Al-nahari, Azzam; Jantti, Riku; Zheng, Gan; Mishra, Deepak; Nie, Mingcheng

Ergodic Secrecy Rate Analysis and Optimal Power Allocation for Symbiotic Radio Networks

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2023.3301186

Published: 01/01/2023

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 July 2023, accepted 26 July 2023, date of publication 2 August 2023, date of current version 9 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3301186

RESEARCH ARTICLE

Ergodic Secrecy Rate Analysis and Optimal Power Allocation for Symbiotic Radio Networks

AZZAM AL-NAHARI[1,2], RIKU JÄNTTI[1], (Senior Member, IEEE), GAN ZHENG[3], DEEPAK MISHRA[4], (Senior Member, IEEE), AND MINGCHENG NIE[4], (Graduate Student Member, IEEE)

[1]Department of Information and Communications Engineering, Aalto University, 02150 Espoo, Finland
[2]Department of Electrical Engineering, Ibb University, Ibb, Yemen
[3]School of Engineering, University of Warwick, CV4 7AL Coventry, U.K.
[4]School of Electrical Engineering and Telecommunications (EET), University of New South Wales (UNSW), Sydney, NSW 2052, Australia

Corresponding author: Azzam Al-Nahari (azzam.al-nahari@aalto.fi)

This work was supported in part by the European Union. The work of Deepak Mishra was supported in part by the Australian Research Council Discovery Early Career Award (DECRA) under Grant DE230101391.

ABSTRACT In this paper, we address the challenge of establishing secure communication within a symbiotic radio (SR) network. This network comprises a primary transmitter (PT), a primary receiver (PR), a passive backscatter device (BD), and an eavesdropper (ED) attempting to intercept the BD's transmitted information signal. The PT simultaneously transmits an information-bearing signal to the PR and artificial noise (AN) to confound the ED. The objective is that the BD conveys confidential information to the PR by leveraging the PT's signal. The PR performs joint decoding of both the symbols transmitted by the PT and the BD. In this system configuration, we derive a closed-form expression for the ergodic secrecy rate of the BD, providing an analytical framework for evaluating its security performance. Furthermore, we derive an expression for the secrecy rate in the asymptotic regime characterized by a large number of transmit antennas. These derived expressions allow us to optimize both the reflection coefficient and power allocation factor, enabling the maximization of the BD's ergodic secrecy rate while considering the quality of service (QoS) requirements of the primary system. The derived analytical results provide valuable insights into the influence of key system parameters on the secrecy performance. Notably, the derived analytical results quantify the effect of key system parameters on the secrecy performance. In particular, we show that the using AN can always improve the secrecy rate given the QoS constraints of the primary user. Moreover, we show that the secrecy rate can be improved by increasing the reflection coefficient at the BD even with better channel condition for the ED than the legitimate link.

INDEX TERMS Symbiotic radio, physical layer security, artificial noise, ergodic secrecy rate.

I. INTRODUCTION

Backscatter communications have emerged as promising solutions for future energy-efficient and low-cost Internet of Things (IoT) devices [1], [2]. These communication systems can be categorized into three main types: monostatic, bistatic, and ambient backscattering [3]. Among these, ambient backscatter communication (AmBC) has gained significant attention as an emerging technology that supports energy-efficient IoT applications [4]. In AmBC, a backscatter device (BD) transmits its own message by modulating and backscattering the radio frequency (RF) signals emitted by existing legacy communication systems like cellular and WiFi networks. As a result, AmBC offers key advantages such as energy efficiency, low cost, and spectrum efficiency, making it an attractive choice for IoT deployments. However, the main problem with AmBC is the presence of strong interference path at the AmBC receiver. To overcome this problem, a cooperative receiver is proposed to cancel the direct-line interference [5], or to jointly decode the

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

backscattered signal and the signal of the primary user [6]. The analysis in [7] investigated the achievable sum rate of a system comprising both a legacy system and a backscatter communication system, both featuring multiple antennas. In this scenario, the primary transmitter (PT) device employs the Gaussian codebook, while the backscatter device (BD) utilizes either the Gaussian codebook or the Wyner polyphase coding.

Recently, symbiotic radio (SR), a novel technology that combines the advantages of AmBC and cognitive radio (CR), has gained significant attention as a solution for achieving spectrum-efficient, energy-efficient, and cost-effective communications [8], [9], [10]. In SR, the backscatter transmission operates in a parasitic manner alongside the primary transmission. The PT utilizes transmit beamforming techniques to enable the realization of achievable rates for both the primary system and the backscatter transmissions. Similar to CR systems, SR achieves spectrum sharing communication with coexistence of primary and secondary systems without causing interference to the primary system as in CR systems. On the other hand, compared to the ambient backscattering, SR achieves highly reliable backscattering communications through joint decoding.

Securing backscatter communication systems presents significant design challenges due to the potential for malicious attacks, which can result in data interception and privacy breaches [11]. In particular, several practical limitations related to size, cost, and computation impose challenges when securing backscatter communication systems. Accordingly, the conventional cryptography methods are not well-suited for this paradigm. Instead, physical layer security is considered a promising approach to achieve perfect secrecy. Existing literature offers various techniques to secure backscatter communication systems [11], [12], [13], [14], [15], [16]. In [11], an artificial noise (AN) injection scheme was proposed to enhance the physical layer security of monostatic backscatter system. Optimal tag selection schemes were proposed in [12] and [13] to enhance transmission security. The work in [14] investigated AN-assisted multiple-input-multiple-output (MIMO) system to safeguard the radio frequency identification (RFID) systems.

Different from the above mentioned works, [15] and [16] considered cooperative receiver for joint decoding of the BD signal in addition to the main signal. In [15], the authors presented a beamforming design that aims to maximize the secrecy rate while considering outage constraints in non-orthogonal multiple access (NOMA) SR networks. This design assumes that the transmitter possesses knowledge of the channel state information (CSI) for the eavesdropper at its side. In [16], the authors conducted a secrecy outage probability analysis of cognitive AmBC communication system in which a secondary user and BD send signals to legitimate receiver considering underlay CR constraint. Our work is different from [16] as in our work the primary system shares the power and spectrum resources with the BD and joint decoding is applied at the primary receiver. In addition, we propose an AN-assisted transmission scheme for enhancing the ergodic secrecy rate. Therefore, to the best of our knowledge, this is first work that considers AN-assisted physical layer security in SR systems.

In this paper, we investigate securing backscatter transmissions in the SR paradigm, where the BD send its information to the primary receiver (PR) by modulating the PT signal, while keeping it secret from a passive eavesdropper (ED) who is trying to decode the information sent from the BD. This paper focuses on a scenario where the CSI of the eavesdropper is unknown to both the legitimate transmitters and the receiver. In order to maintain the quality of service (QoS) for the primary system, a minimum average signal-to-noise ratio (SNR) is guaranteed. In this context, our goal is to optimize the reflection coefficient of the BD and the power allocation for the confidential and jamming signals to maximize the ergodic secrecy rate of the BD transmissions, while ensuring the QoS cobnstraint of the primary system. The key contributions of this paper are outlined below:

1) We propose a new AN-assisted secure transmission scheme for SR systems, in which the backscattered signal is protected against eavesdropping, where the PT and the BD send and reflect signals to the PR, respectively. A passive eavesdropping scenario is assumed, where only the statistical CSI of the eavesdropper's channel is available to the PT.
2) We derive an analytical expression for the achievable ergodic secrecy rate of the BD within the SR system framework. Additionally, we perform an asymptotic analysis of the ergodic secrecy rate when the number of transmit antennas at the PT is very large. These derived expressions significantly reduce the complexity involved in system design and analysis.
3) We introduce an optimization problem for finding the optimal power allocation and the optimal reflection coefficient that maximize the ergodic secrecy rate of the BD, taking into account the average SNR constraint at the primary system.

The subsequent sections of the paper are organized as follows: Section II introduces the system and channel models. In Section III, we derive the expression for the ergodic secrecy rate. Section IV presents the optimization problem, which aims to maximize the ergodic secrecy rate discussed in Section III. The numerical results are presented in Section V, and finally, Section VI draws conclusions based on the findings.

Notations : $\mathbb{E}[.]$ denotes the expectation operation, $\hat{\mathbf{h}} \triangleq \frac{\mathbf{h}}{\|\mathbf{h}\|}$, and $[x]^+ \triangleq \max(0, x)$. $\mathbf{I}_n$ and $\mathbf{0}_n$denote an $n \times n$ identity matrix, and a vector of length n and zero entries, respectively. $\mathbf{h}^{\mathrm{T}}$ and $\mathbf{h}^{\dagger}$ denote the transpose and conjugate transpose of $\mathbf{h}$, respectively. $\mathbf{x} \sim \mathcal{CN}(\mathbf{0}_N, \Sigma)$ denotes a complex Gaussian distributed random vector $\mathbf{x} \in \mathbb{C}^{N\times 1}$ with zero-mean and covariance matrix Σ. $X \sim \mathrm{Gamma}(\alpha, \beta)$ denotes the Gamma distributed random variable with parameters α and β, and $Y \sim \exp(\lambda)$ denotes the exponentially distributed random variable with parameter λ.

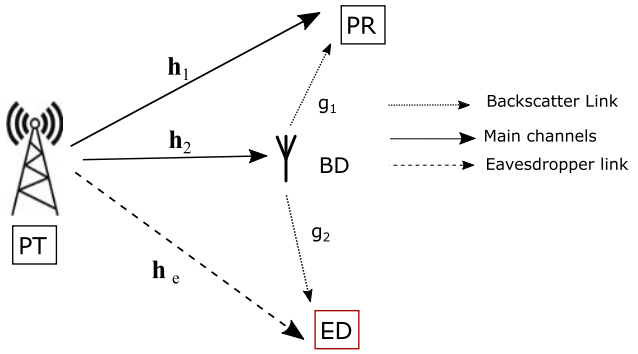


FIGURE 1. Illustration of an SR network which consists of an PT, an PR, an BD that backscatters its information to the PR, and an eavesdropper intercepts the information of the BD.

II. SYSTEM MODEL

We consider a SR network as shown in Fig. 1, which consists of a PT with N_t antennas, a single-antenna PR, a single-antenna BD, and a single-antenna ED. We assume a practical scenario, where the eavesdropper's CSI is completely unknown at the legitimate nodes. As shown in the figure, $\mathbf{h}_1 \in \mathbb{C}^{N_t\times 1}$, $\mathbf{h}_2 \in \mathbb{C}^{N_t\times 1}$, and $\mathbf{h}_e \in \mathbb{C}^{N_t\times 1}$ denote the transmission channel vectors for the PT-PR, PT-BD, and PT-ED links, respectively. We assume that $\mathbf{h}_1 \sim \mathcal{CN}(\mathbf{0}_{N_t}, \Omega_1\mathbf{I}_{N_t})$, $\mathbf{h}_2 \sim \mathcal{CN}(\mathbf{0}_{N_t}, \Omega_2\mathbf{I}_{N_t})$, and $\mathbf{h}_e \sim \mathcal{CN}(\mathbf{0}_{N_t}, \Omega_e\mathbf{I}_{N_t})$.

In this paper, the CSI of the legitimate links, $\mathbf{h}_1$ and $\mathbf{h}_2$, are assumed to be available at the transmitter side [8], [17], [18]. In practical scenarios, in time division duplexing (TDD) systems, the reciprocity of uplink and downlink channels allows the transmitter to estimate the downlink channel by utilizing uplink channel sounding. Under the assumption of TDD transmission, $\mathbf{h}_1$ can be obtained at the PT through a pilot signal transmitted by the PR. Moreover, $\mathbf{h}_2$ can be estimated at the PT as described in [8].

The PT transmits information symbol $s(n)$ with symbol period T_s to the PR. We employ a unit-norm beamforming vector $\mathbf{w} \in \mathbb{C}^{N_t\times 1}$ for transmitting the signal $s(n)$. Since the CSI of the ED is not known at the PT, the remaining degrees of freedom are utilized to send AN to degrade the channel of the ED link. Our aim is to design AN-aided precoding so that the AN is eliminated at both the PR and the BD. Therefore, the PT uses $N_t - 2$ degrees of freedom for transmitting AN vector $\mathbf{z} = [z_1\, z_2 \ldots z_{N_t-2}]^T \sim \mathcal{CN}\big(\mathbf{0}_{N_t-2}, \mathbf{I}_{N_t-2}\big)$, where the vector $\mathbf{z}$ is multiplied by a precoding matrix $\mathbf{W} = [\mathbf{w}_1\mathbf{w}_2 \ldots\ldots \mathbf{w}_{N_t-2}] \in \mathbb{C}^{N_t\times(N_t-2)}$, where $\|\mathbf{w}_i\| = 1, \forall i$. In other words, the precoding matrix $\mathbf{W}$ is designed to lie in the null space of both $\mathbf{h}_1$ and $\mathbf{h}_2$. Therefore, the columns of the matrix $\mathbf{W}$ are designed to form orthonormal basis with $\mathbf{h}_1$ and $\mathbf{h}_2$ and hence the matrix $\mathbf{W}$ must has at most $N_t - 2$ columns. This illustrates why $N_t - 2$ degrees of freedoms are used for transmitting the AN signal. As a result, we get $\mathbf{h}_1^\dagger\mathbf{W} = \mathbf{0}_{N_t-2}^T$ and $\mathbf{h}_2^\dagger\mathbf{W} = \mathbf{0}_{N_t-2}^T$. Using this technique, the AN will degrade the eavesdropper link but not the legitimate links [19], [20]. Moreover, it facilitates deriving simple and insightful secrecy rate expressions. Note also that in the considered system setup, as $N_t - 2$ degrees of freedom are used for transmitting AN signal, we assume that $N_t > 2$. Meanwhile, the BD transmits a signal $\sqrt{\alpha}c$ with symbol period T_c, where c denotes the information signal of the BD and $0 \le \alpha \le \alpha_{max}$ denotes the reflection coefficient. The BD conveys its information by modulating the primary signal, and the resultant reflected signal represents the product of the two signals [21]. We assume that both $s(n)$ and c are distributed as a standard circularly symmetric complex Gaussian distribution with zero mean and unit variance.[1] We assume that the symbol period of the BD spans N consecutive symbols period of the primary system, i.e. $T_c = NT_s$, and in this paper, we consider $N \gg 1$.[2] The PT constructs the transmitted signal as the sum of information signal and the jamming signal as follows

$$\begin{aligned}\mathbf{x} &= \sqrt{p}\mathbf{w}s(n) + \sqrt{q}\mathbf{W}\mathbf{z} \\ &= \sqrt{p}\mathbf{w}s(n) + \sqrt{q}\sum_{i=1}^{N_t-2}\mathbf{w}_i z_i, \end{aligned} \tag{1}$$

where p and q denote the transmit power of the information signal and each AN signal, respectively. Moreover, the total transmit power budget is constrained such that $\mathbb{E}[\|\mathbf{x}\|^2] = P$.

Let $0 < \phi < 1$ denotes the power allocation factor that is dedicated for transmitting the information signal.[3] Therefore, the power devoted to transmit the information signals is ϕP and the total power devoted for AN signals is $(1-\phi)P$. As we have $N_t - 2$ noise signals $\mathbf{z} = [z_1\, z_2 \ldots z_{N_t-2}]^T$, then the total transmit power budget is given as $p + (N_t - 2)q = P$. As the CSI of the eavesdropper is not known at the transmitter side, we assume uniform power allocation between the AN signals. Thus, the transmitted powers p and q can be given as

$$p = \phi P, \tag{2}$$

$$q = \frac{(1-\phi)P}{N_t - 2}. \tag{3}$$

Therefore, the received signal at the PR is given as

$$y_p(n) = \sqrt{p}\mathbf{h}_1^\dagger\mathbf{w}s(n) + \sqrt{\alpha p}g_1 c\mathbf{h}_2^\dagger\mathbf{w}s(n) + n_p, \tag{4}$$

where the first term in the right-hand side of (4) is the direct-link signal and the second term represents the signal backscattered from the BD; g_1 is the channel coefficient of the BD-PR link, which is assumed to be a line-of-sight

[1] The standard Shannon capacity formula used in this paper assumes that the BD uses a Gaussian codebook with constrained mean reflected power α, as in [8], [22] and [23]. This can be achieved assuming that the BD incorporates a reflection amplifier as studied in [24].

[2] The case where $N \gg 1$, commonly referred as commensal setup, is more practical than parasitic setup where $N = 1$. This is because, in practice, the transmission rate of the backscattering link is much lower than the transmission rate of the primary system.

[3] In this paper, we have assumed the worst-case scenario with zero noise at the eavesdropper. Therefore, when all power is devoted to the information signal transmission, i.e., $\phi = 1$, the rate at the eavesdropper's side is infinity and hence the secrecy rate is zero. Therefore, the power split ratio is chosen to be in the range $0 < \phi < 1$.

(LoS) channel with a constant large scale path loss [8], and $n_p \sim \mathcal{CN}(0, \sigma_p^2)$ represents the additive white Gaussian noise (AWGN) at PR. Similarly, the received signals at the ED is given as

$$\hat{y}_e(n) = \sqrt{p}\mathbf{h}_e^\dagger \mathbf{w} s(n) + \sqrt{\alpha p} c g_2 \mathbf{h}_2^\dagger \mathbf{w} s(n) + \sqrt{q}\sum_{i=1}^{N_t-2} \mathbf{h}_e^\dagger \mathbf{w}_i z_i + n_e, \quad (5)$$

where g_2 is the channel coefficient of the BD-ED link, and $n_e \sim \mathcal{CN}(0, \sigma_e^2)$. Considering the fact that the noise at the ED is unknown random variable, we assume the worst-case scenario, where the noise is equal to zero, i.e., $n_e \to 0$ [20], [25]. The ED can use the first term in (5), which represents the primary user signal $s(n)$ as an interference and decode the BD signal. However, as our focus in this paper is to secure the BD transmissions, as a worst case scenario, the ED can use successful interference cancellation (SIC) technique to decode the primary user signal $s(n)$ first and then remove this signal from the received signal. By utilizing this SIC technique, the eavesdropper can achieve a higher SNR at their end, resulting in an increased achievable rate compared to treating the primary user signal as interference. Consequently, this worst-case scenario serves as an upper bound for the eavesdropper's capabilities and a lower bound for the secrecy rate. Therefore, the received signal at the ED receiver is given as

$$y_e(n) = \sqrt{\alpha p} c g_2 \mathbf{h}_2^\dagger \mathbf{w} s(n) + \sqrt{q}\sum_{i=1}^{N_t-2} \mathbf{h}_e^\dagger \mathbf{w}_i z_i \quad (6)$$

III. ERGODIC SECRECY RATE ANALYSIS

In this section, we investigate the secrecy performance of the transmission schemes introduced in Section II. The ergodic secrecy capacity is defined as the maximum average rate of the confidential information sent from the transmitter to the receiver, and below which any average transmission rate is considered achievable secrecy rate. In the following, we derive the achievable ergodic secrecy rate of the BD. Note that such a secure transmission rate is achieved by the coding schemes where codewords span many different channel fading conditions. Therefore, ergodic secrecy rate is commonly considered a suitable performance metric for fast fading channel conditions.

First, we derive the received SNRs and the achievable ergodic rates at different nodes. As our purpose is to maximize the ergodic secrecy rate of the BD for a given average SNR constraint for the primary system, the transmit beamforming vector $\mathbf{w}$ is chosen to match the PT-BD channel, i.e, $\mathbf{w} = \hat{\mathbf{h}}_2$. From (4), when decoding $s(n)$, as the data rate of the BD is far lower than the transmission rate of the primary system, signal in the backscattering path can be treated as a useful multipath component. Hence, the equivalent effective channel that is used for decoding the primary system signal $s(n)$ is $\mathbf{h}_1 + \sqrt{\alpha} g_1 c \mathbf{h}_2$. As the BD signal c is not known at the PR in advance, non-coherent detection of $s(n)$ is required. However, when $N \gg 1$, non-coherent achievable rate can be approximated as coherent achievable rate [8] and thus, the received SNR of the primary link for a given BD signal c is given as

$$\gamma_{s|c} = \frac{p\left|(\mathbf{h}_1 + \sqrt{\alpha} c g_1 \mathbf{h}_2)^\dagger \hat{\mathbf{h}}_2\right|^2}{\sigma_p^2}. \quad (7)$$

In this paper, we consider average SNR constraint for the primary user and focus on the analysis of the ergodic secrecy rate of the secondary backscatter system and the optimal power allocation. Thus, as $c \sim \mathcal{CN}(0, 1)$, the primary SNR averaged over c is given as

$$\gamma_s = \frac{p\left|\mathbf{h}_1^\dagger \hat{\mathbf{h}}_2\right|^2 + p\alpha\left|g_1\right|^2 ||\mathbf{h}_2||^2}{\sigma_p^2}. \quad (8)$$

The ergodic rate of primary system is thus given as

$$R_s = \mathbb{E}\Big[\log_2\big(1 + \gamma_s\big)\Big]. \quad (9)$$

The following lemma gives closed-form expression for R_s.

Lemma 1: The ergodic rate of the primary user is given as

$$R_s = \frac{-e^{\lambda}\mathrm{Ei}(-\lambda)}{\ln(2)(1 - \frac{\Omega_2}{\Omega_1}\alpha\left|g_1\right|^2)^{N_t}}, \quad (10)$$

where Ei(.) *is the exponential integral* [26, Eq. (8.211.1)], *and* $\lambda \triangleq \frac{\sigma_p^2}{p\Omega_1}$.

Proof: See Appendix I ∎

Note from (10) that, as $\lambda > 0$, $\lim_{\lambda\to\infty} -e^{\lambda}\mathrm{Ei}(-\lambda) = 0$ and hence the achievable rate of the primary user R_s is decreasing in λ. Thus, R_s is increasing in ϕ. Moreover, R_s is increasing in α. Therefore, R_s exhibits an increase with respect to both ϕ and α. However, our primary goal is to maximize the secrecy rate of the BD. Hence, the optimization of variables ϕ and α is aimed at achieving the maximum secrecy rate of the BD while simultaneously upholding a predetermined value for average SNR of the primary system, as will be described in the next section.

Now, we determine the SNR of the BD signal. After decoding $s(n)$, the successive interference cancellation (SIC) technique is used at the cooperative receiver to remove this signal. Let $\mathbf{s} = [s(1), s(2), \ldots, s(N)]^{\mathrm{T}}$ denotes the vector of the transmitted information symbols of the PT during one BD symbol period. Thus, the received signal vector at the PR during one symbol duration of the BD, after removing the decoded signals of the primary user, can be written as

$$\hat{\mathbf{y}}_p = \sqrt{\alpha p} g_1 ||\mathbf{h}_2||^2 \mathbf{s} c + \mathbf{n}_p. \quad (11)$$

Then, for a given $\mathbf{s}$, we perform maximum ratio combining (MRC) for decoding c and the resulting SNR is given as

$$\gamma_{c|\mathbf{s}} = \frac{p\alpha\left|g_1\right|^2 \left\|\mathbf{h}_2\right\|^2 \left\|\mathbf{s}\right\|^2}{\sigma_p^2}. \quad (12)$$

As the BD transmits only one symbol during N successive symbols of the primary system, the achievable rate of BD transmission is given as

$$\hat{R}_c = \frac{1}{N}\mathbb{E}_{\mathbf{s}}\Big[\log_2\big(1+\gamma_{c|\mathbf{s}}\big)\Big], \tag{13}$$

where the expectation is taken over $\mathbf{s}$. The rate $\hat{R}_c$ in (13) is mathematically intractable. However, from (12) and in commensal setup where $N \gg 1$, as $\mathbb{E}[s(n)] = 1$, the SNR at the PR for decoding the BD symbol c using MRC can be well-approximated as [8] and [21]

$$\gamma_c = \frac{p\alpha N\big|g_1\big|^2||\mathbf{h}_2||^2}{\sigma_p^2}. \tag{14}$$

Thus, the ergodic rate of the BD is given as

$$R_c = \frac{1}{N}\mathbb{E}\Big[\log_2\big(1+\gamma_c\big)\Big]. \tag{15}$$

The following lemma provides closed-form expression for R_c.

Lemma 2: The ergodic rate of the BD is given as

$$R_c = \frac{1}{N\ln(2)}e^{\frac{1}{\beta_1}}\sum_{k=1}^{N_t}E_{N_t-k+1}\Big(\frac{1}{\beta_1}\Big), \tag{16}$$

where $\beta_1 \triangleq \frac{p}{\sigma_p^2}\alpha N\big|g_1\big|^2\Omega_2$, *and* $E_n(.)$ *is the generalized exponential integral of order* n [27, Eq. (11)].

Proof: Note that $\gamma_c = \frac{p}{\sigma_p^2}\alpha N\big|g_1\big|^2\big\|\mathbf{h}_2\big\|^2 \sim$ Gamma $(N_t, \frac{p}{\sigma_p^2}\alpha N\big|g_1\big|^2\Omega_2 \triangleq \beta_1)$. Thus, R_c is calculated as

$$\begin{aligned} R_c &= \frac{1}{N\ln 2}\mathbb{E}\big[\ln(1+\gamma_c)\big] \\ &= \frac{1}{N\ln(2)\beta_1^{N_t}(N_t-1)!}\int_0^\infty \ln(1+\gamma)\gamma^{N_t-1}e^{-\frac{\gamma}{\beta_1}}d\gamma. \end{aligned}$$

Using the identity given in [28, Appendix A3], the integral in the previous equation can be solved, and hence (16) is obtained. ∎

Following similar procedure as that for obtaining (12) and (13), the SNR and the achievable rate at the ED are, respectively, given as

$$\gamma_{e|\mathbf{s}} = \frac{p\alpha N\big|g_2\big|^2||\mathbf{h}_2||^2\big\|\mathbf{s}\big\|^2}{q\sum_{i=1}^{N_t-2}\big|\mathbf{h}_e^\dagger\mathbf{w}_i\big|^2}, \tag{17}$$

$$\hat{R}_e = \frac{1}{N}\mathbb{E}_{\mathbf{s}}\Big[\log_2\big(1+\gamma_{e|\mathbf{s}}\big)\Big]. \tag{18}$$

When $N \gg 1$, the SNR and the ergodic rate of ED are given as

$$\gamma_e = \frac{p\alpha N\big|g_2\big|^2||\mathbf{h}_2||^2}{q\sum_{i=1}^{N_t-2}\big|\mathbf{h}_e^\dagger\mathbf{w}_i\big|^2}, \tag{19}$$

$$R_e = \frac{1}{N}\mathbb{E}\Big[\log_2\big(1+\gamma_e\big)\Big]. \tag{20}$$

The following lemma provides closed-form expression for R_e.

Lemma 3: The ergodic rate of the ED is given as

$$\begin{aligned} R_e = \frac{1}{N\ln(2)}\sum_{n=0}^{N_t-1}\frac{1}{(N_t+n-2)}\Big(\frac{\beta_3}{\beta_2}\Big)^n \\ \times\ {}_2F_1\Big(N_t+n-2, n+1; N_t+n-1; 1-\frac{\beta_3}{\beta_2}\Big), \end{aligned} \tag{21}$$

where ${}_2F_1(a,b;c;z)$ *is the Gauss hypergeometric function,* $\beta_2 \triangleq \alpha pN\big|g_2\big|^2\Omega_2$, *and* $\beta_3 \triangleq q\Omega_e$.

Proof: See Appendix II. ∎

Now, given an ergodic secrecy capacity C_{sec}, as $c \sim \mathcal{CN}(0,1)$, an achievable ergodic secrecy rate R_{sec}, which is a lower bound on C_{sec}, can be given as [25] and [29]

$$C_{sec} \geq R_{sec} = [R_c - R_e]^+, \tag{22}$$

To this end, combining (16), (21), and (22), we get a closed-form expression for the ergodic secrecy rate of the secondary backscatter communication system.

IV. JOINT OPTIMIZATION OF POWER ALLOCATION AND REFLECTION COEFFICIENT

In this section, we address the problem of maximizing the ergodic secrecy rate given in (22) by joint optimization of the power allocation at the PT and the reflection coefficient of the BD. First, the optimization problem is formulated and accordingly, its feasible condition and the optimal reflection coefficient are determined. Then, we derive asymptotic expression for the secrecy rate, where the number of transmit antennas increases without bound, and accordingly, we derive the optimal power allocation factor ϕ. The utilization of the large-antennas approximation proves particularly advantageous in scenarios involving massive MIMO deployment. A study [30] demonstrates that incorporating a large number of antenna elements at the transmitter side can significantly enhance the spectral and energy efficiency of backscatter communication systems. Furthermore, the subsequent subsections will present concise asymptotic analytical results that provide valuable insights into the impact of system parameters on performance. For instance, leveraging these derived asymptotic results, we will investigate the conditions required to achieve a positive secrecy rate.

A. PROBLEM FORMULATION, FEASIBLE CONDITION, AND OPTIMAL REFLECTION COEFFICIENT

In the following optimization problem, our objective is to maximize the ergodic secrecy rate by jointly optimizing the power allocation factor and the reflection coefficient of the BD as follows

$$\begin{aligned} \mathbf{P1}: \max_{\phi,\alpha}\quad & R_{sec} = [R_c - R_e]^+ \\ s.t.\quad & \bar{\gamma}_s \geq \gamma_s^{th} && (23)\\ & 0 < \phi < 1 && (24)\\ & 0 \leq \alpha \leq \alpha_{max} && (25) \end{aligned}$$

where the constraint (23) ensures a minimum predefined average SNR $\bar{\gamma}_s$ for the primary signal,[4] which is given as

$$\begin{aligned}\bar{\gamma}_s &= \mathbb{E}[\gamma_s] \\ &= \frac{\phi P \mathbb{E}\Big[\big|\mathbf{h}_1^\dagger \hat{\mathbf{h}}_2\big|^2\Big] + \phi P \alpha \big|g_1\big|^2 \mathbb{E}\Big[||\mathbf{h}_2||^2\Big]}{\sigma_p^2} \\ &= \frac{\phi P \Omega_1 + \phi \alpha P \big|g_1\big|^2 N_t \Omega_2}{\sigma_p^2}, \end{aligned} \tag{26}$$

where the last equation is obtained as $\big|\mathbf{h}_1^\dagger \hat{\mathbf{h}}_2\big|^2 \sim \exp\big(\frac{1}{\Omega_1}\big)$ and $||\mathbf{h}_2||^2 \sim \text{Gamma}(N_t, \Omega_2)$. Before solving **P1**, we investigate its feasible condition. As γ_s^{th} is a system parameter to be set, we find the maximum feasible value of γ_s^{th}, which is denoted as $\gamma_{s,max}^{th}$, so that the constraints in (23)-(25) are met and thus **P1** is feasible. The maximum feasible threshold $\gamma_{s,max}^{th}$ can be obtained by substituting $\phi = 1$ and $\alpha = \alpha_{max}$ in (26). Therefore, **P1** is feasible if $\gamma_s^{th} < \frac{P\Omega_1 + \alpha_{max} P |g_1|^2 N_t \Omega_2}{\sigma_p^2} \triangleq \gamma_{s,max}^{th}$.

Note that, using (26), the constraints (23) and (24) can be combined into one constraint, and therefore, **P1** can be reformulated as follows

$$\mathbf{P2}: \max_{\phi,\alpha} \; R_{sec} = [R_c - R_e]^+$$

$$s.t. \quad \kappa \le \phi < 1 \tag{27}$$

$$0 \le \alpha \le \alpha_{max} \tag{28}$$

where $\kappa \triangleq \frac{\gamma_s^{th}}{(P\Omega_1 + \alpha P |g_1|^2 N_t \Omega_2)/\sigma_p^2}$. Note that when $\alpha = \alpha_{max}$, we have $\kappa = \frac{\gamma_s^{th}}{\gamma_{s,max}^{th}}$. To solve the problem **P2**, first, we find the optimal value of α as summarized by the following theorem.

Theorem 1: The optimal value of the reflection coefficient of the BD is the maximum value, i. e., $\alpha^* = \alpha_{max}$.

Proof: Note that from (14) and (19) that both γ_c and γ_e increase linearly with α. Moreover, it can be inferred from (22) that positive secrecy rate is obtained when $\gamma_c > \gamma_e$. Thus, whenever positive secrecy rate is achieved, i.e., $\gamma_c > \gamma_e$, as both γ_c and γ_e are directly proportional with α, we can conclude that R_{sec} is an increasing function of α. Note also that as α increases, κ decreases, and thus the lower bound of ϕ, given in (27) decreases. Thus, we can conclude that choosing $\alpha = \alpha_{max}$ does not affect the choice of ϕ in (27) that maximizes R_{sec}, and hence the optimal reflection coefficient is $\alpha^* = \alpha_{max}$ and it is independent on the power allocation factor ϕ. ■

B. LARGE SYSTEM ANALYSIS AND OPTIMIZATION OF POWER ALLOCATION

In order to optimize the power allocation factor ϕ and also provide useful insights on the impact of some key system parameters on the secrecy performance, in this subsection, we conduct large antenna analysis when the number of antenna elements grows indefinitely large, i.e., $N_t \to \infty$. In this case, $||\mathbf{h}_2||^2 \to \Omega_2 N_t$ and $\frac{\sum_{i=1}^{N_t-2} \big|\mathbf{h}_e^\dagger \mathbf{w}_i\big|^2}{N_t - 2} \to \Omega_e$ [31]. Thus, from (14) and (19), the asymptotic SNRs are given as

$$\gamma_c^\infty = \frac{\phi \alpha P N \big|g_1\big|^2 \Omega_2 N_t}{\sigma_p^2}, \tag{29}$$

$$\gamma_e^\infty = \frac{\phi}{(1-\phi)} \frac{\alpha N \big|g_2\big|^2 \Omega_2 N_t}{\Omega_e}. \tag{30}$$

The asymptotic secrecy rate can then be written as

$$\begin{aligned} R_{sec}^\infty &= \frac{1}{N \ln(2)} \left[\ln\Big(\frac{1+\gamma_c^\infty}{1+\gamma_e^\infty}\Big) \right]^+ \\ &= \frac{1}{N \ln(2)} \left[\ln\Big(\frac{1+(\beta-1)\phi - \beta\phi^2}{1+(\zeta-1)\phi}\Big) \right]^+, \end{aligned} \tag{31}$$

where $\beta \triangleq \alpha_{max} P N \big|g_1\big|^2 \Omega_2 N_t / \sigma_p^2$, and $\zeta \triangleq \alpha_{max} N \big|g_2\big|^2 \Omega_2 N_t / \Omega_e$.

We note from (31) that $\lim_{\phi \to 0} R_{sec}^\infty = 0$, which means that when the entire power is used for AN generation, there is no information transmission and thus the secrecy rate is zero. Moreover, from (31) it is easy to show that positive secrecy rate can be obtained only when $\frac{1+(\beta-1)\phi-\beta\phi^2}{1+(\zeta-1)\phi} > 1$, or equivalently $\phi < 1 - \frac{\zeta}{\beta} \triangleq \phi_1$. In other words, ϕ must be always less than one, which means that the AN is essential to achieve positive secrecy rate in our considered system setup. It should be noted that the necessity of AN to achieve positive secrecy rate stems from our assumption of zero noise at the ED side. On the other hand, when $\phi \ge \phi_1$, the generated AN is not sufficient for preventing the eavesdropper from being able to decode the transmitted message signal and thus the secrecy rate is zero. Therefore, we can notice that there exists an optimal value of ϕ, in the range $0 < \phi < \phi_1$, which maximizes the underlying achievable ergodic secrecy rate.

Now, for a given optimal $\alpha = \alpha_{max}$, and without taking into account the primary user performance constraint given in (27), the optimization of the power allocation factor ϕ that maximizes the asymptotic secrecy rate given in (31) can be formulated as follows

$$\mathbf{P3}: \max_{\phi} \; \frac{1+(\beta-1)\phi - \beta\phi^2}{1+(\zeta-1)\phi} \tag{32}$$

Note that the objective function in **P3** is unimodal in the variable ϕ. Therefore, by taking the first derivative of the objective function with respect of ϕ, we obtain a quadratic equation in ϕ, and by equating the first derivative of the objective function to zero, the resultant solution for optimal ϕ that lies in the correct range is obtained as follows

$$\hat{\phi}^* = \frac{-\beta + \sqrt{\zeta\beta(1+\beta-\zeta)}}{\beta(\zeta-1)}. \tag{33}$$

[4]Note that the transmission rate using the average SNR constitutes the upper bound on the achievable ergodic rate of the primary signal. Another option, but with slightly more complex optimization procedure, is to make constraint on the ergodic rate given in (10) such that $R_s \ge R_s^{th}$.

Now, the optimal ϕ, taking into consideration the constraint (27), is given as

$$\phi^* = \max(\hat{\phi}^*, \kappa). \tag{34}$$

Equation (34) suggests that the ideal power allocation factor, denoted as ϕ^*, that maximizes the secrecy rate of the BD, can be represented by $\hat{\phi}^*$ as long as $\hat{\phi}^* < \kappa$. However, in cases where $\hat{\phi}^*$ exceeds a certain threshold κ, a higher value of ϕ becomes necessary to ensure the QoS for the primary user. As a result, ϕ^* is set to κ as it achieves both the minimum required SNR for the primary user and serves as the optimal value to maximize the secrecy rate of the BD under this condition. Moreover, it can be shown from (33) that $\hat{\phi}^*$ is a decreasing function of the number of transmit antennas N_t. This can be interpreted as follows. As N_t increases, the SNR of the primary user γ_s increases due to the array gain of using matched filter precoding that matches the PT-BD link. Thus, the fraction of power required to satisfy the QoS of the primary user decreases.

C. CONDITIONS FOR POSITIVE SECRECY RATE

In this subsection, in order to get further insights, we investigate the condition under which a positive secrecy rate can be achieved using the asymptotic ergodic secrecy rate derived in the previous subsection. From (31), the condition for positive secrecy rate reduces to $\gamma_c^\infty > \gamma_e^\infty$, which can be written as

$$\left(\frac{d_{BE}}{d_{BP}}\right)^2 > \frac{\sigma_p^2}{(1-\phi)P\Omega_e}. \tag{35}$$

Note from (35) that the relative distance $\frac{d_{BE}}{d_{BP}}$ is an important factor. If the location of the BD is much closer to the ED than the PR, i.e., $\frac{d_{BE}}{d_{BP}} \ll 1$, then achieving positive secrecy rate requires allocating more power to the AN signal. However, interestingly, we can also infer from (35) that better channel condition for PT-ED link, i.e., large value of Ω_e, decreases the required AN power for achieving positive secrecy rate. This is due to the fact that in the considered SR network setup, the information signal to be secured is only reflected from the BD, but the AN is transmitted through the direct PT-ED link. Moreover, from (35), the required total transmit power for achieving positive secrecy rate can be lower bounded as

$$P > \left(\frac{d_{BP}}{d_{BE}}\right)^2 \frac{\sigma_p^2}{(1-\phi)\Omega_e}. \tag{36}$$

The lower bound in (36) indicates the minimum transmit power required for positive secrecy rate. This lower bound is particularly important in system design. For instance, it can be used to adjust the power allocation factor ϕ that minimizes the required transmit power to achieve positive secrecy rate. This process should take into account the QoS requirement of the primary user. Hence, there exists a tradeoff between minimizing the overall power consumption needed to achieve a positive secrecy rate and meeting the QoS demands of the primary system. For instance, reducing the parameter ϕ will lower the minimum power allocation necessary to attain a positive secrecy rate, but it will come at the expense of compromising the QoS performance of the primary user. Moreover, it can be inferred from (36) that if the location of the BD is much closer to the ED than the PR, the minimum power required for achieving positive secrecy rate increases.

V. SIMULATION RESULTS

In this section, we verify the proposed secure transmission schemes for SR via simulations. Unless otherwise stated, we set $P = 30$dBm, $\sigma_p^2 = -140$dBm, $N = 64$, $\alpha_{max} = 0.25$, and $\kappa = 0.5$. The distances of the different links, i.e., PT-PR, PT-BD, PT-ED, BD-PR, and BD-ED are, respectively, given as $d_1 = 200$m, $d_2 = 200$m, $d_e = 200$m, $d_{BP} = 1$m, and $d_{BE} = 1$m. The path loss models between the PT and the different nodes are calculated as follows [22], [30], $\Omega_1 = \varrho G_t G_r d_1^{-\vartheta}$, $\Omega_2 = \varrho G_t G_b d_2^{-\vartheta}$, and $\Omega_e = \varrho G_t G_e d_e^{-\vartheta}$ where $\varrho = (\frac{3\times 10^8}{4\pi f})^2$ is the average channel attenuation at unit reference distance with $f = 915$MHz being the transmit frequency, and the path loss exponent $\vartheta = 3$; G_t, G_r, G_b, and G_e denote the antenna gains for PT, PR, BD, and ED, respectively, which are assumed to equal 6dB [32]. Moreover, $|g_1|^2 = \varrho G_b G_r d_{BP}^{-2}$ and $|g_2|^2 = \varrho G_b G_e d_{BE}^{-2}$. The average SNR for the PT-PR direct link is defined as $\gamma_d \triangleq \frac{P\Omega_1}{\sigma_p^2}$.

First, we plot the transmission rates against γ_d as shown in Fig. 2. In Fig. 2(a), we compare the secrecy rate R_{sec} with the simulated exact secrecy rate $\hat{R}_{sec} = [\hat{R}_c - \hat{R}_e]^+$, where $\hat{R}_c$ and $\hat{R}_e$ are given in (13) and (18), respectively. The primary rate shown in Fig. 2(b) is obtained using (10) and the simulation results are obtained by substituting (7) into (9) and averaging over c. Note that the secrecy rate of the BD, shown in Fig. 2(a) is generally much lower than the transmission rate of the primary user. This is because we considered the commensal setup in this paper, where one BD symbol spans over N primary symbols, and also the BD signal causes no interference to the primary signal. From Fig. 2(a), R_{sec} can well approximate $\hat{R}_{sec}$ when N is equal or larger than 32. Interestingly, from Fig. 2(b), we note that the primary rate decrease as N increases. Although there is no direct proportionality between γ_s and N as inferred from (8), it can be shown that the optimal power allocation factor ϕ^*, given in (33), is inversely proportional with N, and therefore the primary rate slightly decreases with increasing N. Numerical results show that all theoretical results match well with Monte-Carlo simulation results.

Fig. 3 shows the ergodic secrecy rate against the normalized SNR threshold $\kappa \triangleq \frac{\gamma_s^{th}}{\gamma_{s,max}^{th}}$ of the primary user, with different values of γ_d. We observe that the secrecy rate remains unchanged up to the point where $\kappa = \hat{\phi}^*$. When $\kappa > \hat{\phi}^*$, then $\phi^* = \kappa$ and hence, the secrecy rate starts to decrease gradually as more power allocated to the information signal than for AN signal. The value of κ where the secrecy rate is zero depends on the SNR of the direct link γ_d. When $\kappa = 1$, zero AN signal is transmitted and the secrecy rate is zero. Therefore, the SNR threshold γ_s^{th} plays important

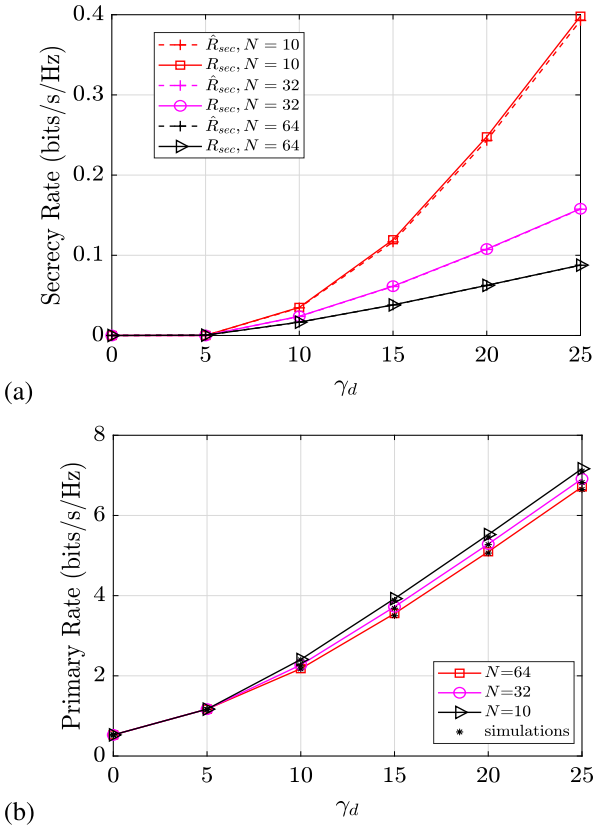


FIGURE 2. Transmission rate versus the backscattered SNR γ_d, with $N_t = 4$, $\kappa = 0.5$, and different values of N. (a) Ergodic secrecy rate. (b) Ergodic primary transmission rate.

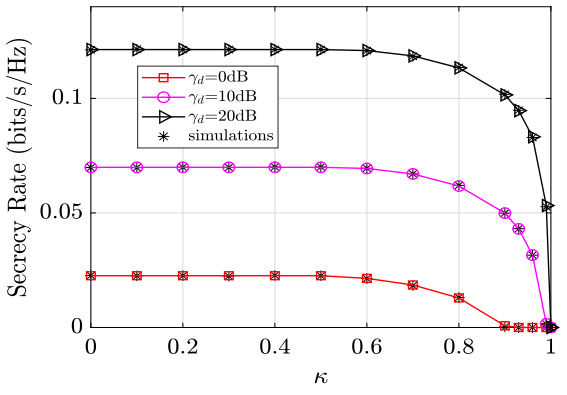


FIGURE 3. Ergodic secrecy rate versus $\kappa \triangleq \frac{\gamma_s^{th}}{\gamma_{s,max}^{th}}$, with $N_t = 4$, $N = 64$, and different values of γ_d.

role in determining the secrecy performance of the secondary backscatter transmission in SR systems.

Next, we examine the impact of the power allocation factor ϕ on the secrecy rate. Fig. 4 illustrates the ergodic secrecy rates of the BD, plotted against ϕ for various values of the reflection coefficient α. The optimal values of ϕ, determined using equation (34), are represented by blue circles. The graph demonstrates that the secrecy rate rises with increasing α, and this increment is more pronounced when ϕ has

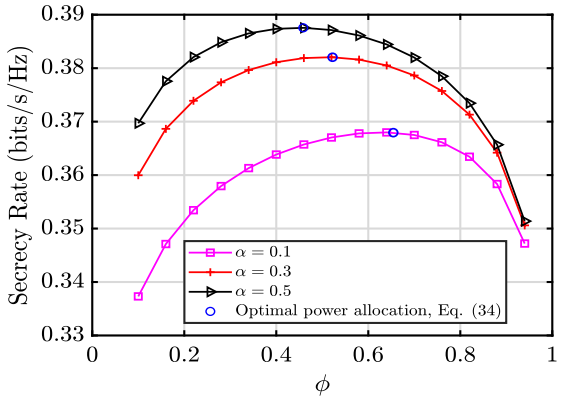


FIGURE 4. Ergodic secrecy rate versus ϕ, with $N_t = 4$, $N = 64$, $\kappa = 0.3$, and different values of the reflection coefficient α.

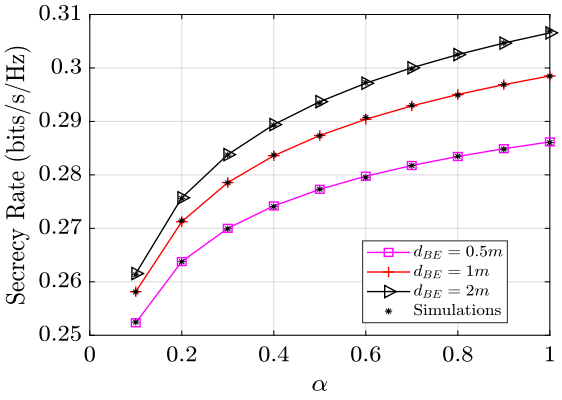


FIGURE 5. Ergodic secrecy rate versus α, with $N_t = 4$, $d_{BP} = 1$m, and different values of d_{BE}.

smaller values. Interestingly, the optimal ϕ decreases as α increases, indicating that a larger proportion of power should be allocated to generate AN as α increases.

In Fig. 5, we plot the reflection coefficient α versus the secrecy rate for different distances between BD and the ED. In this figure, we first observe that the secrecy rate increases as α increases even when $d_{BE} = 0.5$m, where the BD is closer to the ED than the PR. This observation confirms the analytical results that the optimum value of the reflection coefficient is to be set to the maximum value irrespective of the distance between the BD and the ED. Furthermore, the figure reveals a strong correlation between the secrecy rate and the distance between the BD and ED. Specifically, as this distance decreases, the secrecy rate diminishes since a greater amount of AN power is needed to confuse the ED.

Fig. 6 shows the impact of the number of transmit antennas on the optimal power allocation factor ϕ^*. The figure shows the optimal power allocation factor ϕ^* versus the number of transmit antennas N_t for different values of d_{BE}. The solid lines represent ϕ^* obtained using the asymptotic result given in (34), while the * markers indicate the optimal values that are obtained by exhaustive search. It is noted that, for a fixed d_{BE}, as N_t increases, ϕ^* decrease,

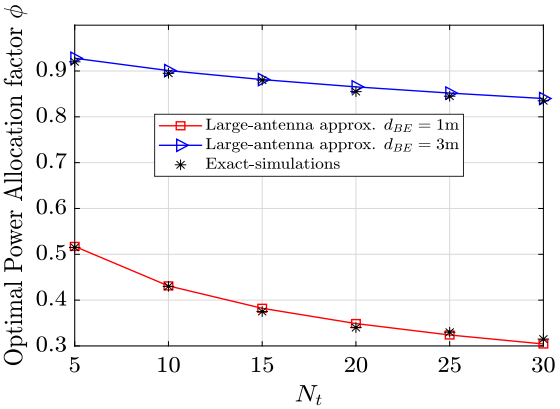


FIGURE 6. Optimal power allocation factor versus N_t, for various values of d_{BE}.

i.e., as N_t increases, more power should be allocated to the AN generation as discussed in Section IV-B. It is also seen that increasing the BD-ED distance reduces ϕ^*, which implies that as d_{BE} decreases, more power should be used to generate the AN signal. Note that the numerical results converges well with the exact simulation results even with small values of N_t.

VI. CONCLUSION

In paper, we addressed the issue of secure transmissions within SR networks. Specifically, we designed the transceiver of the primary system to support the transmissions of both the PT and the BD. Our goal is to propose a transmission scheme that incorporates AN to maximize the ergodic secrecy rate of the BD, while considering the QoS constraints of the primary system. To achieve this objective, we derived a closed-form expression for the achievable ergodic secrecy rate of the BD. Additionally, we conducted a large system analysis by considering a scenario with a large number of transmit antennas at the PT. We jointly optimized the power allocation factor and the reflection coefficient to maximize the ergodic secrecy rate. The analytical and simulation results indicated that AN-assisted beamforming is a powerful technique that can ensure the confidentiality of date transmission in SR networks in the presence of a passive eavesdropper. Interestingly, our findings demonstrated that using the maximum reflection coefficient is optimal, even when the channel condition of the BD-ED link is better than that of the BD-PR link. To validate the accuracy of our derived analytical results, we performed numerical simulations for various scenarios. The simulations further supported our findings and confirmed the effectiveness of the proposed transmission scheme in enhancing the security of SR networks.

APPENDIX I.
PROOF OF LEMMA 1

The following proposition summarizes some helpful distributions that will be used in the subsequent derivations.

Proposition 1: [33] *The cumulative distribution function (CDF) and probability density function (PDF) of a continuous Gamma distributed random variable X, with parameters α and β, are respectively given as*

$$F_X(x) = \frac{\gamma(\alpha, \frac{x}{\beta})}{(\alpha-1)!} = 1 - \sum_{n=0}^{\alpha-1} \frac{x^n e^{-\frac{x}{\beta}}}{\beta^n n!}, \tag{37}$$

$$f_X(x) = \frac{x^{\alpha-1} e^{-\frac{x}{\beta}}}{\beta^\alpha (\alpha-1)!}. \tag{38}$$

First, define $X \triangleq \frac{p}{\sigma_p^2}\left|\mathbf{h}_1^\dagger \hat{\mathbf{h}}_2\right|^2$ and $Y \triangleq \frac{p}{\sigma_p^2}\alpha\left|g_1\right|^2 ||\mathbf{h}_2||^2$, so that $\gamma_s = X + Y$. Note that $X \sim \exp\left(\frac{\sigma_p^2}{p\Omega_1} \triangleq \lambda\right)$, and $Y \sim \text{Gamma}(N_t, \frac{p}{\sigma_p^2}\alpha\left|g_1\right|^2\Omega_2 \triangleq \theta)$ [29, proof of Lemma 1]. Now, we show that X and Y are independent. Note that conditioned on $\mathbf{h}_2$, $\mathbf{h}_1^\dagger \hat{\mathbf{h}}_2$ is a complex Gaussian random variable with zero mean and variance Ω_1 which does not depend on $\mathbf{h}_2$. Therefore, $\mathbf{h}_1^\dagger \hat{\mathbf{h}}_2$ and the elements of $\mathbf{h}_2$ are independent, and hence X and Y are independent. The PDF of Y $f_Y(y)$ can be obtained using Proposition 1, and the CDF of X is $F_X(x) = 1 - e^{-\lambda x}$. Now, we find the CDF of γ_s as follows

$$\begin{aligned} F_{\gamma_s}(\gamma) &= \int_0^\infty \int_0^{\gamma-y} f_X(x) f_Y(y) dx dy \\ &= \int_0^\infty F_X(\gamma - y) f_Y(y) dy \\ &= 1 - \frac{e^{-\lambda\gamma}}{\theta^{N_t}(N_t-1)!} \int_0^\infty y^{N_t-1} e^{-y(\frac{1}{\theta}-\lambda)} dy \\ &= 1 - \frac{e^{-\lambda\gamma}}{(1-\lambda\theta)^{N_t}}, \end{aligned} \tag{39}$$

where the last integral is solved using [26, Eq. (3.381.4)]. Then, the ergodic rate of the primary user is given as

$$\begin{aligned} R_s &= \frac{1}{\ln(2)} \mathbb{E}\left[\ln(1+\gamma_s)\right] \\ &= \frac{1}{\ln(2)} \int_0^\infty \ln(1+\gamma) f_{\gamma_s}(\gamma) d\gamma \\ &\overset{a}{=} \frac{1}{\ln(2)} \int_0^\infty \frac{1 - F_{\gamma_s}(\gamma)}{(1+\gamma)} d\gamma \\ &\overset{b}{=} \frac{\lambda}{\ln(2)(1-\lambda\theta)^{N_t}} \int_0^\infty \frac{e^{-\lambda\gamma}}{(1+\gamma)} d\gamma, \end{aligned} \tag{40}$$

where integration by parts is used for obtaining equality a, while equality b is obtained by substituting (39) into (40). Using [26, Eq. (3.352.4)] to solve the last integral in (40) gives (10).

APPENDIX II.
PROOF OF LEMMA 3

First, we find the CDF of γ_e that is given in (19). Define $X_1 \triangleq \alpha p N \left|g_2\right|^2 ||\mathbf{h}_2||^2$ and $X_2 \triangleq q \sum_{i=1}^{N_t-2} \left|\mathbf{h}_e^\dagger \mathbf{w}_i\right|^2$. We have

$X_1 \sim \text{Gamma}(N_t, \alpha pN|g_2|^2\Omega_2 \triangleq \beta_2)$ and $X_2 \sim \text{Gamma}(N_t-2, q\Omega_e \triangleq \beta_3)$. The CDF of γ_e is then given as

$$\begin{aligned} F_{\gamma_e}(\gamma) &= \Pr[X_1 \le \gamma X_2] \\ &= \int_0^\infty F_{X_1}(\gamma x_2) f_{X_2}(x_2) dx_2 \\ &= 1 - \sum_{n=0}^{N_t-1} \frac{\gamma^n}{\beta_3^{N_t-2}(N_t-3)!n!\beta_2^n} \\ &\quad \times \int_0^\infty x_2^{N_t+n-3} e^{-(\frac{1}{\beta_3}+\frac{\gamma}{\beta_2})x_2} dx_2 \\ &= 1 - \sum_{n=0}^{N_t-1} \frac{\beta_2^{N_t-2}(N_t+n-3)!}{\beta_3^{N_t-2}(N_t-3)!n!} \\ &\quad \times \gamma^n (\frac{\beta_2}{\beta_3}+\gamma)^{-N_t-n+2}, \end{aligned} \tag{41}$$

where [26, Eq. (3.381.4)] is used to solve the last integral in (41). Now, the ergodic rate at the ED is given as

$$\begin{aligned} R_e &= \frac{1}{N\ln 2}\mathbb{E}\big[\ln(1+\gamma_e)\big] \\ &= \frac{1}{N\ln(2)} \int_0^\infty \ln(1+\gamma) f_{\gamma_e}(\gamma) d\gamma \\ &\overset{a}{=} \frac{1}{N\ln(2)} \int_0^\infty \frac{1-F_{\gamma_e}(\gamma)}{(1+\gamma)} d\gamma \\ &\overset{b}{=} \frac{1}{N\ln(2)} \sum_{n=0}^{N_t-1} \frac{\beta_2^{N_t-2}(N_t+n-3)!}{\beta_3^{N_t-2}(N_t-3)!n!} \\ &\quad \times \int_0^\infty \frac{\gamma^n(\frac{\beta_2}{\beta_3}+\gamma)^{-N_t-n+2}}{(1+\gamma)} d\gamma. \end{aligned} \tag{42}$$

As in (40), integration by parts is used for obtaining equality a and equality b is obtained by substituting (41) into (42). Using [26, Eq. (3.227.1)] to solve the last integral in (42), (21) is obtained.

ACKNOWLEDGMENT

The views and opinions expressed are however those of the author(s) only and do not necessarily reflect the views of Hexa-X-II Consortium nor those of the European Union or Horizon Europe SNS-JU. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

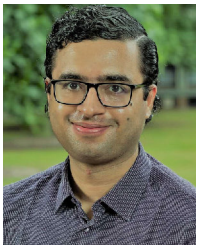
[1] C. Boyer and S. Roy, "Backscatter communication and RFID: Coding, energy, and MIMO analysis," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 770–785, Mar. 2014.
[2] L. Bariah, L. Mohjazi, S. Muhaidat, P. C. Sofotasios, G. K. Kurt, H. Yanikomeroglu, and O. A. Dobre, "A prospective look: Key enabling technologies, applications and open research topics in 6G networks," *IEEE Access*, vol. 8, pp. 174792–174820, 2020.
[3] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2889–2922, 4th Quart., 2018.
[4] C. Liaskos, A. Tsioliaridou, S. Ioannidis, A. Pitsillides, and I. F. Akyildiz, "Realizing ambient backscatter communications with intelligent surfaces in 6G wireless systems," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 178–185, Feb. 2022.
[5] H. Guo, Q. Zhang, S. Xiao, and Y.-C. Liang, "Exploiting multiple antennas for cognitive ambient backscatter communication," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 765–775, Feb. 2019.
[6] G. Yang, Q. Zhang, and Y.-C. Liang, "Cooperative ambient backscatter communications for green Internet-of-Things," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1116–1130, Apr. 2018.
[7] R. Duan, R. Jäntti, H. Yigitler, and K. Ruttik, "On the achievable rate of bistatic modulated rescatter systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9609–9613, Oct. 2017.
[8] R. Long, Y.-C. Liang, H. Guo, G. Yang, and R. Zhang, "Symbiotic radio: A new communication paradigm for passive Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1350–1363, Feb. 2020.
[9] Y.-C. Liang, Q. Zhang, E. G. Larsson, and G. Y. Li, "Symbiotic radio: Cognitive backscattering communications for future wireless networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 4, pp. 1242–1255, Dec. 2020.
[10] Q. Zhang, L. Zhang, Y.-C. Liang, and P.-Y. Kam, "Backscatter-NOMA: A symbiotic system of cellular and Internet-of-Things networks," *IEEE Access*, vol. 7, pp. 20000–20013, 2019.
[11] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3442–3451, Jun. 2014.
[12] Y. Zhang, F. Gao, L. Fan, X. Lei, and G. K. Karagiannidis, "Secure communications for multi-tag backscatter systems," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1146–1149, Aug. 2019.
[13] Z. Liu, Y. Ye, X. Chu, and H. Sun, "Secrecy performance of backscatter communications with multiple self-powered tags," *IEEE Commun. Lett.*, vol. 26, no. 12, pp. 2875–2879, Dec. 2022.
[14] Q. Yang, H.-M. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7547–7560, Nov. 2016.
[15] Y. Li, M. Jiang, Q. Zhang, and J. Qin, "Secure beamforming in MISO NOMA backscatter device aided symbiotic radio networks," 2019, *arXiv:1906.03410*.
[16] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. K. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1066–1076, Sep. 2021.
[17] G. Yang, J. Zhang, and Y.-C. Liang, "Optimal beamforming in cooperative cognitive backscatter networks for wireless-powered IoT," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Dec. 2018, pp. 56–61.
[18] T. Wu, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Beamforming design in multiple-input-multiple-output symbiotic radio backscatter systems," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1949–1953, Jun. 2021.
[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[20] A. Al-Nahari, G. Geraci, M. Al-Jamali, M. H. Ahmed, and N. Yang, "Beamforming with artificial noise for secure MISOME cognitive radio transmissions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1875–1889, Aug. 2018.
[21] H. Guo, Y.-C. Liang, R. Long, S. Xiao, and Q. Zhang, "Resource allocation for symbiotic radio system with fading channels," *IEEE Access*, vol. 7, pp. 34333–34347, 2019.
[22] D. Mishra and E. G. Larsson, "Sum throughput maximization in multi-tag backscattering to multiantenna reader," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5689–5705, Aug. 2019.
[23] A. Al-Nahari, R. Jäntti, R. Duan, D. Mishra, and H. Yigitler, "Multi-bounce effect in multi-tag monostatic backscatter communications," *IEEE Wireless Commun. Lett.*, vol. 11, no. 1, pp. 43–47, Jan. 2022.
[24] J. Kimionis, A. Georgiadis, A. Collado, and M. M. Tentzeris, "Enhancement of RF tag backscatter efficiency with low-power reflection amplifiers," *IEEE Trans. Microw. Theory Techn.*, vol. 62, no. 12, pp. 3562–3571, Dec. 2014.
[25] 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.
[26] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Elsevier, 2007.
[27] M.-S. Alouini and A. J. Goldsmith, "Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1165–1181, Jul. 1999.

[28] G. Alfano, A. Lozano, A. M. Tulino, and S. Verdu, "Mutual information and eigenvalue distribution of MIMO ricean channels," in *Proc. Int. Symp. Inf. Theory Appl.*, Parma, Italy, Oct. 2004, pp. 1–6.
[29] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.
[30] A. Al-Nahari, R. Jäntti, D. Mishra, and J. Hämäläinen, "Massive MIMO beamforming in monostatic backscatter multi-tag networks," *IEEE Commun. Lett.*, vol. 25, no. 4, pp. 1323–1327, Apr. 2021.
[31] I. Krikidis, "Retrodirective large antenna energy beamforming in backscatter multi-user networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 678–681, Aug. 2018.
[32] P. V. Nikitin and K. V. S. Rao, "Antennas and propagation in UHF RFID systems," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 277–288.
[33] 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.

AZZAM AL-NAHARI received the B.Sc. degree in electronics and communications engineering from the University of Technology, Iraq, and the M.Sc. and Ph.D. degrees in electrical communications from the Faculty of Electronic Engineering, Menoufia University, Egypt, in 2008 and 2011, respectively. Since 2011, he was an Assistant Professor with the Department of Electrical Engineering, Ibb University, Yemen, and became an Associate Professor, in 2017. In 2012, he held a postdoctoral position with the Department of Electrical and Information Technology, Lund University, Sweden. He also held a postdoctoral position with University at Buffalo, Buffalo, NY, USA, in 2014. Since July 2019, he has been a Visiting Scholar with the Department of Information and Communications Engineering, Aalto University, Espoo, Finland. His current research interests include backscatter communications, massive MIMO systems, physical layer security, cognitive radio networks, and signal processing for wireless communications.

RIKU JÄNTTI (Senior Member, IEEE) received the M.Sc. degree (Hons.) in electrical engineering and the D.Sc. degree (Hons.) in automation and systems technology from the Helsinki University of Technology (TKK), Espoo, Finland, in 1997 and 2001, respectively. He is currently a Full Professor of communications engineering and the Head with the Department of Communications and Networking, School of Electrical Engineering, Aalto University (formerly, known as TKK), Espoo. Prior to joining Aalto University, in August 2006, he was a Professor pro tem with the Department of Computer Science, University of Vaasa, Vaasa, Finland. His research interests include radio resource control and optimization for machine type communications, cloud-based radio access networks, spectrum and co-existence management, quantum communications, and RF inference. He is an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He is also a IEEE VTS Distinguished Lecturer (Class 2016).

GAN ZHENG received the B.Eng. and M.Eng. degrees in electronic and information engineering from Tianjin University, Tianjin, China, in 2002 and 2004, respectively, and the Ph.D. degree in electrical and electronic engineering from The University of Hong Kong, in 2008. He is currently a Professor in connected systems with the School of Engineering, University of Warwick, U.K. His research interests include machine learning for wireless communications, UAV communications, mobile edge caching, full-duplex radio, and wireless power transfer. He was a first recipient of the 2013 IEEE SIGNAL PROCESSING LETTERS Best Paper Award. He was also received the 2015 GLOBECOM Best Paper Award and the 2018 IEEE Technical Committee on Green Communications and Computing Best Paper Award. He was listed as a Highly Cited Researcher by Thomson Reuters/Clarivate Analytics, in 2019. He currently serves as an Associate Editor for IEEE WIRELESS COMMUNICATIONS LETTERS.



DEEPAK MISHRA (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the Indian Institutes of Technology (IIT) Delhi, in 2017. He is currently an Australian Research Council (ARC) Discovery Early Career Researcher Award (DECRA) Fellow with the School of Electrical Engineering and Telecommunications, University of New South Wales (UNSW) Sydney, where he joined as a Senior Research Associate, in August 2019. Before that, he was a Postdoctoral Researcher with Linköping University, Sweden, from August 2017 to July 2019. He has also been a Visiting Researcher with Northeastern University, USA; the University of Rochester, USA; Huawei Technologies, France; and Southwest Jiaotong University, China. He serves as an Associate Editor for IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE ACCESS, and *Communication Theory Track of Frontiers in Communications and Networks*. His research interests include energy harvesting cooperative communication networks, MIMO, backscattering, physical layer security, and signal processing and energy optimization schemes for the uninterrupted operation of wireless networks.

MINGCHENG NIE (Graduate Student Member, IEEE) received the B.E. degree (Hons.) in electrical engineering from the University of New South Wales (UNSW), Sydney, Australia, in 2021, where he is currently pursuing the M.Phil. degree. His research interests include the delay-Doppler domain signal processing and physical layer security.