Secure Cooperative Spectrum Sharing in Full-Duplex Multi-Antenna Cognitive Radio Networks with Jamming

Zahra Mobini

Abstract

We consider a secure overlay cognitive radio network with an eavesdropper wherein a multi-antenna secondary transmitter performs transmission in primary spectrum, on the condition that it helps primary system to perform secure and reliable transmission via cooperative relaying and jamming. To improve secrecy performance of primary network, we propose full-duplex jammer protocol and zero-forcing based beamforming design, which completely cancels the interferences at the primary and secondary users and simultaneously avoids the leakage of confidential information to eavesdropper. Moreover, we present new expressions for the average secrecy rate and a lower bound for the secrecy outage probability. Furthermore, an asymptotic analysis in the high signal-to-noise ratio regime is carried out to obtain closed-form average secrecy rate. Our analytical findings reveal that by exploiting beamforming and full-duplex at the secondary transmitter secrecy outage probability can be significantly reduced and a diversity order of min $(\mathsf{N_R}-1, \mathsf{N_T}-2)$ can be achieved where $\mathsf{N_R}$ and $\mathsf{N_T}$ are the number of received and transmit antennas at secondary transmitter. Simulation results also demonstrate that as compared to the half-duplex scenario without jamming, the proposed cooperative FD overlay CR scheme with jamming can improve the average secrecy rate up to 224%.

Index Terms

Average secrecy rate, secrecy outage probability, jamming, full-duplex (FD), beamforming.

Z. Mobini is with the Faculty of Engineering, Shahrekord University, Shahrekord 115, Iran (email: z.mobini@sku.ac.ir)

I. Introduction

Cognitive radio (CR) is foreseen as one of the promising technologies of spectrum-constrained fifth generation (5G) wireless networks [1]. The key idea of CR is to allow licensed users, known as primary users (PUs), and unlicensed users, known as secondary users (SUs), coexist and share the same spectrum while the PUs have the higher priorities in using the spectrum [2]. From different possible implementation spectrum sharing strategies, the overlay and underlay methods are the most popular ones. In the underlay approach, the secondary user is allowed to use the spectrum of the primary user when the interference from the secondary user is less than the interference level which the primary user can tolerate. Hence, the transmission power of the secondary user is constrained not to exceed the interference level. In the overlay approach, the secondary user uses the same spectrum concurrently with the primary user while maintaining or improving the transmission of the primary user by applying sophisticated signal processing and coding [3].

However, in practice, there are still many challenges ahead for CR networks, including network coverage and security of the confidential information signals [4], [5]. In particular, due to the open and dynamic characteristics of spectrum sharing CR networks, legitimate users are exposed to multiple internal and/or external malicious threats which make security issues much more emergent and prominent [6]. Among four different phases of cognitive cycle, the sensing (observe) and acting (communication) phases are more important from security view point since they are most prone to attacks. Cognitive networks has special challenges in each cycle for underlay and overlay modes. For example among several, in the underlay mode, to protect the PU from harmful interference, the communication requirements of SU are limited by the regulators. One main goal of malicious attackers is trying to make failure on the CR network by creating a situation not allowed by the regulator which poses more challenge for security of successful implementation of CR in underlay mode compared to its overlay counterpart [7]. As another example, as it will be discussed later in the next section, in the cooperation based overlay CR systems where SUs act as a relay to forward the PUs' information signal, the transmission protocol performs into two transmission phases and eavesdropper can overhear the information signal from two phases. Hence, these transmissions

are more vulnerable to the eavesdropping attack than conventional non-cooperative underlay communications.

To ensure security, wireless physical-layer security methods can be exploited to notably enhance the secrecy rate which is defined as the difference between the instantaneous rate of the legitimate link and that of the wiretap link. If the secrecy rate falls below zero, the eavesdropper can intercept confidential information. To this end some recent efforts were devoted to improving the wireless secrecy rate by using multiple-input multiple-output (MIMO) and beamforming [8]–[12]. The physical layer security of MIMO underlay cognitive radio systems with multiple-antennas SUs, PUs, and eavesdropper were studied in [13] wherein the impact of system parameters, including number of transmit/receive antennas, channel qualities, and fading parameter on the secrecy performance were thoroughly investigated.

Furthermore, cooperative relaying is emerging as a promising mean of improving the reliability, capacity, and security of wireless networks [14], [15]. Particularly, the relay nodes may act as conventional cooperative nodes to help the transmitter to send the information signal, or may act as the jammer by transmitting jamming signal to deteriorate the received signal of the potential eavesdroppers [11], [12], [14]. In [14], two different cooperation strategies, namely relay-jammer and cluster-beamforming, were proposed. In the former, two individual SUs act as a relay and a friendly jammer to enhance the PU's secrecy. In the latter, PU cooperates with a cluster of SUs to improve the secrecy using collaborative beamforming. Secure cooperative communications for PUs in orthogonal frequency-division multiple-access (OFDMA) CR networks in the presence of a set of passive eavesdroppers have been studied in [16]. Instantaneous and ergodic resource allocation problems for the relay-based cooperative CR network to maximize the secrecy rate of the SU subject to the minimum required PU's secrecy rate was studied in [17]. The secrecy performance of dual-hop multi-antenna spectrum sharing relaying systems under the presence of an eavesdropper has been investigated in [8]. The authors in [9] presented a downlink cascaded beamforming scheme to ensure the secure transmission for a two-cell MIMO CR network. Beamforming optimization for the secure primary transmission using the multi-antenna secondary user in a CR network was studied in [10]. In [18] joint secondary user scheduling, power, and time al-

location schemes to maximize the secondary network ergodic rate under the primary network secrecy constraint for cooperative cognitive wireless powered communication network were investigated. A secure CR network with cooperative jamming wherein multiple SUs interfere with multiple eavesdroppers to protect the PU and gain transmission opportunities were investigated in [19], and the problem of optimizing the resource allocation for maximizing the SUs ergodic transmission rate under PU secrecy outage and SUs transmission power constraints was solved.

On the other hand, full-duplex (FD) technique has recently received significant research interest, because of its great potential to double the spectral efficiency of traditional HD relaying by allowing concurrent transmission and reception in the same frequency band [20]. Self-interference (SI) problem due to signal leakage from the output of the transceiver to the input, is considered as one of the major bottleneck in practical implementation of FD. Nevertheless, many effective and practical SI suppression methods such as passive SI suppression, analog and digital baseband cancellation techniques, have been developed today [21]–[23]. Specifically, spatial suppression techniques such as null-space projection [21] and multiple-antenna techniques [24], [25] help us to use FD relays with cooperative relaying and cooperative jamming [26] in secure wireless networks. However, to the best of our knowledge, the performance of the spectrum-sharing overlay CR network with multi-antenna full-duplex relaying and jamming has not been well understood. Recent work in [27] investigated the dual-hop randomize-and-forward (RaF) underlay cognitive wiretap networks over Rayleigh fading channels, in which the RaF relay is considered both as half-duplex and full-duplex operations. The authors in proposed [28] a collaboration interference transmission scheme for cognitive full-duplex wireless wiretap networks by using antenna selection and beamforming technics to improve the performance of the network. The considered CR system models and the proposed beamforming designs in [27], [28] are completely different from our paper. Also, [27] impose a simplifying assumption that the self-interference (SI) is completely nulled out at the full-duplex relay. Moreover, the influence of SI is not taken into consideration in the beamforming design.

Motivated by all above, in this paper we develop a novel cooperative FD multi-antenna

spectrum sharing overlay CR scheme with jamming that achieves high reliability and also high secrecy performance against an eavesdropper. More specifically, we focus on the CR communication scenario with one pair of PUs, one pair of SUs, and one passive eavesdropper wherein the SUs perform transmission in the primary spectrum, on the condition that they help the PUs to perform secure and reliable transmission. FD multi-antenna secondary transmitter (STx) acts as a cooperative jammer and cooperative relay in two transmission stages, respectively. In the stage of cooperative jamming, thanks to FD operation, the STx receives the information signal of the primary network while simultaneously sends a jamming signal to confound the eavesdropper. In the stage of cooperative relaying, STx superposes its own information signal over that of the primary transmitter (PTx), then amplifies and forwarders to both secondary and primary receivers. Furthermore, at each transmission stage, we design beamforming vectors at the STx that benefit the PUs and/or SUs and hurt the eavesdropper. The main contributions of this work are as follows:

- In the first transmission phase, we propose beamforming design at the STx such that the jamming signal to the eavesdropper and hence the security level is maximized, while the SI signal at the STx is completely cancelled. Moreover, in the second transmission phase beamforming vectors are designed such that not only the interfering signals from the STx and PTx at the PRx and SRx are respectively cancelled but also the PTx's signal relayed by STx is completely nulled out at the eavesdropper. Accordingly, the proposed scheme is not interference limited (i.e., there is no interference at the primary and secondary networks from the STx and PTx transmissions, respectively) and does not have any primary information leakage in the relaying path.
- In order to highlight the system behavior and provide important insights into the performance, closed-form expressions for the average secrecy rates and secrecy outage probability lower bound are presented which shows a diversity order of min $(\mathsf{N_R}-1, \mathsf{N_T}-2)$ can be achieved where $\mathsf{N_R}$ and $\mathsf{N_T}$ are the number of received and transmit antennas. These results reveal the effects of key system parameters such as the number of STx antennas and the transmission powers on the system performance.
- Our findings reveal that the proposed cooperative FD multi-antenna overlay CR scheme

with jamming can achieve, up to $224\%(480\%)$ average secrecy gains compared to its HD counterpart without jamming and with conventional beamforming (with ZF beamforming). In addition, the additional transmit antenna significantly enhances the average secrecy performance, while the average secrecy performance is less sensitive to the number of receive antennas at the STx.

Notation: We use bold upper case letters to denote matrices, bold lower case letters to denote vectors. The superscripts $(\cdot)^\dagger$ and $(\cdot)^{-1}$ stand for conjugate transpose, and matrix inverse, respectively; the Euclidean norm of the vector is denoted by $\|\cdot\|$; Pr$(\cdot)$ denotes the probability; $f_X(\cdot)$ and $F_X(\cdot)$ denote the probability density function (pdf), and cumulative distribution function (cdf) of the random variable (RV) X, respectively; and $\mathcal{CN}(0,\sigma^2)$ denotes a zero-mean circularly symmetric complex Gaussian RV X with variance σ^2. We also use the notation $X \sim \chi^2_{2K}$ to denote a chi-square distributed RV X with $2K$ degrees-of-freedom. $\Gamma(a)$ is the Gamma function [29, Eq. (8.310.1)]; $\Gamma(a,x)$ and $\gamma(a,x)$ are upper and lower incomplete Gamma functions, respectively [29, Eq. (8.350)]; $\mathsf{E_i}(x)$ is the exponential integral function [30, Eq. (5.1.2)]; $\Psi(a,b,x)$ denotes Kummer confluent hypergeometric function [29, Eq. (9.210.1)]; ${}_2F_1(a,b;c;z)$ is Gauss' Hypergeometric function [29, Eq. (9.111)]; $\psi(\cdot)$ is the digamma function [29, Eq. (8.360)].

II. System Model

We consider a secure cooperative FD multi-antenna CR network, consisting of a primary transmitter, PTx, a primary receiver, PRx, a secondary transmitter base station, STx, a secondary receiver, SRx, and one eavsedropper, E, as shown in Fig. 1. In this scenario, the PUs allow the SUs to access their spectrum bands on the condition that base station STx has to relay the confidential message of the primary network. Moreover, the STx operates in the FD mode. Accordingly, it receives the information signal from PTx and simultanously sends a jamming signal to combat the eavesdropping and ensures secure information transmission of the primary network. For the FD operation, the STx has two sets of antennas, i.e., $\mathsf{N_R}$ receiveing antennas and $\mathsf{N_T}$ transmitting antennas. Moreover PTx, PRx, SRx, and E all have a single antenna, and operate in an HD mode.

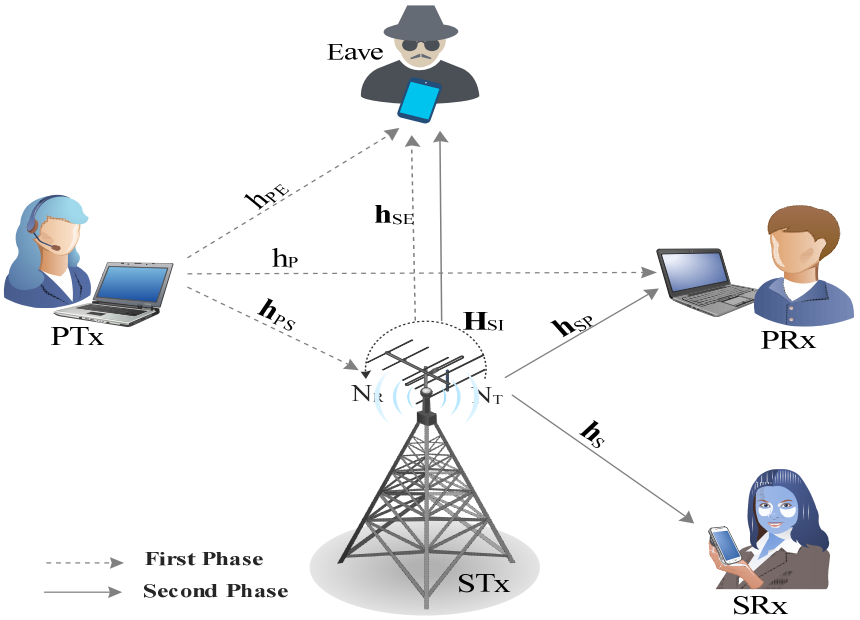

Fig. 1. System model for the proposed cooperative FD multi-antenna CR with jamming.

In order to effectively share the spectrum among the PUs and SUs, the transmission protocol is divided into two phases. In the first phase, the PTx broadcasts its information signal to STx and PRx. At the same time, to avoid the eavesdropper from overhearing the confidential primary network's information, STx sends a jamming signal to mislead the eavesdropper using the transmit beamforming vector $\mathbf{w}_t \in \mathcal{C}^{\mathsf{N_T}\times 1}$. Accordingly, the received signal at the STx can be written as

$$y_{\mathsf{ST},1} = \sqrt{P_{\mathsf{P}}}\mathbf{w}_r^{\dagger}\mathbf{h}_{\mathsf{PS}}x_{\mathsf{P}}[n] + \sqrt{P_{\mathsf{S}}}\mathbf{w}_r^{\dagger}\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t x_{\mathsf{J}}[n] + \mathbf{w}_r^{\dagger}\mathbf{n}_{\mathsf{ST},1}[n], \tag{1}$$

where P_{P} denotes the PTx transmit power, $x_{\mathsf{P}}[n]$ is the PTx information symbol with $\mathbb{E}\left\{x_{\mathsf{P}}[n]x_{\mathsf{P}}^{\dagger}[n]\right\} = 1$, $x_{\mathsf{J}}[n]$ is the jamming signal satisfying $\mathbb{E}\left\{x_{\mathsf{J}}[n]x_{\mathsf{J}}^{\dagger}[n]\right\} = 1$, $\mathbf{w}_r \in \mathcal{C}^{\mathsf{N_R}\times 1}$ is the receive beamformer, $\mathbf{h}_{\mathsf{PS}} \in \mathcal{C}^{\mathsf{N_R}\times 1}$ is the channel between the PTx and STx and its entries follow i.i.d., $\mathcal{CN}(0,\lambda_{ps})$, $\mathbf{H}_{\mathsf{SI}}$ denotes the $\mathsf{N_R}\times\mathsf{N_T}$ residual SI channel which is modeled as identically independent distributed (i.i.d) $\mathcal{CN}(0,\sigma_{RR}^2)$ RVs [21], [31], and $\mathbf{n}_{\mathsf{ST},1}[n]$ denotes the additive white Gaussian noise (AWGN) at the STx with $\mathbb{E}\left\{\mathbf{n}_{\mathsf{ST},1}\mathbf{n}_{\mathsf{ST},1}^{\dagger}\right\} = \sigma_{\mathsf{ST}}^2\mathbf{I}$.

Moreover, the received signals at the PRx during the first phase can be expressed as

$$y_{\mathsf{PR},1} = \sqrt{P_{\mathsf{P}}} h_{\mathsf{P}} x_{\mathsf{P}}[n] + \sqrt{P_{\mathsf{S}}} \mathbf{h}_{\mathsf{SP}}^{\dagger} x_{\mathsf{J}}[n] + n_{\mathsf{PR},1}[n], \tag{2}$$

where $h_{\mathsf{P}} \sim \mathcal{CN}(0,1)$ denotes the channel coefficient of the PTx-PRx link, $\mathbf{h}_{\mathsf{SP}} \in \mathcal{C}^{\mathsf{N_T} \times 1}$ is the channel coefficient of the link between STx and PTx, and $n_{\mathsf{PR},1} \sim \mathcal{CN}(0, \sigma_{\mathsf{PR}}^2)$ is the AWGN at the PTx. On the other hand, the received signal at E in the first phase is given by

$$y_{\mathsf{E},1} = \sqrt{P_{\mathsf{P}}} h_{\mathsf{PE}} x_{\mathsf{P}}[n] + \sqrt{P_{\mathsf{S}}} \mathbf{h}_{\mathsf{SE}}^{\dagger} \mathbf{w}_t x_{\mathsf{J}}[n] + n_{\mathsf{E},1}[n], \tag{3}$$

where $h_{\mathsf{PE}} \sim \mathcal{CN}(0,1)$ and $\mathbf{h}_{\mathsf{SE}} \in \mathcal{C}^{\mathsf{N_T} \times 1}$ denote the channel coefficients of the links between PTx and E and between STx and E, respectively, and $n_{\mathsf{E},1} \sim \mathcal{CN}(0, \sigma_{\mathsf{E}}^2)$ is the AWGN at the E.

During the second phase, the PTx remains silent and the STx multiplies its received signal from the first phase, i.e., $y_{\mathsf{ST},1}$, by the normalization constant G_{S}. Then, it amplifies the resulted normalized signal with the amplification gain G and broadcasts the superposition of this signal and its own non-confidential information signal to the PRx and STx. To this end, STx employs two different transmit beamforming vectors denoted by $\mathbf{w}_{t_{\mathsf{P}}}$ and $\mathbf{w}_{t_{\mathsf{S}}}$ to the normalized information PTx's signal and STx's signal, respectively. We will discuss the design of $\mathbf{w}_{t_{\mathsf{P}}} \in \mathcal{C}^{\mathsf{N_T} \times 1}$ and $\mathbf{w}_{t_{\mathsf{S}}} \in \mathcal{C}^{\mathsf{N_T} \times 1}$ in the next section. Therefore, the received signal at the PRx can be written as

$$\begin{aligned} y_{\mathsf{PR},2} &= G \mathbf{h}_{\mathsf{SP}}^{\dagger} \left(\sqrt{\alpha} \mathbf{w}_{t_{\mathsf{P}}} G_{\mathsf{S}} y_{\mathsf{ST},1}[n] + \sqrt{1-\alpha} \mathbf{w}_{t_{\mathsf{S}}} x_{\mathsf{S}}[n] \right) + n_{\mathsf{PR},2}[n] \\ &= G G_{\mathsf{S}} \sqrt{\alpha P_{\mathsf{P}}} \mathbf{h}_{\mathsf{SP}}^{\dagger} \mathbf{w}_{t_{\mathsf{P}}} \mathbf{w}_r^{\dagger} \mathbf{h}_{\mathsf{PS}} x_{\mathsf{P}}[n] + G G_{\mathsf{S}} \sqrt{\alpha P_{\mathsf{S}}} \mathbf{h}_{\mathsf{SP}}^{\dagger} \mathbf{w}_{t_{\mathsf{P}}} \mathbf{w}_r^{\dagger} \mathbf{H}_{\mathsf{SI}} \mathbf{w}_t x_{\mathsf{J}}[n] \\ &\quad + G \sqrt{(1-\alpha)} \mathbf{h}_{\mathsf{SP}}^{\dagger} \mathbf{w}_{t_{\mathsf{S}}} x_{\mathsf{S}}[n] + G G_{\mathsf{S}} \sqrt{\alpha} \mathbf{h}_{\mathsf{SP}}^{\dagger} \mathbf{w}_{t_{\mathsf{P}}} \mathbf{w}_r^{\dagger} \mathbf{n}_{\mathsf{ST},1}[n] + n_{\mathsf{PR},2}[n], \end{aligned} \tag{4}$$

with

$$G_{\mathsf{S}} = \frac{1}{\sqrt{\mathbf{w}_r^{\dagger} \left(P_{\mathsf{P}} \mathbf{h}_{\mathsf{PS}} \mathbf{h}_{\mathsf{PS}}^{\dagger} + \sigma_{\mathsf{ST}}^2 \mathbf{I} \right) \mathbf{w}_r}}, \tag{5}$$

and

$$G = \sqrt{\frac{P_{\mathsf{S}}}{\mathsf{Trace}\left(\alpha \mathbf{w}_{t_{\mathsf{P}}} \mathbf{w}_{t_{\mathsf{P}}}^{\dagger} + (1-\alpha) \mathbf{w}_{t_{\mathsf{S}}} \mathbf{w}_{t_{\mathsf{S}}}^{\dagger} \right)}}, \tag{6}$$

where $n_{\mathsf{PR},2} \sim \mathcal{CN}(0, \sigma^2_{\mathsf{PR}})$ is the AWGN at PRx in the second phase and α is the power allocation ratio of the PTx's signal to the total STx transmit power P_{S}, $0 \leq \alpha \leq 1$. Moreover, the received signals at the SRx and E in the second phase can be respectively, expressed as

$$\begin{aligned} y_{\mathsf{SR}} &= G\mathbf{h}_{\mathsf{S}}^{\dagger}\left(\sqrt{1-\alpha}\mathbf{w}_{t_{\mathsf{S}}}x_{\mathsf{S}}[n] + \sqrt{\alpha}\mathbf{w}_{t_{\mathsf{P}}}G_{\mathsf{S}}y_{\mathsf{ST},1}[n]\right) + n_{\mathsf{SR}}[n] \\ &= G\sqrt{(1-\alpha)}\mathbf{h}_{\mathsf{S}}^{\dagger}\mathbf{w}_{t_{\mathsf{S}}}x_{\mathsf{S}}[n] + GG_{\mathsf{S}}\sqrt{\alpha P_{\mathsf{P}}}\mathbf{h}_{\mathsf{S}}^{\dagger}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}_r^{\dagger}\mathbf{h}_{\mathsf{PS}}x_{\mathsf{P}}[n] \\ &+ GG_{\mathsf{S}}\sqrt{\alpha P_{\mathsf{S}}}\mathbf{h}_{\mathsf{S}}^{\dagger}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}_r^{\dagger}\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t x_{\mathsf{J}}[n] + GG_{\mathsf{S}}\sqrt{\alpha}\mathbf{h}_{\mathsf{S}}^{\dagger}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}_r^{\dagger}\mathbf{n}_{\mathsf{ST},1}[n] + n_{\mathsf{SR}}[n], \end{aligned} \tag{7}$$

and

$$\begin{aligned} y_{\mathsf{E},2} &= G\mathbf{h}_{\mathsf{SE}}^{\dagger}\left(\sqrt{\alpha}\mathbf{w}_{t_{\mathsf{P}}}G_{\mathsf{S}}y_{\mathsf{ST},1}[n] + \sqrt{1-\alpha}\mathbf{w}_{t_{\mathsf{S}}}x_{\mathsf{S}}[n]\right) + n_{\mathsf{PR},2}[n] \\ &= GG_{\mathsf{S}}\sqrt{\alpha P_{\mathsf{P}}}\mathbf{h}_{\mathsf{SE}}^{\dagger}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}_r^{\dagger}\mathbf{h}_{\mathsf{PS}}x_{\mathsf{P}}[n] + GG_{\mathsf{S}}\sqrt{\alpha P_{\mathsf{S}}}\mathbf{h}_{\mathsf{SE}}^{\dagger}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}_r^{\dagger}\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t x_{\mathsf{J}}[n] \\ &+ G\sqrt{(1-\alpha)}\mathbf{h}_{\mathsf{SE}}^{\dagger}\mathbf{w}_{t_{\mathsf{S}}}x_{\mathsf{S}}[n] + GG_{\mathsf{S}}\sqrt{\alpha}\mathbf{h}_{\mathsf{SE}}^{\dagger}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}_r^{\dagger}\mathbf{n}_{\mathsf{ST},1}[n] + n_{\mathsf{E},2}[n], \end{aligned} \tag{8}$$

where $\mathbf{h}_{\mathsf{S}} \in \mathcal{C}^{\mathsf{N_T}\times 1}$ is the channel coefficients of the links from STx to SRx, $n_{\mathsf{SR}} \sim \mathcal{CN}(0, \sigma^2_{\mathsf{SR}})$ and $n_{\mathsf{E},1} \sim \mathcal{CN}(0, \sigma^2_{\mathsf{E}})$ denote the AWGN at the SRx and E, respectively.

The channel coefficients h_{P} and h_{PE} corresponding to the PTx-PRx link and PTx-E link are assumed to be i.i.d. complex Gaussian RVs with zero-mean and variance Ω_P and Ω_{PE}, respectively. The entries of $\mathbf{h}_{\mathsf{PS}}$, $\mathbf{h}_{\mathsf{SE}}$, $\mathbf{h}_{\mathsf{SP}}$ and $\mathbf{h}_{\mathsf{S}}$ are i.i.d. complex Gaussian RVs with zero-mean and variance Ω_{PS}, Ω_{SE}, Ω_{SP} and Ω_S, respectively.

The PRx uses the maximal-ratio combining (MRC) method to the received signals in (2) and in (4) form the first and second transmission phases, respectively. Further, we assume that the jamming signal in our system is known a priori at the PRx and hence, PRx can eliminate it from the received signal in the first phase, $y_{\mathsf{PR},1}$. It is worth to mention that this is a widely adopted assumption in the physical-layer security with jammer [32]–[34], wherein the jamming signals are produced by using the pseudo-random codes which are not known at the eavesdroppers but available at the legitimate users and hence can be effectively removed. Accordingly, the received signal-to-interference-plus-noise ratio (SINR) at the PRx

can be written as

$$\gamma_{\mathsf{PR}} = \frac{P_{\mathsf{P}}|h_{\mathsf{P}}|^2}{\sigma^2_{\mathsf{PR}}} + \frac{G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{P}}|\mathbf{h}^\dagger_{\mathsf{SP}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{h}_{\mathsf{PS}}|^2}{G^2(1-\alpha)|\mathbf{h}^\dagger_{\mathsf{SP}}\mathbf{w}_{t_{\mathsf{S}}}|^2+G^2G^2_{\mathsf{S}}\alpha\sigma^2_{\mathsf{ST}}|\mathbf{h}^\dagger_{\mathsf{SP}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{n}_{\mathsf{ST},1}|^2+G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{S}}|\mathbf{h}^\dagger_{\mathsf{SP}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma^2_{\mathsf{PR}}}, \tag{9}$$

and the received SINR at the SRx can be written as

$$\gamma_{\mathsf{SR}} = \frac{G^2(1-\alpha)|\mathbf{h}^\dagger_{\mathsf{S}}\mathbf{w}_{t_{\mathsf{S}}}|^2}{G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{P}}|\mathbf{h}^\dagger_{\mathsf{S}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{h}_{\mathsf{PS}}|^2+G^2G^2_{\mathsf{S}}\alpha\sigma^2_{\mathsf{ST}}|\mathbf{h}^\dagger_{\mathsf{S}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{n}_{\mathsf{ST},1}|^2+G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{S}}|\mathbf{h}^\dagger_{\mathsf{S}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma^2_{\mathsf{SR}}} \tag{10}$$

Finally, the received SINR at the E in the first and second transmission phases can be respectively written as

$$\gamma_{\mathsf{E},1} = \frac{P_{\mathsf{P}}|h_{\mathsf{PE}}|^2}{P_{\mathsf{S}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_t|^2+\sigma^2_{\mathsf{E}}}, \tag{11}$$

and

$$\gamma_{\mathsf{E},2} = \frac{G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{P}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{h}_{\mathsf{PS}}|^2}{G^2(1-\alpha)|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{S}}}|^2+G^2G^2_{\mathsf{S}}\alpha\sigma^2_{\mathsf{ST}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{n}_{\mathsf{ST},1}|^2+G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{S}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma^2_{\mathsf{E}}}. \tag{12}$$

Considering the MRC, the overall SINR at E is given by

$$\gamma_{\mathsf{E}} = \frac{P_{\mathsf{P}}|h_{\mathsf{PE}}|^2}{P_{\mathsf{S}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_t|^2+\sigma^2_{\mathsf{E}}} + \frac{G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{P}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{h}_{\mathsf{PS}}|^2}{G^2(1-\alpha)|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{S}}}|^2+G^2G^2_{\mathsf{S}}\alpha\sigma^2_{\mathsf{ST}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{n}_{\mathsf{ST},1}|^2+G^2G^2_{\mathsf{S}}\alpha P_{\mathsf{S}}|\mathbf{h}^\dagger_{\mathsf{SE}}\mathbf{w}_{t_{\mathsf{P}}}\mathbf{w}^\dagger_r\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma^2_{\mathsf{E}}}. \tag{13}$$

III. Beamforming Design

From (9), (10), and (13) we observe that the received SNR/SINRs at the PRx, STx, SRx, and E are the functions of receive and/or transmit beamforming vectors in the first and second transmission phases. Therefore, to have an effective spectral sharing among the PUs and the SUs as well as to cancel the SI effect and further enhance the security of the primary network, in the sequel we present suboptimal receive and transmit beamforming design based on zero forcing (ZF) principle. It is notable that the suboptimal ZF method has known in the literature [24] as a practical and simple scheme which has a lower complexity in comparison with other interference cancelation methods. The significant performance improvements of

the proposed beamforming designs will be shown in Section IV. In the first transmission phase, the primary signal is transmitted from the PTx to the PRx and STx which can be eavesdropped by E. At the same time the FD STx transmits the jamming signal to disrupt the eavesdropping while receiving the PTx's signal. Hence, to maximize the received SINR at STx, we fix the MRC beamforming vector as $\mathbf{w}_r^{\mathsf{MRC}} = \frac{\mathbf{h}_{\mathsf{PS}}}{\|\mathbf{h}_{\mathsf{PS}}\|}$ at the STx. Further, we mitigate the harmful SI by projecting the STx transmit signal to the null space of the received signal at the STx [1] input [24]. Hence, the optimal transmit beamforming vector $\mathbf{w}_t$ which minimizes the received SINR at E is obtained by solving the following problem:

$$\begin{aligned} \max_{\|\mathbf{w}_t\|=1} \quad & |\mathbf{h}_{\mathsf{SE}}^{\dagger}\mathbf{w}_t| \\ \text{s.t.} \quad & \mathbf{h}_{\mathsf{PS}}^{\dagger}\mathbf{H}_{\mathsf{SI}}\mathbf{w}_t = 0. \end{aligned} \tag{14}$$

The optimum transmit beamforming vector $\mathbf{w}_t$ from (14) is derived as [24], $\mathbf{w}_t^{\mathsf{ZF}} = \frac{\mathbf{A}\mathbf{h}_{\mathsf{SE}}}{\|\mathbf{A}\mathbf{h}_{\mathsf{SE}}\|}$, where $\mathbf{A} = \mathbf{I}_{\mathsf{N_T}} - \frac{\mathbf{H}_{\mathsf{SI}}^{\dagger}\mathbf{h}_{\mathsf{PS}}\mathbf{h}_{\mathsf{PS}}^{\dagger}\mathbf{H}_{\mathsf{SI}}}{\|\mathbf{h}_{\mathsf{PS}}^{\dagger}\mathbf{H}_{\mathsf{SI}}\|^2}$.

In the second transmission phase, the STx amplifies the received signal in the first transmission phase and broadcasts the superposition of this signal and its own information signal to the PRx and STx which also can be overheard by E. In this phase, we choose the beamforming vector $\mathbf{w}_{t_{\mathsf{P}}}$ to lie in the null space of the equivalent channel of STx to SRx and STx to E. That is $\mathbf{H}_{\mathsf{S}}\mathbf{w}_{t_{\mathsf{P}}} = \mathbf{0}$, where $\mathbf{H}_{\mathsf{S}} = [\mathbf{h}_{\mathsf{S}}^{\dagger}; \mathbf{h}_{\mathsf{SE}}^{\dagger}]$ is the $2 \times \mathsf{N_T}$ equivalent channel matrix. In this case, the interference caused by the PTx's signal to the SRx is cancelled out. Also, the PTx's information signal relayed by STx is completely nulled out at the E and hence there will be no PUs information leakage to E. Accordingly, the optimal $\mathbf{w}_{t_{\mathsf{P}}}$ which maximizes the received SINR at the PRx can be written as

$$\begin{aligned} \max_{\|\mathbf{w}_{t_{\mathsf{P}}}\|=1} \quad & |\mathbf{h}_{\mathsf{SP}}^{\dagger}\mathbf{w}_{t_{\mathsf{P}}}|, \\ \text{s.t.} \quad & \mathbf{H}_{\mathsf{S}}\mathbf{w}_{t_{\mathsf{P}}} = \mathbf{0}. \end{aligned} \tag{15}$$

Based on projection matrix theory [35], the solution of the optimization problem (15) can be written as $\mathbf{w}_{t_{\mathsf{P}}}^{\mathsf{ZF}} = \frac{\mathbf{C}\mathbf{h}_{\mathsf{SP}}}{\|\mathbf{C}\mathbf{h}_{\mathsf{SP}}\|}$, where $\mathbf{C} = \mathbf{I}_{\mathsf{N_T}} - \mathbf{H}_{\mathsf{S}}^{\dagger}(\mathbf{H}_{\mathsf{S}}\mathbf{H}_{\mathsf{S}}^{\dagger})^{-1}\mathbf{H}_{\mathsf{S}}$.

[1] To employ ZF method, we make the common assumption that the STx has $\mathsf{N_T} > 1$ transmit antennas.

In addition, based on the ZF criterion $\mathbf{w}_{t_\mathsf{S}}$ is designed such that the interference caused by the signals of STx to the PRx is suppressed. Hence, the optimal $\mathbf{w}_{t_\mathsf{S}}$ which maximizes the received SINR at the SRx can be expressed as

$$\begin{aligned} \max_{\|\mathbf{w}_{t_\mathsf{S}}\|=1} \quad & |\mathbf{h}_\mathsf{S}^\dagger \mathbf{w}_{t_\mathsf{S}}|, \\ \text{s.t.} \quad & \mathbf{h}_\mathsf{SP}^\dagger \mathbf{w}_{t_\mathsf{S}} = 0. \end{aligned} \tag{16}$$

The solution of the optimization problem (16) can be derived as $\mathbf{w}_{t_\mathsf{S}}^{\mathsf{ZF}} = \frac{\mathbf{D}\mathbf{h}_\mathsf{SE}}{\|\mathbf{D}\mathbf{h}_\mathsf{SE}\|}$, where $\mathbf{D} = \mathbf{I}_{\mathsf{N_T}} - \mathbf{h}_\mathsf{SP}(\mathbf{h}_\mathsf{SP}^\dagger \mathbf{h}_\mathsf{SP})^{-1}\mathbf{h}_\mathsf{SP}^\dagger$.

By substituting $\mathbf{w}_r^{\mathsf{MRC}}$, $\mathbf{w}_t^{\mathsf{ZF}}$, $\mathbf{w}_{t_\mathsf{P}}^{\mathsf{ZF}}$, and $\mathbf{w}_{t_\mathsf{S}}^{\mathsf{ZF}}$ into (9), after some algebraic manipulation, the received SINR at the PRx can be expressed as

$$\gamma_{\mathsf{PR}} = \gamma_0 + \gamma_R \tag{17}$$

where $\gamma_0 = \rho_p |h_\mathsf{P}|^2$ with $\rho_p = \frac{P_\mathsf{P}}{\sigma^2}$ and

$$\gamma_R = \frac{\gamma_1 \gamma_2}{\gamma_1 + \gamma_2 + 1}, \tag{18}$$

with $\gamma_1 = \rho_p \|\mathbf{h}_\mathsf{PS}\|^2$, and $\gamma_2 = \rho_s \alpha \|\mathbf{C}\mathbf{h}_\mathsf{SP}\|^2$ with $\rho_s = \frac{P_\mathsf{S}}{\sigma^2}$.

In addition, upon substituting $\mathbf{w}_r^{\mathsf{MRC}}$, $\mathbf{w}_t^{\mathsf{ZF}}$, $\mathbf{w}_{t_\mathsf{P}}^{\mathsf{ZF}}$, and $\mathbf{w}_{t_\mathsf{S}}^{\mathsf{ZF}}$ into (10) and (13) and after some algebraic manipulation, the received SNR at SRx and the overheard SINR at the eavesdropper E (from the first transmission phase) can be expressed by

$$\gamma_{\mathsf{SR}} = \frac{P_\mathsf{S}(1-\alpha)}{\sigma^2} \|\mathbf{h}_\mathsf{S}^\dagger \mathbf{w}_{t_\mathsf{S}}\|^2 \tag{19}$$

and

$$\gamma_\mathsf{E} = \frac{P_\mathsf{P} |h_\mathsf{PE}|^2}{P_\mathsf{S} \|\mathbf{h}_\mathsf{SE} \mathbf{w}_t^{\mathsf{ZF}}\|^2 + \sigma^2}, \tag{20}$$

where $\|\mathbf{h}_\mathsf{SE}\mathbf{w}_t^{\mathsf{ZF}}\|^2$ can be further simplified as [36]

$$\|\mathbf{h}_\mathsf{SE}\mathbf{w}_t^{\mathsf{ZF}}\|^2 = \mathbf{h}_\mathsf{SE}^\dagger \Delta^\perp \mathbf{h}_\mathsf{SE} = \hat{\mathbf{h}}_\mathsf{SE}^\dagger \mathsf{diag}(0, 1, \cdots, 1) \hat{\mathbf{h}}_\mathsf{SE} = \|\tilde{\mathbf{h}}_\mathsf{SE}\|^2, \tag{21}$$

where $\hat{\mathbf{h}}_\mathsf{SE} = \mathbf{\Phi}\mathbf{h}_\mathsf{SE}$ with $\mathbf{\Phi}$ is an unitary matrix, and $\tilde{\mathbf{h}}_\mathsf{SE}$ is a $(\mathsf{N_T} - 1) \times 1$ vector, consisting of the $(\mathsf{N_T} - 1)$ last elements of $\hat{\mathbf{h}}_\mathsf{SE}$.

Remark 1. *From* (20) *we observe that the received SNR at the SRx for the proposed overlay CR network with ZF beamforming does not have any interference term due to PTx's*

transmission, and hence will potentially lead to a better performance for the SUs network in compare with conventional overlay CR networks.

It is notable that in the above beamforming designs similar to [37], [38] we assume that the channel state information (CSI) of the STx to E link is available[2]. This assumption is valid for the scenarios wherein the eavesdropper is one of the legitimate users and is trusted on service level and performs true CSI feedback. However, it is data-level malicious and acts as a passive eavesdropper to intercept the primary network confidential information for its own purpose [40]. Further, the assumption of perfect knowledge of the eavesdropper's CSI at the STx enables us to develop fundamental understanding of how jamming and beamforming can enhance security in cooperative FD multi-antenna CR setting by characterizing secrecy rate performance. Nevertheless, for the case when CSI of the E is unavailable, we have the following Remark.

Remark 2. *When the CSI of channels related to E is unavailable, in the first transmission phase* $\mathbf{w}_r$ *and* $\mathbf{w}_t$ *can be chosen based on MRC and random beamforming designs, respectively. In addition, in the second transmission phase, the transmit beamforming vectors* $\mathbf{w}_{t_\mathsf{P}}$ *and* $\mathbf{w}_{t_\mathsf{S}}$ *can be designed using ZF principles. In particular,* $\mathbf{w}_{t_\mathsf{P}}$ *is chosen such that* $|\mathbf{h}_{\mathsf{SP}}^\dagger \mathbf{w}_{t_\mathsf{P}}|$ *is maximized subject to* $|\mathbf{h}_{\mathsf{S}}^\dagger \mathbf{w}_{t_\mathsf{P}}| = 0$*. Similarly,* $\mathbf{w}_{t_\mathsf{S}}$ *is chosen such that* $|\mathbf{h}_{\mathsf{S}}^\dagger \mathbf{w}_{t_\mathsf{S}}|$ *is maximized subject to* $|\mathbf{h}_{\mathsf{SP}}^\dagger \mathbf{w}_{t_\mathsf{S}}| = 0$*. The mathematical analysis and derivations for these beamforming designs are straightforward based on the derived results in this paper and is omitted to avoid clutter.*

IV. Performance Analysis

In this section, we investigate the secrecy performance of the primary network for the proposed cooperative FD multi-antenna CR system with jamming and ZF beamforming in terms of two important secrecy criteria namely average secrecy rate and secrecy outage prob-

[2]When the explicit cooperation between the legitimate nodes and the eavesdropper is not available, perfect knowledge of the eavesdropped's channels is difficult to obtain at the legitimate nodes. For these scenarios the robust secure designs can be applied to ensure achieving the security and robustness [39].

ability. The derived results will highlight the behavior of the system and provide important insights into the performance.

A. Preliminaries

In this subsection, the pdf and the cdf of the SINRs of the main and the eavesdropper's channels are derived, which will facilitate the ensuing secrecy analysis.

Let us derive the cdf of the received SINR at the PRx, γ_{PR}, where $\gamma_{\mathsf{PR}} = \gamma_0 + \gamma_R$. We note that γ_0 is an exponential RV and its cdf is given by

$$F_{\gamma_0}(x) = 1 - e^{-\frac{x}{\bar{\gamma}_0}}, \qquad x \geq 0 \tag{22}$$

where $\bar{\gamma}_0 = \frac{P_{\mathsf{P}}\Omega_P}{\sigma^2}$. Moreover, the cdf of γ_R can be found in [41, Proposition 1].

Although, we have the distribution of γ_0 and γ_R, finding the exact distribution of γ_{PR} seems difficult to obtain, since the distribution of $\gamma_0 + \gamma_R$ is intractable. To overcome this issue, we first apply a widely used tight upper bound to γ_R as $\gamma_R \leq \gamma_{\mathsf{R_L}} = \min(\gamma_1, \gamma_2)$. Therefore, γ_{PR} can be upper bounded as $\gamma_{\mathsf{PR}} \leq \gamma_{\mathsf{PR_L}} = \gamma_0 + \gamma_{\mathsf{R_L}}$. We have the following key result for the cdf of $\gamma_{\mathsf{PR_L}}$.

Lemma 1. *The cdf of $\gamma_{\mathsf{PR_L}}$ is given by*

$$F_{\gamma_{\mathsf{PR_L}}}(x) = \frac{1}{\bar{\gamma}_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})} \sum_{k=0}^{\mathsf{N_T}-2} \Psi(\eta_k, \bar{\gamma}_2) + \frac{1}{\bar{\gamma}_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)} \sum_{k=0}^{\mathsf{N_R}-1} \Psi(\theta_k, \bar{\gamma}_1), \tag{23}$$

where $\eta_k = \mathsf{N_R} + k$, $\theta_k = \mathsf{N_T} + k - 1$, and

$$\Psi(\lambda, \bar{\gamma}) = \frac{\gamma(\lambda, \mu_1 x)}{k!\bar{\gamma}^k \mu_1^\lambda} - e^{-\frac{x}{\bar{\gamma}_0}} \frac{\gamma(\lambda, \mu_2 x)}{k!\bar{\gamma}^k \mu_2^\lambda} \tag{24}$$

with $\mu_1 = \frac{1}{\bar{\gamma}_1} + \frac{1}{\bar{\gamma}_2}$ and $\mu_2 = \frac{1}{\bar{\gamma}_1} + \frac{1}{\bar{\gamma}_2} - \frac{1}{\bar{\gamma}_0}$ with $\bar{\gamma}_1 = \frac{P_{\mathsf{P}}}{\sigma^2}\Omega_{PS}$, and $\bar{\gamma}_2 = \frac{P_{\mathsf{S}}}{\sigma^2}\alpha\Omega_{SP}$.

Moreover, the pdf of $\gamma_{\mathsf{PR_L}}$ is given by

$$f_{\gamma_{\mathsf{PR_L}}}(x) = \frac{e^{-\frac{x}{\bar{\gamma}_0}}}{\bar{\gamma}_0} \left(\frac{1}{\bar{\gamma}_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})} \sum_{k=0}^{\mathsf{N_T}-2} \frac{\gamma(\eta_k, \mu_2 x)}{k!\bar{\gamma}_2^k \mu_2^{\eta_k}} + \frac{1}{\bar{\gamma}_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)} \sum_{k=0}^{\mathsf{N_R}-1} \frac{\gamma(\theta_k, \mu_2 x)}{k!\bar{\gamma}_1^k \mu_2^{\theta_k}} \right). \tag{25}$$

Proof: See Appendix A. ■

We now present the cdf of the received SINR at the E, $F_{\gamma_{\mathsf{E}}}(x)$, in the following lemma.

Lemma 2. *The cdf of the received SINR at the E, γ_{E}, is given by*

$$F_{\gamma_{\mathsf{E}}}(x) = 1 - e^{-\frac{x}{\bar{\gamma}_4}} \left(1 + \frac{\bar{\gamma}_3}{\bar{\gamma}_4} x\right)^{-(\mathsf{N_T}-1)}, \tag{26}$$

where $\bar{\gamma}_3 = \rho_s \Omega_{SE}$ *and* $\bar{\gamma}_4 = \rho_p \Omega_{PE}$. *Moreover, the pdf of* γ_{E} *is given by*

$$f_{\gamma_{\mathsf{E}}}(x) = \left(\frac{\bar{\gamma}_4}{\bar{\gamma}_3}\right)^{\mathsf{N_T}-1} \frac{e^{-\frac{x}{\bar{\gamma}_4}}}{\bar{\gamma}_4} \left(\frac{\bar{\gamma}_4}{\bar{\gamma}_3} + x\right)^{-(\mathsf{N_T}-1)} \left[(\mathsf{N_T}-1)\bar{\gamma}_4 \left(\frac{\bar{\gamma}_4}{\bar{\gamma}_3} + x\right)^{-1} + 1\right]. \tag{27}$$

Proof: See Appendix B. ■

B. Secrecy Rate

To evaluate the security, instantaneous secrecy rate is one of the important secrecy performance criterion defined as [42]

$$C_s = \lfloor C_{\mathsf{P}} - C_{\mathsf{E}} \rfloor^+, \tag{28}$$

where $\lfloor x \rfloor^+ = \max(x, 0)$. Also, C_{P} and C_{E} are the overall rate at the primary network and eavesdropping over the two transmission phases and given by $C_{\mathsf{P}} = \frac{1}{2}\log(1+\gamma_{\mathsf{PR}})$ and $C_{\mathsf{E}} = \frac{1}{2}\log(1+\gamma_{\mathsf{E}})$, respectively. Therefore, PTx can transmit confidential messages to the PRx at a rate C_s to guarantee perfect secrecy. In the delay tolerant transmissions, however, the codeword length is large enough to experience all possible realizations of the channels. As such, average secrecy rate is an appropriate performance criterion which is defined as the instantaneous secrecy rate, C_s, averaged over γ_{PR} and γ_{E} and mathematically can be expressed as [42], [43]

$$\bar{C}_s = \frac{1}{2}\int_0^\infty \int_0^\infty C_s f_{\gamma_{\mathsf{PR}}}(x_1) f_{\gamma_{\mathsf{E}}}(x_2) dx_1 dx_2. \tag{29}$$

The average secrecy rate can be rewritten as [44]

$$\begin{aligned}\bar{C}_s =& \frac{1}{2}\int_0^\infty \left(\int_0^\infty \left[\log\left(\frac{1+x_1}{1+x_2}\right)\right]^+ f_{\gamma_{\mathsf{E}}}(x_2)dx_2\right) f_{\gamma_{\mathsf{PR}}}(x_1)dx_1 \\ \overset{(a)}{=}& \int_0^\infty \left(\int_0^{x_1} \log\left(\frac{1+x_1}{1+x_2}\right) f_{\gamma_{\mathsf{E}}}(x_2)dx_2\right) f_{\gamma_{\mathsf{PR}}}(x_1)dx_1,\end{aligned} \tag{30}$$

where (a) follows from the definition of C_s and the condition $\bar{C}_s \geq 0$, i.e., $\log\left(\frac{1+x_1}{1+x_2}\right) \geq 0$, which implies that $x_2 \leq x_1$.

Using the similar steps as in [45], the average secrecy rate in (30) can be re-expressed as

$$\bar{C}_s = \frac{1}{2\ln(2)} \int_0^\infty \frac{F_{\gamma_{\mathsf{E}}}(x)}{1+x}[1 - F_{\gamma_{\mathsf{PR}}}(x)]dx. \tag{31}$$

From (31) we observe that $\bar{C}_s$ depends on the cdf of γ_{PR} and γ_{E}. Therefore, by substituting (23) and (26) into (31), the exact average secrecy rate can be derived in integral form. We notice that an exact evaluation of $\bar{C}_s$ is tedious, if not impossible, to obtain in closed-form. However, the result can be efficiently calculated numerically using Matlab or Mathematica.

In order to explicitly examine the performance in the high SNR regime, we proceed to derive the asymptotic average secrecy rate. Specifically, in the asymptotic scenario, we assume that both the PTx and STX have the large enough transmit power (i.e., $\rho_p \to \infty$ and $\rho_s \to \infty$)

Proposition 1. *When $\rho_p \to \infty$ and $\rho_s \to \infty$ and assuming that $\frac{\rho_s}{\rho_p} = \kappa$, the asymptotic average secrecy rate of the system is given by*

$$\begin{aligned}\bar{C}_s^{\infty} =& \log_2(a_0\rho_p) + \frac{1}{2\ln(2)}\frac{1}{a_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})}\sum_{k=0}^{\mathsf{N_T}-2}\frac{1}{k!a_2^k}\sum_{n=0}^{\infty}\frac{(-1)^n a_0^{\eta_k+n}\Gamma(\eta_k+n)}{n!b_2^n}\psi(\eta_k+n)\\ &+ \frac{1}{2\ln(2)}\frac{1}{a_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)}\sum_{k=0}^{\mathsf{N_R}-1}\frac{1}{k!a_1^k}\sum_{n=0}^{\infty}\frac{(-1)^n a_0^{\theta_k+n}\Gamma(\theta_k+n)}{n!b_2^n}\psi(\theta_k+n)\\ &+ \frac{1}{2(\mathsf{N_T}-1)\ln(2)}{}_2F_1\left(\mathsf{N_T}-1,1;\mathsf{N_T},1-\frac{a_3}{a_4}\right),\end{aligned} \tag{32}$$

where $a_0 = \Omega_P$, $a_1 = \Omega_{PS}$, $a_2 = \kappa\alpha\Omega_{SP}$, $a_3 = \kappa\Omega_{SE}$, $a_4 = \Omega_{PE}$.

Proof: See Appendix C. ■

We would like to emphasize that our exact expression in (32) is given in closed-form as it involves finite summations of exponentials, Gamma functions, power values, and standard exponential integral functions.

Proposition 1 clearly shows that the average secrecy rate with the proposed beamforming design is independent of the SI strength. Now, to obtain additional insights on the secrecy performance, based on (32), we derive two key performance indicators that determine the average secrecy rate at high SNR, namely the high SNR slope and the high SNR power offset [46]–[48]. The asymptotic average secrecy rate in (32) can be conveniently reexpressed as [47]

$$\bar{C}_s^{\infty} = \mathcal{S}_{\infty}\left(\log_2(\rho_p) - \mathcal{L}_{\infty}\right) + o(1). \tag{33}$$

Here, the two key parameters are $\mathcal{S}_{\infty}$, which denotes the high-SNR slope in bits/s/Hz/(3

dB) given by

$$\mathcal{S}_{\infty} = \lim_{\rho_p \to \infty} \frac{\bar{C}_s^{\infty}}{\log_2(\rho_p)} \tag{34}$$

and $\mathcal{L}_{\infty}$, which represents the zero-order term or high-SNR power offset in 3 dB units given by

$$\mathcal{L}_{\infty} = \lim_{\rho_p \to \infty} \left(\log_2(\rho_p) - \frac{\bar{C}_s^{\infty}}{\mathcal{S}_{\infty}} \right). \tag{35}$$

We have the following key results.

Corollary 3. *The high SNR slope and the high SNR power offset of the proposed beamforming scheme are given by*

$$\mathcal{S}_{\infty} = 1 \tag{36}$$

and

$$\begin{aligned} \mathcal{L}_{\infty} = &- \log_2(a_0) - \frac{1}{2\ln(2)} \frac{1}{a_1^{\mathsf{N_R}} \Gamma(\mathsf{N_R})} \sum_{k=0}^{\mathsf{N_T}-2} \frac{1}{k! a_2^k} \sum_{n=0}^{\infty} \frac{(-1)^n a_0^{\eta_k+n} \Gamma(\eta_k+n)}{n! b_2^n} \psi(\eta_k+n) \\ &- \frac{1}{2\ln(2)} \frac{1}{a_2^{\mathsf{N_T}-1} \Gamma(\mathsf{N_T}-1)} \sum_{k=0}^{\mathsf{N_R}-1} \frac{1}{k! a_1^k} \sum_{n=0}^{\infty} \frac{(-1)^n a_0^{\theta_k+n} \Gamma(\theta_k+n)}{n! b_2^n} \psi(\theta_k+n) - \Xi_2^{\infty}, \end{aligned} \tag{37}$$

Proof: The proof is straightforward using definition of high SNR slope and the high SNR power offset in (34) and (35), respectively, and is thus omitted. ■

From (36), we conclude that the number of receive and transmit antennas at the FD STx and eavesdropper's channel have no impact on the high SNR slope. Moreover, by invoking (37), we find that the high SNR power offset is independent of ρ_p. Furthermore, the contribution of the eavesdropper's channel to $\mathcal{L}_{\infty}$ is characterized by Ξ_2^{∞}. Specifically, Ξ_2^{∞} increases with $\mathsf{N_T}$, and as such the average secrecy capacity increases.

C. Secrecy Outage Probability

The secrecy outage probability is defined as the probability of the achievable secrecy capacity, C_s, being lower than a predetermined secrecy rate, R_s. Mathematically, it can be represented as [42]

$$\begin{aligned} P_{\mathsf{out}} &= \Pr(C_s < R_s) \\ &= \int_0^{\infty} F_{\gamma_{\mathsf{PR}}}(\bar{r}(1+x)-1) f_{\gamma_{\mathsf{E}}}(x) dx, \end{aligned} \tag{38}$$

where $\bar{r} = 2^{2R_s}$. Substituting (23) and (27) into (38), the secrecy outage probability of the primary network can be found. We highlight that although (38) does not seem to admit a closed-form solution, it can be efficiently evaluated numerically. In the sequel, we derive the lower bound of secrecy outage probability

Proposition 2. *The secrecy outage probability of the system with proposed beamforming scheme can be lower bounded as*

$$P_{\mathsf{out}}^{L}(\bar{r}) = \frac{1}{\bar{\gamma}_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})} \sum_{k=0}^{\mathsf{N_T}-2} \frac{1}{k!\bar{\gamma}_2^k} \left(\mathcal{H}(\eta_k, \mu_1, \zeta_1) - \mathcal{H}(\eta_k, \mu_2, \zeta_2)\right) + \frac{1}{\bar{\gamma}_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)} \sum_{k=0}^{\mathsf{N_R}-1} \frac{1}{k!\bar{\gamma}_1^k} \left(\mathcal{H}(\theta_k, \mu_1, \zeta_1) - \mathcal{H}(\theta_k, \mu_2, \zeta_2)\right), \tag{39}$$

where $\zeta_1 = \frac{1}{\bar{\gamma}_4}$, $\zeta_2 = \frac{1}{\bar{\gamma}_4} + \frac{\bar{r}}{\bar{\gamma}_0}$, *and*

$$\mathcal{H}(\lambda, \mu, \zeta) = \frac{1}{\mu^\lambda}\left[1 - \Gamma(\lambda)\sum_{m=0}^{\lambda-1}\left(\bar{r}\mu\frac{\bar{\gamma}_4}{\bar{\gamma}_3}\right)^m\left((\mathsf{N_T}-1)\Psi\left(m+1, m+2-\mathsf{N_T}; \frac{\bar{\gamma}_4}{\bar{\gamma}_3}(\zeta+\bar{r}\mu)\right)\right.\right. + \left.\left.\frac{1}{\bar{\gamma}_3}\Psi\left(m+1, m+3-\mathsf{N_T}; \frac{\bar{\gamma}_4}{\bar{\gamma}_3}(\zeta+\bar{r}\mu)\right)\right)\right]. \tag{40}$$

Proof: See Appendix D. ■

From Proposition 2 we observe that the secrecy outage probability for CR system shows an outage floor at high values of PTx's transmission power. This is expected because with high values of PTx transmit power the overheard signal at eavesdropper from the direct link will be maximal which reduces the secrecy outage performance.

Remark 3. *By inspecting* (39)*, we observe that in the high-SNR regime, assuming that* $\bar{\gamma}_1 \to \infty$, $\bar{\gamma}_2 = \kappa\bar{\gamma}_1$, $\bar{\gamma}_0 = \mu\bar{\gamma}_1$ *when* $\frac{\bar{\gamma}_4}{\bar{\gamma}_3}$ *is fixed, the proposed cooperative FD multi-antenna CR scheme achieves a diversity order of* $\min(\mathsf{N_R}-1, \mathsf{N_T}-2)$.

V. Numerical Results and Discussion

Here, numerical results are presented to demonstrate the performance of the proposed secure cooperative FD multi-antenna CR scheme with jamming and ZF beamforming, which is called FDJ-ZF, in the presence of an eavesdropper, highlight the impact of key system parameters on its performance and also validate the derived analytical expressions. Unless

otherwise stated, the noise variances at E, PRx, and SRx are set to 1, $\alpha = 0.5$, $\Omega_P = 0.25$, $\Omega_P E = 0.5$ $\Omega_{PS} = 0.5$, $\Omega_{SE} = 0.5$, $\Omega_{SP} = 0.5$ and $\Omega_S = 0.5$.

A. Benchmarks

To illustrate the secrecy advantages of our proposed FDJ-ZF scheme, we consider two common cooperative overlay schemes adopted in the literature [3] called HD-ZF and HD-MRC/maximum ratio transmission (MRT) as the benchmarks. In these schemes STx operates in the HD mode and cannot send any jamming signal to E in the first transmission phase due to its HD nature. The HD-ZF and HD-MRC/MRT schemes are outlined as follows. In the HD-ZF scheme during the first time slot, the PTx transmits its signal to the PRx and STx where STx utilizes the MRC linear processing scheme at its receiver side. In the second time slot, the STx superposes its own information signal over that of the PTx, then amplifies and forwards to both SUs and PUs networks with transmit beamforming vectors $\mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}}$ and $\mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}}$, respectively. The transmit weight vectors $\mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}}$ and $\mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}}$ are designed such that the interference due to PTx's signal at the SRx and the interference due to STx's signal at the PRx are mitigated. In particular, according to ZF principles, the transmit weight vector $\mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}}$ is chosen to lie in the orthogonal space of $\mathbf{h}_\mathsf{S}$ such that $\mathbf{h}_\mathsf{S}^\dagger \mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}} = 0$ and $|\mathbf{h}_{\mathsf{SP}}^\dagger \mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}}|$ is maximized. Similarly, $\mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}}$ is chosen in the orthogonal space of $\mathbf{h}_{\mathsf{SP}}$ such that $\mathbf{h}_{\mathsf{SP}}^\dagger \mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}} = 0$ and $|\mathbf{h}_\mathsf{S}^\dagger \mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}}|$ is maximized. The problems of designing the transmit weights, $\mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}}$ and $\mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}}$ at the STx can thus be formulated as

$$\begin{aligned} \max_{\|\mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}}\|=1} \quad & |\mathbf{h}_{\mathsf{SP}}^\dagger \mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}}| \\ \text{s.t.} \quad & \mathbf{h}_\mathsf{S}^\dagger \mathbf{w}_{t_\mathsf{P}}^{\mathsf{HD}} = 0, \end{aligned} \tag{41}$$

and

$$\begin{aligned} \max_{\|\mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}}\|=1} \quad & |\mathbf{h}_\mathsf{S}^\dagger \mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}}| \\ \text{s.t.} \quad & \mathbf{h}_{\mathsf{SP}}^\dagger \mathbf{w}_{t_\mathsf{S}}^{\mathsf{HD}} = 0, \end{aligned} \tag{42}$$

respectively. Using projection matrix theory [35], the weights which satisfy the conditions

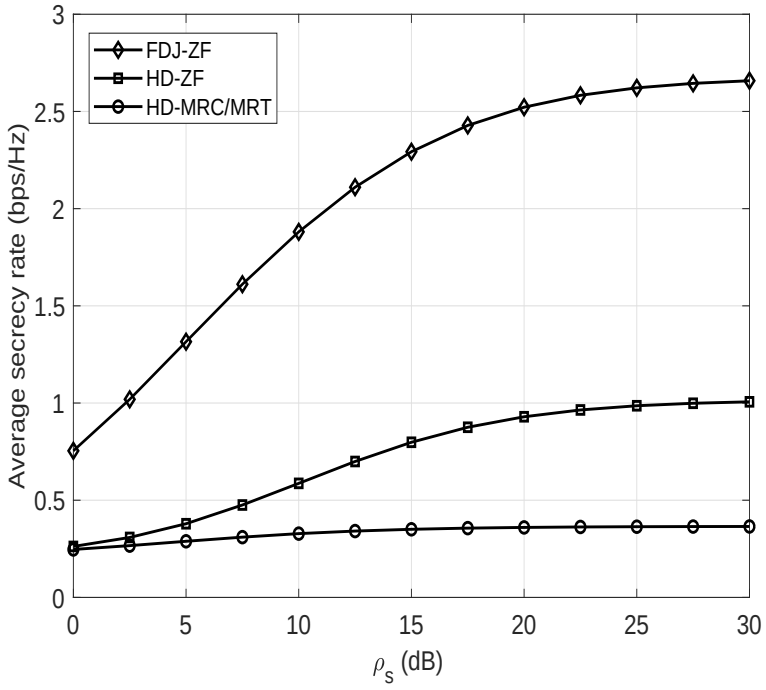

Fig. 2. Average secrecy rate of FDJ-ZF, HD-ZF, and HD-MRC/MRT schemes versus P_{S} ($\mathsf{N_R} = 4, \mathsf{N_T} = 6$, and $P_{\mathsf{P}} = 10$ dB).

in (41) and (42), are given by

$$\mathbf{w}_{t_{\mathsf{P}}}^{\mathsf{HD}} = \frac{\boldsymbol{\Xi}_{\mathsf{P}}^{\perp}\mathbf{h}_{\mathsf{SP}}}{\|\boldsymbol{\Xi}_{\mathsf{P}}^{\perp}\mathbf{h}_{\mathsf{SP}}\|} \quad \text{and} \quad \mathbf{w}_{t_{\mathsf{S}}}^{\mathsf{HD}} = \frac{\boldsymbol{\Xi}_{\mathsf{S}}^{\perp}\mathbf{h}_{\mathsf{S}}}{\|\boldsymbol{\Xi}_{\mathsf{S}}^{\perp}\mathbf{h}_{\mathsf{S}}\|}, \tag{43}$$

where $\boldsymbol{\Xi}_{\mathsf{P}}^{\perp} = \mathbf{I}_{NT} - \mathbf{h}_{\mathsf{S}}(\mathbf{h}_{\mathsf{S}}^{\dagger}\mathbf{h}_{\mathsf{S}})^{-1}\mathbf{h}_{\mathsf{S}}^{\dagger}$ and $\boldsymbol{\Xi}_{\mathsf{S}}^{\perp} = \mathbf{I}_{NT} - \mathbf{h}_{\mathsf{SP}}(\mathbf{h}_{\mathsf{SP}}^{\dagger}\mathbf{h}_{\mathsf{SP}})^{-1}\mathbf{h}_{\mathsf{SP}}^{\dagger}$. Note that in contrast to the FDJ-ZF scheme, the relayed PTx's information signal can be overheard by the E in the HD-ZF scheme.

The transmission protocol in the HD-MRC/MRT scheme is the same as in the HD-ZF scheme, except that the transmit beamforming vectors in the second transmission phase are designed based on the MRT scheme, i.e., $\mathbf{w}_{t_{\mathsf{P}}}^{\mathsf{HD}} = \frac{\mathbf{h}_{\mathsf{SP}}}{\|\mathbf{h}_{\mathsf{SP}}\|}$ and $\mathbf{w}_{t_{\mathsf{S}}}^{\mathsf{HD}} = \frac{\mathbf{h}_{\mathsf{S}}}{\|\mathbf{h}_{\mathsf{S}}\|}$. It is notable that MRT transmit beamforming in the second transmission phase does not allow interference-free transmission for the primary and secondary systems since cancelling the interferences from the PTx's and STx's transmissions on the PRx and SRx, respectively, are not possible.

Fig. 2 illustrates the average secrecy rate of FDJ-ZF, HD-ZF, and HD-MRC/MRT schemes versus STx transmission power, ρ_s, for $\mathsf{N_R} = 4, \mathsf{N_T} = 6$, and $\rho_p = 10$ dB. We observe that the proposed FDJ-ZF outperforms all other schemes for all values of the ρ_s. For example, at

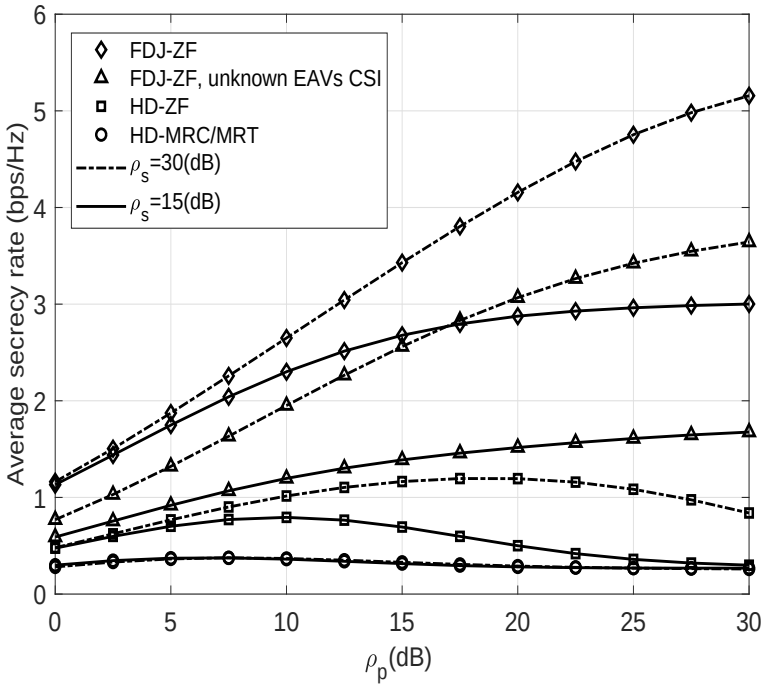

Fig. 3. Average secrecy rate of FDJ-ZF, HD-ZF, and HD-MRC/MRT schemes versus P_{P} for two values of P_{S} ($\mathsf{N_R} = 4$ and $\mathsf{N_T} = 6$).

$\rho_s = 10$ dB, FDJ-HD can achieve 224% and 480% average secrecy gains compared to HD-ZF and HD-MRC/MRT schemes, respectively. This is intuitive since in the proposed FDJ-ZF the jamming signal transmitted from the FD STx degrades the quality of the eavesdropping channel which accordingly enhances the secrecy rate. Also, FDJ-ZF completely avoids information leakage to E in the second phase. In addition, the average secrecy rate of FDJ-ZF, HD-ZFJ and HD-MRC/MRT schemes converge to finite limits at high ρ_s. More specifically, with high ρ_s, the FDJ-ZF almost attains the average secrecy rate of 2.6 bps/Hz, which is about 1.6 times than that of HD-ZF and 6 times than that of HD-MRC/MRT.

Fig. 3 compares the average secrecy rate of FDJ-ZF, HD-ZF, and HD-MRC/MRT schemes versus ρ_p for two different values of ρ_s with $\mathsf{N_R} = 4$ and $\mathsf{N_T} = 6$. The average secrecy rate of the FDJ-ZF scheme improves with increasing ρ_p. In the HD-ZF and HD-MRC/MRT schemes however, the secrecy rate first increases with the ρ_p, and then decreases when ρ_p increases beyond a certain value. The main reason is that large transmission power ρ_p increases the received SINR at the PRx and STx which accordingly enhances the secrecy rate. However,

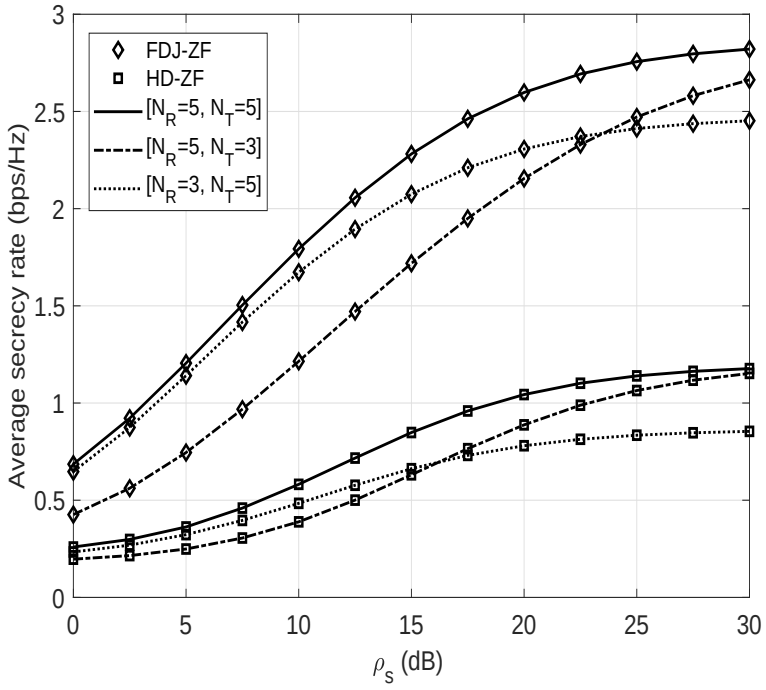

Fig. 4. Average secrecy rate of FDJ-ZF, HD-ZF, and HD-MRC/MRT schemes versus P_{S} for different antenna configurations at STx ($P_{\mathrm{P}} = 10$ dB).

it also improves the achievable rate of the eavesdropper's channel (in contrast to FDJ-ZF, in the HD-ZF and HD-MRC/MRT schemes, the STx cannnot send a jamming signal to interfere with the reception of E due to its HD operation). Morover, we see that the performance gaps between the FDJ-ZF and two other HD schemes increases with increasing ρ_s. This is expected because increasing ρ_s improves the received SINR at the PRx from relaying path and also increases the jamming signal strength which accordingly enhances the secrecy rate. Fig. 3 also shows that the analytical result for average secrecy rate tightly matches simulation result. In Fig. 3 we also present the result of FDJ-ZF for the case when CSI of the eavesdropper is unavailable and beamforming vectors are designed based on Remark 2. It is observed that with unknown eavesdroppe's CSI the PU secrecy performance is degraded compared with the perfect case. But, FDJ-ZF, unknowen eavesdropper's CSI scheme still significantly outperforms HD-ZF and HD-MRC/MRT schemes with perfect CSI.

Fig. 4 shows the average secrecy rate of FDJ-ZF, HD-ZF, and HD-MRC/MRT schemes with different antenna configurations. For the FDJ-ZF scheme, we see that the additional

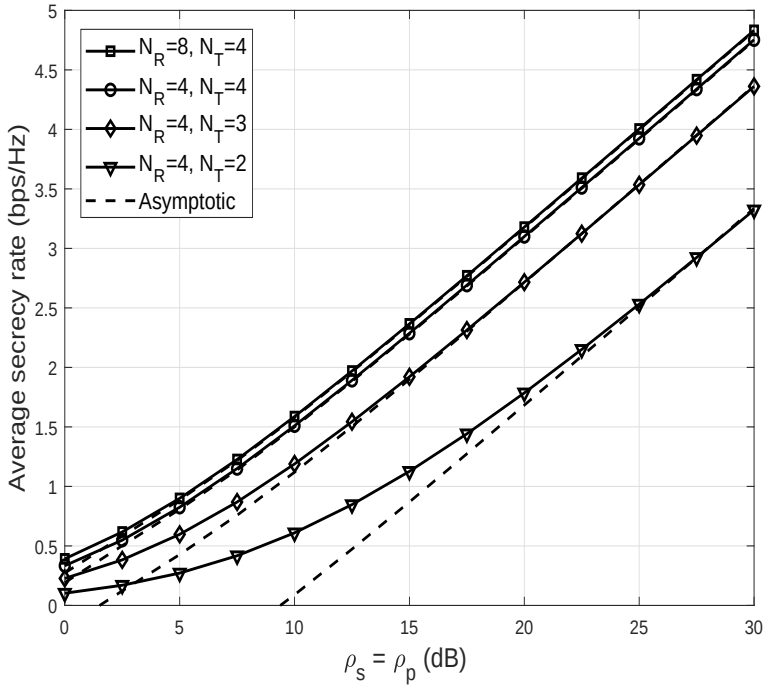

Fig. 5. Average secrecy rate of FDJ-ZF scheme versus $\rho_s = \rho_p$ for different antenna configurations.

transmit antenna could improve the achievable rate at the PTx and degrade the quality of the eavesdropping channel and hence enhance the average secrecy performance. However, the average secrecy performance of FDJ-ZF is less sensitive to $\mathsf{N_R}$ specially for low to average values of ρ_s, since the quality of STx to PRx channel is more critical for the average secrecy rate performance than the PTx to STx channel. The above observations show the existence of different design choices when performance-complexity tradeoff is of interest. Therefore, the beamforming design and antenna configurations have to be carefully decided.

Fig. 5 presents the average secrecy rate of the FDJ-ZF with different antenna configurations and for $\rho_s = \rho_p$. The exact and asymptotic average secrecy rate results are obtained from (31) and Proposition 1, respectively. It is evident that the exact curves closely match with Monte Carlo simulations and the asymptotic curves well approximate the exact ones in the medium-to-high SNR regime. We observe that the curves for different transmit/receive antennas have the same secrecy slope, which is presented by (36). Fig. 5 also shows that the average secrecy rate increases with increasing the number of transmit antennas $\mathsf{N_T}$. This result is in accordance with (37) shows that Ξ_2^{∞} increases with $\mathsf{N_T}$.

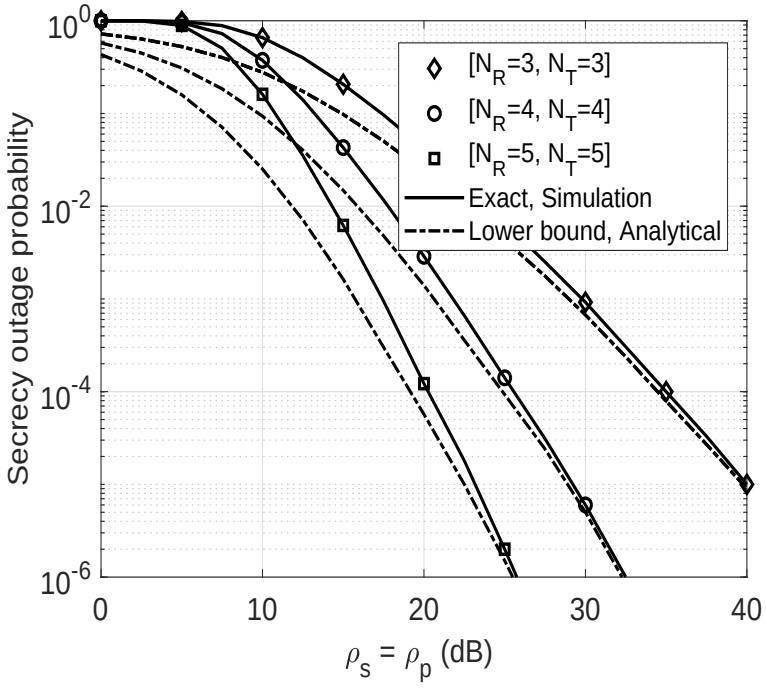

Fig. 6. Secrecy outage probability of FDJ-ZF scheme versus $\rho_s = \rho_p$ for different antenna configurations at STx ($R_s = 1$ bps/Hz).

Fig. 6 depicts the secrecy outage probability of FDJ-ZF scheme for different antenna configurations where the lower bound results are based on Proposition 2. It is observe that the analytical approximations in Proposition 2 is sufficiently accurate, and become almost exact in the high-SNR regime. We see that our proposed scheme achieves a diversity order of $\min(\mathsf{N_R}-1, \mathsf{N_T}-2)$, which is consistent with the analytical results derived in the previous section.

VI. Conclusions

In this paper, we have investigated the secrecy-enhancing design for cooperative overlay CR network in the presence of eavesdropper and with the help of FD multi-antenna STx who acts as the relay and jammer. To improve the average secrecy of the primary network, deal with the SI, and prevent information leakage from the relaying path we have proposed FD cooperative jamming and ZF beamforming. The ZF beamforming design also enables cancelling PTx and STx interferences to the SRx and PRx, respectively. Closed-form expression for the average secrecy rate, lower bound on the secrecy outage performance along with

high-SNR approximations were also presented. We showed that ZF beamforming and FD jamming significantly improve the average secrecy rate and secrecy outage performance of the primary network. However, secrecy performance gains of the proposed scheme over HD counterparts and conventional beamforming design highly depend on the system parameters including the number of antennas at the STx and the transmission powers.

As for future work, it would be interesting to extend these results to multiple eavesdroppers scenario with both non-colluding and colluding eavesdroppers as well as to investigate the secrecy performance of various transmission schemes with multi-antenna SUs/PUs and robust secure beamforming.

APPENDIX A
PROOF OF LEMMA 1

By using the order statistics, the cdf of $\gamma_{\mathsf{PR_L}}$ is expressed as

$$\begin{aligned} F_{\gamma_{\mathsf{PR_L}}}(x) &= \Pr(\gamma_0 + \gamma_{\mathsf{R_L}} \leq x) \\ &= \int_0^x F_{\gamma_0}(x-y) f_{\gamma_{\mathsf{R_L}}}(y) dy. \end{aligned} \tag{44}$$

Therefore, we need to derive the pdf of $\gamma_{\mathsf{R_L}}$. We will start by finding the cdf of $\gamma_{\mathsf{R_L}}$, which by invoking the order statics, can be written as

$$F_{\gamma_{\mathsf{R_L}}}(x) = F_{\gamma_1}(x) + F_{\gamma_2}(x) - F_{\gamma_1}(x) F_{\gamma_2}(x). \tag{45}$$

It can be observed that $\gamma_1 \sim \chi^2_{2\mathsf{N_R}}$, with cdf given by

$$F_{\gamma_1}(x) = 1 - \frac{\Gamma\left(\mathsf{N_R}, \frac{x}{\bar{\gamma}_1}\right)}{\Gamma(\mathsf{N_R})}. \tag{46}$$

Moreover, according to [36], $\gamma_2 \sim \chi^2_{2(\mathsf{N_T}-1)}$ with its cdf given by

$$F_{\gamma_2}(x) = 1 - \frac{\Gamma\left(\mathsf{N_T}-1, \frac{x}{\bar{\gamma}_2}\right)}{\Gamma(\mathsf{N_T}-1)}. \tag{47}$$

Therefore, by substituting (46) and (47) into (45), the cdf of $\gamma_{\mathsf{R_L}}$ can be expressed as

$$F_{\gamma_{\mathsf{R_L}}}(x) = 1 - \frac{\Gamma\left(\mathsf{N_R}, \frac{x}{\bar{\gamma}_1}\right)}{\Gamma(\mathsf{N_R})} \frac{\Gamma\left(\mathsf{N_T}-1, \frac{x}{\bar{\gamma}_2}\right)}{\Gamma(\mathsf{N_T}-1)}. \tag{48}$$

By taking the derivative of $F_{\gamma_{\mathsf{R_L}}}(x)$ with respect to x, the pdf of $\gamma_{\mathsf{R_L}}$ is given by

$$f_{\gamma_{\mathsf{R_L}}}(x) = \frac{x^{\mathsf{N_R}-1}e^{-\frac{x}{\bar{\gamma}_1}}}{\bar{\gamma}_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})\Gamma(\mathsf{N_T}-1)}\Gamma\left(\mathsf{N_T}-1, \frac{x}{\bar{\gamma}_2}\right) + \frac{x^{\mathsf{N_T}-2}e^{-\frac{x}{\bar{\gamma}_2}}}{\bar{\gamma}_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)\Gamma(\mathsf{N_R})}\Gamma\left(\mathsf{N_R}, \frac{x}{\bar{\gamma}_1}\right), \tag{49}$$

where we have used [29, Eq. (8.356.4)]. Now by substituting (22) and (49) into (44) and applying the series expansion of $\Gamma(a,x)$ [29, Eq. (8.352.4)] we get

$$F_{\gamma_{\mathsf{PR_L}}}(x) = \frac{1}{\bar{\gamma}_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})}\sum_{k=0}^{\mathsf{N_T}-2}\frac{1}{k!\bar{\gamma}_2^k}\int_0^x y^{\mathsf{N_R}+k-1}(1-e^{-\frac{x-y}{\bar{\gamma}_0}})e^{-\mu_1 y}dy + \frac{1}{\bar{\gamma}_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)}\sum_{k=0}^{\mathsf{N_R}-1}\frac{1}{k!\bar{\gamma}_1^k}\int_0^x y^{\mathsf{N_T}+k-2}(1-e^{-\frac{x-y}{\bar{\gamma}_0}})e^{-\mu_1 y}dy. \tag{50}$$

To this end, by using the integral identity [29, Eq. (3.351.1)], the desired result in (23) is obtained. Furthermore, by takeing derivative with respect to x, after some simple mathematical manipulation the pdf of $\gamma_{\mathsf{PR_L}}$ is obtained as (25).

APPENDIX B
PROOF OF LEMMA 2

Let us define $X = \frac{P_{\mathsf{P}}}{\sigma^2}|h_{\mathsf{PE}}|^2$ and $Y = \frac{P_{\mathsf{S}}}{\sigma^2}\|\tilde{\mathbf{h}}_{\mathsf{SE}}\|^2$ in (20). It can be readily observed that X is an exponential RV with cdf given by

$$F_X(x) = 1 - e^{-\frac{x}{\bar{\gamma}_4}}, x \geq 0. \tag{51}$$

Furthermore, according to [36], $\|\tilde{\mathbf{h}}_{\mathsf{SE}}\|^2 \sim \chi^2_{2(\mathsf{N_T}-1)}$ with pdf given by

$$f_Y(y) = \frac{y^{\mathsf{N_T}-2}}{\Gamma(\mathsf{N_T}-1)\bar{\gamma}_3^{\mathsf{N_T}-1}}e^{-\frac{y}{\bar{\gamma}_3}}, y \geq 0. \tag{52}$$

By utilizing the order statistics, the cdf of γ_{E} is given by

$$F_{\gamma_{\mathsf{E}}}(z) = \Pr\left(\frac{X}{Y+1} \leq z\right) = \int_0^\infty F_X(z(y+1))f_Y(y)dy. \tag{53}$$

By substituting (51) and (52) into (53), and then applying the integral identity [29, Eq. (3.351.3)], the desired result in (26) is obtained. Moreover, by taking derivative of (26) with respect to z the pdf of γ_{E} can be obtained as (27).

APPENDIX C
PROOF OF PROPOSITION 1

We notice that the average secrecy rate in (31) can be re-expressed as

$$\begin{aligned}\bar{C}_s &= \frac{1}{2\ln(2)}\int_0^{\infty}\left(\int_0^{x_1}\frac{1-\chi_{\gamma_{\mathsf{E}}}(x_2)}{1+x_2}dx_2\right)f_{\gamma_{\mathsf{PR_L}}}(x_1)dx_1 \\ &= \frac{1}{2\ln(2)}\underbrace{\int_0^{\infty}\ln(1+x)f_{\gamma_{\mathsf{PR_L}}}(x_1)dx_1}_{\Xi_1} + \frac{1}{2\ln(2)}\underbrace{\int_0^{\infty}\int_0^{x_1}\frac{\chi_{\gamma_{\mathsf{E}}}(x_2)}{1+x_2}f_{\gamma_{\mathsf{PR_L}}}(x_1)dx_2dx_1}_{\Xi_2}, \quad (54)\end{aligned}$$

In the high SNR regime with $\rho_p \to \infty$ and $\rho_s \to \infty$ we have $\ln(1+x) \approx \ln(x)$. Therefore, Ξ_1 can be approximated as

$$\Xi_1^{\infty} = \frac{1}{2\ln(2)}\int_0^{\infty}\ln(x)f_{\gamma_{\mathsf{PR_L}}}(x)dx, \quad (55)$$

By substituting (25) into (55), we have

$$\begin{aligned}\Xi_1^{\infty} &= \frac{1}{2\ln(2)}\frac{1}{a_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})}\sum_{k=0}^{\mathsf{N_T}-2}\frac{b_2^{\eta_k}}{k!a_2^k}\sum_{n=0}^{\infty}\frac{(-1)^n}{n!(\eta_k+n)}\int_0^{\infty}\frac{e^{-\frac{x}{a_0\rho}}}{a_0\rho}\left(\frac{x}{b_2\rho}\right)^{\eta_k+n}\ln x dx \\ &+ \frac{1}{2\ln(2)}\frac{1}{a_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)}\sum_{k=0}^{\mathsf{N_R}-1}\frac{b_2^{\theta_k}}{k!a_1^k}\sum_{n=0}^{\infty}\frac{(-1)^n}{n!(\theta_k+n)}\int_0^{\infty}\frac{e^{-\frac{x}{a_0\rho}}}{a_0\rho}\left(\frac{x}{b_2\rho}\right)^{\theta_k+n}\ln x dx, \quad (56)\end{aligned}$$

where we have used the series expression of $\gamma(\alpha,x) = \sum_{n=0}^{\infty}\frac{(-1)^n x^{\alpha+n}}{n!(\alpha+n)}$ [29, Eq. (8.354.1)]. By applying [29, Eq. (4.352.1)], and perform some algebraic manipulations, Ξ_1 is derived as

$$\begin{aligned}\Xi_1^{\infty} &= \log_2(a_0\rho) + \frac{1}{2\ln(2)}\frac{1}{a_1^{\mathsf{N_R}}\Gamma(\mathsf{N_R})}\sum_{k=0}^{\mathsf{N_T}-2}\frac{1}{k!a_2^k}\sum_{n=0}^{\infty}\frac{(-1)^n a_0^{\eta_k+n}\Gamma(\eta_k+n)}{n!b_2^n}\psi(\eta_k+n) \\ &+ \frac{1}{2\ln(2)}\frac{1}{a_2^{\mathsf{N_T}-1}\Gamma(\mathsf{N_T}-1)}\sum_{k=0}^{\mathsf{N_R}-1}\frac{1}{k!a_1^k}\sum_{n=0}^{\infty}\frac{(-1)^n a_0^{\theta_k+n}\Gamma(\theta_k+n)}{n!b_2^n}\psi(\theta_k+n). \quad (57)\end{aligned}$$

We now turn our attention to derive Ξ_2 In order to derive the asymptotic expression of Ξ_2, we change the order of integration in (54) and rewrite Ξ_2 as [44]

$$\Xi_2 = \int_0^{\infty}\frac{[1-F_{\gamma_{\mathsf{E}}}(x_2)]}{1+x_2}[1-F_{\gamma_{\mathsf{PR_L}}}(x_2)]dx_2. \quad (58)$$

By applying the Taylor series expansion $\gamma(\alpha,x) = \sum_{j=0}^{k}(-1)^j x^{\alpha+j}/j!(\alpha+j) + o(x^k)$ and $e^x = \sum_{j=0}^{k} x^j/j! + o(x^k)$ in (23), we observe that $F_{\gamma_{\mathsf{PR_L}}}(x_2) \approx 0$ when $\bar{\gamma}_1 \to \infty$ and $\bar{\gamma}_2 \to \infty$ [44]. Therefore, the asymptotic expression for Ξ_2 can be derived as

$$\Xi_2^{\infty} = \int_0^{\infty}\frac{1-F_{\gamma_{\mathsf{E}}}(x_2)}{1+x_2}dx_2. \quad (59)$$

At high SNR regime the received SINR at E in (20) can be approximated as

$$\gamma_{\mathsf{E}} \approx \frac{\rho_P |h_{\mathsf{PE}}|^2}{\rho_S \|\mathbf{h}_{\mathsf{SE}} \mathbf{w}_t^{\mathsf{ZF}}\|^2}. \tag{60}$$

Accordingly, $F_{\gamma_{\mathsf{E}}}(x)$ can be obtained as

$$F_{\gamma_{\mathsf{E}}}(x) = 1 - \left(1 + \frac{a_3}{a_4} x\right)^{-(\mathsf{N_T}-1)}. \tag{61}$$

Therefore, by substituting (61) into (59) and then by applying [29, Eq. (3.197.1)], Ξ_2 can be approximated as

$$\Xi_2^{\infty} = \frac{1}{\mathsf{N_T}-1} {}_2F_1\left(\mathsf{N_T}-1, 1; \mathsf{N_T}, 1 - \frac{a_3}{a_4}\right). \tag{62}$$

By invoking (54), (57), and (62), we derive the asymptotic average secrecy rate as (32)

APPENDIX D
PROOF OF PROPOSITION 2

By adopting the proposed approach in [49], the secrecy outage probability of the system can be lower bounded as

$$P_{\mathsf{out}}(\bar{r}) \geq P_{\mathsf{out}}^{L}(\bar{r}) = \int_0^{\infty} F_{\gamma_{\mathsf{PR}}}(\bar{r}x) f_{\gamma_{\mathsf{E}}}(x) dx. \tag{63}$$

Now by substituting (23) and (27) into (63), the lower bound of secrecy outage probability can be expressed as

$$\begin{aligned} P_{\mathsf{out}}^{L}(\bar{r}) =& \frac{1}{\bar{\gamma}_1^{\mathsf{N_R}} \Gamma(\mathsf{N_R})} \sum_{k=0}^{\mathsf{N_T}-2} \frac{1}{k! \bar{\gamma}_2^k} \left(\mathcal{H}(\eta_k, \mu_1, \zeta_1) - \mathcal{H}(\eta_k, \mu_2, \zeta_2)\right) \\ &+ \frac{1}{\bar{\gamma}_2^{\mathsf{N_T}-1} \Gamma(\mathsf{N_T}-1)} \sum_{k=0}^{\mathsf{N_R}-1} \frac{1}{k! \bar{\gamma}_1^k} \left(\mathcal{H}(\theta_k, \mu_1, \zeta_1) - \mathcal{H}(\theta_k, \mu_2, \zeta_2)\right), \end{aligned} \tag{64}$$

where

$$\mathcal{H}(\lambda, \mu, \zeta) = \frac{1}{\mu^{\lambda}} \left(\frac{\bar{\gamma}_4}{\bar{\gamma}_3}\right)^{\mathsf{N_T}-1} \int_0^{\infty} \gamma(\lambda, \bar{r}\mu x) \left(\frac{(\mathsf{N_T}-1) e^{-\zeta x}}{\left(\frac{\bar{\gamma}_4}{\bar{\gamma}_3} + x\right)^{\mathsf{N_T}}} + \frac{e^{-\zeta x}}{\bar{\gamma}_4 \left(\frac{\bar{\gamma}_4}{\bar{\gamma}_3} + x\right)^{\mathsf{N_T}-1}} \right) dx. \tag{65}$$

Applying the series expansion of $\gamma(a, x)$ [29, Eq. (8.354.1)] and then utilizing the integral identity [29, Eq. (9.211.4)], to solve the resultant integrals, we derive the exact lower bound on the secrecy outage probability as in (39).

REFERENCES

[1] L. Zhang, M. Xiao, G. Wu, M. Alam, Y. Liang, and S. Li, "A survey of advanced techniques for spectrum sharing in 5G networks," *IEEE Wireless Commun. Mag.*, vol. 24, no. 5, pp. 44–51, Oct. 2017.

[2] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, 2008.

[3] R. Manna, R. H. Y. Louie, Y. Li, and B. Vucetic, "Cooperative spectrum sharing in cognitive radio networks with multiple antennas," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5509–5522, Nov. 2011.

[4] Q. Li and D. Xu, "Minimizing secrecy outage probability for primary users in cognitive radio networks," *AEU-International Journal of Electronics and Communications*, vol. 83, pp. 353–358, 2018.

[5] X. L. Y. Zou and Y. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, pp. 2222–2236, Nov. 2014.

[6] 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, 2015.

[7] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[8] 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, 2016.

[9] N. Nandan, S. Majhi, and H. Wu, "Secure beamforming for MIMO-NOMA-based cognitive radio network," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1708–1711, 2018.

[10] B. Chen, Y. Chen, Y. Chen, Y. Cao, Z. Ding, N. Zhao, and X. Wang, "Secure primary transmission assisted by a secondary full-duplex NOMA relay," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7214–7219, 2019.

[11] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 621–634, Mar. 2019.

[12] Z. Mobini, "Secrecy performance of non-orthogonal multiple access cognitive untrusted relaying with friendly jamming," *AEU - International Journal of Electronics and Communications*, vol. 118, pp. 153–156, 2020.

[13] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "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.

[14] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, 2013.

[15] Z. Mobini and M. Khabbazian, "Asymptotic gain analysis of cooperative broadcast in linear wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 485–497, 2016.

[16] M. R. Abedi, N. Mokari, M. R. Javan, and H. Yanikomeroglu, "Secure communication in OFDMA-based cognitive radio networks: An incentivized secondary network coexistence approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1171–1185, 2017.

[17] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, 2014.

[18] D. Xu and Q. Li, "Resource allocation for secure communications in cooperative cognitive wireless powered communication networks," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2431–2442, Sept. 2019.

[19] ——, "Resource allocation for cognitive radio with primary user secrecy outage constraint," *IEEE Syst. J.*, vol. 12, no. 1, pp. 893–904, Mar. 2018.

[20] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full-duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.

[21] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, pp. 5983–5993, Dec. 2011.

[22] C. Psomas, M. Mohammadi, I. Krikidis, and H. A. Suraweera, "Impact of directionality on interference mitigation in full-duplex cellular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 487–502, Jan. 2017.

[23] Z. Mobini, M. Mohammadi, B. K. Chalise, H. A. Suraweera, and Z. Ding, "Beamforming design and performance analysis of full-duplex cooperative NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 18, pp. 3295–3311, June 2019.

[24] H. A. Suraweera, I. Krikidis, G. Zheng, C. Yuen, and P. J. Smith, "Low-complexity end-to-end performance optimization in MIMO full-duplex relay systems," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 913–927, Feb. 2014.

[25] H. Q. Ngo, H. A. Suraweera, M. Matthaiou, and E. G. Larsson, "Multipair full-duplex relaying with massive arrays and linear processing," *IEEE J. Sel. Areas Commun.*, vol. 32, pp. 1721–1737, June 2014.

[26] F. Jafarian, Z. Mobini, and M. Mohammadi, "Secure cooperative network with multi-antenna full-duplex receiver," *IEEE Systems Journal*, vol. 13, pp. 2786–2794, Sept. 2019.

[27] Z. Shang, T. Zhang, Y. Cai, Y. Liu, and W. Yang, "Secure spectrum-sharing wiretap networks with full-duplex relaying," *IEEE Access*, vol. 7, pp. 181 610–181 625, 2019.

[28] M. Li, Y. Huang, H. Yin, Y. Wang, and C. Cai, "Improving the security and spectrum efficiency in overlay cognitive full-duplex wireless networks," *IEEE Access*, vol. 7, pp. 68 359–68 372, 2019.

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

[30] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables.*, 9th ed. New York: Dover, 1970.

[31] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 4296–4307, Dec. 2012.

[32] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, 2012.

[33] H. Zhang, H. Xing, J. Cheng, A. Nallanathan, and V. C. M. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Trans. Ind. Informat.*, vol. 12, no. 5, pp. 1714–1725, 2016.

[34] A. Kuhestani, A. Mohammadi, and P. L. Yeoh, "Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer," *IEEE Trans. Commun.*, vol. 66, no. 6, pp. 2671–2684, 2018.

[35] R. A. Horn and C. A. Johnson, *Matrix Analysis*. 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[36] M. Mohammadi, B. K. Chalise, H. A. Suraweera, C. Zhong, G. Zheng, and I. Krikidis, "Throughput analysis and

optimization of wireless-powered multiple antenna full-duplex relay systems," *IEEE Trans. Commun.*, vol. 64, pp. 1769–1785, Apr. 2016.

[37] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct. 2016.

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

[39] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, 2012.

[40] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

[41] G. Zhu, C. Zhong, H. A. Suraweera, Z. Zhang, and C. Yuen, "Outage probability of dual-hop multiple antenna AF systems with linear processing in the presence of co-channel interference," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2308–2321, Apr. 2014.

[42] M. R. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[43] 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.

[44] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[45] K. P. Peppas, N. C. Sagias, and A. Maras, "Physical layer security for multiple-antenna systems: A unified approach," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 314–328, Jan. 2016.

[46] A. Lozano, A. M. Tulino, and S. Verdu, "High-SNR power offset in multiantenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134–4151, Dec. 2005.

[47] S. Jin, M. R. McKay, C. Zhong, and K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

[48] H. Lei, D. Wang, K. Park, I. S. Ansari, J. Jiang, G. Pan, and M. Alouini, "Safeguarding UAV IoT communication systems against randomly located eavesdroppers," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1230–1244, Feb. 2020.

[49] 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," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, Sept. 2016.