Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4553805, 10 pages
https://doi.org/10.1155/2022/4553805

Research Article

IRS Backscatter-Assisted Security Transmission against Proactive Eavesdropping

Jianling Wang

School of Electronic Information Engineering, Henan Institute of Technology, Xinxiang 453003, China

Correspondence should be addressed to Jianling Wang; 15137372785@hait.edu.cn

Received 16 March 2022; Revised 10 April 2022; Accepted 21 April 2022; Published 5 May 2022

Academic Editor: Lisheng Fan

In this paper, we consider the IRS backscatter-assisted physical layer security, aimed at countering smart eavesdroppers capable of sending jamming signals. Specifically, the eavesdropper increases the eavesdropping rate by sending jamming signals and is able to adjust the transmission strategy according to the received beamforming. By using IRS backscatter communication, the jamming signal sent by the eavesdropper is converted into a useful signal and transmitted. By designing the beamforming of the base station and the IRS phase shift matrix, we established the original optimization problem. Since the eavesdropper's sending strategy is adjusted according to the received signal, we transform the original problem into two subproblems. In the first subproblem, we obtain the eavesdropper's transmit beamforming; in the second subproblem, we optimize the transmit beam alternately with the IRS phase shift matrix. Simulation results demonstrate the superiority of our proposed scheme.

1. Introduction

With the widespread popularity of 5G technology, more and more smart devices are flooding every aspect of people's lives [1, 2]. These smart devices usually require high-speed communication rates to ensure user experience [3–5]. At this time, an unavoidable problem is to ensure the user's communication security [6, 7].

The secure communication in the usual sense focuses on the encryption and encoding of the signal, and the security of the communication is ensured by the key and the complex encryption algorithm [8, 9]. However, the encoding and decoding of encrypted communication will take up extra information, and it is impossible to judge whether the encryption algorithm is decrypted by eavesdroppers [10]. Therefore, physical layer security has received more attention [11].

Early research on user security focused on potential eavesdroppers, increasing the security rate by adding redundant information to the signal [12–15]. However, adding redundant noise will also bring more communication burden to users. Therefore, in the literature [16], etc., it is proposed to use the helper to interfere with the eavesdropper without consuming the transmission power of the user [17, 18].

In recent years, the research on active eavesdropping has also developed gradually [19, 20]. The main purpose of active eavesdropping is not to protect the communication process but to eavesdropper the communication of illegal users. The eavesdropper can send jamming beams to reduce the transmission rate of illegal users, so as to achieve the purpose of successful eavesdropping [21, 22].

Fighting an eavesdropper that uses active eavesdropping mode is a tough job because eavesdroppers can adjust the transmit beam to slow down the communication rate [23]. In this paper, we consider the use of IRS backscatter communication to convert the jamming signal sent by the eavesdropper into a useful signal, thereby increasing the security rate for the user [24, 25].

IRS backscatter is a technique that combines IRS with backscatter communications [26]. Specifically, IRS is a programmable smart material that can reconfigure the input signal to achieve system goals by rewriting the phase and channel [27]. It is worth noting that IRS is a passive device, so it does not need continuous function, which solves the problem of excessive energy consumption in traditional security communication.

There has been some progress in research on secure communications using IRS backscatter. The authors of [28] propose to use the IRS to assist secure communication, using the jamming beam sent by the eavesdropper to reduce the eavesdropper's signal-to-noise ratio, thereby increasing the security rate. The authors of [29] consider reencoding the received signal by backscattering the IRS to improve the user's acceptance rate. In [30], it further considers the multiuser case. However, none of these works consider the situation where the eavesdropper is actively listening.

In this paper, we consider eavesdroppers to intelligently send jamming signals based on received signals. Through the joint design of the transmit beam of the base station and the IRS phase shift matrix, the maximization of the user security rate is realized. The contributions of this paper are summarized as follows:

(1) We consider the security communication problem of eavesdroppers under active eavesdropping and maximize the security rate by designing the transmit beam of the base station and the phase shift matrix of the IRS

(2) We first pay attention to the design of the eavesdropper's transmit beam under proactive eavesdropping and design corresponding strategies according to the eavesdropper's transmit beam

(3) We use the alternate optimization method to jointly optimize the transmit beam of the base station and the phase shift matrix of the IRS

(4) The simulation results show that our proposed optimization method has a great improvement compared with the existing schemes

Notations: in this paper, we use uppercase letters for matrices, lowercase letters for scalars, and lowercase bold letters for vectors. C stands for the set of real numbers. For the matrix A, A^H represents its conjugate transpose. For the vector a, $\|a\|$ represents its norm.

The structure of this paper is as follows: In Materials and Methods, we first introduce the system model of IRS-assisted secure communication against intelligent listeners and then formulate the optimization problem that maximizes the secure rate. Then, we explore the transmission strategy of the intelligent listener and design the transmission strategy of the base station and the phase shift matrix of the IRS accordingly. In Results and Discussion, we conduct simulation experiments and discuss future work. Finally, we conclude this paper.

2. Materials and Methods

In this section, we first introduce the system model and then analyze the working patterns of eavesdroppers and users to establish an optimization problem. Next, we try to obtain the eavesdropper's transmit beam and then design the phase shift matrix of the base station's transmit beam and IRS based on the beamforming of the eavesdropper.

2.1. System Model. The system model is shown in Figure 1, including base station, legitimate receiver, and eavesdropper. We consider that the eavesdropper is a function that can carry out active eavesdropping; i.e., it can actively send interference signals to reduce the reachable rate of legitimate recipients, so as to achieve the purpose of eavesdropping. It is worth noting that the eavesdropper can obtain the channel state information between the emergency and legitimate receivers but cannot obtain the transmission strategy of the base station. We use IRS scatter communication to convert the jamming signal sent by the eavesdropper into a gain signal.

We set the base station to configure N antennas, both legitimate receivers and the illegitimate eavesdroppers are single antennas to receive, and the illegitimate eavesdropper takes K antennas to send jamming signals. Further, we assume that the elements of the IRS is M. At the same time, the eavesdropper configures multiple antennas to transmit interference information.

The accepted signal at the receiver is

$$y_t = h_{st}^H ws + h_{rt}^H \Phi(h_{sr}w + h_{sr}v)s + h_{et}vz + n_t, \tag{1}$$

where $h_{st} \in \mathbb{C}^{N\times 1}$ is the channel from the base station to the user, $w \in \mathbb{C}^{N\times 1}$ is the beamforming vector sent by base station, $s \in \mathbb{C}$ is the symbol from the base station, $h_{rt} \in \mathbb{C}^{M\times 1}$ is the channel from the IRS to the user, $\Phi \in \mathbb{C}^{M\times M}$ is the IRS phase shift matrix, $v \in \mathbb{C}^{K\times 1}$ is the beamforming vector sent by the eavesdropper, $z \in \mathbb{C}$ is the symbol from the eavesdropper, $h_{et} \in C^{K\times 1}$ is the channel from the eavesdropper to the user, and $n_t \in \mathbb{C}$ is the additive noise with zero mean and variance σ_t^2.

Similarly, the accepted signal at the eavesdropper is

$$y_e = h_{se}^H ws + h_{re}^H \Phi(H_{sr}w + H_{sr}v)s + \rho h_{ee}vz + n_e, \tag{2}$$

where $h_{se} \in \mathbb{C}^{N\times 1}$ is the channel from the base station to the eavesdropper, $h_{re} \in \mathbb{C}^{M\times 1}$ is the channel from the IRS to the eavesdropper, $\Phi \in \mathbb{C}^{M\times M}$ is the IRS phase shift matrix, $h_{ee} \in \mathbb{C}^{K\times 1}$ is the self-interference channel, and $n_e \in \mathbb{C}$ is the additive noise with zero mean and variance σ_e^2.

According to (1) and (2), we calculate the signal-to-interference-noise ratio of the receiver and the eavesdropper, respectively, as

$$\begin{aligned} \mathrm{SINR}_t &= \frac{\left|h_{st}^H w + h_{rt}^H \Phi(h_{sr}w + h_{sr}v)\right|^2}{\sigma_t^2 + |\rho h_{et}v|^2}, \\ \mathrm{SINR}_e &= \frac{\left|h_{se}^H w + h_{re}^H \Phi(h_{sr}w + h_{sr}v)\right|^2}{\sigma_e^2 + |\rho h_{ee}v|^2}. \end{aligned} \tag{3}$$

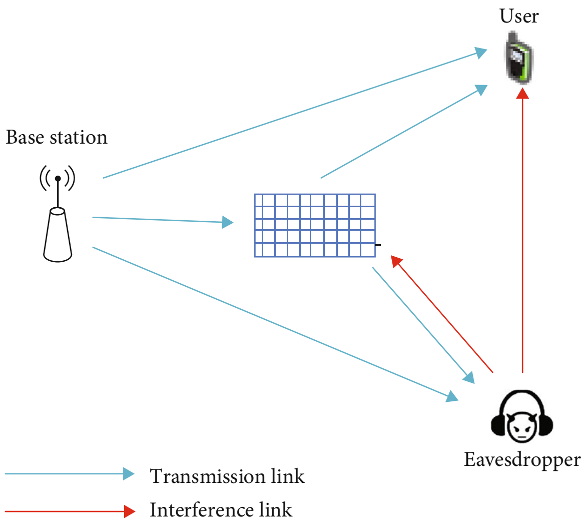

FIGURE 1: System model with IRS backscatter.

Then, we obtain the rate of the user and the eavesdropper as

$$\begin{aligned} R_t &= \log_2(1+\mathrm{SINR}_t), \\ R_e &= \log_2(1+\mathrm{SINR}_e). \end{aligned} \tag{4}$$

Then, we formulate the original problem in the following subsection.

2.2. Problem Formulation. Our goal is to maximize the security rate, which is defined as follows:

$$R_s = |R_t - R_e|^+, \tag{5}$$

where $|x|^+ = \max(x, 0)$ for any x.

Meanwhile, the sum energy is limited in the base station and the eavesdropper. The original problem is formulated as

$$\begin{aligned} &\max_{\{\boldsymbol{w},\boldsymbol{\Phi}\}} R_s \\ &\text{s.t.} \|\boldsymbol{w}\|^2 \le P_w \\ &|\theta_m| \le 1, m \in \mathcal{M} \end{aligned} \tag{6}$$

where $\mathcal{M}$ is the set of IRS elements. We assume that MIRS elements in this set.

It is worth noting that the original problem is strongly nonconvex since the optimization variables w and Φ are coupled in the objective of this problem. Further, the beamforming vector sent by the eavesdropper would be changed if we determine to send the beamforming in the base station and the IRS phase matrix. Hence, we need to obtain the relationship between the beamforming $\boldsymbol{v}$ and $\{w, \Phi\}$. In the next subsection, we would like to obtain the strategy of the eavesdropper.

2.3. Beamforming Acquisition for Eavesdropper. In this subsection, we will obtain the eavesdropper's transmit beamforming. It is worth noting that our purpose is not to design the eavesdropper's transmit beam but to simulate the eavesdropper's behavior pattern. We assume that the eavesdropper can select the corresponding transmission beam according to the transmission signal of the base station, and its purpose is to maximize the eavesdropping rate R_a, which is defined as

$$R_a = \begin{cases} R_t, & \text{if } R_t \le R_e, \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

The goal of the eavesdropper is to maximize the eavesdropping rate R_a according to the received signal y_e. Hence, the problem need to be solved by the eavesdropper is proposed as follows

$$\max_{v} R_a \tag{8}$$

$$\text{s.t.} \|v\|^2 \le P_e \tag{9}$$

By substituting the definition of R_a into the objective of (8), we obtain the following problem:

$$\max_{\boldsymbol{v}} R_t \tag{10}$$

$$\text{s.t.} \|v\|^2 \le P_e \tag{11}$$

$$R_t \le R_e \tag{12}$$

The objective of (10) is replaced as the transmission rate of the user with an additional constraint $R_t \le R_e$. For any given $\{w, \Phi\}$, (10) can be solved via Lagrangian dual method. In specific, we define that the optimal v^* in (10) can be decomposed as

$$v^* = \alpha h_{ee} + \beta h_{e,0}, \tag{13}$$

where $h_{e,0}$ is orthogonal to h_{ee} and maximum ratio to H_{sr}. (13) reveals that when the transmission rate is less than the eavesdropping rate. The beamforming vector in the eavesdropper would be zero. When the transmission rate is larger than the eavesdropping rate, the eavesdropper would firstly send jamming signals in the zeros mean of the self-interference channel to improve the eavesdropping rate as possible. When the transmission rate is too large or the maximum power of the eavesdropper is much too small, the eavesdropping rate would be decreased to reduce the transmission rate as much as possible. The results in (13) would be applied in the eavesdropper. Further, when the beamforming vector sent by base station is changed, the corresponding parameters in (13) would be also changed. But the structure of (13) is fixed.

However, since our goal is not to design the beamforming vector in the eavesdropper, we thus transform (10) into a feasibility analysis problem.

$$\text{find } w, \Phi \tag{14}$$

$$\text{s.t.} \|v\|^2 \le P_e \tag{15}$$

$$R_t \geq R_e \tag{16}$$

When (14) is solvable, the eavesdropping rate would be zero. Hence, we can use the results in (13) and substitute it into the original problem.

2.4. Proposed Solution of Original Problem. According to the beamforming design of the eavesdropper, we can obtain that the beamforming vector in (13) is the sending beamforming vector of the eavesdropper. Then, we obtain the following problem:

$$\max_{\{w,\Phi\}} R_s \tag{17}$$

$$\text{s.t.} \|w\|^2 \leq P_w \tag{18}$$

$$|\theta_m| \leq 1, m \in \mathcal{M} \tag{19}$$

$$= \alpha h_{ee} + \beta h_{e,0} \tag{20}$$

Problem (17) is still a nonconvex problem since w and Φ are coupled. Then, we first try to obtain the optimal beamforming vector for any given Φ.

We transform (17) into the following problem:

$$\max_{w} \frac{\left|h_{st}^H w + h_{rt}^H \Phi (h_{sr} w + h_{sr} v)\right|^2}{\left|h_{se}^H w + h_{re}^H \Phi (h_{sr} w + h_{sr} v)\right|^2} \tag{21}$$

$$\text{s.t.} \|w\|^2 \leq P_w \tag{22}$$

$$v = \alpha h_{ee} + \beta h_{e,0} \tag{23}$$

(21) is still nonconvex; we need to apply semidefinite relaxation method to solve it. In specific, we define a new variable $W = ww^H$ with a rank-1 constraint. Then, we define other parameters in the eavesdropper as

$$H_e = \text{diag}\left\{h_{re}^H\right\} h_{sr}, \tag{24}$$

$$f_e = \text{diag}\left\{h_{re}^H\right\} h_{jr} v, \tag{25}$$

$$G_e^{(1)} = \left[H_e^H ; h_{se}\right], \tag{26}$$

$$f_e^{(1)} = \left[f_e^{(1)}, 0\right], \tag{27}$$

$$G_e = \left[G_e^{(1)} ; f_e^{(1)}\right]. \tag{28}$$

Similarly, we define the parameters in the user as

$$H_u = \text{diag}\left\{h_{ru}^H\right\} h_{sr}, \tag{29}$$

$$f_u = \text{diag}\left\{h_{ru}^H\right\} h_{jr} v, \tag{30}$$

$$G_u^{(1)} = \left[H_u^H ; h_{su}\right], \tag{31}$$

$$f_u^{(1)} = \left[f_u^{(1)}, 0\right], \tag{32}$$

```
Input:$k = 0$, $\Phi^{(0)} = I$, $w^{(0)} = 1/2P_u l$
Output:$\Phi^*$, $w^*$
Repeat:
    Obtain the beamforming vector $v$;
    For fixed $\Phi^{(k)}$, obtain the optimal $W^{(k)}$ in (34);
    Recover rank-1 approximation solutions $w^{(k)}$;
    For fixed $w^{(k)}$, obtain the optimal $\Phi^{(k+1)}$ in (38);
    Set $k = k + 1$;
    If norm $(w^{(k+1)} - w^{(k)}) \leq \varepsilon$:
        Break;
```

Algorithm 1: Beamforming and phase matrix design.

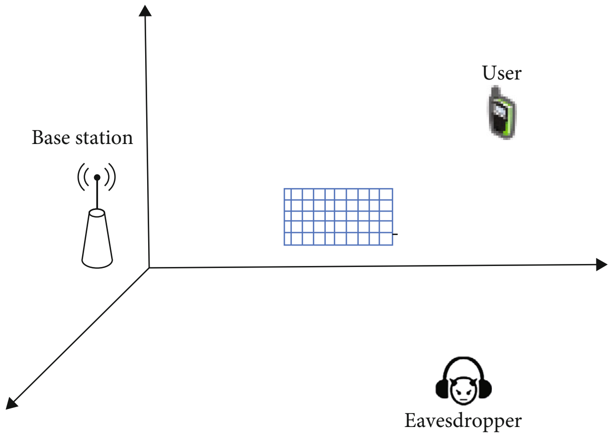

Figure 2: Simulation setup.

$$G_u = \left[G_e^{(1)} ; f_e^{(1)}\right]. \tag{33}$$

It is worth noting that G_e and $G_u$are both the nonlinear function with respect to the matrix W. By substituting (24) and (29) into (21), we obtain the following expression:

$$\max_{W} \frac{Tr(WG_u)}{\sigma_u^2} - \frac{Tr(WG_e)}{\sigma_e^2} \tag{34}$$

$$\text{s.t.} Tr(W) \leq P_w \tag{35}$$

$$v = \alpha h_{ee} + \beta h_{e,0} \tag{36}$$

$$\text{Rank}(W) = 1 \tag{37}$$

We ignore the rank-1 constraint in (34) and use successive convex approximation (SCA) method to obtain the suboptimal solution of (34). Finally, we apply the rank-1 constraint by Gaussian random method.

Then, we solve the IRS phase matrix for fixed beamforming vector. We first reformulate the following problem:

$$\max_{W} \frac{Tr\left(\Phi G_u^{(1)}\right)}{\sigma_u^2} - \frac{Tr\left(\Phi G_e^{(1)}\right)}{\sigma_e^2} \tag{38}$$

Table 1: Temperature and wildlife count in the three areas covered by the study.

Location	Variable	Value
Location of base station	L_b	(0, 0, 10)
Location of user	L_u	(200, 100, 0)
Location of eavesdropper	L_e	(100, -50, 0)
The channel power gain at a reference distance of $d_0 = 1m$	ρ_0	-30 dB
Maximum power in user	P_u	20 dB
Maximum power in eavesdropper	P_e	20 dB
Power of noise	σ_e	-60 dB
Number of antennas in base station	N	20
Number of elements in IRS	M	30
Number of antennas in eavesdropper	K	50

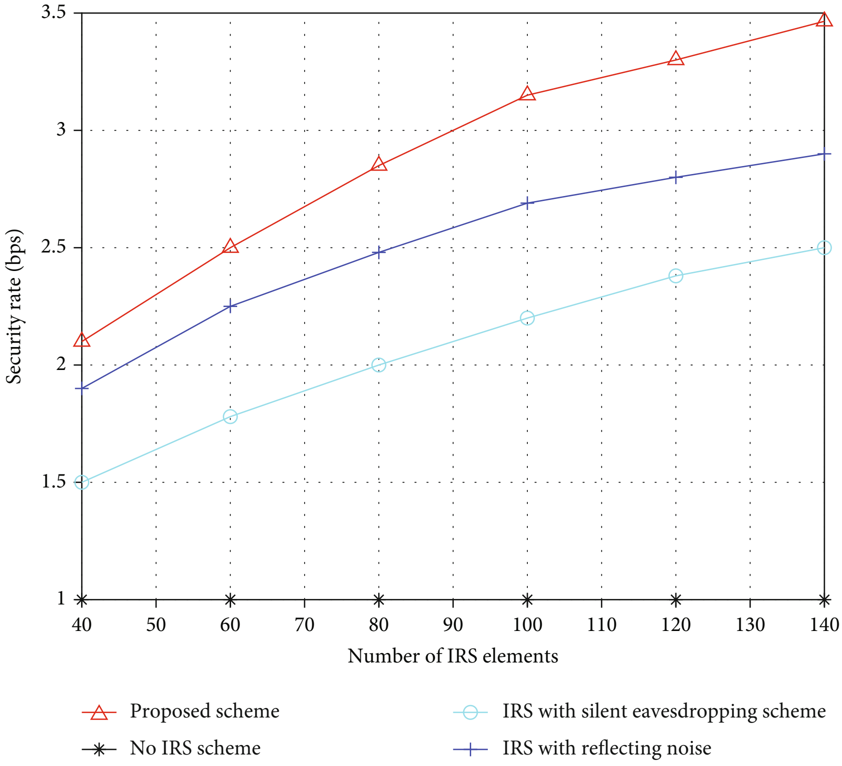

Figure 3: Security rate versus number of IRS element.

$$\text{s.t.} Tr(\Phi) \leq 1 \tag{39}$$

$$v = \alpha h_{ee} + \beta h_{e,0} \tag{40}$$

$$\text{Rank}(\Phi) = 1 \tag{41}$$

Similar as the solution of (34), (38) can be solved by SCA method with ignoring the rank-1 constraint.

The overall algorithm is proposed in Algorithm 1.

Algorithm 1 reveals that the objective function in (34) and (38) does not increase in each iteration, which means that the proposed method will converge to a local optimal solution.

3. Results and Discussion

In this section, we first show the numerical results in the first subsection. We apply the simulation in MATLAB. All results are obtained via Monte Carlo method for 1000 times. We provide the specific parameters and show the superiority of the proposed scheme. Further, we discussed about the finished work and outlook for future work.

3.1. Numerical Results. The specific scenario of our simulation is shown in Figure 2. We assume that the base station is located at the origin (0, 0, 10), the user is located at (200, 100, 0), the IRS is located at (100, 50, 5), and the eavesdropper is located at (100, -50, 0). All signals are empirical

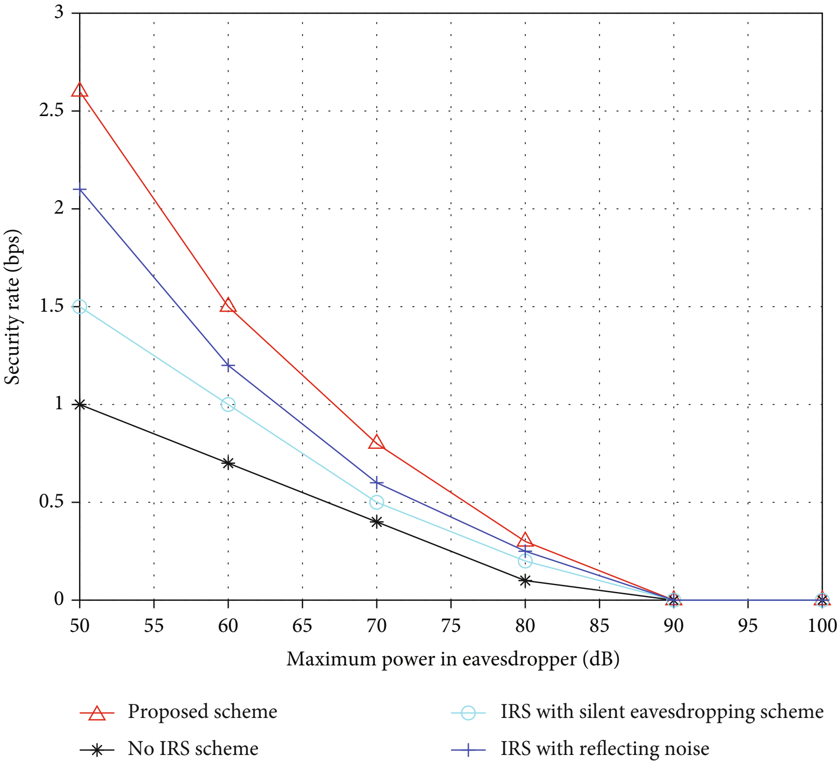

Figure 4: Security rate versus maximum power in eavesdropper.

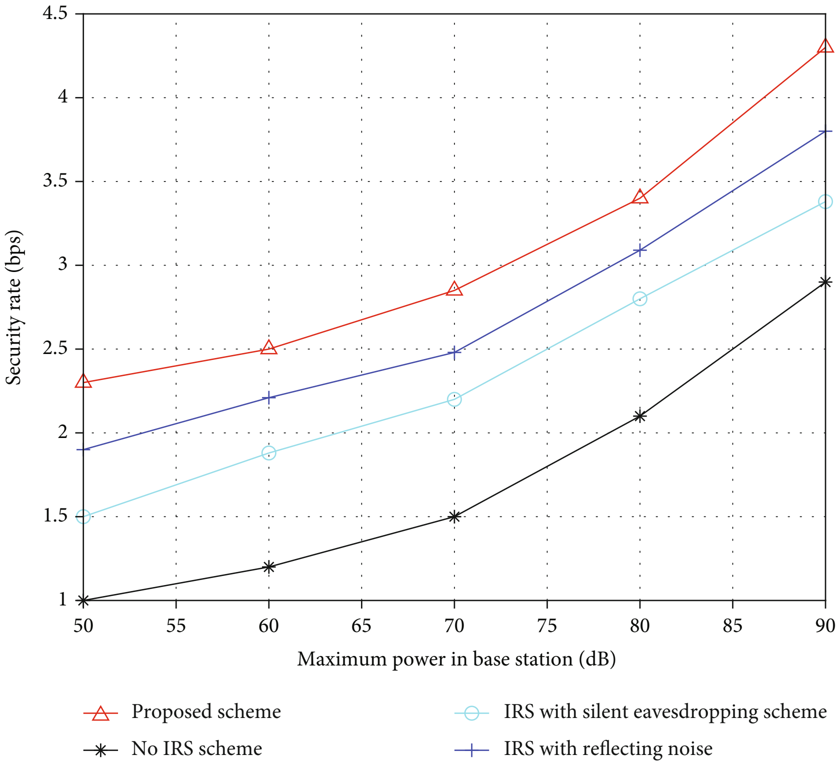

Figure 5: Security rate versus maximum power in base station.

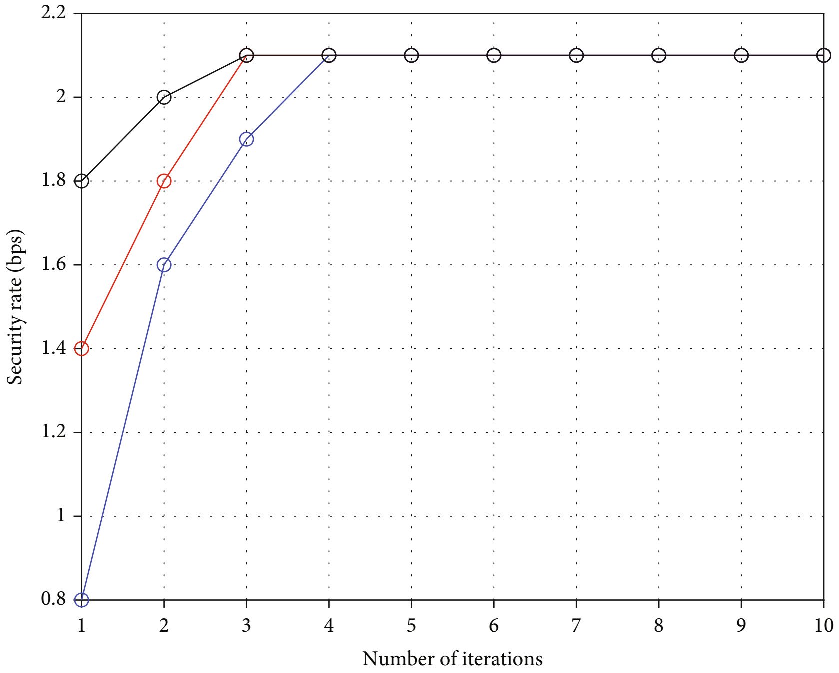

Figure 6: Security rate versus number of iterations.

fading channels, and we use Rayleigh fading model. The specific setting of Rayleigh fading channel is formulated as follows:

$$f(v) = \frac{v}{\sigma_v} \exp\left(-\frac{v^2}{2\sigma_v^2}\right). \tag{42}$$

All parameters are reflected in Table 1.

In this section, we provide four schemes for comparison. The first one is our proposed scheme, the second one is the security transmission without IRS, the third one is the IRS with silent eavesdropping, and the fourth one is the IRS with reflecting noise.

In Figure 3, we show the curve of the security rate versus the number of IRS elements. It can be seen that our proposed scheme outperforms existing schemes. When IRS is not used, its performance does not change with the number of IRS elements. For the other three schemes, an increase in the number of IRS elements brings a significant performance improvement. Further, it can be observed that IRS with reflecting noise would get better performance with respect to IRS with silent eavesdropping since reflecting noise would not only increase the transmission rate but also decrease the eavesdropping rate. For our proposed scheme, the transmission rate would be much larger than the transmission rate in other scheme, which explain the superiority.

We further show the relationship between the security rate and the maximum power at the eavesdropper in Figure 4. It can be observed that when the maximum power at eavesdropper is limited, the security rate for our proposed scheme is better than other schemes, since we transform the jamming noise into useful information for user, which increase the transmission rate. In the scheme of IRS with reflecting noise, the transmission rate is limited by the maximum power in base station. If the eavesdropper's rate is large enough, it must be able to eavesdrop. A possible situation is that the communication rate at this time is close to 0, but this is obviously not what we want to see. Therefore, in order to increase the secure communication rate, a common means is to increase the maximum power of the base station, as we show in the next figure.

Figure 5 shows the variation of the security rate with the power of the base station. When the power of the base station increases, the security rate also increases. In an extreme case, we can send the signal in the null space of the eavesdropping channel and set the corresponding phase of the IRS to the null space as well. At this time, the eavesdropping ability of the eavesdropper can be completely eliminated. However, it is more common that we add some redundant information to improve the overall security performance. When the maximum power in the base station is quite small, our proposed scheme would obtain better performance since the IRS would tend to transform the signal to user but not to the eavesdropper. When the maximum power in the base station is large, the security rate would be better.

In Figure 6, we simulate the performance of the proposed iterative algorithm. It can be found that the convergence speed of the algorithm is very fast for different initial point, and the convergence is achieved in the second or the third iteration. It has been provided that the convergence of the proposed algorithm is not related to the original point selection. Further, although we have proved the convergence of the algorithm in the article, the simulation results intuitively show the convergence speed of our proposed algorithm, which will greatly improve the efficiency of the algorithm.

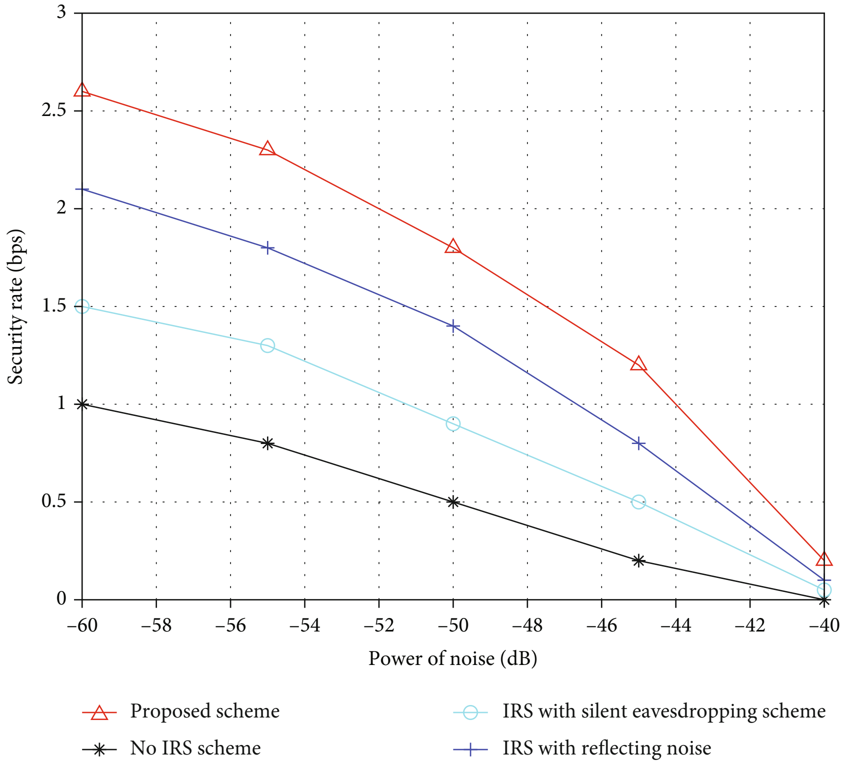

Figure 7: Security rate versus power of noise.

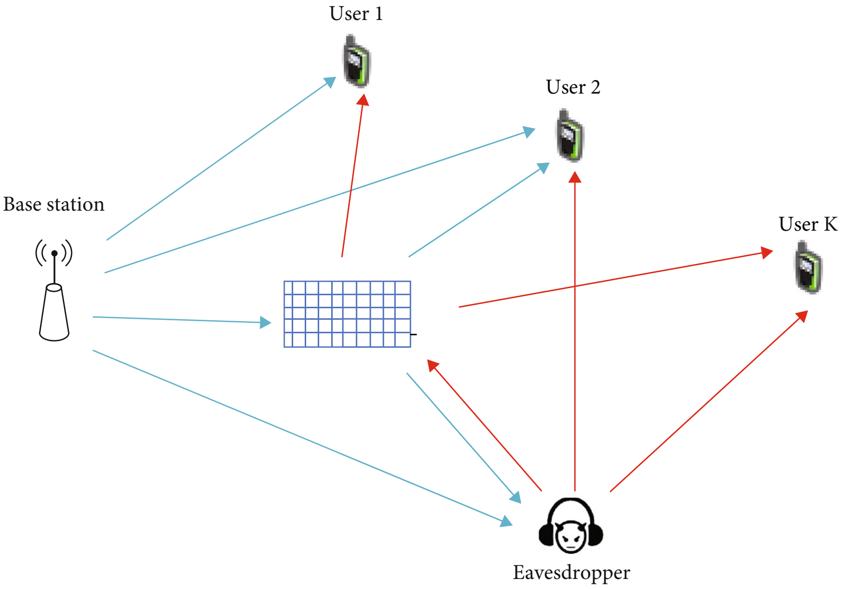

Figure 8: System model with multiuser.

Figure 7 shows the curve of the security rate as a function of noise power. As the noise power increases, the security rate decreases. Although the increase of noise will also reduce the eavesdropping ability of the eavesdropper, we set the background noise power are the same. The increasing of the power of noise would decrease the eavesdropping rate. It can be obtained from the definition of the security rate, and the security rate depends on the transmission capacity of the channel. When the transmission rate is quite small, the security rate would be very small. However, the proposed algorithm can still maintain good performance when the noise power is large, which shows its robustness.

4. Discussion

In this paper, we consider the use of IRS backscatter to enhance secure communications. Our innovations focus on the way eavesdroppers use active eavesdropping and the ability to modify the transmit beam based on environmental factors. We suppress the eavesdropping ability of eavesdroppers through the joint design of the transmit beam of the base station and the phase shift matrix of the IRS.

It is worth noting that we consider the single-user scenario, where it is feasible for the IRS to reencode the information into useful information, but the single-user scenario is relatively rare in practical applications. If there are multiple pairs of users in the same communication area, as shown in Figure 8, the IRS recoding will cause interference to other users, thereby reducing the overall communication efficiency. How to apply IRS backscatter communication to multiuser scenarios requires our further research.

On the other hand, IRS backscatter communication has better performance compared to IRS reflection noise. However, this result cannot be verified theoretically; i.e., we cannot formulate a theorem about this. Therefore, we will also try to prove the optimality condition of backscattering in the follow-up work.

5. Conclusions

In this paper, we use IRS to assist secure communication, and we propose a method for the joint design of base station beam vectors and IRS phase shift matrices, aiming to improve the security rate for users. For the proposed optimization problem, we first consider the case where the eavesdropper sends beams and substitutes its results into the original problem. Further, we carry out an alternate optimization design of the beam vector of the base station and the IRS phase shift matrix. The simulation results show that our proposed algorithm has a better performance improvement compared to the existing benchmark algorithms.

Data Availability

All synthetic data are available on MATLAB.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by Zigbee-based intelligent wireless monitoring system for urban lighting, Funding Project for Young Key Teachers in Henan Province (grant number 12A510011).

References

[1] S. Han, S. Xu, W.-X. Meng, and L. He, "Channel-correlation-enabled transmission optimization for MISO wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 20, no. 2, pp. 858–870, 2021.

[2] J. Du, C. Jiang, J. Wang, Y. Ren, and M. Debbah, "Machine learning for 6G wireless networks: carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 122–134, 2020.

[3] X. Yu, D. Xu, Y. Sun, D. W. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2637–2652, 2020.

[4] S. Xu, S. Han, W.-X. Meng, Y. Du, and L. He, "Multiple-Jammer-aided secure transmission with receiver-side correlation," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3093–3103, 2019.

[5] W. Yan, X. Yuan, and X. Kuai, "Passive beamforming and information transfer via large intelligent surface," *IEEE Wireless Communications Letters*, vol. 9, no. 4, pp. 533–537, 2020.

[6] 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 of Things Journal*, vol. 7, no. 2, pp. 1350–1363, 2020.

[7] Q. Wu and R. Zhang, "Joint active and passive beamforming optimization for intelligent reflecting surface assisted SWIPT under QoS constraints," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1735–1748, 2020.

[8] J. Hu, Y. C. Liang, and Y. Pei, "Reconfigurable intelligent surface enhanced multi-user MISO symbiotic radio system," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2359–2371, 2021.

[9] M. Hua, L. Yang, Q. Wu, C. Pan, C. Li, and A. L. Swindlehurst, "UAV-Assisted intelligent reflecting surface symbiotic radio system," *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5769–5785, 2021.

[10] Z. Wang, P. Babu, and D. P. Palomar, "Design of PAR-constrained sequences for MIMO channel estimation via majorization-minimization," *IEEE Transactions on Signal Processing*, vol. 64, no. 23, pp. 6132–6144, 2016.

[11] X. Guan, Q. Wu, and R. Zhang, "Joint power control and passive beamforming in IRS-assisted spectrum sharing," *IEEE Communications Letters*, vol. 24, no. 7, pp. 1553–1557, 2020.

[12] B. Di, H. Zhang, L. Li, L. Song, Y. Li, and Z. Han, "Practical hybrid beamforming with finite-resolution phase shifters for reconfigurable intelligent surface based multi-user communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4565–4570, 2020.

[13] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 787–790, 2020.

[14] Z. Q. Luo, W. K. Ma, A. M. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20–34, 2010.

[15] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: a new wireless security paradigm," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 152–159, 2017.

[16] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1449–1461, 2016.

[17] D. Hu, Q. Zhang, P. Yang, and J. Qin, "Proactive monitoring via jamming in amplify-and-forward relay networks," *IEEE Signal Processing Letters*, vol. 24, no. 11, pp. 1714–1718, 2017.

[18] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394–5409, 2019.

[19] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[20] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4157–4170, 2019.

[21] C. Huang, S. Hu, G. C. Alexandropoulos et al., "Holographic MIMO surfaces for 6G wireless networks: opportunities, challenges, and trends," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 118–125, 2020.

[22] L. Subrt and P. Pechac, "Intelligent walls as autonomous parts of smart indoor environments," *IET Communications*, vol. 6, no. 8, pp. 1004–1010, 2012.

[23] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 162–169, 2018.

[24] S. Nie, J. M. Jornet, and I. F. Akyildiz, "Intelligent environments based on ultra-massive MIMO platforms for wireless communication in millimeter wave and terahertz bands," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 7849–7853, Brighton, UK, 2019.

[25] P. del Hougne, M. Fink, and G. Lerosey, "Optimally diverse communication channels in disordered environments with tuned randomness," *Nature Electronics*, vol. 2, no. 1, pp. 36–41, 2019.

[26] S. Y. Park and D. I. Kim, "Intelligent reflecting surface-aided phaseshift backscatter communication," in *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, pp. 1–5, Taichung, Taiwan, 2020.

[27] C. L. Holloway, E. F. Kuester, J. A. Gordon, J. O'Hara, J. Booth, and D. R. Smith, "An overview of the theory and applications of metasurfaces: the two-dimensional equivalents of metamaterials," *IEEE Antennas and Propagation Magazine*, vol. 54, no. 2, pp. 10–35, 2012.

[28] L. Dai, B. Wang, M. Wang et al., "Reconfigurable intelligent surface-based wireless communications: antenna design, prototyping, and experimental results," *IEEE Access*, vol. 8, pp. 45913–45923, 2020.

[29] A. Pors and S. I. Bozhevolnyi, "Plasmonic metasurfaces for efficient phase control in reflection," *Optics Express*, vol. 21, no. 22, pp. 27438–27451, 2013.

[30] A. S. da Silva, F. Monticone, G. Castaldi, V. Galdi, A. Alú, and N. Engheta, "Performing mathematical operations with metamaterials," *Science*, vol. 343, no. 6167, pp. 160–163, 2014.