. Throughout this paper, the following assumptions are adopted.

1) Similar to [3], [10], and [19], 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.
2) Without loss of generality, the main and wiretap channels are assumed to be quasi-static independent and nonidentical fading channels, following the Rayleigh distribution. The corresponding channel power gain between the nodes K and T is denoted as $|h_{\mathrm{KT}}|^2$, which is an exponentially distributed random variable (RV) with variance λ_{KT}.
3) Similar to [17], [20], and [21], all channel state information (CSI) is known at Bob, i.e., the CSI of Eve to Bob link[1] and the CSI of Alice to Bob link.

To exploit the advantages of multiple antennas, we consider three different secure transmission schemes, i.e., MRC with HD operation, SC/SJ with FD operation, and SC/ZFB with FD operation. For MRC with HD scenario, Bob adopts the MRC to strengthen the signal detection, and thus, the instantaneous

[1]This case is applicable in the multicast and unicast networks where the users play dual roles as legitimate ones for transmitting and receiving nonconfidential information and eavesdroppers for other confidential information [17], [22].

SNR between Alice and Bob is given by

$$\gamma_{\mathrm{B}_1} = \frac{P_{S_1}}{\sigma^2} \|\mathbf{h}_{\mathrm{AB}}\|^2 \tag{1}$$

where $\mathbf{h}_{\mathrm{AB}}$ is an $N_{\mathrm{B}} \times 1$ 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 [3]

$$P_{S_1} = \min\left(\frac{Q}{|h_{\mathrm{AP}}|^2}, P_t\right) \tag{2}$$

where P_t is the maximum transmit power constraint at Alice and Q denotes the interference temperature constraint at the PU. In addition, h_{AP} is the channel coefficient between Alice and PR, which can be obtained through a spectrum-band manager that mediates between the licensed and unlicensed users [23].

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

$$\gamma_{\mathrm{E}_1} = \frac{P_{S_1}}{\sigma^2} |h_{\mathrm{AE}}|^2 \tag{3}$$

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

For SC/SJ with FD operation, Bob first selects the best antenna based on the CSI of the main channel, and utilizes the best antenna in the remaining $N_{\mathrm{B}} - 1$ antennas to send the jamming signal, based on the channel between Bob and Eve, in which only one of the antennas at Bob is selected to send the jamming not all antennas due to the lower computational load of implementation. Hence, the instantaneous SNR at Bob and the instantaneous signal-to-interference-plus-noise ratio (SINR) at Eve, when SC/SJ is assumed, are, respectively, given by[2]

$$\gamma_{\mathrm{B}_2} = \frac{P_{S_2}}{\sigma^2} \max_{1 \le i \le N_{\mathrm{B}}} \left(|h_{\mathrm{AB}i}|^2\right) \tag{4}$$

and

$$\gamma_{\mathrm{E}_2} = \frac{P_{S_2}|h_{\mathrm{AE}}|^2}{P_B \max\limits_{1 \le j \le N_{\mathrm{B}}-1} \left(|h_{\mathrm{B}j\mathrm{E}}|^2\right) + \sigma^2} \tag{5}$$

where $h_{\mathrm{AB}i}$ denotes the channel coefficient between Alice and the ith antenna of Bob, and $h_{\mathrm{B}j\mathrm{E}}$ is the channel coefficient between the jth antenna of Bob and the Eve. Please note that, in order to meet the interference temperature constraint, the aggregate interference power at PR from Alice and Bob should satisfy the following inequality:

$$P_{S_2}|h_{\mathrm{AP}}|^2 + P_B|h_{\mathrm{B}j^*\mathrm{P}}|^2 \le Q \tag{6}$$

where j^* is the index of the selected antenna in the remaining $N_{\mathrm{B}} - 1$ antennas, and $h_{\mathrm{B}j^*\mathrm{P}}$ is the channel coefficient between the selected antenna of Bob and PR, which can also be obtained through a spectrum-band manager, as in [23]. In order to make the analysis tractable, we assume that the transmit powers of P_{S_2} and P_B are equal.[3] Therefore

$$P_{S_2} = \min\left(\frac{Q}{|h_{\mathrm{AP}}|^2 + |h_{\mathrm{B}j^*\mathrm{P}}|^2}, P_t\right) \tag{7}$$

and

$$P_B = \min\left(\frac{Q}{|h_{\mathrm{AP}}|^2 + |h_{\mathrm{B}j^*\mathrm{P}}|^2}, P_t\right). \tag{8}$$

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

$$\begin{aligned} &\max_{\mathbf{w}_{\mathrm{ZF}}} \left|\mathbf{h}_{\mathrm{BE}}^{\dagger}\mathbf{w}_{\mathrm{ZF}}\right| \\ &s.t. \ \left|\mathbf{h}_{\mathrm{BP}}^{\dagger}\mathbf{w}_{\mathrm{ZF}}\right| = 0 \ \& \ \|\mathbf{w}_{\mathrm{ZF}}\|_F = 1 \end{aligned} \tag{9}$$

where $\dagger$ is the conjugate transpose operator and $\|\cdot\|_F$ denotes the Frobenius norm, $\mathbf{h}_{\mathrm{BE}}$ and $\mathbf{h}_{\mathrm{BP}}$ denote the $(N_{\mathrm{B}} - 1) \times 1$ channel vectors between the remaining $N_{\mathrm{B}} - 1$ antennas of the Bob and the Eve, and the remaining $N_{\mathrm{B}} - 1$ antennas of the Bob and the PR, respectively. Now, using the projection matrix theory [31], the optimal weight vector can be obtained as

$$\mathbf{w}_{\mathrm{ZF}} = \frac{\mathrm{T}^{\perp}\mathbf{h}_{\mathrm{BE}}}{\|\mathrm{T}^{\perp}\mathbf{h}_{\mathrm{BE}}\|} \tag{10}$$

where $\mathrm{T}^{\perp} = \left(\mathbf{I} - \mathbf{h}_{\mathrm{BP}}\left(\mathbf{h}_{\mathrm{BP}}^{\dagger}\mathbf{h}_{\mathrm{BP}}\right)^{-1}\mathbf{h}_{\mathrm{BP}}^{\dagger}\right)$ is the projection idempotent matrix with rank $N_{\mathrm{B}} - 2$. As a result, the instantaneous SNR of the main and the instantaneous SINR of the wiretap channels, respectively, can be expressed as

$$\gamma_{\mathrm{B}_3} = \frac{P_{S_3}}{\sigma^2} \max_{1 \le i \le N_{\mathrm{B}}} \left(|h_{\mathrm{AB}i}|^2\right) \tag{11}$$

and

$$\gamma_{\mathrm{E}_3} = \frac{P_{S_3}|h_{\mathrm{AE}}|^2}{P_Z\left|\mathbf{h}_{\mathrm{BE}}^{\dagger}\mathbf{w}_{\mathrm{ZF}}\right|^2 + \sigma^2} \tag{12}$$

where the transmit power of Alice P_{S_3} is the same in (2), and P_Z denotes the power of the jamming signal from Bob. Notice that different from P_B, the jamming power P_Z will not be affected by the interference threshold Q; hence, it can take the maximum transmit power constraint in practice to maximize the secrecy performance.

As mentioned in [32], the achievable secrecy rate of the multiantenna cognitive wiretap channels is given by

$$C_S = \begin{cases} C_{\mathrm{B}_i} - C_{\mathrm{E}_i}, & \gamma_{\mathrm{B}_i} > \gamma_{\mathrm{E}_i} \\ 0, & \gamma_{\mathrm{B}_i} \le \gamma_{\mathrm{E}_i} \end{cases} \tag{13}$$

[2]Note that for the FD mechanism, we assume that the self-interference can be completely suppressed at Bob. As in [17] and [24]–[29], this assumption is widely used to study the information theoretic oriented performance, i.e., outage probability and capacity. Although full cancelation of self-interference cannot be achieved even with the help of state-of-the-art techniques in [30].

[3]Since the main purpose of this work is to investigate the impact of HD and FD mechanism on the secrecy performance of multiantenna cognitive wiretap channels, it suffices to consider the equal power scenario. For the general distinct P_{S_2} and P_B scenario, we leave it as a future work.

where $i = \{1, 2, 3\}$ represents MRC, SC/SJ, and SC/ZFB, respectively, $C_{\mathrm{B}_i} = \log_2(1 + \gamma_{\mathrm{B}_i})$ and $C_{\mathrm{E}_i} = \log_2(1 + \gamma_{\mathrm{E}_i})$ are the achievable instantaneous rates at Bob and Eve, respectively.

For the reader's convenience, we define $\rho = \frac{Q}{P_t}$, $\bar{\gamma}_{\mathrm{B}} = \frac{P_t}{\sigma^2}\lambda_{\mathrm{AB}} = \frac{Q}{\rho\sigma^2}\lambda_{\mathrm{AB}}$, $\bar{\gamma}_{\mathrm{E}} = \frac{P_t}{\sigma^2}\lambda_{\mathrm{AE}} = \frac{Q}{\rho\sigma^2}\lambda_{\mathrm{AE}}$, $\bar{\gamma}_{\mathrm{J}} = \frac{P_t}{\sigma^2}\lambda_{\mathrm{BE}} = \frac{Q}{\rho\sigma^2}\lambda_{\mathrm{BE}}$, and $\bar{\gamma}_{\mathrm{Z}} = \frac{P_Z}{\sigma^2}\lambda_{\mathrm{BE}}$.

III. Secrecy Performance Analysis

In this section, we investigate the secrecy outage performance of the cognitive wiretap systems with the proposed secure transmission schemes. In [33], 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 [33]

$$P_{\mathrm{out}}(R_{\mathrm{S}}) = \Pr(C_S < R_{\mathrm{S}}) = \int_0^\infty F_{\gamma_{\mathrm{B}_i}}\left(2^{R_{\mathrm{S}}}(1+x)-1\right) f_{\gamma_{\mathrm{E}_i}}(x)\,dx. \quad (14)$$

Next, we present a detail analysis for the secrecy outage probability of multiantenna cognitive wiretap channels with the MRC, SC/SJ, and SC/ZFB, respectively.

A. MRC Scheme

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 RV, $G_1 = |h_{\mathrm{AP}}|^2$, in P_{S_1}. To tackle this problem, we adopt the condition-and-average approach. Specifically, 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's channel conditioned on the RV G_1, respectively.

According to (1) and with the help of [34], the conditional CDF of γ_{B_1} is given by

$$F_{\gamma_{\mathrm{B}_1}}(x|G_1) = 1 - e^{-\frac{\sigma^2 x}{P_{S_1}\lambda_{\mathrm{AB}}}} \sum_{k=0}^{N_{\mathrm{B}}-1} \frac{1}{k!}\left(\frac{\sigma^2 x}{P_{S_1}\lambda_{\mathrm{AB}}}\right)^k. \quad (15)$$

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

$$f_{\gamma_{\mathrm{E}_1}}(y|G_1) = \frac{\sigma^2}{P_{S_1}\lambda_{\mathrm{AE}}} \exp\left(-\frac{\sigma^2 y}{P_{S_1}\lambda_{\mathrm{AE}}}\right). \quad (16)$$

Lemma 1: The secrecy outage probability of multiantenna CRNs employing MRC with HD operation is given by

$$P_{\mathrm{out}}^{\mathrm{MRC}}(R_{\mathrm{S}}) = \left[1 - \sum_{k=0}^{N_{\mathrm{B}}-1} \frac{1}{k!}\frac{1}{(\bar{\gamma}_{\mathrm{B}})^k}\frac{1}{\bar{\gamma}_{\mathrm{E}}} \exp\left(-\frac{2^{R_{\mathrm{S}}}-1}{\bar{\gamma}_{\mathrm{B}}}\right) \times \sum_{i=0}^{k}\binom{k}{i}\left(2^{R_{\mathrm{S}}}-1\right)^{k-i}\left(2^{R_{\mathrm{S}}}\right)^i i! \left(\frac{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{E}}}{2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}} + \bar{\gamma}_{\mathrm{B}}}\right)^{i+1}\right] \times \left[1 - \exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right)\right] + \exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right) - \sum_{k=0}^{N_{\mathrm{B}}-1} \frac{1}{k!\left(\rho\bar{\gamma}_{\mathrm{B}}\right)^k \rho\bar{\gamma}_{\mathrm{E}}} \times \sum_{i=0}^{k}\binom{k}{i}\left(2^{R_{\mathrm{S}}}-1\right)^{k-i}\left(2^{R_{\mathrm{S}}}\right)^i \left(\frac{\rho\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{E}}}{2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}} + \bar{\gamma}_{\mathrm{B}}}\right)^{i+1} \frac{i!}{\lambda_{\mathrm{AP}}} \times \left(\frac{\rho\bar{\gamma}_{\mathrm{B}}\lambda_{\mathrm{AP}}}{(2^{R_{\mathrm{S}}}-1)\lambda_{\mathrm{AP}} + \rho\bar{\gamma}_{\mathrm{B}}}\right)^{k-i+1} \Gamma\left(k-i+1, \frac{\left(2^{R_{\mathrm{S}}}-1\right)\lambda_{\mathrm{AP}} + \rho\bar{\gamma}_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}\lambda_{\mathrm{AP}}}\right) \quad (17)$$

where $\Gamma(\cdot,\cdot)$ is the incomplete gamma function [35, eq. (8.350.2)].

Proof: See Appendix A.

B. SC/SJ Scheme

Similar to MRC, γ_{B_2} and γ_{E_2} are statistically dependent due to the existence of the common RV $G_2 = |h_{\mathrm{AP}}|^2 + |h_{\mathrm{B}j^*\mathrm{P}}|^2$. As such, we first seek the conditional CDF of γ_{B_2} and the conditional PDF of γ_{E_2}.

Utilizing (4) and after some algebraic manipulations, the conditional CDF of γ_{B_2} can be written as

$$F_{\gamma_{\mathrm{B}_2}}(x|G_2) = \left[1 - \exp\left(-\frac{\sigma^2 x}{P_{S_2}\lambda_{\mathrm{AB}}}\right)\right]^{N_{\mathrm{B}}} = 1 - \sum_{n=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{n}(-1)^{n-1}\exp\left(-\frac{\sigma^2 n x}{P_{S_2}\lambda_{\mathrm{AB}}}\right). \quad (18)$$

Lemma 2: The PDF of γ_{E_2} conditioned on the RV G_2 is given by

$$f_{\gamma_{\mathrm{E}_2}}(y|G_2) = \sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1}\exp\left(-\frac{\sigma^2 y}{P_{S_2}\lambda_{\mathrm{AE}}}\right) \times \frac{m P_{S_2}\lambda_{\mathrm{AE}} P_B \lambda_{\mathrm{JE}}}{(m P_{S_2}\lambda_{\mathrm{AE}} + P_B\lambda_{\mathrm{JE}} y)^2} + \sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m} \times \frac{(-1)^{m-1} m\sigma^2}{m P_{S_2}\lambda_{\mathrm{AE}} + P_B\lambda_{\mathrm{JE}} y}\exp\left(-\frac{\sigma^2 y}{P_{S_2}\lambda_{\mathrm{AE}}}\right). \quad (19)$$

Proof: See Appendix B. ∎

Armed with (18) and (19), we now give the secrecy outage probability of multiantenna CRNs using the SC/SJ scheme with the FD mechanism in the following lemma.

Lemma 3: The secrecy outage probability of multiantenna CRNs using SC/SJ with FD is given by

$$P_{\mathrm{out}}^{\mathrm{SC/SJ}}(R_{\mathrm{S}}) = 1 - \sum_{n=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{n}(-1)^{n-1}\sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1} I_1 - \sum_{n=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{n}(-1)^{n-1}\sum_{m=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1} I_2 \quad (20)$$

where

$$I_1 = \left[1 - \exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right) - \frac{\rho}{\lambda_{\rm AP}} \exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)\right] \times \exp\left(-\frac{n\left(2^{R_{\rm S}}-1\right)}{\bar{\gamma}_{\rm B}}\right)\left[1 + \frac{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm E}} \times \exp\left(\frac{\left(n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}\right)m}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm J}}\right){\rm Ei}\left(-\frac{\left(n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}\right)m}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm J}}\right)\right] + \sum_{k=0}^{1}\frac{(b\rho)^{2-k}\rho^k c}{\left(\lambda_{\rm AP}\right)^2}\left[\sum_{i=0}^{1-k}\binom{1+i}{i}\mu^{2+i}\left(\frac{1}{a}\right)^{1-k-i}\Psi\left(1,k+i;\frac{a}{b}\right) + \sum_{j=0}^{1}\binom{1-k+j}{j}(-1)^{2-k}\nu^{2-k+j}\left(\frac{1}{c}\right)^{1-j}\Psi\left(1,j;\frac{c}{b}\right)\right] \quad (21)$$

and

$$I_2 = \left[1-\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)-\frac{\rho\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)}{\lambda_{\rm AP}}\right]\exp\left(-\frac{n\left(2^{R_{\rm S}}-1\right)}{\bar{\gamma}_{\rm B}}\right) \times \left[-\frac{m}{\bar{\gamma}_{\rm J}}\exp\left(\frac{\left(n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}\right)m}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm J}}\right){\rm Ei}\left(-\frac{\left(n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}\right)m}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm J}}\right)\right] + \exp\left(-\frac{a}{b}\right)\frac{m}{\rho\bar{\gamma}_{\rm J}}\sum_{k=0}^{2}\frac{2}{k!}\frac{(b\rho)^{3-k}\rho^k}{\left(\lambda_{\rm AP}\right)^2}\left[(-\nu)^{3-k}\Psi\left(1,1;\frac{c}{b}\right) + \sum_{t=0}^{2-k}(-1)\,\mu^{1+t}\left(\frac{1}{a}\right)^{2-k-t}\Psi\left(1,k+t-1;\frac{a}{b}\right)\right] \quad (22)$$

with ${\rm Ei}(\cdot)$ being the exponential integral function [35, eq. (8.211.1)] and $\Psi(\cdot,\cdot;\cdot)$ being the confluent hypergeometric function of the second kind [35, eq. (9.211.4)], respectively.

Proof: See Appendix C. ■

C. SC/ZFB Scheme

Similar to MRC, in this case, $\gamma_{{\rm B}_3}$ and $\gamma_{{\rm E}_3}$ are not statistically independent due to the presence of the common RV $G_1 = |h_{\rm AP}|^2$ in P_{S_3}. Hence, we first give the conditional CDF of $\gamma_{{\rm B}_3}$ and the conditional PDF of $\gamma_{{\rm E}_3}$, and we have

$$F_{\gamma_{{\rm B}_3}}(x|G_1) = 1 - \sum_{n=1}^{N_{\rm B}}\binom{N_{\rm B}}{n}(-1)^{n-1}\exp\left(-\frac{\sigma^2 n x}{P_{S_3}\lambda_{\rm AB}}\right). \quad (23)$$

In the following lemma, we derive the conditional PDF of $\gamma_{{\rm E}_3}$.

Lemma 4: The PDF of $\gamma_{{\rm E}_3}$ conditioned on the RV G_1 is given by

$$f_{\gamma_{{\rm E}_3}}(y|G_1) = \frac{\sigma^2}{P_{S_3}\lambda_{\rm AE}}\exp\left(-\frac{\sigma^2 y}{P_{S_3}\lambda_{\rm AE}}\right) \times \left(\frac{P_{S_3}\lambda_{\rm AE}}{P_Z\lambda_{\rm JE}y + P_{S_3}\lambda_{\rm AE}}\right)^{N_{\rm B}-2} + \exp\left(-\frac{\sigma^2 y}{P_{S_3}\lambda_{\rm AE}}\right) \times \frac{(N_{\rm B}-2)\,P_Z\lambda_{\rm JE}\left(P_{S_3}\lambda_{\rm AE}\right)^{N_{\rm B}-2}}{\left(P_Z\lambda_{\rm JE}y + P_{S_3}\lambda_{\rm AE}\right)^{N_{\rm B}-1}}. \quad (24)$$

Proof: See Appendix D. ■

To this end, according to (23) and (24), we can present the secrecy outage probability of multiantenna CRNs using SC/ZFB with FD operation in the following key lemma.

Lemma 5: The secrecy outage probability of multiantenna CRNs using SC/ZBF with FD operation can be given by

$$P_{\rm out}^{\rm SC/ZFB}(R_{\rm S}) = 1 - \sum_{n=1}^{N_{\rm B}}\binom{N_{\rm B}}{n}(-1)^{n-1}\exp\left(-\frac{n\left(2^{R_{\rm S}}-1\right)}{\bar{\gamma}_{\rm B}}\right) \times \left[1-\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)\right]\left[\frac{1}{\bar{\gamma}_{\rm Z}}\Psi\left(1,4-N_{\rm B};\frac{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm Z}}\right) + (N_{\rm B}-2)\,\Psi\left(1,3-N_{\rm B};\frac{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm Z}}\right)\right] - \sum_{n=1}^{N_{\rm B}}\binom{N_{\rm B}}{n}(-1)^{n-1}\frac{\rho\bar{\gamma}_{\rm B}\exp\left(-\frac{n\left(2^{R_{\rm S}}-1\right)\lambda_{\rm AP}+\rho\bar{\gamma}_{\rm B}}{\lambda_{\rm AP}\bar{\gamma}_{\rm B}}\right)}{n\left(2^{R_{\rm S}}-1\right)\lambda_{\rm AP}+\rho\bar{\gamma}_{\rm B}} \times \left[\frac{1}{\bar{\gamma}_{\rm Z}}\Psi\left(1,4-N_{\rm B};\frac{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm Z}}\right) + (N_{\rm B}-2)\,\Psi\left(1,3-N_{\rm B};\frac{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm Z}}\right)\right]. \quad (25)$$

Proof: See Appendix E. ■

In lemmas 1, 3, and 5, closed-form expressions for the secrecy outage probability of multiantenna CRNs are presented, which provide an efficient means to evaluate the impact of different system parameters on the secrecy performance of multiantenna cognitive wiretap channels. 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 Signal-to-Noise Ratio Analysis

In this section, we focus on the asymptotic high SNR analysis. Specifically, two separate scenarios are studied: 1) $\bar{\gamma}_{\rm B} \to \infty$ and fixed $\bar{\gamma}_{\rm E}$, which is a scenario where the main channel quality is much better than the eavesdropper's channel, i.e., when the eavesdropper is located far away from Alice, or the eavesdropper's channel is severely blocked due to heavy shadowing. 2) $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E} \to \infty$, which is a scenario where both the main channel and eavesdropper's channel experience similar fading conditions.

A. Scenario I: $\bar{\gamma}_{\rm B} \to \infty$ and Fixed $\bar{\gamma}_{\rm E}$

1) MRC Scheme:

Corollary 1: The secrecy outage probability for MRC under $\bar{\gamma}_{\rm B} \to \infty$ and fixed $\bar{\gamma}_{\rm E}$ can be approximated as

$$P_{\rm out}^{\rm MRC}(R_{\rm S}) \approx \Delta_{\rm MRC}\bar{\gamma}_{\rm B}^{-N_{\rm B}} \quad (26)$$

where Δ_{MRC} is given by

$$\Delta_{\mathrm{MRC}} = \frac{2^{N_{\mathrm{B}}R_{\mathrm{S}}}}{N_{\mathrm{B}}!\bar{\gamma}_{\mathrm{E}}}\sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q} q!\bar{\gamma}_{\mathrm{E}}^{q+1} \times \left[1-\exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right)\right] + \left(\frac{2^{R_{\mathrm{S}}}}{\rho}\right)^{N_{\mathrm{B}}}\frac{1}{N_{\mathrm{B}}!\bar{\gamma}_{\mathrm{E}}}\sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q} \times \left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q} q!\bar{\gamma}_{\mathrm{E}}^{q+1}\left(\frac{1}{\lambda_{\mathrm{AP}}}\right)^{-N_{\mathrm{B}}}\Gamma\left(N_{\mathrm{B}}+1,\frac{\rho}{\lambda_{\mathrm{AP}}}\right). \tag{27}$$

Proof: See Appendix F. ■

2) SC/SJ Scheme:

Corollary 2: The secrecy outage probability for SC/SJ under $\bar{\gamma}_{\mathrm{B}} \to \infty$ and fixed $\bar{\gamma}_{\mathrm{E}}$ can be approximated as

$$P_{\mathrm{out}}^{\mathrm{SC/SJ}}(R_{\mathrm{S}}) \approx \Delta_{\mathrm{SC/SJ}}\bar{\gamma}_{\mathrm{B}}^{-N_{\mathrm{B}}} \tag{28}$$

where $\Delta_{\mathrm{SC/SJ}}$ is expressed as

$$\Delta_{\mathrm{SC/SJ}} = 2^{N_{\mathrm{B}}R_{\mathrm{S}}}(\Theta_1+\Theta_2) \times \left[1-\exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right)-\frac{\rho}{\lambda_{\mathrm{AP}}}\exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right)\right] + \left(\frac{2^{R_{\mathrm{S}}}}{\rho}\right)^{N_{\mathrm{B}}}(\Theta_1+\Theta_2)\left(\frac{1}{\lambda_{\mathrm{AP}}}\right)^{-N_{\mathrm{B}}}\Gamma\left(N_{\mathrm{B}}+2,\frac{\rho}{\lambda_{\mathrm{AP}}}\right) \tag{29}$$

with

$$\Theta_1 = \sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1}\sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q} \times \left(\frac{m\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{J}}}\right)^{q}\Gamma(q+1)\Psi\left(q+1,q;\frac{m}{\bar{\gamma}_{\mathrm{J}}}\right) \tag{30}$$

and

$$\Theta_2 = \sum_{m=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1}\sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q} \times \left(\frac{m\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{J}}}\right)^{q+1}\frac{1}{\bar{\gamma}_{\mathrm{E}}}\Gamma(q+1)\Psi\left(q+1,q+1;\frac{m}{\bar{\gamma}_{\mathrm{J}}}\right). \tag{31}$$

Proof: See Appendix G. ■

3) SC/ZFB Scheme:

Corollary 3: The secrecy outage probability for SC/ZBF under $\bar{\gamma}_{\mathrm{B}} \to \infty$ and fixed $\bar{\gamma}_{\mathrm{E}}$ can be approximated as

$$P_{\mathrm{out}}^{\mathrm{SC/ZFB}}(R_{\mathrm{S}}) \approx \Delta_{\mathrm{SC/ZFB}}\bar{\gamma}_{\mathrm{B}}^{-N_{\mathrm{B}}} \tag{32}$$

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

$$\Delta_{\mathrm{SC/ZFB}} = 2^{N_{\mathrm{B}}R_{\mathrm{S}}}(\Lambda_1+\Lambda_2)\left[1-\exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right)\right] + \left(\frac{2^{R_{\mathrm{S}}}}{\rho}\right)^{N_{\mathrm{B}}}(\Lambda_1+\Lambda_2)\left(\frac{1}{\lambda_{\mathrm{AP}}}\right)^{-N_{\mathrm{B}}}\Gamma\left(N_{\mathrm{B}}+1,\frac{\rho}{\lambda_{\mathrm{AP}}}\right) \tag{33}$$

with

$$\Lambda_1 = \sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q}\frac{1}{\bar{\gamma}_{\mathrm{E}}}\left(\frac{\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{J}}}\right)^{q+1} \times \Gamma(q+1)\Psi\left(q+1,4+q-N_{\mathrm{B}};\frac{1}{\bar{\gamma}_{\mathrm{J}}}\right) \tag{34}$$

and

$$\Lambda_2 = \sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q}\left(\frac{\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{J}}}\right)^{q}(N_{\mathrm{B}}-2) \times \Gamma(q+1)\Psi\left(q+1,3+q-N_{\mathrm{B}};\frac{1}{\bar{\gamma}_{\mathrm{J}}}\right). \tag{35}$$

Proof: Following a similar procedure as in the proof of Corollary 2, the desired result can be obtained. ■

From the above corollaries, we have the following key remark:

Remark: The MRC, SC/SJ, and SC/ZFB achieve the same secrecy diversity, $G_d = N_{\mathrm{B}}$, under Scenario I, which is independent of the quality of the eavesdropper's channel and the primary networks. However, the parameters of the eavesdropper's channel and the primary networks affect the secrecy performance through the coding gain, i.e.,

$$G_c = (\Delta_\star)^{-\frac{1}{N_{\mathrm{B}}}} \tag{36}$$

where $\star \in \{\mathrm{MRC}, \mathrm{SC/SJ}, \mathrm{SC/ZFB}\}$.

B. Scenario II: $\bar{\gamma}_{\mathrm{B}} \to \infty$ and $\bar{\gamma}_{\mathrm{E}} \to \infty$

We now turn our attention to analyze the approximative secrecy outage probability of multiantenna cognitive wiretap channels under Scenario II.

1) MRC Scheme:

Corollary 4: The approximative secrecy outage probability for MRC under $\bar{\gamma}_{\mathrm{B}} \to \infty$ and $\bar{\gamma}_{\mathrm{E}} \to \infty$ is given by

$$P_{\mathrm{out}}^{\mathrm{MRC}}(R_{\mathrm{S}}) \approx \left[1-\sum_{k=0}^{N_{\mathrm{B}}-1}\frac{\left(2^{R_{\mathrm{S}}}\right)^k}{\left(\bar{\gamma}_{\mathrm{B}}\right)^k\bar{\gamma}_{\mathrm{E}}}\left(\frac{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{E}}}{2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}}+\bar{\gamma}_{\mathrm{B}}}\right)^{k+1}\right] \times \left[1-\exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right)\right]+\exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}}\right) - \sum_{k=0}^{N_{\mathrm{B}}-1}\frac{1}{\left(\bar{\gamma}_{\mathrm{B}}\right)^k\bar{\gamma}_{\mathrm{E}}}\left(2^{R_{\mathrm{S}}}\right)^k\left(\frac{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{E}}}{2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}}+\bar{\gamma}_{\mathrm{B}}}\right)^{k+1}\Gamma\left(1,\frac{\rho}{\lambda_{\mathrm{AP}}}\right). \tag{37}$$

Proof: Based on (17), the asymptotic secrecy outage probability can be easily derived after some mathematical manipulations. ■

2) SC/SJ Scheme:

Corollary 5: The approximative secrecy outage probability for SC/SJ under $\bar{\gamma}_{\mathrm{B}} \to \infty$ and $\bar{\gamma}_{\mathrm{E}} \to \infty$ is given by

TABLE I
COMPARISON OF THE MRC, SC/SJ, AND SC/ZFB SCHEMES

	MRC	SC/SJ	SC/ZFB
CSI requirement	$\mathbf{h}_{\mathrm{AB}}$ and h_{AP}	$h_{\mathrm{AB}\,i}$, h_{AP}, $h_{\mathrm{B}\,j\mathrm{E}}$ and $h_{\mathrm{B}\,j*\mathrm{P}}$	$h_{\mathrm{AB}\,i}$, h_{AP}, $\mathbf{h}_{\mathrm{BE}}$ and $\mathbf{h}_{\mathrm{BP}}$
Antenna number N_{B} requirement	None	$N_{\mathrm{B}} \geq 2$	$N_{\mathrm{B}} \geq 3$
Diversity order	N_{B} /0	N_{B} /0	N_{B} /0
Impact of SU destination antenna	G_d and G_c/only G_c	G_d and G_c/only G_c	G_d and G_c/only G_c

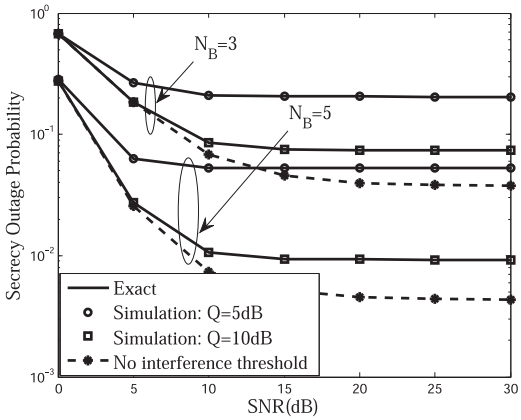


Fig. 2. Secrecy outage probability of the system with the MRC scheme for different interference thresholds Q when $N_{\mathrm{B}} = 3$ and $N_{\mathrm{B}} = 5$, respectively.

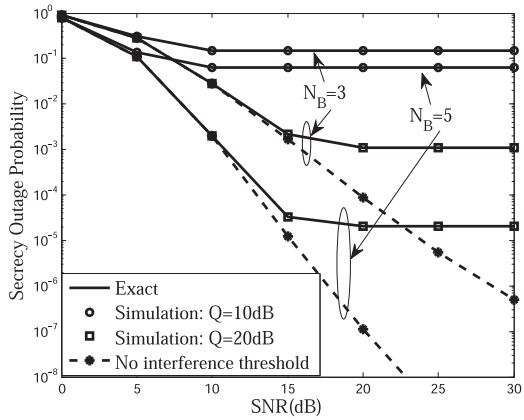


Fig. 3. Secrecy outage probability of the system with SC/SJ scheme for different interference threshold Q when $N_{\mathrm{B}} = 3$ and $N_{\mathrm{B}} = 5$, respectively.

$$P_{\mathrm{out}}^{\mathrm{SC/SJ}}(R_{\mathrm{S}}) \approx 1 - \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \sum_{m=1}^{N_{\mathrm{B}}-1} \binom{N_{\mathrm{B}}-1}{m} \times (-1)^{m-1} \Psi\left(1, 0; \frac{\bar{\gamma}_{\mathrm{B}} + n2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{J}}/m}\right) - \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \times \sum_{m=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}-1}{m} (-1)^{m-1} \frac{m}{\bar{\gamma}_{\mathrm{J}}} \Psi\left(1, 1; \frac{\bar{\gamma}_{\mathrm{B}} + n2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{J}}/m}\right). \tag{38}$$

Proof: See Appendix H. ■

3) SC/ZFB Scheme:

Corollary 6: The approximative secrecy outage probability for SC/ZFB under $\bar{\gamma}_{\mathrm{B}} \to \infty$ and $\bar{\gamma}_{\mathrm{E}} \to \infty$ is given by

$$P_{\mathrm{out}}^{\mathrm{SC/ZFB}}(R_{\mathrm{S}}) \approx 1 - \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \frac{1}{\bar{\gamma}_{\mathrm{Z}}} \times \Psi\left(1, 4 - N_{\mathrm{B}}; \frac{n2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}} + \bar{\gamma}_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{Z}}}\right) - \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \times (N_{\mathrm{B}} - 2)\, \Psi\left(1, 3 - N_{\mathrm{B}}; \frac{n2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}} + \bar{\gamma}_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{Z}}}\right). \tag{39}$$

Proof: Following a similar procedure as in the proof of Corollary 5, the above result can be easily obtained. ■

Remark: In contrast to Scenario I, all three schemes exhibit the secrecy outage floor when $\bar{\gamma}_{\mathrm{B}} \to \infty$ and $\bar{\gamma}_{\mathrm{E}} \to \infty$, which indicates that no secrecy diversity can be obtained.

C. Comparison of the Proposed Schemes

We now provide a detailed comparison of the proposed three schemes. In the previous analysis, the CSI requirement to perform jamming or ZFB was not explicitly mentioned. In practice, the acquisition of CSI involves additional feedback overhead, which must be considered in the design of wireless systems. On the other hand, if a large amount of CSI is available, more sophisticated transmission schemes should be designed in order to improve the secrecy performance. Hence, to make a fair comparison among different schemes, the CSI requirement of each individual scheme must be characterized in Table I.

V. NUMERICAL RESULTS

In this section, we present representative numerical results to verify the analytical ones, make a comprehensive comparison between our proposed schemes and the SC scheme, and give a detail investigation on the impact of different system parameters on the secrecy outage performance of multiantenna cognitive wiretap systems. Without loss of generality, we assume that the secrecy rate is $R_{\mathrm{S}} = 2$, 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 simulation results and the asymptotic curves remain sufficiently tight across the entire SNR range of interest, which validates the accuracy of the analytical expressions.

Figs. 2–4 illustrate the secrecy outage probability of the cognitive wiretap network with MRC, SC/SJ and SC/ZFB for a different number of antennas N_{B} and a different interference

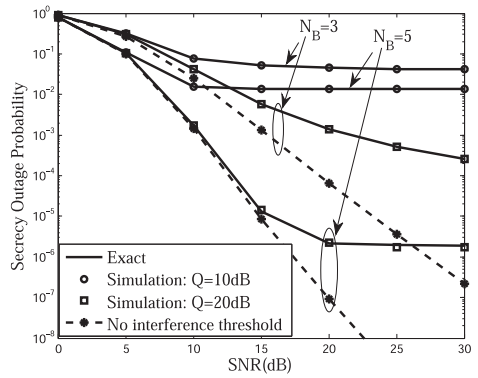


Fig. 4. Secrecy outage probability of the system with the SC/ZFB scheme for different interference thresholds Q when $N_{\mathrm{B}} = 3$ and $N_{\mathrm{B}} = 5$, respectively.

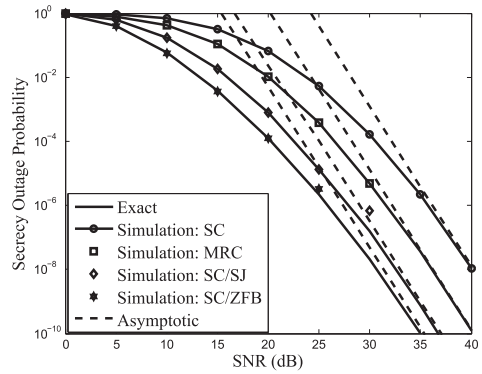


Fig. 5. Exact and asymptotic secrecy outage probabilities for SC, MRC, SC/SJ, and SC/ZFB schemes under Scenario I when $N_{\mathrm{B}} = 5$ and $\bar{\gamma}_{\mathrm{E}} = 10$ dB.

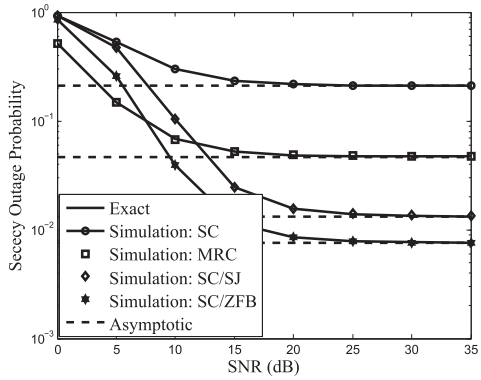


Fig. 6. Exact and asymptotic secrecy outage probabilities for SC, MRC, SC/SJ, and SC/ZFB schemes under Scenario II when $N_{\mathrm{B}} = 5$.

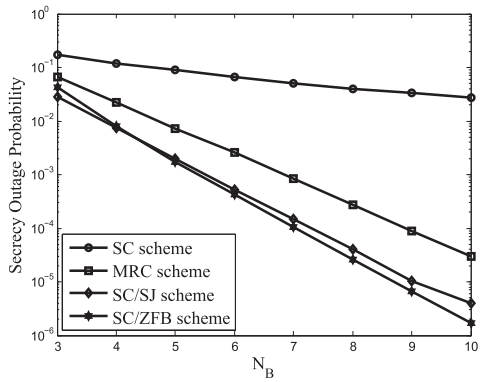


Fig. 7. Secrecy outage probabilities of SC, MRC, SC/SJ, and SC/ZFB schemes versus the number of antennas of Bob when $P_t = 10$ dB.

thresholds Q, respectively. The secrecy outage probability of conventional noncognitive wiretap network without interference temperature constraint is also provided as a benchmark for comparison. It is evident from these figures that by increasing N_{B}, the secrecy outage probability can be significantly reduced for all three schemes. This is rather intuitive, since increasing N_{B} provides additional secrecy diversity or secrecy coding gain. We also observe that the secrecy outage probability of the cognitive wiretap network is inferior to that of the conventional noncognitive wiretap network, and the secrecy outage performance can be substantially improved when the interference threshold Q at the primary receiver is loose, i.e., for higher Q. In addition, the secrecy performance of SC/SJ and SC/ZFB is superior to MRC in conventional noncognitive wiretap networks since the jamming signal from the FD Bob can degrade the secrecy diversity of the eavesdropper.

Fig. 5 plots the secrecy outage probability versus SNR for the three proposed schemes and the SC scheme when Bob is located close to Alice. It is observed that all schemes achieve the same secrecy diversity order of N_{B}. Furthermore, we see that the SC/ZFB scheme always attains better performance than the MRC and SC/SJ schemes, while they all outperform the SC scheme, which indicates that using the MRC scheme at Bob or by transmitting jamming signals from a FD Bob will improve the secrecy array gain of the system compared to the SC scheme under Scenario I.

Fig. 6 presents the secrecy outage probabilities versus SNR for the three proposed schemes and the SC scheme when $N_{\mathrm{B}} = 5$ and $\frac{\bar{\gamma}_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{E}}} = 10$ dB. As illustrated, the secrecy outage probability of all schemes settle in the high SNR regime, which confirms the analytical results under Scenario II. It is also observed that all the proposed schemes achieve better secrecy performance than the SC scheme. In addition, the MRC scheme outperforms the SC/SJ and SC/ZFB schemes at the low SNR regime, while the opposite holds in the high SNR regime.

Figs. 7 and 8 illustrate the impact of antenna numbers N_{B} and the interference threshold Q on the secrecy outage performance of the SC, MRC, SC/SJ, and SC/ZFB schemes, respectively. It can be observed from both figures that the secrecy performance can be improved by increasing the number of antennas or the interference threshold. In addition, when the interference threshold becomes large, the secrecy performance gradually approach to that of the conventional noncognitive wiretap network without interference temperature constraint. Moreover, when the interference threshold is large, the SC/ZFB scheme always attains better performance than the SC/SJ scheme, and they both achieve better performance than the MRC scheme. This can be explained by the fact that a large Q implies loose constraint at the PR, thus, the transmit power of jamming signal can be made large. In addition, our proposed schemes achieve better performance than the SC scheme, especially when the number

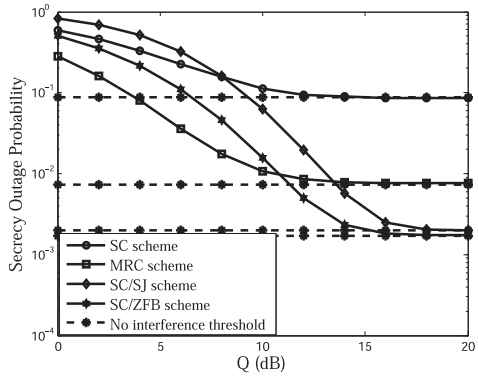


Fig. 8. Secrecy outage probabilities of SC, MRC, SC/SJ, and SC/ZFB schemes versus the interference threshold Q when $N_{\rm B} = 5$ and $P_t = 10\,$dB.

of antennas is large or the interference threshold Q is large, which demonstrates the advantage of our proposed schemes.

VI. Conclusion

In this paper, we have investigated the secrecy outage performance of multiantenna CRNs over Rayleigh fading channels. To exploit the advantages of the multiple antennas, we have proposed three secure transmission schemes with both HD and FD operations. Specifically, closed-form expressions of the secrecy outage probability of all 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 results of this paper suggest that the full diversity, i.e., $N_{\rm B}$, can be achieved when only quality of the main channel is much better than the eavesdropper's channel. However, when the main and the eavesdropper's channels experience similar fading conditions, the diversity reduces to zero. Moreover, MRC with HD operation outperforms SC/SJ and SC/ZFB with the FD operation at the low interference threshold regime, while the opposite holds in the high interference threshold regime. In addition, our proposed schemes tend to achieve better performance than SC scheme, which validate the efficiency of our proposed schemes.

Appendix A
Proof of Lemma 1

Substituting (15) and (16) into (14) and performing some simple mathematical manipulations, the conditional secrecy outage probability can be expressed as

$$P_{\rm out}^{\rm MRC}\left(R_{\rm S}|G_1\right)=\int_0^\infty F_{\gamma_{\rm B_1}}\left(2^{R_{\rm S}}\left(1+y\right)-1|G_1\right) f_{\gamma_{\rm E_1}}\left(y|G_1\right) dy$$
$$= 1-\sum_{k=0}^{N_{\rm B}-1}\frac{1}{k!}\left(\frac{\sigma^2}{P_{S_1}\lambda_{\rm AB}}\right)^k\frac{\sigma^2}{P_{S_1}\lambda_{\rm AE}}\exp\left(-\frac{\sigma^2\left(2^{R_{\rm S}}-1\right)}{P_{S_1}\lambda_{\rm AB}}\right)$$
$$\times\sum_{i=0}^{k}\binom{k}{i}\left(2^{R_{\rm S}}-1\right)^{k-i}\left(2^{R_{\rm S}}\right)^i i!\left(\frac{P_{S_1}\lambda_{\rm AB}P_{S_1}\lambda_{\rm AE}/\sigma^2}{2^{R_{\rm S}}P_{S_1}\lambda_{\rm AE}+P_{S_1}\lambda_{\rm AB}}\right)^{i+1}. \tag{40}$$

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

$$P_{\rm out}^{\rm MRC}\left(R_{\rm S}\right)=\int_0^\infty P_{\rm out}^{\rm MRC}\left(R_{\rm S}|G_1\right)f_{G_1}\left(g\right)dg$$
$$=\int_0^{Q/P_t}\left[1-\exp\left(-\frac{2^{R_{\rm S}}-1}{\bar{\gamma}_{\rm B}}\right)\sum_{k=0}^{N_{\rm B}-1}\sum_{i=0}^{k}\binom{k}{i}\right.$$
$$\left.\times\left(\frac{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm E}}{2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}\right)^{i+1}\frac{\left(2^{R_{\rm S}}-1\right)^{k-i}\left(2^{R_{\rm S}}\right)^i i!}{\left(\bar{\gamma}_{\rm B}\right)^k\bar{\gamma}_{\rm E}k!}\right]f_{G_1}\left(g\right)dg$$
$$+\int_{Q/P_t}^\infty\left[1-\sum_{k=0}^{N_{\rm B}-1}\sum_{i=0}^{k}\binom{k}{i}\frac{\left(2^{R_{\rm S}}-1\right)^{k-i}\left(2^{R_{\rm S}}\right)^i i!}{\rho\bar{\gamma}_{\rm E}\left(\rho\bar{\gamma}_{\rm B}\right)^k k!}g^{k-i}\right.$$
$$\left.\times\left(\frac{\rho\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm E}}{2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}\right)^{i+1}\exp\left(-\frac{g\left(2^{R_{\rm S}}-1\right)}{\rho\bar{\gamma}_{\rm B}}\right)\right]f_{G_1}\left(g\right)dg. \tag{41}$$

To this end, substituting the PDF of G_1 into (41) and utilizing the equality [35, eq. (3.381.4)], the desired result can be derived after some algebraic manipulations.

Appendix B
Proof of Lemma 2

Let us define $Z=\frac{P_B}{\sigma^2}\max_{j\in N_{\rm B}-1}\left(|h_{j\rm E}|^2\right)$. Recall that the conditional CDF and PDF of Z are given by

$$F_Z\left(z|G_2\right)=\left[1-\exp\left(-\frac{\sigma^2 z}{P_B\lambda_{\rm JE}}\right)\right]^{N_{\rm B}-1}$$
$$=1-\sum_{m=1}^{N_{\rm B}-1}\binom{N_{\rm B}-1}{m}(-1)^{m-1}\exp\left(-\frac{\sigma^2 mz}{P_B\lambda_{\rm JE}}\right) \tag{42}$$

and

$$f_Z\left(z|G_2\right)=\sum_{m=1}^{N_{\rm B}-1}\binom{N_{\rm B}-1}{m}(-1)^{m-1}\frac{\sigma^2 m}{P_B\lambda_{\rm JE}}$$
$$\times\exp\left(-\frac{\sigma^2 mz}{P_B\lambda_{\rm JE}}\right). \tag{43}$$

Then, the conditional CDF of $\gamma_{\rm E_2}$ can be derived as

$$F_{\gamma_{\rm E_2}}\left(y|G_2\right)=\int_0^\infty F_{X_{\rm E}}\left(y\left(z+1\right)|G_2\right)f_Z\left(z|G_2\right)dz$$
$$=1-\sum_{m=1}^{N_{\rm B}-1}\frac{\binom{N_{\rm B}-1}{m}(-1)^{m-1}mP_{S_2}\lambda_{\rm AE}\exp\left(-\frac{\sigma^2 y}{P_{S_2}\lambda_{\rm AE}}\right)}{P_B\lambda_{\rm JE}y+mP_{S_2}\lambda_{\rm AE}} \tag{44}$$

where $F_{X_{\rm E}}(\cdot)$ is the CDF of $X_{\rm E}=\frac{P_{S_2}|h_{\rm AE}|^2}{\sigma^2}$ conditioned on the RV G_2. To this end, taking the derivative of $F_{\gamma_{\rm E_2}}(y|G_2)$ yields the conditional PDF of $\gamma_{\rm E_2}$ given in (19).

APPENDIX C
PROOF OF LEMMA 3

Similar to (40), we first present the conditional secrecy outage probability in (45), shown at the bottom of the page.

To derive the unconditional secrecy outage probability, we average over RV G_2, which produces two double integrals as (46) and (47), shown at the bottom of the page.

Since the PDF of G_2 can be obtained as

$$f_{G_2}(g) = \left(\frac{1}{\lambda_{\rm AP}}\right)^2 g \exp\left(-\frac{g}{\lambda_{\rm AP}}\right). \tag{48}$$

Substituting (48) into I_5 and performing some simple mathematical manipulations, we have

$$\begin{aligned} I_5 = {} & \exp\left(-\frac{n\left(2^{R_{\rm S}}(1+y)-1\right)}{\bar{\gamma}_{\rm B}}\right)\frac{m\bar{\gamma}_{\rm E}\bar{\gamma}_{\rm J}}{\left(\bar{\gamma}_{\rm J}y+m\bar{\gamma}_{\rm E}\right)^2} \\ & \times\left[1-\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)-\frac{\rho}{\lambda_{\rm AP}}\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)\right] \\ & \times\exp\left(-\frac{y}{\bar{\gamma}_{\rm E}}\right)+\left(\frac{1}{\lambda_{\rm AP}}\right)^2\exp\left(-\frac{y+a}{b}\right) \\ & \times\sum_{k=0}^{1}\frac{(b\rho)^{2-k}(\rho)^k}{(y+a)^{2-k}}\frac{m\bar{\gamma}_{\rm E}\bar{\gamma}_{\rm J}}{\left(\bar{\gamma}_{\rm J}y+m\bar{\gamma}_{\rm E}\right)^2} \end{aligned} \tag{49}$$

where $a=\frac{n(2^{R_{\rm S}}-1)\bar{\gamma}_{\rm E}\lambda_{\rm AP}+\rho\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm E}}{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}\lambda_{\rm AP}+\bar{\gamma}_{\rm B}\lambda_{\rm AP}}$ and $b=\frac{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm E}\lambda_{\rm AP}}{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}\lambda_{\rm AP}+\bar{\gamma}_{\rm B}\lambda_{\rm AP}}$.

Then, substituting (46) into (49), I_1 can be rewritten as

$$\begin{aligned} I_1 = {} & \left[1-\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)-\frac{\rho}{\lambda_{\rm AP}}\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)\right] \\ & \times\exp\left(-\frac{n\left(2^{R_{\rm S}}-1\right)}{\bar{\gamma}_{\rm B}}\right)\left[1+\frac{n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm E}}\right. \\ & \left.\times\exp\left(\frac{\left(n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}\right)m}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm J}}\right)\mathrm{Ei}\left(-\frac{\left(n2^{R_{\rm S}}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}\right)m}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm J}}\right)\right] \\ & +\left(\frac{1}{\lambda_{\rm AP}}\right)^2\underbrace{\int_0^\infty\exp\left(-\frac{y+a}{b}\right)\sum_{k=0}^{1}\frac{(b\rho)^{2-k}(\rho)^k}{(y+a)^{2-k}}\frac{c}{(y+c)^2}dy}_{I_7} \end{aligned} \tag{50}$$

where $c=m\bar{\gamma}_{\rm E}/\bar{\gamma}_{\rm J}$, and I_7 can be further simplified as

$$\begin{aligned} I_7 = {} & \sum_{k=0}^{1}(b\rho)^{2-k}\rho^k c \\ & \times\int_0^\infty\exp\left(-\frac{y+a}{b}\right)\left[\begin{array}{l}\sum\limits_{i=0}^{1-k}\frac{\binom{1+i}{i}\mu^{2+i}}{(y+a)^{2-k-i}} \\ +\sum\limits_{j=0}^{1}\frac{\binom{1-k+j}{j}(-1)^{2-k}\nu^{2-k+j}}{(y+c)^{2-j}}\end{array}\right]dy \end{aligned}$$

$$\begin{aligned} P_{\rm out}^{\rm SC/SJ}(R_{\rm S}|G_2) = {} & \int_0^\infty F_{\gamma_{\rm B_2}}\left(2^{R_{\rm S}}(1+y)-1|G_2\right)f_{\gamma_{\rm E_2}}(y|G_2)\,dy \\ = {} & 1-\sum_{n=1}^{N_{\rm B}}\binom{N_{\rm B}}{n}(-1)^{n-1}\sum_{m=1}^{N_{\rm B}-1}\binom{N_{\rm B}-1}{m}(-1)^{m-1} \\ & \times\underbrace{\int_0^\infty\exp\left(-\frac{\sigma^2n\left(2^{R_{\rm S}}(1+y)-1\right)}{P_{S_2}\lambda_{\rm AB}}\right)\frac{mP_{S_2}\lambda_{\rm AE}P_B\lambda_{\rm JE}}{\left(mP_{S_2}\lambda_{\rm AE}+P_B\lambda_{\rm JE}y\right)^2}\exp\left(-\frac{\sigma^2y}{P_{S_2}\lambda_{\rm AE}}\right)dy}_{I_3} \\ & -\sum_{n=1}^{N_{\rm B}}\binom{N_{\rm B}}{n}(-1)^{n-1}\sum_{m=1}^{N_{\rm B}}\binom{N_{\rm B}-1}{m}(-1)^{m-1} \\ & \times\underbrace{\int_0^\infty\exp\left(-\frac{\sigma^2n\left(2^{R_{\rm S}}(1+y)-1\right)}{P_{S_2}\lambda_{\rm AB}}\right)\frac{\sigma^2m\exp\left(-\frac{\sigma^2y}{P_{S_2}\lambda_{\rm AE}}\right)}{mP_{S_2}\lambda_{\rm AE}+P_B\lambda_{\rm JE}y}dy}_{I_4}. \end{aligned} \tag{45}$$

$$I_1 = \underbrace{\int_0^\infty\int_0^\infty\exp\left(-\frac{\sigma^2n\left(2^{R_{\rm S}}(1+y)-1\right)}{P_{S_2}\lambda_{\rm AB}}\right)\frac{mP_{S_2}\lambda_{\rm AE}P_B\lambda_{\rm JE}}{\left(mP_{S_2}\lambda_{\rm AE}+P_B\lambda_{\rm JE}y\right)^2}\exp\left(-\frac{\sigma^2y}{P_{S_2}\lambda_{\rm AE}}\right)f_{G_2}(g)\,dgdy}_{I_5}. \tag{46}$$

$$I_2 = \underbrace{\int_0^\infty\int_0^\infty\exp\left(-\frac{\sigma^2n\left(2^{R_{\rm S}}(1+y)-1\right)}{P_{S_2}\lambda_{\rm AB}}\right)\frac{\sigma^2m}{mP_{S_2}\lambda_{\rm AE}+P_B\lambda_{\rm JE}y}\exp\left(-\frac{\sigma^2y}{P_{S_2}\lambda_{\rm AE}}\right)f_{G_2}(g)\,dgdy}_{I_6}. \tag{47}$$

$$= \sum_{k=0}^{1} (b\rho)^{2-k} \rho^k c \left[\sum_{i=0}^{1-k} \binom{1+i}{i} \mu^{2+i} \left(\frac{1}{a}\right)^{1-k-i} \Psi\left(1, k+i; \frac{a}{b}\right) + \sum_{j=0}^{1} \binom{1-k+j}{j} (-1)^{2-k} \nu^{2-k+j} \left(\frac{1}{c}\right)^{1-j} \Psi\left(1, j; \frac{c}{b}\right) \right] \quad (51)$$

where $\mu = \frac{1}{a-c}$, and $\nu = \frac{1}{c-a}$.

To this end, substituting (51) into (50), we obtain I_1 as in (21). Similar to the derivation of I_1, I_2 can be obtained.

Appendix D
Proof of Lemma 4

In order to derive the conditional PDF of γ_{E_3}, we first give the PDF of the RV $Z_1 = P_B |\mathbf{h}_{\mathbf{BE}}^{\dagger} \mathbf{w}_{\mathrm{ZF}}|^2 / \sigma^2$ as [36]

$$f_{Z_1}(z) = \frac{z^{N_{\mathrm{B}}-3} \exp\left(-\frac{\sigma^2 z}{P_Z \lambda_{\mathrm{JE}}}\right)}{(N_{\mathrm{B}}-3)! (P_Z \lambda_{\mathrm{JE}}/\sigma^2)^{N_{\mathrm{B}}-2}}, \; N_{\mathrm{B}} \geq 3. \quad (52)$$

Then, the conditional CDF of γ_{E_3} can be expressed as

$$F_{\gamma_{\mathrm{E}_3}}(y|G_1) = \int_0^{\infty} F_{X_{\mathrm{E}}}(y(z+1)|G_1) f_{Z_1}(z)\, dz = 1 - \exp\left(-\frac{\sigma^2 y}{P_{S_3} \lambda_{\mathrm{AE}}}\right) \left(\frac{P_{S_3} \lambda_{\mathrm{AE}}}{P_Z \lambda_{\mathrm{JE}} y + P_{S_3} \lambda_{\mathrm{AE}}}\right)^{N_{\mathrm{B}}-2}. \quad (53)$$

Finally, the conditional PDF of γ_{E_3} can be obtained by taking a simple derivative.

Appendix E
Proof of Lemma 5

Following similar analysis of (45), the conditional secrecy outage probability of the SC/ZFB scheme is as in (54), shown at the bottom of the page.

where Ξ_1 and Ξ_2 can be derived with the help of [35, eq. (9.211.4)] as

$$\Xi_1 = \exp\left(-\frac{\sigma^2 n \left(2^{R_{\mathrm{S}}}-1\right)}{P_{S_3} \lambda_{\mathrm{AB}}}\right) \frac{\sigma^2}{P_B \lambda_{\mathrm{JE}}} \times \Psi\left(1, 4-N_{\mathrm{B}}; \frac{\sigma^2 \left(n 2^{R_{\mathrm{S}}} \lambda_{\mathrm{AE}} + \lambda_{\mathrm{AB}}\right)}{P_B \lambda_{\mathrm{JE}} \lambda_{\mathrm{AB}}}\right) \quad (55)$$

and

$$\Xi_2 = \exp\left(-\frac{\sigma^2 n \left(2^{R_{\mathrm{S}}}-1\right)}{P_{S_3} \lambda_{\mathrm{AB}}}\right) (N_{\mathrm{B}}-2) \times \Psi\left(1, 3-N_{\mathrm{B}}; \frac{\sigma^2 \left(n 2^{R_{\mathrm{S}}} \lambda_{\mathrm{AE}} + \lambda_{\mathrm{AB}}\right)}{P_B \lambda_{\mathrm{JE}} \lambda_{\mathrm{AB}}}\right). \quad (56)$$

Hence, the unconditional secrecy outage probability of the SC/ZFB scheme can be derived as

$$P_{\mathrm{out}}^{\mathrm{SC/ZFB}}(R_{\mathrm{S}}) = \int_0^{\infty} \left[1 - \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \cdot \Xi_1 - \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \cdot \Xi_2\right] f_{G_1}(g)\, dg. \quad (57)$$

Finally, substituting the PDF of G_1 into (57) and performing some simple mathematical manipulations, the desired secrecy outage probability of the SC/ZFB scheme can be obtained.

Appendix F
Proof of Corollary 1

When $\bar{\gamma}_{\mathrm{B}} \to \infty$, the conditional CDF of γ_{B_1} can be approximated as

$$F_{\gamma_{\mathrm{B}_1}}(x|G_1) \approx \frac{1}{N_{\mathrm{B}}!} \left(\frac{\sigma^2 x}{P_{S_1} \lambda_{\mathrm{AB}}}\right)^{N_{\mathrm{B}}}. \quad (58)$$

Also, the conditional PDF of γ_{E_1} can be written as

$$f_{\gamma_{\mathrm{E}_1}}(y|G_1) = \frac{1}{\bar{\gamma}_{\mathrm{E}}} \exp\left(-\frac{y}{\bar{\gamma}_{\mathrm{E}}}\right). \quad (59)$$

Substituting (58) and (59) into (14) and applying the binomial expansion, the asymptotic secrecy outage probability of the MRC scheme conditioned on the RV G_1 is given by

$$P_{\mathrm{out}}^{\mathrm{MRC}}(R_{\mathrm{S}}|G_1) \approx \int_0^{\infty} F_{\gamma_{\mathrm{B}_1}}\left(2^{R_{\mathrm{S}}}(1+y)-1|G_1\right) f_{\gamma_{\mathrm{E}_1}}(y|G_1) dy = \frac{1}{N_{\mathrm{B}}!} \left(\frac{\sigma^2 2^{R_{\mathrm{S}}}}{P_{S_1} \lambda_{\mathrm{AB}}}\right)^{N_{\mathrm{B}}} \sum_{q=0}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{q} \left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q} q! \bar{\gamma}_{\mathrm{E}}^{q}. \quad (60)$$

$$P_{\mathrm{out}}^{\mathrm{SC/ZFB}}(R_{\mathrm{S}}|G_1) = \int_0^{\infty} F_{\gamma_{\mathrm{B}_3}}\left(2^{R_{\mathrm{S}}}(1+y)-1|G_1\right) f_{\gamma_{\mathrm{E}_3}}(y|G_1)\, dy$$

$$= 1 - \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \underbrace{\int_0^{\infty} \exp\left(-\frac{\sigma^2 n \left(2^{R_{\mathrm{S}}}(1+y)-1\right)}{P_{S_3} \lambda_{\mathrm{AB}}}\right) \frac{\sigma^2 \exp\left(-\frac{\sigma^2 y}{P_{S_3} \lambda_{\mathrm{AE}}}\right)}{P_{S_3} \lambda_{\mathrm{AE}}} \left(\frac{P_{S_3} \lambda_{\mathrm{AE}}}{P_B \lambda_{\mathrm{JE}} y + P_{S_3} \lambda_{\mathrm{AE}}}\right)^{N_{\mathrm{B}}-2} dy}_{\Xi_1}$$

$$- \sum_{n=1}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{n} (-1)^{n-1} \underbrace{\int_0^{\infty} \exp\left(-\frac{\sigma^2 n \left(2^{R_{\mathrm{S}}}(1+y)-1\right)}{P_{S_3} \lambda_{\mathrm{AB}}}\right) \exp\left(-\frac{\sigma^2 y}{P_{S_3} \lambda_{\mathrm{AE}}}\right) \frac{(N_{\mathrm{B}}-2) P_B \lambda_{\mathrm{JE}} (P_{S_3} \lambda_{\mathrm{AE}})^{N_{\mathrm{B}}-2}}{(P_B \lambda_{\mathrm{JE}} y + P_{S_3} \lambda_{\mathrm{AE}})^{N_{\mathrm{B}}-1}} dy}_{\Xi_2}. \quad (54)$$

Now, averaging over G_1 and with the help of equality [35, eq. (3.381.4)], the desired result can be derived.

APPENDIX G
PROOF OF COROLLARY 2

When $\bar{\gamma}_{\mathrm{B}} \to \infty$, the conditional CDF of γ_{B_2} can be approximated as

$$F_{\gamma_{\mathrm{B}_2}}(x|G_2) \approx \left(\frac{\sigma^2 x}{P_{S_2}\lambda_{\mathrm{AB}}}\right)^{N_{\mathrm{B}}}. \tag{61}$$

In addition, the conditional PDF of γ_{E_2} can be rewritten as

$$f_{\gamma_{\mathrm{E}_2}}(y|G_2) = \sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m}\frac{(-1)^{m-1}\, m\bar{\gamma}_{\mathrm{E}}\bar{\gamma}_{\mathrm{J}}}{\left(\bar{\gamma}_{\mathrm{J}}y + m\bar{\gamma}_{\mathrm{E}}\right)^2}\exp\left(-\frac{y}{\bar{\gamma}_{\mathrm{E}}}\right) + \sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1}\frac{m}{\bar{\gamma}_{\mathrm{J}}y + m\bar{\gamma}_{\mathrm{E}}}\exp\left(-\frac{y}{\bar{\gamma}_{\mathrm{E}}}\right). \tag{62}$$

Now, inserting (61) and (62) into (14) and applying the binomial expansion with the help of equality [35, eq. (9.211.4)], the asymptotic secrecy outage probability of the SC/SJ scheme conditioned on the RV G_2 can be expressed as (63), shown at the bottom of the page.

Thus, the unconditional secrecy outage probability of the SC/SJ scheme is given by

$$\begin{aligned} P_{\mathrm{out}}^{\mathrm{SC/SJ}}(R_{\mathrm{S}}) &\approx \int_0^{\infty}\left(\frac{\sigma^2 2^{R_{\mathrm{S}}}}{P_{S_2}\lambda_{\mathrm{AB}}}\right)^{N_{\mathrm{B}}}(\Theta_1+\Theta_2)f_{G_2}(g)\,dg \\ &= \int_0^{Q/P_t}\left(\frac{2^{R_{\mathrm{S}}}}{\bar{\gamma}_{\mathrm{B}}}\right)^{N_{\mathrm{B}}}(\Theta_1+\Theta_2)f_{G_2}(g)\,dg \\ &\quad + \int_{Q/P_t}^{\infty}\left(\frac{2^{R_{\mathrm{S}}}}{\rho\bar{\gamma}_{\mathrm{B}}}g\right)^{N_{\mathrm{B}}}(\Theta_1+\Theta_2)f_{G_2}(g)\,dg. \end{aligned} \tag{64}$$

To this end, substituting the PDF of G_2 into (64) and utilizing the equality [35, eq. (3.381.4)], the desired result can be derived.

APPENDIX H
PROOF OF COROLLARY 5

Similar to (45), the secrecy outage probability of the SC/SJ scheme conditioned on G_2 can be expressed as equation (65), shown at the bottom of the page, where Θ_3 and Θ_4 can be derived, after some simple algebraic manipulations, as

$$\Theta_3 = \exp\left(-\frac{n\left(2^{R_{\mathrm{S}}}-1\right)}{\bar{\gamma}_{\mathrm{B}}}\right)\Psi\left(1,0;\frac{m\left(\bar{\gamma}_{\mathrm{B}}+n2^{R_{\mathrm{S}}}\bar{\gamma}_{\mathrm{E}}\right)}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{J}}}\right) \tag{66}$$

$$\begin{aligned} P_{\mathrm{out}}^{\mathrm{SC/SJ}}(R_{\mathrm{S}}|G_2) &\approx \left(\frac{2^{R_{\mathrm{S}}}}{\lambda_{\mathrm{AB}}P_{S_2}/\sigma^2}\right)^{N_{\mathrm{B}}} \\ &\times \underbrace{\sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1}\sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q}\left(\frac{m\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{J}}}\right)^{q}\Gamma(q+1)\,\Psi\left(q+1,q;\frac{m}{\bar{\gamma}_{\mathrm{J}}}\right)}_{\Theta_1} \\ &+ \left(\frac{2^{R_{\mathrm{S}}}}{\lambda_{\mathrm{AB}}P_{S_2}/\sigma^2}\right)^{N_{\mathrm{B}}}\underbrace{\sum_{m=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1}\sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}\left(\frac{2^{R_{\mathrm{S}}}-1}{2^{R_{\mathrm{S}}}}\right)^{N_{\mathrm{B}}-q}\left(\frac{m\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{J}}}\right)^{q+1}\frac{1}{\bar{\gamma}_{\mathrm{E}}}\Gamma(q+1)\,\Psi\left(q+1,q+1;\frac{m}{\bar{\gamma}_{\mathrm{J}}}\right)}_{\Theta_2}. \end{aligned} \tag{63}$$

$$\begin{aligned} P_{\mathrm{out}}^{\mathrm{SC/SJ}}(R_{\mathrm{S}}|G_2) &= 1 - \sum_{n=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{n}(-1)^{n-1}\sum_{m=1}^{N_{\mathrm{B}}-1}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1} \\ &\times \underbrace{\int_0^{\infty}\exp\left(-\frac{\sigma^2 n\left(2^{R_{\mathrm{S}}}(1+y)-1\right)}{P_{S_2}\lambda_{\mathrm{AB}}}\right)\frac{mP_{S_2}\lambda_{\mathrm{AE}}P_B\lambda_{\mathrm{JE}}}{\left(mP_{S_2}\lambda_{\mathrm{AE}}+P_B\lambda_{\mathrm{JE}}y\right)^2}\exp\left(-\frac{\sigma^2 y}{P_{S_2}\lambda_{\mathrm{AE}}}\right)dy}_{\Theta_3} \\ &- \sum_{n=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{n}(-1)^{n-1}\sum_{m=1}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}-1}{m}(-1)^{m-1}\underbrace{\int_0^{\infty}\exp\left(-\frac{\sigma^2 n\left(2^{R_{\mathrm{S}}}(1+y)-1\right)}{P_{S_2}\lambda_{\mathrm{AB}}}\right)\frac{\sigma^2 m\exp\left(-\frac{\sigma^2 y}{P_{S_2}\lambda_{\mathrm{AE}}}\right)}{mP_{S_2}\lambda_{\mathrm{AE}}+P_B\lambda_{\mathrm{JE}}y}dy}_{\Theta_4}. \end{aligned} \tag{65}$$

$$\Theta_4 = \exp\left(-\frac{n\left(2^{R_S}-1\right)}{\bar{\gamma}_B}\right)\frac{m}{\bar{\gamma}_J}\Psi\left(1,1;\frac{m\left(\bar{\gamma}_B+n2^{R_S}\bar{\gamma}_E\right)}{\bar{\gamma}_B\bar{\gamma}_J}\right). \quad (67)$$

Finally, substituting (66) and (67) into (65), we obtain the desired result.

REFERENCES

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

[2] Y. Huang, F. S. Al-Qahtani, C. Zhong, Q. Wu, J. Wang, and H. M. Alnuweiri, "Cognitive MIMO relaying networks with primary user's interference and outdated channel state information," *IEEE Trans. Commun.*, vol. 62, no. 12, pp. 4241–4254, Dec. 2014.

[3] F. R. V. Guimaraes, D. B. da Costa, T. A. Tsiftsis, and C. C. Cavalcante, "Multi-user and multi-relay cognitive radio networks under spectrum sharing constraints," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 433–439, Jan. 2014.

[4] Y. Deng, M. Elkashlan, P. L. Yeoh, N. Yang, and R. K. Mallik, "Cognitive MIMO relay networks with generalized selection combining," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4911–4922, Sep. 2014.

[5] Y. Deng, L. Wang, M. Elkashlan, K. J. Kim, and T. Q. Duong, "Generalized selection combining for cognitive relay networks over Nakagami-m fading," *IEEE Trans. Signal Process.*, vol. 63, no. 8, pp. 1993–2006, Apr. 2015.

[6] E. Silva, A. Dos Santos, L. C. P. Albini, and M. N. Lima, "Identity-based key management in mobile ad hoc networks: Techniques and applications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.

[7] 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.

[8] T. Q. Duong, T. T. Duy, M. Elkashlan, N. H. Tran, and O. A. Dobre, "Secured cooperative cognitive radio networks with relay selection," in *Proc. IEEE Global Commun. Conf.*, Austin, TX, USA, 2014, pp. 3074–3079.

[9] H. Jeon, S. W. McLaughlin, and J. Ha, "Secure communications with untrusted secondary users in cognitive radio networks," in *Proc. IEEE Global Commun. Conf.*, Anaheim, CA, USA, 2012, pp. 1072–1078.

[10] 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.

[11] 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. Inform Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

[12] 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.

[13] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2016.2529704.

[14] H. Lei *et al.*, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2016.2574315.

[15] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in correlated channel with maximal ratio combining diversity," *IEEE Trans. Signal Process.*, vol. 60, no. 12, pp. 6745–6751, Dec. 2012.

[16] 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.

[17] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex Bob in the MIMO gaussian wiretap channel: Scheme and performance," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 107–111, Jan. 2016.

[18] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical layer security over SIMO generalized-$\mathcal{K}$ fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.

[19] D. B. da Costa, M. Elkashlan, P. L. Yeoh, N. Yang, and M. D. Yacoub, "Dual-hop cooperative spectrum sharing systems with multi-primary users and multi-secondary destinations over Nakagami-m fading," in *Proc. IEEE 23rd Int. Personal, Indoor Mobile Radio Commun.*, Sydney, Australia, 2012, pp. 1577–1581.

[20] V. N. Q. Bao, N. L. Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[21] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[22] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[23] V. Asghari and S. Aïssa, "Performance of cooperative spectrum-sharing systems with amplify-and-forward relaying," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1295–1230, Apr. 2013.

[24] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[25] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inform. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[26] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.

[27] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[28] S. Simoens, O. Munoz-Medina, J. Vidal, and A. del Coso, "On the gaussian MIMO relay channel with full channel state information," *IEEE Trans. Signal Process.*, vol. 57, no. 9, pp. 3588–3599, Sep. 2009.

[29] V. R. Cadambe and S. A. Jafar, "Degrees of freedom of wireless networks with relays, feedback, cooperation, and full duplex operation," *IEEE Trans. Inform. Theory*, vol. 55, no. 5, pp. 2334–2344, May 2009.

[30] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

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

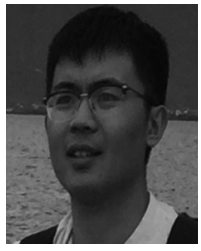
[32] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[33] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 90–103, Jan. 2015.

[34] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

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

[36] A. Afana, V. Asghari, A. Ghrayeb, and S. Affes, "Cooperative relaying in spectrum-sharing systems with beamforming and interference constraints," in *Proc. IEEE 13th Int. Workshop Signal Process. Adv. Wireless Commun.*, Cesme, Turkey, 2012, pp. 429–433.



Tao Zhang (S'13) received the B.S. degree in communication engineering in 2011 from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, where he is currently working toward the Ph.D. degree in communications and information systems.

His current research interest includes cooperative communications, wireless sensor networks, physical layer security, and cognitive radio systems.

Yuzhen Huang (S'12–M'16) received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems both from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2008 and 2013, respectively.

Since 2013, he has been with the College of Communications Engineering, PLA University of Science and Technology, where he is currently an Assistant Professor. Since 2016, he has been a Postdoctoral Research Associate with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include channel coding, multiple-input multiple-output communications systems, cooperative communications, physical layer security, and cognitive radio systems.

Dr. Huang currently serves as an Associate Editor of the *KSII Transactions on Internet and Information Systems*. He and his coauthors received the Best Paper Award at the 2013 Wireless Communications and Signal Processing Conference. He also received the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer Certificate for 2014.

Yueming Cai (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982 and the M.S. degree in microelectronics engineering and the Ph.D. degree in communications and information systems, both from Southeast University, Nanjing, China, in 1988 and 1996, respectively.

His current research interests include multiple-input multiple-output systems, orthogonal frequency-division multiplexing systems, signal processing in communications, cooperative communications, and wireless sensor networks.

Caijun Zhong (S'07–M'10–SM'14) received the B.S. degree in information engineering from Xi'an Jiaotong University, Xi'an, China, in 2004 and the M.S. degree in information security and the Ph.D. degree in telecommunications, both from the University College London, London, U.K., in 2006 and 2010, respectively.

From September 2009 to September 2011, he was a Research Fellow with the Institute for Electronics, Communications and Information Technologies, Queen's University Belfast, Belfast, U.K. Since September 2011, he has been with Zhejiang University, Hangzhou, China, where he is currently an Associate Professor. His research interests include massive multiple-input multiple-output systems, full-duplex communications, wireless power transfer, and physical layer security.

Dr. Zhong is an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS, the *EURASIP Journal of Wireless Communications and Networking*, and the *Journal of Communications and Networks*. He was an Exemplary Reviewer for the IEEE TRANSACTIONS ON COMMUNICATIONS in 2014. He and his coauthors received the Best Paper Award at the 2013 Wireless Communications and Signal Processing Conference. He also received the 2013 IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award.

Weiwei Yang (S'08–M'12) received the B.S., M.S., and Ph.D. degrees from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2003, 2006, and 2011, respectively.

His research interests include orthogonal frequency domain multiplexing systems, signal processing in communications, cooperative communications, wireless sensor networks, and network security.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pithagorion, Samos Island, Greece. He received the University Diploma (five years) and Ph.D. degrees, both in electrical and computer engineering, from the University of Patras, Patron, Greece, in 1987 and 1999, respectively.

From 2000 to 2004, he was a Senior Researcher with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Athens, Greece. In June 2004, he joined the Faculty of Aristotle University of Thessaloniki, Thessaloniki, Greece, where he is currently a Professor in the Electrical and Computer Engineering Department and the Director of Digital Telecommunications Systems and Networks Laboratory. He is also an Honorary Professor with the South West Jiaotong University, Chengdu, China. He is the author or coauthor of more than 400 technical papers published in scientific journals and presented at international conferences. He is also the author of the Greek edition of a book on telecommunications systems and coauthor of the book *Advanced Optical Wireless Communications Systems* (Cambridge Publications, 2012). His research interests include the broad area of digital communications systems with emphasis on wireless communications, optical wireless communications, wireless power transfer and applications, molecular communications, communications and robotics, and wireless security.

Dr. Karagiannidis has been the General Chair, the Technical Program Chair, and a Member of Technical Program Committees at several IEEE and non-IEEE conferences. He was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, a Senior Editor of the IEEE COMMUNICATIONS LETTERS, an Editor of the *EURASIP Journal of Wireless Communications and Networks*, and several times a Guest Editor in the IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS. From 2012 to 2015, he was the Editor-in Chief of the IEEE COMMUNICATIONS LETTERS. He has been selected as the 2015 Thomson Reuters Highly Cited Researcher, and his name was listed in the Thomson Reuters 2015 World's Most Influential Scientific Minds.