Northumbria Research Link

Robust Transmission Design for Intelligent Reflecting Surface Aided Secure Communication Systems with Imperfect Cascaded CSI

Sheng Hong, Cunhua Pan, Hong Ren, Kezhi Wang, Kok Keong Chai, *Member, IEEE*, and Arumugam Nallanathan, *Fellow, IEEE*

Abstract

In this paper, we investigate the design of robust and secure transmission in intelligent reflecting surface (IRS) aided wireless communication systems. In particular, a multi-antenna access point (AP) communicates with a single-antenna legitimate receiver in the presence of multiple single-antenna eavesdroppers, where the artificial noise (AN) is transmitted to enhance the security performance. Besides, we assume that the cascaded AP-IRS-user channels are imperfect due to the channel estimation error. To minimize the transmit power, the beamforming vector at the transmitter, the AN covariance matrix, and the IRS phase shifts are jointly optimized subject to the outage rate probability constraints under the statistical cascaded channel state information (CSI) error model that usually models the channel estimation error. To handle the resulting non-convex optimization problem, we first approximate the outage rate probability constraints by using the Bernstein-type inequality. Then, we develop a suboptimal algorithm based on alternating optimization, the penalty-based and semidefinite relaxation methods. Simulation results reveal that the proposed scheme significantly reduces the transmit power compared to other benchmark schemes.

Index Terms

Intelligent reflecting surface (IRS), Reconfigurable Intelligent Surfaces (RIS), Physical layer security, Robust Design, Imperfect Cascaded CSI

S. Hong is with Information Engineering School of Nanchang University, Nanchang 330031, China. She is also with the School of Electronic Engineering and Computer Science at Queen Mary University of London, London E1 4NS, U.K. (email: shenghong@ncu.edu.cn). C. Pan, H. Ren, K. K. Chai, and A. Nallanathan are with the School of Electronic Engineering and Computer Science at Queen Mary University of London, London E1 4NS, U.K. (e-mail:{c.pan, h.ren, michael.chai, a.nallanathan}@qmul.ac.uk). K. Wang is with Department of Computer and Information Sciences, Northumbria University, UK. (email: kezhi.wang@northumbria.ac.uk).

I. INTRODUCTION

The intelligent reflecting surface (IRS) has emerged due to the advancement in metamaterial techniques, which becomes a promising technology in wireless networks [1]. The IRS, which is also named as reconfigurable intelligent surface (RIS), comprises a large number of passive elements, which can reflect the wireless signal with adjustable phase shifts [2] [3]. The IRS has the capability of reconfiguring the wireless propagation environment between access point (AP) and users in a favourable way by properly designing the phase shifts. Thus, the IRS can improve the performance of wireless networks in various aspects. Since the IRS operates in a passive mode by reflecting incident signals [4], it can significantly improve the spectral and energy efficiency of the wireless networks. Besides, it is very appealing that the IRS is low-cost, and can be deployed easily on buildings facades, interior walls, room ceilings, lamp posts and road signs, etc. Therefore, exploiting the IRS device to assist wireless communication systems has received extensive attentions. The IRS-aided wireless communication systems in the existing literature include the single-user case [5] [6], the downlink multiuser case [7] [8] [9] [10] [11], multicell scenario [12], wireless power transfer design [13], mobile edge computing [14], and cognitive radio system [15].

Recently, the IRS has emerged as a promising technology to enhance the physical layer security in a wireless communication system. There are various schemes to improve the physical layer security [16], such as the cooperative relaying [17], artificial noise (AN) [18], and cooperative jamming [19]. By using these schemes, the AP-eavesdroppers links are impaired, and the information leakage to the eavesdroppers is limited. Combining with these schemes, the IRS can further enhance the physical layer security. On one hand, deploying the IRS costs much less than deploying the relay since no active radio frequency chain is required in IRS-aided systems. On the other hand, the IRS can be programmed to configure the radio propagation environment to make the impairment on the eavesdroppers' channels more effective.

In terms of physical layer security enhancement, the IRS-aided secure communication has received considerable attention from academia [20] [21] [22] [23]. In these contributions, the active transmit beamforming and the passive reflecting beamforming of the IRS were jointly designed to improve the achievable secrecy rate. It was demonstrated that it is preferable to deploy the IRS near the legitimate receiver. The work in [21] assumed that the eavesdropper has a stronger channel than the legitimate user and both channels are highly correlated, and it showed that deploying an IRS can enhance the secrecy rate even in such a challenging scenario. Moreover, the AN is

incorporated with transmit beamforming in IRS-aided wireless secure communications [24] [25]. The phase shift matrix at the IRS as well as the beamforming vectors and AN covariance matrix at the base station (BS) were jointly optimized for maximizing the secrecy rate. It was unveiled that it is beneficial for secrecy enhancement with the aid of AN.

We note that all these existing contributions are based on the ideal assumption of perfect channel state information (CSI) of both the legitimate receiver and the eavesdropper at the transmitters. However, it is difficult to obtain the perfect CSI in IRS-aided wireless communication, because the IRS does not employ any radio frequency (RF) chains. In IRS-aided communication systems, it is challenging to estimate the IRS-related channel of the reflective AP-IRS-user link due to the passive IRS, which thus attracted a lot of research attention. The current channel estimation contributions for the IRS-related channels can be divided into two approaches. The first one is to estimate AP-IRS channel and IRS-user channel separately [26]. As shown in [26], to estimate the two separated IRS-related channels, active transmit radio RF chains are required to be installed at the IRS. The drawback of this approach is that extra hardware and power consumption is required. The second one is to estimate the cascaded AP-IRS-user channel, which is defined as the product of the AP-IRS channel and the IRS-user channel [11] [20] [22] [27]. The benefit of this approach is that the cascaded AP-IRS-user channel can be estimated without installing extra hardware and incurring power cost, and that the estimated cascaded AP-IRS-user channel is sufficient for the transmission beamforming design for the IRS-related links. Thus, more efforts are dedicated to the cascaded channel estimation [28] [29] [30] [31]. The cascaded channel estimation methods were investigated in a single-user multiple-input multiple-output (SU-MIMO) system [28] and a multi-user multiple-input single-output (MU-MISO) system [29], respectively. Then, by exploiting the channel sparsity of the mmWave channels, the compressive sensing methods were adopted to reduce the pilot overhead in [30] and [31] for single-user and multi-user systems, respectively. However, for both approaches, the channel estimation error is inevitable. Therefore, it is imperative to take the channel estimation error into consideration when designing the IRS-aided communication systems.

There are a paucity of contributions investigating the robust transmission design in IRS-aided communications. The work of [32] proposed a worst-case robust design algorithm in an MU-MISO wireless system, where the IRS-user channels were assumed to be imperfect. In addition, a worst-case robust design in IRS-assisted secure communications was investigated in [33], where the IRS-eavesdropper channels were assumed to be imperfect. Both these works only considered

the IRS-user CSI error based on the first IRS-related channel estimation approach. Since it is more practical to consider the cascaded channel uncertainty based on the second IRS-related channel estimation approach, Zhou *et. al* [34] firstly proposed a robust transmission framework with both the bounded and the statistical cascaded CSI errors in an MU-MISO wireless system.

However, to the best of our knowledge, the robust transmission design with cascaded channel error in secure IRS-aided communication systems has not been studied yet. Moreover, the probabilistic CSI error model has not been studied in secure IRS-aided communication systems. To fill this gap, this paper investigates the outage constrained robust secure transmission for IRS-aided secure wireless communication systems, where the statistical model of the cascaded channel error is considered. Specifically, we consider a scenario that a multi-antenna AP serves a single-antenna legitimate user in the presence of several single-antenna eavesdroppers. Moreover, the AN is assumed to be injected to degrade the reception quality of eavesdroppers. In this scenario, we consider an outage-constrained robust design aiming for minimizing the transmit power by considering the imperfect CSI of the eavesdroppers' channels with the outage constraints of maximum information leakage to eavesdroppers and the constraint of minimum information transmission to legitimate users. An outage-constrained power minimization (OC-PM) problem is formulated to jointly optimize the beamforming vector, the AN covariance matrix, and the phase shifts matrix of IRS while satisfying quality of service (QoS) requirements. Since the optimization variables are highly coupled, an alternating optimization (AO) method is proposed to solve it.

The main contributions of this paper can be summarized as follows:

1) To the best of our knowledge, this is the first work to study the outage constrained robust secure transmission for IRS-aided wireless communications. In contrast to [32] and [33] that only considered the bounded CSI error model in secure IRS-aided wireless communications, we first consider the statisitical CSI error model. In addition, the imperfect cascaded channels of AP-eavesdropper are investigated in secure IRS-aided communications for the first time, which is more practical compared to the existing literature considering the imperfect IRS-user channels.

2) For the outage constrained robust secure transmission design, we formulate an OC-PM problem to optimize the beamforming vector, the AN covariance matrix, and the phase shifts matrix of IRS. To solve it, we first transform the probabilistic constraints into the safe and tractable forms by exploiting Bernstein-type inequality (BTI) [35]. Then, the AO

strategy is utilized to transform the original problems into two subproblems, where the designs of beamforming vector, AN covariance matrix, and phase shifts of IRS are handled by semidefinite relaxation (SDR) based methods. For the nonconvex unit modulus constraints of IRS phase shifts, an equivalent rank-one constraint is incorporated, which is further transformed by the first-order Taylor approximation and added into the objective function as a penalty.

3) Simulation results demonstrate that the robust design of beamforming vector and AN co-variance matrix in a secure IRS-aided communication system can reduce the transmit power under the fixed secrecy rate. In comparison to various benchmark methods, the effectiveness of the proposed AO algorithm is verified. Moreover, it is revealed that by deploying the IRS and optimizing the IRS phase shifts, the reliable communication can be guaranteed for the legitimate user, while the information leakage to eavesdropper can be limited. The physical layer security can be significantly enhanced by the robust design in the secure IRS-aided wireless communications.

Notations: Throughout this paper, boldface lower case, boldface upper case and regular letters are used to denote vectors, matrices, and scalars, respectively. $\mathrm{Tr}\left(\mathbf{X}\right)$ and $|\mathbf{X}|$ denote the trace and determinant of $\mathbf{X}$, respectively. $\mathbb{C}^{M \times N}$ denotes the space of $M \times N$ complex matrices. $\mathrm{Re}\{\cdot\}$ denotes the real part of a complex value. $\mathrm{diag}(\cdot)$ is the operator for diagonalization. $\mathbf{1}_M$ presents a column vector with M ones. $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{Z})$ represents a circularly symmetric complex gaussian (CSCG) random vector with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{Z}$. $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\mathrm{H}}$ and $(\cdot)^{*}$ denote the transpose, Hermitian and conjugate operators, respectively.

II. SYSTEM MODEL

In this section, we present the transmission model and CSI error model in a secure IRS-aided communication system as follows.

A. Signal Transmission Model

An IRS-assisted communication system is considered, where an AP equipped with N_t antennas, called Alice, intends to send confidential information to a single-antenna legitimate receiver, called Bob, in the presence of K single-antenna eavesdroppers, called Eves.

As shown in Fig. 1, the signal transmitted from Alice is reflected by the IRS, which comprises M reflecting elements. The direct links of Alice-Bob and Alice-Eve are blocked by obstacles such
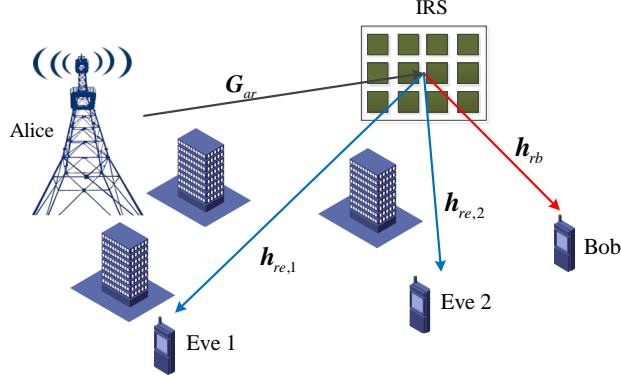
Fig. 1. An IRS-assisted secure communication system.

as buildings. The Bob and Eves can only receive the signals reflected by the IRS. The received signals at Bob and Eves are respectively modeled as

$$y_b(t) = \hat{\mathbf{h}}_b^H \mathbf{x}(t) + n_b(t) = (\mathbf{h}_{rb}^H \mathbf{\Phi} \mathbf{G}_{ar}) \mathbf{x}(t) + n_b(t), \tag{1}$$

$$\mathbf{y}_{e,k}(t) = \hat{\mathbf{h}}_{e,k}^H \mathbf{x}(t) + \mathbf{n}_{e,k}(t) = (\mathbf{h}_{re,k}^H \mathbf{\Phi} \mathbf{G}_{ar}) \mathbf{x}(t) + n_{e,k}(t), \tag{2}$$

where $\hat{\mathbf{h}}_b = \mathbf{G}_{ar}^H \mathbf{\Phi}^H \mathbf{h}_{rb}$, $\hat{\mathbf{h}}_b \in \mathbb{C}^{N_t \times 1}$ is defined as the equivalent channel spanning from Alice to Bob. The channels of the IRS-Bob link and the Alice-IRS link are modeled by $\mathbf{h}_{rb} \in \mathbb{C}^{M \times 1}$ and $\mathbf{G}_{ar} \in \mathbb{C}^{M \times N_t}$, respectively. $\hat{\mathbf{h}}_{e,k} = \mathbf{G}_{ar}^H \mathbf{\Phi}^H \mathbf{h}_{re,k}$, $\hat{\mathbf{h}}_{e,k} \in \mathbb{C}^{N_t \times 1}$ is defined as the equivalent channel spanning from Alice to the kth Eve. The channel of the IRS-Eve link is modeled by $\mathbf{h}_{re,k} \in \mathbb{C}^{M \times 1}$. $n_b(t)$ is the additive white Gaussian noise (AWGN) at Bob with zero mean and noise variance σ_b^2, i.e., $n_b \sim \mathcal{CN}(0, \sigma_b^2)$. $n_{e,k}(t)$ is the AWGN at the kth Eve with zero mean and noise covariance matrix $\sigma_{e,k}^2$, i.e., $n_{e,k} \sim \mathcal{CN}(0, \sigma_{e,k}^2)$. The phase shift coefficients of the IRS are collected in a diagonal matrix defined by $\mathbf{\Phi} = \text{diag}\{\phi_1, \cdots, \phi_m, \cdots, \phi_M\}$, where $\phi_m = e^{j\theta_m}$, and $\theta_m \in [0, 2\pi]$ denotes the phase shift of the m-th reflecting element.

The transmit signal vector is

$$\mathbf{x}(t) = \mathbf{s}(t) + \mathbf{z}(t) = \mathbf{w}s(t) + \mathbf{z}(t), \tag{3}$$

where $s(t)$ is a data stream carrying the confidential information intended for Bob, $\mathbf{z}(t)$ is the noise vector artificially created by Alice to interfere Eves, i.e., the so-called AN, and $\mathbf{w}$ is the beamforming vector. The confidential signal vector $\mathbf{s}(t)$ is assumed to follow a complex Gaussian distribution of $\mathcal{CN}(\mathbf{0}, \mathbf{W})$, where $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ is the transmit covariance matrix to be designed. For the AN, we assume $\mathbf{z}(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{Z})$, where $\mathbf{Z}$ is the AN covariance matrix to be designed.

The equivalent channel $\hat{\mathbf{h}}_b$ can be rewritten as

$$\hat{\mathbf{h}}_b^H = \boldsymbol{\phi}^T \text{diag}(\mathbf{h}_{rb}^H)\mathbf{G}_{ar} \triangleq \boldsymbol{\phi}^T \mathbf{G}_{cb}, \tag{4}$$

where $\boldsymbol{\phi} = [\phi_1, \cdots, \phi_m, \cdots, \phi_M]^T$ and $\mathbf{G}_{cb} = \text{diag}(\mathbf{h}_{rb}^H)\mathbf{G}_{ar}$. $\mathbf{G}_{cb} \in \mathbb{C}^{M \times N_t}$ is defined as the cascaded channel from Alice to Bob via the IRS. Similarly, the equivalent channel $\hat{\mathbf{h}}_{e,k}$ can be expressed in another way as

$$\hat{\mathbf{h}}_{e,k}^H = \boldsymbol{\phi}^T \text{diag}(\mathbf{h}_{re,k}^H)\mathbf{G}_{ar} \triangleq \boldsymbol{\phi}^T \mathbf{G}_{ce,k}, \tag{5}$$

where $\mathbf{G}_{ce,k} = \text{diag}(\mathbf{h}_{re,k}^H)\mathbf{G}_{ar}$, $k = 1, 2, \cdots, K$. $\mathbf{G}_{ce,k} \in \mathbb{C}^{M \times N_t}$ denotes the cascaded channel from Alice to the kth Eve via the IRS.

B. Statistical CSI Error Model

In IRS-aided communications, the cascaded AP-IRS-user channels at the transmitter is challenging to obtain due to the passive features of the IRS. Hence, we consider the CSI error in the cascaded AP-IRS-user channels. Generally, there are two channel error models: the bounded CSI error model and the statistical CSI error model. In this paper, we focus on the statistical CSI error of the cascaded channel for Eves since the bounded CSI error is more conservative. Furthermore, the statistical CSI error model is more closely related to the channel estimation error, while the bounded CSI error usually models the quantization error.

We assume the cascaded channel $\mathbf{G}_{ce,k}$ from Alice to the kth Eve is imperfect, which can be represented as

$$\mathbf{G}_{ce,k} = \bar{\mathbf{G}}_{ce,k} + \triangle\mathbf{G}_{ce,k}, \mathbf{g}_{ce,k} \triangleq \text{vec}(\triangle\mathbf{G}_{ce,k}) \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma}_{e,k}), \tag{6}$$

where the CSI error vector $\mathbf{g}_{ce,k} \triangleq \text{vec}(\triangle\mathbf{G}_{ce,k})$ is assumed to follow the CSCG distribution, and $\boldsymbol{\Sigma}_{e,k} \in \mathbb{C}^{MN_t \times MN_t}$ is the semidefinite error covariance matrix.

III. PROBLEM FORMULATION

In this section, we first derive the secrecy rate expression and then formulate the outage-constrained power minimization problem.

A. Secrecy Rate

The achievable data rate (bit/s/Hz) of Bob is given by

$$
\begin{aligned}
C_b(\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi}) &= \log\left(1 + \frac{\hat{\mathbf{h}}_b^H \mathbf{W} \hat{\mathbf{h}}_b}{\sigma_b^2 + \hat{\mathbf{h}}_b^H \mathbf{Z} \hat{\mathbf{h}}_b}\right) \\
&= \log\left(1 + \frac{(\boldsymbol{\phi}^T \mathbf{G}_{cb})\mathbf{W}(\boldsymbol{\phi}^T \mathbf{G}_{cb})^H}{\sigma_b^2 + (\boldsymbol{\phi}^T \mathbf{G}_{cb})\mathbf{Z}(\boldsymbol{\phi}^T \mathbf{G}_{cb})^H}\right),
\end{aligned}
\tag{7}
$$

where the cascaded channel $\mathbf{G}_{cb}$ from Alice to Bob is utilized. The achievable data rate (bit/s/Hz) of the kth Eve is given by

$$
\begin{aligned}
C_{e,k}(\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi}) &= \log\left(1 + \frac{\hat{\mathbf{h}}_{e,k}^H \mathbf{W} \hat{\mathbf{h}}_{e,k}}{\sigma_{e,k}^2 + \hat{\mathbf{h}}_{e,k}^H \mathbf{Z} \hat{\mathbf{h}}_{e,k}}\right) \\
&= \log\left(1 + \frac{(\boldsymbol{\phi}^T \mathbf{G}_{ce,k})\mathbf{W}(\boldsymbol{\phi}^T \mathbf{G}_{ce,k})^H}{\sigma_{e,k}^2 + (\boldsymbol{\phi}^T \mathbf{G}_{ce,k})\mathbf{Z}(\boldsymbol{\phi}^T \mathbf{G}_{ce,k})^H}\right),
\end{aligned}
\tag{8}
$$

where the cascaded channel $\mathbf{G}_{ce,k}$ from Alice to the kth Eve is applied.

Then the achievable secrecy rate is

$$
R_s(\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi}) = \min_{k=1,2,\cdots,K}\left\{C_b(\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi}) - C_{e,k}(\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi})\right\}.
\tag{9}
$$

B. Power Minimization

In this paper, we aim to jointly optimize the transmit beamforming vector $\mathbf{w}$ (or the transmit beamforming matrix $\mathbf{W} = \mathbf{w}\mathbf{w}^H$), the covariance matrix $\mathbf{Z}$ of AN and the IRS phase shifts $\boldsymbol{\Phi}$ to minimize the transmit power subject to the Bob's data rate requirement and leaked data rate outage for Eves. The OC-PM problem can be formulated as

$$
\min_{\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi}} \mathrm{Tr}(\mathbf{W}+\mathbf{Z})
\tag{10a}
$$

$$
\text{s.t.} \quad C_b(\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi}) \geq \log\gamma,
\tag{10b}
$$

$$
\mathrm{Pr}_{\mathbf{g}_{ce,k}}\left\{C_{e,k}(\mathbf{W}, \mathbf{Z}, \boldsymbol{\Phi}) \leq \log\beta\right\} \geq 1 - \rho_k, k = 1, 2, \cdots, K,
\tag{10c}
$$

$$
\mathbf{Z} \succeq 0,
\tag{10d}
$$

$$
\mathbf{W} \succeq 0,
\tag{10e}
$$

$$
\mathrm{rank}(\mathbf{W}) = 1,
\tag{10f}
$$

$$
|\phi_m| = 1, m = 1, \cdots, M,
\tag{10g}
$$

where γ, β, and $\rho_k, \forall k$ are constant values, and (10c) can be seen as the constraints of per-Eve secrecy outage probability.

IV. PROBLEM SOLUTION

Due to the coupling relation of various optimization variables and the complicated probabilistic constraints, the proposed OC-PM problem is nonconvex and challenging to solve. To tackle it, we first transform the probabilistic constraints into the safe and tractable forms. Then, the AO strategy is utilized to decouple the parameters and transform the original problems into two subproblems.

A. Problem Reformulation

We first reformulate the constraint in (10b). Specifically, it can be simplified by removing the log function as

$$\log\left(1 + \frac{\hat{\mathbf{h}}_b^H \mathbf{W} \hat{\mathbf{h}}_b}{\sigma_b^2 + \hat{\mathbf{h}}_b^H \mathbf{Z} \hat{\mathbf{h}}_b}\right) \geq \log \gamma \tag{11a}$$

$$\Leftrightarrow \text{Tr}([\mathbf{W} - (\gamma - 1)\mathbf{Z}]\hat{\mathbf{h}}_b \hat{\mathbf{h}}_b^H) \geq (\gamma - 1)\sigma_b^2, \tag{11b}$$

$$\Leftrightarrow \text{Tr}([\mathbf{W} - (\gamma - 1)\mathbf{Z}](\mathbf{G}_{cb}^H \boldsymbol{\phi}^*)(\boldsymbol{\phi}^T \mathbf{G}_{cb})) \geq (\gamma - 1)\sigma_b^2, \tag{11c}$$

$$\Leftrightarrow \text{Tr}(\mathbf{G}_{cb}[\mathbf{W} - (\gamma - 1)\mathbf{Z}]\mathbf{G}_{cb}^H \mathbf{E}) \geq (\gamma - 1)\sigma_b^2, \tag{11d}$$

where $\mathbf{E} \triangleq \boldsymbol{\phi}^* \boldsymbol{\phi}^T$. Then, we reformulate the per-Eve outage probability constraint (10c), which is not tractable to handle due to the log function and the probability requirement. We first eliminate the log function, then transform the probability constraint into the deterministic constraint. There are two steps to reformulate the chance constraint (10c) as follows.

Step 1): Firstly, the data rate leakage expression in (10c) can be simplifed as

$$\log\left(1 + \frac{\hat{\mathbf{h}}_{e,k}^H \mathbf{W} \hat{\mathbf{h}}_{e,k}}{\sigma_{e,k}^2 + \hat{\mathbf{h}}_{e,k}^H \mathbf{Z} \hat{\mathbf{h}}_{e,k}}\right) \leq \log \beta \tag{12a}$$

$$\Leftrightarrow \hat{\mathbf{h}}_{e,k}^H [\mathbf{W} - (\beta - 1)\mathbf{Z}]\hat{\mathbf{h}}_{e,k} \leq (\beta - 1)\sigma_{e,k}^2. \tag{12b}$$

By substituting $\hat{\mathbf{h}}_{e,k}^H = \boldsymbol{\phi}^T(\bar{\mathbf{G}}_{ce,k} + \triangle\mathbf{G}_{ce,k})$ into (12b) and defining $\boldsymbol{\Xi}_e \triangleq (\beta - 1)\mathbf{Z} - \mathbf{W}$, we have

$$(12a) \Leftrightarrow [\boldsymbol{\phi}^T(\bar{\mathbf{G}}_{ce,k} + \triangle\mathbf{G}_{ce,k})]\boldsymbol{\Xi}_e[\boldsymbol{\phi}^T(\bar{\mathbf{G}}_{ce,k} + \triangle\mathbf{G}_{ce,k})]^H + (\beta - 1)\sigma_{e,k}^2 \geq 0, \tag{13a}$$

$$\Leftrightarrow \underbrace{\boldsymbol{\phi}^T \triangle\mathbf{G}_{ce,k} \boldsymbol{\Xi}_e \triangle\mathbf{G}_{ce,k}^H \boldsymbol{\phi}^*}_{f_1} + 2\text{Re}\{\underbrace{\boldsymbol{\phi}^T \triangle\mathbf{G}_{ce,k} \boldsymbol{\Xi}_e \bar{\mathbf{G}}_{ce,k}^H \boldsymbol{\phi}^*}_{f_2}\}$$

$$+ \underbrace{(\boldsymbol{\phi}^T \bar{\mathbf{G}}_{ce,k})\boldsymbol{\Xi}_e(\boldsymbol{\phi}^T \bar{\mathbf{G}}_{ce,k})^H + (\beta - 1)\sigma_{e,k}^2}_{c_k} \geq 0. \tag{13b}$$

Let us equivalently represent the CSI error $\mathbf{g}_{ce,k} = \text{vec}(\triangle\mathbf{G}_{ce,k})$ as $\mathbf{g}_{ce,k} = \boldsymbol{\Sigma}_{e,k}^{1/2}\mathbf{v}_{ce,k}$, where $\mathbf{v}_{ce,k} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{MN_t})$, $\boldsymbol{\Sigma}_{e,k} = \boldsymbol{\Sigma}_{e,k}^{1/2}\boldsymbol{\Sigma}_{e,k}^{1/2}$ and $(\boldsymbol{\Sigma}_{e,k}^{1/2})^H = \boldsymbol{\Sigma}_{e,k}^{1/2}$. The expression f_1 in (13b) can be reformulated as

$$
\begin{aligned}
f_1 &= \text{Tr}(\triangle\mathbf{G}_{ce,k}\boldsymbol{\Xi}_e\triangle\mathbf{G}_{ce,k}^H\boldsymbol{\phi}^*\boldsymbol{\phi}^T) \\
&= \text{Tr}(\triangle\mathbf{G}_{ce,k}^H\mathbf{E}\triangle\mathbf{G}_{ce,k}\boldsymbol{\Xi}_e) \\
&\overset{(a)}{=} \text{vec}^H(\triangle\mathbf{G}_{ce,k})(\boldsymbol{\Xi}_e^T\otimes\mathbf{E})\text{vec}(\triangle\mathbf{G}_{ce,k}) \\
&= \mathbf{g}_{ce,k}^H(\boldsymbol{\Xi}_e^T\otimes\mathbf{E})\mathbf{g}_{ce,k} \\
&= \mathbf{v}_{ce,k}^H\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T\otimes\mathbf{E})\boldsymbol{\Sigma}_{e,k}^{1/2}\mathbf{v}_{ce,k} \\
&\triangleq \mathbf{v}_{ce,k}^H\mathbf{A}_k\mathbf{v}_{ce,k},
\end{aligned}
\tag{14}
$$

where $\mathbf{A}_k \triangleq \boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T\otimes\mathbf{E})\boldsymbol{\Sigma}_{e,k}^{1/2}$, and the (a) is obtained by invoking the identity $\text{Tr}(\mathbf{A}^H\mathbf{BCD}) = \text{vec}^H(\mathbf{A})(\mathbf{D}^T\otimes\mathbf{B})\text{vec}(\mathbf{C})$. The expression f_2 in (13b) can be reformulated as

$$
\begin{aligned}
f_2 &= \text{Tr}(\triangle\mathbf{G}_{ce,k}\boldsymbol{\Xi}_e(\bar{\mathbf{G}}_{ce,k}^H\boldsymbol{\phi}^*)\boldsymbol{\phi}^T) \\
&= \text{Tr}(\triangle\mathbf{G}_{ce,k}\boldsymbol{\Xi}_e(\bar{\mathbf{G}}_{ce,k}^H\mathbf{E})) \\
&\overset{(b)}{=} \text{vec}^H(\mathbf{E}\bar{\mathbf{G}}_{ce,k})(\boldsymbol{\Xi}_e^T\otimes\mathbf{I}_M)\text{vec}(\triangle\mathbf{G}_{ce,k}) \\
&= \text{vec}^H(\mathbf{E}\bar{\mathbf{G}}_{ce,k})(\boldsymbol{\Xi}_e^T\otimes\mathbf{I}_M)\mathbf{g}_{ce,k} \\
&= \text{vec}^H(\mathbf{E}\bar{\mathbf{G}}_{ce,k})(\boldsymbol{\Xi}_e^T\otimes\mathbf{I}_M)\boldsymbol{\Sigma}_{e,k}^{1/2}\mathbf{v}_{ce,k} \\
&\triangleq \mathbf{u}_{ce,k}^H\mathbf{v}_{ce,k},
\end{aligned}
\tag{15}
$$

where $\mathbf{u}_{ce,k}^H \triangleq \text{vec}^H(\mathbf{E}\bar{\mathbf{G}}_{ce,k})(\boldsymbol{\Xi}_e^T\otimes\mathbf{I}_M)\boldsymbol{\Sigma}_{e,k}^{1/2}$, and the (b) is obtained by invoking the identity $\text{Tr}(\mathbf{ABC}^H) = \text{vec}^H(\mathbf{C})(\mathbf{B}^T\otimes\mathbf{I})\text{vec}(\mathbf{A})$. The expression c_k in (13b) can be reformulated as

$$
c_k = \text{Tr}[\bar{\mathbf{G}}_{ce,k}\boldsymbol{\Xi}_e\bar{\mathbf{G}}_{ce,k}^H\mathbf{E}] + (\beta-1)\sigma_{e,k}^2.
\tag{16}
$$

By substituting (14), (15) and (16) into (13b), we have

$$
(12a) \Leftrightarrow \mathbf{v}_{ce,k}^H\mathbf{A}_k\mathbf{v}_{ce,k} + 2\text{Re}\{\mathbf{u}_{ce,k}^H\mathbf{v}_{ce,k}\} + c_k \geq 0.
\tag{17}
$$

The leakage data rate constraint in (10c) becomes

$$
(10c) \Leftrightarrow \text{Pr}_{\mathbf{v}_{ce,k}}\left\{\mathbf{v}_{ce,k}^H\mathbf{A}_k\mathbf{v}_{ce,k} + 2\text{Re}\{\mathbf{u}_{ce,k}^H\mathbf{v}_{ce,k}\} + c_k \geq 0\right\} \geq 1 - \rho_k, k = 1, 2, \cdots, K.
\tag{18}
$$

Step 2): the chance constraint is transformed into a deterministic constraint by using the BTI, which provides a safe approximation for (18).

The equivalence in (18) implies that the outage probability in (10c) can be characterized by the quadratic inequality with respect to (w.r.t.) the Gaussian random vector $\mathbf{v}_{ce,k}$. Generally, the Bernstein-type inequality is utilized to approximate a chance constraint safely, which is given in the following Lemma.

Lemma 1:

(Bernstein-Type Inequality) For any $(\mathbf{A}, \mathbf{u}, c) \in \mathbb{H}^n \times \mathbb{C}^n \times \mathbb{R}, \mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_n)$ and $\rho \in (0,1]$, the following implication holds:

$$\mathrm{Pr}_{\mathbf{v}} \left\{ \mathbf{v}^H \mathbf{A} \mathbf{v} + 2\mathrm{Re}\{\mathbf{u}^H \mathbf{v}\} + c \geq 0 \right\} \geq 1 - \rho$$

$$\Longleftrightarrow \mathrm{Tr}(\mathbf{A}) - \sqrt{2\ln(1/\rho)}\sqrt{\|\mathbf{A}\|_F^2 + 2\|\mathbf{u}\|^2} + \ln(\rho) \cdot \lambda^+(-\mathbf{A}) + c \geq 0,$$

$$\Longleftrightarrow \begin{cases} \mathrm{Tr}(\mathbf{A}) - \sqrt{-2\ln(\rho)} \cdot x + \ln(\rho) \cdot y + c \geq 0, \\ \left\| \begin{bmatrix} \mathrm{vec}(\mathbf{A}), \\ \sqrt{2}\mathbf{u} \end{bmatrix} \right\|_2 \leq x, \\ y\mathbf{I}_n + \mathbf{A} \succeq \mathbf{0}, y \geq 0, \end{cases}$$

where $\lambda^+(\mathbf{A}) = \max(\lambda_{\max}(\mathbf{A}), 0)$. x and y are slack variables.

By invoking Lemma 1 and introducing the slack variables $\mathbf{x} = [x_1, x_2, \cdots, x_K]^T$ and $\mathbf{y} = [y_1, y_2, \cdots, y_K]^T$, we arrive at the desired safe approximation of OC-PM, which is shown as

$$\min_{\mathbf{W}, \mathbf{Z}, \phi, \mathbf{A}, \mathbf{x}, \mathbf{y}} \mathrm{Tr}(\mathbf{W} + \mathbf{Z}) \tag{19a}$$

$$\mathrm{s.t.} \quad \mathrm{Tr}(\mathbf{A}_k) - \sqrt{-2\ln(\rho_k)} \cdot x_k + \ln(\rho_k) \cdot y_k + c_k \geq 0, \tag{19b}$$

$$\left\| \begin{bmatrix} \mathrm{vec}(\mathbf{A}_k) \\ \sqrt{2}\mathbf{u}_{ce,k} \end{bmatrix} \right\|_2 \leq x_k, \tag{19c}$$

$$y_k \mathbf{I}_{MN_t} + \mathbf{A}_k \succeq \mathbf{0}, y_k \geq 0, \tag{19d}$$

$$\mathrm{Tr}(\mathbf{G}_{cb}[\mathbf{W} - (\gamma - 1)\mathbf{Z}]\mathbf{G}_{cb}^H \mathbf{E}) \geq (\gamma - 1)\sigma_b^2, \tag{19e}$$

$$(10d), (10e), (10f), (10g), \tag{19f}$$

where $\mathbf{A} = [\mathbf{A}_1, \mathbf{A}_2, \cdots, \mathbf{A}_K]$. The constraint (19e) is obtained by substituting (11d) into (10b). The constraints (19b), (19c) and (19d) can be further simplified by some mathematical transformations as follows.

The $\mathrm{Tr}(\mathbf{A}_k)$ in (19b) can be rewritten as

$$\mathrm{Tr}(\mathbf{A}_k) = \mathrm{Tr}(\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}^{1/2}) = \mathrm{Tr}((\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}). \tag{20}$$

The $\|\text{vec}(\mathbf{A}_k)\|_2^2$ in (19c) can be written as

$$\|\text{vec}(\mathbf{A}_k)\|_2^2 = \|\mathbf{A}_k\|_F^2 = \text{Tr}[\mathbf{A}_k\mathbf{A}_k^H] = \text{Tr}[\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}^{1/2}\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^* \otimes \mathbf{E}^H)\boldsymbol{\Sigma}_{e,k}^{1/2}]$$

$$= \text{Tr}[(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})^H\boldsymbol{\Sigma}_{e,k}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}]$$

$$\overset{(c)}{=} \text{vec}^H(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})(\boldsymbol{\Sigma}_{e,k}^T \otimes \boldsymbol{\Sigma}_{e,k})\text{vec}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})$$

$$= \text{vec}^H(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})[(\boldsymbol{\Sigma}_{e,k}^{1/2T}\boldsymbol{\Sigma}_{e,k}^{1/2T}) \otimes (\boldsymbol{\Sigma}_{e,k}^{1/2}\boldsymbol{\Sigma}_{e,k}^{1/2})]\text{vec}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})$$

$$= \text{vec}^H(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})[(\boldsymbol{\Sigma}_{e,k}^{1/2T} \otimes \boldsymbol{\Sigma}_{e,k}^{1/2})^H(\boldsymbol{\Sigma}_{e,k}^{1/2T} \otimes \boldsymbol{\Sigma}_{e,k}^{1/2})]\text{vec}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})$$

$$= \left\|(\boldsymbol{\Sigma}_{e,k}^{1/2T} \otimes \boldsymbol{\Sigma}_{e,k}^{1/2})\text{vec}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\right\|_2^2, \tag{21}$$

where the (c) is obtained by invoking the identity $\text{Tr}(\mathbf{A}^H\mathbf{B}\mathbf{C}\mathbf{D}) = \text{vec}^H(\mathbf{A})(\mathbf{D}^T \otimes \mathbf{B})\text{vec}(\mathbf{C})$.

The $\|\mathbf{u}_{ce,k}\|_2^2$ in (19c) can be written as

$$\|\mathbf{u}_{ce,k}\|_2^2 = \mathbf{u}_{ce,k}^H\mathbf{u}_{ce,k}$$

$$= \text{vec}^H(\mathbf{E}\bar{\mathbf{G}}_{ce,k})(\boldsymbol{\Xi}_e^T \otimes \mathbf{I}_M)\boldsymbol{\Sigma}_{e,k}^{1/2}\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^* \otimes \mathbf{I}_M)\text{vec}(\mathbf{E}\bar{\mathbf{G}}_{ce,k})$$

$$= \left\|\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{I}_M)\text{vec}(\mathbf{E}\bar{\mathbf{G}}_{ce,k})\right\|_2^2. \tag{22}$$

The constraint $y_k\mathbf{I}_n + \mathbf{A}_k \succeq \mathbf{0}, y_k \geq 0$ in (19d) can be written as

$$y_k\mathbf{I}_{N_tM} + \boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}^{1/2} \succeq \mathbf{0}, y_k \geq 0. \tag{23}$$

Finally, by substituting (20), (21), (22) and (23) into (19), the OC-PM Problem can be recast as

$$\min_{\mathbf{W},\mathbf{Z},\phi,\mathbf{x},\mathbf{y}} \text{Tr}(\mathbf{W}+\mathbf{Z}) \tag{24a}$$

$$\text{s.t.} \quad \text{Tr}((\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}) - \sqrt{-2\ln(\rho_k)} \cdot x_k + \ln(\rho_k) \cdot y_k$$

$$+ \text{Tr}[\bar{\mathbf{G}}_{ce,k}\boldsymbol{\Xi}_e\bar{\mathbf{G}}_{ce,k}^H\mathbf{E}] + (\beta - 1)\sigma_{e,k}^2 \geq 0, \tag{24b}$$

$$\left\|\begin{bmatrix} (\boldsymbol{\Sigma}_{e,k}^{1/2T} \otimes \boldsymbol{\Sigma}_{e,k}^{1/2})\text{vec}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E}) \\ \sqrt{2}\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{I}_M)\text{vec}(\mathbf{E}\bar{\mathbf{G}}_{ce,k}) \end{bmatrix}\right\|_2 \leq x_k, \tag{24c}$$

$$y_k\mathbf{I}_{N_tM} + \boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}^{1/2} \succeq \mathbf{0}, y_k \geq 0, \tag{24d}$$

$$(19e), (10d), (10e), (10f), (10g). \tag{24e}$$

B. Solving the Beamforming Matrix and AN Covariance Matrix

Problem (24) is not convex due to the coupled $\boldsymbol{\Xi}_e$ and $\boldsymbol{\phi}$. To solve it, we use the AO method to update $\{\mathbf{W}, \mathbf{Z}, \mathbf{x}, \mathbf{y}\}$ and $\boldsymbol{\phi}$ iteratively. Specifically, when $\boldsymbol{\phi}$ is fixed, Problem (24) becomes convex for $\{\mathbf{W}, \mathbf{Z}, \mathbf{x}, \mathbf{y}\}$ if the rank one constraint in (10f) is relaxed. By the SDR technique, the problem of optimizing $\{\mathbf{W}, \mathbf{Z}, \mathbf{x}, \mathbf{y}\}$ becomes

$$\min_{\mathbf{W}, \mathbf{Z}, \mathbf{x}, \mathbf{y}} \mathrm{Tr}(\mathbf{W} + \mathbf{Z}) \tag{25a}$$

$$\text{s.t.} \quad \mathrm{Tr}((\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}) - \sqrt{-2\ln(\rho_k)} \cdot x_k + \ln(\rho_k) \cdot y_k$$
$$+ \mathrm{Tr}[\bar{\mathbf{G}}_{ce,k}\boldsymbol{\Xi}_e \bar{\mathbf{G}}_{ce,k}^H \mathbf{E}] + (\beta - 1)\sigma_{e,k}^2 \geq 0, \tag{25b}$$

$$\left\| \begin{bmatrix} (\boldsymbol{\Sigma}_{e,k}^{1/2T} \otimes \boldsymbol{\Sigma}_{e,k}^{1/2})\mathrm{vec}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E}) \\ \sqrt{2}\boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{I}_M)\mathrm{vec}(\mathbf{E}\bar{\mathbf{G}}_{ce,k}) \end{bmatrix} \right\|_2 \leq x_k, \tag{25c}$$

$$y_k \mathbf{I}_{N_t M} + \boldsymbol{\Sigma}_{e,k}^{1/2}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E})\boldsymbol{\Sigma}_{e,k}^{1/2} \succeq \mathbf{0}, y_k \geq 0, \tag{25d}$$

$$(19\mathrm{e}), (10\mathrm{d}), (10\mathrm{e}). \tag{25e}$$

Problem (25) is convex, and can be solved by the CVX toolbox. Due to the SDR, the obtained $\mathbf{W}$ of Problem (25) may not be a rank-one solution. If not, the suboptimal beamforming vector can be obtained by using the Gaussian randomization method. Numerical simulations show that the obtained $\mathbf{W}$ always satisfies the rank-one constraint. Thus, the beamforming vector $\mathbf{w}$ can be obtained from the eigen-decomposition of $\mathbf{W}$.

C. Solving the Phase Shifts of IRS

When $\{\mathbf{W}, \mathbf{Z}, \mathbf{x}, \mathbf{y}\}$ are fixed, Problem (24) becomes a feasibility check problem. In order to improve the converged solution in the optimization process, the data rate inequalities for Bob in (11d) and Eve in (13a) are rewritten by introducing slack variables, and recast respectively as

$$\mathrm{Tr}(\mathbf{G}_{cb}[\mathbf{W} - (\gamma - 1)\mathbf{Z}]\mathbf{G}_{cb}^H \mathbf{E}) \geq (\gamma - 1)\sigma_b^2 + \delta_0, \delta_0 \geq 0, \tag{26a}$$

$$[\boldsymbol{\phi}^T(\bar{\mathbf{G}}_{ce,k} + \triangle\mathbf{G}_{ce,k})]\boldsymbol{\Xi}_e[\boldsymbol{\phi}^T(\bar{\mathbf{G}}_{ce,k} + \triangle\mathbf{G}_{ce,k})]^H + (\beta - 1)\sigma_{e,k}^2 + \delta_k \geq 0, \delta_k \geq 0. \tag{26b}$$

Then by fixing $\mathbf{W}$ and $\mathbf{Z}$ obtained in the previous iteration, and using the BTI for the outage of leaked data rate again, the optimization problem for ϕ becomes

$$\max_{\phi, \boldsymbol{\delta}, \mathbf{x}, \mathbf{y}} \quad \|\boldsymbol{\delta}\|_1 \tag{27a}$$

$$\text{s.t.} \quad \text{Tr}((\boldsymbol{\Xi}_e^T \otimes \mathbf{E}) \boldsymbol{\Sigma}_{e,k}) - \sqrt{-2\ln(\rho_k)} \cdot x_k + \ln(\rho_k) \cdot y_k$$

$$+ \text{Tr}[\bar{\mathbf{G}}_{ce,k} \boldsymbol{\Xi}_e \bar{\mathbf{G}}_{ce,k}^H \mathbf{E}] + (\beta - 1)\sigma_{e,k}^2 + \delta_k \geq 0, \tag{27b}$$

$$\left\| \begin{bmatrix} (\boldsymbol{\Sigma}_{e,k}^{1/2T} \otimes \boldsymbol{\Sigma}_{e,k}^{1/2}) \text{vec}(\boldsymbol{\Xi}_e^T \otimes \mathbf{E}) \\ \sqrt{2} \boldsymbol{\Sigma}_{e,k}^{1/2} (\boldsymbol{\Xi}_e^T \otimes \mathbf{I}_M) \text{vec}(\mathbf{E}\bar{\mathbf{G}}_{ce,k}) \end{bmatrix} \right\|_2 \leq x_k, \tag{27c}$$

$$y_k \mathbf{I}_{N_t M} + \boldsymbol{\Sigma}_{e,k}^{1/2} (\boldsymbol{\Xi}_e^T \otimes \mathbf{E}) \boldsymbol{\Sigma}_{e,k}^{1/2} \succeq \mathbf{0}, y_k \geq 0, \tag{27d}$$

$$\text{Tr}(\mathbf{G}_{cb}[\mathbf{W} - (\gamma - 1)\mathbf{Z}]\mathbf{G}_{cb}^H \mathbf{E}) \geq (\gamma - 1)\sigma_b^2 + \delta_0, \tag{27e}$$

$$\boldsymbol{\delta} \succeq \mathbf{0}, \tag{27f}$$

$$(10\text{g}), \tag{27g}$$

where $\boldsymbol{\delta} = [\delta_0, \delta_1, \delta_2, \cdots, \delta_K]^T$. Then, the only nonconvex constraint in Problem (27) is the unit-modulus constraint (10g). There is no general approach to solve unit modulus constrained non-convex optimization problems optimally. To deal with it, the semidefinite programming (SDP) method is utilized. To facilitate SDP, Problem (27) is recast as

$$\max_{\mathbf{E}, \boldsymbol{\delta}, \mathbf{x}, \mathbf{y}} \quad \|\boldsymbol{\delta}\|_1 \tag{28a}$$

$$\text{s.t.} \quad (27\text{b}), (27\text{c}), (27\text{d}), (27\text{e}), (27\text{f}) \tag{28b}$$

$$\text{Diag}(\mathbf{E}) = \mathbf{1}_M, \tag{28c}$$

$$\mathbf{E} \succeq \mathbf{0}, \tag{28d}$$

$$\text{rank}(\mathbf{E}) = 1, \tag{28e}$$

where the constraints (28c), (28d) and (28e) are equivalent to the constraint (10g), and they are imposed to ensure that the phase shifts vector ϕ with unit modulus can be recovered from $\mathbf{E}$. The Problem (28) is convex except the nonconvex constraint (28e). Although the SDR method can be used to solve Problem (28) by removing constraint (28e) and solving the resulted SDP problem, the rank of solved $\mathbf{E}$ is generally larger than one. To handle this problem, we construct a convex constraint equivalent to the rank one constraint (28e), and the following Lemma is utilized.

Lemma 2: For any positive semidefinite matrix $\mathbf{A}$, the following inequality holds

$$|\mathbf{I} + \mathbf{A}| \geq 1 + \mathrm{Tr}(\mathbf{A}), \tag{29}$$

and the equality in (29) holds if and only if $\mathrm{rank}(\mathbf{A}) \leq 1$. *Proof*: Let $r_A = \mathrm{rank}(\mathbf{A})$. Since $r_A = 0$ is trivial, the nonzero eigenvalues of $\mathbf{A}$ are denoted by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{r_A} > 0$. Then we have

$$|\mathbf{I} + \mathbf{A}| = \prod_{i=1}^{r_A}(1 + \lambda_i) = 1 + \sum_{i=1}^{r_A}\lambda_i + \sum_{i \neq k}\lambda_i \lambda_k + \cdots$$

$$\geq 1 + \sum_{i=1}^{r_A}\lambda_i = 1 + \mathrm{Tr}(\mathbf{A}). \tag{30}$$

It can be seen from (30) that the equality holds if and only if $\mathrm{rank}(\mathbf{A}) = 1$. ∎

By invoking Lemma 2, we can build an equivalent constraint as

$$(28e) \Leftrightarrow |\mathbf{I} + \mathbf{E}| \leq 1 + \mathrm{Tr}(\mathbf{E}), \tag{31a}$$

$$\Leftrightarrow \log \det(\mathbf{I} + \mathbf{E}) \leq \log(1 + M), \tag{31b}$$

where $\mathrm{Tr}(\mathbf{E}) = M$. The constraint (31b) ensures the rank one equality, thus is equivalent to constraint (28e). By utilizing the penalty-based method and putting the constraint (31b) into the objective function (OF) of Problem (28), Problem (28) can be cast as

$$\max_{\mathbf{E}, \boldsymbol{\delta}, \mathbf{x}, \mathbf{y}} \quad \|\boldsymbol{\delta}\|_1 + \kappa[\log(1 + M) - \log \det(\mathbf{I} + \mathbf{E})] \tag{32a}$$

$$\text{s.t.} \quad (27b), (27c), (27d), (27e), (27f), (28c), (28d), \tag{32b}$$

where κ is a penalty factor penalizing the violation of constraint $\mathrm{rank}(\mathbf{E}) = 1$. Since the $\log \det(\mathbf{I} + \mathbf{E})$ is a concave function with respect to $\mathbf{E}$, the upper bound of it can be obtained by using the first-order Taylor approximation as

$$\log \det(\mathbf{I} + \mathbf{E}) \leq (\log e)\mathrm{Tr}\{((\mathbf{I} + \mathbf{E}^{(n)})^{-1})^*(\mathbf{E} - \mathbf{E}^{(n)})\} + (\log e)\log \det(\mathbf{I} + \mathbf{E}^{(n)}), \tag{33}$$

where e denotes natural logarithm, and the $\frac{\partial \ln(|\det(\mathbf{X})|)}{\partial \mathbf{X}} = (\mathbf{X}^{-1})^T$ is utilized. By substituting (33) into the OF of Problem (32) and removing the constant terms, Problem (32) can be written as

$$\max_{\mathbf{E}, \boldsymbol{\delta}, \mathbf{x}, \mathbf{y}} \quad \|\boldsymbol{\delta}\|_1 + \kappa[-(\log e)\mathrm{Tr}\{((\mathbf{I} + \mathbf{E}^{(n)})^{-1})^*(\mathbf{E} - \mathbf{E}^{(n)})\}] \tag{34a}$$

$$\text{s.t.} \quad (27b), (27c), (27d), (27e), (27f), (28c), (28d). \tag{34b}$$

Problem (34) is jointly convex with respect to $\{\mathbf{E}, \boldsymbol{\delta}, \mathbf{x}, \mathbf{y}\}$, hence it can be efficiently solved by standard convex program solvers such as CVX. A rank-one solution $\mathbf{E}^\star$ can be obtained by solving

---

Algorithm 1 Alternating Optimization Algorithm

1: Parameter Setting: Set the maximum number of iterations $n_{\max}$ and the first iterative number $n = 1$; Give the penalty factor κ and error tolerance ε;

2: Initialize the variables $\mathbf{w}^{(1)}$, $\mathbf{Z}^{(1)}$ and $\phi^{(1)}$ in the feasible region; Compute the OF value of Problem (24) as $\mathrm{OF}(\mathbf{w}^{(1)}, \mathbf{Z}^{(1)})$;

3: Solve Problem (25) to obtain the $\mathbf{w}^{(n)}$, $\mathbf{Z}^{(n)}$ by fixing $\phi^{(n-1)}$; Calculate the OF value of Problem (25) as $\mathrm{OF}(\mathbf{w}^{(n)}, \mathbf{Z}^{(n)})$;

4: Solve Problem (34) to obtain the $\phi^{(n)}$ by fixing $\mathbf{w}^{(n)}, \mathbf{Z}^{(n)}$;

5: If $\left|\mathrm{OF}(\mathbf{w}^{(n)}, \mathbf{Z}^{(n)}) - \mathrm{OF}(\mathbf{w}^{(n-1)}, \mathbf{Z}^{(n-1)})\right| / \mathrm{OF}(\mathbf{w}^{(n-1)}, \mathbf{Z}^{(n-1)}) < \varepsilon$ or $n \geq n_{\max}$, terminate. Otherwise, update $n \leftarrow n + 1$ and jump to Step 3.

Problem (34) for a sufficiently small value of penalty factor κ. The maximum value of Problem (34) serves as the lower bound for the optimal value of Problem (32). The overall AO algorithm proposed is summarized in Algorithm 1. By iteratively solving Problem (25) and Problem (34) optimally in Step 3 and Step 4 in Algorithm 1, the transmit power can be monotonically reduced with guaranteed convergence.

V. SIMULATION RESULTS

A. Simulation Setup

One appealing benefit of deploying an IRS in secure wireless systems is to establish favorable communication links for legitimate user that is blocked by obstacles. We consider a scenario where the direct links from the AP to the legitimate user and evesdroppers are blocked. The simulated system model is shown in Fig. 2. The Alice is located at (0,10) m. The IRS is installed at a height of 25 m. The Bob and Eves can be randomly distributed on the x axis.

The channel matrix between the Alice and the IRS is modeled as $\mathbf{G}_{ar} \in \mathbb{C}^{M \times N_t}$, which is

$$\mathbf{G}_{ar}^T = \sqrt{L_0 d_{ar}^{-\alpha_{ar}}} \left(\sqrt{\frac{\beta_{ar}}{1 + \beta_{ar}}} \mathbf{G}_{ar}^{LOS} + \sqrt{\frac{1}{1 + \beta_{ar}}} \mathbf{G}_{ar}^{NLOS} \right), \tag{35}$$

where $L_0 = \left(\frac{\lambda_c}{4\pi}\right)^2$ is a constant with λ_c being the wavelength of the center frequency of the information carrier. The distance between the AP and the IRS is denoted by d_{ar}, while α_{ar} denotes the corresponding path loss exponent. The small-scale fading is assumed to be Ricean fading with Ricean factor β_{ar}. The $\mathbf{G}_{ar}^{LOS}$ denotes the light of sight (LoS) component of the Alice-IRS channel.
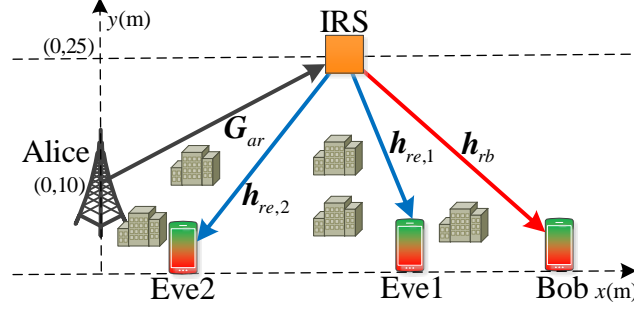
Fig. 2. The simulated secure communication scenario

By assuming that the antennas at the Alice and the passive reflecting elements at the IRS are both arranged in a uniform linear array (ULA), the $\mathbf{G}_{ar}^{LOS}$ can be modeled as $\mathbf{G}_{ar}^{LOS} = \mathbf{c}\mathbf{d}^H$, where $\mathbf{c} = [c_1, c_2, \cdots, c_{N_t}]^T$ denotes the transmit steering vector of the Alice, and $\mathbf{d} = [d_1, d_2, \cdots, d_M]^T$ denotes the receive steering vector of the IRS. The mth elements of $\mathbf{c}$ and $\mathbf{d}$ are written as

$$c_m = \exp(j2\pi \frac{d_a}{\lambda_c}(m-1)\sin\theta_a), \tag{36a}$$

$$d_m = \exp(j2\pi \frac{d_r}{\lambda_c}(m-1)\sin\theta_r), \tag{36b}$$

where d_a and d_r are respectively the element intervals at Alice and the IRS; θ_a represents the elevation angle of the LoS link from Alice; θ_r represents the elevation angle of the LoS link to the IRS. We set $\frac{d_a}{\lambda_c} = \frac{d_r}{\lambda_c} = 0.5$, $\theta_a = \tan^{-1}(\frac{y_r - y_a}{x_r - x_a})$, and $\theta_r = \pi - \theta_a$. $\mathbf{G}_{ar}^{NLOS}$ denotes the non-LoS (NLoS) component of the Alice-IRS channel, which is modeled as Rayleigh fading. The channels of the IRS-Bob link and IRS-Eve link are modeled similarly, where both the LoS component and NLoS component exist simultaneously.

For the statistical cascaded CSI error model, the variance matrix of $\mathbf{g}_{ce,k} = \mathrm{vec}(\triangle \mathbf{G}_{ce,k})$ is defined as $\mathbf{\Sigma}_{e,k} = \varepsilon_{g,k}^2 \mathbf{I}$, where $\varepsilon_{g,k}^2 = \delta_{g,k}^2 \left\| \mathrm{vec}(\bar{\mathbf{G}}_{ce,k}) \right\|_2^2$. $\delta_{g,k}^2 \in [0,1)$ is the normalized CSI error, which measures the relative amount of CSI uncertainties. The system parameters used in the following simulations are listed in Table I.

B. Benchmark Schemes

We demonstrate the advantage of the proposed AO algorithm by comparing its performance with the following benchmark schemes:

TABLE I

SIMULATION PARAMETERS

Carrier center frequency	2.4GHz
Path loss exponents for Alice-IRS channels α_{ar}, IRS-Bob channels α_{rb}, IRS-Eve channels α_{re},	2
Rician factor for Alice-IRS channel, β_{ar}	5
Rician factor for IRS-Bob channel, β_{rb}	5
Rician factor for IRS-Eve channel, β_{re}	5
Noise power at Bob and Eves, σ_b^2, $\sigma_{e,k}^2$	-75dBm
Penalty factor, κ	5×10^{-8}
Convergence tolerance, ε	10^{-3}
Outage probability, ρ_k	0.05

- Random-MRT: It performs maximum ratio transmission (MRT) based beamforming design, i.e., $\mathbf{w} = \sqrt{p_w}\frac{\hat{\mathbf{h}}_b}{\|\hat{\mathbf{h}}_b\|} = \sqrt{p_w}\frac{\mathbf{G}_{ar}^H\boldsymbol{\Phi}^H\mathbf{h}_{rb}}{\|\hat{\mathbf{h}}_b\|}$, where p_w is the power allocated to legitimate user Bob. It applies an isotropic AN [36], i.e., the AN covariance matrix is chosen as $\mathbf{Z} = p_z\mathbf{P}_{\hat{\mathbf{h}}_b}^{\perp}$, where $\mathbf{P}_{\hat{\mathbf{h}}_b}^{\perp} = \mathbf{I}_{N_t} - \hat{\mathbf{h}}_b\hat{\mathbf{h}}_b^H / \left\|\hat{\mathbf{h}}_b\right\|^2$ is the orthogonal complement projector of $\hat{\mathbf{h}}_b$, and p_z is the power invested on AN. Both the beamforming precoder $\mathbf{w}$ and the AN covariance matrix $\mathbf{Z}$ rely on the phase shifts $\boldsymbol{\Phi}$ of IRS. For Random-MRT schemes, we assume the phase shifts $\boldsymbol{\Phi}$ of IRS is randomly chosen. The allocated power p_w to beamforming and the allocated power p_z to AN are optimized to satisfy the secrecy constraints in Problem (25).

- Optimized-MRT: Based on the MRT beamforming and isotropic AN, the phase shifts $\boldsymbol{\Phi}$ of IRS is obtained by using the proposed method. The allocated power p_w to beamforming and the allocated power p_z to AN are optimized to satisfy the secrecy constraints in Problem (25).

- Random-IRS: It does not optimize the phase shifts of IRS, and the phase shifts of IRS $\boldsymbol{\Phi}$ is randomly selected. The beamforming matrix $\mathbf{W}$ and AN covariance matrix $\mathbf{Z}$ are optimized by solving Problem (25).

The Random-MRT and Optimized-MRT schemes only exploit the CSI of Bob by assuming that the CSI of Eves is unknown, while the Random-IRS scheme and the proposed algorithm exploit the CSI of both Bob and Eves to realize robust transmission design. The Optimized-MRT is compared with the Random-MRT to demonstrate the importance of the optimization of IRS phase shifts. For Random-IRS scheme, the phase shifts of IRS $\boldsymbol{\Phi}$ are not optimized, and only the beamforming matrix $\mathbf{W}$ and AN covariance matrix $\mathbf{Z}$ are optimized robustly, while the proposed algorithm
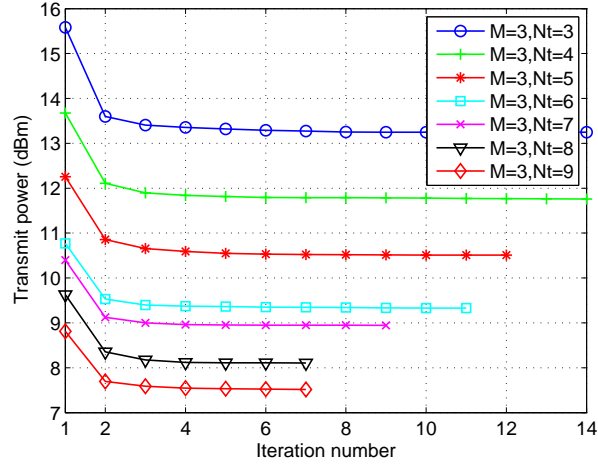
(a) Convergence of the proposed algorithm with different values of N_t.
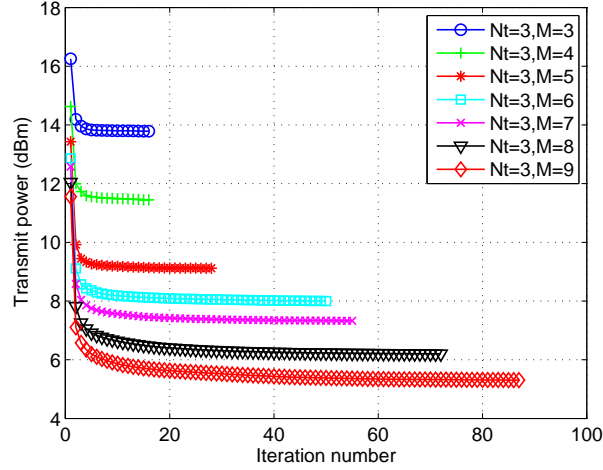
(b) Convergence of the proposed algorithm with different values of M.

Fig. 3. Convergence of the proposed algorithm with $\log \gamma = 3$ bit/s/Hz and $\log \beta = 1$ bit/s/Hz, $K = 2$, $\delta_{g,k}^2 = 0.0001$, $\forall k$. The location of AP is (0, 10) m, the location of IRS is (100, 25) m, the location of Bob is (180, 0) m, and the locations of Eves are (160, 0) m and (170, 0) m.

optimizes these variables jointly. By comparing the proposed algorithm with the Random-IRS scheme, the importance of the optimization of the IRS phase shifts in robust transmission design is verified.

C. Convergence Analysis

The convergence of the proposed method with different antenna numbers of transmitter and different numbers of IRS phase shifts are investigated in Fig. 3. As observed from Fig. 3(a),

TABLE II

TIME COST

Versus	Average CPU time (secs) in Fig. 3(a)						
M	$M=3$	$M=4$	$M=5$	$M=6$	$M=7$	$M=8$	$M=9$
$N_t=3$	2.0932	2.9118	6.5124	9.4720	13.1437	18.5433	20.9004
Versus	Average CPU time (secs) in Fig. 3(b)						
N_t	$N_t=3$	$N_t=4$	$N_t=5$	$N_t=6$	$N_t=7$	$N_t=8$	$N_t=9$
$M=3$	1.6999	1.7960	1.9247	1.9806	2.2405	2.3101	2.7319
Versus	Average CPU time (secs) in Fig. 4(a)						
$\log\gamma$ (bit/s/Hz)	$\log\gamma$=5.5	$\log\gamma$=5	$\log\gamma$=4.5	$\log\gamma$=4	$\log\gamma$=3.5	$\log\gamma$=3	$\log\gamma$=2.5
$\log\beta$=2 (bit/s/Hz)	25.7724	26.7880	29.8244	36.3530	44.6590	67.7409	97.2034
Versus	CPU time (secs) in Fig. 4(b)						
$\log\beta$ (bit/s/Hz)	$\log\beta$=1.5	$\log\beta$=2	$\log\beta$=2.5	$\log\beta$=3	$\log\beta$=3.5	$\log\beta$=4	$\log\beta$=4.5
$\log\gamma$=4.7 (bit/s/Hz)	24.4419	28.2168	30.1735	37.1616	48.4290	66.7990	90.5877

the proposed algorithm is likely to converge with fewer iterations when the number of transmit antennas increases. With increased N_t, the dimension of optimization variables $\mathbf{W}$ and $\mathbf{Z}$ in the CVX problem of each iteration becomes large, which requires more computation time for each iteration. Thus, the computation time consumed by the proposed algorithm with a larger N_t still increases even with fewer iterations. Fig. 3(b) shows the convergence of the proposed algorithm with different values of M. It is seen that the proposed algorithm is likely to converge with more iterations when the number of IRS elements increases. Since the quality of the cascaded channel relies on the phase shifts of the IRS, larger M will bring more degrees of freedom to adjust the cascaded channel, thus more iterations are required for the fine adjustment. With increased M, the dimension of the optimization variable $\boldsymbol{\Phi}$ in the CVX problem of each iteration becomes large, thus the computation time of the proposed algorithm increases with M. The average central processing unit (CPU) running time of the proposed algorithm versus N_t and M with the parameters in Fig. 3(a) and Fig. 3(b) is shown in Table II. The data is obtained by using a computer with a 3.40GHz i7-6700 CPU and 16GB RAM. It is observed from Table II that the average CPU running time required by our proposed algorithm increases with either N_t or M. The average CPU time increases with N_t less slowly than with M, this is because the required iterations decrease with N_t. The convergence of the proposed algorithm for different values of $\log\gamma$ and $\log\beta$ is shown in Fig. 4. It is demonstrated that more iterations are required by decreasing the minimum channel capacity
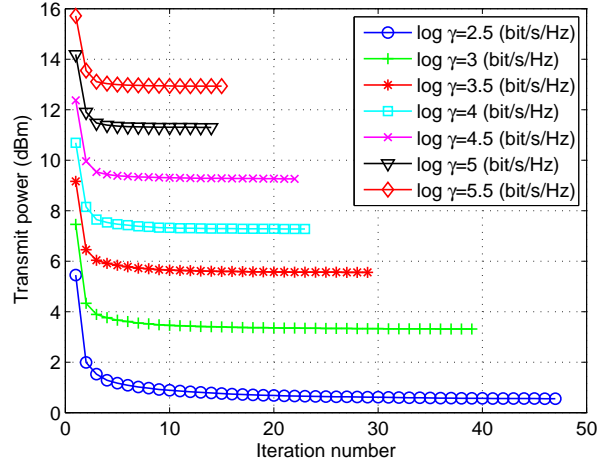
(a) Convergence of the proposed algorithm for different values of $\log \gamma$ for $\log \beta = 2$ bit/s/Hz.
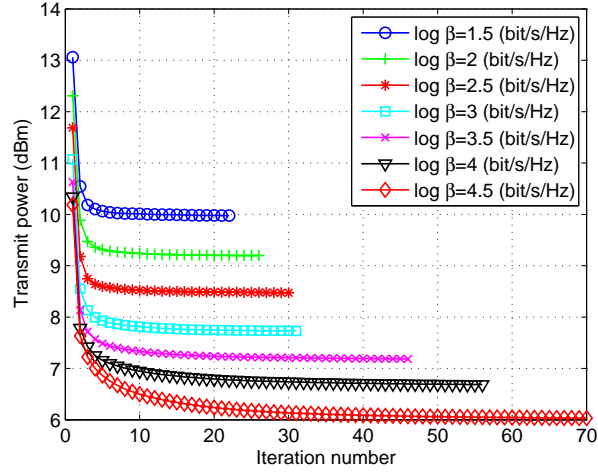
(b) Convergence of the proposed algorithm for different values of $\log \beta$ for $\log \gamma = 4.7$ bit/s/Hz.

Fig. 4. Convergence of the proposed algorithm with $N_t = M = 6$, $K = 2$, $\delta_{g,k}^2 = 0.0001$, $\forall k$. The location of AP is (0, 10) m, the location of IRS is (50, 25) m, the location of Bob is (180, 0) m, and the locations of Eves are (20, 0) m and (10, 0) m.

$\log \gamma$ of the legitimate user and increasing the maximum tolerable channel capacity $\log \beta$ of the eavesdroppers. Since the dimension of the CVX problem in each iteration is not changed with different $\log \gamma$ and $\log \beta$, more iterations in Fig. 4 signify more computation time. The average CPU running time of the proposed algorithm versus $\log \gamma$ and $\log \beta$ with the parameters in Fig. 4(a) and Fig. 4(b) is shown in Table II. It is found in Table II that more CPU time is required for

the small value of secrecy rate.

D. Transmit Power Versus the Minimum Channel Capacity of the Legitimate User

In Fig. 5, we show the transmit power versus the minimum channel capacity $\log \gamma$ of the legitimate user, while limiting the information leakage to the potential eavesdroppers as $\log \beta = 2$ bit/s/Hz. From Fig. 5, we find that the transmit power increases monotonically with the minimum channel capacity of the Bob. This is because more transmit power is required to satisfy the increased data rate of Bob. By comparing our proposed method with the other benchmark schemes, it is seen that the power budget of the proposed method is lower than the other benchmark schemes. In particular, the MRT schemes only exploit the channel information of Bob, thus their power consumptions stay at a high level. The optimized MRT scheme is better than the random MRT scheme, because the IRS-relied cascaded channel has been greatly improved by optimizing the phase shifts of IRS. The Random-IRS scheme consumes more power than the proposed method, which demonstrates the necessity of optimizing the phase shifts of IRS. Fig. 5 reveals that the security communication in LoS blocked environment can be realized by deploying an IRS, and the phase shifts of IRS should be optimized.
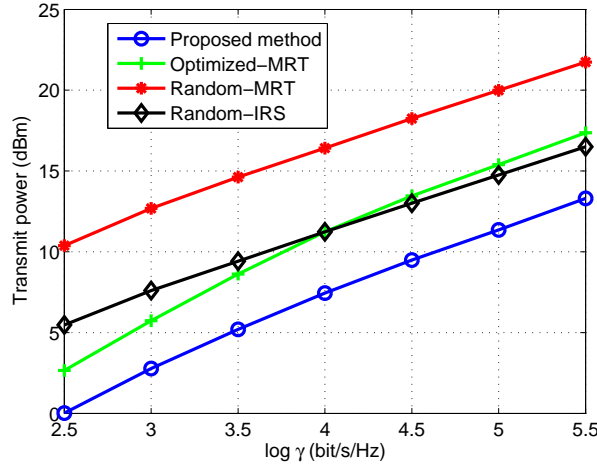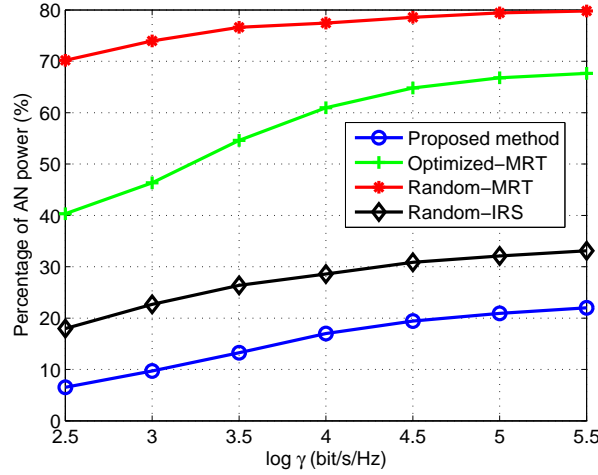

Fig. 5.   Transmit power versus the minimum channel capacity $\log \gamma$ of the legitimate user with $N_t = M = 6$, $K = 2$, and $\delta_{g,k}^2 = 0.0001$, $\forall k$. The location of AP is (0, 10) m, the location of IRS is (50, 25) m, the location of Bob is (180, 0) m, and the locations of Eves are (20, 0) m and (10, 0) m.

The percentage of AN power in the total transmit power versus the minimum channel capacity $\log \gamma$ of the legitimate user is shown in Fig. 6. When $\log \gamma$ is small, a small portion of transmit power is allocated to transmit AN to deteriorate the achievable rates of Eves. When $\log \gamma$ increases,

more transmit power should be emitted, thus the data rates of both Bob and Eve increase. To control the data rates of Eves under the threshold $\log \beta$, more AN power should be emitted to interfere the Eves. By comparing the proposed method with the other benchmark schemes, we find that the Optimized-MRT and Random-MRT schemes have much higher AN power percentage than the proposed method and the Random-IRS scheme. By optimizing the IRS phase shifts, the AN power percentage of the proposed method further reduces compared with the Random-IRS scheme.

Fig. 6. Percentage of AN power versus the minimum channel capacity $\log \gamma$ of the legitimate user with $N_t = M = 6$, $K = 2$, and $\delta_{g,k}^2 = 0.0001$, $\forall k$. The location of AP is (0, 10) m, the location of IRS is (50, 25) m, the location of Bob is (180, 0) m, and the locations of Eves are (20, 0) m and (10, 0) m.

E. Transmit Power Versus the Maximum Tolerable Channel Capacity of the Eavesdroppers

Fig. 7 depicts the transmit power versus the maximum tolerable channel capacity $\log \beta$ of the Eves by assuming that the minimum channel capacity of the legitimate user is $\log \gamma$=4.7 bit/s/Hz. As shown in Fig. 7, when $\log \beta$ becomes large, more information leakage is allowed for the Eves, and less AN noise power is required. Thus the transmit power decreases versus the increased maximum tolerable channel capacity $\log \beta$ of Eves. When $\log \beta$ becomes larger, the consumed transmit power of the Random-MRT scheme approaches that of the Random-IRS scheme, while the consumed transmit power of the Optimized-MRT scheme approaches that of the proposed algorithm. This is because, when more information leakage to Eves is allowed, the importance of robust transmission design by exploiting the Eves' CSI is weakened. By comparing with other benchmark schemes, the proposed method consumes the lowest transmit power, which confirms the effectiveness of the proposed algorithm.
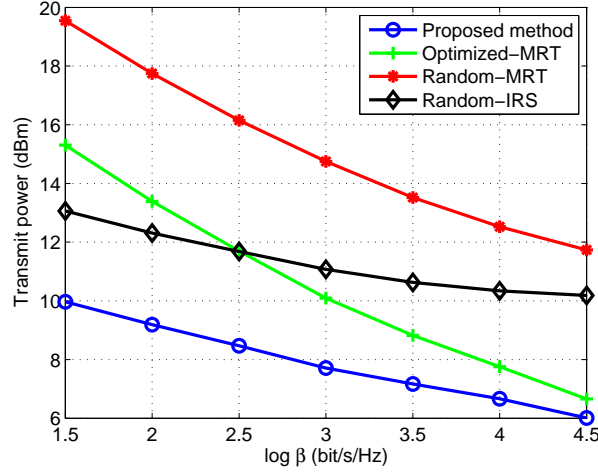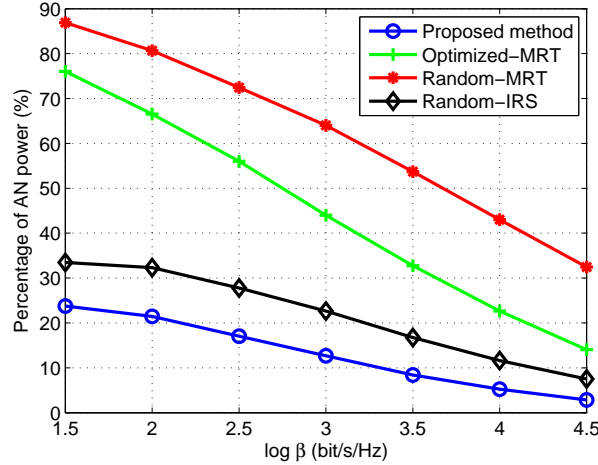
Fig. 7. Transmit power versus the maximum tolerable channel capacity $\log \beta$ of the eavesdropper with $N_t = M = 6$, $K = 2$ and $\delta^2_{g,k} = 0.0001$, $\forall k$. The location of AP is $(0, 10)$ m, the location of IRS is $(50, 25)$ m, the location of Bob is $(180, 0)$ m, and the locations of Eves are $(20, 0)$ m and $(10, 0)$ m.

Fig. 8. Percentage of AN power versus the maximum channel capacity $\log \beta$ of the eavesdropper with $N_t = M = 6$, $K = 2$ and $\delta^2_{g,k} = 0.0001$, $\forall k$. The location of AP is $(0, 10)$ m, the location of IRS is $(50, 25)$ m, the location of Bob is $(180, 0)$ m, and the locations of Eves are $(20, 0)$ m and $(10, 0)$ m.

The percentage of AN power in the total transmit power versus the maximum tolerable channel capacity $\log \beta$ of the Eves is depicted in Fig. 8. When $\log \beta$ becomes large, the percentages of AN power for all methods reduce. It is shown that when $\log \beta$ is small, a large portion of the transmit power is allocated to transmit AN to deteriorate the achievable rates of the potential eavesdroppers, and therefore, there is less power transmitted for legitimate user. As $\log \beta$ increases, the constraints on the performance of the Eves are relaxed, and more transmit power is allocated to beamform to

Bob. The percentages of AN power of both Random-MRT and Optimized MRT schemes are higher than those of the Random-IRS and the proposed method. This is because the channel information of Eves is not utilized for the MRT schemes. The percentage of AN power for the proposed method is the lowest, which demonstrates the effectiveness of the robust transmission design.

F. Transmit Power Versus the Number of IRS Elements

We further examine the minimum transmit power consumption versus different numbers of IRS elements in Fig. 9. The maximum tolerable channel capacity of the Eves is $\log \beta = 1$ bit/s/Hz. The required minimum data rate for the Bob is set as $\log \gamma = 3$ bit/s/Hz. The transmit power is reduced when the IRS element number M increases. To enhance the security, the phase shifts of the IRS can be optimized to help the data transmission for Bob while degrade the data transmission for Eves. A large value of M will bring more degrees of freedom to adjust the cascaded channels, thus less transmit power is required to guarantee the data transmission for Bob and impair the data transmission for Eves. The transmit power of the Optimized-MRT scheme and the proposed
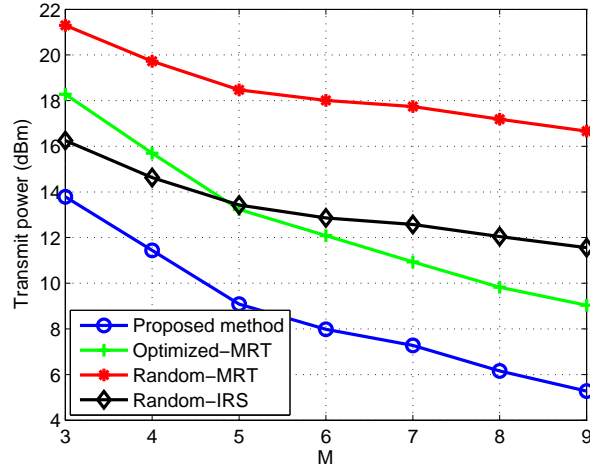

Fig. 9. Transmit power versus the IRS element number M with $N_t = 3$, $K = 2$, $\delta_{g,k}^2 = 0.0001$, $\forall k$, $\log \beta = 1$ bit/s/Hz and $\log \gamma = 3$ bit/s/Hz. The location of AP is (0, 10) m, the location of IRS is (100, 25) m, the location of Bob is (180, 0) m, and the locations of Eves are (160, 0) m and (170, 0) m.

algorithm decreases more quickly than that of the Random-MRT scheme and Random-IRS scheme, which shows that optimizing the phase shifts of IRS can reduce the transmit power effectively. The transmit power of the Random-MRT and Random-IRS schemes decreases slowly when M is large, which shows that the transmit power cannot be effectively reduced without IRS phase shift

optimization. Compared with the other benchmark schemes, the proposed algorithm requires the lowest transmit power, which validates the superiority of the proposed algorithm.

G. Transmit Power Versus the Number of Transmit Antennas

We further examine the transmit power consumption versus different number of transmit antennas N_t in Fig. 10. The maximum tolerable channel capacity of the Eves is $\log \beta = 1$ bit/s/Hz. The required minimum data rate for the Bob is set as $\log \gamma = 3$ bit/s/Hz. Fig. 10 shows that the transmit power of all schemes reduces when the number of transmit antennas increases. A large value of N_t helps improve the channels for both the Bob and Eves. Then, the robust beamforming design for Bob and AN design for Eves are easier to achieve with a larger N_t. Thus, the required transmit power reduces with increased N_t. Compared with the Random-MRT scheme and Optimized-MRT scheme, the required transmit power of the Random-IRS scheme and proposed algorithm decreases more quickly with N_t. This is because, the MRT schemes do not exploit the Eves' CSI, while the Random-IRS scheme and the proposed algorithm exploit the Eve's CSI robustly. The required transmit power of Random-IRS scheme is further reduced by the proposed algorithm, which validate the effectiveness of the proposed robust transmission design.
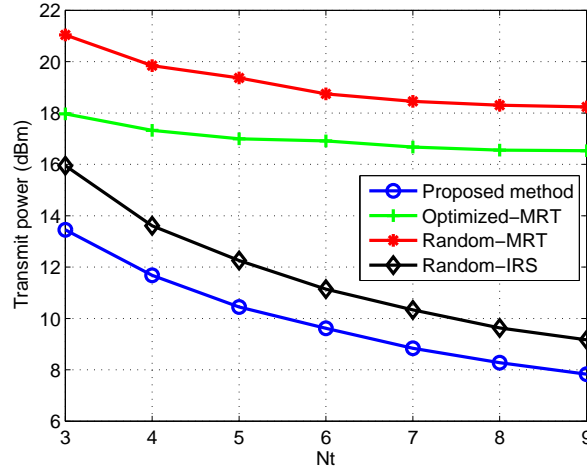

Fig. 10. Transmit power versus transmit antenna number N_t with $M = 3$, $K = 2$, $\delta_{g,k}^2 = 0.0001$, $\forall k$, $\log \beta = 1$ bit/s/Hz and $\log \gamma = 3$ bit/s/Hz. The location of AP is (0, 10) m, the location of IRS is (100, 25) m, the location of Bob is (180, 0) m, and the locations of Eves are (160, 0) m and (170, 0) m.

H. Transmit Power Versus CSI Uncertainty

Fig. 11 shows the transmit power versus the normalized CSI error variance δ^2, where the normalized CSI errors of different eavesdroppers are assumed to be identical, i.e., $\delta_{g,k} = \delta$, $\forall k$. As can be observed, for the proposed scheme and the other benchmark schemes, the transmit power increases as the quality of the CSI degrades. When the CSI errors of Eves' channels increase, more AN power is required to interfere Eves for information leakage limitation, thus the allocated power for beamforming must also increase to guarantee Bob's data requirement. This leads to the increase of total transmit power with deteriorating channel. In comparison to other three benchmark schemes, the required transmit power of the proposed method has been significantly reduced. Both the Random MRT and Optimized MRT schemes need much more transmit power to impair the Eves, which shows that the utilization of Eves' CSI can help reduce the transmit power. The Random IRS scheme also needs much more transmit power than the proposed method, which indicates the effectiveness of the optimization on the IRS phase shifts in the robust transmission design. It can also be found from Fig. 11 that the transmit power of the Random MRT and Optimized MRT schemes increases more quickly than the proposed method, which shows that they are more sensitive to the CSI errors, and that the proposed method is more robust with respect to the CSI error.
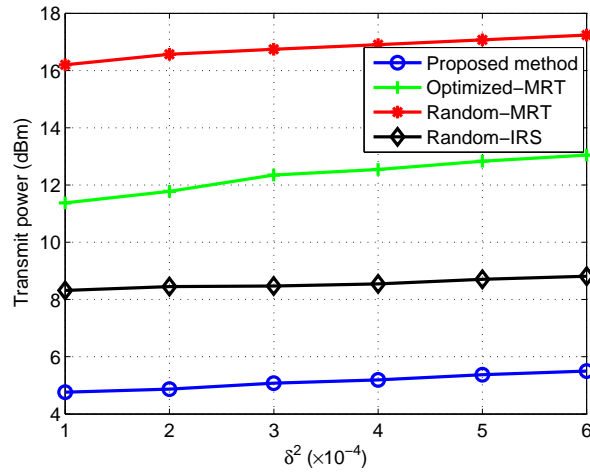

Fig. 11. Transmit power versus normalized CSI error variance δ^2 with $N_t = M = 6$, $K = 2$, $\log \beta = 1$ bit/s/Hz and $\log \gamma = 3$ bit/s/Hz. The location of AP is (0, 10) m, the location of IRS is (100, 25) m, the location of Bob is (180, 0) m, and the locations of Eves are (160, 0) m and (170, 0) m.

Fig. 12 gives the percentage of AN power in the total transmit power versus the normalized CSI error variance δ^2. It is shown in Fig. 12 that the percentage of AN power increases with CSI
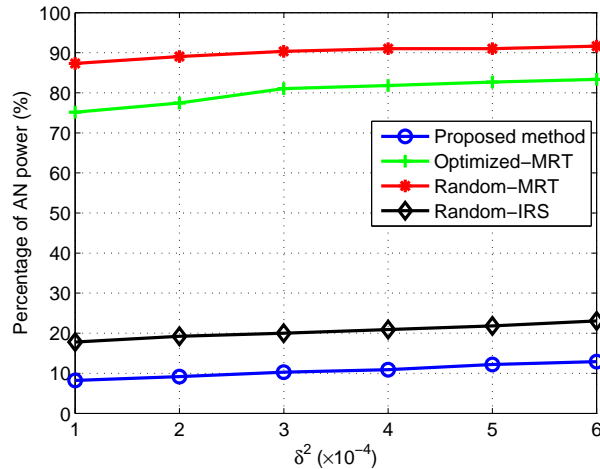
Fig. 12. Percentage of AN power versus normalized CSI error variance δ^2 with $N_t = M = 6$, $K = 2$, $\log \beta = 1$ bit/s/Hz and $\log \gamma = 3$ bit/s/Hz. The location of AP is $(0, 10)$ m, the location of IRS is $(100, 25)$ m, the location of Bob is $(180, 0)$ m, and the locations of Eves are $(160, 0)$ m and $(170, 0)$ m.

estimation error. When the quality of the CSI degrades, more AN power is required to interfere the eavesdroppers. The percentages of AN power in the total transmit power for the Optimized MRT and Random MRT schemes are more than 70%, while the percentages of AN power in the total transmit power for the proposed method and Random IRS scheme are less than 20%. Without the Eves's CSI, more AN power is required to impair the Eves. On the contrary, by exploiting the Eves' CSI robustly, the AN interference becomes more effective, thus less percentage of AN power is required. Compared with the Random IRS scheme, less AN power percentage is required for the proposed method, which demonstrates that the optimization of IRS phase shifts helps impair the Eves' channel, thus makes less AN power interferes the Eves more effectively.

VI. CONCLUSION

In this paper, we designed the outage constrained robust transmission in the secure IRS-aided wireless communications. The statistical CSI error of cascaded IRS channel was taken into consideration for the first time in secure communications, and the OC-PM problem was formulated to minimize the transmit power by jointly optimizing the transmit beamforming vector, AN covariance, and IRS phase shifts. To solve it, an AO based method was proposed, where the optimization variables are optimized alternately. The BTI was utilized to tackle the chance constraint. The SDR scheme was utilized when designing the beamforming vector and IRS phase shifts. Specifically, the nonconvex unit modulus constrained was handled by a penalty method. Simulation results have

verified the effectiveness of IRS on enhancing the physical layer security of wireless communications. The robustness of the proposed method has also been confirmed when the statistical CSI error exists, which is meaningful. The superiority of the proposed method over the benchmark methods has also been validated.

REFERENCES

[1] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2019.

[2] J. Zhao and Y. Liu, "A survey of intelligent reflecting surfaces (IRSs): Towards 6G wireless communication networks." [Online]. Available: https://arxiv.org/abs/1907.04789

[3] T. J. Cui, M. Q. Qi, X. Wan, J. Zhao, and Q. Cheng, "Coding metamaterials, digital metamaterials and programmable metamaterials," *Light: Science & Applications*, vol. 3, no. 10, pp. 218–218, 2014.

[4] K. Ntontin, M. Di Renzo, J. Song, F. Lazarakis, J. de Rosny, D.-T. Phan-Huy, O. Simeone, R. Zhang, M. Debbah, G. Lerosey *et al.*, "Reconfigurable intelligent surfaces vs. relaying: Differences, similarities, and performance comparison." [Online]. Available: https://arxiv.org/abs/1908.08747

[5] X. Yu, D. Xu, and R. Schober, "MISO wireless communication systems via intelligent reflecting surfaces," in *2019 IEEE/CIC International Conference on Communications in China (ICCC)*, 2019, pp. 735–740.

[6] Y. Yang, B. Zheng, S. Zhang, and R. Zhang, "Intelligent reflecting surface meets OFDM: Protocol design and rate maximization," *IEEE Transactions on Communications*, vol. early access, pp. 1–1, 2020.

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

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

[9] H. Guo, Y.-C. Liang, J. Chen, and E. G. Larsson, "Weighted sum-rate optimization for intelligent reflecting surface enhanced wireless networks." [Online]. Available: https://arxiv.org/abs/1905.07920

[10] Q.-U.-A. Nadeem, A. Kammoun, A. Chaaban, M. Debbah, and M.-S. Alouini, "Large intelligent surface assisted MIMO communications." [Online]. Available: https://arxiv.org/abs/1903.08127

[11] G. Zhou, C. Pan, H. Ren, K. Wang, W. Xu, and A. Nallanathan, "Intelligent reflecting surface aided multigroup multicast MISO communication systems." [Online]. Available: https://arxiv.org/abs/1909.04606

[12] C. Pan, H. Ren, K. Wang, W. Xu, M. Elkashlan, A. Nallanathan, and L. Hanzo, "Intelligent reflecting surface for multicell MIMO communications." [Online]. Available: https://arxiv.org/abs/1907.10864

[13] C. Pan, H. Ren, K. Wang, M. Elkashlan, A. Nallanathan, J. Wang, and L. Hanzo, "Intelligent reflecting surface enhanced MIMO broadcasting for simultaneous wireless information and power transfer." [Online]. Available: https://arxiv.org/abs/1908.04863

[14] T. Bai, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, "Latency minimization for intelligent reflecting surface aided mobile edge computing." [Online]. Available: https://arxiv.org/abs/1910.07990

[15] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for irs-assisted full-duplex cognitive radio systems." [Online]. Available: https://arxiv.org/abs/2003.07467

[16] 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 Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[17] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on signal processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[18] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Robust and secure resource allocation for full-duplex MISO multicarrier NOMA systems," *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4119–4137, 2018.

[19] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2009.

[20] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces." [Online]. Available: https://arxiv.org/abs/1904.09573

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

[22] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, 2019.

[23] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[24] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication via joint beamforming and jamming." [Online]. Available: https://arxiv.org/abs/1907.12839

[25] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for secure IRS-assisted multiuser MISO systems." [Online]. Available: https://arxiv.org/abs/1907.03085

[26] A. Taha, M. Alrabeiah, and A. Alkhateeb, "Enabling large intelligent surfaces with compressive sensing and deep learning." [Online]. Available: https://arxiv.org/abs/1904.10136

[27] S. Zhang and R. Zhang, "Capacity characterization for intelligent reflecting surface aided MIMO communication." [Online]. Available: https://arxiv.org/abs/1910.01573

[28] Z. Zhou, N. Ge, Z. Wang, and L. Hanzo, "Joint transmit precoding and reconfigurable intelligent surface phase adjustment: A decomposition-aided channel estimation approach." [Online]. Available: https://www.researchgate.net/publication/337824343

[29] Z. Wang, L. Liu, and S. Cui, "Channel estimation for intelligent reflecting surface assisted multiuser communications: Framework, algorithms, and analysis." [Online]. Available: https://arxiv.org/abs/1912.11783

[30] P. Wang, J. Fang, H. Duan, and H. Li, "Compressed channel estimation and joint beamforming for intelligent reflecting surface-assisted millimeter wave systems." [Online]. Available: https://arxiv.org/abs/1911.07202

[31] J. Chen, Y.-C. Liang, H. V. Cheng, and W. Yu, "Channel estimation for reconfigurable intelligent surface aided multi-user MIMO systems." [Online]. Available: https://arxiv.org/abs/1912.03619

[32] G. Zhou, C. Pan, H. Ren, K. Wang, M. Di Renzo, and A. Nallanathan, "Robust beamforming design for intelligent reflecting surface aided MISO communication systems." [Online]. Available: https://arxiv.org/abs/1911.06237

[33] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces." [Online]. Available: https://arxiv.org/abs/1912.01497

[34] 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." [Online]. Available: https://arxiv.org/abs/2001.07054

[35] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Transactions on Signal Processing*, vol. 62, no. 21, pp. 5690–5705, 2014.

[36] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2010.