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 Mutiple-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 metasurface 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. The work of Y. Fang was supported in part by U.S. National Science Foundation under Grant CNS-2106589. The work of K. Xue was supported in part by the National Natural Science Foundation of China under Grant 61972371 and in part by Youth Innovation Promotion Association of the Chinese Academy of Sciences (CAS) under Grant Y202093.
(Corresponding author: Yuguang Fang.)
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 Mutiple-Input Mutiple-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 Mutiple-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,[1] if one legitimate user' 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 letters 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 $\mathbf{A}^H$, $\mathrm{Rank}(\mathbf{A})$ and $\mathrm{Tr}(\mathbf{A})$, respectively. For a complex number c, $|c|$ denotes the modulus. $\angle(x)$ denotes the phase of the complex value x. The set of n-by-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 $\mathcal{N}(\mu,\sum)$ denotes the Gaussian distribution with mean μ and covariance matrix $\sum$.

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].

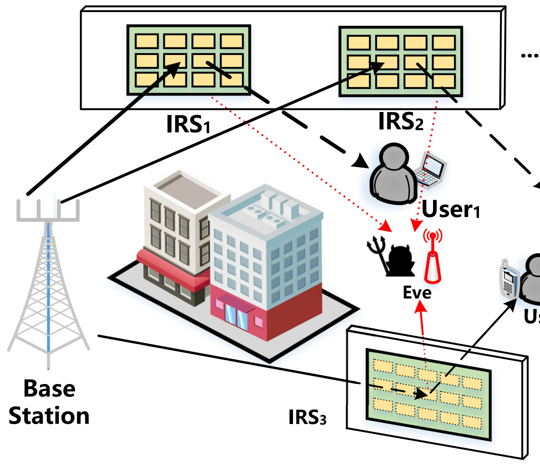


Fig. 1. A typical IRSs-assisted communication system with multiple users under eavesdropping.

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 I 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 base station to IRS link, IRS's reflection with phase shift and IRS to user/Eve link. The equivalent channels from the base station to the kth IRS, the ith user and Eve are denoted by $\boldsymbol{G}_k^H \in \mathbb{C}^{N\times M}$, $\boldsymbol{h}_i^H \in \mathbb{C}^{1\times M}$, $\boldsymbol{h}_e^H \in \mathbb{C}^{1\times M}$, respectively. The equivalent channels from the kth IRS to the ith user and Eve are denoted by $\boldsymbol{g}_{i,k}^H \in \mathbb{C}^{1\times N}$, $\boldsymbol{g}_e^H \in \mathbb{C}^{1\times N}$, respectively. Since IRS is a passive reflecting device, we consider a Time Division Duplexing (TDD) protocol[2] for uplink and downlink transmissions and quasi-static (constant within the transmission frame) flat-fading model[3] 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 ith user can be described as

$$s_i = \boldsymbol{\omega}_i d_i + z_i, i \in \mathcal{U}, \tag{1}$$

where $\boldsymbol{\omega}_i \in \mathbb{C}^{M\times 1}$ is the beamforming vector for the ith user, d_i is the corresponding transmitted data, $z_i \in \mathbb{C}^{M\times 1}$ is an AN vector, and $\mathcal{U}$ 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 ith user, i.e., the ith user can receive reflecting signal through the kth IRS if $\alpha_{i,k} = 1$. Meanwhile, let $\boldsymbol{\Theta}_k = \mathrm{diag}(A_{k,1}e^{j\theta_{k,1}}, \ldots, A_{k,N}e^{j\theta_{k,N}}) \in \mathbb{C}^{N\times N}$ denote the diagonal phase-shifting matrix of the kth IRS, while $A_{k,n} \in [0,1]$ and $\theta_{k,n} \in [0, 2\pi)$ denote the amplitude reflection coefficient and the phase shift of the nth element on the kth IRS. In practice, each element of an IRS is usually designed to maximize the signal reflection [14]. Thus, we set $A_{k,n} = 1$ in this paper. In this case, for the ith user, the received signal from base station and IRSs can be represented by

$$\begin{aligned} \boldsymbol{y}_i = &\left(\sum_{k=1}^{K} \alpha_{i,k}\boldsymbol{g}_{i,k}^H \boldsymbol{\Theta}_k \boldsymbol{G}_k^H + \boldsymbol{h}_i^H\right)(\boldsymbol{\omega}_i d_i + z_i) \\ &+ \sum_{j\neq i}(\sum_{k=1}^{K} \alpha_{j,k}\boldsymbol{g}_{i,k}^H \boldsymbol{\Theta}_k \boldsymbol{G}_k^H + \boldsymbol{h}_i^H)(\boldsymbol{\omega}_j d_j + z_j) + n_0, \end{aligned} \tag{2}$$

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

$$\begin{aligned} \boldsymbol{y}_i^e = &\left(\sum_{k=1}^{K} \alpha_{i,k}\boldsymbol{g}_{e,k}^H \boldsymbol{\Theta}_k \boldsymbol{G}_k^H + \boldsymbol{h}_e^H\right)(\boldsymbol{\omega}_i d_i + z_i) \\ &+ \sum_{j\neq i}(\sum_{k=1}^{K} \alpha_{j,k}\boldsymbol{g}_{e,k}^H \boldsymbol{\Theta}_k \boldsymbol{G}_k^H + \boldsymbol{h}_e^H)(\boldsymbol{\omega}_j d_j + z_j) + n_0. \end{aligned} \tag{3}$$

For notational simplicity, let $\hat{D}_{i,j} = \sum_{k=1}^{K} \alpha_{j,k}\boldsymbol{g}_{i,k}^H \boldsymbol{\Theta}_k \boldsymbol{G}_k^H + \boldsymbol{h}_i^H \in \mathbb{C}^{1\times M}$, $\boldsymbol{D}_{e,i} = \sum_{k=1}^{K} \alpha_{i,k}\boldsymbol{g}_{e,k}^H \boldsymbol{\Theta}_k \boldsymbol{G}_k^H + \boldsymbol{h}_e^H \in \mathbb{C}^{1\times M}$. Accordingly, the SINR of received signal at the ith 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.

$$SINR_i = \frac{|(\sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{i,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_i^H)\boldsymbol{\omega}_i|^2}{\sum_{j\neq i}|\hat{\boldsymbol{D}}_{i,j}\boldsymbol{\omega}_j|^2 + \sum_{j\in\mathcal{U}}|\hat{\boldsymbol{D}}_{i,j}\boldsymbol{z}_j|^2 + N_0}, \tag{4}$$

where N_0 is the power of AWGN. Similarly, the SINR of the ith user's signal at the eavesdropper can be calculated by

$$SINR_i^e = \frac{|(\sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{e,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_e^H)\boldsymbol{\omega}_i|^2}{\sum_{j\neq i}|\boldsymbol{D}_{e,j}\boldsymbol{\omega}_j|^2 + \sum_{j\in\mathcal{U}}|\boldsymbol{D}_{e,j}\boldsymbol{z}_j|^2 + N_0}. \tag{5}$$

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 $\bar{\boldsymbol{\omega}} = [\boldsymbol{\omega}_1, \boldsymbol{\omega}_2 \ldots, \boldsymbol{\omega}_I]$ and AN matrix $\bar{z} = [z_1, z_2, \ldots, z_I]$ at the base station, phase shift matrix $\bar{\boldsymbol{\Theta}} = [\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2, \ldots, \boldsymbol{\Theta}_K]$ at IRSs and surface selection matrix $\bar{\boldsymbol{\alpha}} = \begin{bmatrix} \alpha_{1,1} & \ldots & \alpha_{1,K} \\ \ldots & \ldots & \ldots \\ \alpha_{I,1} & \ldots & \alpha_{I,K} \end{bmatrix}$ between users and IRSs, the optimization problem can be formulated as

$$\textbf{Problem 1}: \quad \max_{\bar{\boldsymbol{\omega}},\bar{z},\bar{\boldsymbol{\Theta}},\bar{\boldsymbol{\alpha}}} \ \min_i \quad [R_i^u - R_i^e]^+ \tag{6}$$

$$s.t. \quad ||\boldsymbol{\omega}_i||^2 + ||z_i||^2 \leq P_{max}, \ \forall i \in \mathcal{U}, \tag{C1}$$

$$0 \leq \theta_{k,n} \leq 2\pi, \ k \in [1,K], \forall n \in [1,N], \tag{C2}$$

$$\sum_k \alpha_{i,k} = 1, \ \alpha_{i,k} \in \{0,1\}, \ \forall i \in \mathcal{U}, \tag{C3}$$

where (C1) represents the transmission power constraint, (C2) implies the unit modulus for each element, i.e., $|e^{j\theta_{k,n}}| = 1$, and (C3) indicates that each user should be served by one IRS in the system. Considering the SINR expression in (4), (5) and applying the Shannon capacity theorem, the achievable secrecy rate (bits/s/Hz) in (6) can be calculated by

$$\begin{aligned} R_i^u - R_i^e = &\log_2\left(1 + \frac{|(\sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{i,k}^H\boldsymbol{\Theta}_k G_k^H + \boldsymbol{h}_i^H)\boldsymbol{\omega}_i|^2}{\sum_{j\neq i}|\hat{\boldsymbol{D}}_{i,j}\boldsymbol{\omega}_j|^2 + \sum_{j\in\mathcal{U}}|\hat{\boldsymbol{D}}_{i,j}\boldsymbol{z}_j|^2 + N_0}\right) \\ &- \log_2\left(1 + \frac{|(\sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{e,k}^H\boldsymbol{\Theta}_k G_k^H + \boldsymbol{h}_e^H)\boldsymbol{\omega}_i|^2}{\sum_{j\neq i}|\boldsymbol{D}_{e,j}\boldsymbol{\omega}_j|^2 + \sum_{j\in\mathcal{U}}|\boldsymbol{D}_{e,j}\boldsymbol{z}_j|^2 + N_0}\right). \end{aligned} \tag{7}$$

It is intuitive that variables $\bar{\boldsymbol{\omega}}$, $\bar{z}$, $\bar{\boldsymbol{\Theta}}$ and $\bar{\boldsymbol{\alpha}}$ in *Problem 1* are coupled, which makes *Problem 1* hard to solve. However, if only one variable is considered, the original problem becomes solvable. Inspired by the alternating optimization approaches in [5], [14], [19], [20], [21], [27], we adopt Block Coordinate Descent (BCD) method to decouple variables and obtain the sub-optimal solution efficiently. As a powerful and computationally efficient optimization technique to solve multi-variable involved problems, BCD method has been widely adopted in wireless communication and signal processing. By using the BCD method, we can transform the original problem into several solvable (e.g., convex) sub-problems in an iterative manner. To optimize a multi-variable objective in BCD method, we optimize the objective in terms of one of the coordinate blocks while the other blocks are fixed at each iteration. Thus, *Problem 1* is divided into three sub-problems and each sub-problem is solved iteratively as descried 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 descried in the following sub-sections.

Algorithm 1. BCD-Based Algorithm

Input: Number of elements N, number of antennas M, number of surfaces K;
Output: Beamforming vector $\bar{\boldsymbol{\omega}}$, AN vector $\bar{z}$, phase -shift matrix $\bar{\boldsymbol{\Theta}}$ and IRS selection vector $\bar{\alpha}$;
Initialize:
- Initialize $\bar{\boldsymbol{\omega}}^{(0)}$, $\bar{z}^{(0)}$, $\bar{\boldsymbol{\Theta}}^{(0)}$ and $\bar{\boldsymbol{\alpha}}^{(0)}$;
- $t = 0$, $\Delta^{(t)} = Intmax$;

while $\Delta^{(t)} < \delta$ **do**
  Solve each sub-problem to find solution for $\bar{\boldsymbol{\omega}}^{(t+1)}$, $\bar{z}^{(t+1)}$, $\bar{\boldsymbol{\Theta}}^{(t+1)}$ and $\bar{\boldsymbol{\alpha}}^{(t+1)}$ for given $\bar{\boldsymbol{\omega}}^{(t)}$, $\bar{z}^{(t)}$, $\bar{\boldsymbol{\Theta}}^{(t)}$ and $\bar{\boldsymbol{\alpha}}^{(t)}$, respectively;
  Calculate $\rho^{(t+1)} = \min_i \quad [R_i^u - R_i^e]$;
  Update $t = t+1$ and $\Delta^{(t)} = \rho^{(t+1)} - \rho^{(t)}$;
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 $\bar{\boldsymbol{\Theta}}$ and surface matching $\bar{\boldsymbol{\alpha}}$, with $[x]^+ = \max\{0, x\}$, we can rewrite *Problem 1* as

$$\textbf{Problem 2a}: \quad \max_{\bar{\boldsymbol{\omega}},\bar{z}} \ \min_i \quad [R_i^u - R_i^e]^+ \tag{8}$$

$$s.t. \quad ||\boldsymbol{\omega}_i||^2 + ||z_i||^2 \leq P_{max}, \ \forall i \in \mathcal{U}. \tag{C1}$$

Due to the max function in (8), we can rewrite the objective as

$$[R_i^u - R_i^e]^+ = \begin{cases} 0, (\boldsymbol{\omega}_i, \boldsymbol{z}_i) \in \mathcal{A}, \\ R_i^u - R_i^e, (\boldsymbol{\omega}_i, \boldsymbol{z}_i) \in \mathcal{A}^+, \end{cases} \tag{9}$$

where $\mathcal{A}$ and $\mathcal{A}^+$ denote the solution space for non-positive and positive values, respectively. Once $\mathcal{A}^+$ is non-empty, the optimal solution must satisfy $(\boldsymbol{\omega}_i^*, \boldsymbol{z}_i^*) \in \mathcal{A}^+$. In this case, we can rewrite (8) as $R_i^u - R_i^e$ 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 *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 $\boldsymbol{W}_i = \boldsymbol{\omega}_i\boldsymbol{\omega}_i^H \in \mathbb{C}^{M\times M}$, $\boldsymbol{Z}_i = z_i z_i^H \in \mathbb{C}^{M\times M}$, $\boldsymbol{D}_i = \sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{i,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_i^H \in \mathbb{C}^{1\times M}$, $\hat{\boldsymbol{D}}_{i,j} = \sum_{k=1}^{K}\alpha_{j,k}\boldsymbol{g}_{i,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_i^H \in \mathbb{C}^{1\times M}$, $\boldsymbol{D}_{e,i} = \sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{e,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_e^H \in \mathbb{C}^{1\times M}$. Then, the achievable secrecy rate can be reformulated as

$$\bigtriangledown_{\boldsymbol{W}_i} F_i^3(\boldsymbol{W}_i,\boldsymbol{Z}_i)=0,\ \bigtriangledown_{\boldsymbol{Z}_i} F_i^3(\boldsymbol{W}_i,\boldsymbol{Z}_i)=\frac{1}{\ln 2}\frac{(\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})^H}{\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+N_0}, \tag{11}$$

$$\bigtriangledown_{\boldsymbol{W}_i} F_i^4(\boldsymbol{W}_i,\boldsymbol{Z}_i)=\frac{1}{\ln 2}\frac{(\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})^H}{\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_{e,i}^H\boldsymbol{D}_{e,i})+\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+N_0}, \tag{12}$$

$$\bigtriangledown_{\boldsymbol{Z}_i} F_i^4(\boldsymbol{W}_i,\boldsymbol{Z}_i)=\frac{1}{\ln 2}\frac{(\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})^H}{\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_{e,i}^H\boldsymbol{D}_{e,i})+\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+N_0}. \tag{13}$$

$$\begin{aligned}
R_i^u-R_i^e&=\log_2\left(1+\frac{\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_i^H\boldsymbol{D}_i)}{\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+N_0}\right)\\
&-\log_2\left(1+\frac{\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_{e,i}^H\boldsymbol{D}_{e,i})}{\sum_{j\neq i}(\mathrm{Tr}(\boldsymbol{W}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+N_0}\right),\\
&=\log_2\Bigg(\frac{\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_i^H\boldsymbol{D}_i)+\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+N_0}{\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+N_0}\\
&\cdot\frac{\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+N_0}{\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_{e,i}^H\boldsymbol{D}_{e,i})+\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+N_0}\Bigg),\\
&=F_i^1+F_i^2-F_i^3-F_i^4,
\end{aligned} \tag{10}$$

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

$$F_i^1=\log_2\left(\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_i^H\boldsymbol{D}_i)+\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+N_0\right), \tag{14}$$

$$F_i^2=\log_2\left(\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+N_0\right), \tag{15}$$

$$F_i^3=\log_2\left(\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\hat{\boldsymbol{D}}_{i,j}^H\hat{\boldsymbol{D}}_{i,j})+N_0\right), \tag{16}$$

$$F_i^4=\log_2\left(\mathrm{Tr}(\boldsymbol{W}_i\boldsymbol{D}_{e,i}^H\boldsymbol{D}_{e,i})+\sum_{j\neq i}\mathrm{Tr}(\boldsymbol{W}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+\sum_{j\in\mathcal{U}}\mathrm{Tr}(\boldsymbol{Z}_j\boldsymbol{D}_{e,j}^H\boldsymbol{D}_{e,j})+N_0\right). \tag{17}$$

However, the secrecy rate $R_i^u-R_i^e$ in (10) is still in the form of Difference of Convex (DC) functions. Since the non-convexity of the DC problem prevents the application of standard primal/dual decomposition techniques for convex problems, we have to find an efficient method to convert the DC problem to a convex one. To solve the DC problem in (10), we adopt SCA method [21], [31], [32], [33] to obtain a convex upper bound for the DC objective in an iterative manner. The main idea of SCA method is to generate a sequence of feasible solutions $(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})$ 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 $(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})$, the differentiable convex functions $F_i^3(\boldsymbol{W}_i,\boldsymbol{Z}_i)$ and $F_i^4(\boldsymbol{W}_i,\boldsymbol{Z}_i)$ satisfy the following inequalities:[4]

$$\begin{aligned}
F_i^3(\boldsymbol{W}_i,\boldsymbol{Z}_i)&\leq F_i^3(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})\\
&\quad+\mathrm{Tr}\Big(\bigtriangledown_{\boldsymbol{W}_i}F_i^3(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})^H(\boldsymbol{W}_i-\boldsymbol{W}_i^{(t)})\Big)\\
&\quad+\mathrm{Tr}\Big(\bigtriangledown_{\boldsymbol{Z}_i}F_i^3(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})^H(\boldsymbol{Z}_i-\boldsymbol{Z}_i^{(t)})\Big)\\
&=\widetilde{F}_i^3(\boldsymbol{W}_i,\boldsymbol{Z}_i,\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)}),
\end{aligned} \tag{18}$$

$$\begin{aligned}
F_i^4(\boldsymbol{W}_i,\boldsymbol{Z}_i)&\leq F_i^4(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})\\
&\quad+\mathrm{Tr}\Big(\bigtriangledown_{\boldsymbol{W}_i}F_i^4(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})^H(\boldsymbol{W}_i-\boldsymbol{W}_i^{(t)})\Big)\\
&\quad+\mathrm{Tr}\Big(\bigtriangledown_{\boldsymbol{Z}_i}F_i^4(\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)})^H(\boldsymbol{Z}_i-\boldsymbol{Z}_i^{(t)})\Big)\\
&=\widetilde{F}_i^4(\boldsymbol{W}_i,\boldsymbol{Z}_i,\boldsymbol{W}_i^{(t)},\boldsymbol{Z}_i^{(t)}),
\end{aligned} \tag{19}$$

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 $\boldsymbol{W}_i$ and $\boldsymbol{Z}_i$ are given in (11), (12), and (13). Hence, a convex lower bound of objective function in (10) can be obtained as $R_i^u-R_i^e=F_i^1+F_i^2-\widetilde{F}_i^3-\widetilde{F}_i^4$. Let $f_i(\boldsymbol{W}_i,\boldsymbol{Z}_i)=F_i^1+F_i^2-F_i^3-F_i^4$ and $g_i(\boldsymbol{W}_i,\boldsymbol{Z}_i)=F_i^1+F_i^2-\widetilde{F}_i^3-\widetilde{F}_i^4$. Since $f_i(\boldsymbol{W}_i,\boldsymbol{Z}_i)\geq g_i(\boldsymbol{W}_i,\boldsymbol{Z}_i)$ according to (18) and (19), as long as we guarantee $g_i(\boldsymbol{W}_i,\boldsymbol{Z}_i)\geq 0$, $f_i(\boldsymbol{W}_i,\boldsymbol{Z}_i)>0$ 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

$$\textbf{Problem 2b}:\quad \max_{x,\bar{\boldsymbol{W}},\bar{\boldsymbol{Z}}}\quad x \tag{20}$$

$$s.t.\quad \mathrm{Tr}(\boldsymbol{W}_i)+\mathrm{Tr}(\boldsymbol{Z}_i)\leq P_{max},\ \forall i\in\mathcal{U}, \tag{C1}$$

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 $f(y)\leq\frac{f((1-\lambda)x+\lambda y)-(1-\lambda)f(x)}{\lambda}=f(x)+\frac{f(x+\lambda(y-x))-f(x)}{\lambda}\rightarrow f(x)+\bigtriangledown f(x)(y-x)$ as $\lambda\rightarrow 0$ [34, Proposition 1.8].

$$0 \le x \le F_i^1 + F_i^2 - \widetilde{F}_i^3 - \widetilde{F}_i^4, \forall i \in \mathcal{U}, \tag{C4}$$

$$\text{Rank}(\boldsymbol{W}_i) = 1,\ \text{Rank}(\boldsymbol{Z}_i) = 1,\ \forall i \in \mathcal{U}, \tag{C5}$$

$$\boldsymbol{W}_i \succeq \boldsymbol{0},\ \boldsymbol{Z}_i \succeq \boldsymbol{0},\ \forall i \in \mathcal{U}, \tag{C6}$$

where $\bar{\boldsymbol{W}} = [\boldsymbol{W}_1, \boldsymbol{W}_2, \ldots, \boldsymbol{W}_I], \bar{\boldsymbol{Z}} = [\boldsymbol{Z}_1, \boldsymbol{Z}_2, \ldots, \boldsymbol{Z}_I] \in \mathbb{C}^{IM\times IM}$. Since constraint (C5) is non-convex, we drop this rank-1 constraint by applying SDR. If the obtained solution $(\boldsymbol{W}_i^{(t)}, \boldsymbol{Z}_i^{(t)})$ are of rank-1, they can be written as $\boldsymbol{W}_i^{(t)} = \boldsymbol{\omega}_i\boldsymbol{\omega}_i^H$ and $\boldsymbol{Z}_i^{(t)} = \boldsymbol{z}_i\boldsymbol{z}_i^H$, then the optimal beamforming vector $\boldsymbol{\omega}_i$ and AN $\boldsymbol{z}_i$ can be obtained by applying eigenvalue decomposition.[5] Otherwise, we can adopt Gaussian Randomization to recover $\boldsymbol{\omega}_i$ and $\boldsymbol{z}_i$ approximately from higher rank solution $(\boldsymbol{W}_i^{(t)}, \boldsymbol{Z}_i^{(t)})$ [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 $(\bar{\boldsymbol{W}}^*, \bar{\boldsymbol{Z}}^*)$ satisfying the Karush-Kuhn-Tucker (KKT) conditions of the original problems in (8).*

Proof. For notational convenience, let $f_i(\boldsymbol{W}_i, \boldsymbol{Z}_i) = F_i^1 + F_i^2 - F_i^3 - F_i^4$ and $g_i(\boldsymbol{W}_i, \boldsymbol{Z}_i) = F_i^1 + F_i^2 - \widetilde{F}_i^3 - \widetilde{F}_i^4$. The constraint (C4) can be rewritten as $x \le \min_i\{g_i(\boldsymbol{W}_i, \boldsymbol{Z}_i)\}$.

According to (18) and (19), we can obtain $\max_i\{f_i(\boldsymbol{W}_i^{(t)}, \boldsymbol{Z}_i^{(t)})\} \ge \max_i\{g_i(\boldsymbol{W}_i^{(t)}, \boldsymbol{Z}_i^{(t)})\}, \forall \bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}} \in \mathbb{C}^{IM\times IM}$. Since constraints (C1), (C4) and (C6) are always satisfied, the optimal solution $(\bar{\boldsymbol{W}}^{(t)}, \bar{\boldsymbol{Z}}^{(t)})$ of the approximated problem (20) at the tth iteration always belongs to the feasible set of the original problem (8) At each iteration, it follows that [37], [38]

$$\begin{aligned}
\max_i\{f_i(\boldsymbol{W}_i^{(t)}, \boldsymbol{Z}_i^{(t)})\} &\ge \max_i\{g_i(\boldsymbol{W}_i^{(t)}, \boldsymbol{Z}_i^{(t)})\} \\
&= \min_{\bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}}\ \max_i\{g_i(\boldsymbol{W}_i, \boldsymbol{Z}_i)\} \\
&\ge \max_i\{g_i(\boldsymbol{W}_i^{(t-1)}, \boldsymbol{Z}_i^{(t-1)})\} \\
&= \max_i\{f_i(\boldsymbol{W}_i^{(t-1)}, \boldsymbol{Z}_i^{(t-1)})\},
\end{aligned}$$

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

5. For an SDR solution $\boldsymbol{W}$, the eigen-decomposition can be applied to obtain $\boldsymbol{W} = \sum_{n=1}^{r} \lambda_n \boldsymbol{q}_n \boldsymbol{q}_n^H$, where $r = \text{Rank}(\boldsymbol{W})$, $\lambda_1 \ge \ldots \ge \lambda_r > 0$ are the eigenvalues, and $\boldsymbol{q}_1, \ldots, \boldsymbol{q}_n \in \mathbb{C}^{n\times 1}$ are the respective eigenvectors [28]. Thus, the optimal and the only one solution for the original problem, i.e., $\boldsymbol{\omega} = \sqrt{\lambda_1}q_1$, can be obtained from the eigenvalue decomposition if $\boldsymbol{W}$ satisfies the rank-1 condition.

Algorithm 2. SCA-Based Algorithm

Input: Number of elements N, number of antennas M, number of surfaces K;
Output: Beamforming $\bar{\boldsymbol{W}}^*$, AN $\bar{\boldsymbol{Z}}^*$;
1 **Initialize:**
  • Initialize $\bar{\boldsymbol{W}}^{(0)}$, $\bar{\boldsymbol{Z}}^{(0)}$, $t = 1$, $\Delta^{(t)} = Intmax$;
2 **while** $\Delta^{(t)} < \delta$ **do**
3   Solve problem (20) to find solution $\bar{\boldsymbol{W}}^{(t)}$, $\bar{\boldsymbol{Z}}^{(t)}$;
4   Update $t = t + 1$ and $\Delta^{(t)} = x^{(t+1)} - x^{(t)}$;
5 **end**

Next, we prove that $(\bar{\boldsymbol{W}}^*, \bar{\boldsymbol{Z}}^*)$ satisfies the KKT conditions[6] of the original problem. From (20), the optimal solution can be found when $x = \min_i\{g_i(\boldsymbol{W}_i, \boldsymbol{Z}_i)\}$, thus, *Problem 2b* can be rewritten as

$$\begin{aligned}
&\max_{x, \bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}} \quad \min_i\{g_i(\boldsymbol{W}_i, \boldsymbol{Z}_i)\} \\
&s.t. \quad (C1), (C6).
\end{aligned} \tag{21}$$

Then, the Lagrangian for (21) is

$$L(\bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}, \boldsymbol{\sigma}) = \min_i\{g_i(\boldsymbol{W}_i, \boldsymbol{Z}_i)\} + \sum_{i\in\mathcal{U}} \sigma_i(\text{Tr}(\boldsymbol{W}_i) + \text{Tr}(\boldsymbol{Z}_i)),$$

where σ_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

$$L'(\bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}, \boldsymbol{\sigma}) = \min_i\{f_i(\boldsymbol{W}_i, \boldsymbol{Z}_i)\} + \sum_{i\in\mathcal{U}} \sigma_i(\text{Tr}(\boldsymbol{W}_i) + \text{Tr}(\boldsymbol{Z}_i)),$$

For a feasible point $(\bar{\boldsymbol{W}}^{(t-1)}, \bar{\boldsymbol{Z}}^{(t-1)})$ 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., $(\bar{\boldsymbol{W}}^{(t-1)}, \bar{\boldsymbol{Z}}^{(t-1)})$ is feasible for (21) and there exist nonnegative real values $\sigma_i, i \in \mathcal{U}$ satisfying

$$\begin{aligned}
&\triangledown L(\bar{\boldsymbol{W}}^{(t-1)}, \bar{\boldsymbol{Z}}^{(t-1)}, \boldsymbol{\sigma})|_{\boldsymbol{W},\boldsymbol{Z}} = 0, \\
&\sigma_i\Big(\text{Tr}(\boldsymbol{W}_i^{(t-1)}) + \text{Tr}(\boldsymbol{Z}_i^{(t-1)})\Big) = 0,\ \forall i \in \mathcal{U}.
\end{aligned}$$

Since the gradient of the first-order Taylor approximations $\widetilde{F}_i^3(\boldsymbol{W}_i, \boldsymbol{Z}_i)$ and $\widetilde{F}_i^4(\boldsymbol{W}_i, \boldsymbol{Z}_i)$ are the same as $F_i^3(\boldsymbol{W}_i, \boldsymbol{Z}_i)$ and $F_i^4(\boldsymbol{W}_i, \boldsymbol{Z}_i)$, we can also verify that

$$\begin{aligned}
&\triangledown L'(\bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}, \boldsymbol{\sigma})|_{\bar{\boldsymbol{W}}=\bar{\boldsymbol{W}}^{(t-1)}} = \triangledown L(\bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}, \boldsymbol{\sigma})|_{\bar{\boldsymbol{W}}=\bar{\boldsymbol{W}}^{(t-1)}}, \\
&\triangledown L'(\bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}, \boldsymbol{\sigma})|_{\bar{\boldsymbol{Z}}=\bar{\boldsymbol{Z}}^{(t-1)}} = \triangledown L(\bar{\boldsymbol{W}}, \bar{\boldsymbol{Z}}, \boldsymbol{\sigma})|_{\bar{\boldsymbol{Z}}=\bar{\boldsymbol{Z}}^{(t-1)}}.
\end{aligned}$$

which implies that $(\bar{\boldsymbol{W}}^{(t-1)}, \bar{\boldsymbol{Z}}^{(t-1)})$ 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 $(\bar{\boldsymbol{W}}^*, \bar{\boldsymbol{Z}}^*)$. This completes the proof. □

3.2 Subproblem for Phase Shift

For given beamforming matrix $\bar{\boldsymbol{\omega}}$, AN matrix $\bar{z}$ and surface selection matrix $\bar{\boldsymbol{\alpha}}$, we can rewrite *Problem 1* as

6. KKT condition is the first derivative test for a solution to a nonlinear programming problem to be optimal, provided that some regularity conditions are satisfied [39].

$$\textbf{Problem 3a}: \quad \max_{\bar{\boldsymbol{\Theta}}} \ \min_{i} \quad [R_i^u - R_i^e]^+ \tag{22}$$

$$s.t. \quad 0 \le \theta_{k,n} \le 2\pi, \ k \in [1, K], \forall n \in [1, N]. \tag{C2}$$

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 $\boldsymbol{\mathcal{G}}_{i,k} = \alpha_{i,k}\mathrm{diag}(\boldsymbol{g}_{i,k}^H)\boldsymbol{G}_k^H \in \mathbb{C}^{N\times M}$,[7] $\hat{\boldsymbol{\mathcal{G}}}_{i,j,k} = \alpha_{j,k}\mathrm{diag}(\boldsymbol{g}_{i,k}^H)\boldsymbol{G}_k^H \in \mathbb{C}^{N\times M}$. Let $\boldsymbol{\kappa}_{i,k} = \boldsymbol{\mathcal{G}}_{i,k}\boldsymbol{\omega}_i \in \mathbb{C}^{N\times 1}$, $\hat{\boldsymbol{\kappa}}_{i,j,k} = \hat{\boldsymbol{\mathcal{G}}}_{i,j,k}\boldsymbol{\omega}_j \in \mathbb{C}^{N\times 1}$, $\boldsymbol{\mu}_k = [\mu_{k,1}, \mu_{k,2}, \ldots, \mu_{k,N}] \in \mathbb{C}^{1\times N}$ and $\mu_{k,n} = e^{j\theta_{k,n}}$. Then, the power of received signal at the ith user in (4) becomes

$$\left| \sum_{k=1}^{K}\Big(\alpha_{i,k}\boldsymbol{g}_{i,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H\boldsymbol{\omega}_i + \boldsymbol{h}_i^H\Big)\boldsymbol{\omega}_i\right|^2 = \left|\sum_{k=1}^{K}\boldsymbol{\mu}_k\boldsymbol{\kappa}_{i,k} + \boldsymbol{h}_i^H\boldsymbol{\omega}_i\right|^2.$$

Accordingly, the power of the received signal of the ith user at the eavesdropper in (5) becomes

$$\left| \sum_{k=1}^{K}\Big(\alpha_{i,k}\boldsymbol{g}_{e,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_i^H\Big)\boldsymbol{\omega}_i\right|^2 = \left|\sum_{k=1}^{K}\boldsymbol{\mu}_k\boldsymbol{\kappa}_{e,k} + \boldsymbol{h}_e^H\boldsymbol{\omega}_i\right|^2.$$

Furthermore, let $\boldsymbol{v} = [\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_K] \in \mathbb{C}^{1\times NK}$, and $\boldsymbol{a}_i = [\boldsymbol{\kappa}_{i,1}; \boldsymbol{\kappa}_{i,2}; \ldots; \boldsymbol{\kappa}_{i,K}] \in \mathbb{C}^{NK\times 1}$, $\hat{\boldsymbol{a}}_{i,j} = [\hat{\boldsymbol{\kappa}}_{i,j,1}; \hat{\boldsymbol{\kappa}}_{i,j,2}; \ldots; \hat{\boldsymbol{\kappa}}_{i,j,K}] \in \mathbb{C}^{NK\times 1}$. Thus, we have $\sum_{k=1}^{K}\boldsymbol{\mu}_k^H\boldsymbol{\kappa}_{i,k} = \boldsymbol{v}\boldsymbol{a}_i$. Let $b_i = \boldsymbol{h}_i^H\boldsymbol{\omega}_i$, $\hat{b}_{i,j} = \boldsymbol{h}_i^H\boldsymbol{\omega}_j$, $\boldsymbol{\mathcal{G}}_{i,k}^e = \alpha_{i,k}\mathrm{diag}(\boldsymbol{g}_{e,k}^H)\boldsymbol{G}_k$, $b_i^e = \boldsymbol{h}_e^H\boldsymbol{\omega}_i$. Also, let $\hat{\boldsymbol{\kappa}}_{i,j,k}^{noise} = \hat{\boldsymbol{\mathcal{G}}}_{i,j,k}\boldsymbol{z}_i \in \mathbb{C}^{N\times 1}$, $\boldsymbol{a}_{i,j}^{noise} = [\boldsymbol{\kappa}_{i,j,1}^{noise}; \boldsymbol{\kappa}_{i,j,2}^{noise}; \ldots; \boldsymbol{\kappa}_{i,j,K}^{noise}] \in \mathbb{C}^{NK\times 1}$, $c_{i,j} = \boldsymbol{h}_i^H\boldsymbol{z}_j$. Then, the achievable secrecy rate in (7) can be reformulated as

$$\begin{aligned} R_i^u - R_i^e = &\log_2\left(1 + \frac{|\boldsymbol{v}\boldsymbol{a}_i + b_i|^2}{\sum_{j\ne i}|\boldsymbol{v}\hat{\boldsymbol{a}}_{i,j} + \hat{b}_{i,j}|^2 + \sum_{j\in\mathcal{U}}|\boldsymbol{v}\boldsymbol{a}_{i,j}^{noise} + c_{i,j}|^2 + N_0}\right) \\ &- \log_2\left(1 + \frac{|\boldsymbol{v}\boldsymbol{a}_i^e + b_i^e|^2}{\sum_{j\ne i}|\boldsymbol{v}\boldsymbol{a}_{e,j} + \hat{b}_{e,j}|^2 + \sum_{j\in\mathcal{U}}|\boldsymbol{v}\boldsymbol{a}_{e,j}^{noise} + c_{e,j}|^2 + N_0}\right). \end{aligned} \tag{23}$$

Note that $|\boldsymbol{v}\boldsymbol{a}_i + b_i|^2 = \widetilde{\boldsymbol{v}}^H\boldsymbol{R}_i\widetilde{\boldsymbol{v}}$, and $\widetilde{\boldsymbol{v}}^H\boldsymbol{R}_i\widetilde{\boldsymbol{v}} = \mathrm{Tr}(\boldsymbol{R}_i\widetilde{\boldsymbol{v}}\widetilde{\boldsymbol{v}}^H)$. Define $\boldsymbol{V} = \widetilde{\boldsymbol{v}}\widetilde{\boldsymbol{v}}^H$, which needs to satisfy $\boldsymbol{V} \succeq \boldsymbol{0}$ and $\mathrm{Rank}(\boldsymbol{V}) = 1$. Note that $\boldsymbol{R}_i = [\boldsymbol{a}_i\boldsymbol{a}_i^H, \boldsymbol{a}_ib_i^H; b_i\boldsymbol{a}_i^H, 0] \in \mathbb{C}^{NK+1\times NK+1}$, $\hat{\boldsymbol{R}}_{i,j} = [\hat{\boldsymbol{a}}_{i,j}\hat{\boldsymbol{a}}_{i,j}^H, \hat{\boldsymbol{a}}_{i,j}\hat{b}_{i,j}^H; \hat{b}_{i,j}\hat{\boldsymbol{a}}_{i,j}^H, 0] \in \mathbb{C}^{NK+1\times NK+1}$, $\boldsymbol{R}_{i,j}^{noise} = [\boldsymbol{a}_{i,j}^{noise}\boldsymbol{a}_{i,j}^{noiseH}, \boldsymbol{a}_{i,j}^{noise}c_{i,j}^H; c_{i,j}\boldsymbol{a}_{i,j}^{noiseH}, 0] \in \mathbb{C}^{NK+1\times NK+1}$, $\widetilde{\boldsymbol{v}} = [\boldsymbol{v}, \boldsymbol{1}]^H \in \mathbb{C}^{NK+1\times 1}$. Then (23) can be further reformulated as

$$R_i^u - R_i^e = F_i^1 + F_i^2 - F_i^3 - F_i^4, \tag{24}$$

where F_i^1, F_i^2, F_i^3 and F_i^4 are

$$\begin{aligned} F_i^1 = \log_2\Bigg(&\mathrm{Tr}(\boldsymbol{R}_i\boldsymbol{V}) + |b_i|^2 + \sum_{j\ne i}(Tr(\hat{\boldsymbol{R}}_{i,j}\boldsymbol{V}) + |\hat{b}_{i,j}|^2) \\ &+ \sum_{j\in\mathcal{U}}(\mathrm{Tr}(\boldsymbol{R}_{i,j}^{noise}\boldsymbol{V}) + |c_{i,j}|^2) + N_0\Bigg), \end{aligned} \tag{25}$$

$$\begin{aligned} F_i^2 = \log_2\Bigg(&\sum_{j\ne i}(\mathrm{Tr}(\hat{\boldsymbol{R}}_{e,j}\boldsymbol{V}) + |\hat{b}_{e,j}|^2) \\ &+ \sum_{j\in\mathcal{U}}(\mathrm{Tr}(\boldsymbol{R}_{e,j}^{noise}\boldsymbol{V}) + |c_{e,j}|^2) + N_0\Bigg), \end{aligned} \tag{26}$$

$$\begin{aligned} F_i^3 = \log_2\Bigg(&\sum_{j\ne i}(\mathrm{Tr}(\hat{\boldsymbol{R}}_{i,j}\boldsymbol{V}) + |\hat{b}_{i,j}|^2) \\ &+ \sum_{j\in\mathcal{U}}(\mathrm{Tr}(\boldsymbol{R}_{i,j}^{noise}\boldsymbol{V}) + |c_{i,j}|^2) + N_0\Bigg), \end{aligned} \tag{27}$$

$$\begin{aligned} F_i^4 = \log_2\Bigg(&\mathrm{Tr}(\boldsymbol{R}_e\boldsymbol{V}) + |b_i^e|^2 + \sum_{j\ne i}(\mathrm{Tr}(\hat{\boldsymbol{R}}_{e,j}\boldsymbol{V}) + |\hat{b}_{e,j}|^2) \\ &+ \sum_{j\in\mathcal{U}}(\mathrm{Tr}(\boldsymbol{R}_{e,j}^{noise}\boldsymbol{V}) + |c_{e,j}|^2) + N_0\Bigg). \end{aligned} \tag{28}$$

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

$$\begin{aligned} F_i^3(\boldsymbol{V}) &\le F_i^3(\boldsymbol{V}^{(t)}) + \mathrm{Tr}\Big(\triangledown_{\boldsymbol{V}}F_i^3(\boldsymbol{V}^{(t)})^H(\boldsymbol{V} - \boldsymbol{V}^{(t)})\Big) \\ &= \widetilde{F}_i^3(\boldsymbol{V}, \boldsymbol{V}^{(t)}), \end{aligned} \tag{29}$$

$$\begin{aligned} F_i^4(\boldsymbol{V}) &\le F_i^4(\boldsymbol{V}^{(t)}) + \mathrm{Tr}\Big(\triangledown_{\boldsymbol{V}}F_i^4(\boldsymbol{V}^{(t)})^H(\boldsymbol{V} - \boldsymbol{V}^{(t)})\Big) \\ &= \widetilde{F}_i^4(\boldsymbol{V}, \boldsymbol{V}^{(t)}). \end{aligned} \tag{30}$$

Thus, *Problem 3a* is transformed into a convex problem by introducing auxiliary variable x

$$\textbf{Problem 3b}: \quad \max_{x,\boldsymbol{V}} \quad x \tag{31}$$

$$s.t. \quad 0 \le \theta_{k,n} \le 2\pi, \ k \in [1, K], \forall n \in [1, N], \tag{C2}$$

$$0 \le x \le F_i^1 + F_i^2 - \widetilde{F}_i^3 - \widetilde{F}_i^4, \forall i \in \mathcal{U}, \tag{C7}$$

$$\boldsymbol{V} \succeq \boldsymbol{0}. \tag{C8}$$

To restore the desired solution $\boldsymbol{\Theta} = \mathrm{diag}(\boldsymbol{v})$ from the convex Semi-Definite Programming (SDP) solution $\boldsymbol{V}$, 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]

$$\mu_{k,n} = e^{j\angle\left(\frac{v'_n}{v'_{NK+1}}\right)}, n = 1, 2, \ldots, NK, \tag{32}$$

where $\boldsymbol{v}' = \{v'_1, v'_2, \ldots, v'_{NK+1}\}$ denotes the solution after eigenvalue decomposition from obtained solution $\boldsymbol{V}$, $\angle(x)$

7. This is due to $\boldsymbol{A}\cdot\mathrm{diag}(e^{j\theta_1}, e^{j\theta_2}, \ldots, e^{j\theta_N}) = [e^{j\theta_1}, e^{j\theta_2}, \ldots, e^{j\theta_N}]\cdot\mathrm{diag}(\boldsymbol{A})$ when matrix $\boldsymbol{A} \in \mathbb{C}^{1\times N}$ and $\mathrm{diag}(e^{j\theta_1}, e^{j\theta_2}, \ldots, e^{j\theta_N}) \in \mathbb{C}^{N\times N}$. Thus, transmitter-IRS-user channel gives $\boldsymbol{g}_{i,k}^H\boldsymbol{\Theta}_k\boldsymbol{G}_k^H = \boldsymbol{\mu}_k\mathrm{diag}(\boldsymbol{g}_{i,k}^H)\boldsymbol{G}_k^H$.

denotes the phase of x and the obtained solution can satisfy $|\mu_{k,n}| = 1$.

3.3 Subproblem for Surface Selection

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

$$\textbf{Problem 4a}: \quad \max_{\bar{\boldsymbol{\alpha}}} \ \min_{i} \quad [R_i^u - R_i^e]^+ \tag{33}$$

$$s.t. \quad \sum_k \alpha_{i,k} = 1, \ \alpha_{i,k} \in \{0,1\}, \ \forall i \in \mathcal{U}. \tag{C3}$$

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 ith user becomes

$$\begin{aligned}
&\left|\left(\sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{i,k}^H\mathbf{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_i^H\right)\boldsymbol{\omega}_i\right|^2 \\
&= \underbrace{\sum_{k=1}^{K}\sum_{k' \neq K}\alpha_{i,k}\alpha_{i,k'}(T_{i,k}\boldsymbol{\omega}_i)^H T_{i,k}\boldsymbol{\omega}_i}_{k^2} + (\boldsymbol{h}_i^H\boldsymbol{\omega}_i)^H\boldsymbol{h}_i^H\boldsymbol{\omega}_i \\
&\quad + \sum_{k=1}^{K}\alpha_{i,k}(T_{i,k}\boldsymbol{\omega}_i)^H\boldsymbol{h}_i^H\boldsymbol{\omega}_i + \sum_{k=1}^{K}\alpha_{i,k}T_{i,k}\boldsymbol{\omega}_i(\boldsymbol{h}_i^H\boldsymbol{\omega}_i)^H \\
&= \underbrace{\sum_{k=1}^{K}\alpha_{i,k}(T_{i,k}\boldsymbol{\omega}_i)^H T_{i,k}\boldsymbol{\omega}_i}_{k} + (\boldsymbol{h}_i^H\boldsymbol{\omega}_i)^H\boldsymbol{h}_i^H\boldsymbol{\omega}_i \\
&\quad + \sum_{k=1}^{K}\alpha_{i,k}(T_{i,k}\boldsymbol{\omega}_i)^H\boldsymbol{h}_i^H\boldsymbol{\omega}_i + \sum_{k=1}^{K}\alpha_{i,k}T_{i,k}\boldsymbol{\omega}_i(\boldsymbol{h}_i^H\boldsymbol{\omega}_i)^H \\
&= \sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{i,i,k}^1 + \hat{T}_{i,i,k}^2) + |b_i|^2,
\end{aligned} \tag{34}$$

where $T_{i,k} = \boldsymbol{g}_{i,k}^H\mathbf{\Theta}_k\boldsymbol{G}_k^H$, $T_{e,k} = \boldsymbol{g}_{e,k}^H\mathbf{\Theta}_k\boldsymbol{G}_k^H$, $\hat{T}_{i,j,k}^1 = (T_{i,k}\boldsymbol{\omega}_j)^H T_{i,k}\boldsymbol{\omega}_j$, $\hat{T}_{i,j,k}^2 = (T_{i,k}\boldsymbol{\omega}_j)^H\boldsymbol{h}_i^H\boldsymbol{\omega}_j + T_{i,k}\boldsymbol{\omega}_j(\boldsymbol{h}_i^H\boldsymbol{\omega}_j)^H$. Similarly, the power of the received signal for the ith user at eavesdropper in (5) can be expressed as

$$\begin{aligned}
&\left|\left(\sum_{k=1}^{K}\alpha_{i,k}\boldsymbol{g}_{e,k}^H\mathbf{\Theta}_k\boldsymbol{G}_k^H + \boldsymbol{h}_e^H\right)\boldsymbol{\omega}_i\right|^2 \\
&\quad = \sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{e,i,k}^1 + \hat{T}_{e,i,k}^2) + |b_i^e|^2.
\end{aligned} \tag{35}$$

Furthermore, let $T\hat{N}_{i,j,k}^1 = (T_{i,k}z_j)^H T_{i,k}z_j$, $T\hat{N}_{i,j,k}^2 = (T_{i,k}z_j)^H\boldsymbol{h}_i^H z_j + T_{i,k}z_j(\boldsymbol{h}_i^H z_j)^H$. In this case, the achievable secrecy rate in (7) can be reformulated as

$$R_i^u - R_i^e = F_i^1 + F_i^2 - F_i^3 - F_i^4,$$

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

$$\begin{aligned}
F_i^1 = \log_2\Bigg(&\sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{i,i,k}^1 + \hat{T}_{i,i,k}^2) + |b_i|^2 + \sum_{j \neq i}\sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{i,j,k}^1 + \hat{T}_{i,j,k}^2) \\
&+ |\hat{b}_{i,j}|^2 + \sum_{j \in \mathcal{U}}\sum_{k=1}^{K}\alpha_{i,k}(T\hat{N}_{i,j,k}^1 + T\hat{N}_{i,j,k}^2) + |c_{i,j}|^2 + N_0\Bigg),
\end{aligned} \tag{36}$$

$$\begin{aligned}
F_i^2 = \log_2\Bigg(&\sum_{j \neq i}\sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{e,j,k}^1 + \hat{T}_{e,j,k}^2) + |\hat{b}_{e,j}|^2 \\
&+ \sum_{j \in \mathcal{U}}\sum_{k=1}^{K}\alpha_{i,k}(T\hat{N}_{e,j,k}^1 + T\hat{N}_{e,j,k}^2) + |c_{e,j}|^2 + N_0\Bigg),
\end{aligned} \tag{37}$$

$$\begin{aligned}
F_i^3 = \log_2\Bigg(&\sum_{j \neq i}\sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{i,j,k}^1 + \hat{T}_{i,j,k}^2) + |\hat{b}_{i,j}|^2 \\
&+ \sum_{j \in \mathcal{U}}\sum_{k=1}^{K}\alpha_{i,k}(T\hat{N}_{i,j,k}^1 + T\hat{N}_{i,j,k}^2) + |c_{i,j}|^2 + N_0\Bigg),
\end{aligned} \tag{38}$$

$$\begin{aligned}
F_i^4 = \log_2\Bigg(&\sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{e,i,k}^1 + \hat{T}_{e,i,k}^2) + |b_i|^2 \\
&+ \sum_{j \neq i}\sum_{k=1}^{K}\alpha_{i,k}(\hat{T}_{e,j,k}^1 + \hat{T}_{e,j,k}^2) + |\hat{b}_{e,j}|^2 \\
&+ \sum_{j \in \mathcal{U}}\sum_{k=1}^{K}\alpha_{i,k}(T\hat{N}_{e,j,k}^1 + T\hat{N}_{e,j,k}^2) + |c_{e,j}|^2 + N_0\Bigg).
\end{aligned} \tag{39}$$

In order to solve this subproblem, we first relax integer variable $\bar{\boldsymbol{\alpha}}$, then we solve the problem by using convex optimization. After rounding the relaxed solution, we can get feasible $\bar{\boldsymbol{\alpha}}$ for *Problem 4a*. Similarly, we adopt the SCA method to construct global upper bounds of F_i^3 and F_i^4

$$\begin{aligned}
F_i^3(\bar{\boldsymbol{\alpha}}_i) &\leq F_i^3(\bar{\boldsymbol{\alpha}}_i) + \mathrm{Tr}\Big(\bigtriangledown_{\bar{\boldsymbol{\alpha}}_i}F_i^3(\bar{\boldsymbol{\alpha}}_i^{(t)})^H(\bar{\boldsymbol{\alpha}}_i - \bar{\boldsymbol{\alpha}}_i^{(t)})\Big) \\
&= \widetilde{F}_i^3(\bar{\boldsymbol{\alpha}}_i, \bar{\boldsymbol{\alpha}}_i^{(t)}),
\end{aligned} \tag{40}$$

$$\begin{aligned}
F_i^4(\bar{\boldsymbol{\alpha}}_i) &\leq F_i^4(\bar{\boldsymbol{\alpha}}_i) + \mathrm{Tr}\Big(\bigtriangledown_{\bar{\boldsymbol{\alpha}}_i}F_i^4(\bar{\boldsymbol{\alpha}}_i^{(t)})^H(\bar{\boldsymbol{\alpha}}_i - \bar{\boldsymbol{\alpha}}_i^{(t)})\Big) \\
&= \widetilde{F}_i^4(\bar{\boldsymbol{\alpha}}_i, \bar{\boldsymbol{\alpha}}_i^{(t)}),
\end{aligned} \tag{41}$$

where $\bar{\boldsymbol{\alpha}}_i = [\boldsymbol{\alpha}_{i,1}, \ldots, \boldsymbol{\alpha}_{i,K}]$. Thus, *Problem 4a* can be transformed into a convex problem by introducing auxiliary variable x

$$\textbf{Problem 4b}: \quad \max_{x, \bar{\boldsymbol{\alpha}}} \quad x \tag{42}$$

$$s.t. \quad 0 \leq x \leq F_i^1 + F_i^2 - \widetilde{F}_i^3 - \widetilde{F}_i^4, \forall i \in \mathcal{U}, \tag{C9}$$

$$\sum_k \alpha_{i,k} = 1, \ \alpha_{i,k} \in [0,1], \ \forall i \in \mathcal{U}. \tag{C10}$$

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

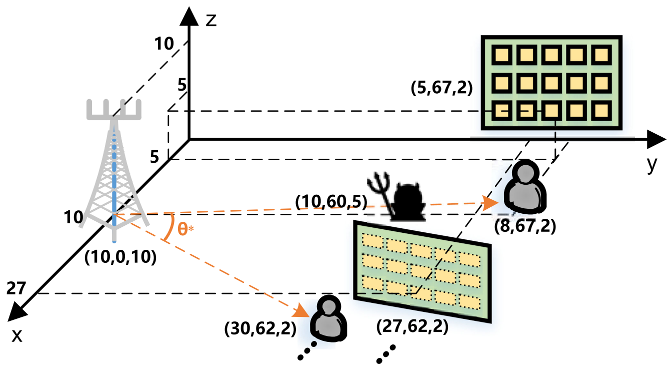


Fig. 2. The illustration of our evaluation setups, the users and IRSs are located on a circle with the center being the base station.

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),[8] IRSs and legitimate users are uniformly distributed around base station with a constant angle θ^*. The first user and IRS 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 $\boldsymbol{h} = \sqrt{L_0 d_{ab}^{-\beta}}\boldsymbol{h}^*$, where L_0 denotes the reference path loss at 1 meter, β denotes the path loss exponent, d_{ab} denotes the distance from location a to location b, and $\boldsymbol{h}^*$ is the small-scale fading component with Rician fading [40], [41], [42]

$$\boldsymbol{h}^* = \sqrt{\frac{K'}{K'+1}}\boldsymbol{h}^*_{LoS} + \sqrt{\frac{1}{K'+1}}\boldsymbol{h}^*_{NLoS}, \tag{43}$$

where K' represents the Rician factor, $\boldsymbol{h}^*_{LoS}$ and $\boldsymbol{h}^*_{NLoS}$ 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 $\boldsymbol{h}^*_{LoS} = \boldsymbol{a}_m(\theta)\boldsymbol{a}_n(\theta)^H$. The array response of an N-elements IRS can be calculated by

$$\boldsymbol{a}_m = \exp\left(j\frac{2\pi}{\lambda}d_t(m-1)\sin\phi_{LoS_1}\sin\theta_{LoS_1}\right), m = 1,\ldots,M,$$

$$\boldsymbol{a}_n = \exp\left(j\frac{2\pi}{\lambda}d_r(m-1)\sin\phi_{LoS_2}\sin\theta_{LoS_2}\right), n = 1,\ldots,N,$$

where d_t and d_r are the inter-antenna separation distance at the transmitter and receiver, ϕ_{LoS_1} and ϕ_{LoS_2} are the LoS azimuth at the base station and the IRS, and θ_{LoS_1} and θ_{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. [9] 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:

TABLE 1
Evaluation Parameters

Parameter	Value
Carrier frequency	800MHz
IRS configuration	Uniform rectangular array with 5 elements in a row and $N/5$ columns with $3\lambda/8$ spacing
Path loss exponent	$\beta_{BU} = \beta_{BE} = 4$, $\beta_{BI} = \beta_{IU} = \beta_{IE} = 2$, respectively
Rician channel factor	$K'_{BU} = K'_{BE} = 0$, $K'_{BI} = K'_{IU} = K'_{IE} = \infty$, respectively
Path loss at 1 meter	$L_0 = -30dB$
Other parameters	$N_0 = -174$dBm, Tx $= 4$, $\delta = 10^{-3}$, $\theta^* = 20°$

- *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 perform better than AN-disabled scheme by up to 18.9%. Here, for a fair comparison, we also set $\beta_{BU} = \beta_{BE} = 2$ 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,

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., $L_0(d_0) = 20\log_{10}(\frac{4\pi d_0}{\lambda})$, where d_0 denotes the reference distance and λ denotes the wave length [43].

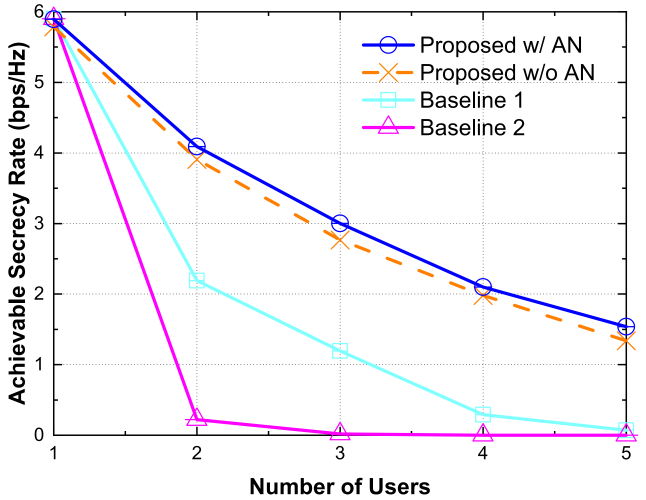


Fig. 3. The achievable secrecy rate versus the number of users ($P_{max} = 40dBm$, $N = 20$).

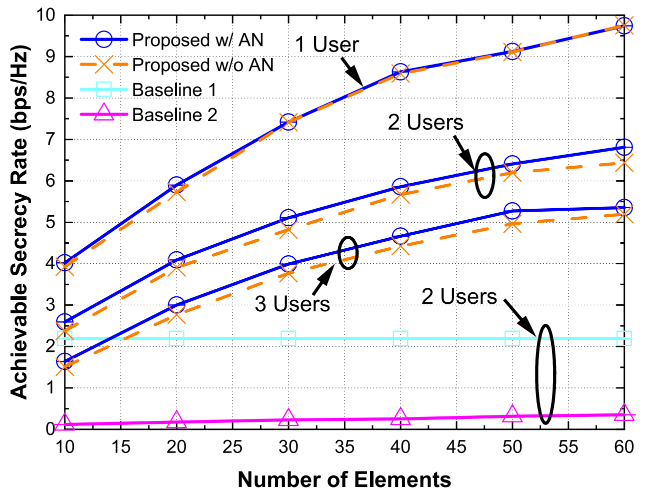


Fig. 4. The achievable secrecy rate versus the number of elements ($P_{max} = 40dBm$).

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 shows the influence of different number of reflecting elements N on each IRS. Due to the existence of obstacles, the LoS component is relatively poor for wireless transmissions between the base station and the user. When only one user is considered, the proposed scheme with AN has almost the same performance as the one without AN, which is is also verified in [14]. When there are 2 or more users, additional AN can help improve secrecy rate about 4-6% especially with the increase in N. Without the assistance of IRSs and AN, baseline 1 has the worst performance

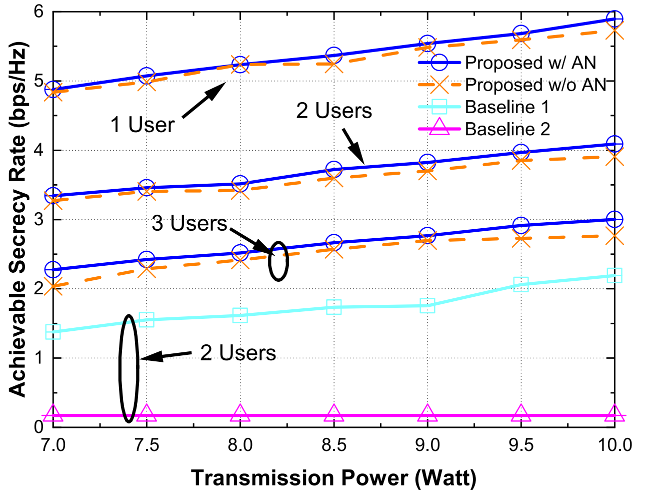


Fig. 5. The achievable secrecy rate versus maximum transmission power ($N = 30$).

compared with other schemes since the direct channel between the base station and the user is blocked (nearly zero when $\beta_{BU} = \beta_{BE} = 4$). For fair comparison, we further change $\beta_{BU} = \beta_{BE} = 2$ for the beamforming scheme. Since the eavesdropper, located in between the base station and the first user, can easily intercept the signals, the result in Fig. 4 also shows that the performance of beamforming scheme is relatively poor. For baseline 2, since users are distributed further apart from each other, the environmental diversity provided by the single IRS cannot meet the requirement for secure communications.

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.

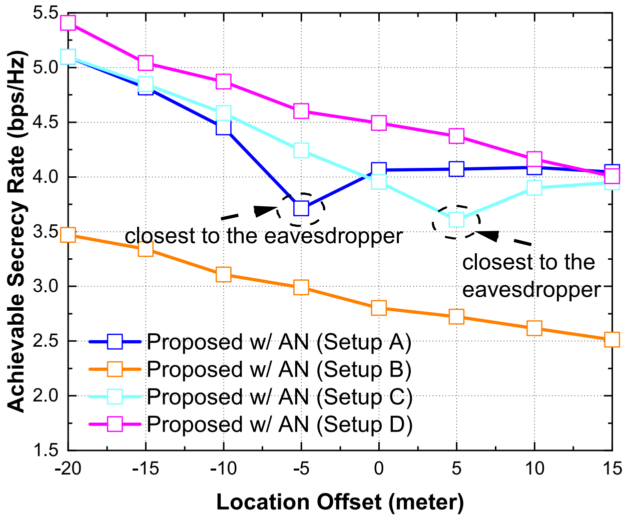


Fig. 6. The achievable secrecy rate versus position setting ($P_{max} = 40dBm$, $N = 20$, $User = 2$).

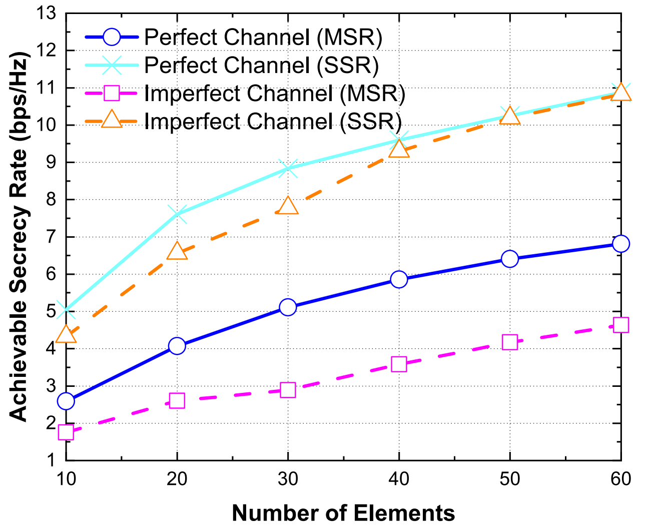


Fig. 7. The achievable secrecy rate with imperfect CSI model ($P_{max} = 40dBm$, $User = 2$).

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 IRS 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.

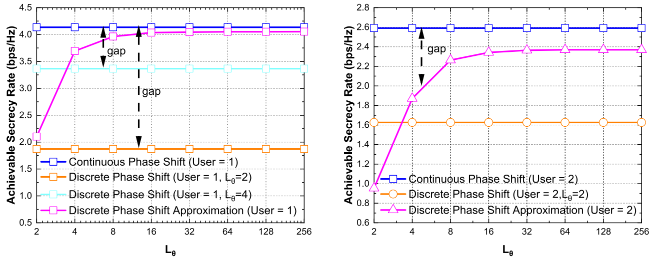
4.3 Performance With Imperfect CSI and Discrete Adjustment

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 $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{C})$ represent Circularly Symmetric Complex Gaussian (CSCG) random vector with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{C}$. 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 $\boldsymbol{g}_{e,k}^H$ and $\boldsymbol{G}_k^H$ considered in our previous system model can be respectively characterized as

$$\boldsymbol{g}_{e,k}^H = \overline{\boldsymbol{g}_{e,k}^H} + \Delta \boldsymbol{g}_{e,k}^H, \tag{44}$$

$$\boldsymbol{h}_e^H = \overline{\boldsymbol{h}_e^H} + \Delta \boldsymbol{h}_e^H, \tag{45}$$

where $\overline{\boldsymbol{g}_{e,k}^H}$ and $\boldsymbol{h}_e^H$ denote the mean of the channel gain, and $\Delta \boldsymbol{g}_{e,k}^H$ and $\Delta \boldsymbol{h}_e^H$ capture the uncertainty (i.e., CSI error vectors) in the channel. The CSI error vectors $\Delta \boldsymbol{g}_{e,k}^H$ and $\Delta \boldsymbol{h}_e^H$ are



(a) $User = 1$ (b) $User = 2$

Fig. 8. The achievable secrecy rate with discrete phase shift ($P_{max} = 40dBm, N = 10$).

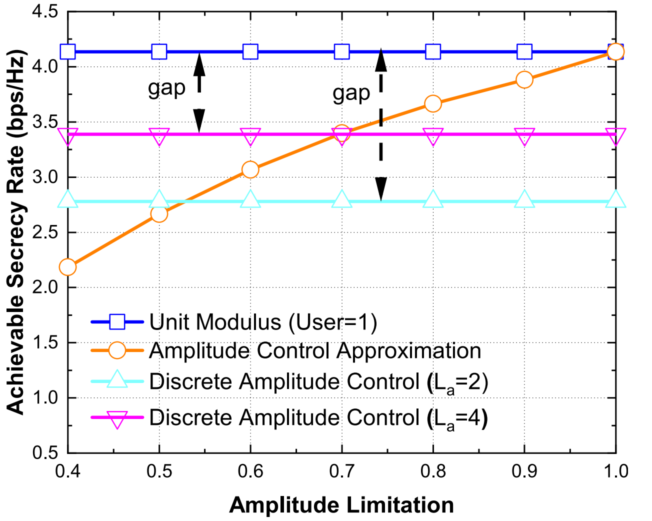


Fig. 9. The achievable secrecy rate with discrete amplitude control ($P_{max} = 40dBm, N = 10, User = 1$).

assumed to follow the CSCG distribution. Here, the parameter setting of CSCG distribution is similar to [44], [45], $\boldsymbol{\mu} = \mathbf{0}$ is adopted, and the variance matrix of $\text{vec}(\Delta \boldsymbol{g}_{e,k}^H)$ and $\text{vec}(\Delta \boldsymbol{h}_e^H)$ is defined as $\mathbf{C} = \varepsilon_{e,k}^2 \mathbf{I}$, where $\varepsilon_{e,k}^2 = \delta_{e,k} \|\text{vec}(\Delta \boldsymbol{g}_{e,k}^H)\|$ and $\varepsilon_e^2 = \delta_e \|\text{vec}(\Delta \boldsymbol{h}_e^H)\|$, and $\delta_{e,k} \in [0,1)$ 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 kth IRS we considered in Section 2 can be further modeled as

$$\boldsymbol{\Theta}_k = \text{diag}(A_{k,1} e^{j\theta_{k,1}}, \ldots, A_{k,N} e^{j\theta_{k,N}}) \in \mathbb{C}^{N \times N}, \tag{46}$$

where $\theta_{k,n} \in \{0, \frac{2\pi}{L}, \ldots, \frac{2\pi(L-1)}{L}\}$ with $L_\theta = 2^{q_\theta}$, i.e., the discrete phase-shift values are assumed to be equally spaced in the interval $[0, 2\pi)$, and $A_{k,n} \in \{a_1, \ldots, a_{L_a}\}$ denotes the controllable amplitude set which satisfies $L_a = 2^{q_a}$. When $q_a = 0$, 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 $q_a = 1$, 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_θ 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 $\boldsymbol{\Theta}_k$ obtained from the proposed algorithm, the modulus coefficient for amplitude control scheme in the figure will be applied to all $A_{k,n}$ in $\boldsymbol{\Theta}_k$. 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

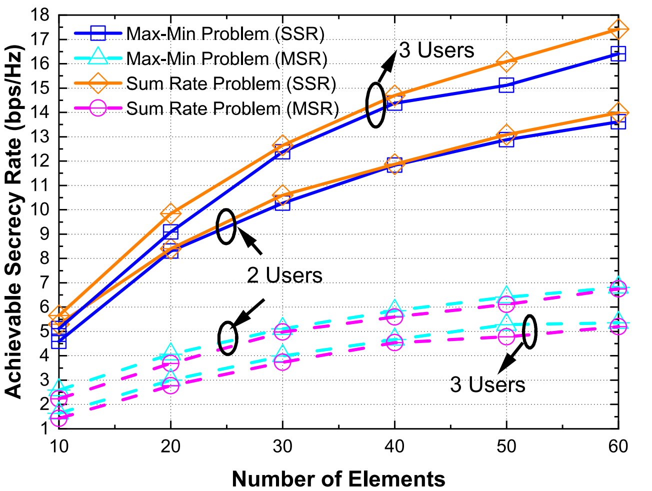


Fig. 10. Max-min problem versus sum-rate problem in terms of the number of elements ($P_{max} = 40dBm$).

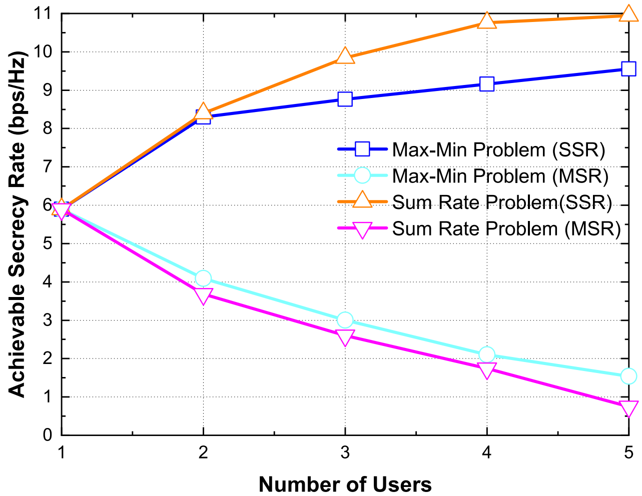


Fig. 11. Max-min problem versus sum-rate problem in terms of the number of users ($P_{max} = 40dBm, N = 20$).

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 (C3) can be reformulated as

$$\begin{aligned} &\max_{\bar{\boldsymbol{\omega}},\bar{z},\bar{\boldsymbol{\Theta}},\bar{\boldsymbol{\alpha}}} \sum_i [R_i^u - R_i^e]^+ \\ &s.t. \quad (C1) - (C3). \end{aligned} \tag{47}$$

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 the 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

[1] M. Chraiti, A. Ghrayeb, and C. Assi, "Achieving full secure degrees-of-freedom for the MISO wiretap channel with an unknown eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7066–7079, Nov. 2017.

[2] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[3] X. He and A. Yener, "MIMO wiretap channels with unknown and varying eavesdropper channel states," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6844–6869, Nov. 2014.

[4] H.-M. Wang, X. Zhang, Q. Yang, and T. A. Tsiftsis, "Secure users oriented downlink MISO NOMA," *IEEE J. Sel. Top. Signal Process.*, vol. 13, no. 3, pp. 671–684, Jun. 2019.

[5] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[6] W. Wang *et al.*, "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, Aug. 2020.

[7] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan./Feb. 2015.

[8] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[9] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information-and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[10] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[11] M. Di Renzo *et al.*, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

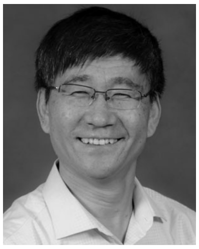
[12] M. Di Renzo *et al.*, "Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, 2019.

[13] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.
[14] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.
[15] D. Zhao, H. Lu, Y. Wang, H. Sun, and Y. Gui, "Joint power allocation and user association optimization for IRS-assisted mmWave systems," *IEEE Trans. Wireless Commun.*, early access, Jul. 27, 2021, doi: 10.1109/TWC.2021.3098447.
[16] L. Zhang, L. Yan, B. Lin, H. Ding, Y. Fang, and X. Fang, "Augmenting transmission environments for better communications: Tunable reflector assisted mmWave WLANs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7416–7428, Jul. 2020.
[17] L. Zhang, L. Yan, B. Lin, Y. Fang, and X. Fang, "Tunable reflectors enabled environment augmentation for better mmWave WLANs," in *Proc. IEEE/CIC Int. Conf. Commun. China*, 2019, pp. 7–12.
[18] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.
[19] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 19, no. 11, pp. 7543–7556, Nov. 2020.
[20] B. Lyu, D. T. Hoang, S. Gong, D. Niyato, and D. I. Kim, "IRS-based wireless jamming attacks: When jammers can attack without power," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1663–1667, Oct. 2020.
[21] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for secure IRS-assisted multiuser MISO systems," in *Proc. IEEE Globecom Workshops.*, 2019, pp. 1–6.
[22] K. Feng, Q. Wang, X. Li, and C.-K. Wen, "Deep reinforcement learning based intelligent reflecting surface optimization for MISO communication systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 745–749, May 2020.
[23] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning based intelligent reflecting surface for secure wireless communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 375–388, Jan. 2021.
[24] X. Li, S. Liu, H. Chen, and K. Wang, "A potential information capacity index for link prediction of complex networks based on the cannikin law," *Entropy*, vol. 21, no. 9, 2019, Art. no. 863.
[25] C. Min, N. Chang, J. Cha, and J. Kang, "MIMO-OFDM downlink channel prediction for IEEE802. 16e systems using kalman filter," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2007, pp. 942–946.
[26] B. Zheng and R. Zhang, "Intelligent reflecting surface-enhanced OFDM: Channel estimation and reflection optimization," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 518–522, Apr. 2020.
[27] J. Li, K. Xue, D. S. Wei, J. Liu, and Y. Zhang, "Energy efficiency and traffic offloading optimization in integrated satellite/terrestrial radio access networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2367–2381, Apr. 2020.
[28] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
[29] Z. Luo, W. Ma, A. M. So, Y. Ye, and S. Zhang, "Semidefinite relaxation and its applications in signal processing and communications," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.
[30] W.-K. Ma, "Semidefinite relaxation and its applications in signal processing and communications," Jul. 2012. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.453.156&rep=rep1&type=pdf
[31] M. Razaviyayn, "Successive convex approximation: Analysis and applications," Ph.D. dissertation, Univ. Minnesota, Minneapolis, MN, USA, 2014.
[32] Y. Sun, D. W. K. Ng, Z. Ding, and R. Schober, "Optimal joint power and subcarrier allocation for full-duplex multicarrier non-orthogonal multiple access systems," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1077–1091, Mar. 2017.
[33] A. Alvarado, G. Scutari, and J.-S. Pang, "A new decomposition method for multiuser DC-programming and its applications," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2984–2998, Jun. 2014.
[34] M. Simchowitz, "Course notes for EE227C (spring 2018): Convex optimization and approximation," Jun. 2018. [Online]. Available: https://ee227c.github.io/notes/ee227c-notes.pdf
[35] SeDuMi Software. Accessed: Sep. 1, 2020. [Online]. Available: http://sedumi.ie.lehigh.edu/
[36] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, Mar. 2014. [Online]. Available: http://cvxr.com/cvx
[37] A. A. Nasir, D. T. Ngo, X. Zhou, R. A. Kennedy, and S. Durrani, "Joint resource optimization for multicell networks with wireless energy harvesting relays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6168–6183, Aug. 2016.
[38] T. Wang and L. Vandendorpe, "Successive convex approximation based methods for dynamic spectrum management," in *Proc. IEEE Int. Conf. Commun.*, 2012, pp. 4061–4065.
[39] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[40] H. Han, J. Zhao, D. Niyato, M. Di Renzo, and Q.-V. Pham, "Intelligent reflecting surface aided network: Power control for physical-layer broadcasting," in *Proc. IEEE Int. Conf. Commun.*, 2020, pp. 1–7.
[41] Y. Han, W. Tang, S. Jin, C.-K. Wen, and X. Ma, "Large intelligent surface-assisted wireless communication exploiting statistical CSI," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8238–8242, Aug. 2019.
[42] M.-M. Zhao, Q. Wu, M.-J. Zhao, and R. Zhang, "Exploiting amplitude control in intelligent reflecting surface aided wireless communication with imperfect CSI," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4216–4231, Jun. 2021.
[43] V. Erceg *et al.*, "An empirically based path loss model for wireless channels in suburban environments," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 7, pp. 1205–1211, Jul. 1999.
[44] 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 Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2487–2501, Apr. 2021.
[45] G. Zhou, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "A framework of robust transmission design for IRS-aided MISO communications with imperfect cascaded channels," *IEEE Trans. Signal Process.*, vol. 68, pp. 5092–5106, Aug. 2020, doi: 10.1109/TSP.2020.3019666.
[46] Y. Wang, H. Lu, and H. Sun, "Channel estimation in IRS-enhanced mmWave system with super-resolution network," *IEEE Commun. Lett.*, vol. 25, no. 8, pp. 2599–2603, Aug. 2021.
[47] M. Jung, W. Saad, M. Debbah, and C. S. Hong, "On the optimality of reconfigurable intelligent surfaces (RISs): Passive beamforming, modulation, and resource allocation," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4347–4363, Jul. 2021.
[48] S. Abeywickrama, R. Zhang, Q. Wu, and C. Yuen, "Intelligent reflecting surface: Practical phase shift model and beamforming optimization," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5849–5863, Sep. 2020.

Jian Li (Member, IEEE) received the BS degree from the Department of Electronics 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 Wireless Communications*, the *IEEE Transactions on Dependable and Secure Computing*, and the *IEEE Transactions on Network and Service Management*. He is an IET Fellow.



Yuguang Fang (Fellow, IEEE) received the MS degree from Qufu Normal University, Shandong, China, in 1987, the PhD degree from Case Western Reserve University in 1994, and the PhD degree from Boston University in 1997. In 2000, he joined the Department of Electrical and Computer Engineering, University of Florida, as an assistant professor, then was promoted to an associate professor in 2003, a full professor in 2005, and has been a distinguished professor since 2019. He holds a University of Florida Foundation Term Professorship from 2019 to 2022, a University of Florida Foundation Professorship from 2017 to 2020 and from 2006 to 2009, and a University of Florida Term Professorship from 2017 to 2019 and from 2019 to 2021. He was the editor-in-chief of the *IEEE Transactions on Vehicular Technology* from 2013 to 2017 and the *IEEE Wireless Communications* from 2009 to 2012, and is/was on several editorial boards of premier journals. He was the technical program co-chair of the IEEE INFOCOM'2014. He is a fellow of AAAS. He was the recipient of U. S. NSF Career Award in 2001, U.S. ONR Young Investigator Award in 2002, 2018 IEEE Vehicular Technology Outstanding Service Award, the 2015 IEEE Communications Society CISTC Technical Recognition Award, 2014 IEEE Communications Society WTC Recognition Award, Best Paper Award from IEEE ICNP 2006, and the 2010-2011 UF Doctoral Dissertation Advisor/Mentoring Award.

Qibin Sun (Fellow, IEEE) received the PhD degree from the Department of Electronic Engineering and Information Science (EEIS), University of Science and Technology of China (USTC), in 1997. Currently, he is a professor in the School of Cyber Science and Technology, USTC. His research interests include multimedia security, network intelligence and security and so on. He has published more than 120 papers in international journals and conferences.