Beamforming with Artificial Noise for Secure MISOME Cognitive Radio Transmissions

Azzam Al-nahari, Giovanni Geraci, *Member, IEEE*, Mukarram Al-jamali, Mohamed H. Ahmed, *Senior Member, IEEE*, and Nan Yang, *Member, IEEE*

Abstract—In this paper, we consider multiple-input single-output multi-eavesdropper (MISOME) cognitive radio networks (CRNs), where a secondary user (SU) aims to transmit confidential information to a legitimate SU receiver (SU-RX) in the presence of a primary user (PU) and a multi-antenna passive eavesdropper in fast fading environments. For this system setting, we study beamforming with artificial noise (AN) for the SU to achieve confidential communications. We consider designing an AN-assisted optimal beamforming scheme, denoted cognitive beamforming (CB), that maximizes the ergodic secrecy rate. Moreover, we propose two suboptimal beamforming schemes, namely, scaled beamforming (SB) and projected beamforming (PB). We develop an analytical framework to assess the performance of the proposed schemes in a unified manner. First, we analyze the achievable ergodic secrecy rate of the three schemes. Second, we derive the optimal power allocation for the information and AN signals that maximize the achievable ergodic secrecy rate in the large-antenna regime. Third, we study the performance of the three schemes in terms of the secrecy outage probability. Using numerical simulations, we validate our analytical results and show that CB achieves the best performance among the three proposed schemes. In addition, we provide insights into the effect of various system parameters on the secrecy performance. In particular, we show that the interference threshold at the PU plays an important role in the beamforming design.

Index Terms—Cognitive radio, artificial noise, physical layer security, ergodic secrecy rate, secrecy outage probability.

I. INTRODUCTION

The explosive growth in demand for ultra-high wireless data rates has led to increasing requirements for more spectrum. Cognitive radio networks (CRNs) are one of the most promising technologies that aim to address the spectrum scarcity. In CRNs, an unlicensed user, denoted secondary user (SU) can access the spectrum and concurrently transmit on the same frequency bands allocated for a licensed primary user (PU), as long as the interference power at the PU does not exceed a certain limit [1]. Not only are CRNs expected to increase spectrum reuse, but they are also required to guarantee the confidentiality of communications. Such a task is especially critical due to the open nature of CRNs. Physical layer security is regarded as a new paradigm to secure transmissions

while overcoming the vulnerabilities of traditional higher-layer cryptography [2]–[5]. To improve the physical layer security of wireless transmissions, several techniques were proposed, leveraging multiple-input-multiple-output (MIMO) systems [6]–[10] and cooperative relays [11], [12].

The role of physical layer security in CRNs has been attracting growing attention. The secrecy capacity of CRNs with external eavesdroppers was studied in [13]. In [14] and [15], the authors followed a numerical approach to obtain the secrecy capacity of the secondary system assuming perfect and imperfect channel state information (CSI) of the eavesdropper, respectively. In [16], multiuser scheduling was proposed for improving physical layer security in CRNs. In [17], the impact of the presence of a passive eavesdropper on the secondary network was investigated with antenna selection at the receiver side. Beamforming with artificial noise (AN) is a well-known and effective method to ensure secrecy when considering passive eavesdroppers [18]–[20]. However, as opposed to beamforming with AN in conventional networks, the following two aspects should be considered in CRNs: (i) beamforming design should take into account the affordable interference power at the PU, such that the quality of service (QoS) requirements at the PU are satisfied; and (ii) the CSI of both SU and PU should be accounted for at the transmitter in the beamforming design. Secure transmission in a multiple-input single-output (MISO) CRN was studied in [21] with the objective of maximizing the PU throughput via beamforming and AN. In [22], beamforming was proposed to maximize the power of the AN while maintaining a SU target rate.

Unlike the aforementioned works, we consider designing an AN-assisted optimal beamforming scheme, denoted *cognitive beamforming*, for secure transmissions in MISOME-CRNs with passive eavesdropping in fast fading environments. Furthermore, we also propose two suboptimal beamforming schemes, namely *scaled beamforming* and *projected beamforming*. In particular, the main differences between our work and the one in [21] can be outlined as follows: (i) while [21] evaluated the secrecy throughput in a slow fading environment, we focus on a fast fading environment and adopt the ergodic secrecy rate as the main performance metric; (ii) while [21] considered cooperative jamming with the objective of maximizing the secrecy throughput of the primary network, the objective of our work is to optimize the ergodic secrecy rate of the SU; and (iii) while [21] considered a null-steering beamforming scheme, we propose cognitive beamforming to maximize the ergodic secrecy rate of the SU. Another key feature of our work is that unlike previous work in [14]–[16], [21], [22], which adopted a computationally complex numerical approach, we obtain insightful asymptotic closed-

A. Al-nahari is with the Department of Electrical Engineering, Ibb University, Yemen (e-mail: azzamyn@gmail.com).

G. Geraci is with Nokia Bell Labs, Dublin, Ireland (e-mail: dr.giovanni.geraci@gmail.com).

M. Al-jamali is with University of Science and Technology, Yemen. (e-mail: mukarramja@gmail.com).

M. H. Ahmed is with the Faculty of Engineering and Applied Science, Memorial University of Newfoundland, Canada (e-mail: mhahmed@mun.ca).

N. Yang is with the Research School of Engineering, Australian National University, Canberra, ACT2601, Australia (e-mail: nan.yang@anu.edu.au).

form expressions. Such expressions shed light on the impact of different parameters on the secrecy performance achieved by beamforming with AN in MISOME-CRNs.

In this paper, we consider the secure transmission for a SU pair over the fast fading channel environments, where the SU transmitter (SU-TX) is transmitting confidential information to the SU receiver (SU-RX), in the presence of a passive eavesdropper. The QoS of the PU is satisfied by ensuring that the received interference power at the PU not to exceed a threshold I . We investigate the scenario where only the statistical CSI of the eavesdropper is known at the SU-TX. We consider designing beamforming for the information signal and AN for providing protection against eavesdropping. Our objective is to maximize the achievable ergodic secrecy rate of the secondary transmission by optimizing the beamforming vector of the information signal and the power allocation between the information and jamming signals. Two power constraints are imposed in the considered setting: (i) a transmit power budget at the SU-TX, and (ii) a maximum affordable interference power at the PU. The main contributions of this paper are summarized as follows

- 1) We propose an AN-assisted optimal cognitive beamforming (CB) scheme. The beamforming vector of the information signal is designed such that it maximizes the achievable ergodic secrecy rate, while the AN is transmitted along with the information signal to guarantee secure transmission. We derive exact expression for the achievable ergodic secrecy rate of this scheme.
- 2) We derive new closed-form expressions for two suboptimal beamforming schemes with AN; the two schemes are defined as follows: (i) scaled beamforming (SB), where the beamforming vector of the information signal is chosen as a function of the SU channel, and the transmitted power is adjusted such that the interference at the PU is guaranteed not to exceed a threshold I ; and (ii) projected beamforming (PB), where the beamforming vector is designed such that the received interference power at the PU is completely removed.
- 3) We carry out large system analysis when the number of SU transmit antennas goes to infinity. The optimal power allocation between the information and AN signals that maximizes the achievable ergodic secrecy rate of the three schemes is derived. The obtained asymptotic expressions give insights on the effect of different system parameters, such as I and the number of antennas at the SU, on the beamforming design.
- 4) We derive new closed-form expressions for the secrecy outage probability with the three proposed beamforming schemes, and investigate the effect of the various system parameters on the secrecy outage performance.

The remainder of this paper is organized as follows. In Section II, the system and channel models are introduced. In Section III, the proposed beamforming schemes are presented and analysed in terms of the achievable ergodic secrecy rate. The secrecy outage probability analysis is presented in Section IV. Finally, Section V gives the concluding remarks.

Notations: We define $[x]^+ \triangleq \max(0, x)$ and $\hat{\mathbf{h}} \triangleq \frac{\mathbf{h}}{\|\mathbf{h}\|}$, where $\|\cdot\|$ denotes Euclidean norm. We denote by $\mathbf{h}^T$ and $\mathbf{h}^\dagger$ the transpose and conjugate transpose of $\mathbf{h}$, respectively. $\mathbf{I}_N$

Fig. 1. Illustration of a MISOME cognitive radio network.

and $\mathbf{0}_N$ denote the $N \times N$ identity matrix and the all-zero column vector of length N , respectively. $\mathbf{x} \sim \mathcal{CN}(\mathbf{0}_N, \mathbf{\Sigma})$ indicates that $\mathbf{x} \in \mathbb{C}^{N \times 1}$ is a circularly symmetric complex Gaussian vector with zero-mean and covariance matrix $\mathbf{\Sigma}$. $X \sim \text{Gamma}(\alpha, \beta)$ indicates that X is Gamma distributed with parameters α and β . $Y \sim \exp(\lambda)$ indicates that Y is exponentially distributed with parameter λ . $\underline{X}$ and $\overline{X}$ denote lower and upper bounds on X , respectively.

II. SYSTEM AND CHANNEL MODELS

We consider a MISOME-CRN as shown in Fig. 1, which consists of: a SU-TX, a single-antenna SU-RX, an eavesdropping receiver (ED-RX), and a single-antenna PU receiver (PU-RX). The SU-TX and the ED-RX are assumed to be equipped with N_t and N_e antennas, respectively. We assume that the CSI of the eavesdropper is unknown for all nodes in the network. The channel vector $\mathbf{h}_s \in \mathbb{C}^{N_t \times 1}$ represents the channel fading vector from the SU-TX to SU-RX, $\mathbf{h}_p \in \mathbb{C}^{N_t \times 1}$ is the channel fading vector from the SU-TX to PU-RX, and $\mathbf{H}_e \in \mathbb{C}^{N_e \times N_t}$ is the channel fading matrix from the SU-TX to ED-RX. $\mathbf{h}_s \sim \mathcal{CN}(\mathbf{0}_{N_t}, \sigma_s^2 \mathbf{I}_{N_t})$ and $\mathbf{h}_p \sim \mathcal{CN}(\mathbf{0}_{N_t}, \sigma_p^2 \mathbf{I}_{N_t})$. Moreover, the elements of $\mathbf{H}_e$ are independent complex Gaussian random variables each with zero mean and variance σ_e^2 .

In this paper, we have assumed that downlink CSI for both the PU-RX and SU-RX, $\mathbf{h}_s$ and $\mathbf{h}_p$, is available at the SU-TX, which is commonplace in the literature [14]–[16], [21], [22]. In practice, in time-division duplexing (TDD) systems, downlink channels can be estimated through uplink signaling thanks to channel reciprocity. This makes the training time proportional to the number of receive antennas, and it is assumed in our paper. On the other hand, a frequency-division duplexing (FDD) system relies on channel feedback. Moreover, it requires a considerably longer training time, proportional to the number of transmit antennas, and is therefore less suitable for multi-user systems with a large transmit array [23]. In our case, under a TDD assumption, the SU-TX may simply obtain the SU-RX CSI through a pilot signal transmitted by the SU-RX. Regarding the PU-RX CSI, if coordination is in place, the SU-TX may receive a pilot signal sent by PU-RX to its serving PU-TX, and use it for channel estimation. If such coordination is not in place, the SU-TX may acquire the CSI through a learning process, as proposed in [24], or it may periodically obtain the channel subspace occupied by the PU-RX through a channel covariance estimation. During the channel covariance estimation procedure, the SU-TX remains silent, and it thus

receive signals periodically transmitted by the PU-RX, which is an active device. The CSI, in the form of the channel subspace occupied by the PU-RX, can then be obtained by averaging over multiple symbol intervals [25]–[27], and it is sufficient for the purposes of our beamforming design.

The SU-TX transmits a confidential signal s to the SU-RX with $\mathbb{E}[|s|^2] = 1$. Moreover, the SU-TX uses $N_t - 2$ antennas for transmitting AN vector $\mathbf{z} = [z_1 \ z_2 \ \dots \ z_{N_t-2}]^T \sim \mathcal{CN}(\mathbf{0}_{N_t-2}, \mathbf{I}_{N_t-2})$. Therefore, in this system model, $N_t > 2$. The transmitted signal at the SU-TX is given by

$$\mathbf{x} = \sqrt{p_b} \mathbf{w}_b s + \sqrt{q_b} \mathbf{W} \mathbf{z} = \sqrt{p_b} \mathbf{w}_b s + \sqrt{q_b} \sum_{i=1}^{N_t-2} \mathbf{w}_i z_i, \quad (1)$$

where p_b and q_b are the transmitted power of the information and jamming signals, respectively; $\mathbf{b} \in \{\text{SB}, \text{PB}, \text{CB}\}$ denotes the beamforming scheme. The beamforming vector of the information signal $\mathbf{w}_b \in \mathbb{C}^{N_t \times 1}$ is normalized such that $\|\mathbf{w}_b\| = 1$. $\mathbf{W} = [\mathbf{w}_1 \ \mathbf{w}_2 \ \dots \ \mathbf{w}_{N_t-2}] \in \mathbb{C}^{N_t \times (N_t-2)}$ is the precoding matrix of the jamming signal $\mathbf{z}$; the column vectors of $\mathbf{W}$ are normalized such that $\|\mathbf{w}_i\| = 1, \forall i$. In this paper, we design the precoding matrix $\mathbf{W}$ such that the AN is completely nulled out, i.e., suppressed, at the SU-RX and PU-RX. We design the AN to lie in the null space of the channels of the legitimate receivers for two reasons: (i) the AN is intended to degrade the eavesdropping channels, but not the legitimate channels, and (ii) the use of null-space-based AN entails simplified design and better analytical tractability, allowing to derive more insightful closed-form expressions. We note that the same approach is commonly used in the physical layer security literature, and examples can be found in [18]–[20], [28], and references therein¹. Therefore, the matrix $\mathbf{W}$ is designed such that its columns are the orthonormal basis of the null space of both $\mathbf{h}_s^\dagger$ and $\mathbf{h}_p^\dagger$, i.e., $\mathbf{h}_s^\dagger \mathbf{W} = \mathbf{0}_{1 \times (N_t-2)}^T$ and $\mathbf{h}_p^\dagger \mathbf{W} = \mathbf{0}_{1 \times (N_t-2)}^T$. Hence, the columns of $\mathbf{W}$ and $\hat{\mathbf{h}}_s$ constitute an orthonormal set. Similarly, the columns of $\mathbf{W}$ and $\hat{\mathbf{h}}_p$ constitute an orthonormal set. In other words, $[\hat{\mathbf{h}}_s \ \mathbf{W}]$ and $[\hat{\mathbf{h}}_p \ \mathbf{W}]$ are unitary matrices. This also illustrates why only $N_t - 2$ antennas are used for AN transmission. We also assume that $N_t > N_e$, because the eavesdropper cannot eliminate the AN term in (1) with this condition [19].

Let P denotes the total transmit power budget and $0 < \phi_b < 1$ be the fraction of the power devoted to the information signal². Hence, p_b and q_b can be bounded as

$$p_b \leq \phi_b P, \quad (2)$$

$$q_b \leq \frac{(1 - \phi_b)P}{N_t - 2}. \quad (3)$$

Therefore, the received signal at the SU-RX is given as

¹A more general assumption would be to let a portion of the AN to lie in the direction of the main channel of the SU, as studied in [29]. However, this may result in an increased design and analysis complexity, and yield to limited gains [29]. Within the scope of this paper, we denote as optimal beamformer a secrecy-rate-maximizing beamformer where the AN is constrained to lie in the null space of the legitimate channels.

²In this paper, we have assumed zero noise at the ED-RX to ensure security. As a result, when $\phi_b = 1$, no AN is transmitted, and hence, an infinite rate at the eavesdropper (i.e., zero secrecy rate) is achieved. Therefore, we considered the power allocation factor in the range $0 < \phi_b < 1$.

$$y_s = \sqrt{p_b} \mathbf{h}_s^\dagger \mathbf{w}_b s + n_s, \quad (4)$$

where $n_s \sim \mathcal{CN}(0, 1)$ represents the additive white Gaussian noise (AWGN) at SU-RX. Similarly, the received signals at the ED-RX and PU-RX are given by

$$\mathbf{y}_e = \sqrt{p_b} \mathbf{H}_e \mathbf{w}_b s + \sqrt{q_b} \sum_{i=1}^{N_t-2} \mathbf{H}_e \mathbf{w}_i z_i + \mathbf{n}_e, \quad (5)$$

$$y_p = \sqrt{p_b} \mathbf{h}_p^\dagger \mathbf{w}_b s + n_p, \quad (6)$$

where $n_p \in \mathcal{CN}(0, 1)$ and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}_{N_e}, \mathbf{I}_{N_e})$. As the noise at the eavesdropper side is unknown, and in order to ensure security, the eavesdropper's noise at the ED-RX is assumed equal to zero, i.e., $\mathbf{n}_e \rightarrow \mathbf{0}_{N_e}$ [19], [30], [31]; this assumption gives an upper bound on the secrecy capacity of the eavesdropper's link. As a result, the secrecy performance is not affected by the location of the ED-RX relative to the SU-TX. Moreover, without loss of generality, we assume that the channels of PU and SU have unit variances³.

III. ACHIEVABLE ERGODIC SECRECY RATE ANALYSIS

In this section, we propose an optimal beamforming scheme that maximizes the achievable ergodic secrecy rate of MISOME-CRNs. Moreover, two sub-optimal beamforming schemes are proposed. The achievable ergodic secrecy rate of the different schemes is derived. This performance measure is more suitable for fast fading channels, which allows for capacity-achieving channel codes. As mentioned before, the precoding matrix $\mathbf{W}$ is designed for all schemes such that the AN signal is completely nulled out at the SU-RX and PU-RX. On the other hand, we aim to design the beamforming vector $\mathbf{w}_b$ for each scheme. Moreover, p_b and q_b are allocated taking into account the constraints given in (2)–(3). The optimal power allocation for the information and AN signals that maximizes the ergodic secrecy rate is also derived.

A. Preliminaries

For the eavesdropper to perform optimal detection that maximizes her SNR γ_e^b , the eavesdropper is assumed to be aware of $\mathbf{H}_e \mathbf{w}_b$ and the correlation matrix $q_b \mathbf{W}^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{W}$ of the AN signal [32]. As a result, the SNRs at the SU-RX and ED-RX are given as

$$\gamma_s^b = p_b |\mathbf{h}_s^\dagger \mathbf{w}_b|^2, \quad (7)$$

$$\gamma_e^b = \frac{p_b}{q_b} \mathbf{w}_b^\dagger \mathbf{H}_e^\dagger (\mathbf{W}^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{W})^{-1} \mathbf{H}_e \mathbf{w}_b. \quad (8)$$

An ergodic secrecy capacity C_{sec}^b is lower bounded by the achievable ergodic secrecy rate R_{sec}^b as follows [19], [30]

$$C_{sec}^b \geq R_{sec}^b = [C_s^b - C_e^b]^+, \quad (9)$$

³Considering these parameters in the analysis is straightforward but leads to more cumbersome and less insightful equations. However, due to zero-noise assumption at the ED-RX, the SNR of the eavesdropper is independent of σ_e^2 and P . Therefore, considering different locations for the SU-RX relative to the ED-RX can be investigated by changing the value of P .

where $C_s^b = E[\log_2(1 + \gamma_s^b)]$ and $C_e^b = E[\log_2(1 + \gamma_e^b)]$ represent the ergodic rate of the source-destination and source-eavesdropper links, respectively. The following two propositions summarize some useful distributions.

Proposition 1. Given the transmitted power p_b and q_b , if the matrix $[\mathbf{w}_b \mathbf{W}]$ is unitary, the CDF and PDF of γ_e^b , defined in (8), are respectively given as

$$F_{\gamma_e^b}(\gamma) = 1 - \sum_{n=0}^{N_e-1} \frac{\binom{N_t-2}{n} q_b^n}{p_b^n} \gamma^n \left(1 + \frac{q_b}{p_b} \gamma\right)^{-N_t+2}, \quad (10)$$

$$f_{\gamma_e^b}(\gamma) = \sum_{m=0}^{N_e-1} \frac{\binom{N_t-2}{m} (N_t-2) q_b^{m+1}}{p_b^{m+1}} \gamma^m \left(1 + \frac{q_b}{p_b} \gamma\right)^{-N_t+1} - \sum_{m=1}^{N_e-1} \frac{\binom{N_t-2}{m} m q_b^m}{p_b^m} \gamma^{m-1} \left(1 + \frac{q_b}{p_b} \gamma\right)^{-N_t+2}. \quad (11)$$

Proof: Since $\mathbf{H}_e$ has i.i.d. complex Gaussian entries, if the matrix $[\mathbf{w}_b \mathbf{W}]$ is unitary, then $\mathbf{H}_e[\mathbf{w}_b \mathbf{W}]$ has also i.i.d. complex Gaussian entries [19]. Therefore, the elements of $\mathbf{H}_e \mathbf{w}_b$ and $\mathbf{H}_e \mathbf{W}$ are independent. As a result, the quantity $\mathbf{w}_b^\dagger \mathbf{H}_e^\dagger (\mathbf{W}^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{W})^{-1} \mathbf{H}_e \mathbf{w}_b$ is equivalent to the signal-to-interference ratio of a N_e -branch minimum mean square error (MMSE) diversity combiner with N_t-2 interferers [33]. Equation (10), the CDF of γ_e^b , is then obtained from [33], whereas (11) follows by differentiating (10). $\square$

Proposition 2. [34] The CDF and PDF of the random variable $X \sim \text{Gamma}(\alpha, \beta)$ are given as

$$F_X(x) = \frac{\gamma(\alpha, \frac{x}{\beta})}{\Gamma(\alpha)} = 1 - \sum_{n=0}^{\alpha-1} \frac{x^n e^{-\frac{x}{\beta}}}{\beta^n n!}, \quad (12)$$

$$f_X(x) = \frac{x^{\alpha-1} e^{-\frac{x}{\beta}}}{\beta^\alpha \Gamma(\alpha)}. \quad (13)$$

For notational convenience in following analysis in this section, we will use ϕ instead of ϕ_b for the different schemes and distinguish them upon driving the optimal power allocation.

B. Scaled Beamforming (SB)

The main idea of this scheme is that the transmitted power of the information signal p_{SB} is scaled in order to keep the interference power at the PU-RX below the interference power threshold I . As a result, the interference power at the PU-RX is not present and the channel is reduced to MISOME wiretap channel. As the CSI of the eavesdropper is not known at the SU-TX, the available option is to design $\mathbf{w}_{\text{SB}}$ to perform as a maximum ratio transmission (MRT) beamformer toward the SU-RX as follows

$$\mathbf{w}_{\text{SB}} = \hat{\mathbf{h}}_s. \quad (14)$$

For the interference received at the PU not to exceed I , the transmitted power must satisfy $p_{\text{SB}} \leq \frac{I}{|\mathbf{h}_p^\dagger \mathbf{w}_{\text{SB}}|^2}$. Moreover, we have from (2), $p_{\text{SB}} \leq \phi P$. Therefore, the transmitted power p_{SB} should be varied as

$$p_{\text{SB}} = \min\left(\phi P, \frac{I}{|\mathbf{h}_p^\dagger \hat{\mathbf{h}}_s|^2}\right). \quad (15)$$

Note that p_{SB} is a random variable but is limited by the maximum transmitted power ϕP allocated for the information signal. As the jamming signal affects only the ED-RX, the jamming power transmitted from each of the N_t-2 antennas should be maximized and hence, from (3), it is given by

$$q_{\text{SB}} = \frac{(1-\phi)P}{N_t-2}. \quad (16)$$

Substituting (14)-(16) into (7)-(8), the SNRs at the SU-RX and ED-RX are, respectively, given as

$$\gamma_s^{\text{SB}} = p_{\text{SB}} |\mathbf{h}_s^\dagger \hat{\mathbf{h}}_s|^2 = p_{\text{SB}} \|\mathbf{h}_s\|^2 = \min(\phi P, \frac{I}{Z_2}) Z_1, \quad (17)$$

$$\gamma_e^{\text{SB}} = \frac{p_{\text{SB}}}{q_{\text{SB}}} \hat{\mathbf{h}}_s^\dagger \mathbf{H}_e^\dagger (\mathbf{W}^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{W})^{-1} \mathbf{H}_e \hat{\mathbf{h}}_s, \quad (18)$$

where, in (17), we have defined $Z_1 \triangleq \|\mathbf{h}_s\|^2$ and $Z_2 \triangleq |\mathbf{h}_p^\dagger \hat{\mathbf{h}}_s|^2$. The following two lemmas give exact expressions for the ergodic rate of the SU and eavesdropper.

Lemma 1. The achievable ergodic rate of the SU using SB scheme is given as

$$C_s^{\text{SB}} = \sum_{n=0}^{N_t-1} \frac{\theta \Psi(n+1, n+1, \frac{1}{\phi P})}{\ln 2 (\phi P)^n} + \sum_{n=0}^{N_t-1} \sum_{k=1}^n \frac{(k-1)! \Gamma(n-k+1, \frac{I}{\phi P})}{\ln 2 (-1)^{k-n} I^{n-k} n!} + \Delta, \quad (19)$$

where

$$\Delta = \begin{cases} \sum_{n=0}^{N_t-1} \sum_{k=0}^n k! \binom{n}{k} \frac{(\frac{I}{\phi P})^{n-k} \text{Ei}(\frac{-1}{\phi P}) e^{\frac{1-I}{\phi P}} + \Gamma(n-k, \frac{I}{\phi P})}{\ln 2 (-1)^{1-n} I^{n-k-1} n! (I-1)^{k+1}}, & I \neq 1 \\ \sum_{n=0}^{N_t-1} \frac{(\frac{I}{\phi P})^{n-1} \text{Ei}(\frac{-1}{\phi P}) + \Gamma(n+1, \frac{I}{\phi P})}{\ln 2 (-1)^{1-n} I^n n! (n+1)}, & I = 1, \end{cases}$$

where $\Psi(\cdot, \cdot, \cdot)$ is the Tricomi's (confluent hypergeometric) function [35, Eq. (9.211.4)], $\text{Ei}(\cdot)$ is the exponential integral function, $\Gamma(\cdot, \cdot)$ denotes the incomplete upper gamma function, and $\theta \triangleq 1 - e^{-\frac{I}{\phi P}}$.

Proof: See Appendix A. $\square$

Lemma 2. The achievable ergodic rate of the eavesdropper using SB scheme is given as

$$C_e^{\text{SB}} = \sum_{n=0}^{N_e-1} \frac{\binom{N_t-2}{n} \theta q_{\text{SB}}^n}{\ln 2 (\phi P)^n} B(n+1, N_t-n-2) \times {}_2F_1(N_t-2, n+1; N_t-1; 1 - \frac{q_{\text{SB}}}{\phi P}) + \sum_{n=0}^{N_e-1} \frac{\binom{N_t-2}{n} \mathcal{J}_n(N_t, I, q_{\text{SB}})}{\ln 2 I^n q_{\text{SB}}^{-n}} B(n+1, N_t-n-2), \quad (20)$$

where the integral $\mathcal{J}_n(N_t, I, q_{\text{SB}})$ is defined in (78) and can be computed numerically. $B(\cdot, \cdot)$ is the Beta function and ${}_2F_1(\cdot, \cdot, \cdot, \cdot)$ is the Gauss hypergeometric function.

Proof: See Appendix B. $\square$

Substituting (19) and (20) into (9), the achievable ergodic secrecy rate of the SB scheme is obtained.

C. Projected Beamforming (PB)

In this scheme, the beamforming vector $\mathbf{w}_{\text{PB}}$ of the information signal is designed to impose zero forcing at the PU-RX such that the interference power at the PU-RX is always completely removed. Let $\hat{\mathbf{h}}_s$ denotes the projection of $\mathbf{h}_s$ onto the null space of $\mathbf{h}_p$; $\hat{\mathbf{h}}_s$ is given as

$$\hat{\mathbf{h}}_s = \mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s, \quad (21)$$

where $\mathbf{Q} \in \mathbb{C}^{N_t \times (N_t - 1)}$ is an orthonormal matrix with columns represent the bases vectors of the null space of the vector $\mathbf{h}_p$. Therefore, $\mathbf{w}_{\text{PB}}$ is designed as the unit-norm vector of the projected vector given in (21) as follows

$$\mathbf{w}_{\text{PB}} = \hat{\mathbf{h}}_s. \quad (22)$$

Note that p_{PB} should be maximized because this power is transmitted at the null space of the PU's channel. Moreover, as discussed before, the SU-TX should transmits at maximum AN power. Therefore, p_{PB} and q_{PB} are given as

$$p_{\text{PB}} = \phi P, \quad (23)$$

$$q_{\text{PB}} = \frac{(1 - \phi)P}{N_t - 2}. \quad (24)$$

Hence, the SNRs at the SU-RX and ED-RX are given as

$$\gamma_s^{\text{PB}} = p_{\text{PB}} |\mathbf{h}_s^\dagger \hat{\mathbf{h}}_s|^2, \quad (25)$$

$$\gamma_e^{\text{PB}} = \frac{p_{\text{PB}}}{q_{\text{PB}}} \hat{\mathbf{h}}_s^\dagger \mathbf{H}_e^\dagger (\mathbf{W}^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{W})^{-1} \mathbf{H}_e \hat{\mathbf{h}}_s. \quad (26)$$

Note that $\gamma_s^{\text{PB}} = p_{\text{PB}} \frac{|\mathbf{h}_s^\dagger \mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s|^2}{\|\mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s\|^2} = p_{\text{PB}} |(\mathbf{Q}^\dagger \mathbf{h}_s)^\dagger \frac{\mathbf{Q}^\dagger \mathbf{h}_s}{\|\mathbf{Q}^\dagger \mathbf{h}_s\|}|^2$. The last equality follows from the fact that $\|\mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s\|^2 = (\mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s)^\dagger \mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s = (\mathbf{Q}^\dagger \mathbf{h}_s)^\dagger \mathbf{Q}^\dagger \mathbf{h}_s = \|\mathbf{Q}^\dagger \mathbf{h}_s\|^2$. Therefore, $\gamma_s^{\text{PB}} \sim \text{Gamma}(N_t - 1, p_{\text{PB}})$. The following two lemmas give closed-form expressions for the ergodic rate of the SU and the eavesdropper.

Lemma 3. The achievable ergodic rate of the SU using PB scheme is given as

$$C_s^{\text{PB}} = \frac{e^{\frac{1}{p_{\text{PB}}}}}{\ln 2} \sum_{k=1}^{N_t-1} E_k\left(\frac{1}{p_{\text{PB}}}\right), \quad (27)$$

where $E_k(\cdot)$ is the generalized exponential integral function.

Proof: As $\gamma_s^{\text{PB}} \sim \text{Gamma}(N_t - 1, p_{\text{PB}})$, its PDF can be obtained using Proposition 2. Therefore, the achievable ergodic rate of the SU can be calculated as

$$\begin{aligned} C_s^{\text{PB}} &= \mathbb{E}[\log_2(1 + \gamma_s^{\text{PB}})] \\ &= \frac{1}{\ln 2 p_{\text{PB}}^{N_t-1} (N_t - 1)!} \int_0^\infty \frac{\ln(1 + \gamma)}{\gamma^{2-N_t}} e^{-\frac{\gamma}{p_{\text{PB}}}} d\gamma. \end{aligned} \quad (28)$$

The integral in the last equation is calculated using the identity given in [36, Appendix A3], which gives (27). $\square$

Lemma 4. The achievable ergodic rate of the eavesdropper using PB scheme is given as

$$\begin{aligned} C_s^{\text{PB}} &= \sum_{n=0}^{N_e-1} \frac{q_{\text{PB}}^n (N_t + n - 3)!}{\ln 2 p_{\text{PB}}^n (N_t - 3)! n!} B(n + 1, N_t - 2) \\ &\quad \times F_1\left(N_t + n - 2, n + 1; N_t + n - 1; 1 - \frac{q_{\text{PB}}}{p_{\text{PB}}}\right). \end{aligned} \quad (29)$$

Proof: See Appendix C. $\square$

Substituting (27) and (29) into (9), the achievable ergodic secrecy rate of PB scheme is obtained.

D. Cognitive Beamforming (CB)

In this subsection, we characterize the optimal beamforming that maximizes the ergodic secrecy rate defined in (9). In this scheme, the problem is reduced to the beamforming in the conventional MISO-CR channel [37], [38]. In other words, it is considered that the eavesdropper is not present, and the beamforming in this case is the optimal beamforming of the conventional MISO-CR channel. Note that in our system setup, where the CSI of the eavesdropper is not available, which also means that the beamforming vector $\mathbf{w}_{\text{CB}}$ is not a function of $\mathbf{H}_e$, the optimal option is to design $\mathbf{w}_{\text{CB}}$ as the optimal solution for the MISO-CR channel. Therefore, the beamforming vector $\mathbf{w}_{\text{CB}}$ for the information signal in this scheme is designed as [37]

$$\mathbf{w}_{\text{CB}} = \alpha_{\text{CB}} \hat{\mathbf{h}}_p + \beta_{\text{CB}} \hat{\mathbf{h}}_s, \quad (30)$$

where α_{CB} and β_{CB} are weights, so that $\mathbf{w}_{\text{CB}}$ is given as [37]

$$\mathbf{w}_{\text{CB}} = \begin{cases} \left(\frac{\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s}{\|\mathbf{h}_s\|} \hat{\mathbf{h}}_p + \frac{\hat{\mathbf{h}}_s^\dagger \mathbf{h}_s}{\|\mathbf{h}_s\|} \hat{\mathbf{h}}_s \right) \triangleq \mathbf{w}_{\text{CB}_1}, & Z_2 \leq \frac{I}{p_{\text{CB}}} \\ \left(\lambda \frac{\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s}{\|\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s\|} \hat{\mathbf{h}}_p + \sqrt{1 - \lambda^2} \frac{\hat{\mathbf{h}}_s^\dagger \mathbf{h}_s}{\|\hat{\mathbf{h}}_s^\dagger \mathbf{h}_s\|} \hat{\mathbf{h}}_s \right) \triangleq \mathbf{w}_{\text{CB}_2} \text{ O.W.}, & \end{cases} \quad (31)$$

where $\lambda = \sqrt{\frac{I}{p_{\text{CB}} \|\mathbf{h}_p\|^2}}$. Note that $\mathbf{w}_{\text{CB}}$ is a function of both the available channels pair $(\mathbf{h}_s, \mathbf{h}_p)$ and I . As given in [37], the SU-TX transmits at maximum power. Moreover, the transmitted power of the jamming signal should be maximized. Therefore, p_{CB} and q_{CB} are given as

$$p_{\text{CB}} = \phi P, \quad (32)$$

$$q_{\text{CB}} = \frac{(1 - \phi)P}{N_t - 2}. \quad (33)$$

Considering (7), (8), and (31), the SNRs at the SU-RX and ED-RX are, respectively, given as

$$\gamma_s^{\text{CB}} = \begin{cases} p_{\text{CB}} |\mathbf{h}_s^\dagger \mathbf{w}_{\text{CB}_1}|^2 \triangleq \gamma_{s_1}^{\text{CB}} & Z_2 \leq \frac{I}{p_{\text{CB}}}, \\ p_{\text{CB}} |\mathbf{h}_s^\dagger \mathbf{w}_{\text{CB}_2}|^2 \triangleq \gamma_{s_2}^{\text{CB}} & \text{otherwise}, \end{cases} \quad (34)$$

$$\gamma_e^{\text{CB}} = \begin{cases} \underbrace{\frac{p_{\text{CB}}}{q_{\text{CB}}} \mathbf{w}_{\text{CB}_1}^\dagger \mathbf{H}_e^\dagger (\mathbf{W}^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{W})^{-1} \mathbf{H}_e \mathbf{w}_{\text{CB}_1}}_{\gamma_{e_1}^{\text{CB}}} & Z_2 \leq \frac{I}{p_{\text{CB}}}, \\ \underbrace{\frac{p_{\text{CB}}}{q_{\text{CB}}} \mathbf{w}_{\text{CB}_2}^\dagger \mathbf{H}_e^\dagger (\mathbf{W}^\dagger \mathbf{H}_e^\dagger \mathbf{H}_e \mathbf{W})^{-1} \mathbf{H}_e \mathbf{w}_{\text{CB}_2}}_{\gamma_{e_2}^{\text{CB}}} & \text{otherwise.} \end{cases} \quad (35)$$

From (9), (34), and (35), the achievable ergodic secrecy rate for CB can be expressed as

$$\begin{aligned} C_{\text{sec}}^{\text{CB}} &= [C_{s_1}^{\text{CB}} - C_{e_1}^{\text{CB}}]^+ \Pr[Z_2 \leq \frac{I}{p_{\text{CB}}}] \\ &\quad + [C_{s_2}^{\text{CB}} - C_{e_2}^{\text{CB}}]^+ \Pr[Z_2 > \frac{I}{p_{\text{CB}}}], \end{aligned} \quad (36)$$

where $C_{s_i}^{\text{CB}} = \mathbb{E}[\log_2(1 + \gamma_{s_i}^{\text{CB}})]$ and $C_{e_i}^{\text{CB}} = \mathbb{E}[\log_2(1 + \gamma_{e_i}^{\text{CB}})]$, $i \in \{1, 2\}$ represent the ergodic rates corresponding to the different SNRs defined in (34) and (35).

Now, we calculate the different terms in (36). First note that $\Pr[Z_2 \leq \frac{I}{p_{\text{CB}}}] = \theta$ and $\Pr[Z_2 > \frac{I}{p_{\text{CB}}}] = 1 - \theta$. Moreover, it can be shown that (see Appendix D)

$$\gamma_{s_1}^{\text{CB}} = p_{\text{CB}} \|\mathbf{h}_s\|^2. \quad (37)$$

Following similar steps as those for deriving (27), the achievable ergodic rate of the SU when $\gamma_s^{\text{CB}} = \gamma_{s_1}^{\text{CB}}$ is derived as

$$C_{s_1}^{\text{CB}} = \mathbb{E}[\log_2(1 + \gamma_{s_1}^{\text{CB}})] = \frac{e^{\frac{1}{p_{\text{CB}}}}}{\ln 2} \sum_{k=1}^{N_t} \mathbb{E}_k\left(\frac{1}{p_{\text{CB}}}\right). \quad (38)$$

Substituting for $\mathbf{w}_{\text{CB}2}$ from (31) into (34), $\gamma_{s_2}^{\text{CB}}$ is given as

$$\gamma_{s_2}^{\text{CB}} = \left(\underbrace{\sqrt{\frac{I}{Z}} |\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s|}_U + \underbrace{\sqrt{p_{\text{CB}} - \frac{I}{Z}} |\hat{\mathbf{h}}_s^\dagger \mathbf{h}_s|}_V \right)^2, \quad (39)$$

where $Z \triangleq \|\mathbf{h}_p\|^2$. Note that $|\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s|^2 \sim \exp(1)$ and $|\hat{\mathbf{h}}_s^\dagger \mathbf{h}_s|^2 \sim \text{Gamma}(N_t - 1, 1)$. Thus, conditioned on Z , U is a scaled Rayleigh random variable and V is a scaled generalized gamma distributed random variable; using probability theory, their conditional PDFs can be easily obtained as

$$f_{U|Z}(u) = \frac{2Z}{I} u e^{-\frac{Zu}{I}}, \quad (40)$$

$$f_{V|Z}(v) = \frac{2Z^{N_t-1} v^{2N_t-3} e^{-\frac{Zv^2}{p_{\text{CB}}Z-I}}}{(p_{\text{CB}}Z - I)^{N_t-1} (N_t - 2)!}. \quad (41)$$

The PDF of $(U + V)$, conditioned on Z , is evaluated as

$$f_{(U+V)|Z}(\gamma) = \int_0^\gamma f_{U|\{Z=z\}}(u) f_{V|\{Z=z\}}(\gamma - u) du. \quad (42)$$

Using the theory of transformation of random variables, and then averaging over $Z \sim \text{Gamma}(N_t, 1)$, it can be shown from (42) that the PDF of $\gamma_{s_2}^{\text{CB}} = (U + V)^2$ is given as

$$f_{\gamma_{s_2}^{\text{CB}}}(\gamma) = \int_{\frac{I}{\phi P}}^\infty \int_0^{\sqrt{\gamma}} \frac{2}{\sqrt{\gamma}} f_{U|\{Z=z\}}(u) f_{V|\{Z=z\}}(\sqrt{\gamma} - u) du dz. \quad (43)$$

The ergodic rate of the SU when $\gamma_s^{\text{CB}} = \gamma_{s_2}^{\text{CB}}$ is derived as

$$C_{s_2}^{\text{CB}} = \frac{1}{\ln 2} \int_0^\infty \ln(1 + \gamma) f_{\gamma_{s_2}^{\text{CB}}}(\gamma) d\gamma, \quad (44)$$

where $f_{\gamma_{s_2}^{\text{CB}}}(\gamma)$ is given in (43). Note also that, using Proposition 1, $\gamma_{e_1}^{\text{CB}}$ and $\gamma_{e_2}^{\text{CB}}$ given in (35) have the same distribution as γ_e^{PB} . Therefore, $C_{e_1}^{\text{CB}} = C_{e_2}^{\text{CB}} = C_e^{\text{PB}}$, which is given in (29). Substituting (38), (44) and the values of $C_{e_1}^{\text{CB}}$ and $C_{e_2}^{\text{CB}}$ into (36), the ergodic secrecy rate of CB is obtained.

E. Optimal Power Allocation

In this subsection, we consider the optimal power allocation for the information and AN signals. We carry out large N_t analysis and derive expressions for the optimal ϕ . The asymptotic results are concise and are good approximations of the finite case, and allow us to draw conclusions and insights. It should be mentioned that in the presence of an eavesdropper with large number of antennas, the secrecy rate is degraded severely as will be shown in Section III-G. Therefore, considering large number of antennas at SU-TX is essential to maintain a good secure communication link.

1) *Optimal power allocation for SB*: Asymptotically, when $N_t \rightarrow \infty$, the SNRs given in (17)-(18) are converged as

$$\gamma_{s,\infty}^{\text{SB}} \triangleq \lim_{N_t \rightarrow \infty} \gamma_s^{\text{SB}} = \min\left(\phi P, \frac{I}{Z_2}\right) N_t, \quad (45)$$

$$\gamma_{e,\infty}^{\text{SB}} \triangleq \lim_{N_t \rightarrow \infty} \gamma_e^{\text{SB}} = \frac{\min\left(\phi P, \frac{I}{Z_2}\right) \|\mathbf{H}_e \hat{\mathbf{h}}_s\|^2}{(1 - \phi) P}. \quad (46)$$

Lemma 5. The optimal power allocation factor ϕ_{SB}^* for SB that maximizes the asymptotic ergodic secrecy rate is obtained by solving the following fixed point equation

$$\begin{aligned} & \frac{1 - N_e + N_e e^{-\frac{I}{\phi_{\text{SB}}^* P}}}{1 - \phi_{\text{SB}}^* + N_e \phi_{\text{SB}}^* - N_e \phi_{\text{SB}}^* e^{-\frac{I}{\phi_{\text{SB}}^* P}} - \frac{IN_e}{P} \text{Ei}\left(\frac{-I}{\phi_{\text{SB}}^* P}\right)} \\ & + \frac{1 - e^{-\frac{I}{\phi_{\text{SB}}^* P}}}{\phi_{\text{SB}}^*} - \frac{1}{1 - \phi_{\text{SB}}^*} = 0. \end{aligned} \quad (47)$$

Proof: See Appendix E. $\square$

Note that the different system parameters in (47) are deterministic and can be assigned for long term transmission.

2) *Optimal power allocation for PB*: The SNRs for PB scheme given in (25)-(26) are asymptotically given as

$$\gamma_{s,\infty}^{\text{PB}} \triangleq \lim_{N_t \rightarrow \infty} \gamma_s^{\text{PB}} = p_{\text{PB}}(N_t - 1), \quad (48)$$

$$\gamma_{e,\infty}^{\text{PB}} \triangleq \lim_{N_t \rightarrow \infty} \gamma_e^{\text{PB}} = \frac{\phi}{1 - \phi} \|\mathbf{H}_e \hat{\mathbf{h}}_s^\dagger\|^2. \quad (49)$$

The corresponding asymptotic achievable ergodic rates at the SU and the eavesdropper are, respectively, given as

$$C_{s,\infty}^{\text{PB}} = \log_2(1 + \gamma_{s,\infty}^{\text{PB}}) = \log_2(1 + p_{\text{PB}}(N_t - 1)), \quad (50)$$

$$C_{e,\infty}^{\text{PB}} = \mathbb{E}[\log_2(1 + \gamma_{s,\infty}^{\text{PB}})] = \frac{e^{\frac{1-\phi}{\phi}}}{\ln 2} \sum_{k=1}^{N_e} \mathbb{E}_k\left(\frac{1-\phi}{\phi}\right). \quad (51)$$

Eq. (51) is obtained using similar steps as those for obtaining (27). The asymptotic ergodic secrecy rate is then given as

$$C_{\text{sec},\infty}^{\text{PB}} = [C_{s,\infty}^{\text{PB}} - C_{e,\infty}^{\text{PB}}]^+. \quad (52)$$

Similar procedure as proposed in [19] can be followed to obtain the optimal ϕ that maximizes the rate in (52) as

$$\phi_{\text{PB}}^* = \frac{1}{1 + \sqrt{N_e}}. \quad (53)$$

It can be noted from (53) that ϕ_{PB}^* depends only on N_e , where more power should be allocated to the jamming signal as the number of eavesdropper's antennas increases.

3) *Optimal power allocation for CB*: In this case, when $N_t \rightarrow \infty$, $\|\mathbf{h}_p\|^2 \rightarrow N_t$ and hence $\lambda \rightarrow 0$. Therefore, from (31), (34), (35) and (37), it can be easily shown that

$$C_{sec,\infty}^{CB} = \begin{cases} C_{sec,\infty}^{SB} & Z_2 \leq \frac{I}{\phi P}, \\ C_{sec,\infty}^{PB} & Z_2 > \frac{I}{\phi P}. \end{cases} \quad (54)$$

Moreover, when $Z_2 \leq \frac{I}{\phi P}$, the SNRs of the SB given in (45)-(46) reduce to that of PB given in (48)-(49) after considering the approximation $(N_t - 1) \approx N_t$ at $N_t \rightarrow \infty$. Therefore, when $Z_2 \leq \frac{I}{\phi P}$, $C_{sec,\infty}^{SB} = C_{sec,\infty}^{PB}$. As a result, from (54), $C_{sec,\infty}^{CB} = C_{sec,\infty}^{PB}$. Thus, the optimal ϕ for CB is given as

$$\phi_{CB}^* = \frac{1}{1 + \sqrt{N_e}}. \quad (55)$$

F. Implications

In the following, we study the secrecy performance of the three schemes under asymptotic values of I and N_t .

- 1) $I \rightarrow \infty$ and arbitrary N_t : This case represents no interference power constraint at the PU. In other words, the network model reduces to MISOME [19]. In this case, as can be inferred from (34), the condition $Z_2 \leq \frac{I}{\phi P}$ is always satisfied, so that $\gamma_s^{CB} = \gamma_{s1}^{CB}$. As a result, it can be shown from (17), (34) and (37) that $\gamma_s^{SB} = \gamma_s^{CB}$. Therefore, SB and CB have the same performance, which is the performance of the MRT beamforming.
- 2) $I \rightarrow 0$ and arbitrary N_t : In this case, no interference is allowed at the PU-RX. It is clear from (17) that SB fails to achieve positive secrecy rate, and it is unsuitable for such scenarios of stringent QoS requirements at the PU. On the other hand, PB is the best choice in this case as the interference is always removed. Note also from (34) that when $I \rightarrow 0$ (or $P \rightarrow \infty$), $\gamma_s^{CB} = \gamma_{s2}^{CB}$ and $\lim_{I \rightarrow 0} \gamma_{s2}^{CB} = \gamma_s^{PB}$. As a result, CB reduces to PB.
- 3) $N_t \rightarrow \infty$ and arbitrary I : In this case, the SU-TX is assumed to be equipped with massive antenna array. This case is investigated in the previous subsection. It is concluded from (54) that $C_{sec,\infty}^{CB} = C_{sec,\infty}^{PB}$. It should be noted that this conclusion is valid even with the extreme case $I \rightarrow \infty$, which means that PB achieves the best performance when $N_t \rightarrow \infty$ irrespective of the QoS requirements at the PU.

G. Numerical Results

In this subsection, we provide the analytical results to illustrate the secrecy performance of the SB, PB, and CB schemes in terms of the achievable ergodic secrecy rate. Moreover, Monte Carlo simulations consisting of independent trials are performed in order to verify the analytical derivations. The impact of the different system parameters such as the number of antennas, i.e. N_t and N_e , and the interference temperature limit I on the secrecy performance is also investigated.

In Fig. 2, the achievable ergodic secrecy rate is plotted versus the power P for the three schemes. $I = 0$ dB and the

Fig. 2. Achievable ergodic secrecy rate vs. P with $I = 0$ dB, $N_t = 4$, and $N_e = 2$.

Fig. 3. Achievable ergodic secrecy rate vs. I with $P = 10$ dB, $N_t = 6$, and different values of N_e .

optimal power allocation results derived in Section III-E are used to obtain the results. As shown, CB achieves the best performance over the range of P and the secrecy rate of the SB scheme gradually increases with P before it saturates. The secrecy rate of SB is close to that of CB at low power region and is deviated from it at high values of P due to the power constraint in (15). On the other hand, PB approaches the performance of CB at high power region, which confirms the analytical results in Section III-F. Note also that the analytical results matches well with the simulation results.

In Fig. 3, the ergodic secrecy rate for the three schemes is plotted versus I . The variation of I is from -15 dB to 15 dB. It is shown that SB fails at low values of I and approaches the performance of CB at the high values of I , which is consistent with the results obtained in Section III-F. The secrecy rate of PB remains constant over all values of I since it is independent of I , and with 6 transmit antennas, CB can achieve up to 25% gains in the ergodic secrecy rate with respect to PB. The performance of SB fails at low values of I , but it is close to that of CB at higher values of I . The

Fig. 4. Achievable ergodic secrecy rate vs. N_t with $P = 15$ dB, $I = 0$ dB, $N_t = 4$, and $N_e = 2$.

Fig. 5. Optimal power allocation factor ϕ_b^* vs. N_t with $P = 10$ dB, $I = 0$ dB, and different values of N_e .

detrimental effect of increasing N_e is also shown.

Fig. 4 shows the effect of increasing N_t on the ergodic secrecy rate. The large N_t approximation is also shown. The SB curve with a large number of antennas approximation is obtained based on (83), (84), and (87) and that of PB and CB using (50), (51) and (52). Note that the convergence is fast and hence the derived approximations are accurate. Furthermore, increasing N_t improves the ergodic secrecy rate. Moreover, as expected, SB has the lowest performance with $I = 0$ dB.

Next, in Fig. 5, we investigate the impact of N_t and N_e on ϕ_b^* . The figure plots ϕ_b^* versus N_t with different values of N_e . The solid lines indicate the optimal values of the power allocation factor that are obtained using exhaustive numerical search, while the dashed lines indicate the values obtained from the the approximation of large number of antennas given in (47), (53) and (55). We notice that, for fixed N_e , an increase in N_t leads to a slight increase in the values of ϕ_b^* before it saturates. This confirms our analytical results, where ϕ_b^* does not depend on N_t when N_t is large. It can be seen that increasing N_e reduces ϕ_b^* , which implies that more power

Fig. 6. Optimal power allocation factor ϕ_b^* vs. I with $P = 10$ dB, $N_t = 6$, and different values of N_e .

should be allocated to AN signal as N_e increases. It should be noted that ϕ_{SB}^* gives a useful approximation for the exact value. Note also that for PB and CB, ϕ_b^* converges well at higher values of N_e .

Fig. 6 illustrates the impact of I on ϕ_b^* for all schemes with $P = 10$ dB and different values of N_e . As shown, the optimal power allocation factor of PB and CB are approximately independent of I . For SB, ϕ_{SB}^* is small at small values of I , due to the power constraint given in (15). Therefore, most of the power should be allocated to the AN signal. As I increases, ϕ_{SB}^* increases gradually with I , and at high values of I (over 15 dB), all schemes have the same value of ϕ_b^* .

IV. SECRECY OUTAGE PROBABILITY ANALYSIS

In this section, we introduce the secrecy outage probability as another performance metric for the proposed beamforming schemes. We derive closed-form and exact expressions for the secrecy outage probability of these schemes. For nonergodic channels, the secrecy outage probability is considered the most appropriate performance metric. A secrecy outage occurs when the instantaneous secrecy rate is less than a target secrecy rate R_s . Therefore, the secrecy outage probability for a scheme $b \in \{SB, PB, CB\}$ is given by

$$P_{out}^b = \Pr \left[\log_2 \left(\frac{1 + \gamma_s^b}{1 + \gamma_e^b} \right) \leq R_s \right] = \Pr \left[\gamma_s^b \leq \varepsilon(\gamma_e^b) \right], \quad (56)$$

where $\varepsilon(\gamma_e^b) \triangleq 2^{R_s}(1 + \gamma_e^b) - 1$.

A. Secrecy outage probability for SB

From (56), and considering (17) and (18), the secrecy outage probability of SB is expressed as

$$P_{out}^{SB} = \int_0^\infty \int_0^\infty F_{\gamma_s^{SB}|\{Z_2=z_2\}}(\varepsilon(\gamma_e)) f_{\gamma_e^{SB}|\{Z_2=z_2\}}(\gamma_e) \times f_{Z_2}(z_2) d\gamma_e dz_2. \quad (57)$$

Lemma 6. The secrecy outage probability of SB is given as

$$\begin{aligned}
P_{out}^{SB} = & 1 - \sum_{n=0}^{N_t-1} \sum_{m=0}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} (N_t-2) (m+k)!}{n! 2^{-kR_s} (2R_s-1)^{k-n} q_{SB}^k} \\
& \times \Psi\left(m+k+1, -N_t+m+k+3; \frac{2R_s}{q_{SB}}\right) \\
& \times \left[\frac{\theta(\phi P)^{k-n}}{e^{\frac{2R_s-1}{\phi P}}} + \frac{I \Gamma(n-k+1, \frac{I+2R_s-1}{\phi P})}{(I+2R_s-1)^{n-k+1}} \right] \\
& + \sum_{n=0}^{N_t-1} \sum_{m=1}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} m (m+k-1)!}{n! 2^{-kR_s} (2R_s-1)^{k-n} q_{SB}^k} \\
& \times \Psi\left(m+k, -N_t+m+k+3; \frac{2R_s}{q_{SB}}\right) \\
& \times \left[\frac{\theta(\phi P)^{k-n}}{e^{\frac{2R_s-1}{\phi P}}} + \frac{I \Gamma(n-k+1, \frac{I+2R_s-1}{\phi P})}{(I+2R_s-1)^{n-k+1}} \right]. \quad (58)
\end{aligned}$$

Proof: See Appendix F. $\square$

B. Secrecy outage probability for PB

As in (56), and considering (25) and (26), the secrecy outage probability for PB is given as

$$P_{out}^{PB} = \int_0^\infty F_{\gamma_{s1}^{PB}}(\varepsilon(\gamma_e)) f_{\gamma_e^{PB}}(\gamma_e) d\gamma_e. \quad (59)$$

Lemma 7. The secrecy outage probability of PB is given as

$$\begin{aligned}
P_{out}^{PB} = & 1 - \sum_{n=0}^{N_t-2} \sum_{m=0}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} (N_t-2) p_{PB}^{k-n} (m+k)!}{n! e^{\frac{2R_s-1}{p_{PB}}} 2^{-kR_s} (2R_s-1)^{k-n} q_{PB}^k} \\
& \times \Psi\left(m+k+1, -N_t+m+k+3; \frac{2R_s}{q_{PB}}\right) \\
& + \sum_{n=0}^{N_t-2} \sum_{m=1}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} m p_{PB}^{k-n} (m+k-1)!}{n! e^{\frac{2R_s-1}{p_{PB}}} 2^{-kR_s} (2R_s-1)^{k-n} q_{PB}^k} \\
& \times \Psi\left(m+k, -N_t+m+k+3; \frac{2R_s}{q_{PB}}\right). \quad (60)
\end{aligned}$$

Proof: See Appendix G. $\square$

C. Secrecy outage probability for CB

Considering (34) and (35), the secrecy outage probability for this scheme can be expressed as

$$\begin{aligned}
P_{out}^{CB} = & \underbrace{\Pr[\gamma_{s1}^{CB} \leq \varepsilon(\gamma_{e1}^{CB})]}_{\Xi_1} \underbrace{\Pr[Z_2 \leq \frac{I}{p_{CB}}]}_{\Xi_2} \\
& + \underbrace{\Pr[\gamma_{s2}^{CB} \leq \varepsilon(\gamma_{e2}^{CB})]}_{\Xi_3} \underbrace{\Pr[Z_2 > \frac{I}{p_{CB}}]}_{\Xi_4}. \quad (61)
\end{aligned}$$

It can be easily shown that $\Xi_2 = \theta$ and $\Xi_4 = 1 - \theta$. The CDF of $\gamma_{s1}^{CB} \sim \text{Gamma}(N_t, p_{CB})$ is obtained from (12) and

the PDF of γ_{e1}^{CB} is obtained from (11). Following similar steps as those in Appendix G for obtaining (60), Ξ_1 is solved as

$$\begin{aligned}
\Xi_1 = & \int_0^\infty F_{\gamma_{s1}^{CB}}(\varepsilon(\gamma_e)) f_{\gamma_{e1}^{CB}}(\gamma_e) d\gamma_e \\
= & 1 - \sum_{n=0}^{N_t-1} \sum_{m=0}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} (N_t-2) p_{CB}^{k-n} (m+k)!}{n! q_{CB}^k 2^{-kR_s} (2R_s-1)^{k-n} e^{\frac{2R_s-1}{p_{CB}}}} \\
& \times \Psi\left(m+k+1, -N_t+m+k+3; \frac{2R_s}{q_{CB}}\right) \\
& + \sum_{n=0}^{N_t-1} \sum_{m=1}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} m p_{CB}^{k-n} (m+k-1)!}{n! q_{CB}^k 2^{-kR_s} (2R_s-1)^{k-n} e^{\frac{2R_s-1}{p_{CB}}}} \\
& \times \Psi\left(m+k, -N_t+m+k+3; \frac{2R_s}{q_{CB}}\right). \quad (62)
\end{aligned}$$

The probability Ξ_3 is computed as follows

$$\Xi_3 = \int_{\frac{I}{\phi P}}^\infty \int_0^\infty F_{\gamma_{s2}^{CB}|\{Z=z\}}(\varepsilon(\gamma_e)) f_{\gamma_{e2}^{CB}}(\gamma_e) f_Z(z) d\gamma_e dz. \quad (63)$$

$f_{\gamma_{e2}^{CB}}(\gamma_e)$ is obtained from (11), and $f_Z(z)$ from (13). In order to find $F_{\gamma_{s2}^{CB}|\{Z=z\}}(\varepsilon(\gamma_e))$, we first find the CDF of the random variable $(U+V)$ conditioned on Z as follows

$$F_{(U+V)|Z}(\gamma) = \int_0^\gamma F_{U|\{Z=z\}}(\gamma-v) f_{V|\{Z=z\}}(v) dv. \quad (64)$$

Knowing that $\gamma_{s2}^{CB} = (U+V)^2$, $F_{\gamma_{s2}^{CB}|Z}$ can be obtained using transformation of random variables as follows

$$F_{\gamma_{s2}^{CB}|Z}(\gamma) = \int_0^{\sqrt{\gamma}} F_{U|\{Z=z\}}(\sqrt{\gamma}-v) f_{V|Z}(v) dv. \quad (65)$$

From (40), it can be shown that $F_{U|Z}(u) = 1 - e^{-\frac{Zu^2}{I}}$ while $f_{V|Z}(v)$ is given in (41). Substituting these results into (65), and then (65) into (63), Ξ_3 is obtained. Finally, substituting $\Xi_1 - \Xi_4$ in (61), the secrecy outage probability is obtained.

In the following, our objective is to find the optimal power allocation factor $\phi_{b,out}^*$ for the different beamforming schemes that minimizes the secrecy outage probability given in (58), (60) and (61) for a given R_s . We express $\phi_{b,out}^*$ as

$$\phi_{b,out}^* = \arg \min_{0 < \phi < 1} P_{out}^b(R_s). \quad (66)$$

A closed-form solution for $\phi_{b,out}^*$ is intractable. However, we determine $\phi_{b,out}^*$ using the exhaustive search method, which allows us to determine the optimal value of the secrecy outage probability as will be shown in next subsection. $\square$

D. Numerical Results

In this subsection, the impact of N_t , N_e and I on the secrecy outage probability and the optimal power fraction $\phi_{b,out}^*$ is investigated. Fig. 7 plots the secrecy outage probability versus $\phi_{b,out}$ with different values of N_t and N_e . The analytical curves were obtained from (58), (60) and (61). It can be noted that, at small values of $\phi_{b,out}$, the secrecy outage probability is high because the system uses more power to transmit the AN but little for the information signal, which causes low SNR at SU-RX. As $\phi_{b,out}$ increases, the secrecy outage probability decreases until it reaches a minimum value (corresponding to the optimal value $\phi_{b,out}^*$) and then starts to increase due to the fact that less power is used to transmit

Fig. 7. Secrecy outage probability vs. $\phi_{b,out}$ with $N_e = 2$, $P = 15$ dB, $R_s = 0.5$, $I = 0$ dB, and different values of N_t and N_e .

Fig. 8. Secrecy outage probability vs. R_s with $N_t = 4$, $N_e = 2$, $P = 10$ dB, and $I = 0$ dB.

AN than that required for optimal performance. As seen in the figure, CB gives the best performance. With 6 transmit antennas, CB can provide up to a two-fold reduction in the minimum secrecy outage probability with respect to PB. We also find that increasing N_t reduces the secrecy outage probability significantly, which reflects the importance of using multiple antennas at SU-TX. On the other hand, increasing N_e leads to increase in the secrecy outage probability, which reflects the detrimental effect of using multiple antennas at the ED-RX. Finally, note that the simulation results agree well with the analytical results, which demonstrates the accuracy of the derived results.

Fig. 8 shows the secrecy outage probability versus the target secrecy rate R_s . We observe that CB gives also the best performance over different values of R_s . In particular, with 4 transmit antennas, CB can achieve non-zero secrecy rates with outage probabilities of 15% and below, whereas PB cannot. The SB has better performance than PB at small values of R_s , while PB achieves better outage performance at higher values of R_s . It should be noted that with higher

Fig. 9. Optimal power allocation factor $\phi_{b,out}^*$ vs. N_t for $P = 15$ dB, $N_e = 2$, $R_s = 1$, and $I = 0$ dB.

Fig. 10. Optimal power allocation factor $\phi_{b,out}^*$ vs. N_e for $P = 15$ dB, $N_t = 6$, $R_s = 1$, and $I = 0$ dB.

values of I , SB achieves better performance than PB does.

In Fig. 9, we examine the impact of N_t on the optimal power allocation factor $\phi_{b,out}^*$. The figure plots $\phi_{b,out}^*$ versus N_t for the three schemes. It is clearly seen that increasing N_t leads to a decrease in the value of $\phi_{b,out}^*$. This implies that SU-TX should allocate more power to the AN signal as N_t increases. Interestingly, this observation is different from that observed in Fig. 5 for ϕ_b^* that maximizes the achievable ergodic secrecy rate, where ϕ_b^* increases with increasing N_t . This conclusion agrees with that obtained in [20] for minimizing the hybrid outage probability.

Next, we investigate the impact of increasing N_e on the optimal power allocation factor. Fig. 10 plots $\phi_{b,out}^*$ versus N_e for the three schemes. We observe from the figure that increasing N_e leads to a decrease in $\phi_{b,out}^*$ for PB and CB schemes. For SB, increasing N_e leads to a slight increase in $\phi_{b,out}^*$ before it saturates. As N_e , in practice, is not known at SU-TX, SB is a good choice in this case as $\phi_{SB,out}^*$ is almost independent of N_e .

V. CONCLUSIONS

In this paper, we addressed the problem of physical layer security in MISOME-CRNs with passive eavesdropping in fast fading environments, while taking into account the QoS constraints of the PU. We proposed an optimal CB scheme with AN that maximizes the achievable ergodic secrecy rate. Moreover, we proposed two suboptimal beamforming schemes namely, SB and PB. We considered two performance metrics: ergodic secrecy rate and secrecy outage probability. In order to investigate the secrecy performance of the proposed schemes and design the different transmission parameters, such as the transmitted power and the number of transmit antennas, we derived exact and closed-form expressions of the two performance metrics. We used numerical simulations to validate the analysis. The provided results showed that beamforming with AN is a vital tool to guarantee secure transmission in the presence of a passive eavesdropper in CRNs, and more power should be allocated to the AN signal as the number of eavesdropper antennas increases. We determined the optimal power allocation that maximizes the secrecy rate and minimizes the secrecy outage probability. Moreover, we provided important insights onto the impact of the different system parameters on the beamforming design. In particular, we showed that beamforming design highly depends on the interference limit at the PU. This is responsible for the superiority of CB, which depending on this interference limit can be regarded as a combination of SB and PB.

In this paper, we assumed perfect CSI of the legitimate users, and focused on beamforming design. Possible future extensions include consideration of imperfect CSI. Moreover, developing schemes in multi-user and massive MIMO scenarios is regarded as an interesting future research direction.

APPENDIX A PROOF OF LEMMA 1

The CDF of γ_s^{SB} can be expressed as

$$F_{\gamma_s^{\text{SB}}}(\gamma) = \underbrace{\Pr\left(Z_1 \leq \frac{\gamma}{\phi P}, Z_2 \leq \frac{I}{\phi P}\right)}_{\mathcal{I}_1} + \underbrace{\Pr\left(\frac{Z_1}{Z_2} \leq \frac{\gamma}{I}, Z_2 \geq \frac{I}{\phi P}\right)}_{\mathcal{I}_2}. \quad (67)$$

Note that $Z_1 \sim \text{Gamma}(N_t, 1)$, $Z_2 \sim \exp(1)$, and they are independent. Therefore, $\mathcal{I}_1$ and $\mathcal{I}_2$ can be derived as

$$\mathcal{I}_1 = F_{Z_1}\left(\frac{\gamma}{\phi P}\right) F_{Z_2}\left(\frac{I}{\phi P}\right) = \theta - \theta \sum_{n=0}^{N_t-1} \frac{\gamma^n e^{-\frac{\gamma}{\phi P}}}{(\phi P)^n n!}, \quad (68)$$

$$\begin{aligned} \mathcal{I}_2 &= \int_{\frac{I}{\phi P}}^{\infty} F_{Z_1}\left(\frac{\gamma z_2}{I}\right) f_{Z_2}(z_2) dz_2 \\ &= 1 - \theta - \sum_{n=0}^{N_t-1} \frac{\Gamma(n+1, \frac{I+\gamma}{\phi P})}{I^n n! \gamma^{-n}}, \end{aligned} \quad (69)$$

where $\theta \triangleq 1 - e^{-\frac{I}{\phi P}}$. Substituting (68) and (69) into (67), the CDF of γ_s^{SB} is obtained as

$$F_{\gamma_s^{\text{SB}}}(\gamma) = 1 - \sum_{n=0}^{N_t-1} \frac{\theta \gamma^n e^{-\frac{\gamma}{\phi P}}}{(\phi P)^n n!} - \sum_{n=0}^{N_t-1} \frac{\gamma^n \Gamma(n+1, \frac{I+\gamma}{\phi P})}{I^n n! (1 + \frac{\gamma}{I})^{n+1}}. \quad (70)$$

The ergodic rate of the SU is derived as follows

$$\begin{aligned} C_s^{\text{SB}} &= \frac{1}{\ln 2} \int_0^{\infty} \ln(1 + \gamma) f_{\gamma_s^{\text{SB}}}(\gamma) d\gamma \\ &\stackrel{a}{=} \frac{1}{\ln 2} \int_0^{\infty} \frac{1 - F_{\gamma_s^{\text{SB}}}(\gamma)}{(1 + \gamma)} d\gamma \\ &\stackrel{b}{=} \sum_{n=0}^{N_t-1} \frac{\theta \Psi(n+1, n+1, \frac{1}{\phi P})}{\ln 2 (\phi P)^n} + \sum_{n=0}^{N_t-1} \frac{1}{\ln 2 I^n n!} \\ &\quad \times \underbrace{\int_0^{\infty} \gamma^n (1 + \gamma)^{-1} \int_{\frac{I}{\phi P}}^{\infty} t^n e^{-(1+\frac{\gamma}{I})t} dt d\gamma}_{\Xi_5}, \end{aligned} \quad (71)$$

where equality *a* is obtained by using integration by parts and *b* by substituting (70) into (71) and using [35, Eq. (9.211.4)] and [35, Eq. (3.381.3)]. Ξ_5 can be solved by integrating with respect to γ using [35, Eq. (3.353.5)], which gives

$$\begin{aligned} \Xi_5 &= (-1)^{n-1} \underbrace{\int_{\frac{I}{\phi P}}^{\infty} t^n e^{-t(1+\frac{1}{I})} \text{Ei}\left(\frac{-t}{I}\right) dt}_{\Xi_6} \\ &\quad + \sum_{k=1}^n (k-1)! (-1)^{n-k} I^k \Gamma(n-k+1, \frac{I}{\phi P}). \end{aligned} \quad (72)$$

For solving Ξ_6 , we distinguish between two cases:

1) When $I \neq 1$, Ξ_6 is evaluated using partial integration as

$$\int_{\frac{I}{\phi P}}^{\infty} u dv = \lim_{t \rightarrow \infty} uv - \lim_{t \rightarrow \frac{I}{\phi P}} uv - \int_{\frac{I}{\phi P}}^{\infty} v du. \quad (73)$$

First, let $u = \text{Ei}\left(\frac{-t}{I}\right)$ and $dv = t^n e^{-t(1+\frac{1}{I})} dt$. Thus, we have $du = t^{-1} e^{-\frac{t}{I}}$. Using [35, Eq. (2.321.2)], it can be shown that $v = e^{-t(1+\frac{1}{I})} \sum_{k=0}^n k! \binom{n}{k} (I-1)^{-k-1} I^{k+1} t^{n-k}$. Substituting these values in (73), we see that $\lim_{t \rightarrow \infty} uv = 0$. Thus, we get

$$\Xi_6 = \sum_{k=0}^n \frac{k! \binom{n}{k} \text{Ei}\left(\frac{-1}{\phi P}\right) I^{n-1} e^{\frac{1-I}{\phi P}}}{I^{1-n} (\phi P)^{n-k} (I-1)^{k+1}} + \sum_{k=0}^n \frac{k! \binom{n}{k} \Gamma(n-k, \frac{I}{\phi P})}{I^{1-k} (I-1)^{k+1}}. \quad (74)$$

2) When $I = 1$, Ξ_6 is derived in a similar way, which gives

$$\Xi_6 = -\frac{\left(\frac{I}{\phi P}\right)^{n+1} \text{Ei}\left(\frac{-I}{\phi P}\right) + \Gamma(n+1, \frac{I}{\phi P})}{(n+1)}. \quad (75)$$

Substituting for Ξ_6 , given in (74) and (75), into (72) and then (72) into (71), (19) is obtained, which completes the proof.

APPENDIX B PROOF OF LEMMA 2

Note that in (18), $\mathbf{H}_e$ has i.i.d. complex Gaussian entries and the matrix $[\hat{\mathbf{h}}_s \mathbf{W}]$ is unitary. Thus, the elements of the vector $\mathbf{H}_e \hat{\mathbf{h}}_s$ and the matrix $\mathbf{H}_e \mathbf{W}$ are i.i.d. complex Gaussian [19]. Therefore, from Proposition 1, we get

$$F_{\gamma_e^{\text{SB}}|Z_2}(\gamma) = 1 - \sum_{n=0}^{N_e-1} \frac{\binom{N_t-2}{n} \gamma^n \left(1 + \frac{q_{\text{SB}}}{u(Z_2)^n} \gamma\right)^{-N_t+2}}{q_{\text{SB}}^{-n} u(Z_2)^n}. \quad (76)$$

As in (71), the ergodic rate of the eavesdropper is derived as

$$C_e^{\text{SB}} = \frac{1}{\ln 2} \int_0^\infty \int_0^\infty \frac{1 - F_{\gamma_s^{\text{SB}}|\{Z_2=z_2\}}(\gamma)}{(1+\gamma)} e^{-z_2} d\gamma dz_2$$

$$= \sum_{n=0}^{N_e-1} \frac{\binom{N_t-2}{n}}{\ln 2 q_{\text{SB}}^{-n}} \underbrace{\int_0^\infty \int_0^\infty \frac{\gamma^n (1 + \frac{q_{\text{SB}}}{u(z_2)^n} \gamma)^{-N_t+2}}{u(z_2)^n (1+\gamma) e^{z_2}} d\gamma dz_2}_{\Xi_7} \quad (77)$$

In order to evaluate Ξ_7 , we distinguish between two cases; when $Z_2 \leq \frac{I}{\phi P}$, $u(Z_2) = \phi P$, and when $Z_2 > \frac{I}{\phi P}$, $u(Z_2) = \frac{I}{Z_2}$. As a result, Ξ_7 is calculated as follows

$$\Xi_7 = (\phi P)^{-n} \int_0^{\frac{I}{\phi P}} e^{-z_2} dz_2 \int_0^\infty \frac{\gamma^n (1 + \frac{q_{\text{SB}}}{\phi P} \gamma)^{-N_t+2}}{(1+\gamma)} d\gamma$$

$$+ I^{-n} \int_{\frac{I}{\phi P}}^\infty z_2^n e^{-z_2} \int_0^\infty \frac{\gamma^n (1 + \frac{q_{\text{SB}} z_2}{I} \gamma)^{-N_t+2}}{(1+\gamma)} d\gamma dz_2$$

$$= \theta(\phi P)^{-n} B(n+1, N_t - n - 2)$$

$$\times {}_2F_1(N_t - 2, n+1; N_t - 1; 1 - \frac{q_{\text{SB}}}{\phi P})$$

$$+ I^{-n} B(n+1, N_t - n - 2)$$

$$\times \int_{\frac{I}{\phi P}}^\infty \frac{z_2^n}{e^{z_2}} {}_2F_1(N_t - 2, n+1; N_t - 1; 1 - \frac{q_{\text{SB}}}{\phi P} z_2) dz_2. \quad (78)$$

In the first equality of (78), the second integral in each term is solved using [35, Eq. (3.227.1)]. Denoting the last integral as $\mathcal{J}_n(N_t, I, q_{\text{SB}})$, and substituting (78) in (77), (20) is obtained.

APPENDIX C PROOF OF LEMMA 4

As $\tilde{\mathbf{h}}_s$ is the projection of $\mathbf{h}_s$ on the null space of $\mathbf{h}_p$ and the matrix $[\hat{\mathbf{h}}_p \mathbf{W}]$ is unitary, the matrix $[\tilde{\mathbf{h}}_s \mathbf{W}]$ is also unitary. Using similar argument as in Appendix B, it can be shown that the elements of the vector $\mathbf{H}_e \tilde{\mathbf{h}}_s$ and the matrix $\mathbf{H}_e \mathbf{W}$ are i.i.d. complex Gaussian. Therefore, $F_{\gamma_e^{\text{PB}}}(\gamma)$ is given in (10), and hence, as in (71), the ergodic rate of the eavesdropper is derived as

$$C_e^{\text{PB}} = \sum_{n=0}^{N_e-1} \frac{\binom{N_t-2}{n} q_{\text{PB}}^n}{\ln 2 p_{\text{PB}}^n} \int_0^\infty \frac{\gamma^n (1 + \frac{q_{\text{PB}}}{p_{\text{PB}}} \gamma)^{-N_t+2}}{(1+\gamma)} d\gamma. \quad (79)$$

Solving the last integral using [35, Eq. (3.227.1)] gives (29).

APPENDIX D PROOF OF (37)

Recall that $\tilde{\mathbf{h}}_s = \mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s$ is the projection of $\mathbf{h}_s$ on the null space of $\mathbf{h}_p$. Therefore, $\mathbf{h}_s$ can be expressed as

$$\mathbf{h}_s = \mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s + \hat{\mathbf{h}}_p^\dagger \mathbf{h}_s \hat{\mathbf{h}}_p. \quad (80)$$

As $\tilde{\mathbf{h}}_s$ and $\mathbf{h}_p$ are orthogonal, it can be easily shown that

$$\|\mathbf{h}_s\|^2 = \|\mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s\|^2 + \|\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s \hat{\mathbf{h}}_p\|^2$$

$$= \|\mathbf{Q}^\dagger \mathbf{h}_s\|^2 + \|\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s\|^2. \quad (81)$$

On the other hand, substituting for $\mathbf{w}_{\text{CB}_1}$ from (31) into (34), we get

$$\gamma_{s_1}^{\text{CB}} = p_{\text{CB}} \frac{(\|\hat{\mathbf{h}}_p^\dagger \mathbf{h}_s\|^2 + \|\hat{\mathbf{h}}_s^\dagger \mathbf{h}_s\|^2)^2}{\|\mathbf{h}_s\|^2}. \quad (82)$$

Moreover, $\|\hat{\mathbf{h}}_s^\dagger \mathbf{h}_s\|^2 = \frac{\|(\mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s)^\dagger \mathbf{h}_s\|^2}{\|\mathbf{Q}\mathbf{Q}^\dagger \mathbf{h}_s\|^2} = \frac{\|\mathbf{Q}^\dagger \mathbf{h}_s\|^4}{\|\mathbf{Q}^\dagger \mathbf{h}_s\|^2} = \|\mathbf{Q}^\dagger \mathbf{h}_s\|^2$; substituting this result in (81) and then (81) into (82), (37) is obtained.

APPENDIX E PROOF OF LEMMA 5

The ergodic rate of the SU when $N_t \rightarrow \infty$ is derived as

$$C_{s,\infty}^{\text{SB}} = \frac{1}{\ln 2} \mathbb{E}[\ln(1 + \gamma_{s,\infty}^{\text{SB}})]$$

$$= \frac{1}{\ln 2} \left(\ln(1 + \phi P N_t) + \text{Ei}(\frac{-I}{\phi P}) - e^{IN_t} \text{Ei}(-IN_t - \frac{I}{\phi P}) \right). \quad (83)$$

Using Jensen's inequality, an upper bound on $C_{s,\infty}^{\text{SB}}$ is given as

$$\bar{C}_{e,\infty}^{\text{SB}} = \frac{1}{\ln 2} \ln \left(1 + \frac{\mathbb{E}[\min(\phi P, \frac{I}{Z_2})] \mathbb{E}[\|\mathbf{H}_e \hat{\mathbf{h}}_s\|^2]}{(1 - \phi)P} \right), \quad (84)$$

where the last equality is obtained because $\|\mathbf{H}_e \hat{\mathbf{h}}_s\|^2$ and Z_2 are independent. Note that $\|\mathbf{H}_e \hat{\mathbf{h}}_s\|^2 \sim \text{Gamma}(N_e, 1)$. Therefore, $\mathbb{E}[\|\mathbf{H}_e \hat{\mathbf{h}}_s\|^2] = N_e$. Also, we have

$$\mathbb{E}[\min(\phi P, \frac{I}{Z_2})] = \phi P \int_0^{\frac{I}{\phi P}} e^{-z_2} dz_2 + I \int_{\frac{I}{\phi P}}^\infty \frac{e^{-z_2}}{z_2} dz_2$$

$$= \phi P - \phi P e^{-\frac{I}{\phi P}} - I \text{Ei}(\frac{-I}{\phi P}). \quad (85)$$

Substituting (85) into (84) gives

$$\bar{C}_{e,\infty}^{\text{SB}} = \frac{1}{\ln 2} \ln \left(\frac{1 - \phi + N_e \phi - N_e \phi e^{-\frac{I}{\phi P}} - N_e \frac{I}{P} \text{Ei}(\frac{-I}{\phi P})}{1 - \phi} \right). \quad (86)$$

A lower bound on $C_{\text{sec},\infty}^{\text{SB}}$ is then given as

$$\underline{C}_{\text{sec},\infty}^{\text{SB}} = [C_{s,\infty}^{\text{SB}} - \bar{C}_{e,\infty}^{\text{SB}}]^+. \quad (87)$$

The optimal value of ϕ that maximizes the rate in (87) satisfies

$$\frac{\partial C_{s,\infty}^{\text{SB}}}{\partial \phi} - \frac{\partial \bar{C}_{e,\infty}^{\text{SB}}}{\partial \phi} = 0. \quad (88)$$

Differentiating both terms in (88) gives (47).

APPENDIX F PROOF OF LEMMA 6

Define $u(Z_2) \triangleq \min(\frac{I}{Z_2}, \phi P)$. Then, given Z_2 , $\gamma_s^{\text{SB}} = u(Z_2) \|\mathbf{h}_s\|^2 \sim \text{Gamma}(N_t, u(Z_2))$. The conditional CDF of γ_s^{SB} , $F_{\gamma_s^{\text{SB}}|Z_2}$, is obtained from (12) and the conditional PDF of γ_e^{SB} , $f_{\gamma_e^{\text{SB}}|Z_2}$, is obtained from (11). Substituting for $F_{\gamma_s^{\text{SB}}|Z_2}$ and $f_{\gamma_e^{\text{SB}}|Z_2}$ into (57), and expanding $\varepsilon(\gamma_e)^n = \sum_{k=0}^n \binom{n}{k} \gamma_e^k 2^{kR_s} (2^{R_s} - 1)^{n-k}$ using binomial theorem gives

$$\begin{aligned}
P_{out}^{SB} = & 1 - \sum_{n=0}^{N_t-1} \sum_{m=0}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} (N_t-2) q_{SB}^{m+1}}{n! (2R_s-1)^{k-n} 2^{-kR_s}} \\
& \times \underbrace{\int_0^\infty \int_0^\infty \frac{\gamma_e^{m+k} e^{-\frac{\varepsilon(\gamma_e)}{u(z_2)}} e^{-z_2}}{u(z_2)^{n+m+1} \left(1 + \frac{q_{SB}}{u(z_2)} \gamma_e\right)^{N_t-1}} d\gamma_e dz_2}_{\Xi_8} \\
& + \sum_{n=0}^{N_t-1} \sum_{m=1}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} m q_{SB}^m}{n! (2R_s-1) 2^{-kR_s}} \\
& \times \underbrace{\int_0^\infty \int_0^\infty \frac{\gamma_e^{m+k-1} e^{-\frac{\varepsilon(\gamma_e)}{u(z_2)}} e^{-z_2}}{u(z_2)^{n+m} \left(1 + \frac{q_{SB}}{u(z_2)} \gamma_e\right)^{N_t-2}} d\gamma_e dz_2}_{\Xi_9}. \quad (89)
\end{aligned}$$

Following similar steps as those for solving Ξ_7 yields

$$\begin{aligned}
\Xi_8 = & \frac{\theta(\phi P)^{k-n} e^{-\frac{2R_s-1}{\phi P}}}{q_{SB}^{m+k+1}} \int_0^\infty \frac{t^{m+k} e^{-\frac{2R_s}{q_{SB}} t}}{(1+t)^{N_t-1}} dt \\
& + \frac{I^{k-n}}{q_{SB}^{m+k+1}} \int_{\frac{I}{\phi P}}^\infty \frac{e^{-(1+\frac{2R_s-1}{I})z_2}}{z_2^{k-n}} dz_2 \int_0^\infty \frac{x^{m+k} e^{-\frac{2R_s}{q_{SB}} x}}{(1+x)^{N_t-1}} dx, \quad (90)
\end{aligned}$$

where [35, Eq. (3.381.3)], and [35, Eq. (9.211.4)] have been employed for solving (90). Ξ_9 is solved in a similar way. Substituting Ξ_8 and Ξ_9 into (89) yields (58).

APPENDIX G PROOF OF LEMMA 3

As $\gamma_s^{PB} \sim \text{Gamma}(N_t - 1, p_{PB})$, $F_{\gamma_s^{PB}}(\varepsilon(\gamma_e))$ is obtained from (12). Moreover, $f_{\gamma_e^{PB}}(\gamma_e)$ is given in (11). Substituting these expressions into (59), we get

$$\begin{aligned}
P_{out}^{PB} = & 1 - \sum_{n=0}^{N_t-2} \sum_{m=0}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} e^{-\frac{2R_s-1}{p_{PB}}} (N_t-2) q_{PB}^{m+1}}{n! p_{PB}^{n+m+1} 2^{-kR_s} (2R_s-1)^{k-n}} \\
& \times \int_0^\infty \gamma_e^{m+k} e^{-\frac{2R_s}{p_{PB}} \gamma_e} \left(1 + \frac{q_{PB}}{p_{PB}} \gamma_e\right)^{-N_t+1} d\gamma_e \\
& + \sum_{n=0}^{N_t-2} \sum_{m=1}^{N_e-1} \sum_{k=0}^n \frac{\binom{n}{k} \binom{N_t-2}{m} e^{-\frac{2R_s-1}{p_{PB}}} m q_{PB}^m}{n! p_{PB}^{n+m} 2^{-kR_s} (2R_s-1)^{k-n}} \\
& \times \int_0^\infty \gamma_e^{m+k-1} e^{-\frac{2R_s}{p_{PB}} \gamma_e} \left(1 + \frac{q_{PB}}{p_{PB}} \gamma_e\right)^{-N_t+2} d\gamma_e. \quad (91)
\end{aligned}$$

The two integrals in (91) can be solved by substituting $x = \frac{q_{PB}}{p_{PB}} \gamma_e$, and then using [35, Eq. (9.211.4)], which give (60).

REFERENCES

- [1] E. Biliary, A. Goldsmith, L. Greenstein, N. Mandayam, and H. V. Poor, *Principles of Cognitive Radio*. Cambridge University Press, 2013.
- [2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [3] A. Mukherjee, A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quarter 2014.
- [4] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.

- [5] N. Yang, L. Wang, G. Geraci, M. ElKashlan, J. Yuan, and M. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
- [6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Oct. 2007.
- [7] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.
- [8] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.
- [9] G. Geraci, A. Al-nahari, J. Yuan, and I. B. Collings, "Linear precoding for broadcast channels with confidential messages under transmit-side channel correlation," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1164–1167, Jun. 2013.
- [10] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.
- [11] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
- [12] A. Al-nahari, I. Krikidis, A. S. Ibrahim, M. I. Dessouky, and F. A. El-Samie, "Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers," *Trans. Emerging Tel. Tech (ETT)*, vol. 25, no. 4, pp. 445–460, Apr. 2014.
- [13] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," in *IEEE CrownCom*, May 2008.
- [14] Y. Pei, Y. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1592, Apr. 2010.
- [15] Y. Pei, Y. Liang, K. C. Teh, and K. H. Li, "Secure communication in multi-antenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.
- [16] Y. Zou, X. Wang, and W. Shen, "Physical layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, 2013.
- [17] M. ElKashlan, L. Wang, T. Q. Doung, and G. K. Karagiannis, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.
- [18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jul. 2008.
- [19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [20] N. Yang, M. ElKashlan, T. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.
- [21] C. Wang and H. Wang, "On the security throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.
- [22] J. Xiong, D. Ma, K. Wong, and J. Wei, "Robust masked beamforming for MISO cognitive radio networks with unknown eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 744–755, Feb. 2016.
- [23] T. L. Marzetta and B. M. Hochwald, "Fast transfer of channel state information in wireless systems," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1268–1278, Apr. 2006.
- [24] F. Gao, R. Zhang, Y. C. Liang, and X. Wang, "Design of learning-based MIMO cognitive radio systems," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1707–1720, May 2010.
- [25] G. Geraci, A. Garcia Rodriguez, D. Lopez-Perez, A. Bonfante, L. Galati Giordano, and H. Claussen, "Operating massive MIMO in unlicensed bands for enhanced coexistence and spatial reuse," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1282–1293, Jun. 2017.
- [26] J. Hoydis, K. Hosseini, S. T. Brink, and M. Debbah, "Making smart use of excess antennas: Massive MIMO, small cells, and TDD," *Bell Labs Tech. J.*, vol. 18, no. 2, pp. 5–21, Sep. 2013.
- [27] A. Garcia Rodriguez, G. Geraci, L. Galati Giordano, A. Bonfante, M. Ding, and D. Lopez-Perez, "Massive MIMO unlicensed: A new approach to dynamic spectrum access," *IEEE Commun. Magazine*, vol. PP, no. 99, pp. 1–7, Nov. 2017.
- [28] A. E. Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3871–3886, May 2017.
- [29] P. H. Lin, S. H. Lai, S. C. Lin, and H. J. Su, "On secrecy rate of the generalized artificial noise assisted secure beamforming for wiretap

channels,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

- [30] J. Zhu, R. Schober, and V. K. Bhargava, “Secure transmission in multicell massive MIMO systems,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4782, Sep. 2014.
- [31] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, “Artificial-noise-aided secure multi-antenna transmission with limited feedback,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, Jan. 2015.
- [32] A. Mukherjee and A. L. Swindlehurst, “Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
- [33] H. Gao, P. J. Smith, and M. V. Clark, “Theoretical reliability of MMSE linear diversity combining in rayleigh-fading additive interference channels,” *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.
- [34] D. B. da Costa and S. Aissa, “Cooperative dual-hop relaying systems with beamforming over Nakagami-m fading channels,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3950–3954, Aug. 2009.
- [35] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. Elsevier, 2007.
- [36] G. Alfano, A. Lozano, A. M. Tulino, and S. Verdu, “Mutual information of eigenvalue distribution of MIMO Ricean channels,” in *Int. Symp. On Inform. Theory and its Appl. (ISITA)*, Parma, Italy, Oct. 2004.
- [37] R. Zhang and Y. C. Liang, “Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks,” *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 88–102, Feb. 2008.
- [38] N. Jamal and P. Mitran, “Performance tradeoffs offered by beamforming in cognitive radio systems: an analytic approach,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3766–3777, Oct. 2012.

Azzam Al-nahari received the B. Sc. degree in electronic and communication engineering from the University of Technology, Iraq. He received the M. Sc. and Ph. D. degrees in electrical communications from the Faculty of Electronic Engineering, Menoufia University, Egypt in 2008, and 2011, respectively. During 2012, he had a postdoc position at the Department of Electrical and Information Technology, Lund University, Sweden. He had also a postdoc position at University at Buffalo, NY, USA in 2014. He is currently an Associate Professor at the Department of Electrical Engineering, Ibb University, Yemen.

His current research interests include massive MIMO systems, physical layer security, cognitive radio networks, and signal processing for wireless communications.

Giovanni Geraci (S’11, M’14) was born in Sicily, Italy. He received the B.Sc. and M.Sc. degrees in telecommunications engineering from Università di Palermo and Politecnico di Milano, Italy, in 2005 and 2009, respectively. He earned the Ph.D. degree in electrical engineering from the University of New South Wales, Australia, in 2014. Since 2016, Giovanni is a Research Scientist at Nokia Bell Labs, Ireland. Prior to joining Bell Labs, he was a Postdoctoral Fellow with the Singapore University of Technology and Design, Singapore, between

2014–2015. He has also held research appointments at the University of Texas at Austin, USA, in 2013, at Supélec, Gif-sur-Yvette, France, in 2012, and at Alcatel-Lucent, Vimercate, Italy, in 2009. His research interests cover various aspects of wireless communications, networking, and signal processing, currently focusing on heterogeneous networks, massive MIMO systems, unlicensed spectrum technologies, and UAV communications. Giovanni has published over 40 between book chapters, journal articles, and conference papers, all in recognized venues, and he is co-inventor of several patent applications on wireless communication networks.

Mukarram Al-jamali received the B. Sc. degree in Electronics and Telecommunications Engineering from Zagazig University, Egypt, in 2005. He received the M. Sc. degree in Communications Engineering from University of Science and Technology, Yemen. He is also working as a Lecturer Assistant at the Electronics Engineering Department, University of Science and Technology, Yemen. His research interests are wireless communications, cooperative communications, cognitive radio, and physical layer security.

Dr. Mohamed Hossam Ahmed obtained his Ph.D. degree in Electrical Engineering in 2001 from Carleton University, Ottawa, where he worked from 2001 to 2003 as a senior research associate. In 2003, he joined the Faculty of Engineering and Applied Science, Memorial University where he works currently as a Full Professor. Dr. Ahmed published more than 140 papers in international journals and conferences. He serves as an Editor for IEEE Communication Surveys and Tutorials and as an Associate Editor for Wiley International

Journal of Communication Systems and Wiley Communication and Mobile Computing (WCMC). He served as a Guest Editor of a special issue on Fairness of Radio Resource Allocation, EURASIP JWCN in 2009, and as a Guest Editor of a special issue on Radio Resource Management in Wireless Internet, Wiley Wireless and Mobile Computing Journal, 2003. Dr. Ahmed is a Senior Member of the IEEE. He served as a cochair of the Signal Processing Track in ISSPIT’14 and served as a cochair of the Transmission Technologies Track in VTC’10-Fall, and the multimedia and signal processing symposium in CCECE’09. Dr. Ahmed won the Ontario Graduate Scholarship for Science and Technology in 1997, the Ontario Graduate Scholarship in 1998, 1999, and 2000, and the Communication and Information Technology Ontario (CITO) graduate award in 2000. His research interests include radio resource management in wireless networks, multi-hop relaying, cooperative communication, vehicular ad-hoc networks, cognitive radio networks, and wireless sensor networks. Dr. Ahmed’s research is sponsored by NSERC, CFI, QNRF, Bell/Aliant and other governmental and industrial agencies. Dr. Ahmed is a registered Professional Engineer (P.Eng.) in the province of Newfoundland, Canada.

Nan Yang (S’09–M’11) received the B.S. degree in electronics from China Agricultural University in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He has been with the Research School of Engineering at the Australian National University since July 2014, where he currently works as a Future Engineering Research Leadership Fellow and a Senior Lecturer. Prior to this, he was a Postdoctoral Research Fellow at the University of New South Wales (2012–2014)

and a Postdoctoral Research Fellow at the Commonwealth Scientific and Industrial Research Organization (2010–2012). He received the Exemplary Reviewer Award of the IEEE TRANSACTIONS ON COMMUNICATIONS in 2015 and 2016, the Top Reviewer Award from the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2015, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award and the Exemplary Reviewer Award of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2014, and the Exemplary Reviewer Award of the IEEE COMMUNICATIONS LETTERS in 2013 and 2012. He is also a co-recipient of the Best Paper Awards from the IEEE GlobeCOM 2016 and the IEEE VTC 2013-Spring. He is currently serving in the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. His general research interests lie in the areas of communications theory and signal processing, with specific interests in massive multi-antenna systems, millimeter wave communications, ultra-reliable low latency communications, cyber-physical security, and molecular communications.