Robust Secure Transmission for IRS-Aided NOMA Networks with Hybrid Beamforming

Jifa Zhang, Wei Wang, Jie Tang, Senior Member, IEEE, Nan Zhao, Senior Member, IEEE,
Kai-Kit Wong, Fellow, IEEE, and Xianbin Wang, Fellow, IEEE

Abstract—Due to its capability of channel reconfiguration and enhancement, intelligent reflecting surface (IRS) can be introduced to improve the secrecy rate of non-orthogonal multiple access (NOMA) networks. However, the cost and hardware complexity of full-digital beamforming in existing related studies are high, especially for the systems with massive antennas. This paper studies the robust secure transmission for IRS-aided NOMA networks with cost-effective hybrid beamforming. Specifically, we deploy an IRS to assist the secure transmission from a base station with cost-effective hybrid beamforming to a cell-center user (U1) and a cell-edge user (U2), with the existence of a potential eavesdropper. Two schemes are proposed for guaranteeing the secure transmission of U1 with the perfect and imperfect channel state information (CSI), respectively. With the perfect CSI, the secrecy rate of U1 is maximized subject to the constant modulus constraint and the quality of service (QoS) constraint of U2 via optimizing the hybrid beamforming and phase shifts of IRS. With the imperfect CSI, the achievable rate at U1 is maximized, satisfying its worst-case eavesdropping rate constraint, the constant modulus constraint and the QoS constraint of U2. Because of the non-convexity, we first decompose each problem into two subproblems, respectively, then, the subproblems are solved via the penalty-based algorithm and the successive convex approximation. Simulation results verify that the two proposed schemes have higher energy efficiency and can boost the security of IRS-aided NOMA networks with perfect and imperfect CSI, respectively.

Index Terms—Hybrid beamforming, IRS, NOMA, physical layer security.

I. INTRODUCTION

As a promising technique, intelligent reflecting surface (IRS) can boost the performance of wireless communications via reconfiguring wireless channels intelligently [2]. Specifically, IRS consists of enormous low-cost passive reflection elements integrated on a plane, and passive beamforming can be performed via coordinating the phase shift at every reflection element. In addition, IRS can outperform the conventional active relays in hardware complexity, energy consumption and cost. Cho et al. in [4] deployed multiple IRSs to decrease the power consumption of UAV subject to the data constraint for each user. Thanks to the enhanced capacity of desired channels through reconfiguration, IRS can boost the security of wireless communications [5]–[10]. Guan et al. in [5] maximized the secrecy rate via optimizing the transmit beamforming and the phase shifts of IRS. Considering the hardware impairment at base station (BS), Zhou et al. in [6] proposed a secrecy rate maximization scheme for IRS-aided systems. Wu et al. in [7] maximized the secrecy energy efficiency (SEE) of IRS-aided cognitive radio networks. Pang et al. in [8] studied the secure transmission for IRS-aided unmanned aerial vehicle (UAV) networks. Yu et al. in [9] proposed a robust transmission scheme to guarantee the security of IRS-aided wireless communications with the imperfect eavesdropping channel state information (CSI). Xu et al. in [10] deployed an IRS to enhance the security of satellite-ground integrated networks, and the signal-to-interference-plus-noise ratio (SINR) of eavesdropper was minimized via the joint design of the transmit beamforming and IRS phase shift-matrix.

With the growing number of wireless devices, orthogonal multiple access (OMA) can not satisfy the increasing demand for wireless connections due to limited radio resources. Non-orthogonal multiple access (NOMA) can outperform the conventional OMA in spectrum efficiency via sharing the same resource among all users [11]. For instance, the signals for all power-domain NOMA users are superposed at the transmitter, and then transmitted over a single resource. Then, successive interference cancellation (SIC) is adopted by every user to decode its own signal [12]. To ensure user fairness of power-domain NOMA, user with weaker channel gain is allocated with more transmit power, which makes it more vulnerable to eavesdropping. Owing to its capability of channel reconfiguration and enhancement, IRS can be integrated with NOMA to further improve the security and spectrum efficiency [13]–[17]. In [13], Zhang et al. proposed a robust transmission scheme to guarantee the security of IRS-aided NOMA networks with the imperfect eavesdropping CSI. Unknowing the eavesdropping CSI, Wang et al. in [14] proposed a transmission scheme to improve the security of IRS-aided NOMA systems. Zeng et al. in [15] maximized the sum achievable rate of IRS-
aided NOMA networks via jointly designing the active and passive beamforming. In [16], an IRS was employed by Zhang et al. to improve the security of NOMA networks, and the minimum secrecy rate was maximized. Xie et al. in [17] investigated the energy efficiency (EE) of multi-IRS aided multi-cluster NOMA networks and minimized the transmit power via designing the beamforming and the phase-shift matrix at every IRS.

All the above works assume that the BS adopts the full-digital beamforming (FDB), in which each antenna is connected to a power-hungry radio frequency (RF) chain. Although FDB has better performance, it is not cost-effective to deploy FDB in the systems with massive antennas because of high hardware complexity and power consumption [18]. On the contrary, the hybrid beamforming (HBF) and analog beamforming consist of lots of low-cost phase shifters and much fewer RF chains. Therefore, HBF and analog beamforming have the advantages of low hardware complexity, low power consumption and easy deployment, which are more suitable for the deployment of massive antennas. In [19], Ning et al. investigated the secure transmission for the systems with massive antennas via low-cost analog beamforming, and maximized the secrecy rate via optimizing the analog beamforming. Ding et al. in [20] introduced the finite-resolution analog beamforming to NOMA networks to decrease the cost. Xiao et al. in [21] employed the analog beamforming for the downlink NOMA network, and the sum rate was maximized. Compared with analog beamforming and FDB, HBF can achieve a better balance between performance and complexity, thus has been widely investigated. Hong et al. in [22] maximized the transmission rate of IRS-aided systems with HBF via designing the HBF and the phase shifts of IRS. In [23], Li et al. investigated the information transmission for IRS-aided systems, where the BS adopted sub-connected HBF to reduce cost and hardware complexity. Moreover, integrating HBF with NOMA not only decreases hardware complexity but also boosts EE [24], [25]. Pang et al. in [24] combined HBF and NOMA to improve the EE and decrease hardware complexity. Feng et al. in [25] integrated HBF with NOMA to achieve higher spectral efficiency.

To the best of our knowledge, the robust secure transmission for IRS-aided NOMA networks with HBF has not been well investigated. In this paper, we propose two secure transmission schemes for IRS-aided NOMA networks with HBF under the case of perfect and imperfect CSI, respectively. We compare our work with the relevant works in Table I and contributions of this paper can be listed as below.

- We propose to preserve the robust security for IRS-aided NOMA networks. Specifically, the BS adopts the cost-effective HBF to decrease the power consumption and hardware complexity. The security is guaranteed via jointly designing the HBF and the phase shifts of IRS with the perfect and imperfect CSI, respectively.
- With the perfect CSI, we propose a secrecy rate maximization scheme that maximizes the secrecy rate of cell-center user (U1) subject to the constant modulus constraint and the quality of service (QoS) constraint of cell-edge user (U2). Owing to the coupled variables and non-convexity, the problem is first transformed into two subproblems. Then, each subproblem is alternately solved via the penalty-based algorithm and the successive convex approximation (SCA). Furthermore, the proposed iterative algorithm is extended to the multi-user case.
- With the imperfect CSI, we propose a robust secure transmission scheme that maximizes the achievable rate at U1 subject to its worst-case eavesdropping rate constraint, the worst-case QoS constraint of U2, and the constant modulus constraint. To handle this non-convex problem, we first transform it into a more tractable form via S-Procedure and generalized S-Procedure. Then, an iterative algorithm based on the alternating optimization (AO), the penalty-based algorithm and the SCA is developed to solve it. Moreover, we extend the proposed robust secure transmission scheme to the case of imperfect SIC.

The differences between [16] and our work are listed as below. 1) The FDB is adopted in [16], while our work adopts the HBF. 2) [16] assumes that the statistical CSI of the eavesdropper is available and derives the SOP as the security metric. The Bernstein-type inequality is employed to deal with the SOP constraint. By contrast, we consider both the perfect and imperfect instantaneous eavesdropping CSI. Furthermore, the secrecy rate is investigated as the security metric. S-Procedure and generalized S-Procedure are utilized to deal with the semi-definite constraints introduced by the imperfect CSI. 3) [16] assumes that the CSI of the users are perfect, while we consider the channel estimation error of the IRS-U2 channel. 4) The eavesdropper is equipped with a single antenna in [16], while a multi-antenna eavesdropper is considered in our work.

The rest of this paper is organized as below. Section II introduces the system model. Section III presents the proposed secrecy rate maximization scheme with the perfect CSI. Section IV presents the proposed robust secure transmission scheme with the imperfect CSI. Section V provides the simulation results to verify the effectiveness of the two proposed schemes. This paper is concluded in Section VI.

**Notation:** $\cdot$ denotes the modulus of a scalar. $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$ and $(\cdot)^{-1}$ stand for transpose, conjugate, Hermitian and inverse, respectively. The complex Gaussian distribution with mean vector $\mu$ and covariance matrix $\Sigma$ is denoted by $CN(\mu, \Sigma)$. $\| \cdot \|$ and $\| \cdot \|_F$ and $\| \cdot \|_*$ represent the Euclidean/spectral norm, Frobenius norm and nuclear norm, respectively. $\lambda_{\text{max}}(\cdot)$ refers to the eigenvalue corresponding to the maximum eigenvalue of a matrix. $\nabla_Y$ represents the gradient of variable $Y$. $\text{Tr}(\cdot)$ and $\text{rank}(\cdot)$ stand for the trace and rank of a matrix, respectively. $\text{diag}(x)$ stands for a diagonal matrix whose main diagonal is $x$.

**II. SYSTEM MODEL**

Consider an IRS-aided secure NOMA network consisting of a BS with $N_t$ antennas, a single-antenna cell-center user (U1), a single-antenna cell-edge user (U2), an IRS with $M$ reflection elements and an eavesdropper with $N_e$ antennas, as illustrated in Fig. 1. Moreover, the BS adopts the HBF to reduce the power consumption. To guarantee the user fairness of power-domain NOMA [12], U2 is allocated with higher transmit power via designing the beamforming and the phase-shift matrix of this paper can be listed as below.

- The FDB is adopted in [16], while our work adopts the HBF. 2) [16] assumes that the statistical CSI of the eavesdropper is available and derives the SOP as the security metric. The Bernstein-type inequality is employed to deal with the SOP constraint. By contrast, we consider both the perfect and imperfect instantaneous eavesdropping CSI. Furthermore, the secrecy rate is investigated as the security metric. S-Procedure and generalized S-Procedure are utilized to deal with the semi-definite constraints introduced by the imperfect CSI. 3) [16] assumes that the CSI of the users are perfect, while we consider the channel estimation error of the IRS-U2 channel. 4) The eavesdropper is equipped with a single antenna in [16], while a multi-antenna eavesdropper is considered in our work.

The rest of this paper is organized as below. Section II introduces the system model. Section III presents the proposed secrecy rate maximization scheme with the perfect CSI. Section IV presents the proposed robust secure transmission scheme with the imperfect CSI. Section V provides the simulation results to verify the effectiveness of the two proposed schemes. This paper is concluded in Section VI.

**Notation:** $\cdot$ denotes the modulus of a scalar. $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$ and $(\cdot)^{-1}$ stand for transpose, conjugate, Hermitian and inverse, respectively. The complex Gaussian distribution with mean vector $\mu$ and covariance matrix $\Sigma$ is denoted by $CN(\mu, \Sigma)$. $\| \cdot \|$ and $\| \cdot \|_F$ and $\| \cdot \|_*$ represent the Euclidean/spectral norm, Frobenius norm and nuclear norm, respectively. $\lambda_{\text{max}}(\cdot)$ refers to the eigenvalue corresponding to the maximum eigenvalue of a matrix. $\nabla_Y$ represents the gradient of variable $Y$. $\text{Tr}(\cdot)$ and $\text{rank}(\cdot)$ stand for the trace and rank of a matrix, respectively. $\text{diag}(x)$ stands for a diagonal matrix whose main diagonal is $x$.

**II. SYSTEM MODEL**

Consider an IRS-aided secure NOMA network consisting of a BS with $N_t$ antennas, a single-antenna cell-center user (U1), a single-antenna cell-edge user (U2), an IRS with $M$ reflection elements and an eavesdropper with $N_e$ antennas, as illustrated in Fig. 1. Moreover, the BS adopts the HBF to reduce the power consumption. To guarantee the user fairness of power-domain NOMA [12], U2 is allocated with higher transmit power.
TABLE I

<table>
<thead>
<tr>
<th>Publication</th>
<th>Beamforming</th>
<th>Direct links</th>
<th>User CSI</th>
<th>Eavesdropping CSI</th>
<th>Access mode</th>
<th>AN</th>
<th>security metric</th>
<th>number of antennas at EVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[5]</td>
<td>FDB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>w/ SR</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[6]</td>
<td>FDB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>w/ SR</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[7]</td>
<td>FDB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>w/o SR</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[8]</td>
<td>FDB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>w/o SR</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[9]</td>
<td>FBB</td>
<td>w/o</td>
<td>PI</td>
<td>N/A</td>
<td>w/ SR</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[10]</td>
<td>FDB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>w/ SR</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[11]</td>
<td>FDB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[12]</td>
<td>FBB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[13]</td>
<td>FDB</td>
<td>w/</td>
<td>PI</td>
<td>IPI</td>
<td>NOMA</td>
<td>w/</td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[14]</td>
<td>FDB</td>
<td>w/o</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[15]</td>
<td>FBB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[16]</td>
<td>FBB</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[17]</td>
<td>HIIF</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[18]</td>
<td>HIIF</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[19]</td>
<td>HIIF</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[20]</td>
<td>HIIF</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[21]</td>
<td>HIIF</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[22]</td>
<td>HIIF</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>[23]</td>
<td>HIIF</td>
<td>w/</td>
<td>PI</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
<tr>
<td>Proposed</td>
<td>HIIF</td>
<td>w/o</td>
<td>PI</td>
<td>IPI</td>
<td>N/A</td>
<td></td>
<td>single</td>
<td></td>
</tr>
</tbody>
</table>

1 AN: artificial noise, 2 PI: perfect instantaneous, 3 SR: secrecy rate, 4 SOP: secrecy outage probability, 5 IPI: imperfect instantaneous.

The signal received by U2 can be expressed as

\[ y_2 = h_2^H \Phi H_{ia} x + n, \]  

where \( n \sim CN(0, \sigma^2) \) denotes the AWGN at the U2.

Similarly, the signal received by the eavesdropper can be expressed as

\[ y_e = H_{ie} \Phi H_{ia} x + n_e, \]  

where \( n_e \sim CN(0, \sigma_e^2 I) \) denotes the AWGN vector at the eavesdropper.

Owing to that the U1 is near the IRS, while the U2 is far away from it, we assume the channel gains of U1 and U2 satisfy \( ||h_1||^2 > ||h_2||^2 > 0 \). According to the power-domain NOMA [26], each user first detects the U2’s signal via regarding the U1’s signal as noise. Then, the U1 can decode its own signal via eliminating the detected U2’s signal from the received signal. As a result, the achievable rate of U2 and U1 at the U1 can be formulated as

\[ R_{1,2} = \log_2 \left( 1 + \frac{\gamma |h_1^H \Phi H_{ia} f_2|^2}{\gamma |h_1^H \Phi H_{ia} f_1|^2 + 1} \right), \]  

\[ R_{1,1} = \log_2 \left( 1 + \frac{|h_1^H \Phi H_{ia} f_2|^2}{\gamma |h_1^H \Phi H_{ia} f_1|^2 + 1} \right), \]

respectively, where \( \gamma = 1/\sigma^2 \).

Similarly, the achievable rate of U2 at the U2 can be given by

\[ R_{2,2} = \log_2 \left( 1 + \frac{\gamma |h_1^H \Phi H_{ia} f_2|^2}{\gamma |h_1^H \Phi H_{ia} f_1|^2 + 1} \right). \]

For the eavesdropper, the eavesdropping rate towards the private information \( s_1 \) can be given by

\[ R_e = \log_2 \left| 1 + Q_e^{-1} (H_{ie} \Phi H_{ia}) f_1^H (H_{ie} \Phi H_{ia})^H \right| \]

\[ = \log_2 \left| 1 + Q_e^{-1} \gamma_e (H_{ie} \Phi H_{ia}) f_1^H (H_{ie} \Phi H_{ia})^H \right|, \]

where \( Q_e = (H_{ie} \Phi H_{ia}) f_2^H (H_{ie} \Phi H_{ia})^H + \sigma_e^2 I \). \( \tilde{Q}_e \) = \( \gamma_e (H_{ie} \Phi H_{ia}) f_2^H (H_{ie} \Phi H_{ia})^H + I \) and \( \gamma_e = 1/\sigma_e^2 \).

Therefore, the secrecy rate of U1 can be expressed as

\[ R_s = \max(R_{1,1} - R_e, 0). \]

In the following, we propose a secrecy rate maximization scheme with the perfect CSI in Section III and a robust secure transmission scheme with the imperfect CSI in Section IV, respectively.
III. SECURE TRANSMISSION WITH PERFECT CSI

In this section, the perfect CSIs of all channels are assumed to be available at BS and the secrecy rate of U1 is maximized via designing the HBF and phase shifts\(^1\). Then, an iterative algorithm is developed to address this non-convex problem. Moreover, we extend the secure transmission scheme to the multi-user case.

A. Problem Formulation

With the perfect CSI, the secrecy rate of U1 is maximized while satisfying the constant modulus constraint, the transmit power constraint, the SIC decoding constraint and the QoS constraint of U2. The optimization problem can be given by

\[
\begin{align}
\max_{\mathbf{f}_1, \mathbf{f}_2, p_1, p_2, \mathbf{v}}
R_s & \quad \text{s.t.} \quad \begin{align}
|\mathbf{f}_1(i)| &= \sqrt{\frac{p_1}{N_i}}, \quad i = 1, \cdots, N_t, \\
|\mathbf{f}_2(i)| &= \sqrt{\frac{p_2}{N_i}}, \quad i = 1, \cdots, N_t, \\
p_1 + p_2 &\leq P_{\text{max}}, \quad p_1 \geq 0, \quad p_2 \geq 0, \\
R_{2,2} &\geq \zeta, \\
|\nu(i)| &= 1, \quad i = 1, \cdots, M, \\
R_{1,2} &\geq R_{2,2}, \\
|\mathbf{h}_k^H \mathbf{\Phi}_a \mathbf{f}_2|^2 &\geq |\mathbf{h}_k^H \mathbf{\Phi}_a \mathbf{f}_1|^2, \quad k = 1, 2, \\
\end{align}
\end{align}
\]

where (10b) and (10c) denote the constant modulus constraints. (10d) represents the transmit power constraint at BS. (10e) denotes that the achievable rate at U2 should be no less than a given threshold \(\zeta > 0\). (10f) denotes the unit-modulus constraint for the IRS. (10g) guarantees the successful SIC at U1. (10h) implicates the SIC decoding order of users. Problem (10) is difficult to tackle owing to the highly coupled variables, the non-convex constraints and the non-concave objective function. In the below subsections, an iterative algorithm based on the AO, the penalty-based algorithm and the SCA is proposed to tackle this non-convex problem.

B. \((f_1, f_2, p_1, p_2)\) Optimization With Given v

For any given \(\mathbf{v}\), we denote \(\mathbf{F}_1 = f_1 \mathbf{f}_1^H (\mathbf{F}_1 \succeq 0, \text{rank}(\mathbf{F}_1) = 1)\) and \(\mathbf{F}_2 = f_2 \mathbf{f}_2^H (\mathbf{F}_2 \succeq 0, \text{rank}(\mathbf{F}_2) = 1)\).

\(^1\)In this section, the eavesdropper is assumed to be an internal eavesdropper, which is a registered user without authority to access the private information. Thus, the perfect eavesdropping CSI can be obtained via the existing channel estimation methods, such as [27] and [28].

respectively. (10) can be equivalently expressed as

\[
\begin{align}
\min_{\mathbf{F}_1, \mathbf{F}_2, p_1, p_2}
R_s & \quad \text{s.t.} \quad \begin{align}
\text{diag}(\mathbf{F}_i) &= \frac{p_i}{N_i}, \quad i = 1, 2, \\
\text{rank}(\mathbf{F}_i) &= 1, \quad i = 1, 2, \\
\mathbf{F}_i &\succeq 0, \quad i = 1, 2, \\
p_1 + p_2 &\leq P_{\text{max}}, \quad p_1 \geq 0, \quad p_2 \geq 0, \\
\log_2 \left(1 + \frac{\gamma \text{Tr}(\mathbf{M}_2 \mathbf{F}_2)}{\gamma \text{Tr}(\mathbf{M}_2 \mathbf{F}_1) + 1}\right) &\geq \zeta, \\
\gamma \text{Tr}(\mathbf{M}_1 \mathbf{F}_2) + 1 &\geq \gamma \text{Tr}(\mathbf{M}_1 \mathbf{F}_1) + 1, \\
\text{Tr}(\mathbf{M}_k \mathbf{F}_2) &\geq \text{Tr}(\mathbf{M}_k \mathbf{F}_1), \quad k = 1, 2, \\
\end{align}
\end{align}
\]
\[ \tilde{R}_s = \log_2 (1 + \gamma_1 \text{Tr}(M_1 F_1)) - \log_2 \left| I + \tilde{Q}_e^{-1}\gamma_e (H_{ie} \Phi H_{ie}) F_1 (H_{ie} \Phi H_{ie})^H \right|. \] (12)

rank-one constraint (11c) like SDR, we formulate it into an equivalent form as

\[ (11c) \leftrightarrow \|F_i\|_s - \|F_i\|_2 \leq 0, \quad i = 1, 2. \] (19)

For any \( F \in \mathbb{H}^{N_i} \) and \( F \succeq 0 \), the inequality \( \|F\|_s = \sum_{i=1}^{N_i} \lambda_i \geq \|F\|_2 = \lambda_1 \) holds, where \( \lambda_i \) stands for the \( i \)-th biggest eigenvalue of \( F \). The equality in (19) holds if and only if \( F_i \) is rank-one [31, Lem. 1]. The constraint (19) is non-convex and the penalty-based algorithm in [31] is utilized to tackle it. Specifically, we move the constraint (19) into the objective function as a penalty term, yielding the following optimization problem as

\[
\min_{F_1,F_2,p_1, p_2, \beta, \nu} \tilde{R}_s + \frac{1}{2\rho} \sum_{i=1}^{2} (\|F_i\|_s - \|F_i\|_2)
\text{s.t.} \quad (11b),(11d),(11e),(11h),(13),(15),(17),(18),
\] (20a)

where \( \rho > 0 \) denotes the penalty coefficient. All constraints of (20) are convex. As for the non-convex objective function in (20), the SCA is utilized to tackle it. Specifically, the objective function is first transformed into a difference of convex, i.e.,

\[ -\tilde{R}_s = N_1 - D_1, \] where

\[ N_1 = -\log_2 (1 + \gamma \text{Tr}(M_1 F_1)) \]
\[ - \log_2 \left| I + \gamma_e \tilde{H}_e F_2 \tilde{H}_e^H \right| + \frac{1}{2\rho} \sum_{i=1}^{2} \|F_i\|_s - \|F_i\|_2, \] (21a)

\[ D_1 = -\log_2 \left| I + \gamma_e \tilde{H}_e (F_1 + F_2) \tilde{H}_e^H \right| + \frac{1}{2\rho} \sum_{i=1}^{2} \|F_i\|_2, \] (21b)

and \( \tilde{H}_e = H_{ie} \Phi H_{ie} \). Both \( N_1 \) and \( D_1 \) are jointly convex w.r.t. \( F_1 \) and \( F_2 \). Then, we introduce Lemma 1 to get a convex upper bound of this non-convex objective function.

**Lemma 1.** Let \( f_i \) be a real-valued function of the matrices \( Z \succeq 0 \) and \( Y \succeq 0 \), \( i = 1, 2 \), which is jointly convex w.r.t. \( Z \) and \( Y \). For the function \( g \overset{d}{=} f_1 - f_2 \), its convex upper bound can be formulated as \( \tilde{f}_1 - \tilde{f}_2 \), where \( \tilde{f}_2 \) stands for the first-order Taylor expansion of \( f_2 \) at the reference point \( (Z_0, Y_0) \), as

\[ \tilde{f}_2 = \text{Tr}(\nabla^H f_2(Z_0,Y_0))(Z - Z_0) + \text{Tr}(\nabla^H f_2(Z_0,Y_0))(Y - Y_0). \] (22)

**Proof:** Due to that \( f_2 \) is jointly convex w.r.t. \( Z \) and \( Y \), \( f_2 \) is lower bounded by \( \tilde{f}_2 \), i.e., \( f_2 \geq \tilde{f}_2 \). Moreover, \( f_2 \) is an affine function w.r.t. \( Z \) and \( Y \). Therefore, we have

\[ f_1 - f_2 \leq f_1 - \tilde{f}_2, \] (23)

and \( f_1 - \tilde{f}_2 \) is jointly convex w.r.t. \( Z \) and \( Y \).

According to Lemma 1, the objective function in (20) can be replaced with its convex upper bound at the reference point \( (F_1', F_2') \) in \( t \)-th inner-layer iteration, which yields the problem as

\[
\min_{F_1,F_2,p_1, p_2, \beta, \nu} N_1 - \text{Tr}(\nabla^H F_1 D_1 (F_1', F_2') (F_1 - F_1')) - \\
\text{Tr}(\nabla^H F_1 D_1 (F_1', F_2') (F_2 - F_2')) - D_1 (F_1', F_2')
\text{s.t.} \quad (11b),(11d),(11e),(11h),(13),(15),(17),(18),
\] (24a)

where \( \nabla F_1 D_1 (F_1', F_2') \) can be formulated as

\[
\nabla F_1 D_1 (F_1', F_2') = \frac{1}{2\rho} \lambda_{\max} (F_1')^H H_{max} (F_1') - \\
\text{Tr}(\nabla F_1 D_1 (F_1', F_2') (F_2 - F_2')) - D_1 (F_1', F_2')
\] (25)

Therefore, (11) is changed to a convex one (24), which can be solved utilizing CVX. According to [9], a rank-one solution \( (F_1', F_2') \) can be obtained via solving (24) with sufficiently small \( \rho \). Then, the optimal solution \( \tilde{f}_i \) can be recovered from \( F_i \) via the eigen-decomposition, \( i = 1, 2 \).

The penalty-based algorithm for (24) is described in Algorithm 1. Through iteratively solving (24) in Step 3, the optimal value of (24) tends to that of (20). According to [31, Prop. 1], the sequence \( \{F_1', F_2'\}_{t \in \mathbb{N}} \) converges to a stationary point of (20) in polynomial time.

**Algorithm 1** Penalty-Based Algorithm for (24)

1: Initialization: Given an initial point \( (F_1', F_2') \), and set the index of inner-layer iteration \( t = 0 \) and the convergence tolerance \( \phi \).

2: **Repeat**

3: With the given \( (F_1', F_2', p_1', p_2') \), obtain \( (F_1^{t+1}, F_2^{t+1}, p_1^{t+1}, p_2^{t+1}) \) via solving (24).

4: \( t = t + 1 \).

5: **Until** \( \|F_1^{t+1}\|_s - \|F_1^{t+1}\|_2 \leq \phi \) and \( \|F_2^{t+1}\|_s - \|F_2^{t+1}\|_2 \leq \phi \).

6: **Output**: \( (F_1^{t+1}, F_2^{t+1}, p_1^{t+1}, p_2^{t+1}) \).

C. Optimization With Given \((f_1, f_2, p_1, p_2)\)

For any given \((f_1, f_2, p_1, p_2)\), we denote \( V = vv^H \) \((-\text{rank}(V) = 1, V \succeq 0)\). Accordingly, (10) can be equivalently formulated as

\[
\min_{V} -\tilde{R}_s
\text{s.t.} \quad V \succeq 0, \quad \text{diag}(V) = 1, \quad \text{rank}(V) = 1,
\] (26a)

\[
\log_2 \left( 1 + \frac{\gamma \text{Tr}(\tilde{f}_2 H_{l2}^H V^T)}{\gamma \text{Tr}(\tilde{f}_2 H_{l2}^H V^T) + 1} \right) \geq \zeta,
\] (26b)

\[
\gamma \text{Tr}(\tilde{f}_2 H_{l2}^H V^T) + 1 \geq \gamma \text{Tr}(\tilde{f}_2 H_{l2}^H V^T) + 1,
\] (26c)

\[
\text{Tr}(\tilde{f}_2 H_{l2}^H V^T) \geq \text{Tr}(\tilde{f}_2 H_{l1}^H V^T), \quad k = 1, 2.
\] (26d)
where \( \hat{f}_{mn} = \text{diag}(h_{mn}^H)h_{mn}f_m, n = 1, 2, m = 1, 2, \hat{h}_k = H_{ai}f_k, k = 1, 2, Q_e = I + \gamma_e H_{ae} \text{diag}(\hat{h}_1) \text{diag}(h_{1e}^H)H_{ie}^H, \) and \( \hat{R}_s \) is given by (27) at the top of next page. The objective function and all the constraints except (26b) and (26f) are non-convex. To address this non-convex problem, we first formulate the non-convex constraint (26d) into an equivalent form as

\[
\gamma \text{Tr}(\hat{f}_{21} \hat{f}_{21}^H V^T) - (2\kappa - 1)(\gamma \text{Tr}(\hat{f}_{21} \hat{f}_{21}^H V^T) + 1) \geq 0,
\]

(28)

which is convex w.r.t. \( V \).

Recalling (15)-(18), the constraint (26e) can be reformulated as

\[
2\gamma \text{Tr}(\hat{f}_{11} \hat{f}_{11}^H V^T) \geq \left( \gamma \text{Tr}(\hat{f}_{11} \hat{f}_{11}^H V^T) + 1 \right)^2 - (\beta a)^2,
\]

(29a)

\[
\gamma \text{Tr}(\hat{f}_{21} \hat{f}_{21}^H V^T) \leq -d^2 + 2\nu \nu,
\]

(29b)

\[
\left[ \gamma \text{Tr}(\hat{f}_{21} \hat{f}_{21}^H V^T) + 1 \right] \nu \geq 0.
\]

(29c)

Accordingly, the penalized version of (26) can be given by

\[
\min_{\nu, \beta \geq 0, \nu} -R_s + \frac{1}{2\rho} (||V||_* - ||V||_2) \quad \text{s.t.} \quad (26b), (26f), (28), (29).
\]

(30a)

All the constraints in (30) are convex. As for the non-convex objective function in (30), we first reformulate it into a difference of convex as

\[
-N_1 - D_1 = \log_2 \left( 1 + \gamma \text{Tr}(\hat{f}_{11} \hat{f}_{11}^H V^T) \right) + \frac{||V||_*}{2\rho} - \log_2 \left| I + \gamma_e H_{ae} \text{diag}(\hat{h}_1) \text{diag}(h_{1e}^H)H_{ie}^H \right|,
\]

(32a)

\[
-D_1 = -\log_2 \left| I + \sum_{k=1}^2 \gamma_e H_{ae} \text{diag}(\hat{h}_k) \text{diag}(h_{ke}^H)H_{ie}^H \right| + \frac{||V||_2^2}{2\rho}.
\]

(32b)

Both \( N_1 \) and \( D_1 \) are convex w.r.t. \( V \). According to Lemma 1, the objective function in (30) can be replaced with its convex upper bound at the reference point \( V^* \), which yields the following problem as

\[
\min_{\nu, \beta \geq 0, \nu} -N_1 - D_1 (V^*) - \text{Tr} (\nabla_V^H \hat{D}_1 (V^*) (V - V^*)) \quad \text{s.t.} \quad (26b), (26f), (28), (29),
\]

(33a)

where \( \nabla_V \hat{D}_1 (V^*) \) is formulated as (34) at the top of this page and \( X = I + \sum_{k=1}^2 \gamma_e H_{ae} \text{diag}(\hat{h}_k) V^T \text{diag}(h_{ke}^H)H_{ie}^H \). Thus, the problem (26) is changed to a convex one (33) and can be solved utilizing CVX.

D. Algorithm Analysis

In summary, the problem (10) is transformed into two convex subproblems (24) and (33), and the proposed AO-based algorithm for (10) is described in Algorithm 2, which alternatively solves the two subproblems and guarantees to converge to a stationary point in polynomial time [32].

According to [33, Th. 3.12], the computational complexity of the proposed AO-based algorithm in each iteration can be formulated as

\[
O \left( \ln \frac{1}{\zeta} \left( I_1 (3N_1^2 + 9N_2^2 + 27N_3^2) + I_2 (2M_1^2 + 4M_2^2 + 8M_3^2) \right) \right),
\]

(35)

where \( \zeta \) denotes the convergence tolerance, and \( I_1 \) and \( I_2 \) represent the iteration number of Algorithm 1 for tackling (24) and (33), respectively.

Algorithm 2 AO-based Algorithm for (10)

1: Initialization: Given an initial point \( (\hat{f}_1^0, \hat{f}_2^0, p_1^0, p_2^0, \nu^0) \), and set the outer-layer iteration index \( n = 0 \).

2: Repeat

3: With the given \( (\hat{f}_1^0, \hat{f}_2^0, p_1^0, p_2^0, \nu^0) \), tackle (24) using Algorithm 1 and update \( (\hat{f}_1^{n+1}, \hat{f}_2^{n+1}, p_1^{n+1}, p_2^{n+1}) \).

4: Decompose \( \hat{f}_1^{n+1} = f_1^{n+1} + f_1^{n+1}_1, f_2^{n+1}, p_1^{n+1}, p_2^{n+1}, \nu^{n+1} \), tackle (33) via Algorithm 1 and update \( \nu^{n+1} \).

5: Decompose \( \nu^{n+1} = \nu^{n+1} + \nu^{n+1}_1, \nu^{n+1} \), \( H \).

6: \( n = n + 1 \).

8: Until convergence.

9: Output: \( (\hat{f}_1^{n+1}, \hat{f}_2^{n+1}, p_1^{n+1}, p_2^{n+1}, \nu^{n+1}) \).

E. Multi-user Case

In this subsection, we extend the proposed scheme to the multi-user case. Assume that \( K \) single-antenna users (denoted by \( U_1, i_1, \cdots, K \)) are served and only the signal for \( U_1 \) is confidential. Therefore, the transmitted signal from the BS can be expressed as

\[
x = W P S = \sum_{k=1}^K \sqrt{p_k} w_k s_k = \sum_{k=1}^K f_k s_k,
\]

(36)

where \( P = \text{diag}(\sqrt{p_1}, \cdots, \sqrt{p_K}), W = [w_1, \cdots, w_K], s = [s_1, \cdots, s_K]^T \sim \mathcal{CN}(0, I) \) and \( f_k = \sqrt{p_k} w_k, k = 1, \cdots, K \).

Without loss of generality, we assume that the channel gains from IRS to users satisfy

\[
||h_1||^2 > ||h_2||^2 > \cdots > ||h_K||^2 > 0,
\]

(37)

where \( h_k \) refers to the channel between IRS and \( U_k \).

Furthermore, the decoding order can be determined by the channel gains. Therefore, we have

\[
|h_k^H \Phi H_{ai} f_K| \geq \cdots \geq |h_1^H \Phi H_{ai} f_i|, \quad \forall k.
\]

(38)
Accordingly, \( U_1 \) first eliminates the signal of other users via SIC before decoding its own signal. The formulation of achievable rate of \( U_1 \) at the \( U_3 \) is same as (6), and the achievable rate of \( U_i \) at the \( U_k (k \leq i) \) can be given by

\[
R_{k,i} = \log_2 \left( 1 + \frac{\gamma |h_k^H \Phi h_i f_i|^2}{\gamma \sum_{j=1}^{i-1} |h_k^H \Phi h_{j} f_j|^2 + 1} \right), \quad i \geq 2. \tag{39}
\]

To guarantee the successful SIC, we have

\[
\min \{ R_1, i, R_2, i, \cdots, R_{i-1}, i \} \geq R_{i,i} \geq \zeta_i, \quad i \geq 2, \tag{40}
\]

where \( \zeta_i \) denotes the target rate of \( U_i \).

The eavesdropping rate towards the private information \( s_1 \) can be reformulated as

\[
R_e = \log_2 \left| I + \tilde{Q}_{e}^{-1} \tilde{H}_e \tilde{f}_e \tilde{f}_e^H \tilde{H}_e^H \right|, \tag{41}
\]

where \( \tilde{Q}_{e} = \sum_{k=2}^{K} \gamma_e |h_k^H \Phi h_e f_k|^2 \tilde{H}_k^H + I \).

Thus, the secrecy rate maximization problem can be reformulated as

\[
\max_{\{f_k(i), \bar{p}_k, \bar{v}(i)\}} R_s \tag{42a}
\]

s.t. \( |f_k(i)| = \sqrt{\frac{\bar{p}_k}{N_t}}, \forall i, k, \quad (42b) \)

\[
\sum_{k=1}^{K} \bar{p}_k \leq P_{max}, \quad \bar{p}_k \geq 0, \forall k, \quad (42c) \)

\[
|\bar{v}(i)| = 1, \quad i = 1, \cdots, M, \quad (42d) \)

\[
\min \{ R_1, i, \cdots, R_{i-1}, i \} \geq R_{i,i} \geq \zeta_i, \quad i \geq 2, \quad (42e) \)

\[
|h_k^H \Phi h_1 f_k|^2 \geq \cdots \geq |h_k^H \Phi h_i f_i|^2, \quad \forall k, \quad (42f) \)

which can be solved via the iterative algorithm similar to Algorithm 2 and the details are omitted for brevity.

IV. SECURE TRANSMISSION WITH IMPERFECT CSI

In this section, we assume that the CSIs of both IRS-U2 channel and IRS-eavesdropper channel are imperfect.\(^2\) We propose a robust secure transmission scheme that maximizes the rate of \( U_1 \) satisfying its worst-case eavesdropping rate constraint and worst-case QoS constraint of \( U_2 \), via the joint design of HBF and phase shifts. Then, an iterative algorithm is proposed to solve this non-convex robust optimization problem. Furthermore, the robust secure transmission scheme is extended to the case of imperfect SIC.

\(^2\)In this section, we assume the eavesdropper is an external and passive eavesdropper, whose perfect CSI is difficult to obtain.

A. CSI Error Model

Considering a more practical scenario, we assume that there is a channel estimation error of the IRS-U2 channel, because the \( U_2 \) is far away from the IRS. In addition, since the eavesdropper tends to hide its existence and does not cooperate with the IRS to estimate wireless channels, it is difficult to get the perfect eavesdropping CSI. Accordingly, the deterministic model adopted for these channels to describe the CSI uncertainty can be formulated as [34]

\[
h_{2} = \hat{h}_2 + \Delta h_2, \quad \Omega_{2} = \{ \Delta h_2 \mid ||\Delta h_2||_2 \leq \epsilon_2 \}, \tag{43a}
\]

\[
H_{ie} = \hat{H}_{ie} + \Delta H_{ie}, \quad \Omega_{e} = \{ \Delta H_{ie} \mid ||\Delta H_{ie}||_F \leq \epsilon_e \}, \tag{43b}
\]

where \( \hat{h}_2 \) and \( \hat{H}_{ie} \) stand for the estimated channel of \( h_2 \) and \( H_{ie} \), respectively, while \( \epsilon_2 > 0 \) and \( \epsilon_e > 0 \) denote the radius of the uncertainty region of estimation errors \( \Delta h_2 \) and \( \Delta H_{ie} \), respectively.

B. Problem Formulation

Owing to the imperfect eavesdropping CSI, it is hard to formulate the eavesdropping rate. Therefore, rather than maximizing the secrecy rate, we propose a robust secure transmission scheme, which can keep a balance between transmission rate and security. In particular, we aim at maximizing the transmission rate at \( U_1 \), satisfying its worst-case eavesdropping rate constraint, the constant modulus constraint, the SIC decoding constraint and the worst-case QoS constraint of \( U_2 \). The robust optimization problem can be given by

\[
\max_{f_1, f_2, \bar{p}_1, \bar{p}_2} R_{1,1} \tag{44a}
\]

s.t. \( (10b), (10c), (10d), (10f), \quad (44b) \)

\[
\min_{\Delta h_2 \in \Omega_{2}} R_{2,2} \geq \zeta, \quad (44c) \)

\[
R_{2,2} \geq \max_{\Delta H_{ie} \in \Omega_{e}} R_{2,2}, \quad (44d) \)

\[
|h_1^H \Phi h_2 f_2|^2 \geq |h_1^H \Phi h_2 f_2|^2, \quad (44e) \)

\[
\min_{\Delta h_2 \in \Omega_{2}} |h_1^H \Phi h_2 f_2|^2 - |h_2^H \Phi h_1 f_1|^2 \geq 0, \quad (44f) \)

\[
\max_{\Delta H_{ie} \in \Omega_{e}} R_e \leq \xi. \quad (44g) \)

The constraint (44c) denotes that the worst-case achievable rate at \( U_2 \) should be no less than a given threshold \( \zeta > 0 \). The constraints (44d)-(44f) guarantee the successful SIC under the imperfect CSI. The constraint (44g) denotes that the maximum eavesdropping rate at the eavesdropper should be no more than a given threshold \( \xi \). The secrecy rate of \( U_1 \) is lower bounded by \( R_{1,1} - \xi \), and thus the security can be guaranteed.

The problem (44) is difficult to tackle owing to the non-convex objective function, the non-convex constraints and the inequality constraints. In the following subsection, we resort to S-Procedure [35, B.2] and generalized S-Procedure [36, Th. 3.3] to relax problem (44) to a more tractable one.
C. Problem Transformation

To tackle (44), we first formulate the constraint (44c) into an equivalent form as

\[
(2^\gamma - 1)\sigma_a^2 + h_f^H R_1 h_2 \leq 0, \quad \forall \Delta h_2 \in \Omega_2,
\]

where \( R_1 = \Phi H_{ai} ((2^\gamma - 1)f_1 H)^H - f_2 H_2^H \Phi H_f^H \).

The constraint (44d) can be equivalently formulated as

\[
\frac{\gamma |h_i^H \Phi H_{ai} f_2|^2}{\gamma |h_i^H \Phi H_{ai} f_1|^2 + 1} \geq \max_{\Delta h_2 \in \Omega_2} \frac{\gamma |h_l^H \Phi H_{ai} f_2|^2}{\gamma |h_l^H \Phi H_{ai} f_1|^2 + 1}.
\]

(46)

Via introducing a slack variable \( \varpi > 0 \), the constraint (46) can be reformulated as

\[
\gamma |h_i^H \Phi H_{ai} f_2|^2 \geq \varpi (\gamma |h_i^H \Phi H_{ai} f_1|^2 + 1),
\]

(47a)

\[
\max_{\Delta h_2 \in \Omega_2} \frac{\gamma |h_l^H \Phi H_{ai} f_2|^2}{\gamma |h_l^H \Phi H_{ai} f_1|^2 + 1} \leq \varpi.
\]

(47b)

According to the AGM inequality, the constraint (47a) can be approximated as

\[
2\gamma |h_i^H \Phi H_{ai} f_2|^2 \geq \left( \frac{\gamma |h_i^H \Phi H_{ai} f_1|^2 + 1}{\varpi} \right)^2 + (\varpi a)^2,
\]

where the equivalence holds if and only if \( a = \sqrt{\gamma |h_i^H \Phi H_{ai} f_1|^2 + 1}/\varpi \).

By introducing a slack variable \( \mu > 0 \), the constraint (47b) can be approximate formulated as

\[
\gamma |h_l^H \Phi H_{ai} f_2|^2 \leq \mu \varpi, \quad \forall \Delta h_2 \in \Omega_2.
\]

(49a)

and

\[
\gamma |h_l^H \Phi H_{ai} f_1|^2 + 1 \geq \mu, \quad \forall \Delta h_2 \in \Omega_2.
\]

(49b)

Similar to (14b), the constraint (49a) can be reformulated as

\[
\gamma |h_l^H \Phi H_{ai} f_2|^2 \leq 2i \epsilon - i^2, \quad \forall \Delta h_2 \in \Omega_2,
\]

(50a)

\[
\left[ \begin{array}{c} \mu \\ i \\ \varpi \end{array} \right] \succeq 0,
\]

(50b)

where \( i \) denotes a reference point of \( \epsilon \).

Submitting \( h_2 = h_2 + \Delta h_2 \) into (45), we have

\[
(2^\gamma - 1)\sigma_a^2 + h_f^H R_1 h_2 + h_f^H R_1 \Delta h_2 + h_f^H R_1 h_2 + h_f^H R_1 \Delta h_2 \leq 0, \quad \forall \Delta h_2 \in \Omega_2.
\]

The constraint (51) consists of several inequality constraints, which is very difficult to treat.

According to S-Procedure, the constraint (51) can be transformed into a more tractable form as

\[
\eta \left[ \begin{array}{c} I \\ 0 \end{array} \right] - \left[ \begin{array}{c} R_1 \\ h_f^H R_1 h_2 \end{array} \right] - \left[ \begin{array}{c} R_2 \\ h_f^H R_2 h_2 \end{array} \right] \geq 0,
\]

where \( \eta \geq 0 \) denotes a slack variable.

Similarly, the constraints (44f), (49b) and (50a) can be formulated into LMI as

\[
(\text{44f}) \Rightarrow \tau \left[ \begin{array}{c} I \\ 0 \end{array} \right] - \left[ \begin{array}{c} R_2 \\ h_f^H R_2 h_2 \end{array} \right] \geq 0.
\]

(53a)

\[
(\text{49b}) \Rightarrow \nu \left[ \begin{array}{c} I \\ 0 \end{array} \right] - \left[ \begin{array}{c} R_3 \\ h_f^H R_3 h_2 + \mu - 1 \end{array} \right] \geq 0.
\]

(53b)

\[
(\text{50a}) \Rightarrow \tau \left[ \begin{array}{c} I \\ 0 \end{array} \right] - \left[ \begin{array}{c} R_4 \\ h_f^H R_4 h_2 - 2i \epsilon + i^2 \end{array} \right] \geq 0.
\]

(53c)

where \( R_2 = \Phi H_{ai} (f_1 h_f^H - f_2 h_2^H) H_f^H \Phi H_f^H \), \( R_3 = -\Phi H_{ai} f_1 H_2^H \Phi H_f^H \), and \( R_4 = \Phi H_{ai} f_2 H_2^H \Phi H_f^H \). \( \theta \geq 0, \quad \forall \theta \geq 0, \tau \geq 0 \) are slack variables.

According to [9, Prop. 1], the constraint (44g) can be equivalently formulated as

\[
\max_{\Delta h_e \in \Omega_e} (2^\gamma - 1)\sigma_e^2 I + H_e R_5 H_e^T \geq 0,
\]

(54)

where \( R_5 = \Phi H_{ai} ((2^\gamma - 1)f_2 h_2^H - f_3 h_3^H)^H \Phi H_f^H \). Substituting \( H_e = H_e + \Delta H_e h_2 \) into (54), we have

\[
(2^\gamma - 1)\sigma_e^2 I + H_e R_5 H_e^T + \Delta H_e R_5 H_e^T + \Delta H_e R_5 \Delta H_e^T + \Delta H_e \Delta H_e^T \geq 0, \quad \forall \Delta H_e \in \{ Y | Tr(e^{-2YY^T}) \leq 1 \}.
\]

(55)

However, the constraint (55) consists of an infinite number of LMIs, which is difficult to handle. According to the generalized S-Procedure, the constraint (55) can be transformed into an LMI as

\[
P + SR_5 S^H \succeq 0,
\]

(56)

where \( S = [H_e^T, I_{N_e}]^T \),

\[
P = \left[ \begin{array}{c} ((2^\gamma - 1)\sigma_e^2 - \varepsilon)I_{N_e} \\ 0 \\ \varepsilon e_2^\top I_M \end{array} \right],
\]

and \( \varepsilon \geq 0 \) is a slack variable.

Accordingly, the problem (44) can be transformed into a more tractable form as

\[
\min_{f_1, f_2, p_1, p_2, \nu, \eta, \varpi, \theta, \tau, \nu, i, \epsilon, \varpi} \quad R_{1,1}
\]

s.t. \( (44b), (44e), (48), (50b), (52), (53), (56) \)

\[
\eta \geq 0, \quad \varepsilon \geq 0, \quad \theta \geq 0, \quad \tau \geq 0, \quad \varepsilon \geq 0, \quad \varpi \geq 0.
\]

(58c)

The problem (58) is non-convex and an iterative algorithm based on the AO, the penalty-based algorithm and the SCA is proposed to further treat it.

D. Alternative Optimization Algorithm

For any given \( v \), we denote \( F_1 = f_1 h_f^H \) (\( F_1 \succeq 0, \quad \text{rank}(F_1) = 1 \)) and \( F_2 = f_2 h_2^H \) (\( F_2 \succeq 0, \quad \text{rank}(F_2) = 1 \)), respectively. Therefore, the penalized version of (58) can be formulated as

\[
\min_{f_1, f_2, p_1, p_2, \nu, \eta, \varpi, \theta, \tau, \nu, i, \epsilon, \varpi} \quad -\log_2(1 + \gamma Tr(M_1 F_1)) + \sum_{i=1}^{\rho} \frac{||F_i||_x - ||F_i||_2}{i} + \sum_{i=1}^{\rho} \frac{||F_i||_x - ||F_i||_2}{i}
\]

s.t. \( (11b), (11d), (11e),(50b),(52),(53),(56),(58c) \)

\[
2\gamma Tr(M_1 F_2) \geq \left( \frac{\gamma Tr(M_1 F_1 + 1)}{a} \right)^2 + (\varpi a)^2,
\]

(59b)

\[
\text{Tr}(M_1 F_2) \geq \text{Tr}(M_1 F_1)
\]

(59c)

All constraints of the problem (59) are convex. As for the non-convex objective function, we first reformulate it into a difference of convex, i.e., \( N_2 - D_2 \), where

\[
N_2 = -\log_2(1 + \gamma Tr(M_1 F_1)) + \sum_{i=1}^{\rho} \frac{||F_i||_x - ||F_i||_2}{i}
\]

(60a)

\[
D_2 = \frac{1}{2\rho} \sum_{i=1}^{\rho} ||F_i||_2.
\]

(60b)
Both $N_3$ and $D_2$ are jointly convex w.r.t. $F_1$ and $F_2$. According to Lemma 1, the objective function in $(59)$ can be replaced with its convex upper bound function at the reference point $(\bar{F}_1, \bar{F}_2)$, yielding the following problem as
\[
\min_{F_1, F_2, p_1, p_2, \epsilon, \eta, \theta, \tau, \nu, \omega} N_2 - \text{Tr}(\nabla F_1 D_2(F_1^2)(F_1 - F_1')) - \text{Tr}(\nabla F_2 D_2(F_1', F_2')(F_2 - F_2')) - D_2(F_1', F_2') \quad (61a)
\]
\[
s.t. \quad (59a), (59b), (59c), \quad (61b)
\]
where $\nabla F_1 D_2(F_1, F_2') = \frac{1}{2p} \lambda_{\max}(F_1') \lambda_{\max}(F_2')$, $i = 1, 2$. The problem $(61)$ is convex, which can be solved utilizing CVX.

For any given $(f_1, f_2, p_1, p_2)$, we denote $V = vv^H$ ($V \succeq 0, \text{rank}(V) = 1$). The matrix $R_i, i = 1, \cdots, 5$, can be recast as
\[
R_1 = \xi \text{diag}(\bar{h}_1) V \text{diag}(\bar{h}_1^H) - \text{diag}(\bar{h}_2) V \text{diag}(\bar{h}_2^H), \quad (62a)
\]
\[
R_2 = \text{diag}(\bar{h}_1) V \text{diag}(\bar{h}_1^H) - \text{diag}(\bar{h}_2) V \text{diag}(\bar{h}_2^H), \quad (62b)
\]
\[
R_3 = -\gamma \text{diag}(\bar{h}_1) V \text{diag}(\bar{h}_1^H), \quad (62c)
\]
\[
R_4 = \gamma \text{diag}(\bar{h}_2) V \text{diag}(\bar{h}_2^H), \quad (62d)
\]
\[
R_5 = \xi \text{diag}(\bar{h}_2) V \text{diag}(\bar{h}_2^H) - \text{diag}(\bar{h}_1) V \text{diag}(\bar{h}_1^H), \quad (62e)
\]
respectively, where $\xi = 2\epsilon - 1$ and $\xi = 2\epsilon - 1$.

Therefore, the penalized version of $(58)$ can be given by $(63)$ at the top of next page. All constraints of $(63)$ are convex. To tackle the non-convex objective function in $(63)$, we first rewrite it into a difference of convex as $(62)$ at the top of next page. All constraints of $(63)$ are convex. To tackle convex the objective function in $(63)$, we first rewrite it into a difference of convex as $(64)$ at the top of next page.

The approximate computational complexity of the proposed AO-based Algorithm 3 in each iteration can be given by $(66)$ at the top of next page, where $n_1 = 7$, $n_2 = 6$, $\epsilon$ denotes the convergence tolerance, and $I_1$ and $I_2$ denote the iteration number of Algorithm 1 to solve $(61)$ and $(65)$, respectively.

Algorithm 3 AO-based Algorithm for $(58)$

1: Initialization: Given an initial point $(f_1^0, f_2^0, p_1^0, p_2^0, v^0)$, and set the iteration index $n = 0$.

2: **Repeat**

3: With the given $(f_1^n, f_2^n, p_1^n, p_2^n, v^n)$, solve $(61)$ via Algorithm 1 and update $(f_1^{n+1}, f_2^{n+1}, p_1^{n+1}, p_2^{n+1})$.

4: Decompose $F_n^{n+1} = F_n^{n+1} F_n^{n+1} H_n^2 + 1, i = 1, 2$.

5: With the given $(f_1^{n+1}, f_2^{n+1}, p_1^{n+1}, p_2^{n+1}, v^{n+1})$, solve $(65)$ via Algorithm 1 and update $V^{n+1}$.

6: Decompose $V^{n+1} = v^{n+1} v^{n+1} H_n^2$.

7: $n = n + 1$.

8: **Until** convergence.

9: Output: $(f_1^{n+1}, f_2^{n+1}, p_1^{n+1}, p_2^{n+1}, v^{n+1})$.

F. Imperfect SIC Case

Since the imperfect CSI can cause the imperfect SIC, we extend the robust secure transmission scheme to the case of imperfect SIC in this subsection. Under the imperfect SIC, U1 is interfered by the residual signal for U2 when decoding its own signal. Thus, the achievable rate of U1 at U1 can be reformulated as
\[
R_{1,1} = \log_2 \left(1 + \frac{\gamma |h_2^H \Phi H_{a1} f_2|^2}{\theta |h_2^H \Phi H_{a1} f_1|^2 + 1} \right), \quad (67)
\]
where $\theta \in [0, 1]$ refers to the error propagation coefficient. $\theta = 0$ corresponds to the perfect SIC, while $\theta = 1$ stands for the totally unsuccessful SIC.

Nevertheless, the imperfect SIC does not influence the eavesdropping rate and the achievable rate of U2 at U2, because the eavesdropper does not adopt the SIC and U2 directly decodes its own signal via regarding the signal for U1 as noise.

Accordingly, the robust secure transmission problem can be reformulated as
\[
\max_{f_1, f_2, v, p_1, p_2} R_{1,1} \quad (68a)
\]
\[
s.t. \quad (10b) - (10d), (10f), (44c) - (44g), \quad (68b)
\]
which can be solved via modifying Algorithm 3.

V. Simulation Results

In this section, we present simulation results to demonstrate the effectiveness of the two proposed secure transmission schemes. The locations of BS, IRS, U1, U2 and eavesdropper are $(10, -20, 5), (0, 0, 2), (5, 0, 0), (5, 8, 0)$ and $(7, 7, 0)$ in meters, respectively. We set $N_t = 4$, $N_e = 2$, $M = 20$ and $\sigma_r^2 = \sigma_e^2 = -75$ dBm, respectively. We assume all channels are Rician channels. For instance, the channel between BS and IRS can be formulated as
\[
H_{ai} = \sqrt{L_0 d_{ai}}^{-\alpha_{ai}} \left( \sqrt{\frac{k_{ai}}{1 + k_{ai}}} H_{ai}^{H} + \sqrt{\frac{1}{1 + k_{ai}}} H_{ai}^{NL} \right), \quad (69)
\]
where $k_{ai}$ represents the Rician factor, $L_0 = -30$ dB, $\alpha_{ai}$ represents the path-loss exponent and $d_{ai}$ stands for the distance between IRS and BS. $H_{ai}^{H}$ refers to the line-of-sight (LoS) component, which can be formulated as the product of

---

3The proposed Algorithm 2 and Algorithm 3 can be extended to the scenarios with direct links.
the transmit and receive steering vectors. $\mathbf{H}_{ni}^{\text{ML}} \sim \mathcal{CN}(0, \mathbf{I})$ represents the non-LoS component. The path-loss exponent for $\mathbf{h}_{ni}$ is set to 2, and those for $\mathbf{h}_{1i}$, $\mathbf{h}_{2i}$, and $\mathbf{H}_{ce}$ are set to 2.8. The Rician factor for all channels is set to 5. Let $\kappa_2 = \epsilon_2/\|\mathbf{h}_2\|_2$ and $\kappa_e = \epsilon_e/\|\mathbf{H}_{ce}\|_F$ represent the maximum normalized error of the IRS-U2 and IRS-eavesdropper channels, respectively. The convergence tolerance $\bar{\rho}$ and $\bar{\varsigma}$ are set to 0.05 and $10^{-5}$, respectively. $\rho$ is set to 1.

For the performance comparison, we consider the following benchmarks. 1) Random Phase: The phase shift at each element is randomly selected from $[0, 2\pi)$ and the reflection amplitude is set as unit-norm. Thus, only the HBF is optimized. 2) Full Digital: The FDB is adopted by the BS, whose performance is an upper bound of the HBF due to more degrees of freedoms. 3) SRM-IRS [9]: The secure transmission scheme in [9] is adopted. Specifically, the sum rate is maximized subject to the QoS constraint of U2 and eavesdropping rate constraint. Furthermore, the BS adopts FDB and the eavesdropping rate threshold is set as 0.3 bps/Hz. 4) FDMA: The system adopts the frequency division multiple access and each user is allocated with half of the frequency band. Accordingly, the achievable rate of $k$th user can be formulated as

$$R_{k}^{\text{FDMA}} = \frac{1}{2} \log_2 \left(1 + \frac{\|\mathbf{h}_k\|^2}{\sigma^2} \right), \quad k = 1, 2. \tag{70}$$

A. Secrecy Rate Maximization

Fig. 2 illustrates the convergence of the proposed Algorithm 2 versus $N_t$ and $M$, with $(P_{\text{max}}, \zeta) = (25 \text{ dBm}, 0.3 \text{ bps/Hz})$. As shown in the figure, the proposed Algorithm 2 converges quickly. Furthermore, when $N_t$ and $M$ are larger, the proposed Algorithm 2 converges to a higher secrecy rate owing to the higher beamforming gain at BS and IRS. However, it needs more iterations to converge, because the dimensions of variables are proportional to $N_t$ and $M$.

Fig. 3 shows the average secrecy rate at U1 versus the maximum transmit power $P_{\text{max}}$, with $\zeta = 0.3 \text{ bps/Hz}$. We can observe that the average secrecy rate increases with $P_{\text{max}}$ for all the schemes. Moreover, the proposed secrecy rate maximization scheme (Scheme I) outperforms “FDMA”, “Random Phase” and “SRM-IRS [9]” significantly. Specifically, for “FDMA”, each user is allocated with half of the bandwidth, while the whole bandwidth in NOMA is utilized to serve all the users simultaneously, which leads to the better secrecy performance. Compared with the proposed Scheme I, “Random Phase” with limited IRS passive beamforming gain degrades the secrecy rate at U1. Rather than maximizing the secrecy rate of U1, “SRM-IRS [9]” aims to maximize the sum rate of the IRS-aided network, which accordingly underperforms Scheme I in secrecy rate. Moreover, the proposed Scheme I with HBF is much close to “Full Digital” in performance and has the advantages of lower hardware complexity and cost.

In Fig. 4, we investigate the sum rate versus $P_{\text{max}}$, with $\zeta = 0.3 \text{ bps/Hz}$. Fig. 4 shows that the sum rates of all the schemes increase with $P_{\text{max}}$. Furthermore, Scheme I outperforms “SRM-IRS [9]” when $P_{\text{max}}$ is small. However, the performance gap decreases with $P_{\text{max}}$ and “SRM-IRS [9]” is superior to Scheme I when $P_{\text{max}} = 30 \text{ dBm}$, which is driven by its sum rate maximization target. Furthermore, Scheme I is superior to “Full Digital” and “Random Phase”, but slightly inferior to “Full Digital”. “FDMA” outperforms “Random Phase” owing to the higher passive beamforming gain, however the performance gap decreases with $P_{\text{max}}$.

In Fig. 5, we show the average secrecy rate at U1 versus the number of reflecting elements, with $(P_{\text{max}}, \zeta) = (25 \text{ dBm}, 0.3 \text{ bps/Hz})$. From Fig. 5, we can conclude that the secrecy rates of all the schemes, except “SRM-IRS [9]”, increase with $M$, because extra reflecting elements can increase
both the receiving and reflecting beamforming gain of IRS. In addition, the proposed Scheme I outperforms “Random Phase”, “SRM-IRS [9]” and “FDMA”, and the performance gap widens with $M$. Besides, the secrecy rate of the proposed Scheme I is close to that of “Full Digital”.

Fig. 6 illustrates the average secrecy rate at U1 versus the rate threshold $\zeta$ at U2, with $P_{max}=25$ dBm. As shown in the figure, the secrecy rate decreases with $\zeta$ for all the schemes. This is because that U2 is allocated with more transmit power to satisfy its QoS constraint as the rate threshold $\zeta$ increases. Therefore, the SINR at U1 decreases with $\zeta$, which degrades the achievable secrecy rate. Moreover, the proposed Scheme I is superior to “Random Phase” and “FDMA” because of the higher passive beamforming gain and spectrum efficiency. In addition, “SRM-IRS [9]” underperforms Scheme I and the secrecy rate of it decreases with $\zeta$ dramatically.

We also calculate the SEE using the optimal parameters maximizing the secrecy rate or sum rate. Fig. 7 illustrates the SEE versus the antenna number at BS, with $(P_{max}, \zeta) = (25$ dBm, 0.3 bps/Hz). Ignoring the low power consumption of IRS, the SEE can be formulated as [37]

$$\text{SEE} = \frac{R_s}{P_{max} + N_r f P_{rf} + N_p s P_{ps} + P_B} \text{ (bps/Hz/W)},$$  

(71)

where $P_B = 0.2$ W denotes the baseband power consumption. $N_r f$ and $N_p s$ denote the number of RF chains and phase shifters, respectively. $P_{rf} = 0.3$ W and $P_{ps} = 0.04$ W represent the power consumed by each RF chain and phase shifter, respectively. For the FDB, $N_r f = N_i$ and $N_p s = 0$, while $N_r f = 2$ and $N_p s = 2N_i$ for the HBF. As shown in the figure, the proposed Scheme I outperforms the other benchmarks in SEE. Moreover, the SEEs of “Full Digital”
and “SRM-IRS [9]” decrease dramatically with $N_t$ owing to the increase of power-hungry RF chains. Therefore, the HBF is more suitable than the FDB for the deployment of massive antennas.

Fig. 8 investigates the secrecy rate at U1 versus the number of users $K$, with $(P_{\text{max}}, \zeta, N_t) = (25 \text{ dBm}, 0.15 \text{ bps/Hz}, 10)$. It can be seen that the performance of all the schemes decrease with $K$. For “FDMA”, the frequency band allocated to U1 decreases with $K$, which degrades the secrecy rate at U1. For the NOMA based schemes, the SINR at U1 decreases with $K$, because less transmit power is allocated to U1 for guaranteeing the successful SIC. Moreover, the proposed Scheme I significantly outperforms “FDMA” owing to higher spectrum efficiency.

**B. Achievable Rate Maximization**

As for the case of imperfect CSI, we also consider the “nonRobust” benchmark, which regards the estimated $h_2$ and $H_{ie}$ as the perfect CSI. Then, the achievable rate at U1 is maximized via optimizing the phase shifts and HBF. Moreover, the achievable rate of “nonRobust” is the upper bound of that of the proposed robust secure transmission scheme (Scheme II).

Fig. 9 illustrates the average achievable rate at U1 versus the maximum transmit power $P_{\text{max}}$, with $(\zeta, \xi, \kappa_2, \kappa_e) = (0.5 \text{ bps/Hz}, 1 \text{ bps/Hz}, 0.05, 0.05)$. Due to the fact that the additional transmit power can improve the SINR at U1, the average achievable rate increases with $P_{\text{max}}$ for all the schemes. As shown in Fig. 9, the proposed Scheme II is superior to both “Random Phase” and “FDMA” owing to the higher passive
beamforming gain and spectrum efficiency. Moreover, the average achievable rate of the proposed Scheme II is close to that of “Full Digital”. The performance gap between Scheme II and “nonRobust” increases with $P_{\text{max}}$. However, the performance gap between “FDMA” and “Random Phase” decreases with $P_{\text{max}}$, and “Random Phase” outperforms “FDMA” when $P_{\text{max}} = 40$ dBm. The detailed reasons are listed as follows. For “FDMA”, when $P_{\text{max}}$ is large, BS should decrease the transmit power to guarantee the robust eavesdropping rate constraint, which degrades the achievable rate of U1. For “Random Phase”, the BS can fully utilize the transmit power to improve the system performance via NOMA. As compared to “FDMA”, significant NOMA gains can be obtained by the directional hybrid beams, especially when $P_{\text{max}}$ is large. In addition, the signal for U2 with higher power acts as noise to confuse the eavesdropper, which further improves the secrecy performance of U1.

Fig. 10 depicts the average achievable rate at U1 versus the number of reflecting elements, with $(P_{\text{max}}, \zeta, \kappa_2, \kappa_e) = (25$ dBm, 0.5 bps/Hz, 1 bps/Hz, 0.05, 0.05). Due to that additional reflecting elements can improve both the receiving and reflecting beamforming gain of IRS, the average achievable rate increases with $M$ for all the schemes. However, the average rates of the robust transmission schemes increase with $M$ much slowly than “nonRobust” and the performance gap among the robust transmission schemes and “nonRobust” increases with $M$ significantly. Therefore, the perfect CSI is crucial for the performance of IRS-aided network, specifically when $M$ is large. Besides, the proposed Scheme II is superior to both “Random Phase” and “FDMA”, while slightly inferior to “Full Digital”.

Fig. 11 depicts the average achievable rate at U1 versus the maximum normalized error of $h_2$, with $(P_{\text{max}}, \zeta, \kappa_e) = (27.5$ dBm, 0.5 bps/Hz, 1 bps/Hz, 0.05). Fig. 12 shows the percentage of $p_2$ versus the maximum normalized error of $h_2$, with $(P_{\text{max}}, \zeta, \kappa_e) = (27.5$ dBm, 0.5 bps/Hz, 1 bps/Hz, 0.05). Fig. 13 shows the outage probability of U2 versus the maximum normalized error of $h_2$, with $(P_{\text{max}}, \zeta, \kappa_e) = (27.5$ dBm, 0.5 bps/Hz, 1 bps/Hz, 0.05). Fig. 14 shows the average achievable rate at U1 versus the rate threshold $\zeta$ at U2, with $(P_{\text{max}}, \kappa_2, \kappa_e) = (27.5$ dBm, 1 bps/Hz, 0.05, 0.05).
the maximum normalized error of h₂, with \((P_{\text{max}}, \zeta, \xi, \kappa_2, \kappa_e) = (27.5 \text{ dBm}, 0.5 \text{ bps/Hz}, 0.05, 0.05)\). As shown in the figure, the average achievable rates of all the schemes except “nonRobust” decrease with \(\kappa_2\), because more power is allocated to U2 to guarantee its worst-case QoS. Moreover, the average rate of “nonRobust” remains unchanged as \(\kappa_2\) increases, because the imperfect CSI is not taken into consideration. When \(\kappa_2\) is small, the average achievable rate of the proposed Scheme II is very close to that of “nonRobust”. However, the performance gap increases with \(\kappa_2\) significantly. Thanks to the higher passive beamforming gain and spectrum efficiency, the proposed Scheme II outperforms “Random Phase” and “FDMA”. Compared to the “FDMA”, the achievable rate at U1 of the NOMA-based schemes is more greatly affected by \(\kappa_2\), because more transmit power is allocated to U2 to guarantee the successful SIC.

Fig. 12 depicts the percentage of \(p_2\) versus the maximum normalized error of h₂, with \((P_{\text{max}}, \zeta, \xi, \kappa_e) = (27.5 \text{ dBm}, 0.5 \text{ bps/Hz}, 1 \text{ bps/Hz}, 0.05)\). As shown in the figure, the percentage of \(p_2\) for all the schemes except “nonRobust” increases with \(\kappa_2\), because more power is allocated to f₂ to guarantee the worst-case QoS of U2. Moreover, the percentage of \(p_2\) is more than 50% for the NOMA-based schemes due to the weaker channel gain of U2. However, for “FDMA”, more power is allocated to f₁ to maximize the achievable rate of U1. Moreover, compared with the NOMA-based robust transmission schemes, the percentage of \(p_2\) for “FDMA” increases with \(\kappa_2\) much slowly.

Fig. 13 depicts the outage probability of U2 versus the maximum normalized error of h₂, with \((P_{\text{max}}, \zeta, \xi, \kappa_e) = (27.5 \text{ dBm}, 0.5 \text{ bps/Hz}, 1 \text{ bps/Hz}, 0.05)\). Moreover, the outage probability of U2 is denoted as the probability that the QoS constraint of U2 is not satisfied. From Fig. 13, we can see that the outage probability of U2 is zero for all the schemes except “nonRobust”. The outage probability of U2 is very high and increases with \(\kappa_2\) for “nonRobust”. This is because all schemes except “nonRobust” consider the channel error of h₂ and the worst-case QoS constraint of U2 is satisfied, while “nonRobust” regards the estimated channel as perfect.

Fig. 14 illustrates the average achievable rate at U1 versus the rate threshold \(\zeta\) at U2 for all the schemes, with \((P_{\text{max}}, \zeta, \kappa_2, \kappa_e) = (27.5 \text{ dBm}, 1 \text{ bps/Hz}, 0.05, 0.05)\). As shown in the figure, the average achievable rates of all the schemes decrease with \(\zeta\), because U2 is allocated with more transmit power to guarantee its worst-case QoS. Moreover, the proposed Scheme II is superior to both “FDMA” and “Random Phase”, while slightly inferior to “Full Digital”. The performance gap between Scheme II and “nonRobust” increases with \(\zeta\).

Fig. 15 shows the average achievable rate at U1 versus the error propagation coefficient \(\theta\), with \((P_{\text{max}}, \zeta, \xi, \kappa_2, \kappa_e) = (27.5 \text{ dBm}, 1 \text{ bps/Hz}, 0.5 \text{ bps/Hz}, 0.05, 0.05)\). For all NOMA based schemes, the achievable rate at U1 decreases with \(\theta\), because the imperfect SIC degrades the SINR at U1. It can be seen that the performance of “FDMA” remains unchanged with \(\theta\). Moreover, NOMA based schemes become inferior to “FDMA” when \(\theta\) is large. Therefore, perfect SIC is critical to the performance of NOMA based schemes.

VI. CONCLUSION AND FURTHER WORK

In this paper, we deployed an IRS to boost the security of NOMA networks with cost-effective HBF. In addition, we proposed two schemes to guarantee the secure transmission of U1 under the case of perfect and imperfect CSI, respectively. With the perfect CSI, the secrecy rate of U1 was maximized via joint HBF and phase shifts optimization. To handle this non-convex problem with the constant modulus constraint and coupled variables, we first decomposed it into two subproblems, and then solved each subproblem via the penalty-based algorithm and the SCA. With the imperfect CSI, the achievable rate of U1 was maximized while satisfying its worst-case eavesdropping rate constraint and the QoS constraint of U2. We first relaxed the robust optimization problem to a more tractable one via S-Procedure and generalized S-Procedure. Then, an iterative algorithm based on the AO, the penalty-based algorithm and the SCA was proposed to further solve it. In the future, we will investigate the secure transmission for IRS-aided NOMA networks where the CSIs of all the channels are imperfect.

REFERENCES

Authorized licensed use limited to: University College London. Downloaded on September 05, 2023 at 16:19:50 UTC from IEEE Xplore. Restrictions apply.


Jifa Zhang received the M.S. degree from Beihang University, China, in 2023. He is currently pursuing the Ph.D. degree with the School of Information and Communication Engineering, Dalian University of Technology, China. His current research interests include unmanned aerial vehicle communications, optimization theory and intelligent reflection surface.

Wei Wang received the B.S. degree from the Hefei University of Technology, China, in 2018. He is currently pursuing the Ph.D. degree with the School of Information and Communication Engineering, Dalian University of Technology, China. His current research interests include non-orthogonal multiple access, wireless power transfer, and physical layer security.
Jie Tang (Senior Member, IEEE) received the B.Eng. degree from South China University of Technology, China, the M.Sc. degree from the University of Bristol, UK, and the Ph.D. degree from Loughborough University, UK. From 2013 to 2015, he was a research associate at the School of Electrical and Electronic Engineering, University of Manchester, UK. He is now a professor at the School of Electronic and Information Engineering, South China University of Technology, China.

His current research interests include SWIPT, UAV communications, NOMA, reconfigurable intelligent surface. He is currently serving as an Editor for IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE SYSTEMS JOURNAL, and IEEE ACCESS. He is the Guest Editor for two special issues in IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and one special issue in IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY. He also served as a Track Co-Chair of IEEE VTC-Spring 2018, Symposium Co-Chair of IEEE/CIC ICCC 2020, TPC Co-Chair of EAI GreeNets 2019, and Workshop Co-Chair of IEEE ICC/CIC 2019. He is a co-recipient of the ICNC 2018, CSPS 2018, WCSP 2019 and 6GN 2020 Best Paper Awards.

Nan Zhao (Senior Member, IEEE) is currently a Professor at Dalian University of Technology, China. He received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China. Dr. Zhao is serving on the editorial boards of IEEE Wireless Communications and IEEE Wireless Communications Letters. He won the best paper awards in IEEE VTC 2017 Spring, ICNC 2018, WCSP 2018 and WCSP 2019. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018.

Kai-Kit Wong (Fellow, IEEE) received the BEng, the MPhil, and the PhD degrees, all in Electrical and Electronic Engineering, from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. He is Chair Professor of Wireless Communications at the Department of Electronic and Electrical Engineering, University College London. His current research centers around 6G mobile communications. He is one of the early researchers who proposed multiuser MIMO. His first paper on multiuser MIMO was published in WCNC 2000 which appeared to be the first research paper on this topic. He is Fellow of IEEE and IET. He currently serves as the Editor-in-Chief for IEEE Wireless Communications Letters.

Xianbin Wang (Fellow, IEEE) received his Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001.

He is a Professor and a Tier-1 Canada Research Chair in 5G and Wireless IoT Communications with Western University, Canada. Prior to joining Western University, he was with the Communications Research Centre Canada as a Research Scientist/Senior Research Scientist from 2002 to 2007. From 2001 to 2002, he was a System Designer at STMicroelectronics. His current research interests include 5G/6G technologies, Internet of Things, communications security, machine learning, and intelligent communications. He has over 500 highly cited journals and conference papers, in addition to over 30 granted and pending patents and several standard contributions.

Dr. Wang is a Fellow of the Canadian Academy of Engineering and a Fellow of the Engineering Institute of Canada. He has received many prestigious awards and recognitions, including the IEEE Canada R. A. Fessenden Award, Canada Research Chair, Engineering Research Excellence Award at Western University, Canadian Federal Government Public Service Award, Ontario Early Researcher Award, and nine Best Paper Awards. He was involved in many IEEE conferences, including GLOBECOM, ICC, VTC, PIMRC, WCNC, CCECE, and CWIT, in different roles, such as General Chair, TPC Chair, Symposium Chair, Tutorial Instructor, Track Chair, Session Chair, and Keynote Speaker. He serves/has served as the Editor-in-Chief, Associate Editor-in-Chief, and editor/associate editor for over ten journals. He was the Chair of the IEEE ComSoc Signal Processing and Computing for Communications (SPCC) Technical Committee and is currently serving as the Central Area Chair for IEEE Canada.