

QoS Aware Transmit Beamforming for Secure Backscattering in Symbiotic Radio Systems

Mingcheng Nie*, Deepak Mishra*, Azzam Al-nahari[†], Jinhong Yuan*, and Riku Jäntti[†]

*School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia

[†]Department of Communications and Networking, Aalto University, Espoo 02150, Finland

Emails: m.nie@student.unsw.edu.au, d.mishra@unsw.edu.au, azzam.al-nahari@aalto.fi,

j.yuan@unsw.edu.au, and riku.jantti@aalto.fi

Abstract—This paper focuses on secure backscatter transmission in the presence of a passive multi-antenna eavesdropper through a symbiotic radio (SR) network. Specifically, a single-antenna backscatter device (BD) aims to transmit confidential information to a primary receiver (PR) by using a multi-antenna primary transmitter's (PT) signal, where the received symbols are jointly decoded at the PR. Our objective is to achieve confidential communications for BD while ensuring that the primary system's quality of service (QoS) requirements are met. We propose an alternating optimisation algorithm that maximises the achievable secrecy rate of BD by jointly optimising primary transmit beamforming and power sharing between information and artificial noise (AN) signals. Numerical results verify our analytical claims on the optimality of the proposed solution and the proposed methodology's underlying low complexity. Additionally, our simulations provide nontrivial design insights into the critical system parameters and quantify the achievable gains over the relevant benchmark schemes.

I. INTRODUCTION

Backscatter communication may provide a viable solution for future energy-efficient and affordable Internet-of-things (IoT) devices, as recognised by developing technology experts [1]. Recently, a new technology called Symbiotic Radio (SR) has been proposed as a means to achieve spectrum-sharing efficiency and reliable communications for IoT transmissions. In SR, passive backscatter devices (BD) [2] use the ambient backscatter (AmBC) scheme to ride over the received signals from the licensed transmitter [3]. By sharing the same receiver with the primary link, BD transmissions can avoid interference, allowing for reliable transmissions through joint decoding of the primary and backscatter transmissions, unlike cognitive radio (CR) [4]. However, due to the low-cost BDs that can be attached to every physical object and the spectrum-sharing nature, malicious attacks on the BD tags can lead to data interception and privacy breaches [5]. Therefore, securing backscatter communication systems is a critical design issue. It has been discovered that Physical Layer Security (PLS) provides simpler security algorithms compared to cryptographic schemes [6]. This is crucial considering the size, cost, and computation limitations.

A. State-of-the-Art

Studies on backscatter PLS can be categorized into two groups. The first group [7]–[9] focuses on modifying the un-

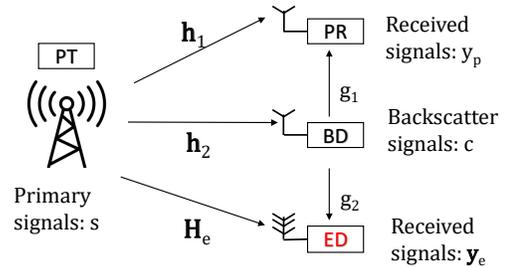


Fig. 1. SR model consists of PR, PT, BD and ED, where the BD backscatters its information to PR and the ED tries to decode the information of the BD.

modulated carrier signal's properties through PLS to improve the decoding error rate for eavesdroppers. For instance, in [7], authors used randomized continuous waves (CW) to achieve secure transmissions, where the secrecy rate is optimized by adjusting the CW's critical parameters. In contrast, [8] used a noise-like signal with varying power to enable covert backscatter communication. [9] explored how randomized modulation and wireless channels can shield commercial RFID tags from eavesdropping when the reader lacked multiple antenna capacity, but the eavesdropper did not.

The second group [10]–[12] uses artificial noise (AN) or interference injection to decrease eavesdropper signal-to-noise-ratio (SNR). In [10], AN signals are injected into conventional CW signals, with optimized power allocation between AN and CW signals. Similarly, [11] proposed AN-aided CW signals for secure backscatter transmission in the presence of proactive eavesdroppers. [12] investigated AN injection precoding strategy for secure MIMO backscatter communications, while [10], [11] considered single antennas and tags. Unlike the works above, [13] suggested secure multiuser SR transmissions by incorporating non-orthogonal multiple access (NOMA) and optimizing corresponding beamforming vectors. [14] conducted an outage and intercept probability analysis for a multiuser C-AmBC network, with single antennas considered at all nodes. Finally, [15] proposed three physical layer authentication schemes for the AmBC-aided NOMA symbiotic network regarding the variations of authentication tags.

B. Motivation and Contributions

In this paper, compared to the existing works [7]–[15], we investigate the secure backscatter transmissions in multi-antenna SR systems by AN injection along with transmit

beamforming. This work provides novel engineering design insights on optimal transmissions for secure SR networking in the presence of eavesdropping attackers. The main contributions are summarized next.

- We propose a secure transmission scheme for the multi-antenna SR system that takes into account quality of service (QoS) and employs AN injection. The scheme is designed to protect against a passive multi-antenna eavesdropper attempting to decode information sent by a passive single-antenna BD. We explore the proposed secure transmission scheme's performance bounds and robustness aspects.
- We proposed to maximize the secure rate of backscatter communications by jointly optimizing the sources of the multi-antenna primary transmitter under the QoS requirements of the primary system. Specifically, we optimized the primary transmit beamforming and the power allocation between signal transmission and AN injection.
- Since the optimization is a non-convex problem, we developed a low-complexity alternating optimization algorithm with fast convergence speed. We also conducted a complexity analysis for this algorithm. Here, we have developed semi-closed form expressions for optimal solutions, which offer new insights for design.
- Numerical results verify our analytical claims regarding optimality and fast convergence with low complexity. We also provide optimal design insights on power allocation and beamforming vectors. Lastly, we conduct a performance comparison study where the proposed scheme is shown to outperform the relevant benchmark schemes.

Notations: We define $[x]^+ \triangleq \max(0, x)$. Note that $|\cdot|$ and $\|\cdot\|$ are the absolute operation and Euclidean norm, respectively. We denote \mathbf{h}^T and \mathbf{h}^\dagger as the transpose and complex conjugate transpose of \mathbf{h} , respectively. \mathbf{I}_N , $\mathbf{0}_N$, and $\mathbf{1}_N$ denote the $N \times N$ identity matrix, the all-zero column vector of length N , and the all-one 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 the circularly symmetric complex Gaussian vector with zero-mean and covariance matrix $\mathbf{\Sigma}$. Note that $\mathbf{v}_{\max}\{\mathbf{M}\}$ represents the generalized principal eigenvector corresponding to maximum eigenvalue $\lambda_{\max}\{\mathbf{M}\}$ of matrix \mathbf{M} .

II. SYSTEM AND CHANNEL MODELS

A. SR Setup and Channel Model

We consider an SR network, as shown in Fig. 1, which consists of a primary transmitter (PT) with N_t antennas, a single-antenna backscatter device (BD), a single-antenna primary receiver (PR), and a multi-antenna eavesdropper (ED) with N_e antennas. Note that $\mathbf{h}_1 \sim \mathcal{CN}(\mathbf{0}_{N_t}, \sigma_s^2 \mathbf{I}_{N_t})$ represents the channel fading vector from the PT to PR, $\mathbf{h}_2 \sim \mathcal{CN}(\mathbf{0}_{N_t}, \sigma_c^2 \mathbf{I}_{N_t})$ is the channel fading vector from the PT to BD, and $\mathbf{H}_e \sim \mathcal{CN}(\mathbf{0}_{N_t N_e}, \sigma_e^2 \mathbf{I}_{N_t N_e})$ is $N_e \times N_t$ channel fading matrix from the PT to ED. In this paper, we assume that \mathbf{h}_1 and \mathbf{h}_2 are available at the PT, which is commonplace in the literature [16], where the CSI can be obtained by channel reciprocity in time-division duplexing (TDD) systems.

B. Transmission Signal Analysis

The PT transmits a primary information symbol s to the PR (primary link). Meanwhile, the BD transmits a secondary information signal $\sqrt{\alpha}c$ by riding over the PT signals (secondary link), where α denotes the reflection coefficient. We assume that the polyphase coding scheme is employed by the PT, i.e., $|s|^2 = 1$, and the Gaussian codebook is employed by the BD, i.e., $c \sim \mathcal{CN}(0, 1)$. Note that this is commonplace for parasitic setup in [17], [18], where the target is to maximize the achievable rate of the secondary system. Moreover, the PT uses $N_t - 2$ degrees of freedom for transmitting AN vector $\mathbf{z} = [z_1 z_2 \cdots z_{N_t-2}]^T \sim \mathcal{CN}(\mathbf{0}_{N_t-2}, \mathbf{I}_{N_t-2})$. Thus, in this system model, $N_t > 2$. The transmitted signal at the PT is

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

where p and q are the transmitted power of the information and jamming signals, respectively, and $\mathbf{w} \in \mathbb{C}^{N_t \times 1}$ is the normalized beamforming vector of the information signal, i.e., $\|\mathbf{w}\| = 1$. Moreover, the total transmitted power P is constrained such that $\|\mathbf{x}\|^2 = P$. $\mathbf{W} = [\mathbf{w}_1 \mathbf{w}_2 \cdots \mathbf{w}_{N_t-2}] \in \mathbb{C}^{N_t \times (N_t-2)}$ is the precoding matrix of the jamming signal \mathbf{z} with column normalization $\|\mathbf{w}_i\| = 1, \forall i$. In this paper, we design the AN to be completely suppressed at the PR, which leads to the precoding matrix \mathbf{W} of the AN to lie in the null space of the channels \mathbf{h}_1 and \mathbf{h}_2 , i.e., $\mathbf{h}_1^\dagger \mathbf{W} = \mathbf{0}_{N_t-2}^T$ and $\mathbf{h}_2^\dagger \mathbf{W} = \mathbf{0}_{N_t-2}^T$. The null-space-based AN design will degrade the eavesdropping channels but not the legitimate channels to facilitate the secure transmission design [19]. We assume that $N_t > N_e$ because the eavesdropper cannot eliminate the AN term in (1) with this condition [20]. Considering $0 \leq \phi \leq 1$ denote the fraction of power devoted to the information signal, the transmitter powers p and q are given by

$$p = \phi P, \quad (2)$$

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

Therefore, the received signal at the PR is given as

$$y_p = \sqrt{p}\mathbf{h}_1^\dagger \mathbf{w}s + \sqrt{p}\sqrt{\alpha}cg_1 \mathbf{h}_2^\dagger \mathbf{w}s + n_p, \quad (4)$$

where the first term of the right-hand side in (4) is the received signals from the primary link, the second term is from the secondary link, $g_1 \sim \mathcal{CN}(0, 1)$ is the channel coefficient of the BD-PR link known at PT, and $n_p \sim \mathcal{CN}(0, 1)$ represents the additive white Gaussian noise (AWGN) at PR. The received signals at the ED are given by

$$\begin{aligned} y_e &= \sqrt{p}\mathbf{H}_e \mathbf{w}s + \sqrt{p}\sqrt{\alpha}cg_2 \mathbf{1}_{N_e} \mathbf{h}_2^\dagger \mathbf{w}s \\ &+ \sqrt{q} \sum_{i=1}^{N_t-2} \mathbf{H}_e \mathbf{w}_i z_i + \mathbf{n}_e, \end{aligned} \quad (5)$$

where the first term of the right-hand side in (5) is the received signals from the PT-ED link, the second term is from the PT-BD-ED link, $g_2 \sim \mathcal{CN}(0, 1)$ is the channel coefficient of the BD-ED link known at PT, and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}_{N_e}, \mathbf{I}_{N_e})$.

In this paper, we consider the worst-case scenario, where the ED has zero noise, i.e., $\mathbf{n}_e \rightarrow \mathbf{0}_{N_e}$, and the ED can decode the PT signal for the sake of intercepting the BD signal. This will result in an upper bound on the achievable rate of the ED and a lower bound on the secrecy rate [19] [20]. Therefore, the received signal at the ED receiver is given as

$$\tilde{\mathbf{y}}_e = \sqrt{p}\sqrt{\alpha}cg_2\mathbf{1}_{N_e}\mathbf{h}_2^\dagger\mathbf{w}s + \sqrt{q}\sum_{i=1}^{N_t-2}\mathbf{H}_e\mathbf{w}_iz_i. \quad (6)$$

III. PROBLEM DEFINITION

A. SNR Analysis and Secrecy Rate Definition

Here we derive the achievable secrecy rate of the considered system setup. We are considering the parasitic case where the symbol period of the BD is equal to that of the primary system [3]. So, the BD signal is treated as interference, and the SNR of the primary system is given from (4) as

$$\gamma_s = \frac{p|\mathbf{h}_1^\dagger\mathbf{w}|^2}{p\alpha|g_1|^2|\mathbf{h}_2^\dagger\mathbf{w}|^2 + 1}. \quad (7)$$

After decoding the primary link signal s and removing it from the received signal in (4) by successive interference cancellation (SIC) technique, the SNR of the BD signal is

$$\gamma_{c|s} = p\alpha|g_1|^2|\mathbf{h}_2^\dagger\mathbf{w}|^2. \quad (8)$$

We assume the eavesdropper to be aware of $\mathbf{H}_e\mathbf{w}$, $\mathbf{h}_2^\dagger\mathbf{w}$, and the correlation matrix $q\mathbf{H}_e\mathbf{W}\mathbf{W}^\dagger\mathbf{H}_e^\dagger$ of the AN signal to perform the optimal detection that maximizes its SNR $\gamma_{e|s}$ [21]. Here we define $\mathbf{X} \triangleq \mathbf{H}_e\mathbf{W}\mathbf{W}^\dagger\mathbf{H}_e^\dagger$ and the SNR at the ED is given as

$$\gamma_{e|s} = \frac{p\alpha|g_2|^2}{q}\mathbf{w}^\dagger\mathbf{h}_2\mathbf{1}_{N_e}^\dagger\mathbf{X}^{-1}\mathbf{1}_{N_e}\mathbf{h}_2^\dagger\mathbf{w}. \quad (9)$$

The instantaneous achievable secrecy rate R_{sec} is defined by

$$R_{sec} = [R_c - R_e]^+, \quad (10)$$

where $R_c = \log_2(1 + \gamma_{c|s})$ and $R_e = \log_2(1 + \gamma_{e|s})$ represent the achievable rates at the backscatter and eavesdropper side, respectively. Here, we expand R_{sec} for later use as follow

$$R_{sec} = \left[\log_2 \left(1 + p\alpha|g_1|^2|\mathbf{h}_2^\dagger\mathbf{w}|^2 \right) - \log_2 \left(1 + \frac{p\alpha|g_2|^2}{q}\mathbf{w}^\dagger\mathbf{h}_2\mathbf{1}_{N_e}^\dagger\mathbf{X}^{-1}\mathbf{1}_{N_e}\mathbf{h}_2^\dagger\mathbf{w} \right) \right]^+. \quad (11)$$

B. Problem Definition of Secrecy Rate Optimization

Our goal is to maximize the achievable secrecy rate in (10) in terms of power allocation factor and beamforming vector, subject to the transmitting power and QoS constraints. Thus, the optimization problem is formulated as follows

$$\mathcal{O}_1 : \max_{\mathbf{w}, \phi} R_{sec} = [R_c - R_e]^+, \quad \text{subject to:} \\ (C1) : \|\mathbf{w}\|^2 \leq 1, \quad (C2) : 0 \leq \phi \leq 1, \quad (C3) : \gamma_s \geq \gamma_s^{th},$$

where γ_s^{th} is the minimum QoS requirement for PT in terms of SNR. Note that the constraint (C1) is convex [22],

[23], (C2) is linear, and (C3) is linear with ϕ as $\frac{\partial \gamma_s}{\partial \phi} = \frac{P|\mathbf{h}_1^\dagger\mathbf{w}|^2}{(p\alpha|g_1|^2|\mathbf{h}_2^\dagger\mathbf{w}|^2+1)^2} > 0$. However, (C3) is nonconvex due to $\frac{\partial^2 \gamma_s}{\partial \mathbf{w}^2} < 0$ and the coupling between \mathbf{w} and ϕ in γ_s in (7). Thus, \mathcal{O}_1 is a nonconvex problem because both constraint (C3) and R_{sec} include the coupling terms between \mathbf{w} and ϕ [22].

IV. PROPOSED SECRECY RATE OPTIMIZATION

Here we propose the optimal solution for the problem \mathcal{O}_1 by alternately optimizing ϕ and \mathbf{w} . Specifically, we investigate the optimal information beamforming vector \mathbf{w} for a given power allocation factor ϕ and optimal ϕ for a given \mathbf{w} in the following two subsections. In this way, the optimal \mathbf{w} and ϕ can be obtained through alternating and iterative updates.

A. Optimal \mathbf{w} for a Given ϕ

The problem of optimal \mathbf{w} that maximizes the achievable secrecy rate for a given ϕ can be defined as

$$\mathcal{O}_{1.1} : \max_{\mathbf{w}} R_{sec}, \quad \text{subject to: (C1), (C3).}$$

1) *Feasible analysis:* Before investigating the optimal solution of $\mathcal{O}_{1.1}$, we discuss the feasibility condition of (C3) by finding the maximum achievable SNR γ_s^{\max} at the PR. We start by rewriting the γ_s in (7) and (C3) in simplified form.

Lemma 1 γ_s can be rewritten and simplified as

$$\gamma_s = \frac{\mathbf{w}^\dagger \mathbf{G}_1 \mathbf{w}}{\mathbf{w}^\dagger \mathbf{G}_2 \mathbf{w}}, \quad (12)$$

where $\mathbf{G}_1 = \phi P \mathbf{h}_1 \mathbf{h}_1^\dagger$ and $\mathbf{G}_2 = \alpha \phi P |g_1|^2 \mathbf{h}_2 \mathbf{h}_2^\dagger + \mathbf{I}_{N_t}$ are both symmetry matrix.

Proof: Note that $|\mathbf{h}_1^\dagger \mathbf{w}|^2 = \mathbf{h}_1^\dagger \mathbf{w} \mathbf{w}^\dagger \mathbf{h}_1 = \mathbf{w}^\dagger \mathbf{h}_1 \mathbf{h}_1^\dagger \mathbf{w}$. Thus, γ_s can be written as $\gamma_s = \frac{\phi P \mathbf{w}^\dagger \mathbf{h}_1 \mathbf{h}_1^\dagger \mathbf{w}}{\mathbf{w}^\dagger (\alpha \phi P |g_1|^2 \mathbf{h}_2 \mathbf{h}_2^\dagger + \mathbf{I}_{N_t}) \mathbf{w}} = \frac{\mathbf{w}^\dagger \mathbf{G}_1 \mathbf{w}}{\mathbf{w}^\dagger \mathbf{G}_2 \mathbf{w}}$. ■

We can observe that γ_s in (12) is a generalized Rayleigh quotient. Thus, the global optimal beamforming vector \mathbf{w}_{e_1} that maximizes γ_s can be obtained by the generalized principal eigenvector of the matrix set $(\mathbf{G}_1, \mathbf{G}_2)$ as [24]

$$\mathbf{w}_{e_1} = \mathbf{v}_{\max}\{(\mathbf{G}_1, \mathbf{G}_2)\}. \quad (13)$$

The maximum SNR γ_s^{\max} for given ϕ can be obtained by substituting \mathbf{w}_{e_1} in (12). Thus, $\mathcal{O}_{1.1}$ is feasible if $\gamma_s^{\max} \geq \gamma_s^{th}$.

2) *Proposed Optimal Solution of \mathbf{w} :* In order to solve $\mathcal{O}_{1.1}$, we rewrite and simplify the achievable secrecy rate R_{sec} in (11) by treating ϕ as a constant and write in terms of \mathbf{w} as

$$R_{sec} = \left[\log_2 \left(1 + p\alpha|g_1|^2\mathbf{w}^\dagger\mathbf{h}_2\mathbf{h}_2^\dagger\mathbf{w} \right) - \log_2 \left(1 + \frac{p\alpha|g_2|^2}{q}\mathbf{w}^\dagger\mathbf{h}_2\mathbf{1}_{N_e}^\dagger\mathbf{X}^{-1}\mathbf{1}_{N_e}\mathbf{h}_2^\dagger\mathbf{w} \right) \right]^+, \\ = \left[\log_2 \left(\mathbf{w}^\dagger \left(\mathbf{I}_{N_t} + p\alpha|g_1|^2\mathbf{h}_2\mathbf{h}_2^\dagger \right) \mathbf{w} \right) - \log_2 \left(\mathbf{w}^\dagger \left(\mathbf{I}_{N_t} + \frac{p\alpha|g_2|^2}{q}\mathbf{h}_2\mathbf{1}_{N_e}^\dagger\mathbf{X}^{-1}\mathbf{1}_{N_e}\mathbf{h}_2^\dagger \right) \mathbf{w} \right) \right]^+, \\ = \left[\log_2 \left(\frac{\mathbf{w}^\dagger \mathbf{G}_3 \mathbf{w}}{\mathbf{w}^\dagger \mathbf{G}_4 \mathbf{w}} \right) \right]^+, \quad (14)$$

where $\mathbf{G}_3 = \mathbf{I}_{N_t} + p\alpha|g_1|^2\mathbf{h}_2\mathbf{h}_2^\dagger$ and $\mathbf{G}_4 = \mathbf{I}_{N_t} + \frac{p\alpha|g_2|^2}{q}\mathbf{h}_2\mathbf{1}_{N_e}^\dagger\mathbf{X}^{-1}\mathbf{1}_{N_e}\mathbf{h}_2^\dagger$. This R_{sec} in (14) is a generalized Rayleigh quotient. Thus, the optimal beamforming vector \mathbf{w}_{e_2} that maximizes R_{sec} in (14) *without constraints* is the generalized principal eigenvector of matrix set $(\mathbf{G}_3, \mathbf{G}_4)$ as [24]

$$\mathbf{w}_{e_2} = \mathbf{v}_{\max}\{(\mathbf{G}_3, \mathbf{G}_4)\}. \quad (15)$$

After investigating the optimal beamforming vector that maximizes the achievable secrecy rate without considering QoS constraint, it is crucial to strike a balance between the secrecy rate maximization and QoS requirement. Thus, we propose a weighted combination of \mathbf{w}_{e_1} and \mathbf{w}_{e_2} as follow

$$\mathbf{w}_{c_1} = \frac{\lambda_1\mathbf{w}_{e_1} + (1 - \lambda_1)\mathbf{w}_{e_2}}{\|\lambda_1\mathbf{w}_{e_1} + (1 - \lambda_1)\mathbf{w}_{e_2}\|}, \quad (16)$$

where λ_1 is the weighting factor and varies in d discrete steps uniformly, resulting in the allocation as $\{0, \frac{1}{d}, \frac{2}{d}, \dots, \frac{d-1}{d}, 1\}$. Note that \mathbf{w}_{e_1} in (13) and \mathbf{w}_{e_2} in (15) are two extremes that maximize the received SNR at PR and unconstrained secrecy rate, respectively, and the optimal \mathbf{w}_{c_1} in (16) balances between those extremes. Here d is chosen based on the tradeoff between the computational complexity and the desired solution quality. To compute the optimal \mathbf{w}_{c_1} , we need to evaluate R_{sec} and γ_s for all λ weights and then choose the maximum constrained secrecy rate among them.

B. Optimal ϕ for a Given \mathbf{w}

For a given \mathbf{w} , the problem of optimal ϕ that maximizes the achievable secrecy rate, subject to total power constraint (C2), can be defined as

$$\mathcal{O}_{1.2} : \max_{\phi} R_{sec}, \quad \text{subject to: (C2), (C3)}.$$

Note that we assume $\phi \neq 0$ because the PT has to send the information signals, and $\phi \neq 1$ because the eavesdropper will obtain an infinity rate, and the secure rate will be 0. Thus, the power factor is chosen as $0 < \phi < 1$. To obtain the solution of $\mathcal{O}_{1.2}$, we next rewrite R_{sec} in (11) by treating \mathbf{w} as a constant.

Lemma 2 *With $A \triangleq P\alpha|g_1|^2|\mathbf{h}_2^\dagger\mathbf{w}|^2$, optimal ϕ is given as*

$$\phi = \frac{A - \sqrt{AB(A - B + 1)}}{A - AB}. \quad (17)$$

where $B \triangleq (N_t - 2)\alpha|g_2|^2\mathbf{w}^\dagger\mathbf{h}_2\mathbf{1}_{N_e}^\dagger\mathbf{X}^{-1}\mathbf{1}_{N_e}\mathbf{h}_2^\dagger\mathbf{w}$.

Proof: Firstly, it is worth noting that R_{sec} can be rewritten in terms of ϕ as

$$R_{sec} = \left[\log_2 \frac{(1 + \phi A)}{\left(1 + \frac{\phi}{(1 - \phi)}B\right)} \right]^+. \quad (18)$$

Here, the obtained optimal ϕ is infeasible if it does not fall within the range $(0, 1)$. To obtain a positive secrecy rate, we need $1 + \phi A > 1 + \frac{\phi}{(1 - \phi)}B \Rightarrow (1 - \phi)A > B$, which leads to $A > B$ as $0 < \phi < 1$. Note that R_{sec} has two critical points

with respect to ϕ by taking $\frac{\partial R_{sec}}{\partial \phi} = 0$. The critical points are shown as follows

$$\phi_1 = \frac{A - \sqrt{AB(A - B + 1)}}{A - AB}, \quad (19)$$

$$\phi_2 = \frac{A + \sqrt{AB(A - B + 1)}}{A - AB}, \quad (20)$$

where $A > 0$ and $B > 0$. Then we take the second-order derivative as $\frac{\partial^2 R_{sec}}{\partial \phi^2} = \frac{2B(B - A - 1)}{((B - 1)\phi + 1)^3}$, where its numerator is negative as $A > B$ and its denominator is positive as $(B - 1)\phi > -1, \forall B > 0$. Thus, R_{sec} is concave and has two maximum values as $\frac{\partial^2 R_{sec}}{\partial \phi^2} < 0$. To select the feasible one among ϕ_1 and ϕ_2 , we first analyse the case when $A - AB < 0 \Rightarrow B > 1$. In this case, ϕ_2 in (20) will always be negative as its numerator is positive. When $A - AB > 0 \Rightarrow B < 1$, we analysis ϕ_2 in (20) as follow

$$\begin{aligned} 0 < \phi_2 < 1 &\Rightarrow 0 < A + \sqrt{AB(A - B + 1)} < A - AB, \\ &\Rightarrow -A < \sqrt{AB(A - B + 1)} < -AB, \end{aligned}$$

where $\sqrt{AB(A - B + 1)} < -AB$ is impossible. Thus, ϕ_2 in (20) is infeasible and only ϕ_1 in (19) is feasible. ■

C. Step-by-Step Algorithm

Next, we show the step-by-step procedure in Algorithm 1. Specifically, Algorithm 1 starts with a given power factor $\phi = 0.5$. Then, we obtain the optimal \mathbf{w} for a given ϕ as shown in Section IV-A, including SNR feasibility check and computation of the weighting beamforming vector \mathbf{w}_{c_1} . Based on the obtained optimal \mathbf{w} , we update the power factor as shown in Section IV-B and in Algorithm 1 line 22. Finally, Algorithm 1 terminates when $(R_{sec}^{(j-1)} - R_{sec}^{(j-2)}) \leq \varepsilon$, where ε is an acceptable tolerance.

D. Complexity Analysis

We first consider the computational complexity of Section IV-A. It is worth noting that the main computational complexity comes from the generalized eigenvectors of the matrix set $(\mathbf{G}_1, \mathbf{G}_2)$ and $(\mathbf{G}_3, \mathbf{G}_4)$ in (13) and (15), respectively. Specifically, the generalized eigenvector problem of two symmetric matrices $(\mathbf{G}_1, \mathbf{G}_2)$ is given as [25]

$$\mathbf{G}_1\mathbf{V} = \mathbf{G}_2\mathbf{V}\mathbf{D}, \quad (21)$$

where \mathbf{V} and \mathbf{D} contain the eigenvectors and eigenvalues, respectively. According to [26], this problem is solved in MATLAB based on matrix inversion as

$$\mathbf{G}_2^{-1}\mathbf{G}_1\mathbf{V} = \mathbf{V}\mathbf{D}. \quad (22)$$

Therefore, the complexity of generalized eigenvectors of two symmetric matrices problem consists of channel inversion and normal eigenvalue computing. Generally, the computational complexity of matrix inversion is $\mathcal{O}(N_t^3)$ [27] and normal eigenvalue computing is also $\mathcal{O}(N_t^3)$ [28]. Thus, the complexity of finding a generalized eigenvector is $\mathcal{O}(2N_t^3)$. The same approach applied to the matrix set $(\mathbf{G}_3, \mathbf{G}_4)$.

Algorithm 1 Alternating optimization of \mathbf{w} and ϕ to maximize R_{sec}

Require: $\mathbf{h}_1, \mathbf{h}_2, \mathbf{H}_e, \mathbf{X}, P, \alpha, g_1, g_2, d, \gamma_s^{th}, \varepsilon$

- 1: Set $j \leftarrow 1, \phi^{(1)} \leftarrow 0.5, R_{sec}^{(1)} \leftarrow 0$
- 2: **repeat**
- 3: Obtain \mathbf{w}_{e1} by substituting $\phi \leftarrow \phi^{(j)}$ into (12) and (13)
- 4: Obtain γ_s^{\max} by substituting $\mathbf{w} \leftarrow \mathbf{w}_{e1}$ into (12)
- 5: **if** $\gamma_s^{th} > \gamma_s^{\max}$ **then**
- 6: **print** \mathcal{O}_1 is not feasible
- 7: **return**
- 8: **else**
- 9: Obtain \mathbf{w}_{e2} by substituting $\phi \leftarrow \phi^{(j)}$ into (14), (15)
- 10: Set $i \leftarrow 0$
- 11: **for** $i \leq d$ **do**
- 12: Set $\lambda_1 = \frac{i}{d}$ in (16) and set the resultant as \mathbf{w}_{c1}
- 13: Substitute \mathbf{w}_{c1} and $\phi^{(j)}$ into γ_s in (12) and set the resultant as γ_{temp}
- 14: Substitute \mathbf{w}_{c1} and $\phi^{(j)}$ into $R_{sec}^{(j)}$ in (14) and set the resultant as R_{temp}
- 15: **if** $\gamma_{temp} \geq \gamma_s^{th}$ and $R_{temp}^{(j)} > R_{sec}$ **then**
- 16: Set $R_{sec}^{(j)} \leftarrow R_{temp}, \mathbf{w}_{opt} \leftarrow \mathbf{w}_{c1}$
- 17: Set $i \leftarrow i + 1$
- 18: Set $j \leftarrow j + 1$
- 19: Substitute $\mathbf{w} \leftarrow \mathbf{w}_{opt}$ into (18) and (17) and set the resultant as $\phi^{(j)}$
- 20: **until** $(R_{sec}^{(j-1)} - R_{sec}^{(j-2)}) \leq \varepsilon$
- 21: $R_{sec} \leftarrow R_{sec}^{(j-1)}, \phi_{opt} \leftarrow \phi^{(j-1)}$

Ensure: $\phi_{opt}, \mathbf{w}_{opt}, R_{sec}$

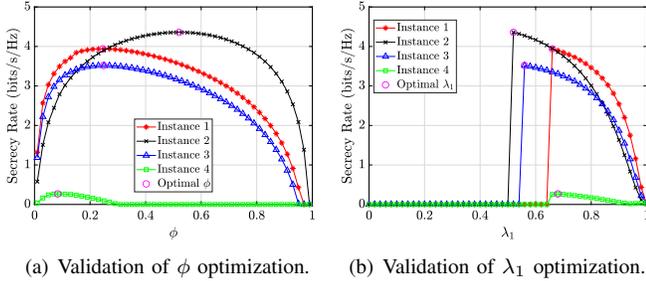


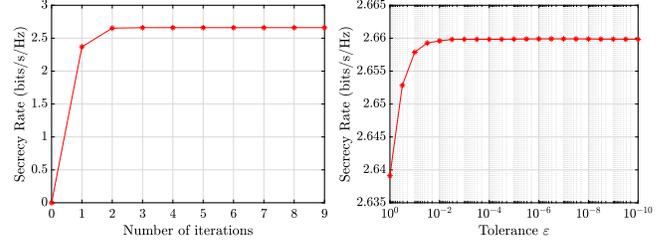
Fig. 2. Validation of the proposed secrecy rate maximization algorithm

Moreover, the complexity of iterations of finding \mathbf{w}_{c1} in (16) is $\mathcal{O}(d+1)$. Note that the complexity of Section IV-B is $\mathcal{O}(1)$. The complexity $\mathcal{O}(J)$ is due to the iterations of convergence, where J is the iteration number of convergence. Finally, we summarize the computational complexity of Algorithm 1 as $\mathcal{O}(J(4N_t^3(d+1)+1))$.

V. NUMERICAL RESULTS

Unless otherwise stated, we set $P = 48\text{dBm}$, $\gamma_s^{th} = 3\text{dB}$, $\gamma_c^{th} = 10\text{dB}$, $\alpha = 0.3$, $N_t = 10$, $N_e = 4$, $\varepsilon = 10^{-10}$, and $d = 100$. We assume $\sigma_s^2 = \sigma_c^2 = \sigma_e^2 = 1$. Note that the MATLAB seed is set as `rng(5)`, and the simulation results are averaged over 10^4 times channel realization.

First, we present the validation plots for the proposed algorithm in Fig. 2. Specifically, Fig. 2(a) and Fig. 2(b) show the secrecy rate against ϕ and λ_1 for four individual instances, respectively, where the optimal values for ϕ and λ_1 obtained by algorithm 1 that maximize the secrecy rate are denoted by magenta circles. We can observe that the globally optimal values match well with the search simulation results for all



(a) Convergence demonstration with increasing number of iterations. (b) Convergence demonstration with more sensitive tolerance ε .

Fig. 3. Convergence of the proposed secrecy rate maximization algorithm

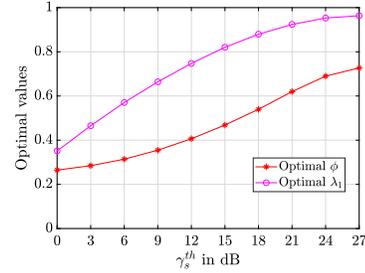


Fig. 4. Optimal ϕ and λ_1 versus γ_s^{th}

instances. Note that the secrecy rate is almost zero when λ_1 is approximately less than 0.5 in Fig. 2(b). This is because we define the secrecy rate to be a positive value in (10), where the eavesdropper rate can be larger than BD's rate when the eavesdropper's channel \mathbf{H}_e is much stronger than the primary link's channel conditions. It is important to acknowledge that our algorithm works on individual optimality rather than joint and ergodic optimality over group realizations, i.e., the sum of individual optimality may not be equal to the joint optimality of the group. Furthermore, the proposed algorithm 1 will converge fast within four iterations and tolerance 10^{-4} as shown in Fig. 3(a) and Fig. 3(b), respectively.

Next, insightful plots are presented for key algorithm parameters. Fig. 4 shows that the values of optimal ϕ and λ_1 tend to increase as the threshold γ_s^{th} increases. This can be attributed to the fact that a more significant value of ϕ results in higher transmission power in the primary link rather than jamming an eavesdropper. In contrast, a more significant

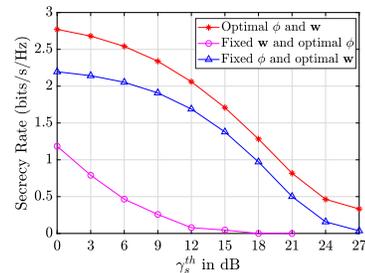
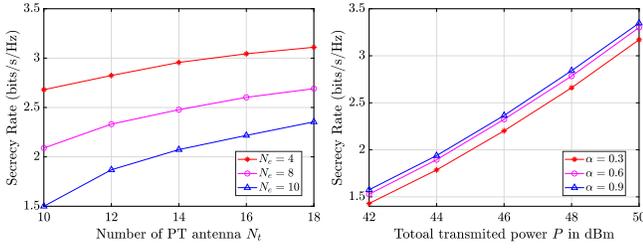


Fig. 5. Secrecy rate comparison between proposed and benchmark schemes, where the fixed beamforming vector is MRT, and the fixed ϕ is 0.5.



(a) Variation with N_t and N_e . (b) Variation with P and α .
 Fig. 6. Insights on achievable secrecy rate R_{sec} for different values of the number of antennas, total transmitted power P , and reflection coefficient α .

value of λ_1 directs the beamforming vector closer to \mathbf{w}_{e_1} , thereby maximizing the received SNR at PR. Consequently, we can expect a decrease in the achievable secrecy rate with an increase in the threshold γ_s^{th} , as shown in Fig. 5. Furthermore, in Fig. 5, the proposed scheme outperforms the conventional schemes at different QoS requirements based on achievable rate comparison. Note that the red line denotes the secrecy rate based on the proposed algorithm, where both power allocation factor ϕ and beamforming vector \mathbf{w} are optimized, the blue line denotes the optimal ϕ with maximum ratio transmitting (MRT) vector $\mathbf{w}_{MRT} = \frac{\mathbf{h}_2}{\|\mathbf{h}_2\|}$, and the magenta line denotes the optimal \mathbf{w} with a fixed $\phi = 0.5$. Moreover, it can be shown from Fig. 6(a) that the secrecy rate is directly proportional to the number of antennas at PT N_t and inversely proportional to the number of antennas at Eve N_e . Fig. 6(b) demonstrates that increased transmission power P and reflection coefficient α result in a higher secrecy rate.

VI. CONCLUSION

In this paper, we delve into the topic of secure transmissions for SR networks with multiple antennas using AN injection. Firstly, we introduce the setup of the secure transmission system. Then, we devise an alternating optimization algorithm to maximize the secrecy rate by designing the power allocation factor ϕ and beamforming vector \mathbf{w} . Our findings reveal that the achievable secrecy rate is significantly impacted by the QoS constraints of the primary system and BD. Furthermore, our secure SR system designs can be extended to multiple tags, primary receivers with multiple antennas, and colluding eavesdroppers in the future.

VII. ACKNOWLEDGMENT

This research work has been supported in part by the Australian Research Council Discovery Early Career Researcher Award (DECRA) - DE230101391.

REFERENCES

- [1] D. Mishra and E. G. Larsson, "Optimizing reciprocity-based backscattering with a full-duplex antenna array reader," in *Proc. IEEE Int. Workshop Signal Process. Adv. Wireless Commun.*, Kalamata, Greece, Jun. 2018.
- [2] A. C. Y. Goay, D. Mishra, and A. Seneviratne, "ASK modulator design for passive RFID tags in backscatter communication systems," in *Proc. IEEE WAMICON*, 2022, pp. 1–4.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
- [7] Q. Yang, H.-M. Wang, Q. Yin, and A. L. Swindlehurst, "Exploiting randomized continuous wave in secure backscatter communications," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3389–3403, Apr. 2020.
- [8] K. Shahzad and X. Zhou, "Covert communication in backscatter radio," in *Proc. IEEE ICC*, May. 2019, pp. 1–6.
- [9] H. Hassanieh, J. Wang, D. Katabi, and T. Kohnho, "Securing RFIDs by randomizing the modulation and channel," in *Proc. 12th USENIX Symp. Netw. Syst. Design Implement.*, 2015, pp. 235–249.
- [10] 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.
- [11] B.-Q. Zhao, H.-M. Wang, and P. Liu, "Safeguarding RFID wireless communication against proactive eavesdropping," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11 587–11 600, Dec. 2020.
- [12] 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.
- [13] Y. Li, M. Jiang, Q. Zhang, and J. Qin, "Secure beamforming in MISO NOMA backscatter device aided symbiotic radio networks," *arXiv preprint arXiv:1906.03410*, 2019.
- [14] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things," *IEEE Trans. Green Commun.*, vol. 5, no. 3, pp. 1066–1076, Sep. 2021.
- [15] X. Li, Q. Wang, M. Zeng, Y. Liu, S. Dang, T. A. Tsiftsis, and O. A. Dobre, "Physical-layer authentication for ambient backscatter-aided NOMA symbiotic systems," *IEEE Trans. Commun.*, Feb. 2023.
- [16] D. Mishra and E. G. Larsson, "Optimal channel estimation for reciprocity-based backscattering with a full-duplex MIMO reader," *IEEE Trans. Signal Process.*, vol. 67, no. 6, pp. 1662–1677, Mar. 2019.
- [17] H. Guo, Y.-C. Liang, R. Long, and Q. Zhang, "Cooperative ambient backscatter system: A symbiotic radio paradigm for passive IoT," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1191–1194, Aug. 2019.
- [18] X. Kang, Y.-C. Liang, and J. Yang, "Riding on the primary: A new spectrum sharing paradigm for wireless-powered IoT devices," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6335–6347, Sep. 2018.
- [19] 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.
- [20] 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.
- [21] 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.
- [22] D. Mishra and E. G. Larsson, "Sum throughput maximization in multi-tag backscattering to multi-antenna reader," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5689–5705, Aug. 2019.
- [23] —, "Multi-tag backscattering to MIMO reader: Channel estimation and throughput fairness," *IEEE Trans. Wireless Commun.*, vol. 18, no. 12, pp. 5584–5599, Dec. 2019.
- [24] R. Saini, D. Mishra, W. Xiong, and J. Yuan, "IRS-Assisted secure OFDMA with untrusted users," in *Proc. IEEE Global Commun. Conf. Workshops (GC Wkshps)*, Dec. 2022, pp. 619–624.
- [25] B. N. Parlett, *The Symmetric Eigenvalue Problem*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.
- [26] K. Faber, "On solving generalized eigenvalue problems using MATLAB," *J. Chemom.*, vol. 11, no. 1, pp. 87–91, Jun. 1997.
- [27] S. Li, W. Yuan, Z. Wei, and J. Yuan, "Cross domain iterative detection for orthogonal time frequency space modulation," *IEEE Trans. Wireless Commun.*, vol. 21, no. 4, pp. 2227–2242, Sept. 2021.

- [28] V. Y. Pan and Z. Q. Chen, "The complexity of the matrix eigenproblem," in *Proc. ACM Symp. Theory Comput.*, May, 1999, pp. 507–516.