Article:
Miao, Y., Shao, Y. and Zhang, J. (2024) IRS backscatter-based secrecy enhancement against active eavesdropping. Electronics, 13 (2). 265. ISSN: 1450-5843

https://doi.org/10.3390/electronics13020265

electronics

MDPI

Article

IRS Backscatter-Based Secrecy Enhancement against Active Eavesdropping

Yuanyuan Miao [1,*], Yu Shao [2] and Jie Zhang [1]

[1] Department of Electronic and Electrical Engineering, University of Sheffield, Sheffield S1 4ET, UK; jie.zhang@sheffield.ac.uk
[2] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; shaoyu@cqupt.edu.cn
* Correspondence: ymiao8@sheffield.ac.uk

Abstract: This paper proposes to combat active eavesdropping using intelligent reflecting surface (IRS) backscatter techniques. To be specific, the source (Alice) sends the confidential information to the intended user (Bob), while the eavesdropper (Willie) transmits a jamming signal to interrupt the transmission for more data interception. To enhance the secrecy, an IRS is deployed and connected with Alice through fiber to transform the jamming signal into the confidential signal by employing backscatter techniques. Based on the considered model, an optimization problem is formulated to maximize the signal-to-interference-plus-noise ratio (SINR) at Bob under the constraints of the transmit power at Alice, the reflection vector at the IRS, and the allowable maximum the SINR at Willie. To address the optimization problem, an alternate optimization algorithm is developed. The simulation results verify the achievable secrecy gain of the proposed scheme. The proposed scheme is effective in combating active eavesdropping. Furthermore, the deployment of large-scale IRS significantly enhances the secrecy rate.

Keywords: intelligent reflecting surface; backscatter; active eavesdropping; physical layer security

Citation: Miao, Y.; Shao, Y.; Zhang, J. IRS Backscatter-Based Secrecy Enhancement against Active Eavesdropping. *Electronics* **2024**, *13*, 265. https://doi.org/10.3390/electronics13020265

Academic Editor: Aryya Gangopadhyay

Received: 5 December 2023
Revised: 2 January 2024
Accepted: 3 January 2024
Published: 6 January 2024

1. Introduction

With the development of wireless communication technology, more and more private information is transmitted through public channels, which increases the risk of information leakage. Numerous studies have been conducted on physical layer security in wireless communication [1–3]. However, the security rate of traditional secure communication methods is limited when the eavesdropper's interference signal power is high [4]. To break this limit, an intelligent reflecting surface (IRS) can be combined with backscatter technology and integrated into the wireless communication system. The integration of backscatter in IRS can enhance the communication security of the system by utilizing the power of the interference signal emitted by the active eavesdropper. The signal reflected by the IRS can reduce the impact of the eavesdropper's interference signal and strengthen the required signal received by the legitimate user. This dual capability enhances the reliability of communication, fortifying the received signal quality for legitimate users in the system.

The IRS is capable of reflecting incident wireless signals, as a plane containing numerous passive reflecting elements constitutes it. As the demand for enhanced performance in various wireless communication systems continues to rise, there is a simultaneous increase in expectations for advanced wireless communication technologies. Beyond merely seeking an improved performance, there is a growing demand for solutions that offer low deployment costs and minimal power consumption. In response to this demand, intelligent reflecting surface technology has emerged. This technology aims to effectively enhance the performance of wireless communication systems while adhering to the requirements of cost effectiveness and energy efficiency. Each reflecting element of IRS has the capability to apply a phase shift to the incident signal, and when acting in unison, all reflective elements

can jointly adjust their phase shifts [5]. The IRS is extensively used in wireless communications to enhance the communication performance in various ways [6]. By adaptively adapting the amplitude and phase shift of the reflective elements, the IRS can reconfigure the wireless propagation environment and enhance the desired signals [7–9], thereby effectively addressing channel fading and interference. Through the collaborative design of transmission beamforming at the transmitter and reflective beamforming at the IRS, communication systems assisted by IRS can achieve optimal transmission power [10,11] and maximum energy efficiency [12,13]. The system performance of IRS-assisted non-orthogonal multiple-access and orthogonal multiple-access networks for downlink and uplink transmission is described [14]. In practical application, the IRS stands out due to its light weight, low deformation, and flexible size adjustment. These characteristics simplify the installation and disassembly processes, allowing for easy and adaptable deployment. IRS can serve as an auxiliary device in wireless communication systems and can be flexibly integrated into it, with high compatibility.

1.1. Motivation and Contributions

The integration of ambient backscatter and IRS is explored across various communication scenarios. A hybrid device-to-device (D2D) communication paradigm is introduced to consider the impact of environmental factors on communication performance [15]. A new scheme has been designed to improve the error rate performance of environmental backscattering by using an IRS located in its proximity [16]. A framework based on deep reinforcement learning has been proposed to jointly optimize IRS and reader beamforming, which can promote effective environmental backscatter communication [17]. Motivated by these studies, we propose a novel approach, called BackCom-IRS, that utilizes the combination of IRS and backscatter to improve secure communication and mitigate the effects of eavesdropping. This research aims to maximizing the signal-to-interference-plus-noise ratio (SINR) at the legitimate user under the allowable maximum SINR at the eavesdropper via the proposed scheme to combat active eavesdropping.

Specifically, our proposed approach, BackCom-IRS, leverages the power of interference signals through backscattering to improve the security communication rate, with higher eavesdropper power leading to greater benefits for secure communication. This paper proposes a method to enhance system security by limiting the SINR at the eavesdropper. Meanwhile, we jointly optimize the IRS reflection coefficient and the source beamforming vector to maximize the SINR at the legal user. The optimization problem is non-convex so it is challenging to solve the optimization problem. To solve the non-convex optimization problem, we developed an alternation optimization algorithm. Transform the optimization problem into two convex problems and then optimize each of them alternatively. These two convex problems are positive semi-definite programs that can be solved using existing convex optimization solvers. The eavesdropper in this paper passively eavesdrops and sends interference signals. By leveraging the power of the interference signal through backscattering, the proposed scheme improves the legal user's SINR. Simulation results prove the efficacy of the BackCom-IRS approach in enhancing communication system security.

1.2. Organization

The rest of the paper is structured as follows. Section 2 discusses the related works. Section 3 presents the system model and optimization problem formulation. The alternating optimization method is presented in Section 4. Section 5 presents numerical results and discussion. Finally, the conclusion and future work is drawn in Section 6.

2. Related Works

The use of the IRS can increase the data rate of legitimate receivers while reducing the data rate of eavesdroppers, thereby enhancing the system's security rate. The prevalent strategies for mitigating eavesdropping attacks such as artificial noise (AN) [1] and multi-antenna beamforming [2] suffer from high energy consumption, additional hardware costs,

or optimization difficulties due to the high correlation between legitimate and illegitimate links. To maximize the security rate, Yu et al. jointly optimized the transmitted information beam, AN, and reflection coefficient [18]. Cui et al. investigated how to maximize the security rate of the communication system when the transmission power is fixed, and the reflection parameters set at the IRS are limited [4]. Shen et al. maximized the security rate of the multi-input single-output (MISO) communication via joint majorization of the emission covariance at the source and the phase shift matrix at the IRS [19]. A secure wireless body area networks' (WBAN) transmission scheme based on IRS-assisted reinforcement learning is proposed, which enables coordinators to jointly optimize sensor encryption keys and transmission power, as well as IRS phase shift combat active eavesdropping [20]. This scheme also involves the balance of secure transmission games between coordinators and eavesdroppers, which is not covered in the system model studied in this paper.

The uniqueness of the backscatter channel provides important insights into the physical layer security of communication systems [3]. In backscatter communication systems, a backscatter transmitter modulates and reflects received radio frequency (RF) signals to transmit data, rather than generating RF signals independently [21]. This unique mechanism presents distinct challenges and opportunities for securing information transmission. Backscatter communication is generally categorized into three types: monostatic backscatter communication, bistatic backscatter communication, and ambient backscatter communication [22]. Ambient backscatter communication utilizes available ambient RF sources in the environment [23,24]. The characteristics of backscatter channels can be utilized to generate security keys. The unique features of backscatter communication can be used to establish security keys and thus enhance the security of the communication system. A lightweight cryptography-based approach to address the security of backscatter communication is presented in [25]. Ambient backscatter communication, which utilizes existing RF signals in the environment, can be leveraged for secure key generation. The randomness and variability in ambient signals can be used to generate cryptographic keys, enhancing the security of communication between devices. Although cryptography can achieve better security performance, it has limitations that rely on key generation, which can result in high communication overhead and computational complexity [3]. In order to break these limitations, research on physical layer security suitable for the characteristics of backscatter channels has been developed. The method of physical layer security is to utilize the characteristics of wireless channels to prevent eavesdroppers from obtaining information from transmitters. Physical layer security can be not only an alternative to cryptography but also a complement to enhance encryption technology. In addition, injecting artificially generated noise can deteriorate the eavesdropper's channel conditions to enhance secure transmission [26].

Backscatter communication systems can use jamming to enhance security. The presence of interference in the backscatter channel can provide a diversity of communication paths, and the diversity of paths may make it more challenging for eavesdroppers to jam communications. Since backscatter devices utilize ambient signals or dedicated sources in the environment, they may not be as susceptible to traditional jamming techniques. This resilience contributes to the security of the communication link. The maximization of confidentiality in multi-input multi-output (MIMO) backscatter wireless systems is investigated by jointly optimizing the power supply of the injected AN and the precoding matrix [27]. An interference-based multi-tag scheduling method is proposed, which selects one tag for data transmission and another for AN generation to have a deleterious effect on the eavesdropper [28]. Backscatter systems can be designed to be resilient to traditional eavesdropping methods, offering a more secure communication channel. Backscatter communication can be used for secure localization and authentication in applications where device positioning and identity verification are critical. Backscatter communication is well suited for Internet of Things (IoT) applications where security and energy efficiency are crucial due to the low-power nature of backscatter devices. The researches of [29] provided an optimization framework that maximizes the secrecy rate of backscatter communications

in multi-cell non-orthogonal multiple access networks and the reflection coefficients of the backscatter nodes are optimized for the presence of multiple eavesdroppers in each cell. To summarize, the inherent characteristics of backscatter communication systems, including their low power consumption, resistance to jamming, and adaptability to the RF environment, provide opportunities to enhance security in diverse applications, ranging from IoT networks to secure key generation. The combination of IRS and backscatter has been shown to have advantages in suppressing interference signals [30].

IRS [4,18–20] and backscatter [27–29] have demonstrated good performance, respectively, in physical layer security across various communication scenarios. As mentioned in the above works, the combination of IRS and backscatter has been developed to enhance the communication performance [15–17,30]. In secure communication, this combined technology deserves more in-depth research, especially under different communication scenarios. In this paper, the proposed scheme is developed for a MISO communication system to enhance communication security by combating active eavesdropping. We jointly optimize the transmission power of the transmitter and the reflection coefficient of the IRS to maximize the SINR of the legal user.

3. System Model and Optimization Problem Formulation

Consider an IRS-based backscatter wireless communication system countermeasure against active eavesdropping, as shown in Figure 1. A source (Alice), an IRS, a legitimate user (Bob), and an eavesdropper (Willie) constitute the communication system of this paper. In this system, Alice continuously transmits information to all directions. Willie is sending interference signals to prevent Bob from receiving the required signals to eavesdrop. Generally, the stronger the interference signals from an eavesdropper like Willie, the lower the communication system security is, which needs the IRS to enhance this system's security. The IRS, as a transmitter, aims to convert all received signals into desired signals through backscattering. The signal processed by IRS uses the interference signal from Willie to ensure the communication safety of legal user Bob. The number of antennas equipped by Alice is N, while Willie and Bob are equipped with one antenna each. IRS has L elements. It is assumed that all channels in the system experience quasi-static flat fading. Additionally, we consider that the channel state information (CSI) of all the involved channels in the system is precisely and accurately known in order to determine the limit of the security rate. We assume the frequency is non-selective and constant in each fading block.

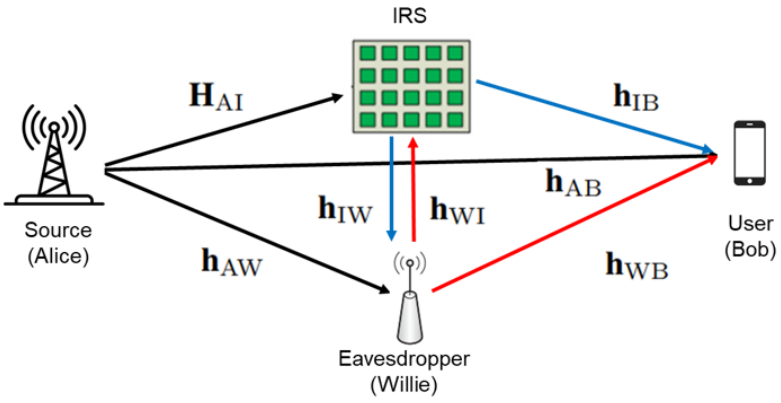

Figure 1. An IRS-aided backscatter wireless communication system under active eavesdropper's attack.

The channel gains from Alice to Bob, from the IRS to Bob, from Willie to Bob, from Willie to the IRS, from Alice to the IRS, from the IRS to Willie, and from Alice to Willie are represented by the following notations: $\mathbf{h}_{AB} \in \mathbb{C}^{N\times 1}$, $\mathbf{h}_{IB} \in \mathbb{C}^{L\times 1}$, $\mathbf{h}_{WB} \in \mathbb{C}^{1\times 1}$, $\mathbf{h}_{WI} \in \mathbb{C}^{L\times 1}$, $\mathbf{H}_{AI} \in \mathbb{C}^{L\times N}$, $\mathbf{h}_{IW} \in \mathbb{C}^{1\times L}$, and $\mathbf{h}_{AW} \in \mathbb{C}^{1\times N}$. The beamforming vector used by Alice to transmit the desired signal s is denoted by $\mathbf{w} \in \mathbb{C}^{N\times 1}$, while the beamforming vector used by Willie to transmit the interference signal a is represented by $\mathbf{v} \in \mathbb{C}^{1\times 1}$. The signals s and a represent the transmitted signals from Alice, the le-

gitimate transmitter, and Willie, the eavesdropper, respectively. In addition, $\mathbb{E}[|s|^2] = 1$ and $\mathbb{E}[|a|^2] = 1$. n_{B} and n_{W} represent the Gaussian white noise at Bob and Willie, respectively. These noises have zero mean and variances of σ_{B}^2 and σ_{W}^2, respectively. The amplitude and phase shift incurred by the l-th reflective element of the IRS are represented by $\mathbf{\Theta} = \mathrm{diag}(\beta_1 e^{j\alpha_1}, \beta_2 e^{j\alpha_2}, \cdots, \beta_L e^{j\alpha_L})$ with $\alpha_l = [0, 2\pi]$, $l \in \mathcal{L} = \{1, 2, \cdots, L\}$ and $\beta_l = [0, 1]$. In this model, we do not consider the interaction of IRS-neighboring reflective units and assume that each IRS reflective unit reflects the signal independently. Due to strong path loss, we overlook signals that were reflected multiple times by the IRS. After the above design and construction of the whole system, the received signals at Bob and Willie can be respectively formulated as

$$y_{\mathrm{B}} = \mathbf{h}_{\mathrm{AB}}^H \mathbf{w} s + \mathbf{h}_{\mathrm{WB}}^H \mathbf{v} a + \mathbf{h}_{\mathrm{IB}}^H \mathbf{\Theta} (\mathbf{h}_{\mathrm{AI}} \mathbf{w} s + \mathbf{h}_{\mathrm{WI}} \mathbf{v} a) + n_{\mathrm{B}}, \tag{1}$$

$$y_{\mathrm{W}} = \mathbf{h}_{\mathrm{AW}}^H \mathbf{w} s + \mathbf{h}_{\mathrm{IW}}^H \mathbf{\Theta} (\mathbf{H}_{\mathrm{AI}} \mathbf{w} s + \mathbf{h}_{\mathrm{WI}} \mathbf{v} a) + n_{\mathrm{W}}. \tag{2}$$

In this system, the backscattering of signals through IRS does not need to distinguish the source signal s and the interference signal a. The goal of this system is to maximize the SINR at Bob γ while we constrained Willie's SINR ξ by setting the maximum value. The transmit powers at Alice and Willie are represented as P_s and P_a, respectively. Define $\boldsymbol{\theta} = [\beta_1 e^{j\theta_1}, \beta_2 e^{j\theta_2}, \cdots, \beta_L e^{j\theta_L}]^H$. The problem of this system is expressed as

$$\max_{\boldsymbol{\theta}, \mathbf{w}} \quad \gamma = \frac{\left| \mathbf{h}_{\mathrm{AB}}^H \mathbf{w} + \mathbf{h}_{\mathrm{IB}}^H \mathbf{\Theta} (\mathbf{H}_{\mathrm{AI}} \mathbf{w} + \mathbf{h}_{\mathrm{WI}} \mathbf{v}) \right|^2}{\sigma_{\mathrm{B}}^2 + \left| \mathbf{h}_{\mathrm{WB}}^H \mathbf{v} \right|^2}, \tag{3}$$

$$s.t. \quad \mathrm{Tr}(\mathbf{w}\mathbf{w}^H) \leq P_s, \tag{4}$$

$$\theta_l \leq 1, \forall l \in \mathcal{L}, \tag{5}$$

$$\xi \leq \varepsilon. \tag{6}$$

The SINR at Bob is primarily dependent on two key variables: the beamforming vector $\mathbf{w}$ used by Alice and the reflection coefficient vector $\boldsymbol{\theta}$ utilized by the IRS. The SINR at Willie is formulated as

$$\xi = \frac{\left| \mathbf{h}_{\mathrm{AW}}^H \mathbf{w} + \mathbf{h}_{\mathrm{IW}}^H \mathbf{\Theta} (\mathbf{H}_{\mathrm{AI}} \mathbf{w} + \mathbf{h}_{\mathrm{WI}} \mathbf{v}) \right|^2}{\sigma_{\mathrm{W}}^2}. \tag{7}$$

The goal of this system model is to jointly optimize the transmission power of the transmitter and the reflection coefficient of the IRS to maximize the SINR of the legitimate user Bob, while considering the constrain that the signal-to-interference-plus-noise ratio of the eavesdropper is below the threshold. The optimization problem in this model is non-convex. To solving this optimization problem involves transforming problem (3) into a quadratically constrained quadratic programming (QCQP) problem. Subsequently, finding a sub-optimal solution to problem (3) involves employing Alternating Optimization (AO) optimization methods.

4. Alternation Optimization

We develop an alternating optimization algorithm to solve problem (3). Due to the coupling between the variables $\boldsymbol{\theta}$ and $\mathbf{w}$, directly solving the non-convex problem (3) can be challenging. Specifically, we address this non-convex problem by iteratively solving two sub-problems: sub-problem 1, which focuses on optimizing the beamforming vector $\mathbf{w}$ with a fixed reflection coefficient vector $\boldsymbol{\theta}$, and sub-problem 2, which focuses on optimizing $\boldsymbol{\theta}$ with a fixed $\mathbf{w}$.

Before optimizing these two sub-problems respectively, we need to convert the objective function equivalently. Since $\mathbf{\Theta} = \mathrm{diag}\{\boldsymbol{\theta}^H\}$, that expression can be converted to

$$\mathbf{h}_{\mathrm{AB}}^H\mathbf{w} + \mathbf{h}_{\mathrm{IB}}^H\mathbf{\Theta}(\mathbf{H}_{\mathrm{AI}}\mathbf{w} + \mathbf{h}_{\mathrm{WI}}\mathbf{v}) = \mathbf{h}_{\mathrm{AB}}^H\mathbf{w} + \boldsymbol{\theta}^{\boldsymbol{H}}\mathbf{\Phi}\mathbf{w} + \boldsymbol{\theta}^H\mathbf{a}. \tag{8}$$

$\mathbf{\Phi} = \mathrm{diag}\left\{\mathbf{h}_{\mathrm{IB}}^H\right\}\mathbf{H}_{\mathrm{AI}}$ and $\boldsymbol{a} = \mathrm{diag}\left\{\mathbf{h}_{\mathrm{IB}}^H\right\}\mathbf{h}_{\mathrm{WI}}\mathbf{v}$. Then Equation (8) is transformed as:

$$\mathbf{h}_{\mathrm{AB}}^H\mathbf{w} + \boldsymbol{\theta}^{\boldsymbol{H}}\mathbf{\Phi}\mathbf{w} + \boldsymbol{\theta}^H\mathbf{a} = ([\boldsymbol{\theta}^H, 1][\mathbf{\Phi}^H, \mathbf{h}_{\mathrm{AB}}]^H)\mathbf{w} + \boldsymbol{\theta}^H\mathbf{a} = \hat{\boldsymbol{\theta}}\hat{\mathbf{\Phi}}\mathbf{w} + \boldsymbol{\theta}^H\mathbf{a}, \tag{9}$$

letting $\hat{\boldsymbol{\theta}} = [\boldsymbol{\theta}^H, 1]^H$ and $\hat{\mathbf{\Phi}} = [\mathbf{\Phi}^H, \mathbf{h}_{\mathrm{AB}}]^H$. Convert expression (6) to

$$\hat{\boldsymbol{\theta}}\hat{\mathbf{\Phi}}\mathbf{w} + \boldsymbol{\theta}^H\mathbf{a} = \hat{\boldsymbol{\theta}}\hat{\mathbf{\Phi}}\mathbf{w} + [\boldsymbol{\theta}^H, 1]^H[\boldsymbol{a}^H, 0]^H = \hat{\boldsymbol{\theta}}\hat{\mathbf{\Phi}}\mathbf{w} + \hat{\boldsymbol{\theta}}\hat{\boldsymbol{a}}, \tag{10}$$

assuming $\hat{\boldsymbol{a}} = [\boldsymbol{a}^H, 0]^H$. Letting $\hat{\mathbf{w}} = [\mathbf{w}^H, 1]^H$, and $\check{\mathbf{\Phi}} = [\hat{\mathbf{\Phi}}, \hat{\boldsymbol{a}}]^H$, expression (7) can be transformed into

$$\hat{\boldsymbol{\theta}}\hat{\mathbf{\Phi}}\mathbf{w} + \hat{\boldsymbol{\theta}}\hat{\boldsymbol{a}} = \hat{\boldsymbol{\theta}}(\hat{\mathbf{\Phi}}\mathbf{w} + \hat{\boldsymbol{a}}) = \hat{\boldsymbol{\theta}}\check{\mathbf{\Phi}}\hat{\mathbf{w}}. \tag{11}$$

Therefore, the objective equation can be deduced as

$$\left|\mathbf{h}_{\mathrm{AB}}^H\mathbf{w} + \mathbf{h}_{\mathrm{IB}}^H\mathbf{\Theta}(\mathbf{H}_{\mathrm{AI}}\mathbf{w} + \mathbf{h}_{\mathrm{WI}}\mathbf{v})\right|^2 = \hat{\boldsymbol{\theta}}^H\check{\mathbf{\Phi}}\hat{\mathbf{w}}\hat{\mathbf{w}}^H\check{\mathbf{\Phi}}^H\hat{\boldsymbol{\theta}}. \tag{12}$$

Similarly, for the expression for the SINR at Willie, we transform it in the same way.

$$\mathbf{h}_{\mathrm{AW}}^H\mathbf{w} + \mathbf{h}_{\mathrm{IW}}^H\mathbf{\Theta}(\mathbf{H}_{\mathrm{AI}}\mathbf{w} + \mathbf{h}_{\mathrm{WI}}\mathbf{v}) = \hat{\boldsymbol{\theta}}\check{\boldsymbol{\delta}}\hat{\mathbf{w}}, \tag{13}$$

letting $\check{\boldsymbol{\delta}} = [\hat{\boldsymbol{\delta}}, \hat{\boldsymbol{b}}]^H$, $\hat{\boldsymbol{\delta}} = [\boldsymbol{\delta}^H, \mathbf{h}_{\mathrm{AW}}]^H$, $\hat{\boldsymbol{b}} = [\boldsymbol{b}^H, 0]^H$, $\boldsymbol{\delta} = \mathrm{diag}\left\{\mathbf{h}_{\mathrm{IW}}^H\right\}\mathbf{H}_{\mathrm{AI}}$ and $\boldsymbol{b} = \mathrm{diag}\left\{\mathbf{h}_{\mathrm{IW}}^H\right\}\mathbf{h}_{\mathrm{WI}}\mathbf{v}$.

Define $\hat{\mathbf{W}} = \hat{\mathbf{w}}\hat{\mathbf{w}}^H$, $\hat{\mathbf{\Theta}} = \hat{\boldsymbol{\theta}}\hat{\boldsymbol{\theta}}^H$, $\mathrm{rank}(\hat{\mathbf{W}}) = 1$, $\mathrm{rank}(\hat{\mathbf{\Theta}}) = 1$, $\hat{\mathbf{W}} \succeq \mathbf{0}$, $\hat{\mathbf{\Theta}} \succeq \mathbf{0}$. Then problem (3) is reformulated as

$$\max_{\hat{\mathbf{\Theta}}, \hat{\mathbf{W}}} \quad \hat{\boldsymbol{\theta}}^H\check{\mathbf{\Phi}}\hat{\mathbf{w}}\hat{\mathbf{w}}^H\check{\mathbf{\Phi}}^H\hat{\boldsymbol{\theta}} = \mathrm{Tr}(\hat{\mathbf{W}}\check{\mathbf{\Phi}}^H\hat{\mathbf{\Theta}}\check{\mathbf{\Phi}}), \tag{14}$$

$$s.t. \quad \mathrm{Tr}(\hat{\mathbf{W}}) \leq P_s + 1, \tag{15}$$

$$\hat{\boldsymbol{W}}_{N+1,N+1} = 1, \tag{16}$$

$$\hat{\mathbf{\Theta}}_{l,l} = 1,\ l \in \mathcal{L} \text{ or } l = L + 1, \tag{17}$$

$$\hat{\mathbf{\Theta}} \succeq \mathbf{0}, \mathrm{rank}(\hat{\mathbf{\Theta}}) = 1, \tag{18}$$

$$\hat{\mathbf{W}} \succeq \mathbf{0}, \mathrm{rank}(\hat{\mathbf{W}}) = 1, \tag{19}$$

$$\xi \leq \varepsilon. \tag{20}$$

We transform problem (14) into its relaxed form by removing the constraints of $\mathrm{rank}(\hat{\mathbf{W}}) = 1$ and $\mathrm{rank}(\hat{\mathbf{\Theta}}) = 1$. Subsequently, problem (14) is more tractable and can be solved using convex optimization techniques. This relaxation allows for a wider range of solutions. In addition, (14) can be expressed as

$$\mathrm{Tr}(\hat{\mathbf{W}}\check{\mathbf{\Phi}}^H\hat{\mathbf{\Theta}}\check{\mathbf{\Phi}}) = \mathrm{vec}(\check{\mathbf{\Phi}})^H\left(\hat{\mathbf{W}}^T \otimes \hat{\mathbf{\Theta}}\right)\mathrm{vec}(\check{\mathbf{\Phi}}). \tag{21}$$

Sub-problem 1 is transformed into optimizing $\hat{\mathbf{W}}$ under the condition of given $\hat{\mathbf{\Theta}}$. Sub-problem 2 is transformed into optimizing $\hat{\mathbf{\Theta}}$ with fixed $\hat{\mathbf{W}}$.

(sub-problem 1) When $\hat{\boldsymbol{\Theta}}$ is given,

$$\max_{\hat{\mathbf{W}}} \quad \mathrm{Tr}(\hat{\mathbf{W}}\check{\boldsymbol{\Phi}}^H\hat{\boldsymbol{\Theta}}\check{\boldsymbol{\Phi}}), \tag{22}$$

$$s.t. \quad \mathrm{Tr}(\hat{\mathbf{W}}) \leq P_s + 1, \tag{23}$$

$$\hat{\boldsymbol{W}}_{N+1,N+1} = 1, \tag{24}$$

$$\hat{\mathbf{W}} \succeq \mathbf{0}, \tag{25}$$

$$\xi \leq \varepsilon. \tag{26}$$

(sub-problem 2) When $\hat{\mathbf{W}}$ is given,

$$\max_{\hat{\boldsymbol{\Theta}}} \quad \mathrm{Tr}(\hat{\mathbf{W}}\check{\boldsymbol{\Phi}}^H\hat{\boldsymbol{\Theta}}\check{\boldsymbol{\Phi}}), \tag{27}$$

$$s.t. \quad \hat{\boldsymbol{\Theta}}_{l,l} = 1,\ l \in \mathcal{L} \text{ or } l = L+1, \tag{28}$$

$$\hat{\boldsymbol{\Theta}} \succeq \mathbf{0}, \tag{29}$$

$$\xi \leq \varepsilon. \tag{30}$$

The two subproblems resulting from the relaxation are convex. We can converge to an optimized solution for $\hat{\mathbf{W}}^*$ and $\hat{\boldsymbol{\Theta}}^*$ through iteratively solving the relaxed sub-problems 1 and 2 alternately. The above problem currently is a convex-positive semi-definite program (SDP), and it can be efficiently solved using existing convex optimization solvers. If $\hat{\mathbf{W}}^*$ and $\hat{\boldsymbol{\Theta}}^*$ are rank 1, restore $\hat{\mathbf{w}}^*$ and $\hat{\boldsymbol{\theta}}^*$ using singular value decomposition (SVD). When using the SVD for rank reduction, we can choose to keep the first few largest singular values and set the others to zero. This will result in a lower rank approximation, but not usually a complete reduction to rank one. A rank-one solution is a special case and is unlikely to be realized in the general case. In other cases, recover the approximate solution $\mathbf{w}^*$ and $\boldsymbol{\theta}^*$ using the standard Gaussian randomization method. This randomization method provides an approximate solution and is particularly useful when dealing with matrices of higher rank. The quality of the approximation depends on the properties of the original matrices and the size of the random matrix.

According to the above analysis, we recapitulate the overall algorithm for problem (3) as Algorithm 1. The objective value of optimizing problem (3) is represented by $\mathrm{R}^{(k)}$ with variables $\hat{\boldsymbol{\Theta}}^{(k)}$ and $\hat{\mathbf{W}}^{(k)}$ in the k-th iteration, while ϵ denotes a small threshold set to 0.001. The alternating optimization algorithm has many applications in wireless communication [4,5,18]. Algorithm 1 always converges, as the objective value is non-decreasing over iterations and has a finite upper bound.

Algorithm 1 Algorithm for Solving Problem (3)–(6)

1: **Initialization**: Set $k = 0$, $\hat{\boldsymbol{\theta}}^{(0)} = 1_L$. Input variables: $\hat{\boldsymbol{\Theta}}^{(0)}, \hat{\mathbf{W}}^{(0)}$.
2: Compute $\hat{\boldsymbol{\Theta}}^{(0)} = \hat{\boldsymbol{\theta}}^{(0)H}\hat{\boldsymbol{\theta}}^{(0)}$; $\mathrm{R}^{(0)} = f(\hat{\mathbf{W}}^{(0)}, \hat{\boldsymbol{\Theta}}^{(0)})$, according to (14).
3: **repeat**
4: Set $k = k + 1$.
5: With given $\hat{\boldsymbol{\Theta}}^{(k-1)}$, optimize the sub-problem 1, $\hat{\mathbf{W}}^{(k)}$ by (13).
6: With given $\hat{\mathbf{W}}^{(k)}$, optimize the sub-problem 2, $\hat{\boldsymbol{\Theta}}^{(k)}$ by (14).
7: Compute $\mathrm{R}^{(k)} = f(\hat{\mathbf{W}}^{(k)}, \hat{\boldsymbol{\Theta}}^{(k)})$.
8: **until** $\frac{\mathrm{R}^{(k)} - \mathrm{R}^{(k-1)}}{\mathrm{R}^{(k)}} < \epsilon$.
9: Recover rank-one approximate solution output variables $\mathbf{w}^*$ and $\boldsymbol{\theta}^*$.

5. Numerical Results and Discussion

In order to evaluate the security of the proposed approach in this paper, numerical simulations were conducted on an IRS-assisted backscatter communication system. Additionally, for comparative analysis, this paper also provides several different schemes.

The first scheme considers the transmission scenario of a traditional wireless communication system that does not incorporate an IRS, which is expressed as Without-IRS. By comparing the performance of the IRS-assisted system against this Without-IRS scenario, we can evaluate the added benefits or improvements brought by the IRS. The optimization for this scheme is specifically for the beamformer $\mathbf{w}$. Therefore, it may not take advantage of the additional capabilities that an IRS can offer in terms of enhancing communication links, mitigating interference, or improving the overall system performance.

The second scheme is the wireless communication system assisted by passive reflection IRS, which is denoted by Reflection-IRS. This scheme involves the integration of an IRS into the wireless communication system. In this system, the IRS acts as a passive relay, reflecting signals to enhance communication links. This scheme jointly optimizes the IRS reflection coefficient $\boldsymbol{\theta}$ and the source beamformer $\mathbf{w}$. The optimization process considers both the reflection properties of the IRS and the beamforming at the source. In contrast, the difference in the scheme proposed in this paper is that the IRS in the backscatter system utilizes the interference from the eavesdropper to enhance the receiving power of the legitimate user. This scheme is used to compare the effects of backscatter technology for IRS-assisted communication systems.

The third scheme involves only optimizing the reflection coefficient vector of the IRS using the maximum ratio transmission (MRT), referred to as MRT-IRS. In this approach, the beamforming vector of the source is not involved in optimization. The primary optimization in the MRT-IRS scheme is directed towards the IRS reflection coefficient vector. The goal is to maximize the received signal power at the legal user by adjusting the IRS reflections. By optimizing only the IRS reflection coefficients and not involving the source beamforming vector, it provides a reference for evaluating the impact of IRS reflections alone on the system performance. This scheme simplifies the optimization process and could limit the overall performance compared to schemes that optimize both the source and the IRS.

The last scheme is a relay. By introducing a relay with a set number of antennas and specific transmit power, the performance of this relay-based system can be compared with the IRS-assisted system. This scheme employs a relay with four antennas in place of the IRS, and its position is set to be identical to the IRS in the BackCom-IRS approach for comparison purposes. This positioning ensures a fair and relevant comparison between the two approaches. Unlike the IRS-assisted system, which primarily reflects signals to enhance communication, the relay scheme actively amplifies and forwards signals. The transmit power of this relay is denoted by P_r.

The link from Alice to Willie is modeled as a slow-fading Rayleigh channel. The channel gain from the IRS to Bob follows a Rician distribution with a Rician factor of 3 on a small scale. The path loss model for all channels in the system is denoted by $PL = PL_0 - 10lg(d/d_0)$ dB. The path loss at the reference distance of $d = d_0$ and $d_0 = 1$ m is denoted by $PL_0 = -30$ dB. The transmit power at Alice is $P_s = 9$ dBW. The transmit power of relay is $P_r = 0.1$ W. The noise variance is $\sigma^2 = 10^{-5}$. The distances from Alice to Bob, Alice to the IRS, Alice to Willie, the IRS to Bob, Willie to Bob, and Willie to the IRS are $d_{\mathrm{AB}} = 60$ m, $d_{\mathrm{AI}} = 55$ m, $d_{\mathrm{AW}} = 55$ m, $d_{\mathrm{IB}} = 15$ m, $d_{\mathrm{WB}} = 15$ m, and $d_{\mathrm{WI}} = 15$ m, respectively. The summary of the parameters is presented in Table 1.

Table 1. Parameters setting.

Parameter	Value
Rician factor	$\kappa = 3$
Path loss	$PL_0 = -30$ dB $d_0 = 1$ m
Transmit power at Alice	$P_s = 9$ dBW
Transmit power of relay	$P_r = 0.1$ W
Noise variance	$\sigma^2 = 10^{-5}$
Distances	$d_{AB} = 60$ m, $d_{AI} = 55$ m, $d_{AW} = 55$ m, $d_{IB} = 15$ m, $d_{WB} = 15$ m, $d_{WI} = 15$ m

Figure 2 shows the SINR at user Bob in the BackCom-IRS scheme as a function of the iteration number t under randomly generated observations. It represents a typical result selected from several generated observations. In this case, $P_a = 9$ dBW, $L = 40$. As the iterations progress, the SINR at the legal user Bob tends to stabilize. When the number of iterations reaches ten, the objective function converges to 10^{-3} and the convergence is monotonically increasing.

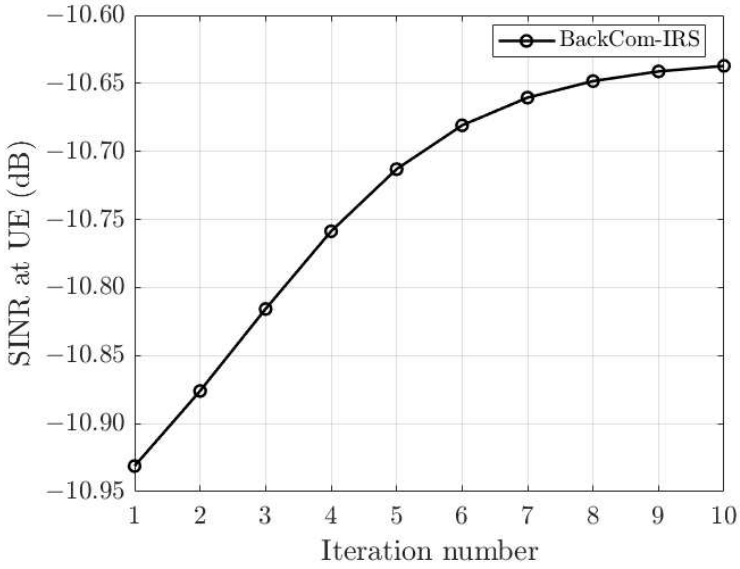

Figure 2. Convergence of the BackCom-IRS scheme in a random observation.

Figure 3 shows that the SINR at Bob changes with the transmission power of the eavesdropper Willie. It can be seen from this figure that the SINR at Bob decreases as P_a increases. Increasing the transmission power at the eavesdropper Willie is detrimental to the user's received information. Higher transmission power of the eavesdropper negatively affects the communication link to user Bob. The proposed scheme outperforms the MRT-IRS scheme, traditional reflection IRS scheme, Relay scheme, and Without-IRS scheme, as demonstrated in the simulation results. This implies that, even under conditions of increased eavesdropper power, the proposed scheme is more effective in maintaining a satisfactory SINR at user Bob. Especially in comparison to the conventional reflection-IRS, the IRS with integrated backscatter exhibits a more substantial difference in the SINR as the eavesdropper's transmit power increases. This implies that backscatter technology can enhance the security of IRS-assisted communication systems. The detailed numerical results presented in Figure 3 are available in Appendix A Table A1. In [4,31], as the transmit power at Tx increases, IRS-assisted systems exhibit better secrecy rate gains. In [14], the downlink network IRS-aided system has better performance than full-dupl decode-and-forward relay (FDR)-aided system in the high signal-to-noise ratio (SNR). In the low-SNR, the IRS transmission experiences severe path loss and performs worse than FDR-aided systems.

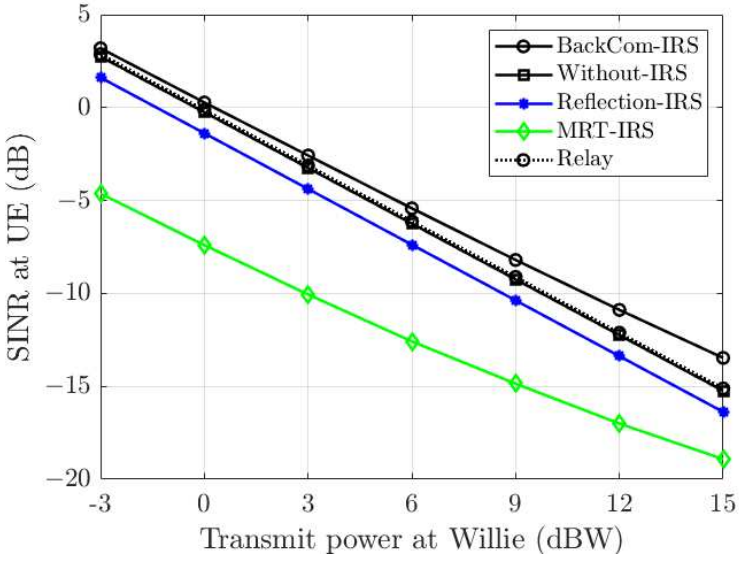

Figure 3. The SINR γ at Bob versus the transmit power P_a at Willie.

Figure 4 illustrates how the SINR at Bob is affected by the total number of reflective elements L at the IRS. This figure shows that the SINR at Bob increases as the number of elements L increases. The number of IRS elements does not affect the Without-IRS and relay scheme. At first, the relay scheme and the without-IRS scheme will be better than the scheme proposed in this paper. As the number of IRS components increases, the scheme proposed in this paper will achieve higher performance gains than other schemes. This implies that a larger number of elements in the IRS contributes positively to the security of the wireless communication system. Both [31,32] indicate that adding more IRS reflective elements is beneficial for improving the secrecy rate in the IRS-assisted system. When the number of reflecting elements is small, the received signal at legal user Bob is dominated by the direct link other than the IRS-assisted link. The performance differences between the proposed scheme and the MRT-IRS scheme increase with the reflecting elements of IRS. This indicates that as the number of reflective elements increases, the joint optimization of the beamforming vector of the source and the reflection coefficient of the IRS becomes more flexible, and the performance gain also becomes higher. The detailed numerical results presented in Figure 4 are available in Appendix A Table A2.

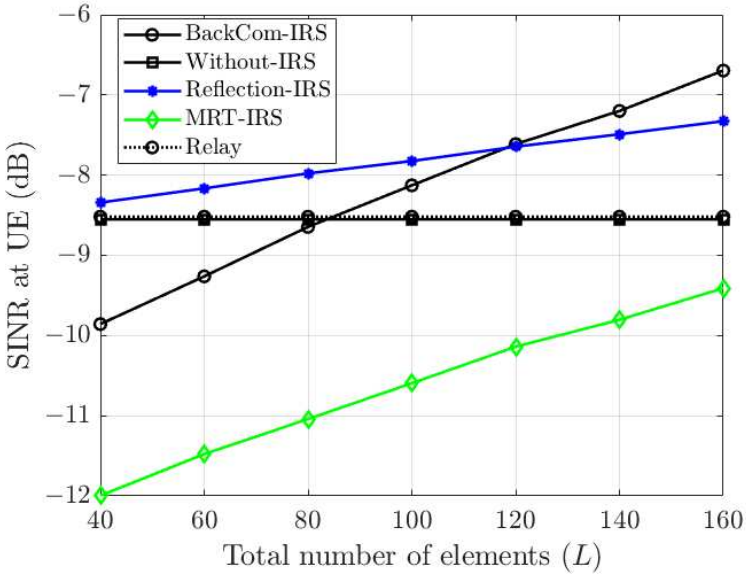

Figure 4. The SINR γ at Bob versus the total number of reflecting elements L at the IRS.

6. Conclusions and Future Work

This paper proposed a scheme to realize secure communication using an IRS backscatter communication system. Under the constraint of the SINR of the eavesdropper, this paper obtained the maximum SINR of the user via the alternate optimization algorithm to solve the non-convex objective problem. Alice's beamforming vector and the IRS's reflection coefficient are jointly optimized. The simulation results validate that the BackCom-IRS scheme outperforms other schemes such as MRT-IRS, reflection-IRS, without-IRS, and relay schemes. This work proved the research value of BackCom-IRS in secure communication. It demonstrates that the addition of the IRS can improve the security performance of communication systems and that IRS using backscattering can provide better security than traditional IRS used only for reflection, especially when the interference of the eavesdropper is significant. Due to the system model in this paper being based on perfect CSI, and in practical situations, especially in secure communication at the physical layer, it is difficult to obtain a perfect CSI. Therefore, future work will focus on further studying the aforementioned issues under imperfect CSI. Additionally, this paper adopts the basic MISO model. In the era of rapid development of communication technology, MIMO communication models are more widely used. The IRS MIMO communication will be investigated in future work.

Author Contributions: Conceptualization, Y.M. and J.Z.; methodology, Y.M.; software, Y.M.; formal analysis, Y.M. and Y.S.; writing—original draft preparation, Y.M.; review and editing and validation, Y.S. and J.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IRS	Intelligent reflecting surface
D2D	Device-to-device
SINR	Signal-to-interference-plus-noise ratio
AN	Artificial noise
MISO	Multi-input single-output
WBAN	Wireless body area networks
RF	Radio frequency
MIMO	Multi-input multi-output
IoT	Internet of Things
CSI	Channel state information
QCQP	Quadratically constrained quadratic programming
AO	Alternating optimization
SDP	Semi-definite program
SVD	Singular value decomposition
MRT	Maximum ratio transmission
FDR	Full-dupl decode-and-forward relay
SNR	Signal-to-noise ratio

Appendix A

Table A1. SINR γ at Bob versus the transmit power P_a at Willie.

P_a (dBW)	Backcom-IRS	Without-IRS	Reflection-IRS	MRT-IRS	Relay
−3	6.4931	5.9826	2.1984	−0.0519	6.4661
0	3.5940	2.9916	−0.7978	−2.7373	3.4750
3	0.6943	−0.0040	−3.7958	−5.3080	0.4795
6	−2.1082	−3.0017	−6.7949	−7.6457	−2.5183
9	−4.8598	−6.0006	−9.7944	−9.8836	−5.5171
12	−7.5319	−9.0000	−12.7941	−11.8968	−8.5166
15	−10.0842	−11.9997	−15.7940	−13.6630	−11.5163

Table A2. SINR γ at Bob versus the total number of reflecting elements L at the IRS.

L	Backcom-IRS	Without-IRS	Reflection-IRS	MRT-IRS	Relay
40	−9.8575	−8.5505	−8.3417	−11.9961	−8.5184
60	−9.2622	−8.5505	−8.1648	−11.4785	−8.5184
80	−8.6452	−8.5505	−7.9777	−11.0418	−8.5184
100	−8.1271	−8.5505	−7.8240	−10.5945	−8.5184
120	−7.6126	−8.5505	−7.6448	−10.1392	−8.5184
140	−7.1994	−8.5505	−7.4898	−9.8034	−8.5184
160	−6.6957	−8.5505	−7.3268	−9.4099	−8.5184

References

1. Li, W.; Ghogho, M.; Chen, B.; Xiong, C. Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis. *IEEE Commun. Lett.* **2012**, *16*, 1628–1631. [CrossRef]
2. Zhou, X.; Ganti, R.K.; Andrews, J.G. Secure wireless network connectivity with multi-antenna transmission. *IEEE Trans. Wirel. Commun.* **2010**, *10*, 425–430. [CrossRef]
3. Saad, W.; Zhou, X.; Han, Z.; Poor, H.V. On the physical layer securityof backscatter wireless systems. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 3442–3451. [CrossRef]
4. Cui, M.; Zhang, G.; Zhang, R. Secure wireless communication via intelligent reflecting surface. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1410–1414. [CrossRef]
5. Chu, Z.; Hao, W.; Xiao, P.; Shi, J. Intelligent reflecting surface aided multi-antenna secure transmission. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 108–112. [CrossRef]
6. Wu, Q.; Zhang, S.; Zheng, B.; You, C.; Zhang, R. Intelligent reflecting surface-aided wireless communications: A tutorial. *IEEE Trans. Commun.* **2021**, *69*, 3313–3351. [CrossRef]
7. Wu, C.; Yan, S.; Zhou, X.; Chen, R.; Sun, J. Intelligent reflecting surface (IRS)-aided covert communication with Warden's statistical CSI. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1449–1453. [CrossRef]
8. Wu, Q.; Zhang, R. Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. *IEEE Commun. Mag.* **2020**, *58*, 106–112. [CrossRef]
9. Gong, C.; Yue, X.; Wang, X.; Dai, X.; Zou, R.; Essaaidi, M. Intelligent reflecting surface aided secure communications for NOMA networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2761–2773. [CrossRef]
10. Wu, Q.; Zhang, R. Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 5394–5409. [CrossRef]
11. Zhou, X.; Yan, S.; Wu, Q.; Shu, F.; Ng, D.W.K. Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 532–547. [CrossRef]
12. Huang, C.; Zappone, A.; Alexandropoulos, G.C.; Debbah, M.; Yuen, C. Reconfigurable intelligent surfaces for energy efficiency in wireless communication. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 4157–4170. [CrossRef]
13. Zhou, S.; Xu, W.; Wang, K.; Di Renzo, M.; Alouini, M.-S. Spectral and energy efficiency of IRS-assisted MISO communication with hardware impairments. *IEEE Commun. Lett.* **2020**, *9*, 1366–1369. [CrossRef]
14. Cheng, Y.; Li, K.H.; Liu, Y.; Teh, K.C.; Vincent Poor, H. Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 3988–4000. [CrossRef]
15. Lu, X.; Jiang, H.; Niyato, D.; Kim, D.I.; Han, Z. Wireless-powered device-to-device communications with ambient backscattering: Performance modeling and analysis. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 1528–1544. [CrossRef]
16. Idrees, S.; Jia, X.; Durrani, S.; Zhou, X. Design of intelligent reflecting surface (IRS)-boosted ambient backscatter systems. *IEEE Access* **2022**, *10*, 65000–65010. [CrossRef]

17. Jia, X.; Zhou, X. IRS-assisted ambient backscatter communications utilizing deep reinforcement learning. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 2374–2378. [CrossRef]
18. Yu, X.; Xu, D.; Sun, Y.; Ng, D.W.K.; Schober, R. Robust and secure wireless communications via intelligent reflecting surfaces. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 2637–2652. [CrossRef]
19. Shen, H.; Xu, W.; Gong, S.; He, Z.; Zhao, C. Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. *IEEE Commun. Lett.* **2019**, *23*, 1488–1492. [CrossRef]
20. Xiao, L.; Hong, S.; Xu, S.; Yang, H.; Ji, X. IRS-aided energy-efficient secure WBAN transmission based on deep reinforcement learning. *IEEE Trans. Commun.* **2022**, *70*, 4162–4174. [CrossRef]
21. Kimionis, J.; Bletsas, A.; Sahalos, J.N. Bistatic backscatter radio for power-limited sensor networks. In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 353–358.
22. Van Huynh, N.; Hoang, D.T.; Lu, X.; Niyato, D.; Wang, P.; Kim, D.I. Ambient backscatter communications: A contemporary survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2889–2922. [CrossRef]
23. Al-Badarneh, Y.H.; Alouini, M.-S.; Georghiades, C.N. Performance analysis of monostatic multi-tag backscatter systems with general order tag selection. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1201–1205. [CrossRef]
24. Vestakis, M.; Alevizos, P.N.; Vougioukas, G.; Bletsas, A. Multistatic narrowband localization in backscatter sensor networks. In Proceedings of the 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Kalamata, Greece, 25–28 June 2018; pp. 1–5.
25. Vahedi, E.; Ward, R.K.; Blake, I.F. Security analysis and complexity comparison of some recent lightweight RFID protocols. In Proceedings of the 4th International Conference, CISIS 2011, Torremolinos-Málaga, Spain, 8–10 June 2011; Volume 6694, pp. 92–99.
26. Wang, H.-M.; Zheng, T.; Xia, X.-G. Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 94–106. [CrossRef]
27. Yang, Q.; Wang, H.-M.; Zhang, Y.; Han, Z. Physical layer security in MIMO backscatter wireless systems. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 7547–7560. [CrossRef]
28. Han, J.Y.; Kim, M.J.; Kim, J.; Kim, S.M. Physical layer security in multi-tag ambient backscatter communications—Jamming vs. Cooperation. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Republic of Korea, 25–28 May 2020; pp. 1–6.
29. Khan, W.U.; Liu, J.; Jameel, F.; Raza Khan, M.T.; Ahmed, S.H.; Jäntti, R. Secure backscatter communications in multi-cell NOMA networks: Enabling link security for massive IoT networks. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 213–218.
30. Xu, S.; Liu, J.; Zhang, J. Resisting undesired signal through IRS-based backscatter communication system. *IEEE Commun. Lett.* **2021**, *25*, 2743–2747. [CrossRef]
31. Yu, X.; Xu, D.; Schober, R. Enabling secure wireless communications via intelligent reflecting surfaces. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
32. Chen, J.; Liang, Y.-C.; Pei, Y.; Guo, H. Intelligent reflecting surface: A programmable wireless environment for physical layer security. *IEEE Access* **2019**, *7*, 82599–82612. [CrossRef]