Secure Transmission by Leveraging Multiple Intelligent Reflecting Surfaces in MISO Systems

Jian Li*, Member, IEEE, Lan Zhang*, Member, IEEE, Kaiping Xue*, Senior Member, IEEE, Yuguang Fang*, Fellow, IEEE, and Qibin Sun, Fellow, IEEE

Abstract—Recent advance of Intelligent Reflecting Surface (IRS) introduces a new dimension for secure communications by reconfiguring the transmission environments. In this paper, we devise a secure transmission scheme for multi-user Multiple-Input Single-Output systems by leveraging multiple collaborative IRSs. Specifically, to guarantee the worst-case achievable secrecy rate among multiple legitimate users, we formulate a max-min problem that can be solved by an alternating optimization method to decouple it into multiple sub-problems. Based on semidefinite relaxation and successive convex approximation, each sub-problem can be further converted into convex problem and easily solved. Extensive experimental results demonstrate that our proposed scheme can adapt to complex scenarios for multiple users and achieve significant gain in terms of achievable secrecy rate. Compared to the traditional single IRS scheme, the proposed scheme can achieve better performance at the range of 2.4-6.4 bps/Hz with the increase in the number of reflecting elements in the multi-user scenarios. We also evaluate the gap between the secrecy rate for our proposed scheme under continuous phase shift/amplitude control and discrete phase shift/amplitude control, and our results show that the secrecy rate obtained from discrete approximation method converges to that achieved from the proposed scheme when increasing the discretization granularity.

Index Terms—Physical layer security, intelligent reflecting surface, secrecy rate

1 INTRODUCTION

Due to the broadcast nature of radio channels, wireless signals can be captured by both legitimate and malicious users, and hence legitimate users’ transmissions can be easily intercepted, which may compromise confidentiality and privacy. To safeguard communication security, physical layer security, which can be traced back to 1970’s Wyner’s seminal work [1], [2], [3], has been regarded as a key complement to higher-layer encryption techniques [4], [5], [6]. In traditional communication systems, beamforming and Artificial Noise (AN) are considered as two effective approaches to defending against wiretapping channel and achieving secure communication [7], [8], [9], [10]. By exploiting multiple antennas and shaped beams, beamforming technology can be implemented to direct the signal towards the legitimate user and thus reduce the signal leakage. In addition to beamforming, AN technology can create significant interference and lower the Signal-to-Interference-plus-Noise Ratio (SINR) at eavesdroppers by properly designing AN signals. Thus, the achievable secrecy rate, which is a widely used performance metric to capture the difference between mutual information of intended transmitter-receiver user channel and transmitter-eavesdropper wiretap channel in order to measure the security level, can be effectively improved especially when the channel states for transmitter-user and transmitter-eavesdropper channels are highly correlated. Nevertheless, due to the complex environment of wireless communications, the proposed approaches do not always work as expected.

As a promising technology to achieve smart radio environment/intelligent radio environment in next generation cellular systems [11], [12], Intelligent Reflecting Surfaces (IRSs) can provide reconfigurable signal propagation environments to support cost-effective and power-efficient wireless communication services. Specifically, IRS is a meta-surface composed of a large number of passive reflecting elements, which consumes much lower energy compared with traditional active relays/ transceivers [13], [14], [15]. By adaptively adjusting the reflection amplitude and/or phase shift of each element, the strength and direction of the incident electromagnetic wave becomes highly controllable [16], [17]. Thus, IRS is regarded as a novel solution to achieving configurable wireless transmission environment/intelligent radio environment/wireless 2.0 with low hardware/energy cost, and has been applied in various wireless applications such as coverage extension, interference cancellation, and energy efficiency enhancement [11], [13]. Due to

* Jian Li, Kaiping Xue, and Qibin Sun are with the School of Cyber Science and Technology, University of Science and Technology of China, Hefei, Anhui 230027, China. E-mail: lijian9, kpxue, qibinsun@ustc.edu.cn.
* Lan Zhang is with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931 USA. E-mail: lanzhang@mtu.edu.
* Yuguang Fang is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA. E-mail: fang@ece.ufl.edu.

Manuscript received 27 January 2021; revised 25 August 2021; accepted 9 September 2021. Date of publication 21 September 2021; date of current version 6 March 2023.

Digital Object Identifier no. 10.1109/TMC.2021.3114167
the aforementioned advantages, the IRS-assisted communication systems have great potential to enhance physical layer security. By jointly optimizing operations on transmitter and passive reflecting elements of IRS, the transmitter-user channel state can be reconfigured to lower the signal leakage to eavesdroppers. Intuitively, users geographically close to the IRS are more likely beneficial from IRS by receiving the tuned signal, whose achievable secrecy rate can be significantly improved.

Recently, some efforts have been made to study IRS-assisted systems for physical layer security. Cui et al. [18] investigated an IRS-aided secure wireless communication systems where a simple scenario with one eavesdropper is investigated to show the effectiveness of IRS. To explore the effectiveness of traditional approach in IRS-assisted scenarios, Guan et al. [5] further considered AN in an IRS-assisted system, whose performance was verified with the significant gain on secrecy rate. To improve the algorithm efficiency, Dong et al. [19] proposed an efficient algorithm adopting block coordinate descent and minorization maximization method for faster convergence for Multiple-Input Multiple-Output (MIMO) systems. Lyu et al. [20] considered a potential IRS threat called IRS jamming attack, which can leverage signals from a transmitter by controlling reflected signals to diminish the signal-to-interference-plus-noise ratio at the user. Since the IRS jammer operates in a passive way, it can be even harder to defend. The multiple IRS-assisted system considered in this paper provides a possible solution. Since IRS jamming is effective based on the knowledge of the Channel State Information (CSI), the Base Station (BS) can randomly select an IRS from multiple ones to transmit the signal to the user. In this case, the attacker can hardly acquire the CSI on the BS-IRS-user channel because the attacker does not know which IRS is used in the next time slot, so the minimization of the received signal at the user can hardly be optimized, and the IRS jamming attack can be hardly effective. Xu et al. [21] studied resource allocation design in multi-user scenarios and also considered AN at transmitter. Due to the non-convexity of the optimization problems in the IRS-aided wireless communication systems, there also exist some research works that apply learning-based methods to address these challenging problems. To maximize the downlink throughput and achieve secure communications against eavesdroppers in Multiple-Input Single-Output (MISO) systems, Feng et al. [22] and Yang et al. [23] respectively developed deep reinforcement learning-based approaches. Their simulation results also validate the effectiveness of such learning-based approaches by demonstrating significant performance gains in terms of throughput and security. However, the aforementioned efforts only focus on the proof-of-concept study by implementing a single IRS, and the learning-based approaches still lack the generalization ability. Thus, the security gain from leveraging multiple collaborative IRSs has not been thoroughly explored as yet, and it is also paramount to jointly optimize wireless transmission environments and allocate resources for legitimate users in multiple IRSs-assisted systems.

To enhance the security transmission from users, in this paper, we study secure transmission schemes for multi-user MISO systems assisted by multiple collaborative IRSs. Compared to the traditional single IRS scheme, on the one hand, the proposed multi-IRS scheme not only needs to solve the transmission strategies, but also should select appropriate IRS to adapt to the complex environment, which enlarges the solution space and makes the problem more difficult to solve. On the other hand, the multiple IRSs can also provide environmental diversity to further improve the performance, which is attractive for users to achieve secure transmissions in wireless systems. To ensure the security for legitimate users, we adopt achievable secrecy rate as the performance metric and formulate an optimization problem. Motivated by the Cannikin Law, if one legitimate user’s security performance cannot be guaranteed and his/her security is compromised, the whole communication system will be insecure because no one knows who is the victim. Thus, we attempt to ensure the worst achievable secrecy rate equally for all users through solving a max-min problem.

The main contributions of this paper are summarized as follows.

- To deal with the threat from potential eavesdroppers, we propose a secure communication scheme in multiple IRSs assisted systems. Considering the security requirement for each legitimate user, we formulate a max-min problem to maximize the lower bound of the secrecy rate to optimize the worst performance of multiple users in case eavesdroppers attempt to “steal” useful information from a user.
- To efficiently solve the formulated max-min problem, we propose an alternating algorithm to decouple it into multiple sub-problems. In each iteration, we apply Semi-Definite Relaxation (SDR) and Successive Convex Approximation (SCA) methods to solve convex optimization problems.
- To verify the effectiveness of the proposed scheme, extensive numerical evaluations are conducted. Based on the results obtained from the proposed scheme and the traditional single IRS scheme, we further evaluate the performance of the proposed scheme under constraints with imperfect CSI and discrete phase/amplitude adjustment, and compare our scheme with the traditional sum-rate maximization to show the gap in the security performance.

Symbol Notation: Boldface lowercase and uppercase let-

ers denote vectors and matrices, respectively. For a vector \( \mathbf{a} \), \( |\mathbf{a}| \) denotes the euclidean norm. For matrix \( \mathbf{A} \), the conjugate transpose, rank and trace of \( \mathbf{A} \) are denoted as \( \mathbf{A}^H \), \( \text{Rank}(\mathbf{A}) \) and \( \text{Tr}(\mathbf{A}) \), respectively. For a complex number \( c \), \( |c| \) denotes the modulus, \( \mathbb{C} \) denotes the phase of the complex value \( x \). The set of \( n \times m \) real matrices, complex matrices and complex Hermitian matrices are denoted as \( \mathbb{R}^{n \times m} \), \( \mathbb{C}^{n \times m} \) and \( \mathbb{H}^{n \times m} \), respectively. \( \mathbf{A} \succeq 0 \) means \( \mathbf{A} \) is a positive semidefinite matrix, and \( \mathcal{N}(\mu, \Sigma) \) denotes the Gaussian distribution with mean \( \mu \) and covariance matrix \( \Sigma \).

1. Cannikin Law is also known as Liebig’s law or the Wooden Bucket Theory, which states that a bucket’s capacity is determined by its shortest stave [24].
Due to the channel reciprocity provided by TDD protocol, for flat fading model, the coherence bandwidth for the channel is 

\[ B = \frac{\pi f_c}{B} \]

where \( f_c \) is the carrier frequency, \( B \) is the bandwidth, and \( \pi \) is the mathematical constant. In practice, this bandwidth is limited by the channel's propagation characteristics.

2 System Model

We consider a wireless communication system as shown in Fig. 1, a base station equipped with \( M \) antennas intends to transmit secure messages to \( J \) legitimate users equipped with single antenna. Moreover, \( K \) IRSs have been deployed in advance to assist wireless communications, and each IRS has \( N \) reflecting elements.

Adversary Model. With respect to the transmitted secure messages, one eavesdropper (Eve) wants to wiretap/intercept transmitted signals through wiretap channel, and further crack the secure messages to steal users’ private information or hack users’ equipments. For legitimate users, the communication link with the base station is setup after authentication. Since the activities of legitimate users can be tracked by the base station, we assume all legitimate users are honest and do not collude with the eavesdropper.

To eliminate the potential threat from the eavesdropper and protect the security of legitimate users, the base station and IRSs need to collaboratively transmit signals to increase received signal power at legitimate users while mitigating the signal leakage at the eavesdropper. In this paper, we attempt to adjust the transmission strategy both at base station and on IRSs to enhance the security level.

Channel Model. For the channel model between the base station and user/Eve, two cases are considered, i.e., direct channel (transmitter to user/Eve) and reflecting channel (transmitter to IRS to user/Eve). The composite reflecting channel is modeled as a combination of three components, i.e., the channel from the base station to the \( k \)th IRS, the \( i \)th user and Eve are denoted by \( G_k^H \in \mathbb{C}^{N \times M} \), \( h_i^H \in \mathbb{C}^{1 \times M} \), \( h_e^H \in \mathbb{C}^{1 \times M} \). respectively. The equivalent channels from the \( k \)th IRS to the \( i \)th user and Eve are denoted by \( g_k^H \in \mathbb{C}^{1 \times N} \), \( g_e^H \in \mathbb{C}^{1 \times N} \), respectively. Since IRS is a passive reflecting device, we consider a Time Division Duplexing (TDD) protocol for uplink and downlink transmissions and quasi-static (constant within the transmission frame) flat-fading model is adopted for all channels. As discussed in [5], [13], [26], by applying various channel acquisition methods, we can acquire all channel information, and hence here for the current study, we also assume that the CSI of all channels are perfectly known.

Linear transmit precoding is considered at the base station similar to [14], and each user served by the base station is assigned with one dedicated beamforming vector. To further enhance the physical layer security, additional AN is also adopted. Thus, the signal transmitted from the base station to the \( i \)th user can be described as

\[ s_i = \omega_i d_i + z_i, \quad i \in U, \]

where \( \omega_i \in \mathbb{C}^{M \times 1} \) is the beamforming vector for the \( i \)th user, \( d_i \) is the corresponding transmitted data, \( z_i \in \mathbb{C}^{M \times 1} \) is an AN vector, and \( U \) represents the user set.

Since multiple IRSs have been deployed in the system, each legitimate user can be served by a selected IRS to receive tuned signal, which is effective especially when there exists an obstacle and no Light-of-Sight (LoS) channel between the base station and a user. Let \( \alpha_{i,k} \in \{0, 1\} \) denote the IRS selection for the \( i \)th user, i.e., the \( i \)th user can receive reflecting signal through the \( k \)th IRS if \( \alpha_{i,k} = 1 \). Meanwhile, let \( \Theta_k = \text{diag}(\mathcal{A}_k \mathcal{E}^\theta_1, \ldots, \mathcal{A}_{k,N} \mathcal{E}^\theta_N) \in \mathbb{C}^{N \times N} \), where \( \mathcal{A}_k \) diagonal phase-shifting matrix of the \( k \)th IRS, while \( \mathcal{A}_{k,n} \in \{0, 1\} \) and \( \theta_{k,n} \in [0, 2\pi) \) denote the amplitude reflection coefficient and the phase shift of the \( n \)th element on the \( k \)th IRS. In practice, each element of an IRS is usually designed to maximize the signal reflection [14]. Thus, we set \( \mathcal{A}_{k,n} = 1 \) in this paper. In this case, for the \( i \)th user, the received signal from base station and IRSs can be represented by

\[ y_i = \left( \sum_{k=1}^{K} \alpha_{i,k} g_k^H \Theta_k G_k^H + h_i^H \right) (\omega_i d_i + z_i) + \sum_{j \neq i} \left( \sum_{k=1}^{K} \alpha_{j,k} g_k^H \Theta_k G_k^H + h_i^H \right) (\omega_j d_j + z_j) + n_0, \]

where \( n_0 \in \mathcal{C} \mathcal{N}(0, \sigma^2) \) is the complex Additive White Gaussian Noise (AWGN). For an eavesdropper, the received signal can be represented by

\[ y_e = \left( \sum_{k=1}^{K} \alpha_{e,k} g_k^H \Theta_k G_k^H + h_e^H \right) (\omega_i d_i + z_i) + \sum_{j \neq i} \left( \sum_{k=1}^{K} \alpha_{j,k} g_k^H \Theta_k G_k^H + h_i^H \right) (\omega_j d_j + z_j) + n_0. \]

For notational simplicity, let \( \hat{D}_{ei} = \sum_{k=1}^{K} \alpha_{j,k} g_k^H \Theta_k G_k^H + h_i^H \in \mathbb{C}^{1 \times M} \), \( \hat{D}_{ei} = \sum_{k=1}^{K} \alpha_{i,k} g_k^H \Theta_k G_k^H + h_i^H \in \mathbb{C}^{1 \times M} \). Accordingly, the SINR of received signal at the \( i \)th user can be calculated by

2. Due to the channel reciprocity provided by TDD protocol between uplink and downlink, both transmission links are assumed to match well, thus CSI for downlink can be obtained at the base station from the uplink channel based on the channel reciprocity [25].

3. For flat fading model, the coherence bandwidth for the channel is larger than that for the signal. Therefore, all frequency components of the signal will experience the same fading.
$$\text{SINR}_i = \frac{\left| \left( \sum_{k=1}^{K} \alpha_{i,k}g_{i,k}^H \Theta_i G_k^H + h_{i,k}^H \right) \omega_i \right|^2}{\sum_{j \neq i} \left| D_{i,j} \omega_j \right|^2 + \sum_{j \neq i} \left| D_{i,j} z_j \right|^2 + N_0},$$

(4)

where $N_0$ is the power of AWGN. Similarly, the SINR of the $i$th user’s signal at the eavesdropper can be calculated by

$$\text{SINR}_e = \frac{\left| \left( \sum_{k=1}^{K} \alpha_{i,k}g_{i,k}^H \Theta_i G_k^H + h_{i,k}^H \right) \omega_i \right|^2}{\sum_{j \neq i} \left| D_{e,j} \omega_j \right|^2 + \sum_{j \neq i} \left| D_{e,j} z_j \right|^2 + N_0}.$$  

(5)

### 3 Problem Formulation and Solution

Considering the security requirement for each legitimate user in the system, we want to guarantee the worst performance of all legitimate users in case an eavesdropper might wiretap/intercept too much useful information from a certain user. Thus, in this paper, we aim to maximize the minimum achievable secrecy rate of legitimate users in the system. By jointly configuring the beamforming matrix $\tilde{\omega}$, $\tilde{\omega}$, $\theta$, and $\alpha$ and AN matrix $\bar{z}$, $\bar{z}$ at the base station, phase shift matrix $\tilde{\Theta}$, $\tilde{\Theta}$, each iteration. Thus, $\text{Problem 1}$ is divided into three sub-problems and each sub-problem is solved iteratively as described in Algorithm 1. For each sub-problem, we utilize SDR and SCA to convert the original problem into a convex problem. The detailed solving process of each sub-problem is described in the following subsections.

#### Algorithm 1. BCD-Based Algorithm

**Input:** Number of elements $N$, number of antennas $M$, number of surfaces $K$;

**Output:** Beamforming vector $\bar{\omega}$, AN vector $\bar{z}$, phase shift matrix $\tilde{\Theta}$ and IRS selection vector $\alpha$;

1. Initialize:
   - Initialize $\tilde{\omega}^{(0)}$, $\bar{z}^{(0)}$, $\Theta^{(0)}$ and $\alpha^{(0)}$;
   - $t = 0$, $\Delta_t^{(0)} = \text{Infmax}$;

2. while $\Delta_t^{(0)} < \delta$ do

3. Solve each sub-problem to find solution for $\tilde{\omega}^{(t+1)}$, $\bar{z}^{(t+1)}$, $\Theta^{(t+1)}$ and $\alpha^{(t+1)}$ for given $\tilde{\omega}^{(t)}$, $\bar{z}^{(t)}$, $\tilde{\Theta}^{(t)}$ and $\alpha^{(t)}$ respectively;

4. Calculate $\rho^{(t+1)} = \min_t \left[ R_t^e - R_t^c \right]$;

5. Update $t = t + 1$ and $\Delta_t^{(t)} = \Delta_t^{(t-1)} - \rho^{(t)}$;

end

#### 3.1 Sub-Problem for Beamforming and AN

At first, beamforming and AN matrices are considered to be solved. For given phase shift operation $\tilde{\Theta}$ and surface matching $\bar{\alpha}$, with $[x]_+ = \max\{0, x\}$, we can rewrite Problem 1 as

$$\text{Problem 2a:} \quad \min_{\bar{\omega} \in \mathcal{A}} \left[ R_t^e - R_t^c \right]^+$$

(8)

s.t.\n
$\| \omega_i \|^2 + \| z_i \|^2 \leq P_{\max}, \; \forall i \in \mathcal{U},$

(9)

$0 \leq \theta_{h,n} \leq 2\pi, \; k \in [1, K], \forall n \in [1, N],$

$\sum_k \alpha_{i,k} = 1, \; \alpha_{i,k} \in \{0, 1\}, \; \forall i \in \mathcal{U},$

(10)

where $\mathcal{A}$ and $\mathcal{A}^+$ denote the solution space for non-negative and positive values, respectively. Once $\mathcal{A}^+$ is non-empty, the optimal solution must satisfy $\left( \alpha^*; z_i^* \right) \in \mathcal{A}^+$ in this case, we can rewrite (8) as $R_t^e - R_t^c$ when $\mathcal{A}^+ \neq \emptyset$.

Since SDR is a powerful computationally efficient approximation technique, it has been successfully applied to solve many difficult optimization problems in communications and signal processing [14], [28], [29], [30], especially the problem containing quadratic terms as in $\text{Problem 2a}$. Thus, to solve this sub-problem for beamforming and AN, we plan to apply SDR in the next. So we start to reformulate the objective with some mathematical transformations. Let $W_t = \omega, \omega^H \in \mathbb{C}^{M \times M}$, $Z_t = z, z^H \in \mathbb{C}^{M \times M}$, $D_t = \sum_{k=1}^{K} \alpha_{i,k} \Theta_{i,k} G_k + h_{i,k}^H \in \mathbb{C}^{M \times M}$, $\tilde{D}_t = \sum_{k=1}^{K} \alpha_{i,k} \Theta_{i,k} G_k + h_{i,k}^H \in \mathbb{C}^{M \times M}$, $D_{i,k} = \sum_{k=1}^{K} \alpha_{i,k} \Theta_{i,k} G_k + h_{i,k}^H \in \mathbb{C}^{M \times M}$. Then, the achievable secrecy rate can be reformulated as
\[ \nabla_{W_i} F_i^3(W_i, Z_i) = 0, \quad \nabla_{Z_i} F_i^3(W_i, Z_i) = \frac{1}{\ln 2} \sum_{j \neq i} \text{Tr}(W_j \hat{D}_{ij}^H \hat{D}_{ij}) + \sum_{j \neq i} \text{Tr}(Z_j \hat{D}_{ij}^H \hat{D}_{ij}) + N_0. \]  
(11)

\[ \nabla_{W_i} F_i^4(W_i, Z_i) = \frac{1}{\ln 2} \text{Tr}(W_i \hat{D}_{ij}^H D_{ij}) + \sum_{j \neq i} \text{Tr}(W_j \hat{D}_{ij}^H D_{ij}) + \sum_{j \neq i} \text{Tr}(Z_j \hat{D}_{ij}^H D_{ij}) + N_0. \]  
(12)

\[ \nabla_{Z_i} F_i^4(W_i, Z_i) = \frac{1}{\ln 2} \text{Tr}(W_i \hat{D}_{ij}^H D_{ij}) + \sum_{j \neq i} \text{Tr}(W_j \hat{D}_{ij}^H D_{ij}) + \sum_{j \neq i} \text{Tr}(Z_j \hat{D}_{ij}^H D_{ij}) + N_0. \]  
(13)

\[ R_{ii}^0 - R_{ii}^1 = \log_2 \left( 1 + \frac{\text{Tr}(W_i \hat{D}_{ij}^H D_{ij})}{\sum_{j \neq i} \text{Tr}(W_j \hat{D}_{ij}^H D_{ij}) + \sum_{j \neq i} \text{Tr}(Z_j \hat{D}_{ij}^H D_{ij}) + N_0} \right) \]  
(10)

where \( F_i^1, F_i^2, F_i^3 \) and \( F_i^4 \) are represented by

\[ F_i^1 = \log_2 \left( \text{Tr}(W_i \hat{D}_{ij}^H D_{ij}) \right) \]  
(14)

\[ F_i^2 = \log_2 \left( \sum_{j \neq i} \text{Tr}(W_j \hat{D}_{ij}^H D_{ij}) + \sum_{j \neq i} \text{Tr}(Z_j \hat{D}_{ij}^H D_{ij}) + N_0 \right), \]  
(15)

\[ F_i^3 = \log_2 \left( \sum_{j \neq i} \text{Tr}(W_j \hat{D}_{ij}^H D_{ij}) + \sum_{j \neq i} \text{Tr}(Z_j \hat{D}_{ij}^H D_{ij}) + N_0 \right). \]  
(16)

\[ F_i^4 = \log_2 \left( \text{Tr}(W_i \hat{D}_{ij}^H D_{ij}) \right) \]  
(17)

The main idea of SCA method is to generate a sequence of feasible solutions \((W_i^{(t)}, Z_i^{(t)})\) by successively solving convex conservative approximation problems. At first, we construct global upper bound of \( F_i^3 \) and \( F_i^4 \), respectively. For any feasible solution \((W_i^{(t)}, Z_i^{(t)})\), the differential functions \( F_i^3(W_i, Z_i) \) and \( F_i^4(W_i, Z_i) \) satisfy the following inequalities:

\[ F_i^1(W_i, Z_i) \leq F_i^3(W_i^{(t)}, Z_i^{(t)}) \]  
(18)

\[ F_i^2(W_i, Z_i) \leq F_i^4(W_i^{(t)}, Z_i^{(t)}) \]  
(19)

where the right hand side terms in (18) and (19) are global upper bound of \( F_i^3 \) and \( F_i^4 \) by using first-order Taylor approximation, respectively. The gradients of functions \( F_i^3 \) and \( F_i^4 \) with respect to \( W_i \) and \( Z_i \) are given in (11), (12), and (13). Hence, a convex lower bound of objective function in (10) can be obtained as \( R_{ii}^0 - R_{ii}^1 = F_i^1 + F_i^2 - F_i^3 - F_i^4 \). Let \( f_i(W_i, Z_i) = F_i^1 + F_i^2 - F_i^3 - F_i^4 \) and \( g_i(W_i, Z_i) = F_i^1 + F_i^2 - F_i^3 - F_i^4 \). Since \( f_i(W_i, Z_i) \geq g_i(W_i, Z_i) \) according to (18) and (19), as long as we guarantee \( g_i(W_i, Z_i) \geq 0 \), \( f_i(W_i, Z_i) \geq 0 \) must be satisfied.

After deploying SCA, the objective function becomes convex. In order to further solve the max-min problem, we also introduce an auxiliary variable \( x \) into the formulation. By doing so, the original Problem 2a can be transformed to

\[ \text{Problem 2b} : \max_{x, W, Z} x \]  
(20)

s.t. \( \text{Tr}(W_i) + \text{Tr}(Z_i) \leq P_{max}, \forall i \in \mathcal{U}, \)  
(21)

4. Since \( F_i^3 \) and \( F_i^4 \) are concave functions, according to the definition of concave function, we have \( (1 - \lambda)f(x) + \lambda f(y) \leq f((1 - \lambda)x + \lambda y) \). In this case, we can construct global upper bound \( f(y) \leq f(x) + \frac{f(x) - f(y)}{x - y}(x - y) \) as \( \lambda \to 0 \).
where \( W = [W_1, W_2, \ldots, W_i], Z = [Z_1, Z_2, \ldots, Z_i] \in \mathbb{C}^{\text{IM} \times \text{IM}} \). Since constraint (C5) is non-convex, we drop this rank-1 constraint by applying SDR. If the obtained solution \((W_i^{(t)}, Z_i^{(t)})\) are of rank-1, they can be written as \( W_i^{(t)} = \omega_i \omega_i^H \) and \( Z_i^{(t)} = z_i z_i^H \), then the optimal beamforming vector \( \omega_i \) and AN \( z_i \) can be obtained by applying eigenvalue decomposition.  

Otherwise, we can adopt Gaussian Randomization to recover \( \omega_i \) and \( z_i \) approximately from the rank-1 solution \((W_i^{(t)}, Z_i^{(t)})\) [28], [29], [30]. In this case, Problem 2b becomes a convex optimization problem. In Algorithm 2, Problem 2b can be efficiently solved at each iteration by using convex optimization solvers, e.g., SeduMi and CVX [35], [36]. In the following, we prove that SCA-based approach in Algorithm 2 can reach the optimal solution at each iteration.

**Proposition 1.** Algorithm 2 generates a sequence of non-decreasing feasible solutions that converge to a point \((W^*, Z^*)\) satisfying the Karush-Kuhn-Tucker (KKT) conditions of the original problems in (8).

**Proof.** For notational convenience, let \( f_i(W_i, Z_i) = F_i^1 + F_i^2 - F_i^3 - F_i^4 \) and \( g_i(W_i, Z_i) = F_i^1 + F_i^2 - F_i^3 - F_i^4 \). The constraint (C4) can be rewritten as \( x = \min_{W, Z} \{ g_i(W_i, Z_i) \} \).

According to (18) and (19), we can obtain \( \max_i \{ f_i(W_i^{(t)}, Z_i^{(t)}) \} = \max_i \{ g_i(W_i^{(t)}, Z_i^{(t)}) \}, \forall \omega_i, Z_i \in \mathbb{C}^{\text{IM} \times \text{IM}} \). Since constraints (C1), (C4) and (C6) are always satisfied, the optimal solution \((W_i^{(t)}, Z_i^{(t)})\) of the approximated problem (20) at the 4th iteration always belongs to the feasible set of the original problem (8). At each iteration, it follows that [37], [38]

\[
\max_i \{ f_i(W_i^{(t)}, Z_i^{(t)}) \} \geq \max_i \{ g_i(W_i^{(t)}, Z_i^{(t)}) \} = \min_{W, Z} \{ g_i(W_i, Z_i) \} \geq \max_i \{ g_i(W_i^{(t-1)}, Z_i^{(t-1)}) \} = \max_i \{ f_i(W_i^{(t-1)}, Z_i^{(t-1)}) \},
\]

where the second inequality holds because \((W_i^{(t)}, Z_i^{(t)})\) is the global optimum of (20) at the 4th iteration, and the last equality holds because \( g_i(W_i^{(t-1)}, Z_i^{(t-1)}) = f_i(W_i^{(t-1)}, Z_i^{(t-1)}) \). This means that \( \max_i \{ f_i(W_i^{(t)}, Z_i^{(t)}) \} = \max_i \{ f_i(W_i^{(t-1)}, Z_i^{(t-1)}) \} \) \( |t = 0, 1, \ldots | \) is a monotonically increasing sequence. As the actual objective value in (20) is non-decreasing after each iteration, Algorithm 2 will eventually converge to a point \((W^*, Z^*)\) as \( t \) increases.

For an SDR solution \( W \), the eigen-decomposition can be applied to obtain \( W = \sum_{r=1}^{n} \lambda_r q_r q_r^H \), where \( r = \text{Rank}(W), \lambda_1 \geq \ldots \geq \lambda_n > 0 \) are the eigenvalues, and \( q_1, \ldots, q_n \in \mathbb{C}^{\text{IM}} \) are the respective eigenvectors [28]. Thus, the optimal and the only solution for the original problem, i.e., \( g = \sqrt{\lambda_n} q_n \), can be obtained from the eigenvalue decomposition if \( W \) satisfies the rank-1 condition.

Next, we prove that \((W^*, Z^*)\) satisfies the KKT conditions of the original problem. From (20), the optimal solution can be found when \( x = \min_{W, Z} \{ g_i(W_i, Z_i) \} \), thus, Problem 2b can be rewritten as

\[
\max_{x, Z} \min_i \{ g_i(W_i, Z_i) \} \quad \text{s.t.} \quad (C1), (C6).
\]

Then, the Lagrangian for (21) is

\[
L(W, Z; \sigma) = \min_i \{ g_i(W_i, Z_i) \} + \sum_{i \in U} \sigma_i (\text{Tr}(W_i) + \text{Tr}(Z_i)),
\]

where \( \sigma_i \) is the Lagrangian multiplier for each constraint. Similar to (20), by adopting mathematical transformations and introducing auxiliary variable \( x \), the Lagrangian for the original problem (8) can be written as

\[
L'(W, Z; \sigma) = \min_i \{ f_i(W_i, Z_i) \} + \sum_{i \in U} \sigma_i (\text{Tr}(W_i) + \text{Tr}(Z_i)),
\]

For a feasible point \((W^{(t-1)}, Z^{(t-1)})\) obtained from Algorithm 2 at the \((t-1)\)th iteration, it is the global optimum for (21), the KKT conditions of (21) must be satisfied, i.e., \((W^{(t-1)}, Z^{(t-1)})\) is feasible for (21) and there exist non-negative real values \( \sigma_i, i \in U \) satisfying

\[
\nabla L(W^{(t-1)}, Z^{(t-1)}; \sigma)|_{W, Z = 0},
\]

\[
\sigma_i (\text{Tr}(W^{(t-1)}) + \text{Tr}(Z^{(t-1)})) = 0, \forall i \in U.
\]

Since the gradient of the first-order Taylor approximations \( F_i(W_i, Z_i) \) and \( F_i(W_i, Z_i) \) are the same as \( F_i(W_i, Z_i) \) and \( F_i(W_i, Z_i) \), we can also verify that

\[
\nabla L'(W, Z; \sigma)|_{W = W^{(t-1)}} = \nabla L(W, Z; \sigma)|_{W = W^{(t-1)}},
\]

\[
\nabla L'(W, Z; \sigma)|_{Z = Z^{(t-1)}} = \nabla L(W, Z; \sigma)|_{Z = Z^{(t-1)}},
\]

which implies that \((W^{(t-1)}, Z^{(t-1)})\) satisfies the KKT conditions for (8). The results imply that the KKT conditions of the original problem will be satisfied after the series of approximations converges to the point \((W^*, Z^*)\). This completes the proof.

**3.2 Subproblem for Phase Shift**

For given beamforming matrix \( \tilde{\omega} \), AN matrix \( \tilde{z} \) and surface selection matrix \( \bar{a} \), we can rewrite Problem 1 as

\[
0 \leq x \leq F_i^1 + F_i^2 - F_i^3 - F_i^4, \forall i \in U.
\]

\[
\text{Rank}(W_i) = 1, \quad \text{Rank}(Z_i) = 1, \forall i \in U,
\]

\[
W_i \succeq 0, \quad Z_i \succeq 0, \forall i \in U,
\]
Problem 3a: \[ \max_{\Theta} \min_{\{\mathbf{R}_i^u, \mathbf{R}_i^v\}} \left[ \mathbf{R}_i^u - \mathbf{R}_i^v \right]^+ \] (22) s.t. \[ 0 \leq \theta_{k,n} \leq 2\pi, \ k \in [1, K], \forall n \in [1, N]. \] (C2)

Next, similar to the procedures in the previous Section 3.1, we also transform the objective function to a solvable convex function by applying SDR and SCA. Let \( \mathbf{g}_{i} = \alpha_i \mathbf{g}_i \mathbf{G}_i^H \in \mathbb{C}^{N \times M} \) and \( \mathbf{g}_{i,k} = \alpha_{i,k} \mathbf{g}_{i,k} \mathbf{G}_i^H \in \mathbb{C}^{N \times M} \). Let \( \mathbf{k}_i, \mathbf{k}_{i,k} = \mathbf{k}_i \mathbf{g}_{i,k} \mathbf{G}_i^H \in \mathbb{C}^{N \times 1} \), \( \mu_k = [\mu_{i,k}; \mu_{i,k+1}; \ldots; \mu_{i,K}^N] \in \mathbb{C}^{N \times 1} \) and \( \mu_{k,n} = e^{j \theta_{k,n}} \). Then, the power of received signal at the \( i \)-th user in (4) becomes

\[
\left| \sum_{k=1}^{K} \left( \alpha_i g_{i,k}^H \mathbf{g}_i \mathbf{G}_i^H + h_i^H \mathbf{w}_i \right) \right|^2 \leq \left| \sum_{k=1}^{K} \mu_i k_i + h_i^H \mathbf{w}_i \right|^2 .
\]

Accordingly, the power of the received signal of the \( i \)-th user at the eavesdropper in (5) becomes

\[
\left| \sum_{k=1}^{K} \left( \alpha_i g_{i,k}^H \mathbf{g}_i \mathbf{G}_i^H + h_i^H \mathbf{w}_i \right) \right|^2 \leq \left| \sum_{k=1}^{K} \mu_i k_i + h_i^H \mathbf{w}_i \right|^2 .
\]

Furthermore, let \( v = [\mu_1, \mu_2, \ldots, \mu_K] \in \mathbb{C}^{1 \times NK} \) and \( a_i = [\mathbf{k}_{i,1}; \mathbf{k}_{i,2}; \ldots; \mathbf{k}_{i,K}] \in \mathbb{C}^{N \times 1} \). Thus, we have \( \sum_{k=1}^{K} \mu_k k_i = va_i \). Let \( b_i = h_i^H \mathbf{w}_i \), \( b_{i,j} = h_i^H \mathbf{w}_i \), \( g_{i} = \alpha_i \mathbf{g}_i \mathbf{G}_i^H \), \( G_{i,k} = \alpha_{i,k} \mathbf{g}_{i,k} \mathbf{G}_i^H \), \( b_j = h_j \mathbf{w}_j \). Also, let \( k_{i,j} = \mathbf{k}_{i,j} \mathbf{G}_i^H \). Then, the achievable secrecy rate in (7) can be reformulated as

\[
F_i^2 = \log_2 \left( \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |b_{i,j}|^2 + \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |c_{i,j}|^2 + N_0 \right) .
\]

(26)

\[
F_i^3 = \log_2 \left( \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |b_{i,j}|^2 + \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |c_{i,j}|^2 + N_0 \right) .
\]

(27)

\[
F_i^4 = \log_2 \left( \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |b_{i,j}|^2 + \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |c_{i,j}|^2 + N_0 \right) .
\]

(28)

Similarly, we apply the SDR method to remove rank-one constraint Rank(\( V \)) = 1 and SCA method to construct global upper bounds of \( F_i^3 \) and \( F_i^4 \) and make (24) become a convex function

\[
F_i^3(\mathbf{V}) = \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |b_{i,j}|^2 + \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |c_{i,j}|^2 + N_0
\]

\[ F_i^4(\mathbf{V}) = \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |b_{i,j}|^2 + \sum_{j \neq i} \text{Tr}(\mathbf{R}_{i,j}^B) + |c_{i,j}|^2 + N_0
\]

(29)

(30)

Thus, Problem 3a is transformed into a convex problem by introducing auxiliary variable \( x \)

\[ \max_{x} F_i^x \]

s.t. \[ 0 \leq \theta_{k,n} \leq 2\pi, \ k \in [1, K], \forall n \in [1, N]. \] (C2)

\[ 0 \leq x \leq F_i^1 + F_i^2 - F_i^3 - F_i^4, \forall i \in U, \] (C7)

\[ V \geq 0 . \] (C8)

To restore the desired solution \( \Theta = \text{diag}(v) \) from the convex Semi-Definite Programming (SDP) solution \( \mathbf{V} \), eigenvalue decomposition with Gaussian randomization can be used to obtain a feasible solution based on the higher-rank solution obtained by solving Problem 3b. Since unit modulus constraint (C2) for each element on IRS should be satisfied, the reflection coefficients can be obtained by \([5, 14]\)

\[ \mu_{k,n} = e^{j \frac{\theta_{k,n}}{NK}}, n = 1, 2, \ldots, NK, \] (32)

7. This is due to \( \mathbf{A} \cdot \text{diag}(\mathbf{e}^{j \phi_1}, \mathbf{e}^{j \phi_2}, \ldots, \mathbf{e}^{j \phi_N}) = \mathbf{e}^{j \phi_1} \cdot \text{diag}(\mathbf{e}^{j \phi_1}, \mathbf{e}^{j \phi_2}, \ldots, \mathbf{e}^{j \phi_N}) \cdot \text{diag}(\mathbf{A}) \) when matrix \( \mathbf{A} \in \mathbb{C}^{N \times N} \) and \( \text{diag}(\mathbf{e}^{j \phi_1}, \mathbf{e}^{j \phi_2}, \ldots, \mathbf{e}^{j \phi_N}) \in \mathbb{C}^{N \times N} \). Therefore, transmit-IRS-user channel gives \( \mathbf{g}_i^H \mathbf{G}_i^H = \mu_i \text{diag}(\mathbf{g}_i^H \mathbf{G}_i^H) \).
denotes the phase of $x$ and the obtained solution can satisfy $|\mu_{kn}| = 1$.

### 3.3 Subproblem for Surface Selection

For given beamforming vector $\tilde{\mathbf{a}}$, AN vector $\tilde{\mathbf{z}}$ and phase shift of IRS $\Theta$, the original problem becomes a 0-1 integer programming problem, and we can rewrite Problem 1 as

Problem 4a: $\max_{\mathbf{a}} \min_{i} \left[ R_i^u - R_i^e \right]$  \hspace{1cm} (33)

subject to $\sum_{k} \alpha_{i,k} = 1, \alpha_{i,k} \in \{0,1\}, \forall i \in \mathcal{U}$. \hspace{1cm} (C3)

At first, according to the constraint described in (C3), each user is served by one specific IRS, and thus, we have $\alpha_{i,k} \alpha_{i,k'} = 0$ when $k \neq k'$ and $\sum_{k=1}^{K} \sum_{k' \neq k} \alpha_{i,k} \alpha_{i,k'} = \sum_{k=1}^{K} \alpha_{i,k}$. Then, we can simplify the expression in (4) and the power of the received signal at the $i$th user becomes

$$\left| \left( \sum_{k=1}^{K} \alpha_{i,k} g_{i,k}^H \Theta_i^H G_k^H + h_i^H \right) \omega_i \right|^2$$

$$= \sum_{k=1}^{K} \alpha_{i,k} \left( \sum_{k' \neq k} \alpha_{i,k'} (T_{i,k} \omega_i)^H T_{i,k} \omega_i + (h_i^H \omega_i)^H h_i^H \omega_i \right)$$

$$+ \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H T_{i,k} \omega_i + \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H T_{i,k} \omega_i + (h_i^H \omega_i)^H h_i^H \omega_i$$

$$+ \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i + \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H T_{i,k} \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{i,k} \omega_i)^H h_i^H \omega_i$$

where $T_{i,k} = g_{i,k}^H \Theta_i g_{i,k}^H$, $T_{i,k} = g_{i,k}^H \Theta_i g_{i,k}^H$, $T_{i,k} = (T_{i,k} \omega_i)^H T_{i,k} \omega_i$, $T_{i,k} = (T_{i,k} \omega_i)^H h_i^H \omega_i + (T_{i,k} \omega_i)^H T_{i,k} \omega_i$, $T_{i,k} = (T_{i,k} \omega_i)^H h_i^H \omega_i$. Similarly, the power of the received signal for the $i$th user at eavesdropper in (5) can be expressed as

$$\left| \left( \sum_{k=1}^{K} \alpha_{i,k} g_{i,k}^H \Theta_i G_k^H + h_i^H \right) \omega_i \right|^2$$

$$= \sum_{k=1}^{K} \alpha_{i,k} \left( \sum_{k' \neq k} \alpha_{i,k'} (T_{e,k} \omega_i)^H T_{e,k} \omega_i + (h_i^H \omega_i)^H h_i^H \omega_i \right)$$

$$+ \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H T_{e,k} \omega_i + \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H T_{e,k} \omega_i + (h_i^H \omega_i)^H h_i^H \omega_i$$

$$+ \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H h_i^H \omega_i + \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H T_{e,k} \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H h_i^H \omega_i$$

$$= \sum_{k=1}^{K} \alpha_{i,k} (T_{e,k} \omega_i)^H h_i^H \omega_i$$

where $\tilde{\mathbf{a}}_i = [a_{i,1}, \ldots, a_{i,K}]$. Thus, Problem 4a can be transformed into a convex problem by introducing auxiliary variable $x$

Problem 4b: $\max_{\mathbf{x}} x$  \hspace{1cm} (42)

subject to $0 \leq x \leq F_i^3 + F_i^2 - F_i^4 - F_i^1$, \hspace{1cm} (C9)

$$\sum_{k} \alpha_{i,k} = 1, \alpha_{i,k} \in \{0,1\}, \forall i \in \mathcal{U}.$$ \hspace{1cm} (C10)

In this case, Problem 4b becomes a general convex problem.
4 NUMERICAL EVALUATION

4.1 Evaluation Setups

To evaluate the performance of the proposed scheme, we conduct a number of numerical evaluations in this section. The overall setup is shown in Fig. 2, we consider the base station is located at (10, 0, 10). IRSs and legitimate users are uniformly distributed around base station with a constant angle $\theta^\prime$. The first user and IRSs are located at (5, 67, 5) and (8, 67, 2), respectively. Eve is located at (10, 60, 5) where in the middle between the base station and the first user. We also assume that the direct channel between the base station and users is blocked by obstacles, which implies the channel state between the base station and a user is much worse than the channel state between the IRS and the user. Specifically, the channels from base station to IRS/users/Eve are assumed to follow the distance-dependent path loss model, which can be generated by $h = \sqrt{L_0 d_a^{-\beta} h^*}$, where $L_0$ denotes the reference path loss at 1 meter, $\beta$ denotes the path loss exponent, $d_{ab}$ denotes the distance from location $a$ to location $b$, and $h^*$ is the small-scale fading component with Rician fading [40], [41], [42]

$$h^* = \frac{K'}{K' + 1} h_{\text{LoS}}^* + \frac{1}{K' + 1} h_{\text{NLoS}}^*,$$  (43)

where $K'$ represents the Rician factor, $h_{\text{LoS}}^*$ and $h_{\text{NLoS}}^*$ represent the deterministic Line-of-Sight (LoS) and Rayleigh fading/Non-LoS (NLoS) components, respectively. The LoS components are expressed as the responses of the $N$-elements uniform linear array $h_{\text{LoS}}^* = a_m(\theta)a_n(\theta)^H$. The array response of an $N$-elements IRS can be calculated by

$$a_m = \exp\left(j \frac{2\pi}{\lambda} d_t (m - 1) \sin \phi_{\text{LoS}_1} \sin \theta_{\text{LoS}_1}\right), m = 1, \ldots, M,$$

$$a_n = \exp\left(j \frac{2\pi}{\lambda} d_r (n - 1) \sin \phi_{\text{LoS}_2} \sin \theta_{\text{LoS}_2}\right), n = 1, \ldots, N,$$

where $d_t$ and $d_r$ are the inter-antenna separation distance at the transmitter and receiver, $\phi_{\text{LoS}_1}$ and $\phi_{\text{LoS}_2}$ are the LoS azimuth at the base station and the IRS, and $\theta_{\text{LoS}_1}$ and $\theta_{\text{LoS}_2}$ are the angle of departure at the base station and the angle of arrival at the IRS, respectively. The rest of parameter settings are listed in Table 1. To validate the effectiveness and superiority of our proposed scheme, we respectively consider the basic transmission scheme in the traditional wireless systems and IRS-assisted systems as the baselines. Thus two baselines below are considered:

- **Baseline 1**: Beamforming is considered at the base station, and the IRS is not deployed in the system.
- **Baseline 2**: Beamforming is considered at the base station, and only one IRS is deployed in the system.

4.2 Performance Comparison and Analysis

The achievable secrecy rate versus the number of users is shown in Fig. 3. As we observe, the performance of all schemes in terms of achievable secrecy rate are degrading rapidly with the increase in the number of users. When there are more than 2 users, the proposed scheme performs better than AN-disabled scheme by up to 18.9%. Here, for a fair comparison, we also set $\beta_{\text{BI}} = \beta_{\text{BE}} = 2$ in baseline 1. The result also shows that the beamforming scheme in baseline 1 cannot deal with multiple users scenarios. Moreover, since the distance between the IRS and users significantly influences the performance of IRS-assisted schemes, we also set up a friendly scenario for baseline 2, i.e., all users are uniformly placed on the line from (8, 67, 2) to (8, 75, 2). When only a single IRS is deployed (baseline 2), the performance becomes even worse than that for baseline 1. The reason is that the environmental diversity provided by the single IRS is very limited. If the overall performance is considered, e.g., the sum of secrecy rate, the system still can sacrifice a part of users’ performance to achieve a better overall performance. If the worst performance in the system is considered as the objective, it becomes hard to optimize since each user matters. In this case, the algorithm tends to sacrifice the users who have the highest secrecy rate and make up for the users who have the worst secrecy rate.

![Fig. 2. The illustration of our evaluation setups, the users and IRSs are located on a circle with the center being the base station.](image-url)

**TABLE 1**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier frequency</td>
<td>800MHz</td>
</tr>
<tr>
<td>IRS configuration</td>
<td>Uniform rectangular array with 5 elements in a row and N/5 columns with 3A/8 spacing</td>
</tr>
<tr>
<td>Path loss exponent</td>
<td>$\beta_{\text{BU}} = \beta_{\text{BE}} = 4$, $\beta_{\text{BI}} = \beta_{\text{BE}} = 2$, respectively</td>
</tr>
<tr>
<td>Rician channel factor</td>
<td>$K'<em>{\text{BU}} = K'</em>{\text{BE}} = 0$, $K'<em>{\text{BI}} = K'</em>{\text{BU}} = \infty$, respectively</td>
</tr>
<tr>
<td>Path loss at 1 meter</td>
<td>$L_0 = -30\text{dB}$</td>
</tr>
<tr>
<td>Other parameters</td>
<td>$N_0 = -174\text{dBm}$, $\text{Tx} = 4$, $\delta = 10^3$, $\theta^\prime = 20^\circ$</td>
</tr>
</tbody>
</table>

---

8. $(x, y, z)$ coordinate is adopted and 3D distance is calculated in the evaluation.

9. The reference path loss is calculated by free-space path loss formula, i.e., $L_d(d_0) = 20\log_{10}(\frac{d_0}{\lambda})$, where $d_0$ denotes the reference distance and $\lambda$ denotes the wave length [43].

Authorized licensed use limited to: University of Science & Technology of China. Downloaded on September 13, 2023 at 05:35:52 UTC from IEEE Xplore. Restrictions apply.
but the compensation is not significant enough due to the lack of environmental diversity. In this case, a poor performance is observed. When only beamforming is considered at the base station (baseline 1), even when it has better channel condition over direct channel (transmitter to users) than that for the proposed scheme, without the assistance of IRSs and reflecting channels, the wireless signals through direct channel can be easily intercepted by the eavesdropper who is located in between the base station and the first user, which results in worse performance than that for the proposed scheme.

![Fig. 4. The achievable secrecy rate versus the number of elements ($P_{\text{max}} = 40dBm$).](image)

The reason why the performance of the proposed scheme with AN and without AN are similar can be explained as follows. Since the total transmission power is shared by both user signal and AN, the usage of AN will also sacrifice the power of user signal. The gain brought by AN can be very limited. Thus, the performance of AN-enabled scheme and AN-disabled scheme are similar. However, when multi-user scenarios are considered, the interference is introduced among users and the achievable rate $R_u$ at the user is therefore degraded. Even adopting the same beamforming direction, AN-enabled scheme can further leverage the reflecting channel provided by IRSs and create additional noise at the eavesdropper while decreasing the interference since part of the power of useful signal is allocated to AN. Thus, AN-enabled scheme does provide better performance under multi-user scenarios.

The performance of achievable secrecy rate versus transmission power is shown in Fig. 5. The maximum transmission power ranges from 7W (38.45dBm) to 10W (40dBm). With the increase in transmission power, the performance of all schemes increase linearly. Similar to the results in Fig. 3, the proposed scheme outperforms the AN-disabled scheme when there are more than 2 users in the system. To have a fair comparison, we also consider LoS channel is not blocked by obstacle and set $\beta_{BU} = \beta_{BE} = 2$ for baseline 1 with 2 users. However, the result shows that the performance of baseline 1 is much lower than IRS-assisted schemes. For baseline 2, since the performance is mainly limited by environmental diversity, it remains relatively steady and increases linearly from 0.9bps/Hz to 0.96bps/Hz with the increase in transmission power.

![Fig. 5. The achievable secrecy rate versus maximum transmission power ($N = 30$).](image)
To explore the influence of positioning to the security performance, we further evaluate the performance of the proposed scheme with different position settings as shown in Fig. 6. Here, we set four different locations for the eavesdropper:

- **Setup A**: The eavesdropper is located in the middle between the base station and the first user at \((10, 60, 5)\).
- **Setup B**: The eavesdropper is located under the base station at \((10, 0, 0)\).
- **Setup C**: The eavesdropper is located in the middle between the first user and the second user at \((19, 64, 5)\).
- **Setup D**: The eavesdropper is located at the other side of the base station at \((10, -60, 5)\).

Based on the location setting we mentioned before, the locations of users and IRSs are further adjusted through Y-axis translation, e.g., users’ coordinates are transformed as \((x, y + l, z)\) for location offset \(l\). For different locations of the eavesdropper, we observe that the best security performance is obtained when the eavesdropper is faraway from the base station and users at \((10, -60, 5)\), and the secrecy rate linearly increases with the decrease of the distance between the base station and users. For other locations, the worst performance is obtained when the eavesdropper is the closest to the first user, and the performance of the proposed scheme increases with the increase of the distance between the eavesdropper and the first user. For different locations of users and IRSs, when the eavesdropper is faraway from users, i.e., Setup B and Setup D, we also find that the performance increases with the decrease of the distance between users and the base station, which implies that the performance is mainly dominated by the communication distance since the eavesdropper hardly intercepts useful signals. Meanwhile, when the eavesdropper is close to users, i.e., Setup A and Setup C, the slope on the right side of the inflection point is smaller than the one on the left side, which implies that the leakage to the eavesdropper is even worse when the eavesdropper is located behind users.

According to the results given above, some deployment strategies can be designed to offer guidance in practice. For multi-user scenarios, multiple surfaces (greater than the number of users) are desired to be deployed to achieve secure transmission with a higher secrecy rate. Meanwhile, considering the nonlinear relationship between secrecy rate and the number of elements, it may not be beneficial to deploy as many elements as possible on each surface, and rather a certain number of elements with the highest performance-cost ratio is preferred. Furthermore, due to the linear relationship between secrecy rate and transmission power, higher transmission power is always preferred. Finally, even though the exact location of the eavesdropper can hardly be known in real-time, the deployment location of surfaces should be as far as possible from potential locations of the eavesdropper in statistics, which can also lead to a more secure transmission environment.

### 4.3 Performance With Imperfect CSI and Discrete Adjustment

Considering hardware limitations in practical systems, the perfect channel state information may not be available, especially considering an eavesdropper passively wiretaps signals. Thus, we conduct some performance comparisons in order to evaluate the impact of such practical constraints. First, due to the existence of channel estimation error in practice, CSI error should be further estimated. Here, we adopt a statistical CSI error model in our analysis. Let \( \mathcal{CN}(\mu, C) \) represent Circularly Symmetric Complex Gaussian (CSCG) random vector with mean \( \mu \) and covariance matrix \( C \). According to the existing works \([44],[45],[46]\), we assume the CSI in the reflecting channel from the transmitter to IRS then to Eve is imperfect, and the CSI on \( g_{e,k}^m \) and \( G_{e}^m \) considered in our previous system model can be respectively characterized as

\[
g_{e,k}^m = g_{e,k}^m + \Delta g_{e,k}^m, \tag{44}
\]

\[
h_{e}^m = h_{e}^m + \Delta h_{e}^m, \tag{45}
\]

where \( g_{e,k}^m \) and \( h_{e}^m \) denote the mean of the channel gain, and \( \Delta g_{e,k}^m \) and \( \Delta h_{e}^m \) capture the uncertainty (i.e., CSI error vectors) in the channel. The CSI error vectors \( \Delta g_{e,k}^m \) and \( \Delta h_{e}^m \) are

---

**Fig. 6.** The achievable secrecy rate versus position setting \((P_{\text{max}} = 40\text{dBm}, N = 20, \text{User} = 2)\).

**Fig. 7.** The achievable secrecy rate with imperfect CSI model \((P_{\text{max}} = 40\text{dBm}, \text{User} = 2)\).
assumed to follow the CSCG distribution. Here, the parameter setting of CSCG distribution is similar to [44], [45], \( \mu = 0 \) is adopted, and the variance matrix of \( \text{vec}(\Delta g^H) \) and \( \text{vec}(\Delta h^H) \) is defined as \( C = \varepsilon^2 \delta I \), where \( \varepsilon^2 = \delta \| \text{vec}(\Delta g^H) \| \) and \( \delta = \delta \| \text{vec}(\Delta h^H) \| \), and \( \delta, \varepsilon \in [0, 1] \) is the normalized CSI error, which measures the relative amount of CSI uncertainties. Fig. 7 shows the performance impact on the proposed scheme under imperfect CSI. We observe that the secrecy rate for the proposed scheme under imperfect CSI can also be improved with the increase of the number of elements on IRSs. These results imply that the eavesdropper information does help optimize the minimum secrecy rate since imperfect CSI error can decrease the minimum secrecy rate in the system, but the impact due to imperfect CSI error on the sum of secrecy rates is limited.

Considering the practical constraint with discrete phase shift, we adopt a discrete phase shift model used in the existing works [42], [47], [48]. Accordingly, the diagonal phase-shifting matrix of the \( k \)-th IRS we considered in Section 2 can be further modeled as

\[
\Theta_k = \text{diag}(A_{k,1}e^{j\theta_{k,1}}, \ldots, A_{k,N}e^{j\theta_{k,N}}) \in \mathbb{C}^{N \times N},
\]

where \( \theta_{k,n} \in [0, \frac{2\pi}{L_q}, \ldots, \frac{2\pi(L_q-1)}{L_q}] \) with \( L_q = 2^m \), i.e., the discrete phase-shift values are assumed to be equally spaced in the interval \( [0, 2\pi] \), and \( A_{k,n} \in \{ a_1, \ldots, a_{L_q} \} \) denotes the controllable amplitude set which satisfies \( L_q = 2^m \). When \( \theta_0 = 0 \), the space of amplitude control reduces to the case of full reflection, which is considered in our previous system model, i.e., \( A_{k,n} = 1 \), when \( \theta_0 = 1 \), the space of amplitude control represents on/off reflection, i.e., \( A_{k,n} \in \{ 0, 1 \} \).

Fig. 8 shows the performance comparisons between the cases under continuous phase shift and discrete phase shift. Note that “Continuous Phase Shift” in the figure represents the proposed scheme, “Discrete Phase Shift” in the figure denotes the proposed scheme with discrete phase shift constraint by executing Algorithm 1, and “Discrete Phase Shift Approximation” in the figure captures the discretization of the results obtained from “Continuous Phase Shift”. Based on the performance under continuous phase shift obtained from the proposed scheme, the performance under discrete phase shift, has a constant gap to the continuous one. Meanwhile, by taking discrete approximation based on the continuous phase shift, the performance of discrete phase shift approximation converges to the performance of the case under the continuous phase shift as \( L_q \) increases. Hence, by taking discrete approximation, the proposed scheme can easily achieve a similar performance in practical systems under the constraint of discrete phase shift.

To evaluate the influence of the amplitude control, we also conduct the performance comparison with discrete amplitude control in Fig. 9. Note that “Unit Modulus” in the figure denotes the proposed scheme, “Discrete Amplitude Control” in the figure represents the proposed scheme with discrete amplitude constraint by executing Algorithm 1, and “Amplitude Control Approximation” in the figure indicates the product of modulus coefficient times the results obtained from “Unit Modulus”. We add the reflecting amplitude limitation to the phase shift \( \Theta_k \) obtained from the proposed algorithm, the modulus coefficient for amplitude control scheme in the figure will be applied to all \( A_{k,n} \) in \( \Theta_k \). Intuitively, we can see that there is no gain when reducing reflecting amplitude on the IRS. Meanwhile, compared to the performance of the proposed scheme with unit modulus (blue line in the figure), the performance of the discrete amplitude control (including \( L_a = 2 \) and \( L_a = 4 \)) by using
brute-force searching also shows that the additional amplitude control cannot bring performance improvement in the proposed scheme.

### 4.4 Performance With Sum-Rate Problem

In general, overall security performance is a common objective considered in related works. To compare the performance of the max-min problem proposed in this paper with the commonly studied sum-rate maximization, we plot Figs. 10 and 11 to show the difference in terms of the minimum secrecy rate and the sum of secrecy rate, where the problem in (6) with constraints (C1), (C3), and (C5) can be reformulated as

\[
\max \sum_{t} \left( R_{t}^{s} - R_{t}^{e} \right) + \theta \alpha
\]

s.t. \( (C1)-(C5) \).

Note that “MSR” and “SSR” in the legend represent the minimum secrecy rate and the sum of secrecy rate, respectively. As shown in Fig. 10, for the performance in terms of the minimum secrecy rate and the sum of secrecy rates, the gap between the proposed scheme and the traditional sum-rate maximization is limited. This phenomenon implies that a max-min problem can achieve better minimum secrecy rate and also reach similar performance in overall secrecy rate in an IRS-assisted system. Meanwhile, in Fig. 11, the sum of secrecy rate increases with the number of users. Even though it can sacrifice some users’ performance to improve overall performance, the curve shows that the gain becomes less and the sum secrecy rate reaches a threshold with the increase in the number of users, which represents the maximum secrecy capacity in the system. For the gap between two different objectives, it also becomes larger with the increase in the number of users, which is reasonable since the solution space becomes larger with more users in the system, and different solutions obtained from the aforementioned objectives do impact more users.

### 5 Conclusion

In this paper, we have focused on physical layer security in wireless systems with IRSs, and investigated a max-min problem regarding secrecy rate under one typical eavesdropper scenario. By placing multiple collaborative IRSs in complex environment, the base station could leverage the environmental diversity to achieve significant improvement in terms of secrecy rate through joint optimization of beamforming and phase shift on the IRS. Based on our numerical evaluation, when multiple users are considered, the additional AN has been proven to effectively create interference at the eavesdropper and further improve the performance in terms of secrecy rate. Compared with the secrecy rate for our proposed scheme under discrete phase shift/amplitude control, we have observed that, with the increase of discretization granularity, the secrecy rate obtained from the discrete approximation method converges to that achieved from the proposed scheme. In the future, we plan to extend our study by considering a general adversary model and explore the specific collaborative protocols/mechanism among multiple IRSs.

### References


Jian Li (Member, IEEE) received the BS degree from the Department of Electronic and Information Engineering, Anhui University, in 2015 and the PhD degree from the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC), in 2020. From November 2019 to November 2020, he was a visiting scholar with the Department of Electronic and Computer Engineering, University of Florida. He is currently a postdoctoral fellow with the School of Cyber Science and Technology, USTC. His research interests include wireless communications, satellite networks, and next-generation Internet.
Lan Zhang (Member, IEEE) received the BE and MS degrees from the University of Electronic Science and Technology of China, in 2013 and 2016, respectively, and the PhD degree from the University of Florida in 2020. She is currently a tenure-track assistant professor with the Department of Electrical and Computer Engineering, Michigan Technological University. Her research interests include wireless communications, distributed machine learning, and cybersecurity for various IoT or CPS applications.

Kaiping Xue (Senior Member, IEEE) received the bachelor’s degree from the Department of Information Security, University of Science and Technology of China (USTC), in 2003 and the PhD degree from the Department of Electronic Engineering and Information Science (EEIS), USTC, in 2007. From May 2012 to May 2013, he was a postdoctoral researcher with Department of Electrical and Computer Engineering, University of Florida. He is currently a professor with the School of Cyber Science and Technology, USTC. He has authored and coauthored more than 100 technical papers in the areas of communication networks and network security. His research interests include next-generation Internet, distributed networks, and network security. He is on the editorial board of several journals, including the IEEE Transactions on Vehicular Technology, the IEEE Transactions on Dependable and Secure Computing, and the IEEE Transactions on Network and Service Management. He is an IET Fellow.

For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/csdl.