Secrecy Outage Performance of Full-Duplex Spectrum Sharing Networks with Different Antenna Reception Schemes

Tao Zhang, *Student Member*, *IEEE*, Yueming Cai, *Senior Member*, *IEEE*, Yuzhen Huang, *Member*, *IEEE*, Trung Q. Duong, *Senior Member*, *IEEE*, and Weiwei Yang, *Member*, *IEEE*

***Abstract*—In this paper, we investigate the secrecy performance of full-duplex multi-antenna spectrum-sharing wiretap networks, in which a jamming signal is simultaneously transmitted by the full-duplex secondary receiver (Bob) based on the zero forcing beamforming (ZFB) algorithm. For the security enhancement, we propose the two antenna reception schemes, i.e., (i) random selection combining (RSC) where Bob selects $L_{\rm B}$ antennas at random to combine the received signals, and (ii) generalized selection combining (GSC) where Bob selects $L_{\rm B}$ strongest antennas to combine the received signals. We derive the exact closed-form expressions for the secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks with ZFB algorithm. In order to explore a new design of the proposed schemes, we provide tractable asymptotic approximations for the secrecy outage probability in high signal-to-noise ratio regime under two distinct scenarios. From the analysis, we demonstrate that a) when the main channel is much better than the eavesdropper's channel, GSC/ZFB scheme achieves full diversity $N_{\rm B}$ while RSC/ZFB scheme only achieves partial diversity $L_{\rm B}$, b) GSC/ZFB scheme achieves better secrecy performance than RSC/ZFB with different antenna numbers at Bob.**

***Index Terms*—Cognitive radio networks, multiple antennas, secrecy outage probability, full duplex.**

I. Introduction

RECENTLY, as an effective solution to alleviate the spectrum shortage problem, cognitive radio has drawn considerable attention from the research community [1]–[4]. In spectrum sharing cognitive radio networks, secondary users (SUs) are allowed to access the licensed spectrum by using underlay, overlay or interweave methods as long as the interference on the primary user (PU) does not exceed a given threshold. Among them, underlay is easy to realize, thus extensive research efforts have been devoted to investigating the cognitive underlay networks with different scenarios, for example, multiple antennas systems [5], relaying systems [6] and multiple-users systems [7].

Nowadays, wireless communication has become an indispensable technique to improve the living standard. Meanwhile, the open and dynamic features of wireless networks have raised concerns regarding the security of the information transmission. As is known to all, the traditional way to ensure the security of data transmission is through various cryptographic schemes in the upper layers. However, with the development of the computation techniques, the traditional cryptographic schemes can be deciphered at vicious nodes. To cope with this problem, as a supplemental approach to encryption, physical layer security has been proposed as a promising solution to improve the security of wireless communications [8], including the secure transmission in cognitive radio networks [9]. However, in cognitive radio networks, the radio frequencies licensed at the PU are shared with SUs, which leads to an increased possibility of the confidential information being eavesdropped from both PU and SUs [10], [11]. Motivated by this, several works have investigated the security issues of cognitive radio networks from the physical layer perspective. In [12], the authors designed the selection combining (SC) scheme in cognitive radio networks with secondary receiver being equipped with multiple antennas. The authors in [13] analyzed the secrecy performance of cognitive radio networks with maximal ratio combining (MRC) scheme at secondary receiver and transmit antenna selection (TAS) scheme at secondary transmitter, and presented an exact closed-form expression for the achievable secrecy rate of the considered system. In [14], generalized selection combining (GSC) scheme was proposed to enhance the security of cognitive radio networks, which offers a performance/implementation tradeoff between SC scheme in [12] and MRC scheme in [13].

In order to further improve the security of information transmission, the cooperative jamming techniques were first proposed in a pioneer work [15]. By designing a special interference signal from other nodes, the difference between the quality of main channel and eavesdropper's channel is enlarged, which can be utilized to improve the secrecy rate [17], [24]. However, the cooperative jamming scheme depends on helper mobility, trustworthiness and synchronization, which makes it difficult to implement. To efficiently solve these

This work was supported by the Natural Science Foundations of China (No. 61471393, 61501507, 61371122 and 61501512) and the Jiangsu Provincial Natural Science Foundation of China (No. BK20150719 and BK20150718). The work of T. Q. Duong was supported by the U.K. Royal Academy of Engineering Research Fellowship under RF1415\14\22 and by the Newton Institutional Link under Grant ID 172719890. This paper was presented in part at the 8th International Conference on Wireless Communications and Signal Processing (WCSP) in Yangzhou, China, Oct. 2016. (Corresponding author: Yueming Cai)

T. Zhang, Y. Cai and W. Yang are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail:ztcool@126.com; 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 (email: yzh_huang@sina.com).

T. Q. Duong is with the School of Electronics, Electrical Engineering and Computer Science, Queens University Belfast, Belfast BT7 1NN, U.K (email: trung.q.duong@qub.ac.uk).

issues and exploit the advantages of jamming techniques, a novel jamming scheme based on the full-duplex technique was designed in [18]–[20], where the legitimate receiver (Bob) can receive the signal from the source (Alice) and transmit jamming signals to illegitimate receiver (Eve) simultaneously. More importantly, compared with the cooperative jamming scheme that uses external helpers, the jamming scheme based on a full-duplex Bob is more easier and reliable to implement. Later, the results in [21] demonstrated that the system using the jamming from full-duplex Bob scheme can achieve a better secrecy performance than the system with a half-duplex Bob. Moreover, with the ability of sending jamming from a full-duplex Bob, the authors proposed a cooperative secrecy transmission scheme and proved its optimality in the sense of achieving the maximal secure degrees of freedom in [22]. However, to the best of the authors' knowledge, the application of full-duplex operation in multi-antenna cognitive radio networks with underlay scheme to improve the secrecy performance has not been well understood.

Motivated by the above discussion, we utilize the spatial diversity into the security enhancement by considering a multi-antenna cognitive radio network, 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). To improve the secrecy performance of the considered network, our aim is to determine the antenna allocation scheme at Bob for reception or for transmission. Specifically, we design two novel secure transmission schemes of multi-antenna full-duplex spectrum-sharing wiretap networks with zero forcing beamforming (ZFB) algorithm, i.e., random selection combining/ZFB scheme and generalized selection combining/ZFB (GSC/ZFB) scheme, respectively. The main contributions of our work are summarized as follows.

- Based on the proposed analytical model, we first derive the closed-form expressions for the secrecy outage probability of multi-antenna spectrum-sharing wiretap networks with two different secrecy transmission schemes, i.e., RSC/ZFB and GSC/ZFB. The derived analytical expressions provide efficient means to evaluate the impact of key system parameters, i.e, the number of antennas and the interference threshold on the secrecy performance of cognitive wiretap networks.
- To achieve additional insights on the application of two proposed schemes into the practical design, we present the asymptotic closed-form expressions for the secrecy outage probability and obtain the secrecy diversity order and secrecy coding gain under two distinct scenarios, i.e., Scenario I: Bob is located close to Alice, and Scenario II: Bob and Eve are both located close to Alice. In particular, we show that, in these two scenarios, the considered system with the proposed schemes achieves different secrecy diversity order and coding gain, respectively.
- Our results demonstrate that GSC/ZFB scheme tends to outperform RSC/ZFB scheme since GSC/ZFB can achieve a more secure degree of freedom of N_{B}, while RSC/ZFB only achieves a secure degree of freedom of L_{B}. Moreover, we find that RSC/ZFB achieves a similar performance to that of GSC/ZFB as L_{B} approaches N_{B}, and the secrecy performance of both schemes is not always improved with the increase of L_{B} under a given N_{B}. Finally, the optimal antenna allocation at Bob for the two proposed schemes is also analyzed.

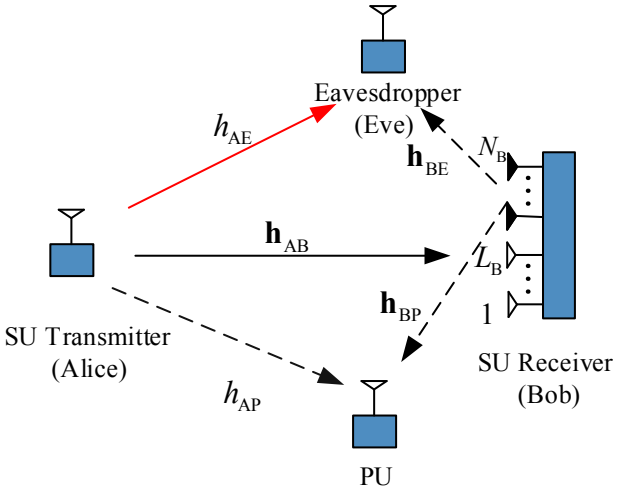

Fig. 1. System model.

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

II. System Model

We consider a multi-antenna cognitive wiretap system as shown in Fig. 1, which consists of a secondary transmitter (Alice), a full-duplex secondary receiver (Bob), an eavesdropper (Eve) and a primary receiver (PR). Similar to [12], [23], we assume that Bob is equipped with N_{B} antennas and other nodes are equipped with a single antenna. Without loss of generality, the following assumptions are adopted throughout this paper: 1) Both main and eavesdropper's channels experience quasi-static independent and non-identical Rayleigh fading, 2) The primary transmitter is far away from Bob and Eve as in [7], [12], thus the interference from the primary transmitter can be ignored at Bob and Eve, and 3) Similar to [22], [24]–[31], the channel state information (CSI) between Eve and Bob link is known at Bob[1], while the CSI of Alice to Eve link is not available at Alice.

To exploit the advantages of multiple antennas and full-duplex techniques, we design two new secure transmission schemes in this paper, in which L_{B} antennas at Bob are allocated for reception, and the remaining $(N_{\mathrm{B}}-L_{\mathrm{B}})$ antennas are

[1]This can be achieved in practical scenarios where Eve is another active user in the system, e.g., in a time division multiple-access (TDMA) environment. In this scenario, the Eve plays dual roles as legitimate ones for transmitting and eavesdroppers for receiving confidential information [22], [32], such that Bob can estimate the eavesdropper's channel during Eve's transmissions.

used to send a weighted jamming signal to degrade the quality of service at Eve. Among different jamming algorithms, we choose ZFB algorithm due to the lower computational load of implementation. In addition, the weight vector $\mathbf{w}_{\mathrm{ZF}}$ based on ZFB algorithm can be designed as

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

where $\dagger$ is the conjugate transpose operator and $\|\cdot\|_F$ denotes the Frobenius norm, $\mathbf{h}_{\mathrm{BE}}$ denotes the $(N_{\mathrm{B}} - L_{\mathrm{B}}) \times 1$ channel vector between the remaining $(N_{\mathrm{B}} - L_{\mathrm{B}})$ antennas at Bob and the Eve with entries following identical and independently distributed Rayleigh fading with parameter $\lambda_{\mathrm{BE}} \propto d_{\mathrm{BE}}^{-\beta}$, where d_{BE} is the distance between Bob and Eve and β is the path loss factor. In addition, $\mathbf{h}_{\mathrm{BP}}$ represents the $(N_{\mathrm{B}} - L_{\mathrm{B}}) \times 1$ channel vector between the remaining $(N_{\mathrm{B}} - L_{\mathrm{B}})$ antennas at Bob and the PR with entries following identical and independently distributed Rayleigh fading with parameter $\lambda_{\mathrm{BP}} \propto d_{\mathrm{BP}}^{-\beta}$, where d_{BP} is the distance between Bob and PR. Moreover, $\mathbf{h}_{\mathrm{BP}}$ can be obtained through a spectrum-band manager [33]. Now, with the help of [34, Theorems 4.21, 4.22] and [35, Lemma 1], the optimal weight vector is given by

$$\mathbf{w}_{\mathrm{ZF}} = \frac{\mathrm{T}^{\perp}\mathbf{h}_{\mathrm{BE}}}{\|\mathrm{T}^{\perp}\mathbf{h}_{\mathrm{BE}}\|}, \tag{2}$$

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 $(N_{\mathrm{B}} - L_{\mathrm{B}} - 1)$.

Given L_{B} reception antennas at Bob, we now propose the two different combining reception schemes. In the first scheme, i.e., RSC/ZFB, Bob selects L_{B} antennas at random to combine the received signals and simultaneously utilizes the remaining $(N_{\mathrm{B}} - L_{\mathrm{B}})$ antennas to send a weighted jamming to degrade the quality of eavesdropper's channel. In the second scheme, i.e., GSC/ZFB, Bob first selects L_{B} strongest antennas based on the CSI of the main channel to combine the received signals, and uses the remaining $(N_{\mathrm{B}} - L_{\mathrm{B}})$ antennas to send the jamming to degrade the quality of eavesdropper's channel. As a result, the instantaneous SNR of the main channel with RSC/ZFB scheme is given by[2]

$$\gamma_{\mathrm{B}_1} = \sum_{i=1}^{L_{\mathrm{B}}} \frac{P_S}{\sigma_{\mathrm{B}}^2}\left(\left|h_{\mathrm{AB}_i}\right|^2\right), \tag{3}$$

where σ_{B}^2 is the noise variance at Bob, $\left|h_{\mathrm{AB}_i}\right|^2$ is the channel gain between Alice and the i-th antenna at Bob with $\mathrm{E}\left[\left|h_{\mathrm{AB}_i}\right|^2\right] = \lambda_{\mathrm{AB}} \propto d_{\mathrm{AB}}^{-\beta}$, where d_{AB} is the distance between Alice and Bob. In the context of spectrum sharing networks, transmission of secondary node cannot cause a harmful interference on the primary network. As such, the transmit power $P_S = \min\left(\frac{Q}{|h_{\mathrm{AP}}|^2}, P_t\right)$, where Q and P_t denote the interference temperature constraint at PR and the maximum transmit power constraint at Alice, respectively, $|h_{\mathrm{AP}}|^2$ is the channel gain between Alice and PR with $\mathrm{E}\left[|h_{\mathrm{AP}}|^2\right] = \lambda_{\mathrm{AP}} \propto d_{\mathrm{AP}}^{-\beta}$, where d_{AP} is the distance between Alice and PR.

Similarly, the instantaneous SNR of the main channel with GSC/ZFB scheme can be computed as

$$\gamma_{\mathrm{B}_2} = \sum_{j=1}^{L_{\mathrm{B}}} \frac{P_S}{\sigma_{\mathrm{B}}^2}\left(\left|h_{\mathrm{AB}_{(j)}}\right|^2\right), \tag{4}$$

where $\left|h_{\mathrm{AB}_{(j)}}\right|^2$ is the channel gain between Alice and the j-th strongest antenna at Bob particularly for GSC/ZFB scheme and we arrange $\left\{\left|h_{\mathrm{AB}_{(j)}}\right|^2, 1 \le j \le N_{\mathrm{B}}\right\}$ in descending order as $\left|h_{\mathrm{AB}_{(1)}}\right|^2 \ge \left|h_{\mathrm{AB}_{(2)}}\right|^2 \ge \cdots \ge \left|h_{\mathrm{AB}_{(N_{\mathrm{B}})}}\right|^2$.

In addition, for the proposed two schemes, the instantaneous signal-to-interference-plus-noise ratio (SINR) of the eavesdropper's channel can be expressed as

$$\gamma_{\mathrm{E}} = \frac{P_S|h_{\mathrm{AE}}|^2}{P_Z\left|\mathbf{h}_{\mathrm{BE}}^{\dagger}\mathbf{w}_{\mathrm{ZF}}\right|^2 + \sigma_{\mathrm{E}}^2}, \tag{5}$$

where σ_{E}^2 is the noise variance at Eve, $|h_{\mathrm{AE}}|^2$ is the channel gain between Alice and Eve with $\mathrm{E}\left[|h_{\mathrm{AE}}|^2\right] = \lambda_{\mathrm{AE}} \propto d_{\mathrm{AE}}^{-\beta}$, where d_{AE} is the distance between Alice and Eve.

Now, according to [41], the achievable secrecy rate of the full-duplex multi-antenna spectrum-sharing wiretap network is given by

$$C_S = \begin{cases} \log_2\left(1 + \gamma_{\mathrm{B}_i}\right) - \log_2\left(1 + \gamma_{\mathrm{E}}\right), & \gamma_{\mathrm{B}_i} > \gamma_{\mathrm{E}} \\ 0, & \gamma_{\mathrm{B}_i} \le \gamma_{\mathrm{E}} \end{cases} \tag{6}$$

where $i \in \{1, 2\}$ represents RSC/ZFB scheme and GSC/ZFB scheme, respectively.

To make the following analysis more tractable, we first define $\rho = \frac{Q}{P_t}$, $\bar{\gamma}_{\mathrm{B}} = \frac{P_t}{\sigma_{\mathrm{B}}^2}\lambda_{\mathrm{AB}} = \frac{Q}{\rho\sigma_{\mathrm{B}}^2}\lambda_{\mathrm{AB}}$, $\bar{\gamma}_{\mathrm{E}} = \frac{P_t}{\sigma_{\mathrm{E}}^2}\lambda_{\mathrm{AE}} = \frac{Q}{\rho\sigma_{\mathrm{E}}^2}\lambda_{\mathrm{AE}}$, and $\bar{\gamma}_Z = \frac{P_Z}{\sigma_{\mathrm{E}}^2}\lambda_{\mathrm{BE}}$.

III. Secrecy Performance Analysis

In this section, we investigate the secrecy outage performance of the full-duplex multi-antenna spectrum-sharing wiretap networks with the proposed two schemes. From the definition of secrecy outage probability, it can be mathematically represented as [42]

$$\begin{aligned} P_{\mathrm{out}}\left(R_s\right) &= \Pr\left(C_S < R_s\right) \\ &= \int_0^{\infty} F_{\gamma_{\mathrm{B}_i}}\left(2^{R_s}\left(1 + x\right) - 1\right) f_{\gamma_{\mathrm{E}}}\left(x\right) dx. \end{aligned} \tag{7}$$

where R_s is a given transmission rate, $F_{\gamma_{\mathrm{B}_i}}(\cdot)$ is the cumulative distribution function (CDF) of γ_{B_i}, and $f_{\gamma_{\mathrm{E}}}(\cdot)$ is the probability density function (PDF) of γ_{E}.

We next present a detailed analysis for the secrecy outage probability of full-duplex multi-antenna spectrum sharing networks with RSC/ZFB and GSC/ZFB schemes.

[2]Please note that, for the full-duplex mechanism, we assume that the self-interference can be completely suppressed at Bob. As that in [18], [20], [22], [36]–[39], this assumption is widely used to study the information-theory oriented performance, i.e., capacity and outage probability. Although full cancelation of self-interference cannot be achieved with the help of state-of-the-art techniques in [40].

A. RSC/ZFB scheme

Since both γ_{B_1} and γ_{E} contain the common random variable (RV), $G = |h_{\mathrm{AP}}|^2$, the traditional means to analyze the secrecy outage performance are not applicable due to the statistical dependence. In order to tackle this problem, the condition-and-average approach is adopted in our analysis. With this in mind, we first present the CDF of γ_{B_1} and PDF of γ_{E} conditioned on G in the following two lemmas.

Lemma 1. *The CDF of γ_{B_1} conditioned on the RV G is given by*

$$F_{\gamma_{\mathrm{B}_1}}(x|G) = 1 - e^{-\frac{\sigma_{\mathrm{B}}^2 x}{P_S \lambda_{\mathrm{AB}}}} \sum_{k=0}^{L_{\mathrm{B}}-1} \frac{1}{k!} \left(\frac{\sigma_{\mathrm{B}}^2 x}{P_S \lambda_{\mathrm{AB}}} \right)^k. \quad (8)$$

Proof: According to (3) and with the help of [43], the desired result can be easily derived after some simple manipulations. ∎

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

$$\begin{aligned} f_{\gamma_{\mathrm{E}}}(y|G) = {} & \frac{\sigma_{\mathrm{E}}^2}{P_S \lambda_{\mathrm{AE}}} \left(\frac{\lambda_{\mathrm{AE}} P_S}{P_Z \lambda_{\mathrm{BE}} y + \lambda_{\mathrm{AE}} P_S} \right)^{N_{\mathrm{B}}-L_{\mathrm{B}}-1} \\ & \times \exp\left(-\frac{\sigma_{\mathrm{E}}^2 y}{P_S \lambda_{\mathrm{AE}}} \right) + \exp\left(-\frac{\sigma_{\mathrm{E}}^2 y}{P_S \lambda_{\mathrm{AE}}} \right) \\ & \times \frac{(N_{\mathrm{B}} - L_{\mathrm{B}} - 1) P_Z \lambda_{\mathrm{BE}} (P_S \lambda_{\mathrm{AE}})^{N_{\mathrm{B}}-L_{\mathrm{B}}-1}}{(P_Z \lambda_{\mathrm{BE}} y + P_S \lambda_{\mathrm{AE}})^{N_{\mathrm{B}}-L_{\mathrm{B}}}}. \end{aligned} \quad (9)$$

Proof: See Appendix A. ∎

Armed with (8) and (9), we now provide the secrecy outage probability of RSC/ZFB scheme in the following theorem.

Theorem 1. *The secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks using RSC/ZBF scheme can be derived as*

$$\begin{aligned} P_{\mathrm{out},1}(R_s) = 1 - {} & \left\{ \sum_{k=0}^{L_{\mathrm{B}}-1} \frac{1}{k!} \sum_{a=0}^{k} \binom{k}{a} \left(2^{R_s}-1\right)^{k-a} \left(2^{R_s}\right)^a \right. \\ & \times \left[\frac{(\bar{\gamma}_{\mathrm{E}})^a}{(\bar{\gamma}_{\mathrm{B}})^k (\bar{\gamma}_Z)^{a+1}} \Psi\left(a+1, 3+L_{\mathrm{B}}+a-N_{\mathrm{B}}; \frac{\bar{\gamma}_{\mathrm{B}} + 2^{R_s}\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_{\mathrm{Z}}} \right) \right. \\ & \times \Gamma(a+1) + \frac{(N_{\mathrm{B}} - L_{\mathrm{B}} - 1)(\bar{\gamma}_{\mathrm{E}})^a}{(\bar{\gamma}_{\mathrm{B}})^k (\bar{\gamma}_Z)^a} \Gamma(a+1) \\ & \left. \left. \times \Psi\left(a+1, 2+L_{\mathrm{B}}+a-N_{\mathrm{B}}; \frac{\bar{\gamma}_{\mathrm{B}} + 2^{R_s}\bar{\gamma}_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{B}}\bar{\gamma}_Z} \right) \right] \right\} \\ & \times \left\{ \left[1 - \exp\left(-\frac{\rho}{\lambda_{\mathrm{AP}}} \right) \right] \exp\left(-\frac{2^{R_s}-1}{\bar{\gamma}_{\mathrm{B}}} \right) \right. \\ & + \left[\frac{\left(2^{R_s}-1\right)\lambda_{\mathrm{AP}} + \rho\bar{\gamma}_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}\lambda_{\mathrm{AP}}} \right]^{a-k-1} \\ & \left. \times \frac{\rho}{\lambda_{\mathrm{AP}}} \Gamma\left(k-a+1, \frac{\left(2^{R_s}-1\right)\lambda_{\mathrm{AP}} + \rho\bar{\gamma}_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}\lambda_{\mathrm{AP}}} \right) \right\}. \end{aligned} \quad (10)$$

where $\Gamma(\cdot)$ is the Gamma function [46, Eq. (8.310.1)] and $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function [46, Eq. (8.350.2)].

Proof: See Appendix B. ∎

Remark 1: According to **Theorem 1**, we find that although the interference from Bob to Eve is high when $L_{\mathrm{B}} = 1$, the secrecy performance of the considered system is poor due to the legal link from Alice to Bob is weak. On the other hand, when L_{B} is large, i.e., $(N_{\mathrm{B}}-2)$, the secrecy performance of the considered system is also poor due to the interference at Eve is weak. Hence, there exists an optimal L_{B}^* to minimize the secrecy outage probability of the considered system. Actually, it can be modeled as

$$\begin{aligned} L_{\mathrm{B}}^* = {} & \arg\min_{L_{\mathrm{B}}} P_{\mathrm{out},1}(L_{\mathrm{B}}) \\ & s.t.\ 1 \le L_{\mathrm{B}} \le N_{\mathrm{B}} - 2 \end{aligned} \quad (11)$$

Please note, obtaining a closed-form expression of L_{B}^* directly from (11) is intractable. As an alternative, it can be solved numerically as in [44].

B. GSC/ZFB scheme

Similar to RSC/ZFB scheme, γ_{B_2} and γ_{E} are statistically dependent due to the common RV G. As such, we first obtain the conditional CDF of γ_{B_2} in the following lemma.

Lemma 3. *The conditional CDF of γ_{B_2} can be derived as*

$$\begin{aligned} F_{\gamma_{\mathrm{B}_2}}(x|G) = {} & \binom{N_{\mathrm{B}}}{L_{\mathrm{B}}} \sum_{S} \sum_{k=0}^{L_{\mathrm{B}}} l_k x^{\mu_k} \\ & \times \left(\frac{\sigma_{\mathrm{B}}^2}{P_S \lambda_{\mathrm{AB}}} \right)^{\mu_k} \exp\left(-\frac{\sigma_{\mathrm{B}}^2 \nu_k x}{P_S \lambda_{\mathrm{AB}}} \right), \end{aligned} \quad (12)$$

where $\mathcal{S} = \left\{ (n_0, n_1) \mid \sum_{j=0}^{1} n_j = N_{\mathrm{B}} - L_{\mathrm{B}} \right\}$, and l_k is given by

$$l_k = \begin{cases} \frac{(N_{\mathrm{B}}-L_{\mathrm{B}})!(-1)^{n_1}}{\prod_{j=0}^{1} n_j!} \left(\frac{n_1}{L_{\mathrm{B}}} + 1 \right)^{-1}, & k = 0 \\ \frac{(N_{\mathrm{B}}-L_{\mathrm{B}})!(-1)^{n_1}}{\prod_{j=0}^{1} n_j!} \left(\Upsilon_1 + \Upsilon_2 - \frac{1-\mathrm{sgn}(n_1)}{(k-1)!} \right)^{-1} & \\ \qquad , 1 \le k \le L_{\mathrm{B}} - 1 & \\ \frac{(N_{\mathrm{B}}-L_{\mathrm{B}})!(-1)^{n_1}}{\prod_{j=0}^{1} n_j!} \left(\Upsilon_3 + \Upsilon_4 - \frac{1-\mathrm{sgn}(n_1)}{(k-1)!} \right)^{-1}, & k = L_{\mathrm{B}} \end{cases} \quad (13)$$

with Υ_1, Υ_2, Υ_3, and Υ_4 as

$$\Upsilon_1 = -\frac{\mathrm{sgn}(n_1)}{(k-1)!} \left(\frac{n_1}{L_{\mathrm{B}}} + 1 \right)^{-1}, \quad (14)$$

$$\Upsilon_2 = \frac{(-1)^{1-k_2} \mathrm{sgn}(n_1)}{(k-1)!} \left(\frac{n_1}{L_{\mathrm{B}}} + 1 \right)^{-1} \left(\frac{n_1}{L_{\mathrm{B}}} \right)^{k_2-1}, \quad (15)$$

$$\Upsilon_3 = -\mathrm{sgn}(n_1) \left(\frac{n_1}{L_{\mathrm{B}}} + 1 \right)^{-(1-k+L_{\mathrm{B}})}, \quad (16)$$

$$\begin{aligned} \Upsilon_4 = {} & \mathrm{sgn}(n_1) \sum_{l=1}^{L_{\mathrm{B}}-1} (-1)^{l+1} \binom{L_{\mathrm{B}}-k+l-1}{l-1} \\ & \times \left(\frac{n_1}{L_{\mathrm{B}}} \right)^{-(L_{\mathrm{B}}-k+l)}, \end{aligned} \quad (17)$$

where μ_k and ν_k are expressed as

$$\mu_k = \begin{cases} 0, & k = 0 \\ k-1, & 1 \le k \le L_{\rm B}-1 \\ k - \mathrm{sgn}(n_1)\,(L_{\rm B}-1) - 1, & k = L_{\rm B} \end{cases} \tag{18}$$

$$\nu_k = \begin{cases} 0, & k = 0 \\ 1, & 1 \le k \le L_{\rm B}-1 \\ \frac{L_{\rm B}+n_1}{L_{\rm B}}, & k = L_{\rm B} \end{cases} \tag{19}$$

Proof: The proof can be found in [45, Theorem 1]. ∎

Now, for GSC/ZFB scheme, we have the following key result.

Theorem 2. *The secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks using GSC/ZBF scheme is given by*

$$\begin{aligned} P_{\mathrm{out},2}\left(R_s\right) =& \binom{N_{\rm B}}{L_{\rm B}} \sum_{S} \sum_{k=0}^{L_{\rm B}} l_k \sum_{m=0}^{\mu_k} \binom{\mu_k}{m} \frac{\left(2^{R_s}-1\right)^{\mu_k-m}\left(2^{R_s}\right)^m}{\left(\bar{\gamma}_{\rm B}\right)^{\mu_k}} \\ &\times \Gamma\left(m+1\right)\left[\frac{1}{\bar{\gamma}_Z}\Psi\left(m+1,3+L_{\rm B}+m-N_{\rm B};\frac{\bar{\gamma}_{\rm B}+\bar{\gamma}_{\rm E}\nu_k 2^{R_s}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right)\right. \\ &\left.+\left(N_{\rm B}-L_{\rm B}-1\right)\Psi\left(m+1,2+L_{\rm B}+m-N_{\rm B};\frac{\bar{\gamma}_{\rm B}+\bar{\gamma}_{\rm E}\nu_k 2^{R_s}}{\bar{\gamma}_{\rm B}\bar{\gamma}_{\rm Z}}\right)\right] \\ &\times \frac{\left(\bar{\gamma}_{\rm E}\right)^m}{\left(\bar{\gamma}_Z\right)^m}\left\{\left[1-\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)\right]\exp\left(-\frac{\nu_k\left(2^{R_s}-1\right)}{\bar{\gamma}_{\rm B}}\right)\right. \\ &+\frac{\rho}{\lambda_{\rm AP}}\left[\frac{\nu_k\left(2^{R_s}-1\right)\lambda_{\rm AP}+\rho\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\lambda_{\rm AP}}\right]^{-\mu_k+m-1} \\ &\left.\times\Gamma\left(\mu_k-m+1,\frac{\nu_k\left(2^{R_s}-1\right)\lambda_{\rm AP}+\rho\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\lambda_{\rm AP}}\right)\right\}, \end{aligned} \tag{20}$$

where $\Psi\left(\cdot,\cdot;\cdot\right)$ is the confluent hypergeometric function of the second kind [46, Eq. (9.211.4)].

Proof: See Appendix C. ∎

Remark 2: Similar to RSC/ZFB scheme, there is an optimal $L_{\rm B}^*$ for GSC/ZFB scheme, which can be numerically achieved.

IV. High SNR Analysis

Although the exact secrecy outage probability expressions obtained in **Theorems 1** and **2** allow us to evaluate the secrecy performance of the two proposed schemes, their intractability cannot reveal any additional insights on the effect of networks parameters. Thus, in this section, we turn our attention to analyze the asymptotic secrecy outage probability in high SNR regimes. Specifically, two distinct scenarios are considered: 1) $\bar{\gamma}_{\rm B} \to \infty$ and fixed $\bar{\gamma}_{\rm E}$, that is a scenario where Bob is located close to Alice while the eavesdropper's channel is severely blocked due to heavy shadowing and 2) $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E} \to \infty$, that is a scenario where Bob and Eve are both located close to Alice, i.e., the main channel and eavesdropper's channel have a similar quality.

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

1) RSC/ZFB Scheme:

Corollary 1. *The secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks with RSC/ZFB scheme under $\bar{\gamma}_{\rm B} \to \infty$ and fixed $\bar{\gamma}_{\rm E}$ is approximated as*

$$P_{out,1}\left(R_s\right) \approx \Delta_1 \bar{\gamma}_{\rm B}^{-L_{\rm B}}, \tag{21}$$

where Δ_1 is given by

$$\begin{aligned} \Delta_1 =& \frac{1}{\left(L_{\rm B}\right)!}\sum_{i=0}^{L_{\rm B}}\binom{L_{\rm B}}{i}\left(2^{R_s}-1\right)^{L_{\rm B}-i}\left(2^{R_s}\right)^i\Gamma\left(i+1\right) \\ &\times\left[\frac{\left(\bar{\gamma}_{\rm E}\right)^i}{\left(\bar{\gamma}_Z\right)^{i+1}}\Psi\left(i+1,3+L_{\rm B}+i-N_{\rm B};\frac{1}{\bar{\gamma}_Z}\right)\right. \\ &\left.+\left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_Z}\right)^i\left(N_{\rm B}-L_{\rm B}-1\right)\Psi\left(i+1,2+L_{\rm B}+i-N_{\rm B};\frac{1}{\bar{\gamma}_Z}\right)\right] \\ &\times\left[1-\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)+\frac{\lambda_{\rm AP}^{L_{\rm B}}}{\rho^{L_{\rm B}}}\Gamma\left(L_{\rm B}+1,\frac{\rho}{\lambda_{\rm AP}}\right)\right]. \end{aligned} \tag{22}$$

Proof: See Appendix D. ∎

2) GSC/ZFB Scheme:

Corollary 2. *The secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks with GSC/ZFB under $\bar{\gamma}_{\rm B} \to \infty$ and fixed $\bar{\gamma}_{\rm E}$ is approximated as*

$$P_{\mathrm{out},2}\left(R_s\right) \approx \Delta_2 \bar{\gamma}_{\rm B}^{-N_{\rm B}}, \tag{23}$$

where Δ_2 is given by

$$\begin{aligned} \Delta_2 =& \binom{N_{\rm B}}{L_{\rm B}}\frac{\left(N_{\rm B}-L_{\rm B}\right)!}{\left(L_{\rm B}\right)^{N_{\rm B}-L_{\rm B}}\left(N_{\rm B}\right)!}\sum_{i=0}^{N_{\rm B}}\binom{N_{\rm B}}{i}\left(2^{R_s}-1\right)^{N_{\rm B}-i} \\ &\times\left(2^{R_s}\right)^i\Gamma\left(i+1\right)\left[\frac{\left(\bar{\gamma}_{\rm E}\right)^i}{\left(\bar{\gamma}_Z\right)^{i+1}}\Psi\left(i+1,3+L_{\rm B}+i-N_{\rm B};\frac{1}{\bar{\gamma}_Z}\right)\right. \\ &\left.+\left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_Z}\right)^i\left(N_{\rm B}-L_{\rm B}-1\right)\Psi\left(i+1,2+L_{\rm B}+i-N_{\rm B};\frac{1}{\bar{\gamma}_Z}\right)\right] \\ &\times\left[1-\exp\left(-\frac{\rho}{\lambda_{\rm AP}}\right)+\frac{\lambda_{\rm AP}^{N_{\rm B}}}{\rho^{N_{\rm B}}}\Gamma\left(N_{\rm B}+1,\frac{\rho}{\lambda_{\rm AP}}\right)\right]. \end{aligned} \tag{24}$$

Proof: When $\bar{\gamma}_{\rm B} \to \infty$, the approximated conditional CDF of $\gamma_{\rm B_2}$ is given by

$$F_{\gamma_{\rm B_2}}\left(x|G\right) \approx \binom{N_{\rm B}}{L_{\rm B}}\frac{\left(N_{\rm B}-L_{\rm B}\right)!}{\left(L_{\rm B}\right)^{N_{\rm B}-L_{\rm B}}\left(N_{\rm B}\right)!}\left(\frac{x}{\bar{\gamma}_{\rm B}}\right)^{N_{\rm B}}. \tag{25}$$

Then, following similar procedure as in the proof of Corollary 1, the desired result can be obtained. ∎

Remark 3: From the above results, we find that RSC/ZFB and GSC/ZFB schemes achieve different secrecy diversity, i.e., $L_{\rm B}$ and $N_{\rm B}$ under Scenario I. Specifically, they are independent of the parameters of primary networks and the eavesdropper's channel. However, the parameters of the eavesdropper's channel and primary networks degrade the secrecy performance of the considered system through the secrecy coding gain, i.e.,

$$\mathcal{G}_1 = {\Delta_1}^{-\frac{1}{L_{\rm B}}}, \tag{26}$$

and

$$\mathcal{G}_2 = {\Delta_2}^{-\frac{1}{N_{\rm B}}}. \tag{27}$$

It is worth noting from the above Remark, the secrecy diversity order and coding gain of RSC/ZFB scheme are similar to GSC/ZFB scheme when $L_{\rm B}$ approaches $N_{\rm B}$. That is to say, RSC/ZFB scheme will achieve a similar performance to that of GSC/ZFB scheme as $L_{\rm B}$ approaches $N_{\rm B}$.

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

Now, we focus on analyzing the approximated secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks under Scenario II.

1) RSC/ZFB Scheme:

Corollary 3. *The secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks with RSC/ZFB scheme under $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E} \to \infty$ is given by*

$$\begin{aligned} P_{{\rm out},1}\left(R_s\right) \approx 1 - \sum_{k=0}^{L_{\rm B}-1} \frac{\left(2^{R_s}\right)^k}{k!} \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right)^k \Gamma\left(k+1\right) \\ \times \left[\frac{1}{\bar{\gamma}_Z} \Psi\left(k+1, 3+k+L_{\rm B}-N_{\rm B}; \frac{\bar{\gamma}_{\rm B}+2^{R_s}\bar{\gamma}_{\rm E}}{\bar{\gamma}_Z\bar{\gamma}_{\rm B}}\right)\right. \\ \left. +(N_{\rm B}-L_{\rm B}-1)\,\Psi\left(k+1, 2+k+L_{\rm B}-N_{\rm B}; \frac{\bar{\gamma}_{\rm B}+2^{R_s}\bar{\gamma}_{\rm E}}{\bar{\gamma}_Z\bar{\gamma}_{\rm B}}\right)\right]. \end{aligned} \tag{28}$$

Proof: See Appendix E. ∎

2) GSC/ZFB Scheme:

Corollary 4. *The secrecy outage probability of full-duplex multi-antenna spectrum-sharing wiretap networks with GSC/ZFB scheme under $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E} \to \infty$ is given by*

$$\begin{aligned} P_{{\rm out},2}\left(R_s\right) \approx \binom{N_{\rm B}}{L_{\rm B}} \sum_{S} \sum_{k=0}^{L_{\rm B}} l_k \left(2^{R_s}\right)^{\mu_k} \Gamma\left(\mu_k+1\right) \\ \times \left[\Psi\left(\mu_k+1, 3+\mu_k+L_{\rm B}-N_{\rm B}; \frac{\nu_k 2^{R_s}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right)\right. \\ \times \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right)^{\mu_k} \frac{1}{\bar{\gamma}_Z} + \left(\frac{\bar{\gamma}_{\rm E}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right)^{\mu_k} (N_{\rm B}-L_{\rm B}-1) \\ \left. \times \Psi\left(\mu_k+1, 2+\mu_k+L_{\rm B}-N_{\rm B}; \frac{\nu_k 2^{R_s}\bar{\gamma}_{\rm E}+\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right)\right]. \end{aligned} \tag{29}$$

Proof: Following similar procedure as in the proof of Corollary 3, the above result can be easily obtained. ∎

Remark 4: Compared with the analysis in Scenario I, we find that there exists a secrecy outage floor for both schemes under $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E} \to \infty$, which indicates that the secrecy diversity of the considered system reduces to zero in this scenario.

C. Comparison of the Proposed Schemes

Now, in this section, we provide a comprehensive comparison between RSC/ZFB scheme and GSC/ZFB scheme. As discussed in the above, $L_{\rm B}$ receive antennas are randomly selected without any comparison among $N_{\rm B}$ antennas in RSC/ZFB scheme. While in GSC/ZFB scheme, the $L_{\rm B}$ strongest receive antennas at Bob are selected from $N_{\rm B}$ antennas after comparison. In addition, the proposed two schemes utilize the remaining $(N_{\rm B}-L_{\rm B})$ antennas to send the weighted jamming signal to improve the secrecy performance of the considered system. Motivated by these observations, the differences between RSC/ZFB scheme and GSC/ZFB scheme are summarized in Table I.

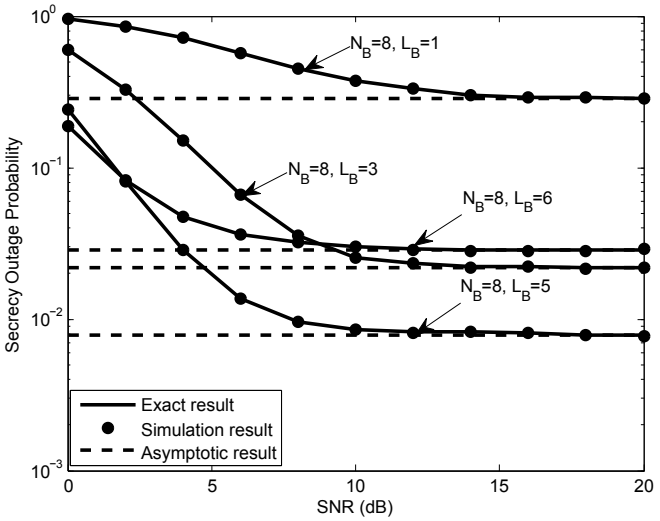

Fig. 2. Secrecy outage probability vs number of antennas for RSC/ZFB scheme, where the interference threshold $Q = 10$dB.

V. Numerical Results

In this section, representative numerical results are provided to evaluate the impacts of different system parameters, i.e., the number of antennas, and different antenna reception schemes, on the secrecy outage performance. Without loss of generality, we assume that the SNR is $\frac{P_t}{\sigma_{\rm B}^2}$, the secrecy rate is $R_s = 2$, and the noise variance is $\sigma_{\rm B}^2 = \sigma_{\rm E}^2 = 1$. In addition, the distance between two nodes is normalized to unit. As shown in these figures, the Monte Carlo simulation results are in exact agreement with the analytical ones, which corroborates the accuracy of the analytical expressions.

Figs. 2 and 3 illustrate the secrecy outage probability of RSC/ZFB and GSC/ZFB schemes with different selection number of antennas, $L_{\rm B}$, for a given $N_{\rm B}$, respectively. As can be expected, we find that the secrecy outage probability is improved by increasing $L_{\rm B}$, but it does not always improve with the increment of $L_{\rm B}$, for example, $L_{\rm B} = 6$ in Fig. 2 and $L_{\rm B} = 5$ and 6 in Fig. 3. This is rather intuitive, since increasing $L_{\rm B}$ results in decreasing the number of antennas that Bob can utilize to transmit jamming signals to confuse Eve. In addition, the secrecy outage floor demonstrates the accuracy of the analysis in (28) and (29), which reveals that the secrecy outage floor appears and the achievable secrecy diversity order reduces to zero under Scenario II.

Fig. 4 plots the secrecy outage probability versus SNR for RSC/ZFB scheme and GSC/ZFB scheme when Bob is located close to Alice. It is observed that, RSC/ZFB and GSC/ZFB schemes achieve different secrecy diversity order of $L_{\rm B}$ and

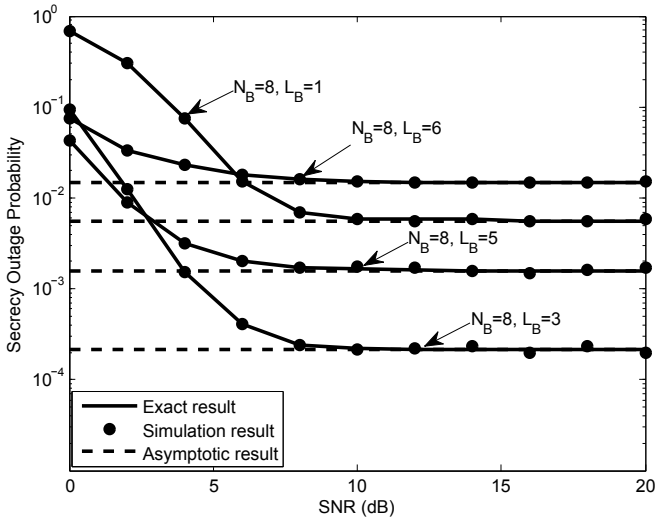

Fig. 3. Secrecy outage probability vs number of antennas for GSC/ZFB scheme, where the interference threshold $Q = 10$dB.

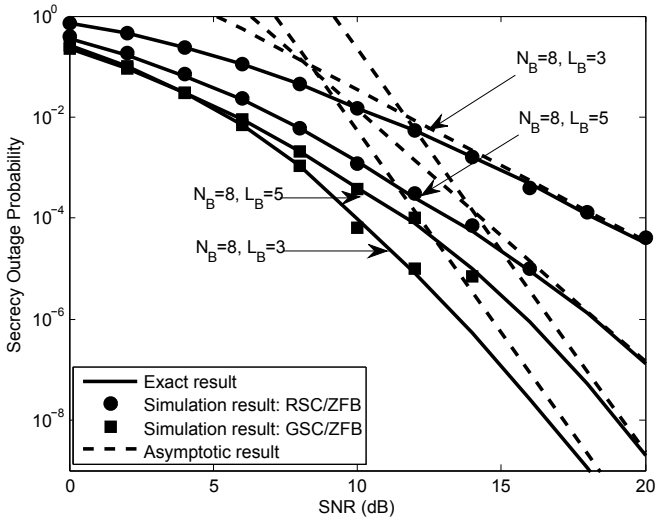

Fig. 4. Exact and asymptotic secrecy outage probabilities for RSC/ZFB and GSC/ZFB schemes, when $\rho = 1$ and $\bar{\gamma}_{\rm E} = 10$dB, respectively.

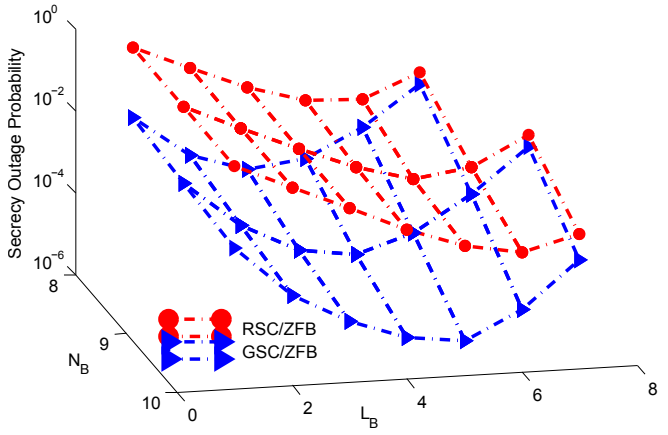

Fig. 5. Secrecy outage probabilities of RSC/ZFB and GSC/ZFB schemes for different number $L_{\rm B}$ and $N_{\rm B}$ when $P_t = 20$dB.

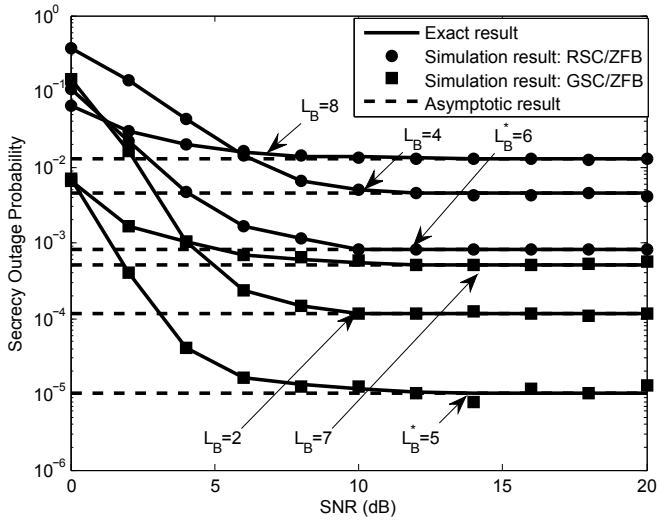

Fig. 6. Secrecy outage probabilities of RSC/ZFB and GSC/ZFB schemes for random $L_{\rm B}$ and optimal $L_{\rm B}^*$ when $N_{\rm B} = 10$ and interference threshold $Q = 10$dB, respectively.

$N_{\rm B}$ under Scenario I, as indicated in (21) and (23), respectively. Furthermore, we can see that GSC/ZFB scheme achieves a better performance than RSC/ZFB scheme. In addition, for GSC/ZFB scheme, the secrecy outage performance of $L_{\rm B} = 3$ outperforms that of $L_{\rm B} = 5$ due to the fact that the coding gain under $L_{\rm B} = 3$ is higher.

Fig. 5 shows the secrecy outage probability of the considered system under different $L_{\rm B}$ for both RSC/ZFB and GSC/ZFB schemes when the number of antennas at Bob $N_{\rm B} = 8, 9, 10$, respectively. As shown in the figure, we can see that both the secrecy outage performance of the considered system with RSC/ZFB and GSC/ZFB schemes improves when the number of antennas at Bob $N_{\rm B}$ increases. In addition, GSC/ZFB scheme achieves better performance than RSC/ZFB scheme. However, this performance gap is narrowed when $L_{\rm B}$ approaches $N_{\rm B}$. The main reason is that when $L_{\rm B}$ approaches $N_{\rm B}$, the proposed two schemes become similar as demonstrated in **Remark 3**.

TABLE I
COMPARISON OF RSC/ZFB AND GSC/ZFB SCHEMES

	RSC/ZFB	**GSC/ZFB**
Cooperative jamming antennas	$N_{\rm B} - L_{\rm B}$	$N_{\rm B} - L_{\rm B}$
Antenna number $N_{\rm B}$, $L_{\rm B}$ requirements	$N_{\rm B} \geq 3$, $L_{\rm B} \leq N_{\rm B} - 2$	$N_{\rm B} \geq 3$, $L_{\rm B} \leq N_{\rm B} - 2$
Diversity order	$L_{\rm B}/0$	$N_{\rm B}/0$
Coding gain	$\mathcal{G}_1 = \Delta_1^{-\frac{1}{L_{\rm B}}}$	$\mathcal{G}_2 = \Delta_2^{-\frac{1}{N_{\rm B}}}$

Fig. 6 plots the secrecy outage probability of the system under random $L_{\rm B}$ and optimal $L_{\rm B}^*$ for both RSC/ZFB and GSC/ZFB schemes when $N_{\rm B}=10$. With the help of **Remark 1** and the simulation results in Fig. 5, we derive that optimal $L_{\rm B}^*=6$ for RSC/ZFB scheme and $L_{\rm B}^*=5$ for GSC/ZFB scheme, respectively. As shown in the Fig. 6, we can see that the secrecy performance will not always improve with the increase of $L_{\rm B}$ under a given $N_{\rm B}$.

VI. Conclusions

In this paper, we analyzed the secrecy performance of full-duplex multi-antenna spectrum-sharing wiretap networks with RSC/ZFB and GSC/ZFB transmission schemes, respectively. Specifically, assuming the Rayleigh fading, exact closed-form expressions for the secrecy outage probability of cognitive wiretap channels with RSC/ZFB and GSC/ZFB schemes were derived, which allows us to evaluate the secrecy performance. Furthermore, we also provided simple asymptotic approximations for the secrecy outage probability under two distinct scenarios and found that GSC/ZFB scheme achieves full diversity $N_{\rm B}$, while RSC/ZFB scheme only achieves partial diversity $L_{\rm B}$ under Scenario I. Finally, the optimal antenna allocation at Bob was investigated, and the simulation results demonstrated that the optimal antenna allocation achieves better secrecy performance than random antenna allocation for both schemes.

Appendix A
Proof of Lemma 1

In order to derive the conditional PDF of $\gamma_{\rm E}$, we first define the RV $X_{\rm E}=P_S|h_{\rm AE}|^2/\sigma_{\rm E}^2$ and give the PDF of the RV $Z_1=P_Z\left|\mathbf{h}_{\mathbf{BE}}^{\dagger}\mathbf{w}_{\rm ZF}\right|^2/\sigma_{\rm E}^2$ as [35]

$$f_{Z_1}(z)=\frac{z^{N_{\rm B}-L_{\rm B}-2}\exp\left(-\frac{\sigma_{\rm E}^2 z}{P_Z\lambda_{\rm BE}}\right)}{(N_{\rm B}-L_{\rm B}-2)!}\left(\frac{\sigma_{\rm E}^2}{P_Z\lambda_{\rm BE}}\right)^{N_{\rm B}-L_{\rm B}-1}. \tag{30}$$

Then, the conditional CDF of $\gamma_{\rm E}$ can be expressed as

$$\begin{aligned}F_{\gamma_{\rm E}}(y|G)&=\int_0^{\infty}F_{X_{\rm E}}\left(y\left(z+1\right)|G\right)f_{Z_1}(z)\,dz\\&=1-\exp\left(-\frac{\sigma_{\rm E}^2 y}{P_S\lambda_{\rm AE}}\right)\left(\frac{P_S\lambda_{\rm AE}}{P_Z\lambda_{\rm BE}y+P_S\lambda_{\rm AE}}\right)^{N_{\rm B}-L_{\rm B}-1}.\end{aligned} \tag{31}$$

To this end, the conditional PDF of $\gamma_{\rm E}$ can be obtained by taking a simple derivative.

Appendix B
Proof of Theorem 1

With the help of (7), we first derive the conditioned secrecy outage probability as (32) at the top of the next page, where Ω_1 and Ω_2 can be derived with some simple mathematical manipulations as

$$\begin{aligned}\Omega_1=&\sum_{a=0}^{k}\binom{k}{a}\left(2^{R_s}-1\right)^{k-a}\left(2^{R_s}\right)^{a}\left(\frac{\sigma_{\rm B}^2}{P_S\lambda_{\rm AB}}\right)^{k}\\&\times\left(\frac{\sigma_{\rm E}^2}{P_S\lambda_{\rm AE}}\right)^{-a}\left(\frac{\sigma_{\rm E}^2}{P_Z\lambda_{\rm BE}}\right)^{a+1}\Gamma\left(a+1\right)\\&\times\Psi\left(a+1,3+L_{\rm B}+a-N_{\rm B};\frac{\bar{\gamma}_{\rm B}+2^{R_s}\bar{\gamma}_{\rm E}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right),\end{aligned} \tag{33}$$

and

$$\begin{aligned}\Omega_2=&\sum_{a=0}^{k}\binom{k}{a}\left(2^{R_s}-1\right)^{k-a}\left(2^{R_s}\right)^{a}\left(N_{\rm B}-L_{\rm B}-1\right)\\&\times\left(\frac{\sigma_{\rm B}^2}{P_S\lambda_{\rm AB}}\right)^{k}\left(\frac{\sigma_{\rm E}^2}{P_S\lambda_{\rm AE}}\right)^{-a}\left(\frac{\sigma_{\rm E}^2}{P_Z\lambda_{\rm BE}}\right)^{a}\Gamma\left(a+1\right)\\&\times\Psi\left(a+1,2+L_{\rm B}+a-N_{\rm B};\frac{\bar{\gamma}_{\rm B}+2^{R_s}\bar{\gamma}_{\rm E}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right).\end{aligned} \tag{34}$$

Then, the unconditioned secrecy outage probability can be derived as

$$\begin{aligned}&P_{\rm out,1}\left(R_s\right)=\\&\int_0^{\infty}\left[1-\sum_{k=0}^{L_{\rm B}-1}\frac{1}{k!}\exp\left(-\frac{\sigma_{\rm B}^2\left(2^{R_s}-1\right)}{P_S\lambda_{\rm AB}}\right)\left(\Omega_1+\Omega_2\right)\right]f_G\left(g\right)dg.\end{aligned} \tag{35}$$

To this end, substituting the PDF of G into (35) and performing some simple mathematical manipulations, the desired secrecy outage probability of RSC/ZFB in (10) is obtained.

Appendix C
Proof of Theorem 2

Similar to (32), we derive the conditioned secrecy outage probability as (36) at the middle of the next page. Then, after performing some simple mathematical manipulations, Ξ_1 and Ξ_2 can be derived as

$$\begin{aligned}\Xi_1=&\left(\frac{\sigma_{\rm E}^2}{P_S\lambda_{\rm AE}}\right)^{-m}\left(\frac{\sigma_{\rm E}^2}{P_Z\lambda_{\rm BE}}\right)^{m+1}\Gamma\left(m+1\right)\\&\times\Psi\left(m+1,3+L_{\rm B}+m-N_{\rm B};\frac{\bar{\gamma}_{\rm B}+\bar{\gamma}_{\rm E}\nu_k 2^{R_s}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right)\end{aligned} \tag{37}$$

and

$$\begin{aligned}\Xi_2=&\frac{\left(P_S\lambda_{\rm AE}\right)^m}{\left(P_Z\lambda_{\rm BE}\right)^m}\left(N_{\rm B}-L_{\rm B}-1\right)\Gamma\left(m+1\right)\\&\times\Psi\left(m+1,2+L_{\rm B}+m-N_{\rm B};\frac{\bar{\gamma}_{\rm B}+\bar{\gamma}_{\rm E}\nu_k 2^{R_s}}{\bar{\gamma}_{\rm B}\bar{\gamma}_Z}\right).\end{aligned} \tag{38}$$

Finally, substituting (37) and (38) into (36) and performing some simple mathematical manipulations, the desired secrecy outage probability of GSC/ZFB in (20) is obtained.

Appendix D
Proof of Corollary 1

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

$$F_{\gamma_{\rm B_1}}(x|G)\approx\frac{1}{L_{\rm B}!}\left(\frac{\sigma_{\rm B}^2 x}{P_S\lambda_{AB}}\right)^{L_{\rm B}}. \tag{39}$$

$$P_{\text{out},1}\left(R_s|G\right)=\int_0^{\infty}F_{\gamma_{\text{B}_1}}\left(2^{R_s}\left(1+y\right)-1|G\right)f_{\gamma_{\text{E}}}\left(y|G\right)dy=1-\sum_{k=0}^{L_{\text{B}}-1}\frac{1}{k!}\exp\left(-\frac{\sigma_{\text{B}}^2\left(2^{R_s}-1\right)}{P_S\lambda_{\text{AB}}}\right)$$
$$\times\Bigg[\underbrace{\int_0^{\infty}\left(\frac{\sigma_{\text{B}}^2\left(2^{R_s}\left(1+y\right)-1\right)}{P_S\lambda_{\text{AB}}}\right)^{k}\frac{\sigma_{\text{E}}^2\exp\left(-\frac{P_S\lambda_{\text{AB}}/\sigma_{\text{B}}^2+2^{R_s}P_S\lambda_{\text{AE}}/\sigma_{\text{E}}^2}{P_S\lambda_{\text{AE}}/\sigma_{\text{E}}^2P_S\lambda_{\text{AB}}/\sigma_{\text{B}}^2}y\right)}{P_S\lambda_{\text{AE}}}\left(\frac{P_S\lambda_{\text{AE}}}{P_Z\lambda_{\text{BE}}y+P_S\lambda_{\text{AE}}}\right)^{N_{\text{B}}-L_{\text{B}}-1}dy}_{\Omega_1}$$
$$+\underbrace{\int_0^{\infty}\left(\frac{\sigma_{\text{B}}^2\left(2^{R_s}\left(1+y\right)-1\right)}{P_S\lambda_{\text{AB}}}\right)^{k}\frac{\exp\left(-\frac{P_S\lambda_{\text{AB}}/\sigma_{\text{B}}^2+2^{R_s}P_S\lambda_{\text{AE}}/\sigma_{\text{E}}^2}{P_S\lambda_{\text{AE}}/\sigma_{\text{E}}^2P_S\lambda_{\text{AB}}/\sigma_{\text{B}}^2}y\right)\left(N_{\text{B}}-L_{\text{B}}-1\right)P_Z\lambda_{\text{BE}}(P_S\lambda_{\text{AE}})^{N_{\text{B}}-L_{\text{B}}-1}}{\left(P_Z\lambda_{\text{BE}}y+P_S\lambda_{\text{AE}}\right)^{N_{\text{B}}-L_{\text{B}}}}dy}_{\Omega_2}\Bigg], \tag{32}$$

$$\begin{aligned}P_{\text{out},2}\left(R_s|G\right)&=\int_0^{\infty}F_{\gamma_{\text{B}_2}}\left(2^{R_s}\left(1+y\right)-1|G\right)f_{\gamma_{\text{E}}}\left(y|G\right)dy\\&=\binom{N_{\text{B}}}{L_{\text{B}}}\sum_{S}\sum_{k=0}^{L_{\text{B}}}l_k\frac{\exp\left(-\frac{\nu_k\left(2^{R_s}-1\right)}{P_S\lambda_{\text{AB}}/\sigma_{\text{B}}^2}\right)}{\left(P_S\lambda_{\text{AB}}/\sigma_{\text{B}}^2\right)^{\mu_k}}\sum_{m=0}^{\mu_k}\binom{\mu_k}{m}\left(2^{R_s}-1\right)^{\mu_k-m}\left(2^{R_s}\right)^{m}\\&\times\Bigg[\underbrace{\int_0^{\infty}y^m\frac{\sigma_{\text{E}}^2\exp\left(-\frac{\sigma_{\text{B}}^2\nu_k2^{R_s}y}{P_S\lambda_{\text{AB}}}\right)}{P_S\lambda_{\text{AE}}}\exp\left(-\frac{\sigma_{\text{E}}^2y}{P_S\lambda_{\text{AE}}}\right)\left(\frac{P_S\lambda_{\text{AE}}}{P_Z\lambda_{\text{BE}}y+P_S\lambda_{\text{AE}}}\right)^{N_{\text{B}}-L_{\text{B}}-1}dy}_{\Xi_1}\\&+\underbrace{\int_0^{\infty}y^m\exp\left(-\frac{\sigma_{\text{B}}^2\nu_k2^{R_s}y}{P_S\lambda_{\text{AB}}}\right)\exp\left(-\frac{\sigma_{\text{E}}^2y}{P_S\lambda_{\text{AE}}}\right)\frac{\left(N_{\text{B}}-L_{\text{B}}-1\right)P_Z\lambda_{\text{BE}}(P_S\lambda_{\text{AE}})^{N_{\text{B}}-L_{\text{B}}-1}}{\left(P_Z\lambda_{\text{BE}}y+P_S\lambda_{\text{AE}}\right)^{N_{\text{B}}-L_{\text{B}}}}dy}_{\Xi_2}\Bigg].\end{aligned} \tag{36}$$

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

$$f_{\gamma_{\text{E}}}\left(y|G\right)=\frac{1}{\bar{\gamma}_{\text{E}}}\exp\left(-\frac{y}{\bar{\gamma}_{\text{E}}}\right)\left(\frac{\bar{\gamma}_{\text{E}}}{\bar{\gamma}_{\text{Z}}y+\bar{\gamma}_{\text{E}}}\right)^{N_{\text{B}}-L_{\text{B}}-1}$$
$$+\exp\left(-\frac{y}{\bar{\gamma}_{\text{E}}}\right)\frac{\left(N_{\text{B}}-L_{\text{B}}-1\right)\bar{\gamma}_{\text{Z}}(\bar{\gamma}_{\text{E}})^{N_{\text{B}}-L_{\text{B}}-1}}{\left(\bar{\gamma}_{\text{Z}}y+\bar{\gamma}_{\text{E}}\right)^{N_{\text{B}}-L_{\text{B}}}}. \tag{40}$$

Substituting (39) and (40) into (32) and applying the binomial expansion, the asymptotic secrecy outage probability of RSC/ZFB scheme conditioned on the RV G is given by

$$\begin{aligned}P_{\text{out},1}\left(R_{\text{S}}|G\right)&\approx\int_0^{\infty}F_{\gamma_{\text{B}_1}}\left(2^{R_s}(1+y)-1|G\right)f_{\gamma_{\text{E}}}\left(y|G\right)dy\\&=\frac{1}{L_{\text{B}}!}\sum_{i=0}^{L_{\text{B}}}\left(2^{R_s}-1\right)^{L_{\text{B}}-i}\left(2^{R_s}\right)^{i}\left(\frac{\sigma_{\text{B}}^2}{P_S\lambda_{\text{AB}}}\right)^{L_{\text{B}}}\\&\times\frac{\left(\bar{\gamma}_{\text{E}}\right)^{i}}{\left(\bar{\gamma}_{\text{Z}}\right)^{i+1}}\Gamma\left(i+1\right)\Psi\left(i+1,3+i+L_{\text{B}}-N_{\text{B}};\frac{1}{\bar{\gamma}_Z}\right)\\&+\frac{1}{L_{\text{B}}!}\sum_{i=0}^{L_{\text{B}}}\left(2^{R_s}-1\right)^{L_{\text{B}}-i}\left(2^{R_s}\right)^{i}\left(\frac{\sigma_{\text{B}}^2}{P_S\lambda_{\text{AB}}}\right)^{L_{\text{B}}}\\&\times\left(\frac{\bar{\gamma}_{\text{E}}}{\bar{\gamma}_{\text{Z}}}\right)^{i}\Gamma\left(i+1\right)\Psi\left(i+1,2+i+L_{\text{B}}-N_{\text{B}};\frac{1}{\bar{\gamma}_Z}\right).\end{aligned} \tag{41}$$

Now, averaging over G and with the help of equality [46, Eq.(3.381.4)], the desired result can be derived.

Appendix E
Proof of Corollary 3

Based on (32), when $\bar{\gamma}_{\text{B}}\to\infty$ and $\bar{\gamma}_{\text{E}}\to\infty$, the conditioned secrecy outage probability can be expanded as (42) at the top of the next page, where Ω_3 and Ω_4 can be easily derived as

$$\Omega_3\approx\sum_{v=0}^{k}\binom{k}{v}\left(2^{R_s}-1\right)^{k-v}\left(2^{R_s}\right)^{v}\frac{\left(\bar{\gamma}_{\text{E}}\right)^{v}}{\left(\bar{\gamma}_{\text{B}}\right)^{k}\left(\bar{\gamma}_Z\right)^{v}\bar{\gamma}_Z}$$
$$\times\Gamma\left(v+1\right)\Psi\left(v+1,3+v+L_{\text{B}}-N_{\text{B}};\frac{\bar{\gamma}_{\text{B}}+2^{R_s}\bar{\gamma}_{\text{E}}}{\bar{\gamma}_Z\bar{\gamma}_B}\right), \tag{43}$$

and

$$\Omega_4\approx\sum_{v=0}^{k}\binom{k}{v}\left(2^{R_s}-1\right)^{k-v}\left(2^{R_s}\right)^{v}\left(N_{\text{B}}-L_{\text{B}}-1\right)\frac{\left(\bar{\gamma}_{\text{E}}\right)^{v}}{\left(\bar{\gamma}_{\text{B}}\right)^{k}\left(\bar{\gamma}_Z\right)^{v}}$$
$$\times\Gamma\left(v+1\right)\Psi\left(v+1,2+v+L_{\text{B}}-N_{\text{B}};\frac{\bar{\gamma}_{\text{B}}+2^{R_s}\bar{\gamma}_{\text{E}}}{\bar{\gamma}_Z\bar{\gamma}_{\text{B}}}\right). \tag{44}$$

Finally, substituting (43) and (44) into (42) yields the final result.

$$P_{\text{out},1}\left(R_s|G\right) \approx 1 - \sum_{k=0}^{L_{\text{B}}-1} \frac{1}{k!} \times \Bigg[\underbrace{\int_0^{\infty} \left(\frac{\sigma_{\text{B}}^2 \left(2^{R_s}\left(1+y\right)-1\right)}{P_S \lambda_{\text{AB}}} \right)^k \frac{\sigma_{\text{E}}^2 \exp\left(- \frac{P_S \lambda_{\text{AB}}/\sigma_{\text{B}}^2 + 2^{R_s} P_S \lambda_{\text{AE}}/\sigma_{\text{E}}^2}{P_S \lambda_{\text{AE}}/\sigma_{\text{E}}^2 P_S \lambda_{\text{AB}}/\sigma_{\text{B}}^2} y \right)}{P_S \lambda_{\text{AE}}} \left(\frac{P_S \lambda_{\text{AE}}}{P_Z \lambda_{\text{BE}} y + P_S \lambda_{\text{AE}}} \right)^{N_{\text{B}}-L_{\text{B}}-1} dy}_{\Omega_3} + \underbrace{\int_0^{\infty} \left(\frac{\sigma_{\text{B}}^2 \left(2^{R_s}\left(1+y\right)-1\right)}{P_S \lambda_{\text{AB}}} \right)^k \frac{\exp\left(- \frac{P_S \lambda_{\text{AB}}/\sigma_{\text{B}}^2 + 2^{R_s} P_S \lambda_{\text{AE}}/\sigma_{\text{E}}^2}{P_S \lambda_{\text{AE}}/\sigma_{\text{E}}^2 P_S \lambda_{\text{AB}}/\sigma_{\text{B}}^2} y \right) \left(N_{\text{B}}-L_{\text{B}}-1\right) P_Z \lambda_{\text{BE}} (P_S \lambda_{\text{AE}})^{N_{\text{B}}-L_{\text{B}}-1}}{\left(P_Z \lambda_{\text{BE}} y + P_S \lambda_{\text{AE}}\right)^{N_{\text{B}}-L_{\text{B}}}} dy}_{\Omega_4} \Bigg], \quad (42)$$

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

[3] Y. Huang, F. S. Al-Qahtani, Q. Wu, C. Zhong, J. Wang, and H. M. Alnuweiri, "Outage analysis of spectrum sharing relay systems with multiple secondary destinations under primary user's interference," *IEEE Trans. Veh. Technol.,* vol. 63, no. 7, pp. 3456-3463, Sep. 2014.

[4] 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. of IEEE Globecom* 2014, Austin, US, pp. 3074-3079.

[5] Y. Deng, M. Elkashlan, N. Yang, P. L. Yeoh, and R. K. Mallik, "Impact of primary network on secondary network with generalized selection combining," *IEEE Trans. Veh. Technol.,* vol. 64, no. 7, pp. 3280-3285, Jul. 2015.

[6] 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.

[7] 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.

[8] 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.

[9] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, J. Wang, and C. Cai, "Secure transmission in spectrum sharing MIMO channels with generalized antenna selection over Nakagami-*m* Channels," *IEEE Access,* vol. 4, pp. 4058-4065, Jul. 2016.

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

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

[12] 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.

[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 appear, 2016, DOI10.1109/TVT.2016.2529704.

[14] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and A. Qaraqe, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.* to appear, 2016, DOI10.1109/TVT.2016.2536801.

[15] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "The Gaussian wiretap channel with a helping interferer," *in Proc. of IEEE ISIT* 2008, Toronto, Canada, pp. 389-393.

[16] 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.

[17] L. Li, Z. Chen, and J. Fang, "On secrecy capacity of gaussian wiretap channel aided by a cooperative jammer," *IEEE Signal Process. Lett.,* vol. 21, no. 11, pp. 1356-1360, Nov. 2014.

[18] 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.

[19] 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.

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

[21] T. Zhang, Y. Cai, Y. Huang, C. Zhong, W. Yang, and G. K. Karagiannidis, "Secure transmission in cognitive wiretap networks," in *Proc. of IEEE VTC-Spring* 2016, Nanjing, China.

[22] 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.

[23] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical layer security over SIMO generalized-K fading channels," accepted for publication in *IEEE Trans. Veh. Technol.*, 2015.

[24] 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.

[25] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.

[26] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359-368, Feb. 2012.

[27] J. Yang, I. M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840-2852, Jun. 2013.

[28] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.,* vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[29] 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.

[30] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *IEEE J. Commun. Net.*, vol. 14, no. 4, pp. 364-373, Aug. 2012.

[31] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative Beamforming and User Selection for Improving the Security of Relay-Aided Systems," *IEEE Tran. Commun.,* vol. 63, no. 12, pp. 5039-5051, Dec. 2015.

[32] 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.

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

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

[35] A. Afana, V. Asghari, A. Ghrayeb, and S. Affes, "Cooperative relaying in spectrum-sharing systems with beamforming and interference constraints", in *Proc. of IEEE SPAWC* 2012, Cesme, Turkey, pp. 429-433.

[36] 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.

[37] 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.

[38] 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.

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

[40] 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.

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

[42] 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.

[43] 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.

[44] A. Afana, A. Ghrayeb, V. Asghari, and S. Affes, "Distributed beamforming for spectrum-sharing systems with AF cooperative two-way relaying," *IEEE Trans. Wireless Commun.*, vol. 62, no. 9, pp. 3180-3195, Sep. 2014.

[45] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054-6067, Nov. 2014.

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

Tao Zhang (S'13) received his B.S. degree in Communication Engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011. He is currently pursuing for the Ph.D. degree in Communications and Information Systems at the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China. His current research interest includes cooperative communications, wireless sensor networks, physical layer security, and cognitive radio systems.

Yueming Cai (M'05-SM'12) received his B.S. degree in Physics from Xiamen University, Xiamen, China in 1982, the M.S. degree in Micro-electronics 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 MIMO systems, OFDM systems, signal processing in communications, cooperative communications and wireless sensor networks.

Yuzhen Huang (S'12-M'16) received his B.S. degree in Communications Engineering, and Ph.D. degree in Communications and Information Systems from College of Communications Engineering, PLA University of Science and Technology, in 2008 and 2013 respectively. He has been with College of Communications Engineering, PLA University of Science and Technology since 2013, and currently as an Assistant Professor. Since 2016, he has been a Post-Doctoral Research Associate with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing. His research interests focus on channel coding, MIMO communications systems, cooperative communications, physical layer security, and cognitive radio systems. He currently serves as an Associate Editor of KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS. He and his coauthors have been awarded a Best Paper Award at the WCSP 2013. He received an IEEE COMMUNICATIONS LETTERS exemplary reviewer certificate for 2014.

Trung Q. Duong (S'05-M'12-SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include physical layer security, energy-harvesting communications, cognitive relay networks. He is the author or co-author of 190 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, and ELECTRONICS LETTERS. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020).

Weiwei Yang (S'08-M'12) received his B.S., M.S., and Ph.D. degrees from 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.