Secure beamforming for intelligent reflecting surface-assisted MISO systems

Kui Yang¹, Guangda Zang², Lingna Hu³, Guochen Pei²a), Shintaro Arai⁴, and Di He⁵

¹Southwest China Institute of Electronic Technology, Chengdu, China
²Institute of Wireless Communications, Shanghai Jiao Tong University, Shanghai, China
³Shanghai Institute of Satellite Engineering, Shanghai, China
⁴Department of Electrical and Electronic Engineering, Okayama University of Science, 1–1 Ridai-cho, Kita-ku, Okayama 700–0005, Japan
⁵Shanghai Key Laboratory of Navigation and Location-based Services, Shanghai Jiao Tong University, Shanghai 200240, China

a) peiguochen@sjtu.edu.cn

Abstract: This paper considers the scenario where the base station and legitimate user are blocked by obstacles and uses an intelligent reflecting surface (IRS) to assist communication. To improve physical layer security, we model the eavesdropper channel as the Rician channel and establish a mathematical model with the goal of minimizing eavesdropper’s rate subject to eavesdropper’s outage probability constraint and legitimate user’s secrecy rate constraint. The resulting problem is very challenging due to the continuous angle range of the eavesdropper’s outage probability constraint and the coupling constraints imposed by the IRS. We first use a Bernstein-Type inequality to transform the continuous constraints into discrete constraints and then propose an alternating algorithm to obtain a suboptimal solution. Numerical results show that the proposed algorithm can reduce the eavesdropper’s communication rate in different cases, which verifies the effectiveness of the proposed algorithm.

Keywords: Secure beamforming, intelligent reflecting surface

Classification: Wireless communication technologies

References

[1] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, “Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications,” IEEE Communications Letters, vol. 23, no. 9, pp. 1488-1492, Sept. 2019. DOI: 10.1109/LCOMM.2019.2924214.

[2] X. Guan, Q. Wu, and R. Zhang, “Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?,” IEEE Wireless Communications Letters, vol. 9, no. 6, pp. 778-782, Jun. 2020. DOI: 10.1109/LWC.2020.2969629.

[3] S. Hong, C. Pan, H. Ren, K. Wang, K. K. Chai, and A. Nallanathan, “Robust Transmission Design for Intelligent Reflecting Surface Aided Secure Communication Systems with Imperfect Cascaded CSI,” IEEE Transactions on Wireless Communications, vol. 20, no. 4, pp. 2487-2501, Apr. 2021. DOI: 10.1109/TWC.2020.3042828.

[4] F. Yang, G. Pei, L. Hu, G. Zang, L. Ding, S. Arai, and D. He, “Optimization of hybrid beamforming for multiuser massive MIMO Systems with individual SINR and SLL constraints,” IEICE Communications Express, Vol.10, No.1, pp. 24–29. 2020. DOI: 10.1587/comex.2020XBL0142.
S. Zhao, J. Liu, Y. Shen, X. Jiang and N. Shiratori, “Secure beamforming for full-duplex MIMO two-way untrusted relay systems,” in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3775-3790, Jun. 2020, DOI: 10.1109/TIFS.2020.3001733.

1 Introduction

Intelligent reflecting surface (IRS) is composed of a reflective surface and a control chip. The reflective surface is composed of a large number of reflecting elements and can reflect the incident signal in each reflecting element after phase change, thereby changing the wireless channel purposefully.

Secure communication can be carried out by using the IRS when the eavesdropper’s channel state information (CSI) is perfectly known [1][2]. By reasonably designing the beamforming matrix at the IRS end, the IRS can also greatly improve the security performance of communication when only the statistical characteristics of the eavesdropper’s CSI can be obtained [3]. However, due to the particularity of the eavesdropper’s role, we can often only obtain the location range of the eavesdropper based on past information. Due to the continuity of the range, it is more difficult to ensure secure communication.

This paper establishes a mathematical model with the goal of minimizing the eavesdropper’s rate subject to the eavesdropper’s outage probability constraint and the legitimate user’s secrecy rate constraint. We propose an alternating algorithm to obtain the local optimal solution. The numerical results show that the proposed algorithm can make the eavesdropper’s communication rate lower in different situations, which verifies the effectiveness of the algorithm.

2 System model and problem formulation

We consider a communication system with an IRS for auxiliary communication. As shown in Fig.1, a base station equipped with \( N \) antennas communicates with one legitimate user with the aid of an IRS equipped with \( M \) reflecting elements. The channel from the base station directly to the legitimate user and the channel from the base station directly to the eavesdropper are blocked by obstacles. The legitimate user and the eavesdropper are both equipped with one antenna.

![Fig. 1. IRS-assisted wireless secrecy communication system](image)

The received signals of the legitimate user and the eavesdropper are given as

\[
y_j = h_{bi}^H \Phi G w s(t) + n_j, \quad j = \begin{cases} b, & \text{user} \\ e, & \text{eavesdropper} \end{cases}
\]  

(1)

where \( h_{bi} \in \mathbb{C}^{M \times 1} \) and \( h_{be} \in \mathbb{C}^{M \times 1} \) denote the channel from the IRS to the legitimate user and the channel from the IRS to the eavesdropper, respectively. \( \Phi \in \mathbb{C}^{M \times M} \) denotes the reflection beamforming matrix of the IRS. \( G \in \mathbb{C}^{M \times N} \) denotes the channel matrix from the base station to the IRS. \( w \in \mathbb{C}^{N} \) denotes the beamforming vector of the base station. \( s(t) \) denotes the transmitted signal. \( n_b \sim \mathcal{CN}(0, \sigma_b^2) \) and \( n_e \sim \mathcal{CN}(0, \sigma_e^2) \) denote the additive white Gaussian noise. The reflection beamforming matrix of the IRS \( \Phi \) is subject to the constant...
modulus constraints, i.e.,
\[ \Phi = \text{diag}(\psi), \psi_m = e^{j\psi_m}, \psi_m \in [0, 2\pi]. \]  
(2)

In practical systems, the eavesdropper often hides its information. \( h_b \) and \( G \) can be perfectly known by channel estimation, and \( h_{\epsilon e} \) can be expressed as
\[ h_{\epsilon e} = \sqrt{P_f(d)} \left( \frac{K_{\epsilon e}}{K_{\epsilon e} + 1} h_{\epsilon e}^s(\theta) + \frac{1}{K_{\epsilon e} + 1} h_{\epsilon e}^n \right), \]  
(3)
where \( P_f(d) \) denotes the path loss related to distance \( d \), \( K_{\epsilon e} \) denotes the Rician factor, \( h_{\epsilon e}^s(\theta) \) denotes the line-of-sight channel, and \( h_{\epsilon e}^n \) denotes the non-line-of-sight channel. \( h_{\epsilon e} \) is composed of the response vector of the IRS, i.e.,
\[ a(\theta) = [1, e^{\frac{2\pi d_1 \sin \theta}{\lambda}}, e^{\frac{2\pi d_2 \sin \theta}{\lambda}}, \ldots, e^{\frac{2\pi (M-1)d_1 \sin \theta}{\lambda}}, 1]^T, \]  
(4)
where \( d_1 \) denotes the antenna spacing and \( \theta \) denotes the departure angle. The approximate range of the eavesdropper can only be obtained based on past information, which can be modeled as
\[ R_{\min} \triangleq \{d, \theta | \theta \in [\theta_{\min}, \theta_{\max}], d \in [d_{\min}, d_{\max}]\}. \]  
(5)

The communication rates of the legitimate user and the eavesdropper are expressed as
\[ R_e(w, \Phi) = \log_2(1 + \frac{h_{\epsilon e}^H \Phi g w \Phi h_{\epsilon e}}{\sigma_i^2}). \]  
(6)

To improve security performance, we require that the communication outage probability of eavesdropper is above a threshold \( 1 - p \) and have the following eavesdropper’s outage probability constraint.
\[ P_e(R_e(w, \Phi) \leq C_e) \geq 1 - p, \ e \in \{d, \theta | \theta \in [\theta_{\min}, \theta_{\max}], d \in [d_{\min}, d_{\max}]\}. \]  
(7)
To ensure the legitimate user’s communication performance, we require that the communication rate of the legitimate user is above a threshold \( C_b \) and have the following legitimate user’s secrecy rate constraint.
\[ R_s(w, \Phi) \geq C_b. \]  
(8)

We aim to minimize the eavesdropper’s rate \( R_e \) subject to the eavesdropper’s outage probability constraint in (7) and the legitimate user’s secrecy rate constraint in (8). Besides, \( \Phi \) is subject to the constant modulus constraints in (2) and \( w \) is subject to a total transmission power constraints at the base station. Thus, we have the following IRS-assisted secure beamforming problem
\[ P_0: \min_{w, \Phi} R_e \]  
\[ \text{s.t. (2), (7), (8),} \]  
\[ w w^H \leq P_0. \]

Compared with the secure beamforming problem (without an IRS) in [5], Problem \( P_0 \) is more complicated due to the coupling between the reflection beamforming matrix of the IRS \( \Phi \) and the beamforming vector of the base station \( w \). The non-convex element-wise constant modulus constraints in (2) are also difficult to handle. Most previous works on secure beamforming cannot be extended to address Problem \( P_0 \). In the following, we shall directly solve Problem \( P_0 \) based on problem reformulation and an alternating optimization method.

3 Problem reformulation

The constraint in (7) is a challenging non-convex constraint, and it restricts the communication rate within a location range. In this section, we reformulate the constraint in (7) into convex constraints.

By introducing an auxiliary matrix \( W = w w^H \), the constraint in (7) can be reformulated as
\[ P_e\left\{ \frac{h_{\epsilon e}^H F \Phi g W G W^H \Phi h_{\epsilon e}}{\sigma_i^2} + 2R e(K_{\epsilon e} h_{\epsilon e}^H(\theta) F \Phi g W G W^H \Phi h_{\epsilon e}(\theta)) \right\} \geq 1 - p, \ \theta \in [\theta_{\min}, \theta_{\max}]. \]  
(9)
The constraint in (9) can be reformulated as
\[ P_i (\mathbf{h}_{RE}^H \mathbf{X} \mathbf{h}_{RE}^H + 2 \text{Re}(\mathbf{X}^H \mathbf{h}_{RES}^H) + x \leq 0) \geq 1 - p, \quad \theta \in [\theta_{\min}, \theta_{\max}], \] 

where \( x = K_{i,0} \mathbf{h}_{RE}^H (\theta) \mathbf{X} \mathbf{h}_{RE}^H (\theta) - (2^C - 1) \sigma^2 \left( \frac{K_{RES} + 1}{\Phi_{1/\Phi}} \right), \quad \mathbf{x} = K_{i,0} \mathbf{h}_{RE}^H (\theta) \mathbf{X}, \quad \text{and} \quad \mathbf{X} = \Phi \mathbf{GWG}^H \Phi^H. \)

**Lemma 1 (Bernstein-Type Inequality):** For any \( \mathbf{v} \in \mathbb{C}^{M \times 1} - \mathcal{C} \mathcal{N}(\mathbf{0}, \mathbf{I}_M), \mathbf{U} \in \mathbb{H}^{M \times M}, \mathbf{u} \in \mathbb{C}^{n \times M}, \) the following implication holds:

\[
P_i (\mathbf{v}^H \mathbf{U} \mathbf{v} + 2 \text{Re}(\mathbf{U}^H \mathbf{v})) + u \leq 0 \geq 1 - p
\]

\[
\Rightarrow \text{Tr}(\mathbf{U}) + \sqrt{2 \ln(1/p)} \sqrt{\left\| \mathbf{U} \right\|_F^2 + 2 \left\| \mathbf{u} \right\|_2^2} - \ln(p) \cdot \lambda^*(\mathbf{U}) + u \leq 0
\]

By using Lemma 1, constraint in (10) can be reformulated as

\[
\text{Tr}(\mathbf{X}) + \sqrt{2 \ln(1/p)} \sqrt{\left\| \mathbf{X} \right\|_F^2 + 2 \left\| \mathbf{x} \right\|_2^2} - \ln(p) \cdot \lambda^*(\mathbf{X}) + x \leq 0
\]

By using Theorem 1 in [4], we have

\[
x \leq K_{i,0} M^2 \max_{i \in Q} (\mathbf{q}_i^H \mathbf{X} \mathbf{q}_i) - (2^C - 1) \sigma^2 \left( \frac{K_{RES} + 1}{\Phi_{1/\Phi}} \right), \theta \in [\theta_{\min}, \theta_{\max}]
\]

(13)

where \( \mathbf{q}_i \) is the eigenvector corresponding to the \( i \)-th eigenvalue of matrix \( \int a(\theta) a^H(\theta) d\theta \) in a descending order, \( Q = \{ i | \mathbf{v} \in \mathcal{M}, \max |a^H(\theta) \mathbf{q}_i| \geq \varepsilon \} \), \( \varepsilon \) is a parameter controlling the accuracy.

By introducing \( x_i = K_{i,0} M^2 \max_{i \in Q} (\mathbf{q}_i^H \mathbf{X} \mathbf{q}_i) - (2^C - 1) \sigma^2 \left( \frac{K_{RES} + 1}{\Phi_{1/\Phi}} \right), i \in Q \) and \( \mathbf{x}_i = M \mathbf{q}_i^H \mathbf{X} \), the constraint in (12) can be reformulated as

\[
\text{Tr}(\mathbf{X}) + \sqrt{2 \ln(1/p)} \sqrt{\left\| \mathbf{X} \right\|_F^2 + 2 \left\| \mathbf{x}_i \right\|_2^2} - \ln(p) \cdot \lambda^*(\mathbf{X}) + x_i \leq 0, i \in Q
\]

(15)

By introducing auxiliary variables \( y_i, z_i \in \mathbb{R}^+ \), we can rewrite the constraint in (15) as

\[
\text{Tr}(\mathbf{X}) + \sqrt{2 \ln(1/p)} y_i - \ln(p) \cdot z_i + x_i \leq 0,
\]

\[
\left\| \text{vec}(\mathbf{X}) \right\|_2 \leq y_i,
\]

\[
z_i \mathbf{I}_M - \mathbf{X} \succeq 0, z_i \geq 0,
\]

(16)

Letting \( P_i = (2^C - 1) \sigma^2 \left( \frac{K_{RES} + 1}{\Phi_{1/\Phi}} \right), \) Problem \( P_0 \) can be reformulated as

\[
P_i: \min_{\mathbf{W}, \Phi} P_i
\]

s.t. \( \mathbf{h}_{RB}^H \Phi \mathbf{GWG}^H \Phi^H \mathbf{h}_{RB} \geq (2^C - 1) \sigma^2 \),

\[
\text{Tr}(\Phi \mathbf{GWG}^H \Phi^H) + \sqrt{2 \ln(1/p)} y_i - \ln(p) \cdot z_i + K_{i,0} M^2 \max_{i \in Q} (\mathbf{q}_i^H \Phi \mathbf{GWG}^H \Phi^H \mathbf{q}_i) - P_i \leq 0, i \in Q.
\]

\[
\left\| \text{vec}(\Phi \mathbf{GWG}^H \Phi^H) \right\|_2 \leq y_i, i \in Q,
\]

\[
z_i \mathbf{I}_M - \Phi \mathbf{GWG}^H \Phi^H \succeq 0, z_i \geq 0, i \in Q,
\]

\[
\text{Tr}(\mathbf{W}) \leq P_0,
\]

\[
\Phi = \text{diag}(\Psi), \Psi_m = e^{j \phi_m}, \phi_m \in [0, 2\pi],
\]

\[
\mathbf{W} \succeq 0,
\]

\[
\text{rank}(\mathbf{W}) = 1.
\]

4 Beamformer design

In this section, we solve Problem \( P_i \) based on an alternating optimization method. The principle of the alternating optimization method is to alternatively optimize the objective function with respect to one block of variables while fixing the other block in each iteration. This leads the following two optimization problems.

First, the beamforming problem at the base station can be expressed as
Problem $\mathcal{P}_2$, which is a convex problem and can be solved by an interior-point method. Note that there is no guarantee that the obtained $\mathbf{W}$ satisfies the rank-1 constraint. Thus, Gaussian randomization is needed for recovering approximately.

$$\begin{align*}
\mathcal{P}_2: \quad & \min_{\mathbf{W}} \mathbf{P}_c \\
\text{s.t.} \quad & \mathbf{h}_{bb}^H \Phi \mathbf{G} \mathbf{W}^H \Phi^H \mathbf{h}_{bb} \geq (2\epsilon_b - 1)\sigma_b^2, \\
& \text{Tr}(\Phi \mathbf{G} \mathbf{W}^H \Phi^H) + \sqrt{2}\ln(1/p) y_i - \ln(p) \cdot z_i + K_{bb}^2 M^2 q_i^H \Phi \mathbf{G} \mathbf{W}^H \Phi^H q_i - P_i \leq 0, i \in \mathcal{Q}, \\
& \left\| \text{vec}(\Phi \mathbf{G} \mathbf{W}^H \Phi^H) \right\|_2 \leq y_i, i \in \mathcal{Q}, \\
& z_i \mathbf{I}_M - \Phi \mathbf{G} \mathbf{W}^H \Phi^H q_i \succeq 0, z_i \geq 0, i \in \mathcal{Q}, \\
& \text{Tr}(\mathbf{W}) \leq P_0, \\
& \mathbf{W} \succeq 0.
\end{align*}$$

For given beamforming matrix $\mathbf{w}$ at base station, $\Phi \mathbf{G} \mathbf{w} = \text{diag}(\Phi \mathbf{G} \mathbf{w})$. By letting $\mathbf{F} = \psi \psi^H$ and $\mathbf{A} = \text{diag}(\Phi \mathbf{G} \mathbf{w})$, we have

$$\Phi \mathbf{G} \mathbf{W}^H \Phi^H = \mathbf{A} \mathbf{F} \mathbf{A}^H. \quad (17)$$

To ensure that the rank of matrix is 1, we add the following convex constraints

$$\text{Tr}\left((\mathbf{I}_M + \mathbf{F}^{(m)})^{-1} (\mathbf{F} - \mathbf{F}^{(m)})\right) + \ln \det(\mathbf{I}_M + \mathbf{F}^{(m)}) - \ln(1 + M) \leq \epsilon, \quad (18)$$

where $\mathbf{F}^{(m)}$ denotes $\mathbf{F}$ in the $m$-th iteration.

Then, the beamforming problem at the IRS can be expressed as

$$\mathcal{P}_3: \min_{\mathbf{F}} \mathbf{P}_c$$

s.t. $\mathbf{h}_{bb}^H \mathbf{A} \mathbf{F} \mathbf{A}^H \mathbf{h}_{bb} \geq (2\epsilon_b - 1)\sigma_b^2$, 
$$\text{Tr}(\mathbf{A} \mathbf{F} \mathbf{A}^H) + \sqrt{2}\ln(1/p) y_i - \ln(p) \cdot z_i + K_{bb}^2 M^2 q_i^H \mathbf{A} \mathbf{F} \mathbf{A}^H q_i - P_i \leq 0, i \in \mathcal{Q},$$
$$\left\| \text{vec}(\mathbf{A} \mathbf{F} \mathbf{A}^H) \right\|_2 \leq y_i, i \in \mathcal{Q},$$
$$z_i \mathbf{I}_M - \mathbf{A} \mathbf{F} \mathbf{A}^H q_i \succeq 0, z_i \geq 0, i \in \mathcal{Q},$$
$$\mathbf{F}^{(m)} = \mathbf{I}, m = 1...M,$$
$$\text{Tr}\left((\mathbf{I}_M + \mathbf{F}^{(m)})^{-1} (\mathbf{F} - \mathbf{F}^{(m)})\right) + \ln \det(\mathbf{I}_M + \mathbf{F}^{(m)}) - \ln(1 + M) \leq \epsilon.$$

Problem $\mathcal{P}_3$ is a convex problem and can be solved by the interior-point method.

The details are summarized as Algorithm 1. The computational complexities of each iteration of an interior-point method for solve Problem $\mathcal{P}_2$ and Problem $\mathcal{P}_3$ are $\mathcal{O}(\max\{N^6, N^4 M\})$ and $\mathcal{O}(M^3)$, respectively.

**Algorithm 1:** Alternating Algorithm

1. Set $m := 0$;
2. repeat
3. Solve Problem $\mathcal{P}_2$ to obtain $\mathbf{W}$;
4. Solve Problem $\mathcal{P}_3$ to obtain $\mathbf{F}$;
5. $m := m + 1$;
6. until Convergence

### 5 Numerical results

In this section, we provide numerical results to illustrate the performance of the proposed algorithm. The proposed algorithm is simulated under different numbers of antennas, numbers of IRS elements, Rican factors, and angle ranges.

The simulation configuration is shown in Fig. 2(a), the coordinate unit is meters. The carrier frequency is 4.15GHz, the noise power at the receiver is -90 dBm, the transmission power is 10 dBm, $C_s$ is 2bps/Hz, and $p$ is 0.9. We compare the proposed algorithm with the other three algorithms. MRT-w, opt-IRS:
Use the maximum ratio transmission (MRT) method to obtain the beamforming matrix at the base station, and use the optimization method to obtain the phase shift phase at IRS; Opt-w, random-IRS: use the optimization method to obtain the beamforming matrix at the base station, and randomly give the phase shift phase of each element at the IRS; Opt-w, reflection-IRS: use the optimization method to obtain the beamforming matrix at the base station, and the phase shift phase of all the elements at the IRS are 0°.

Fig. 2. Simulation configuration and numerical results

It can be observed from Fig. 2 that the proposed algorithm can greatly reduce the communication rate of the eavesdropper in a range under various conditions. The numerical results verify the effectiveness of the proposed algorithm.

6 Conclusion

This paper established a mathematical model with the goal of minimizing the eavesdropper’s rate subject to the eavesdropper’s outage probability constraint and the legitimate user’s secrecy rate constraint. An alternating algorithm is proposed to obtain a sub-optimal solution. The numerical results showed that the proposed algorithm can greatly reduce the eavesdropper's communication rate in different cases, which verified the effectiveness of the proposed algorithm.