IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 19, 2019, accepted December 9, 2019, date of publication December 13, 2019,
date of current version December 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2959597

Secure Spectrum-Sharing Wiretap Networks With Full-Duplex Relaying

ZHIHUI SHANG[1,2], TAO ZHANG[3], YUEMING CAI[1], (Senior Member, IEEE), YONGXIANG LIU[3], AND WEIWEI YANG[1], (Member, IEEE)
[1]College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]College of Medical Information Engineering, Zunyi Medical University, Zunyi 563006, China
[3]The Sixty-third Research Institute, National University of Defense Technology, Nanjing 210007, China

Corresponding author: Tao Zhang (ztcool@126.com)

This work was supported in part by the Project of Natural Science Foundation of China under Grant 61801496, in part by the National Postdoctoral Program for Innovative Talents of China under Grant BX20180374, in part by the National University of Defense Technology Research Project under Grant ZK17-03-25, and in part by the Joint Foundation Project of Zunyi Science and Technology Bureau and the Zunyi Medical University of Guizhou Provincial under Grant E-282.

ABSTRACT In this paper, we investigate the secrecy performance of dual-hop randomize-and-forward (RaF) cognitive wiretap networks over Rayleigh fading channels, in which the RaF relay is considered both as half-duplex (HD) and full-duplex (FD) operations. Specifically, for the HD, maximal-ratio combining/maximal-ratio transmission (MRC/MRT) is adopted at the RaF relay. For the FD, the RaF relay can simultaneously receive the signal from the source and transmit jamming signals to eavesdropper, and the selection combining-zero forcing beamforming/maximal-ratio transmit (SC-ZFB/MRT) and SC-ZFB/ZFB schemes are respectively adopted at the FD relay. To thoroughly assess the secrecy performance achieved from the proposed schemes, the closed-form expressions for the secrecy outage probability (SOP) of the dual-hop RaF cognitive wiretap channels with MRC/MRT, SC-ZFB/MRT and SC-ZFB/ZFB schemes are derived, respectively. In addition, we also provide simple asymptotic approximations for the SOP under two distinct scenarios, depending on the quality of the main and wiretap channels. Additionally, our analytical results and numerical simulations show the efficiency of our proposed solutions for both SC-ZFB/MRT and SC-ZFB/ZFB with FD cases and show considerable performance gains over MRC/MRT with HD scheme. Finally, for the proposed schemes, the SC-ZFB/ZFB scheme is beneficial to improve secrecy performance when the eavesdropper's channel is better than the main channel and the RaF relaying strategy achieves better secrecy performance than that of the decode-and-forward (DF) relaying strategy for dual-hop cognitive wiretap networks.

INDEX TERMS Physical layer security, cognitive radio, full duplex, multiple antennas relay, secrecy outage probability, zero forcing beamforming (ZFB).

I. INTRODUCTION

In the past decade, cognitive radio networks (CRNs) have caught much attention from the research area due to their ability to utilize the spectrum resources [1]. In spectrum sharing CRNs, the unlicensed secondary users (SUs) can have access to the licensed primary users' (PUs') spectrum as long as the quality of service (QoS) of the PUs can reach the requirement. Specifically, three strategies are proposed to maintain the QoS of the PUs, i.e., underlay, overlay and interweave [2], [3]. Among them, underlay is easy to realize, in which the interference of SUs to the PUs should be less than a given threshold.

A. BACKGROUND

Since wireless communication allows frequent interactions and are highly flexible, CRNs are vulnerable to illegal attacking and eavesdropping, which constitute challenging security issues. In order to solve these problems, several works have explored the security issues of CRNs from the physical layer security (PLS) perspective. In [4], Qin *et al.* investigated maximal jamming rate-based scheme, where selecting

The associate editor coordinating the review of this manuscript and approving it for publication was Khaled Rabie.

the secondary user with maximal interference channel and transmitting with a delicately designed rate in CRNs can achieve security at physical layer. In [5], the proposed new method enables the PU to communicate with the SUs through a relay node without sacrificing their individual secrecy capacity to enhance the secrecy performance of CRNs in the underlay multiple-input multiple-output CRNs. Similarly in [6], the authors assumed that receiving antenna can receive information and energy simultaneously from the source node through power splitter architecture for enhancing secrecy performance of underlay CRNs. They designed an artificial noise-assisted optimal beamforming scheme and denoted cognitive beamforming for the secondary users to achieve maximize the ergodic secrecy rate for secure cognitive radio transmissions [7]. There are also many previous studies on PLS of CRNs. The allocation of efficient resource and economic-robust transmission opportunity auction in device-to-device (D2D) are achieved to enhance network's performance [8], [9]. In [10] and [11], the authors consider the single-input multiple-output (SIMO) and multiple-input multipleoutput (MIMO) underlay CRNs over Nakagami-*m* channels with different schemes to improve secrecy performance of the system. The spectrum sharing technology of the ultra-dense and novel unmanned aerial vehicle aided (UAVA) network can be adopted to improve secrecy performance of CRNs [12], [13]. The millimeter-wave (mmWave), the non-orthogonal multiple access (NOMA) and buffer-aided technology were applied to secure the communication of CRNs over Nakagami-m fading channels [14]–[16].

For further secrecy enhancement, different techniques such as multi-antenna relaying and full-duplex (FD) have been widely used by many scholars. On one hand, the use of multi-antenna relay can enable the efficient communication between the SU transmitter and SU receiver, both of which are not directly connected before. Therefore, the transmission efficiency can be improved. In [17], the authors investigated cognitive multiple relays system, in which the multiple relays can switch receiving and transmitting artificial noise function among its different antennas for improving security of the system. In [18], an optimal relay selection was proposed based on two energy harvesting protocols and the achievable closed-form expressions of secrecy outage probability (SOP) was derived in CRNs. On the other hand, the FD technique is put forward to enhance the performance of the traditional cooperative jamming scheme, and the key idea of FD jamming scheme is that the FD user can receive the required signal and transmit jamming signal simultaneously. Different from traditional cooperative jamming scheme that relies on cooperative jamming node mobility, trustworthiness and synchronization, FD jamming scheme is much easier and more reliable to realize. In [19], the FD technique was first proposed with the idea that the FD operation was employed for enhancing the secure transmission. In [20], the authors analyzed the SOP of the FD receiver, the cooperative jamming strategies with different relay selections and the sophisticated power control for enhancing the secrecy performance. The authors of [21] investigated that the FD jammer can broadcast jamming signals and receive signals from the central monitor simultaneously, which can enhance the secrecy performance of the considered system. In [22] and [23], the author designed different schemes of FD operations, in which the secrecy performance of system is improved by receiving and jamming signals simultaneously. A wireless ad-hoc network with numerous legitimate transmitter-receiver pairs and eavesdroppers with FD receiver deployment strategy was put forward to enhance the PLS in [24]. However, to the best of the authors' knowledge, the performance of the spectrum-sharing wiretap networks with FD relay has not been well understood.

B. MOTIVATION AND CONTRIBUTION

Motivated by the above, we consider a dual-hop randomize-and-forward (RaF)[1] cognitive wiretap networks over Rayleigh fading channels under different scenarios, where a secondary transmitter (Alice) communicates to a secondary destination (Bob) with the help of a secondary FD relay (Relay) in the presence of a primary receiver (PU) and an eavesdropper (Eve). Both half-duplex (HD) and FD operations are assumed at Relay, respectively. Specifically, for the HD operation, the Relay employs maximal-ratio combining (MRC) to strengthen the signal detection from Alice and forwards data to Bob using maximal-ratio transmit (MRT) scheme. While for the FD operation, two different secure transmission schemes are proposed: 1) Selection combining-zero forcing beamforming/maximal-ratio transmit (SC-ZFB/MRT) scheme, where the Relay first selects the best antenna to recover the data from the Alice and then utilizes the remaining antennas to transmit the jamming signal simultaneously at the first phase, and the Relay transmits signals to Bob by adopting the MRT scheme at the second phase. 2) SC-ZFB/ZFB scheme, where the Relay also selects the best antenna to recover the data from the Alice and then utilizes the remaining antennas to transmit the jamming signal to eavesdropper simultaneously at the first phase, and the Relay can correctly decode the signal and retransmits it according to the principle of ZFB operation at the second phase. The contributions of this paper are summarized as follows:

- We first derive the exact closed-form and asymptotic expressions for the SOP of the dual-hop RaF cognitive wiretap networks with MRC/MRT scheme, in which the analytical expressions are used to investigate the performance of the MRC/MRT scheme with HD operation. The asymptotic secrecy diversity gain is investigated, and we study two separate scenarios. Scenario I: $\overline{\gamma_B} \rightarrow \infty$ *and fixed* $\overline{\gamma_E}$ reveals that the MRC/MRT scheme can achieve full secrecy diversity gain under the

[1] The RaF transmission protocol has been widely used for secure transmission. The transmitter of each phase uses different codebooks to transmit security information at the two separate transmissions. Due to the transmission heterogeneity of the transmitters of the two phases, the eavesdropper cannot merge the common information of the two phases [25]–[27].

high signal-to-noise ratio (SNR), i.e., the eavesdropper is located far away from the legitimate secondary users. Scenario II: $\overline{\gamma_B} \to \infty$ *and* $\overline{\gamma_E} \to \infty$ reveals that the MRC/MRT scheme can achieve zero secrecy diversity gain under the high SNR, i.e., Relay and eavesdropper are located close to the Alice, where $\overline{\gamma_B}$ and $\overline{\gamma_E}$ represent the high SNR of the main channel and the eavesdropping channel, respectively.

- We derive new closed-form and asymptotic expressions for the SOP and non-zero secrecy rate with arbitrary number of N_R as well as the switched threshold, from which the impact of key system parameters on the secrecy performance of the dual-hop RaF cognitive wiretap networks with the FD operation at Relay under SC-ZFB/MRT and SC-ZFB/ZFB schemes can be readily evaluated. Moreover, for both schemes, the asymptotic secrecy diversity gain is investigated in the high SNR regime under two different Scenarios, which reveals that SC-ZFB/MRT can achieve full secrecy diversity under Scenario I and zero secrecy diversity under Scenario II.
- Through the derivation and analysis of the SOP, we have verified that the SC-ZFB/MRT and SC-ZFB/ZFB schemes are better than MRC/MRT scheme in terms of improving secrecy performance of the considered networks. The secrecy performance of the considered schemes with FD operation is mainly influenced by the secrecy coding gain. Specifically, for the proposed schemes, the SC-ZFB/ZFB scheme is beneficial to improve secrecy performance when the eavesdropper's channel is better than the main channel, while the MRC/MRT scheme will achieve better secrecy performance when the main channel is much better than the eavesdropper's channel. Besides, increasing the number of antennas of Relay and the interference threshold of the primary network within a certain range can improve the secrecy performance of the considered networks. In addition, we also find that the RaF relaying strategy achieves better secrecy performance than the DF relaying strategy for dual-hop cognitive wiretap networks.

The remainder of the paper is organized as follows. The system models are described in Section II. The expressions of SOP of the considered system are analyzed in Section III. In Section IV, we provide the high signal-to-noise ratio (SNR) analysis for SOP. The numerical results and discussions are presented in Section V. Finally, we conclude this paper in Section VI.

II. SYSTEM MODEL

In this section, let us consider a dual-hop RaF cognitive wiretap networks as shown in Fig. 1, which consists of a secondary transmitter (Alice), a secondary relay (Relay), a legitimate receiver (Bob), a primary receiver (PU) and an eavesdropper (Eve). In the considered networks, all users are equipped with a single antenna, except that Relay has N_R antennas. As in [28], we assume that the primary transmitter (PT) is far away from the secondary receiver, thus the interference from the PT can be ignored at the secondary receivers. Both main and wiretap channels experience quasi-static independent and non-identical Rayleigh fading. The corresponding channel coefficient of the nodes $M \to N$ is denoted as h_{MN}, which is an exponentially distributed random variable (RV) with zero mean and variance λ_{MN} as denoted by $\mathcal{CN}(0, \lambda_{MN})$. Similar to [28]–[30], the channel state information (CSI) between Eve and Relay is gained at Relay[2], while the CSI of Alice to Eve link is not available at Alice. Multi-antenna relay can operate both in HD and FD operation. Under FD operation, Relay can receive the signals and transmit jamming signals to eavesdropper simultaneously. For exploring the benefits of multiple antennas, we investigate three different secure transmission schemes, i.e., MRC/MRT with HD operation, SC-ZFB/MRT and SC-ZFB/ZFB with FD operations.

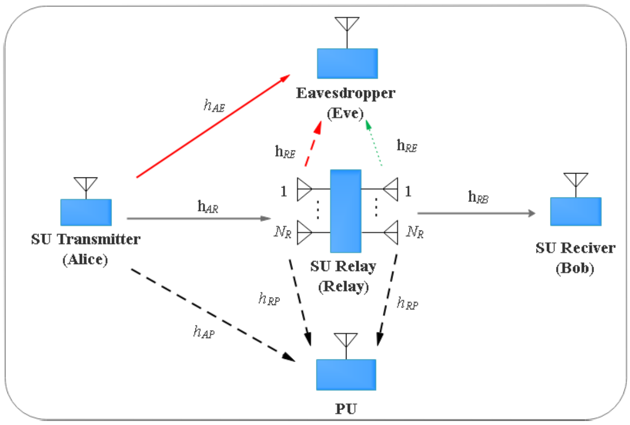

FIGURE 1. System model.

A. MRC/MRT WITH HD SCENARIO

In the first phase, based on HD operation, Relay adopts the MRC scheme to receive signals. Thus, we can write the instantaneous SNR between Alice and Relay as

$$\gamma_{AR,1} = \frac{P_S}{\sigma_R^2} \|\mathbf{h}_{AR}\|^2, \tag{1}$$

where $\mathbf{h}_{AR}$ is an $N_R \times 1$ Alice-Relay channel link vector, σ_R^2 denotes the noise variance at Relay, and P_S is the transmit power of Alice, which must satisfy [28]

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

where P_t is the maximum transmit power constraint at Alice, and Q denotes the interference temperature constraint at the PU, h_{AP} is the channel coefficient for Alice to PU link.

[2] This case can be applied to the scenario where Eve plays dual roles as legitimate one and eavesdropper one (e.g., in TDMA networks and heterogenous networks). Therefore, the Relay can estimate the eavesdropper's CSI when the Eve participates in transmitting information as a legitimate user [28]–[31].

Similarly, the instantaneous SNR of the wiretap channel between Alice and Eve can be written as

$$\gamma_{AE,1}=\frac{P_S|h_{AE}|^2}{\sigma_E^2}, \tag{3}$$

where h_{AE} is the channel coefficient for Alice to Eve link, and σ_E^2 denotes the noise variance at Eve.

In the second phase, Relay adopts the MRT scheme to forward signals, we can write the instantaneous SNR between Relay and Bob as

$$\gamma_{RB,1}=\frac{P_R}{\sigma_B^2}\|\mathbf{h}_{RB}\|^2, \tag{4}$$

where $\mathbf{h}_{RB}$ is an $N_R \times 1$ channel link vector between Relay and Bob, and σ_B^2 denotes the noise variance at Bob. P_R is the transmit power of Relay and it must meet the requirement of $P_R = \min\left(\frac{Q}{|h_{RP}|^2}, P_t\right)$.

Similarly, the instantaneous SNR of the wiretap channel between Relay and Eve as

$$\gamma_{RE,1}=\frac{P_R|h_{RE}|^2}{\sigma_E^2}, \tag{5}$$

where h_{RE} is the channel coefficients for Relay to Eve link.

B. SC-ZFB/MRT WITH FD SCENARIO

In the first phase, based on FD operation, Relay can switch jamming/receiving function between its antennas for enhancing security using SC-ZFB scheme. Specifically, relay first selects the best antenna based on the CSI of the main channel, and utilizes the remaining $N_R - 1$ antennas to send a weighted jamming signal simultaneously. In order to meet the constraints at PU, we use ZFB to avoid undesirable jamming signals at PU.

The optimal weight vector $\mathbf{w}_{ZF}$ is the solution of the following optimization problem:

$$\max_{\mathbf{w}_{ZF}} \left|\mathbf{h}_{RE}^{\dagger}\mathbf{w}_{ZF}\right|$$
$$s.t. \left|\mathbf{h}_{RP}^{\dagger}\mathbf{w}_{ZF}\right| \& \|\mathbf{w}_{ZF}\|_F = 1, \tag{6}$$

where † is the conjugate transpose operator, $\|\cdot\|_F$ denotes the Frobenius norm, and $\mathbf{h}_{RE}$ and $\mathbf{h}_{RP}$ denote the $(N_R - 1) \times 1$ channel vectors between the remaining $N_R - 1$ antennas of the Relay and Eve, and the remaining $N_R - 1$ antennas of the Relay and PU, respectively. By using the projection matrix theory [32], the $\mathbf{w}_{ZF}$ can be marked as

$$\mathbf{w}_{ZF}=\frac{\mathbf{T}^{\perp}\mathbf{h}_{RE}}{\left\|\mathbf{T}^{\perp}\mathbf{h}_{RE}\right\|}, \tag{7}$$

where $\mathbf{T}^{\perp}=\left(\mathbf{I}-\mathbf{h}_{RP}\left(\mathbf{h}_{RP}\mathbf{h}_{RP}^{\dagger}\right)^{-1}\mathbf{h}_{RP}^{\dagger}\right)$ is the projection idempotent matrix with rank $N_R - 2$. If the i-th antenna is selected at Relay, the channel coefficient between Alice and Relay can be expressed as h_{ARi}. As a result, the instantaneous SNR[3] of the main channel and the instantaneous signal-to-interference-plus-noise ratio (SINR) of the wiretap channel can be respectively expressed as

$$\gamma_{AR,2}=\frac{P_S}{\sigma_R^2}\max_{i\in N_R}\left(|h_{ARi}|^2\right), \tag{8}$$

and

$$\gamma_{AE,2}=\frac{P_S|h_{AE}|^2}{P_J\left|\mathbf{h}_{RE}^{\dagger}\mathbf{w}_{ZF}\right|^2+\sigma_E^2}. \tag{9}$$

where P_J is the interference power of Relay to Eve.

In the second phase, Relay adopts the MRT scheme to forward signals, which is similar to the analysis of the second phase of MRC/MRT scenario, i.e., Eq.(4) and Eq. (5). The process won't be proven here again, and the instantaneous SNR of the main channel and the instantaneous SNR of the wiretap channel can be respectively expressed as $\gamma_{RB,2}$ and $\gamma_{RE,2}$.

C. SC-ZFB/ZFB WITH FD SCENARIO

In the first phase, Relay adopts the SC-ZFB with FD operation, which is similar to the analysis of the first phase of SC-ZFB/MRT scheme and is no longer proven here, i.e., Eq.(8) and Eq. (9). The instantaneous SNR of the main channel and the instantaneous SINR of the wiretap channel can be respectively expressed as $\gamma_{AR,3}$ and $\gamma_{AE,3}$.

In the second phase, Relay adopts the ZFB scheme to forward signals. The goal of ZFB scheme is to maximize the reception of SNR at Bob while avoiding the leakage of security information to Eve and the interference to PU. Therefore, the instantaneous SNR of Relay-Bob link is given by

$$\gamma_{RB,3}=\frac{P_{R2}}{\sigma_B^2}\|\mathbf{h}_{RB}\mathbf{w}_{ZF2}\|^2, \tag{10}$$

where $\mathbf{w}_{ZF2}$ is the weight vector, the transmit power of Relay is P_{R2}, which is not constrained by PU. $\mathbf{h}_{RB}$ denotes the $N_R \times 1$ channel vectors between Relay and Bob. Now, we first define an $N_R \times (1{+}1)$ channel matrix, i.e., $\mathbf{H}_{RZ} = [\mathbf{H}_{RP}, \mathbf{H}_{RE}]$, where $\mathbf{H}_{RP}$, $\mathbf{H}_{RE}$ are $N_R \times 1$, $N_R \times 1$ channel link matrices between Relay and PU, Relay and Eve, respectively. For the ZFB scheme, it requires $N_R > 2$. Thus, the optimal weight vector $\mathbf{w}_{ZF2}$ is the solution of the following optimization problem:

$$\max_{\mathbf{w}_{ZF2}} \left|\mathbf{h}_{RB}^{\dagger}\mathbf{w}_{ZF2}\right|$$
$$s.t. \left|\mathbf{H}_{RZ}^{\dagger}\mathbf{w}_{ZF2}\right| \& \|\mathbf{w}_{ZF2}\|_F = 1. \tag{11}$$

[3] It should be noted that for the FD mechanism, based on the self-interference (SI) cancellation technology, the influence of SI at the Relay is not taken into consideration as that in [22] and [33]. The assumption that the SI can be canceled is widely used to explore the information-theory oriented performance, i.e., outage probability and capacity [29], [34]. However, the full suppression of SI still cannot be realized even with the help of latest techniques in [35].

Therefore, by using knowledge provided in (7), the optimal weight vector $\mathbf{w}_{ZF2}$ can be marked as

$$\mathbf{w}_{ZF2}=\frac{\Xi^{\perp}\mathbf{h}_{RB}}{\left\|\Xi^{\perp}\mathbf{h}_{RB}\right\|},\tag{12}$$

where $\Xi^{\perp}=\left(\mathbf{I}-\mathbf{H}_{RZ}\left(\mathbf{H}_{RZ}^{\dagger}\mathbf{H}_{RZ}\right)^{-1}\mathbf{H}_{RZ}^{\dagger}\right)$ is the projection idempotent matrix with rank N_R-3.

Based on the above statement, $\gamma_{AR,j}$, $\gamma_{RB,j}$, $\gamma_{AE,j}$ and $\gamma_{RE,j}$ are statistically dependent due to the presence of containing the common RV, i.e., $G=|h_{AP}|^2$ and $G_1=|h_{RP}|^2$ in P_S and P_R, where $j\in(1,2,3)$ stand for scenario 1, scenario 2 and scenario 3, respectively. To solve this problem, we adopt the condition and average approach. Thus, we first present the cumulative distribution function (CDF) of $\gamma_{AR,j}$, $\gamma_{RB,j}$ and probability density function (PDF) of $\gamma_{AE,j}$, $\gamma_{RE,j}$ conditioned on G and G_1.

Based on RaF protocol, the SOPs of the two time-slots are independent [25]. The instantaneous achievable secrecy capacity of different physical scenes in two time-slots is defined as [36]

$$C_{S,k}=\max\left(C_{Bk}-C_{Ek},0\right)^{+},\tag{13}$$

where C_{Bk} and C_{Ek} are the capacities for main channel and the eavesdropping channel, respectively, $C_{Bk}=\log_2\left(1+\gamma_{Bk}\right)$, $C_{Ek}=\log_2\left(1+\gamma_{Ek}\right)$ and $k=\{1,2\}$ represents the first-hop and the second-hop, respectively. In order to maximize the secrecy capacity C_{Sk}, the C_{Bk} should be maximized and the C_{Ek} should be minimized through the selection of antennas at the Relay in two time-slots.

Two time-slots are independent transmission processes. For more notational convenient analysis, we define $\mu=\frac{Q}{P_t}$, $\varepsilon=\frac{\lambda_{RB}}{\lambda_{AR}}$, $\eta=\frac{\lambda_{RE}}{\lambda_{AE}}$, $\overline{\gamma_Z}=\frac{P_J}{\sigma^2}\lambda_{JE}$, $\overline{\gamma_B}=\frac{P_t}{\sigma^2}\lambda_{AR}=\frac{Q}{\mu\sigma^2}\lambda_{AR}=\frac{P_t}{\varepsilon\sigma^2}\lambda_{RB}=\frac{Q}{\varepsilon\mu\sigma^2}\lambda_{RB}$, $\overline{\gamma_E}=\frac{P_t}{\sigma^2}\lambda_{AE}=\frac{Q}{\mu\sigma^2}\lambda_{AE}=\frac{P_t}{\eta\sigma^2}\lambda_{RE}=\frac{Q}{\eta\mu\sigma^2}\lambda_{RE}$.

III. SECRECY PERFORMANCE ANALYSIS

In this section, we investigate the SOP of the dual-hop RaF cognitive wiretap networks over Rayleigh fading channels with MRC/MRC, SC-ZFB/MRT, SC-ZFB/ZFB schemes. The SOP is defined as the probability of the secrecy capacity, C_S, being lower than a predetermined threshold, R_s. Based on RaF protocol, the SOPs of the two time-slots are independent. Therefore, it is only necessary to solve the SOP of different physical scenes in two time-slots, and the expression can be expressed as [25], [37], [38]

$$\begin{aligned}P_{out}\left(R_s\right)&=\Pr\left(C_{S,k}<R_s\right)\\&=\int_0^{\infty}F_{\gamma_{Bk}}\left(2^{R_s}\left(1+y\right)-1\right)f_{\gamma_{Ek}}\left(y\right)dy\end{aligned}\tag{14}$$

and

$$P_{out}\left(R_s\right)=1-\Pr\left\{C_{S,1}^{\diamondsuit}>R_s\right\}\Pr\left\{C_{S,2}^{\aleph}>R_s\right\},\tag{15}$$

where $C_{S,1}^{\diamondsuit}$ and $C_{S,2}^{\aleph}$ denote the instantaneous secrecy capacity of the first-hop and the second-hop, respectively, $\diamondsuit\in\{MRC,SC-ZFB\}$ in the first hop, $\aleph\in\{MRT,ZFB\}$ in the second hop. The instantaneous secrecy capacity of the first-hop can be expressed as

$$\begin{aligned}C_{S,1}^{MRC}&=\log_2\frac{1+\gamma_{AR,1}}{1+\gamma_{AE,1}}\\&=\log_2\frac{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{\|\mathbf{h}_{AR}\|^2}{\sigma_R^2}}{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{|h_{AE}|^2}{\sigma_E^2}},\end{aligned}\tag{16}$$

and

$$\begin{aligned}C_{S,1}^{SC-ZFB}&=\log_2\frac{1+\gamma_{AR,2}}{1+\gamma_{AE,2}}\\&=\log_2\frac{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{\max\limits_{i\in N_R}\left(|h_{ARi}|^2\right)}{\sigma_R^2}}{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{|h_{AE}|^2}{P_J\left|\mathbf{h}_{RE}^{\dagger}\mathbf{w}_{ZF}\right|^2+\sigma_E^2}}.\end{aligned}\tag{17}$$

The instantaneous secrecy capacity of the second-hop can be expressed as

$$\begin{aligned}C_{S,2}^{MRT}&=\log_2\frac{1+\gamma_{RB,1}}{1+\gamma_{RE,1}}\\&=\log_2\frac{1+\min\left(\frac{Q}{|h_{RP}|^2},P_t\right)\frac{\|\mathbf{h}_{RB}\|^2}{\sigma_B^2}}{1+\min\left(\frac{Q}{|h_{RP}|^2},P_t\right)\frac{|h_{RE}|^2}{\sigma_E^2}}.\end{aligned}\tag{18}$$

The instantaneous secrecy capacity of the ZFB scheme can be expressed as $C_{S,2}^{ZFB}$. Since there is no eavesdropping link C_{E2} in $C_{S,2}^{ZFB}$, therefore $C_{S,2}^{ZFB}$ depends on the main link C_{B2}. And the solution process is given below in ZFB scheme of the SC-ZFB/ZFB scenario.

Using Eqs. (15), (16), (17) and (18), we have

$$\Pr\left\{C_{S,1}^{\diamondsuit}>R_s\right\}=1-\Pr\left\{\gamma_1^{\diamondsuit}\le 2^{R_s}\right\}=1-F_{\gamma_1^{\diamondsuit}}\left(R_s\right),\tag{19}$$

$$\Pr\left\{C_{S,2}^{\aleph}>R_s\right\}=1-\Pr\left\{\gamma_2^{\aleph}\le 2^{R_s}\right\}=1-F_{\gamma_2^{\aleph}}\left(R_s\right),\tag{20}$$

and

$$\gamma_1^{MRC}=\frac{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{\|\mathbf{h}_{AR}\|^2}{\sigma_R^2}}{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{|h_{AE}|^2}{\sigma_E^2}},\tag{21}$$

with

$$\gamma_1^{SC-ZFB}=\frac{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{\max\limits_{i\in N_R}\left(|h_{ARi}|^2\right)}{\sigma_R^2}}{1+\min\left(\frac{Q}{|h_{AP}|^2},P_t\right)\frac{|h_{AE}|^2}{P_J\left|\mathbf{h}_{RE}^{\dagger}\mathbf{w}_{ZF}\right|^2+\sigma_E^2}},\tag{22}$$

and

$$\gamma_2^{MRT}=\frac{1+\min\left(\frac{Q}{|h_{RP}|^2},P_t\right)\frac{\|\mathbf{h}_{RB}\|^2}{\sigma_B^2}}{1+\min\left(\frac{Q}{|h_{RP}|^2},P_t\right)\frac{|h_{RE}|^2}{\sigma_E^2}}.\tag{23}$$

$F_{\gamma_1^{\diamond}}(R_s)$ and $F_{\gamma_2^{\aleph}}(R_s)$ are the CDF of $\gamma_1^{\diamond}$ and $\gamma_2^{\aleph}$, respectively.

When the secondary user transmission link CSI is perfect, armed with (15), the SOP is expressed as

$$P_{out}(R_s) = F_{\gamma_1^{\diamond}}(R_s) + F_{\gamma_2^{\aleph}}(R_s) - F_{\gamma_1^{\diamond}}(R_s) F_{\gamma_2^{\aleph}}(R_s). \quad (24)$$

Next, we will solve the SOP of three different schemes one by one.

A. MRC/MRT WITH HD SCENARIO

In the first phase, on the basis of Eq. (1) and [22], the conditional CDF of first time slot $\gamma_{AR,1}$ is given by

$$F_{\gamma_{AR,1}}(x|G) = 1 - \exp\left(-\frac{\sigma_R^2}{P_S\lambda_{AR}}x\right)\sum_{k=0}^{N_R-1}\frac{1}{k!}\left(\frac{\sigma_R^2 x}{P_S\lambda_{AR}}\right)^k. \quad (25)$$

Similarly, on the basis of (3), the conditional PDF of $\gamma_{AE,1}$ can be represented as

$$f_{\gamma_{AE,1}}(y|G) = \frac{\sigma_E^2}{P_S\lambda_{AE}}\exp\left(-\frac{\sigma_E^2}{P_S\lambda_{AE}}y\right). \quad (26)$$

Then, substituting (25) and (26) into (14), we now give the CDF of γ_1^{MRC} in the following Lemma.

Lemma 1: The CDF of γ_1^{MRC} can be readily written as

$$\begin{aligned}
&F_{\gamma_1^{MRC}}(R_s)\\
&= 1 - \sum_{k=0}^{N_R-1}\frac{1}{k!}\frac{1}{(\overline{\gamma_B})^k\overline{\gamma_E}}\sum_{i=0}^{k}\binom{k}{i}\left(2^{R_s}-1\right)^{k-i}\\
&\quad\times\left(2^{R_s}\right)^i i!\left(\frac{\overline{\gamma_B\gamma_E}}{2^{R_s}\overline{\gamma_E}+\overline{\gamma_B}}\right)^{i+1}\left[\left(1-\exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right)\right.\\
&\quad\times\exp\left(-\frac{2^{R_s}-1}{\overline{\gamma_B}}\right)+\frac{\mu}{\lambda_{AP}}\left(\frac{\overline{\gamma_B}\lambda_{AP}}{\left(2^{R_s}-1\right)\lambda_{AP}+\overline{\gamma_B}\mu}\right)^{k-i+1}\\
&\quad\left.\times\Gamma\left(k-i+1,\frac{\left(2^{R_s}-1\right)\lambda_{AP}+\mu\overline{\gamma_B}}{\overline{\gamma_B}\lambda_{AP}}\right)\right], \quad (27)
\end{aligned}$$

where $\Gamma(\cdot,\cdot)$, as defined in [39, Eq. (8.350.2)], is the incomplete gamma function.

Proof: See Appendix A.

In the second phase, the CDF of γ_2^{MRT} is similar to description process of the Eq. (27) and is not derived here, only with the change of parameters, i.e., $\lambda_{AP} \rightarrow \lambda_{RP}$, $\lambda_{AR} \rightarrow \lambda_{RB}$, $\lambda_{AE} \rightarrow \lambda_{RE}$. The CDF of γ_2^{MRT} can be given as $F_{\gamma_2^{MRT}}(R_s)$.

Substituting the CDF of γ_1^{MRC} and γ_2^{MRT} into (24), the SOP can be derived after a few simple mathematical calculations, Just replace $\diamond$, $\aleph$ with MRC and MRT in the (24), respectively.

B. SC-ZFB/MRT WITH FD SCENARIO

In the first phase, on the basis of Eq. (8) and [38], the conditional CDF of first time slot $\gamma_{AR,2}$ is given by

$$F_{\gamma_{AR,2}}(x|G) = 1 - \sum_{n=1}^{N_R}\binom{N_R}{n}(-1)^{n-1}\exp\left(-\frac{\sigma_R^2 n}{P_S\lambda_{AR}}x\right). \quad (28)$$

Similarly, based on (9), the instantaneous SNR of the eavesdropping link can be expressed as below Lemma.

Lemma 2: The PDF of $\gamma_{AE,2}$ can be computed as

$$\begin{aligned}
&f_{\gamma_{AE,2}}(y|G)\\
&= \frac{\sigma_E^2}{P_S\lambda_{AE}}exp\left(-\frac{\sigma_E^2 y}{P_S\lambda_{AE}}\right)\left(\frac{P_S\lambda_{AE}}{P_J\lambda_{JE}y+P_S\lambda_{AE}}\right)^{N_R-2}\\
&\quad+exp\left(-\frac{\sigma_E^2 y}{P_S\lambda_{AE}}\right)\frac{(N_R-2)P_J\lambda_{JE}(P_S\lambda_{AE})^{N_R-2}}{(P_J\lambda_{JE}y+P_S\lambda_{AE})^{N_R-1}}. \quad (29)
\end{aligned}$$

Proof: See Appendix B.

Then, armed with (28), (29) and (14), the CDF of γ_1^{SC-ZFB} with SC-ZFB scheme can be expressed as below Theorem.

Theorem 1: The CDF of γ_1^{SC-ZFB} can be expressed as

$$\begin{aligned}
&F_{\gamma_1^{SC-ZFB}}(R_s)\\
&= 1 - \sum_{n=1}^{N_R}\binom{N_R}{n}(-1)^{n-1}\left[\frac{1}{\overline{\gamma_Z}}\right.\\
&\quad\times\Psi\left(1,4-N_R,\frac{n2^{R_s}\overline{\gamma_E}+\overline{\gamma_B}}{\overline{\gamma_B\gamma_Z}}\right)+(N_R-2)\\
&\quad\left.\times\Psi\left(1,3-N_R,\frac{n2^{R_s}\overline{\gamma_E}+\overline{\gamma_B}}{\overline{\gamma_B\gamma_Z}}\right)\right]\\
&\quad\times\left[\left(1-\exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right)\right.\\
&\quad\times\exp\left(-\frac{n\left(2^{R_s}-1\right)}{\overline{\gamma_B}}\right)+\frac{\mu\overline{\gamma_B}}{n\left(2^{R_s}-1\right)\lambda_{AP}+\mu\overline{\gamma_B}}\\
&\quad\left.\times\exp\left(-\frac{n\left(2^{R_s}-1\right)\lambda_{AP}+\mu\overline{\gamma_B}}{\overline{\gamma_B}\lambda_{AP}}\right)\right]. \quad (30)
\end{aligned}$$

We obtain (30) with the help of [39, Eq. (9.211.4)].

Proof: See Appendix C.

In the second phase, the CDF of γ_2^{MRT} with the MRT scheme is similar to description process of the $F_{\gamma_2^{MRT}}(R_s)$ of MRC/MRT scenario and is not derived here.

Substituting the CDF of γ_1^{SC-ZFB} and γ_2^{MRT} into (24), the SOP can be derived after a few simple mathematical calculations. Just replace $\diamond$, $\aleph$ with SC-ZFB and MRT in the (24), respectively.

C. SC-ZFB/ZFB WITH FD SCENARIO

In the first phase, Relay adopts the SC-ZFB scheme with FD operation, which is similar to description process of the Eq. (30) and is not derived here.

In the second phase, according to (10) and based on ZFB scheme, the expression of CDF of main link transmission channel can be expressed as $F_{\gamma_2^{ZFB}}$.

Lemma 3: The CDF of γ_2^{ZFB} with the ZFB scheme is given by

$$\begin{aligned}
F_{\gamma_2^{ZFB}}(R_s) &= \Pr\left(\gamma_{RB,3} < \left(2^{R_s}-1\right)\right)\\
&= 1-\exp\left(-\frac{\left(2^{R_s}-1\right)}{\overline{\gamma_B}}\right)\sum_{l=0}^{N_R-3}\frac{1}{l!}\left(\frac{\left(2^{R_s}-1\right)}{\overline{\gamma_B}}\right)^l. \quad (31)
\end{aligned}$$

Substituting (30) and (31) into (24), the SOP of SC-ZFB/ZFB scenario can be derived after a few simple mathematical calculations. Just replace ◇, ℵ with SC-ZFB and ZFB in the (24), respectively.

So far, we have completed the achievable secrecy performance analysis of the MRC/MRT, SC-ZFB/MRT and SC-ZFB/ZFB schemes. The following presents high SNR analysis results of the MRC/MRT over the HD operation and the SC-ZFB/MRT, SC-ZFB/ZFB schemes over FD operation.

IV. HIGH SNR ANALYSIS

The secrecy performance of the system can be verified based on the derived closed-form expressions above. However, the derivation of expression is complex and the analysis of system secrecy performance is limited. Therefore, we gain more insight on system secrecy performance by deriving high SNR analysis expression. Thus, in this section, we will derive and analyze the high SNR in a specific way. Specifically, considering two different scenarios: 1) Scenario I: $\overline{\gamma_{BJ}} \rightarrow \infty$ and fixed $\overline{\gamma_{EJ}}$, that is a scenario where the eavesdropper is located far away from the legitimate secondary users while the SNR of the secondary user transmission link is significantly better than the SNR of the wiretap channel link and 2) Scenario II: $\overline{\gamma_{BJ}} \rightarrow \infty$ and $\overline{\gamma_{EJ}} \rightarrow \infty$, that is a scenario where Relay and eavesdropper are located close to the Alice, i.e., both the main channel link and the wiretap channel link have superior SNR. Finally, the secrecy performance can be expressed, which extract several key secrecy performance indicators by the parameters of the expression, i.e., the high SNR slope, the secrecy diversity gain and secrecy coding gain. In this section, for $\overline{\gamma_{BJ}}$ and $\overline{\gamma_{EJ}}$, $J \in (1, 2, 3)$ stand for scenario 1, scenario 2 and scenario 3, respectively.

A. SCENARIO I: $\overline{\gamma_{BJ}} \rightarrow \infty$ AND FIXED $\overline{\gamma_{Ej}}$

In this case, we use a new way to derive SOP in the following Corollary.

1) MRC/MRT scheme:

Corollary 1: The SOP of the MRC/MRT scheme with HD operation under $\overline{\gamma_{B1}} \rightarrow \infty$ and fixed $\overline{\gamma_{E1}}$ is approximated as

$$P_{out}^{MRC/MRT}(R_s) \approx \Delta_{MRC/MRT}\left(\frac{1}{\overline{\gamma_{B1}}}\right)^{N_R}, \tag{32}$$

where $\Delta_{MRC/MRT}$ is readily given by

$$\begin{aligned}
&\Delta_{MRC/MRT}\\
&= \left(1+\left(\frac{1}{\varepsilon}\right)^{N_R}\right)\left[\left(1-\exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right)\right.\\
&\quad\times\left(\frac{1}{N_R!}\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}q!(\overline{\gamma_{E1}})^{q}\right)\\
&\quad+\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}q!\frac{1}{N_R!}\left(\frac{1}{\mu}\right)^{N_R}\\
&\quad\left.\times(\overline{\gamma_{E1}})^{q}{\lambda_{AP}}^{N_R}\Gamma\left(N_R+1,\frac{\mu}{\lambda_{AP}}\right)\right].
\end{aligned} \tag{33}$$

Proof: See Appendix D.

2) SC-ZFB/MRT scheme:

Corollary 2: The SOP of the SC-ZFB/MRT scheme with FD operation under $\overline{\gamma_{B2}} \rightarrow \infty$ and fixed $\overline{\gamma_{E2}}$ is approximated as

$$P_{out}^{SC-ZFB/MRT}(R_s) \approx \Delta_{SC-ZFB/MRT}\left(\frac{1}{\overline{\gamma_{B2}}}\right)^{N_R}, \tag{34}$$

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

$$\begin{aligned}
&\Delta_{SC-ZFB/MRT}\\
&= (\Lambda_1+\Lambda_2)\left[\left(1-\exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right)+\left(\frac{1}{\mu}\right)^{N_R}\right.\\
&\quad\left.\times\left(\frac{1}{\lambda_{AP}}\right)^{-N_R}\Gamma\left(N_R+1,\frac{\mu}{\lambda_{AP}}\right)\right]+\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}\right)^{q}q!\\
&\quad\times\left(2^{R_s}-1\right)^{N_R-q}(\overline{\gamma_{E2}})^{q}\left(\frac{1}{\varepsilon}\right)^{N_R}\frac{1}{N_R!}\left[\left(1-\exp\left(-\frac{\mu}{\lambda_{RP}}\right)\right)\right.\\
&\quad\left.+\left(\frac{1}{\mu}\right)^{N_R}{\lambda_{RP}}^{N_R}\Gamma\left(N_R+1,\frac{\mu}{\lambda_{RP}}\right)\right],
\end{aligned} \tag{35}$$

with Λ_1 and Λ_2 being expressed as

$$\begin{aligned}
\Lambda_1 &= \sum_{q=0}^{N_R}\binom{N_R}{j}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}\frac{1}{\overline{\gamma_{E2}}}\\
&\quad\times\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^{q+1}\Gamma(q+1)\,\Psi\left(q+1,q+4-N_R;\frac{1}{\overline{\gamma_Z}}\right),
\end{aligned} \tag{36}$$

and

$$\begin{aligned}
\Lambda_2 &= \sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}(N_R-2)\\
&\quad\times\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^{q}\Gamma(q+1)\,\Psi\left(q+1,q+3-N_R;\frac{1}{\overline{\gamma_Z}}\right).
\end{aligned} \tag{37}$$

Proof: See Appendix E.

3) SC-ZFB/ZFB scheme:

Corollary 3: The SOP of the SC-ZFB/ZFB scheme with FD operation under $\overline{\gamma_{B3}} \rightarrow \infty$ and fixed $\overline{\gamma_{E3}}$ is approximated as

$$P_{out}^{SC-ZFB/ZFB}(R_s) \approx \Delta_{SC-ZFB/ZFB}\left(\frac{1}{\overline{\gamma_{B3}}}\right)^{N_R-2}, \tag{38}$$

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

$$\Delta_{SC-ZFB/ZFB} = \frac{1}{(N_R-2)!}\left(2^{R_s}-1\right)^{N_R-2}. \tag{39}$$

Proof: See Appendix F.

Remark 1: In Scenario I, the MRC/MRT and SC-ZFB/MRT schemes achieve N_R secrecy diversity gain, the SC-ZFB/ZFB scheme achieves N_R-2 secrecy diversity gain, which only depends on the number of the antennas of Relay.

In addition, the quality of the main channel and eavesdropper's channel and the primary networks influence the secrecy performance of the considered schemes through the coding gain, i.e., $G_a = \Delta_{MRC/MRT}{}^{-1/N_R}$, $G_b = \Delta_{SC-ZFB/MRT}{}^{-1/N_R}$ and $G_c = \Delta_{SC-ZFB/ZFB}{}^{-1/(N_R-2)}$. In addition, the secrecy coding gain will mainly affects the secrecy performance of the considered networks, which is verified in the simulation section. We also find that the more relay antennas, the better the system performance. Therefore, to improve secrecy performance of the considered networks, the actual system design should increase the number of the antennas at Relay as much as possible.

B. SCENARIO II: $\overline{\gamma_{BJ}} \to \infty$ AND $\overline{\gamma_{Ej}} \to \infty$

Now, we will begin to analyze the approximated SOP of FD multi-antenna spectrum-sharing wiretap networks under the scenario II.

1) MRC/MRT scheme:

Corollary 4: The approximated SOP of FD operation with MRC/MRT scheme under $\overline{\gamma_{B1}} \to \infty$ and $\overline{\gamma_{E1}} \to \infty$ is given by

$$P_{out}^{MRC/MRT}(R_s) \approx 1 - \left(1 - F_{\gamma_1^{MRC}}(R_s)\right)\left(1 - F_{\gamma_2^{MRT}}(R_s)\right), \quad (40)$$

where $F_{\gamma_1^{MRC}}(R_s)$ being expressed as

$$\begin{aligned} F_{\gamma_1^{MRC}}(R_s) &\approx \left(1 - \exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right) \\ &\quad \times \left[1 - \sum_{k=0}^{N_R-1} \frac{\left(2^{R_s}\right)^k}{\left(\overline{\gamma_{B1}}\right)^k \overline{\gamma_{E1}}} \left(\frac{\overline{\gamma_{B1}\gamma_{E1}}}{2^{R_s}\overline{\gamma_{E1}} + \overline{\gamma_{B1}}}\right)^{k+1}\right] \\ &\quad + \exp\left(-\frac{\mu}{\lambda_{AP}}\right) \\ &\quad - \sum_{k=0}^{N_R-1} \frac{\left(2^{R_s}\right)^k}{\left(\overline{\gamma_{B1}}\right)^k \overline{\gamma_{E1}}} \left(\frac{\overline{\gamma_{B1}\gamma_{E1}}}{2^{R_s}\overline{\gamma_{E1}} + \overline{\gamma_{B1}}}\right)^{k+1} \Gamma\left(1, \frac{\mu}{\lambda_{AP}}\right), \end{aligned} \quad (41)$$

and just replace $\lambda_{AP} \to \lambda_{RP}$, $\lambda_{AR} \to \lambda_{RB}$, $\lambda_{AE} \to \lambda_{RE}$ in the (41), which can be written as $F_{\gamma_2^{MRT}}(R_s)$.

Proof: From $F_{\gamma_1^{MRC}}(R_s)$ and $F_{\gamma_2^{MRT}}(R_s)$, when $\overline{\gamma_{B1}} \to \infty$ and $\overline{\gamma_{E1}} \to \infty$, the $F_{\gamma_1^{MRC}}(R_s)$ and $F_{\gamma_2^{MRT}}(R_s)$ can be readily derived after a few simple mathematical calculations. Upon substituting $F_{\gamma_1^{MRC}}(R_s)$ and $F_{\gamma_2^{MRT}}(R_s)$ into (40), the final result of MRC/MRT scheme is request.

2) SC-ZFB/MRT scheme:

Corollary 5: The approximated SOP of the SC-ZFB/MRT scheme with FD operation under $\overline{\gamma_{B2}} \to \infty$ and $\overline{\gamma_{E2}} \to \infty$ is given by

$$P_{out}^{SC-ZFB/MRT}(R_s) \approx 1 - \left(1 - F_{\gamma_1^{SC-ZFB}}(R_s)\right)\left(1 - F_{\gamma_2^{MRT}}(R_s)\right), \quad (42)$$

where $F_{\gamma_1^{SC-ZFB}}(R_s)$ being expressed as

$$\begin{aligned} F_{\gamma_1^{SC-ZFB}}(R_s) &\approx 1 - \sum_{n=1}^{N_R} \binom{N_R}{n} (-1)^{n-1} \\ &\quad \times \left[\frac{1}{\overline{\gamma_Z}} \Psi\left(1, 4 - N_R, \frac{n2^{R_s}\overline{\gamma_{E2}} + \overline{\gamma_{B2}}}{\overline{\gamma_{B2}\gamma_Z}}\right)\right. \\ &\quad \left. - (N_R - 2)\, \Psi\left(1, 3 - N_R, \frac{n2^{R_s}\overline{\gamma_{E2}} + \overline{\gamma_{B2}}}{\overline{\gamma_{B2}\gamma_Z}}\right)\right]. \end{aligned} \quad (43)$$

And $F_{\gamma_2^{MRT}}(R_s)$ is similar to description process of the second phase of MRC/MRT scheme, and is not wrote here.

Proof: Upon substituting (43) and $F_{\gamma_2^{MRT}}(R_s)$ into (42), the final result of SC-ZFB/MRT scheme is obtained.

3) SC-ZFB/ZFB scheme:

Corollary 6: The approximated SOP of the SC-ZFB/ZFB scheme with FD operation under $\overline{\gamma_{B3}} \to \infty$ and $\overline{\gamma_{E3}} \to \infty$ is given by

$$P_{out}^{SC-ZFB/ZFB}(R_s) \approx 1 - \left(1 - F_{\gamma_1^{SC-ZFB}}(R_s)\right)\left(1 - F_{\gamma_2^{ZFB}}(R_s)\right), \quad (44)$$

where $F_{\gamma_1^{SC-ZFB}}(R_s)$ is similar to Eq. (43) and is not wrote here, and $F_{\gamma_2^{ZFB}}(R_s)$ being expressed as

$$F_{\gamma_2^{ZFB}}(R_s) \approx \left(\frac{1}{\overline{\gamma_{B3}}}\right)^{N_R-2} \frac{1}{(N_R-2)!}\left(2^{R_s} - 1\right)^{N_R-2}. \quad (45)$$

Proof: The derivation process is similar to ***Corollary 5*** and will not be described in detail again.

Remark 2: On the contrary of Scenario I, three schemes appear to be the secrecy outage floor when $\overline{\gamma_{BJ}} \to \infty$ and $\overline{\gamma_{EJ}} \to \infty$, which shows that the secrecy diversity cannot be gained. Therefore, the secrecy performance of the system would be affected by the secrecy coding gain, and the SC-ZFB/ZFB scheme achieves the best performance through secrecy coding gain than the other two schemes.

V. NUMERICAL RESULTS

In this section, we present representative numerical results to verify the analytical ones. Numerical results are provided to validate analytical expressions, demonstrate the performance of the MRC/MRT, SC-ZFB/MRT, and SC-ZFB/ZFB schemes and investigate the impact of key system parameters on their performances, i.e., the different number of antennas and thresholds. Without loss of generality, we assume the following simulation parameters for this section: $R_s = 2$, $\sigma^2 = \sigma_R^2 = \sigma_B^2 = \sigma_E^2 = 1$ and $\varepsilon = \eta = 1$. The distance between any two nodes is normalized to 1. The theoretical simulation curves in all the graphs are completely in conformity with the Monte Carlo simulation results, which verify the validity of the theory. We clearly found that the asymptotic curves approximate the exact curve at high SNR. The secrecy diversity order in the asymptotic analysis expressions are also verified by the asymptotic curves.

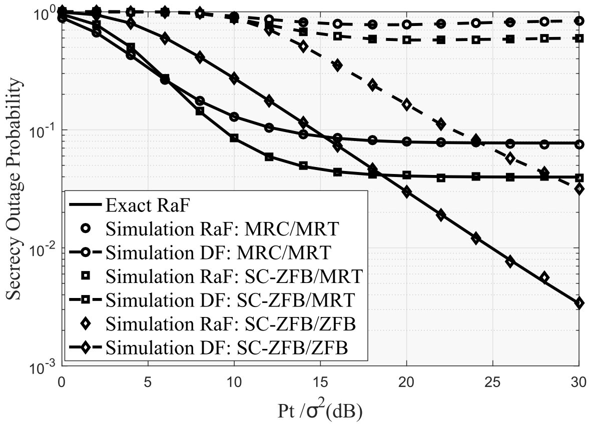

FIGURE 2. Secrecy outage probability of two different relaying strategies for the three proposed schemes.

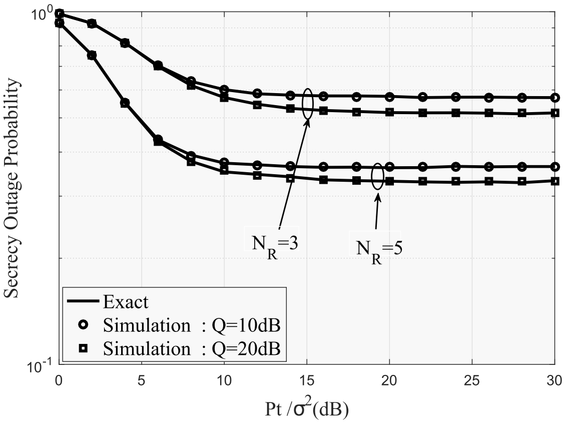

FIGURE 4. Secrecy outage probability of SC-ZFB/MRT scheme for different number N_R and Q.

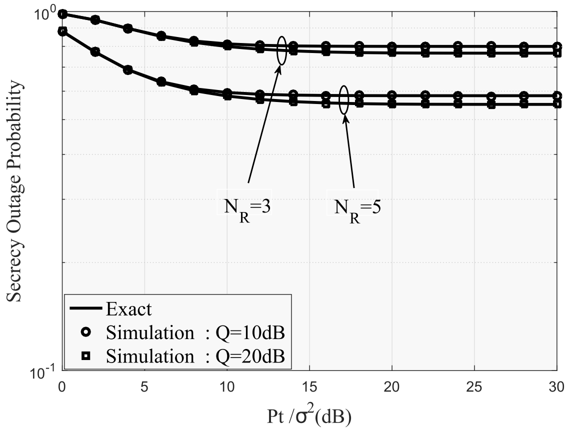

FIGURE 3. Secrecy outage probability of MRC/MRT scheme for different number N_R and Q.

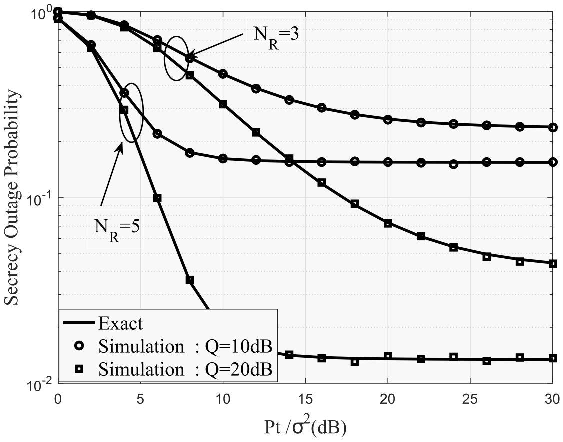

FIGURE 5. Secrecy outage probability of SC-ZFB/ZFB scheme for different number N_R and Q.

Fig. 2 presents the SOP versus P_t/σ^2 of two different relaying strategies for the three proposed schemes when $N_R = 3$, $Q = 20dB$. From this figure, we find that the RaF relaying strategy achieves better secrecy performance than the DF relaying strategy for dual-hop cognitive wiretap networks in improving secrecy performance of system. In addition, the SOP of the considered system using RaF relaying strategy becomes saturated due to the fixed interference temperature constraint, which verifies the analytical results shown in (40), (42) and (44). However, it is observed that the SOP first decreases and then increases as P_t/σ^2 increases by using DF relaying strategy. This is because the instantaneous SNR gap between the main channel and the eavesdropper's channel depends on the interference threshold Q in the condition of high SNR, and the instantaneous SNR gap will decrease by increasing the SNR.

Figs. 3, 4 and 5 illustrate the SOPs of the MRC/MRT, SC-ZFB/MRT and SC-ZFB/ZFB schemes for different number N_R and Q, respectively. The exact curves are obtained from the SOP of MRC/MRT, SC-ZFB/MRT and SC-ZFB/ZFB, respectively. As increasing N_R, the SOPs in three schemes decreases. And in this section, three schemes appear to be the secrecy outage floor when P_t/σ^2 increases. This is because when the maximum transmit power P_t of the secondary user transmitter increases to a certain range, the interference temperature constraint Q of the primary user becomes a major factor affecting the secrecy performance of the system. In addition, when the number of N_R and the interference thresholds Q are fixed in this three schemes, the FD technical operation scheme is better than HD operation to improve secrecy performance of considered system. Thus, we analyze the cases of cognitive wiretap networks with SC-ZFB/MRT and SC-ZFB/ZFB schemes to enhance the secrecy performance of the FD CRNs in the harmful invasion of the eavesdroppers at the illegitimate side. The SC-ZFB/ZFB scheme obviously outperform the SC-ZFB/MRT and MRC/MRT schemes to improve the secrecy performance of wireless communications.

Fig. 6 plots the SOP versus SNR for the three proposed schemes when the secondary user receiver is near to the secondary user transmitter and the asymptotic expressions curves of SOP are obtained from (32), (34) and (38) under

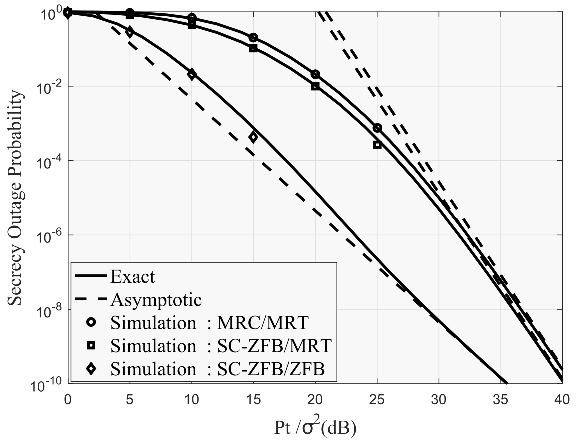

FIGURE 6. Exact and asymptotic secrecy outage probability of MRC/MRT, SC-ZFB/MRT, SC-ZFB/ZFB schemes under Scenario I when $N_R = 5$ and $\overline{\gamma_{EJ}} = 10$ dB.

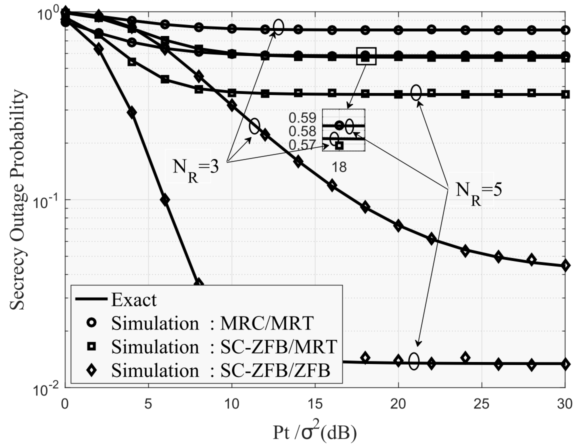

FIGURE 8. Secrecy outage probability of all schemes for different number N_R.

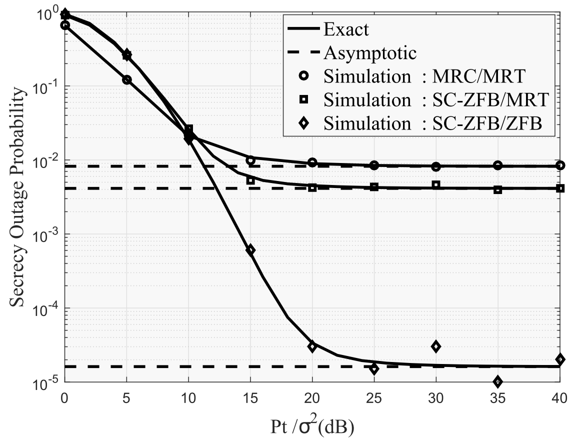

FIGURE 7. Exact and asymptotic secrecy outage probability of MRC/MRT, SC-ZFB/MRT, SC-ZFB/ZFB schemes under Scenario II when $N_R = 5$.

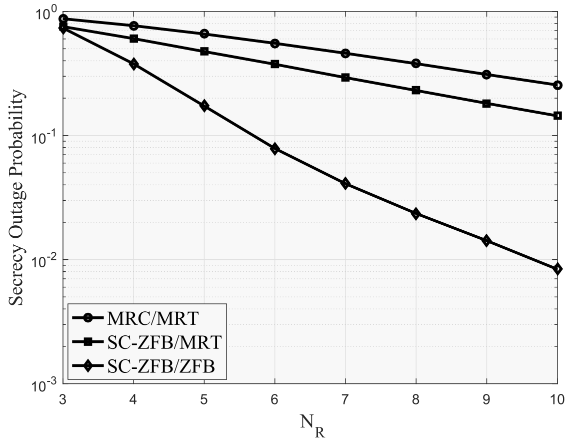

FIGURE 9. Secrecy outage probability of all schemes for different number N_R.

the $\overline{\gamma_{BJ}} \rightarrow \infty$ and fixed $\overline{\gamma_{EJ}}$, respectively. The parallel slope of the asymptote shows that the high SNR slope is independent of the N_R. The SOP of the system decreases as the Q increases. Furthermore, we see that the SC-ZFB/ZFB and SC-ZFB/MRT schemes with FD outperform MRC/MRT scheme with HD, which indicates that using the SC-ZFB scheme between Alice and Relay or by transmitting jamming signals from a FD relay will improve the secrecy diversity gain of the system compared to the MRC/MRT scheme under Scenario I. The SC-ZFB/ZFB scheme achieves the lowest secrecy diversity gain and the higher secrecy coding gain than the other two schemes, which is demonstrated in Fig. 7.

Fig. 7 presents the SOP versus SNR of the three proposed schemes when $N_R = 5$, $\overline{\gamma_{BJ}} \rightarrow \infty$ and $\overline{\gamma_{EJ}} \rightarrow \infty$, and $\overline{\gamma_{BJ}}/\overline{\gamma_{EJ}} = 8$ dB. The asymptotic expressions curves of SOP are obtained from (40), (42) and (44) under the $\overline{\gamma_{BJ}} \rightarrow \infty$ and $\overline{\gamma_{EJ}} \rightarrow \infty$, respectively. Through the analytical results, all schemes achieve better secrecy performance. In addition, the SC-ZFB/MRT and SC-ZFB/ZFB schemes are better than MRC/MRT scheme in terms of improving secrecy performance of the considered networks. The secrecy performance of the considered schemes with FD operation is mainly influenced by the secrecy coding gain. The SC-ZFB/ZFB scheme achieves the best performance through secrecy coding gain than the other two schemes.

Fig. 8 presents the SOP versus SNR of all schemes for different number N_R and interference temperature constraint $Q = 10$ dB. We can know that the SC-ZFB/ZFB scheme outperforms the SC-ZFB/MRT and MRC/MRT schemes. In particular, the value of N_R has a greater impact on the secrecy performance of the system in the SC-ZFB/ZFB scheme than in the SC-ZFB/MRT and MRC/MRT schemes. This is due to the fact that the number of antennas at Relay has more influence on secrecy coding gain of the SC-ZFB/ZFB scheme than that of the other schemes. When the transmit power reaches the certain range, the secrecy outage floor of system tends to be stable, and the Q becomes the main factor affecting the secrecy performance of the considered networks.

Figs. 9 and 10 illustrate the influence of the number of the antennas, N_R and Q on the secrecy outage performance of the

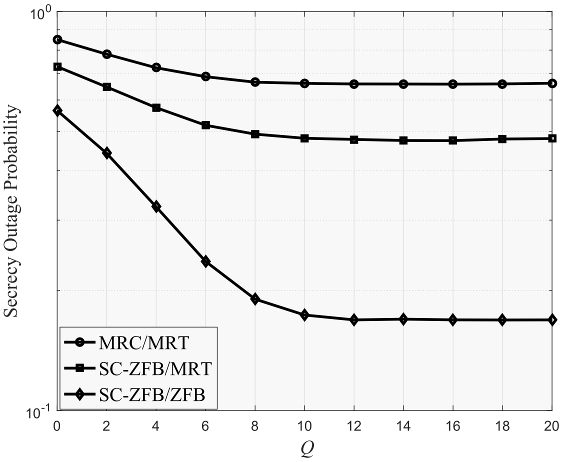

FIGURE 10. Secrecy outage probability of all schemes for different number *Q*.

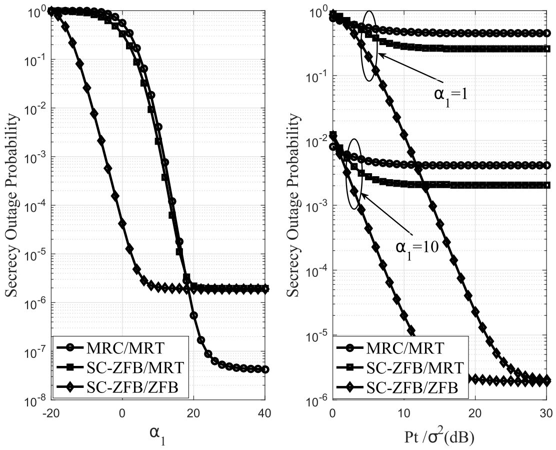

FIGURE 11. Secrecy outage probability of all schemes for different α_1.

three proposed schemes, respectively. In addition, we assume the following simulation parameters: SNR=5dB and $Q = 20$ dB in Fig. 9, SNR=5dB and $N_R = 5$ in Fig. 10. It is obvious from Fig. 8 that by increasing N_R, the SOP can be obviously reduced in these three schemes. This can be rather intuitive because increasing N_R provides additional secrecy diversity or secrecy coding gain. Furthermore, when the Q is large enough, the SC-ZFB/ZFB scheme will outperform than the SC-ZFB/MRT and MRC/MRT schemes, albeit with higher complexity. It is evident from Fig. 10 that by increasing Q, the SOP can be significantly reduced for all schemes. However, when Q is large enough, the SOP appears to be the secrecy outage floor because the transmission power has become the highest. At this point, we can improve the system security by increasing N_R. From these two figures, it can be found that the secrecy performance can be improved by increasing the number of N_R or the interference threshold Q.

Fig. 11 shows the secrecy outage probability vs $\alpha_1 = \lambda_{AR}/\lambda_{AE}$, and $\alpha_2 = \lambda_{RB}/\lambda_{RE} = (\varepsilon/\eta)\,\alpha_1$. When we set the SNR=20dB, $Q = 20$ dB and $N_R = 5$ in the first figure, according to the simulation results, it can be seen from the figure that when α_1 is relative low, the SOP of all schemes decreases with the increase of α_1. When α_1 is less than 18, the SC-ZFB/ZFB scheme always attains better performance than the SC-ZFB/MRT and MRC/MRT schemes. This is because there is little difference between the main channel and the eavesdropping channel. However, when α_1 is more than 18, the eavesdropper has weak eavesdropping ability and the noise power is almost zero, so there is no eavesdropping and interference object for SC-ZFB/MRT and SC-ZFB/ZFB schemes. Therefore, the MRC/MRT scheme achieves better performance than the SC-ZFB/MRT and SC-ZFB/ZFB schemes. In particular, when α_1 is large enough and the difference between the main channel and the eavesdropping channel is large, the SOP appears to be the secrecy outage floor because of the non-existence of eavesdropper. When we set the $Q = 20$ dB and $N_R = 5$ in the second figure, it shows that as the α_1 increases, the SOP of all schemes decreases. When $\alpha_1 = 1$, the MRC/MRT and SC-ZFB/MRT schemes have less influence on the change of the system performance. This is because the eavesdropper has strong eavesdropping ability. When $\alpha_1 = 10$, it can be seen from the figure that the SOP of all schemes have obvious influence on the improvement of secrecy performance of system. In our paper, we assume that eavesdropper has strong eavesdropping ability. Therefore, in Figs. 3, 4 and 8, the SOP of MRC/MRT and SC-ZFB/MRT schemes has less influence on the change of the system performance.

VI. CONCLUSION

In this paper, we have analyzed the secrecy performance of dual-hop RaF cognitive wiretap networks with MRC/MRT, SC-ZFB/MRT and SC-ZFB/ZFB schemes, respectively. To exploit the advantages of dual-hop RaF cognitive wiretap networks, we have put forward three secure transmission schemes with HD or FD operations at Relay. In doing so, the exact closed-form expressions for the SOP of cognitive relaying wiretap channels with MRC/MRT, SC-ZFB/MRT and SC-ZFB/ZFB schemes were derived. Using these expressions, we also investigated simple asymptotic approximations for the SOP in the high SNR under two different scenarios. The closed-form expressions for the exact and asymptotic SOP concisely characterized the secrecy diversity gain and the secrecy coding gain. In addition, we found that the SC-ZFB/ZFB scheme outperforms MRC/MRT and SC-ZFB/MRT schemes, which verifies the validity of our proposed schemes. We also found that the secrecy performance of the proposed schemes with FD operation is mainly influenced by the secrecy coding gain. Finally, the simulation results that when the eavesdropping ability is strong, the FD schemes is more effective than the HD scheme. On the contrary, if the eavesdropping ability is weak, the HD scheme can achieve better performance than FD schemes. Motivated by this, in our further works, we will consider a set of eavesdroppers, as well as imperfect CSI which constitute a more realistic configuration in multi-antenna-based traffic-aware two-way relay systems with unavoidable CSI imperfections at FD Relay nodes.

APPENDIXES

APPENDIX A

PROOF OF LEMMA 1

After conducting a few simple mathematical calculations, the $F_{\gamma_{AR,1}}(y|G)$ can be expressed as

$$\begin{aligned}
&F_{\gamma_{AR,1}}(y|G)\\
&= \int_0^{\infty} F_{\gamma_{AR,1}}\left(2^{R_s}(1+y)-1|G\right) f_{\gamma_{AE,1}}(y|G)\,dy\\
&= 1-\exp\left(-\frac{\sigma_R^2\left(2^{R_s}-1\right)}{P_S\lambda_{AR}}\right)\sum_{k=0}^{N_R-1}\frac{1}{k!}\left(\frac{\sigma_R^2}{P_S\lambda_{AR}}\right)^k\frac{\sigma_E^2}{P_S\lambda_{AE}}\\
&\quad\times\sum_{i=0}^{k}\binom{k}{i}\left(2^{R_s}\right)^i\left(2^{R_s}-1\right)^{k-i}\\
&\quad\times i!\left(\frac{P_S\lambda_{AR}P_S\lambda_{AE}}{\sigma_R^2\left(2^{R_s}P_S\lambda_{AE}+P_S\lambda_{AR}\right)}\right)^{i+1}. \qquad (46)
\end{aligned}$$

Hence, the CDF of $\gamma_{AR,1}$ can be derived as

$$\begin{aligned}
&F_{\gamma_{AR,1}}^{MRC}(R_s)\\
&= \int_0^{\infty}\Bigg(1-\exp\left(-\frac{\sigma_R^2\left(2^{R_s}-1\right)}{P_S\lambda_{AR}}\right)\sum_{k=0}^{N_R-1}\frac{1}{k!}\\
&\quad\times\left(\frac{\sigma_R^2}{P_S\lambda_{AR}}\right)^k\frac{\sigma_E^2}{P_S\lambda_{AE}}\sum_{i=0}^{k}\binom{k}{i}\left(2^{R_s}\right)^i\left(2^{R_s}-1\right)^{k-i}i!\\
&\quad\times\left(\frac{P_S\lambda_{AR}P_S\lambda_{AE}}{\sigma_R^2\left(2^{R_s}P_S\lambda_{AE}+P_S\lambda_{AR}\right)}\right)^{i+1}\Bigg) f_G(g)\,dg. \qquad (47)
\end{aligned}$$

To this end, substituting the PDF of G into (47) and with the help of [39, Eq. (3.381.3)], the desired CDF of γ_1^{MRC} with the MRC scheme result can be derived after a few simple algebraic calculations.

APPENDIX B

PROOF OF LEMMA 2

We first denote $R_1 = \frac{P_J\left|h_{RE}^{\dagger}w_{ZF}\right|^2}{\sigma^2}$. Using Eq. (12) of [40], the expression can be expressed as

$$f_{R_1}(z) = \frac{z^{N_R-3}\exp\left(-\frac{\sigma^2 z}{P_J\lambda_{JE}}\right)}{(N_R-3)!\left(P_J\lambda_{JE}/\sigma^2\right)^{N_R-2}}, N_R \geq 3. \qquad (48)$$

The $\gamma_{AE,2}$ can also be written as

$$\gamma_{AE,2} = \frac{P_S|h_{AE}|^2}{P_J\left|h_{RE}^{\dagger}w_{ZF}\right|^2+\sigma_E^2} = \frac{X_E}{z+1}. \qquad (49)$$

Then, $F_{\gamma_{AE,2}}(y|G)$ can be derived as

$$\begin{aligned}
F_{\gamma_{AE,2}}(y|G) &= 1-\exp\left(-\frac{\sigma_E^2 y}{P_S\lambda_{AE}}\right)\\
&\quad\times\left(\frac{P_S\lambda_{AE}}{P_J\lambda_{JE}y+P_S\lambda_{AE}}\right)^{N_R-2}. \qquad (50)
\end{aligned}$$

Finally, the conditional PDF of $\gamma_{AE,2}$ can be obtained by taking a simple derivative.

APPENDIX C

PROOF OF THEOREM 1

Hence, the $F_{\gamma_{AR,2}}(y|G)$ of the SC-ZFB scheme can be derived as (51), shown at the bottom of this page.

$$\begin{aligned}
&F_{\gamma_{AR,2}}(y|G)\\
&\quad= \int_0^{\infty} F_{\gamma_{AR,2}}\left(2^{R_s}(1+y)-1|G\right) f_{\gamma_{AE,2}}(y|G)\,dy\\
&\quad= 1-\sum_{n=1}^{N_R}\binom{N_R}{n}(-1)^{n-1}\underbrace{\int_0^{\infty}\exp\left(-\frac{\sigma_R^2}{P_S\lambda_{AR}}\left(2^{R_s}(1+y)-1\right)\right)\frac{\sigma_E^2}{P_s\lambda_{AE}}exp\left(-\frac{\sigma_E^2 y}{P_s\lambda_{AE}}\right)\left(\frac{P_S\lambda_{AE}}{P_J\lambda_{JE}y+P_S\lambda_{AE}}\right)^{N_R-2}dy}_{\Xi 1}\\
&\qquad-\sum_{n=1}^{N_R}\binom{N_R}{n}(-1)^{n-1}\underbrace{\int_0^{\infty}\exp\left(-\frac{\sigma_R^2 n}{P_S\lambda_{AR}}\left(2^{R_s}(1+y)-1\right)\right)exp\left(-\frac{\sigma_E^2 y}{P_s\lambda_{AE}}\right)\times\frac{(N_R-2)P_J\lambda_{JE}(P_s\lambda_{AE})^{N_R-2}}{(P_J\lambda_{JE}y+P_S\lambda_{AE})^{N_R-1}}dy}_{\Xi 2}. \qquad (51)
\end{aligned}$$

$$\begin{aligned}
\Xi 1 &= \exp\left(-\frac{\sigma_R^2 n\left(2^{R_s}-1\right)}{P_S\lambda_{AR}}\right)\frac{\sigma^2}{P_J\lambda_{JE}}\Psi\left(1, 4-N_R, \frac{\sigma^2\left(n2^{R_s}\lambda_{AE}+\lambda_{AR}\right)}{P_R\lambda_{JE}\lambda_{AR}}\right)\\
\Xi 2 &= \exp\left(-\frac{\sigma_R^2 n\left(2^{R_s}-1\right)}{P_S\lambda_{AR}}\right)(N_R-2)\,\Psi\left(1, 3-N_R, \frac{\sigma^2\left(n2^{R_s}\lambda_{AE}+\lambda_{AR}\right)}{\lambda_{AR}P_J\lambda_{JE}}\right). \qquad (52)
\end{aligned}$$

Then, we can operate some simple mathematical manipulations. $\Xi 1$ and $\Xi 2$ can be derived on the basis of [39, Eq. (9.211.4)] as (52), shown at the bottom of the previous page. Hence, the CDF of the $\gamma_{AR,2}$ can be derived as

$$F_{\gamma_{AR,2}}^{SC-ZFB}\left(R_s\right) = \int_0^\infty \left[1 - \sum_{n=1}^{N_R} \binom{N_R}{n} \left(-1\right)^{n-1} \Xi 1 - \sum_{n=1}^{N_R} \binom{N_R}{n} \left(-1\right)^{n-1} \Xi 2\right] f_G\left(g\right) dg. \quad (53)$$

Now, substituting PDF of averaging over G into (53) and conducting a few simple mathematical calculations, the desired CDF of γ_1^{SC-ZFB} with the SC-ZFB scheme can be obtained.

APPENDIX D
PROOF OF COROLLARY 1

According to MRC scheme, when $\overline{\gamma_{B1}} \to \infty$, the conditional CDF of $\gamma_{AR,1}$ can be approximated as

$$F_{\gamma_{AR,1}}\left(x|G\right) \approx \frac{1}{N_R!}\left(\frac{\sigma_R^2 x}{P_S \lambda_{AR}}\right)^{N_R}. \quad (54)$$

Also, the conditional PDF of $\gamma_{AE,1}$ can be given by

$$f_{\gamma_{AE,1}}\left(y|G\right) = \frac{1}{\overline{\gamma_{E1}}} \exp\left(-\frac{1}{\overline{\gamma_{E1}}} y\right). \quad (55)$$

By substituting (54) and (55) into (46), the asymptotic $F_{\gamma_{AR,1}}\left(R_s|G\right)$ of MRC scheme conditioned on the RV G is given by

$$F_{\gamma_{AR,1}}\left(R_s|G\right) = \frac{1}{N_R!}\left(\frac{\sigma_R^2}{P_S \lambda_{AR}}\right)^{N_R} \times \sum_{q=0}^{N_R} \binom{N_R}{q} \left(2^{R_s}-1\right)^{N_R-q} \left(2^{R_s}\right)^q q! (\overline{\gamma_{E1}})^q. \quad (56)$$

Now, according to RV G, the desired result can be derived as (57), shown at the bottom of this page.

According to MRT scheme, the MRT scheme with HD operation is similar to description process of the Eq. (57) and is not derived here, only the change of parameters, i.e., $\lambda_{AP} \to \lambda_{RP}$, $\lambda_{AR} \to \lambda_{RB}$, $\lambda_{AE} \to \lambda_{RE}$, it can be easily expressed as $F_{\gamma_2^{MRT}}$.

By substituting (57) and $F_{\gamma_2^{MRT}}$ into (24), the high SNR analysis of MRC/MRT scheme is given by (32).

APPENDIX E
PROOF OF COROLLARY 2

According to SC-ZFB scheme, when $\overline{\gamma_{B2}} \to \infty$, the conditional CDF of $\gamma_{AR,2}$ can be approximated as

$$F_{\gamma_{AR,2}}\left(x|G\right) \approx \left(\frac{\sigma_R^2 x}{P_S \lambda_{AR}}\right)^{N_R}. \quad (58)$$

Also, the conditional PDF of $\gamma_{AE,2}$ can be given by

$$f_{\gamma_{AE,2}}\left(y|G\right) = \frac{1}{\overline{\gamma_{E2}}} exp\left(-\frac{y}{\overline{\gamma_{E2}}}\right)\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z} y + \overline{\gamma_{E2}}}\right)^{N_R-2} + exp\left(-\frac{y}{\overline{\gamma_{E2}}}\right)\frac{\left(N_R-2\right)\overline{\gamma_Z}\left(\overline{\gamma_{E2}}\right)^{N_R-2}}{\left(\overline{\gamma_Z} y + \overline{\gamma_{E2}}\right)^{N_R-1}}. \quad (59)$$

Substituting (58) and (59) into (51), the asymptotic $F_{\gamma_{AR,2}}\left(R_s|G\right)$ of SC-ZFB scheme conditioned on the RV G is given by (60), as shown at the bottom of this page.

Now, according to RV G, the desired result can be readily derived as (61), shown at the top of the next page.

$$F_{\gamma_1^{MRC}}\left(R_s\right) = \left(\frac{1}{\overline{\gamma_{B1}}}\right)^{N_R}\left[\left(\frac{1}{N_R!}\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^q q!\left(\overline{\gamma_{E1}}\right)^q\right)\left(1-\exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right) + \left(\frac{1}{N_R!}\left(\frac{1}{\mu}\right)^{N_R}\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^q q!\left(\overline{\gamma_{E1}}\right)^q\right)\lambda_{AP}^{N_R}\Gamma\left(N_R+1, \frac{\mu}{\lambda_{AP}}\right)\right]. \quad (57)$$

$$F_{\gamma_{AR,2}}\left(R_s|G\right) = \left(\frac{\sigma_R^2}{P_S\lambda_{AR}}\right)^{N_R}\underbrace{\frac{1}{\overline{\gamma_{E2}}}\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^q\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^{q+1}\Gamma\left(q+1\right)\Psi\left(q+1, q+4-N_R; \frac{1}{\overline{\gamma_Z}}\right)}_{\Upsilon 1} + \left(\frac{\sigma_R^2}{P_S\lambda_{AR}}\right)^{N_R}\underbrace{\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^q\left(N_R-2\right)\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^q\Gamma\left(q+1\right)\Psi\left(q+1, q+3-N_R; \frac{1}{\overline{\gamma_Z}}\right)}_{\Upsilon 2}. \quad (60)$$

$$\begin{aligned}
&F_{\gamma_1^{SC-ZFB}}(R_s)\\
&= \left(\frac{1}{\overline{\gamma_{B2}}}\right)^{N_R}\left(\underbrace{\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}\frac{1}{\overline{\gamma_{E2}}}\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^{q+1}\Gamma\left(q+1\right)\Psi\left(q+1,q+4-N_R;\frac{1}{\overline{\gamma_Z}}\right)}_{\Lambda_1}\right.\\
&\quad\left.+\underbrace{\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}\left(N_R-2\right)\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^{q}\Gamma\left(q+1\right)\Psi\left(q+1,q+3-N_R;\frac{1}{\overline{\gamma_Z}}\right)}_{\Lambda_2}\right)\left(1-\exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right)\\
&\quad+\left(\underbrace{\frac{1}{\overline{\gamma_{E2}}}\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^{q+1}\Gamma\left(q+1\right)\Psi\left(q+1,q+4-N_R;\frac{1}{\overline{\gamma_Z}}\right)}_{\Lambda 1}\right.\\
&\quad\left.+\underbrace{\sum_{q=0}^{N_R}\binom{N_R}{q}\left(2^{R_s}-1\right)^{N_R-q}\left(2^{R_s}\right)^{q}\left(N_R-2\right)\left(\frac{\overline{\gamma_{E2}}}{\overline{\gamma_Z}}\right)^{q}\Gamma\left(q+1\right)\Psi\left(q+1,q+3-N_R;\frac{1}{\overline{\gamma_Z}}\right)}_{\Lambda 2}\right)\\
&\quad\times\left(\frac{1}{\mu\overline{\gamma_{B2}}}\right)^{N_R}\left(\frac{1}{\lambda_{AP}}\right)^{-N_R}\Gamma\left(N_R+1,\frac{\mu}{\lambda_{AP}}\right).
\end{aligned}\tag{61}$$

Abbreviated as

$$\begin{aligned}
&F_{\gamma_1^{SC-ZFB}}(R_s)\\
&=\left(\frac{1}{\overline{\gamma_{B2}}}\right)^{N_R}\left[\left(\Lambda_1+\Lambda_2\right)\left(1-\exp\left(-\frac{\mu}{\lambda_{AP}}\right)\right)\right.\\
&\quad\left.+\left(\frac{1}{\mu}\right)^{N_R}\left(\Lambda_1+\Lambda_2\right)\left(\frac{1}{\lambda_{AP}}\right)^{-N_R}\Gamma\left(N_R+1,\frac{\mu}{\lambda_{AP}}\right)\right].
\end{aligned}\tag{62}$$

According to MRT scheme, the MRT scheme with HD operation is similar to description process of the Eq. (57), only the change of parameters, i.e., $\lambda_{AP}\rightarrow\lambda_{RP}$, $\lambda_{AR}\rightarrow\lambda_{RB}$, $\lambda_{AE}\rightarrow\lambda_{RE}$, and is not derived here. Substituting (62) and $F_{\gamma_2^{MRT}}$ into (24), the high SNR analysis of SC-ZFB/MRT scheme is given by (34).

APPENDIX F
PROOF OF COROLLARY 3

According to SC-ZFB scheme, the SC-ZFB scheme with FD operation is similar to description process of the Eq. (62) and is not derived here.

According to ZFB scheme, when $\overline{\gamma_{B3}}\rightarrow\infty$, the conditional CDF of $\gamma_{RB,3}$ can be approximated as

$$F_{\gamma_{RB,3}}(y|R_s)\approx\frac{1}{(N_R-2)!}\left(\frac{y}{\overline{\gamma_{B3}}}\right)^{N_R-2}.\tag{63}$$

Because there is no eavesdropping line interference in ZFB scheme, the desired result can be derived as

$$F_{\gamma_2^{ZFB}}(R_s)=\left(\frac{1}{\overline{\gamma_{B3}}}\right)^{N_R-2}\frac{1}{(N_R-2)!}\left(2^{R_s}-1\right)^{N_R-2}.\tag{64}$$

Substituting (62) and (64) into (24), the high SNR analysis of SC-ZFB/ZFB scheme is given by (38).

REFERENCES

[1] Y. Huang, F. Al-Qahtani, Q. Wu, C. Zhong, J. Wang, and H. 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. 3364–3456, Sep. 2014.

[2] H. Lei, "On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-*m* fading channel," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 614–627, Dec. 2017.

[3] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, Apr. 2009.

[4] M. Qin, S. Yang, H. Deng, and M. H. Lee, "Enhancing security of primary user in underlay cognitive radio networks with secondary user selection," *IEEE Access*, vol. 6, pp. 32624–32636, 2018.

[5] N. Nandan, S. Majhi, and H. Wu, "Maximizing secrecy capacity of underlay MIMO-CRN through bi-directional zero-forcing beamforming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5327–5337, Aug. 2018.

[6] J. Zhang, G. Pan, and H.-M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, Jul. 2016.

[7] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure MISOME cognitive radio transmissions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1875–1889, Aug. 2018.

[8] A. Sultana, L. Zhao, and X. Fernando, "Efficient resource allocation in device-to-device communication using cognitive radio technology," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10024–10034, Nov. 2017.

[9] M. Li, W. Liao, X. Chen, J. Sun, X. Huang, and P. Li, "Economic-robust transmission opportunity auction for D2D communications in cognitive mesh assisted cellular networks," *IEEE Trans. Mobile Comput.*, vol. 17, no. 8, pp. 1806–1819, Aug. 2018.

[10] H. Lei, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[11] H. Lei, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10126–10132, Dec. 2016.

[12] L. Wang, H. Yang, J. Long, K. Wu, and J. Chen, "Enabling ultra-dense UAV-aided network with overlapped spectrum sharing: Potential and approaches," *IEEE Netw.*, vol. 32, no. 5, pp. 85–91, Oct. 2018.

[13] G. Sklivanitis, "Airborne cognitive networking: Design, development, and deployment," *IEEE Access*, vol. 6, pp. 47217–47239, 2018.

[14] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.

[15] Y. Song, W. Yang, Z. Xiang, B. Wang, and Y. Cai, "Secure transmission in mmWave NOMA networks with cognitive power allocation," *IEEE Access*, vol. 7, pp. 76104–76119, 2019.

[16] C. Wei, W. Yang, Y. Cai, X. Tang, and T. Yin, "Secrecy outage performance of buffer-aided underlay cognitive relay networks with outdated CSI," in *Proc. IEEE 7th CIC Int. Conf. Commun. China (CIC ICCC)*, Aug. 2018, pp. 168–173.

[17] S. Jia, J. Zhang, H. Zhao, and R. Zhang, "Relay selection for improved security in cognitive relay networks with jamming," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 662–665, Oct. 2017.

[18] M. Li, H. Yin, Y. Huang, Y. Wang, and R. Yu, "Physical layer security in overlay cognitive radio networks with energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11274–11279, Nov. 2018.

[19] H. Yu, Y. Sung, and Y. H. Lee, "Superposition data transmission for cognitive radios: Performance and algorithms," in *Proc. MILCOM IEEE Military Commun. Conf.*, Nov. 2008, pp. 1–6.

[20] J. Kim, J. Kim, J. Lee, and J. P. Choi, "Physical-layer security against smart eavesdroppers: Exploiting full-duplex receivers," *IEEE Access*, vol. 6, pp. 32945–32957, 2018.

[21] J. Moon, H. Lee, C. Song, S. Lee, and I. Lee, "Proactive eavesdropping with full-duplex relay and cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6707–6719, Oct. 2018.

[22] T. Zhang, Y. Huang, Y. Cai, C. Zhong, W. Yang, and G. K. Karagiannidis, "Secure multiantenna cognitive wiretap networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4059–4072, May 2017.

[23] N.-P. Nguyen, C. Kundu, H. Q. Ngo, T. Q. Duong, and B. Canberk, "Secure full-duplex small-cell networks in a spectrum sharing environment," *IEEE Access*, vol. 4, pp. 3087–3099, 2016.

[24] T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[25] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure transmission in cognitive mimo relaying networks with outdated channel state information," *IEEE Access*, vol. 4, pp. 8212–8224, Sep. 2016.

[26] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[27] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 624–632, Apr. 2014.

[28] 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.

[29] 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.

[30] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 780–787, Apr. 2016.

[31] Z. Shang, T. Zhang, Y. Liu, Y. Cai, and W. Yang, "Secrecy performance analysis of cognitive radio networks with full-duplex relaying," in *Proc. IEEE 8th CIC Int. Conf. Commun. China (ICCC)*, Changchun, China, Aug. 2019, pp. 700–705, doi: 10.1109/ICCChina.2019.8855966.

[32] A. Basilevsky, *Applied Matrix Algebra in the Statistical Sciences*, Courier Corporation, 2013.

[33] 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.

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

[35] 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.

[36] 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.

[37] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[38] T. Zhang, Y. Huang, Y. Cai, and W. Yang, "Secure transmission in spectrum sharing relaying networks with multiple antennas," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 824–827, Apr. 2016.

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

[40] 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. (SPAWC)*, Jun. 2012, pp. 429–433.

ZHIHUI SHANG received the M.S. degree from the Zhengzhou University of Light Industry, in 2017. He is currently pursuing the Ph.D. degree with the Institution of Communications Engineering, Army Engineering University of PLA. His research interests include cooperative communications, cognitive radio systems, physical-layer security, and resource scheduling and management.

TAO ZHANG received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011 and 2016, respectively. Since 2017, he has been an Engineer with The Sixty-third Research Institute, National University of Defense Technology, Nanjing. His current research interests include cooperative communications, wireless sensor networks, physical layer security, and cognitive radio systems.

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 micro-electronics engineering and Ph.D. degree in communications and information systems 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.

YONGXIANG LIU received the M.S. degree in communications and information systems from the Nanjing Institute of Communications Engineering, Nanjing, China, in 1999. He is currently a Senior Engineer with The Sixty-third Research Institute, National University of Defense Technology, Nanjing. His research interests include wireless communications, spectrum management, and communication anti-jamming.

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.