Secrecy Outage Probability Fairness for Intelligent Reflecting Surface-Assisted Uplink Channel

Xiangrui Cheng*, Yiliang Liu†, Zhou Su‡, and Wei Wang†

*School of Software Engineering, Xi’an Jiaotong University, Xi’an 710049, China.
†School of Cyber Science and Engineering, Xi’an Jiaotong University, Xi’an 710049, China.
‡College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China.

Email: innsdcc@stu.xjtu.edu.cn, liuyiliang@xjtu.edu.cn, zhousu@ieee.org, wei_wang@nuaa.edu.cn

Abstract—This paper investigates physical layer security (PLS) in the intelligent reflecting surface (IRS)-assisted multiple-user uplink channel. Since the instantaneous eavesdropper’s channel state information (CSI) is unavailable, the secrecy rate can not be measured. In this case, existing investigations usually focus on the maximization of the minimum (max-min) of signal to interference plus noise power ratio (SINRs) among multiple users, and do not consider secrecy outage probability caused by eavesdroppers. In this paper, we first formulate the minimization of the maximum (min-max) secrecy outage probability among multiple users. The formulated problem is solved by alternately optimizing receiving matrix and phase shift matrix. Simulations demonstrate that the maximum secrecy outage probability is significantly reduced with the proposed algorithm compared to max-min SINR strategies, meaning our scheme has a higher security performance.

I. INTRODUCTION

Recently, intelligent reflecting surfaces (IRS) have attracted much attention due to their excellent potential for the development of 6G networks [1]. As a special meta surface with plenty of reflecting elements, it has the capability of controlling the scattering, reflection, and refraction characteristics of the radio waves. A large body of research has been motivated by IRS to enlarge coverage and improve spectral/energy-efficiencies for wireless communications [2], [3].

On account of increasing security threats of wireless communication, IRS has also been used to strengthen physical layer security (PLS) [4]–[8]. Many IRS-assisted PLS schemes have been conducted to focus on the maximization of secrecy rate by optimizing the phase shift matrix of IRS [5]–[7]. However, secrecy rate or sum secrecy rate of multiple users maximization methods have the following problems. Firstly, the instantaneous CSIs of eavesdroppers are usually unknown, so the secrecy rate can not be measured. It requires deriving the secrecy outage probability [4] to replace the secrecy rate as the optimization objective. Secondly, the sum secrecy rate maximization methods [7] are not suitable for the multiple user uplink channel because they do not consider the fairness of multiple users. Optimization algorithms being so fully engaged in sum secrecy rate maximization may provide some users with very low secrecy capacities or very large secrecy outage probabilities. Hence, a fairness mechanism should be considered in the optimization design. Due to the unknown eavesdropper’s instantaneous CSI, the researchers in [8]–[10] presented the max-min SINR strategy to improve the minimum main channel capacity among multiple users. Nevertheless, the max-min SINR strategy aimed at traditional communication fairness is not designed for minimizing secrecy outage probability, so secrecy outage probability fairness schemes for IRS need more in-depth research.

To solve these problems mentioned above, we formulate a min-max fairness problem in terms of secrecy outage probabilities in the multiple-user uplink channel, where the maximum secrecy outage probability among users can be reduced with the IRS-assisted scheme. To our knowledge, this is the first time the issue has been investigated. The main contributions of this work are summarized as follows.

- We formulate a multiple-user fairness problem in an IRS-assisted uplink channel to minimize the maximum secrecy outage probability among users.

- Since the formulated problem is non-convex and hard to solve, we first transform the original problem into the optimization problems of receiving matrix and phase shift matrix, and solve them via generalized Rayleigh quotient and generalized Dinkelbach’s algorithm. Then, we propose an alternating optimization (AO) algorithm to find the global results for the original problem.

The paper is organized as follows. The system model and problem formulation are introduced in Section II. Then, the alternating optimization algorithm is proposed in Section III. Simulation results are provided in Section IV and conclusions are presented in Section V.

Notations: Bold uppercase letters, such as \( \mathbf{A} \), denote matrices, and bold lowercase letters, such as \( \mathbf{a} \), denote column vectors. \( \mathbf{A}^\dagger \), \( \mathbf{A}^T \), and \( \mathbf{A}^H \) represent the conjugate transformation, transpose, and conjugate transpose of \( \mathbf{A} \), respectively. \( \mathbf{I}_a \) is an identity matrix with its rank \( a \). \( \mathcal{CN}(\mu, \sigma^2) \) is a complex normal (Gaussian) distribution with mean \( \mu \) and variance \( \sigma^2 \). \( (\mathbf{A})^{-1} \) is the inverse function of \( \mathbf{A} \). \( |\mathbf{x}| \) is the Euclidean norm of \( \mathbf{x} \). \( \text{diag}(\mathbf{x}) \) is the diagonal matrix of \( \mathbf{x} \). \( \text{vec}(\mathbf{A}) \) is the vectorization of the diagonal elements of \( \mathbf{A} \).

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

This paper considers an IRS-assisted multiple-user uplink channel as shown in Fig. I, including a base station (BS) with \( N_t \) antennas, an eavesdropper (Eve) with \( N_e \) antennas,
an IRS equipped with $N_s$ programmable phase shift elements, and $K$ legitimate users with single-antenna defined as $\mathcal{U} = \{U_1, \ldots, U_K\}$. Assume that wiretap channels obey spatially-uncorrelated Rayleigh fading, i.e., the channel from $U_k$ to Eve is defined as $h_{e,k} \sim \mathcal{CN}_{N_e,1}(0, I_{N_e})$, and the channel from IRS to Eve is defined as $G_e \sim \mathcal{CN}_{N_s,N_e}(0, I_{N_e}) \otimes I_{N_s}$. The channel from $U_k$ to BS is defined as $h_k \in \mathbb{C}^{N_s \times 1}$, the channel from IRS to BS is defined as $G \in \mathbb{C}^{N_s \times N_s}$, and the channel from $U_k$ to IRS is defined as $f_k \in \mathbb{C}^{N_e \times 1}$. $h_k$, $G$, and $f_k$ are assumed to be estimated perfectly. IRS controls programmable phase shift elements via a phase shift matrix, where the phase shift matrix is defined as an $N_s \times N_s$ matrix $\Phi$, i.e.,

$$\Phi = \text{diag}[\exp(j\theta_1), \ldots, \exp(j\theta_n), \ldots, \exp(j\theta_{N_s})],$$

and $\theta_n \in [0, 2\pi)$ is the phase introduced by the $n$-th phase shifter element of IRS.

In the uplink channels, with the phase shift matrix $\Phi$, the received signals at BS and Eve can be expressed as

$$y = (H + G\Phi F)x + n$$

$$= (h_k + G\Phi f_k)x_k + \sum_{i=1,i\neq k}^{K} (h_i + G\Phi f_i)x_i + n,$$

$$y_e = (H_e + G_e \Phi F)x + n_e,$$  

where $x_k$ is the confidential information-bearing signal of $U_k$ with the power constraint $\mathbb{E}[|x_k|^2] = \rho_k$, and $\rho_k$ is the fixed power of $U_k$, $n_0$ and $n_e$ is the additive white Gaussian noise (AWGN) obeying $\mathcal{CN}_{N_s,1}(0, \sigma_n^2 I_{N_s})$ and $\mathcal{CN}_{N_e,1}(0, \sigma_n^2 I_{N_e})$, respectively. $H$ is an extended channel matrix that combines $h_k$, $\forall k$ by column, do so $F$ and $H_e$. By following the channel model, the secrecy rate of $U_k$ is formulated as

$$C_{s,k} = (C_{m,k} - C_{w,k})^+.$$  

$C_{m,k}$ and $C_{w,k}$ are defined as the main channel capacity and wiretap channel capacity,

$$C_{m,k} = \log_2(1 + \text{SINR}_k),$$

$$\text{SINR}_k = \frac{\rho_k |w_k^H (h_k + G\Phi f_k)|^2}{w_k^H (K_k P\Phi K_k^H + \sigma_n^2 I_{N_s}) w_k},$$

$$P = \text{diag}(\rho_1, \ldots, \rho_{K-1}, \rho_{K+1}, \ldots, \rho_K),$$

$$C_{w,k} = \log_2 \left( 1 + \frac{\rho_k}{\sigma_n^2} |(h_{e,k} + G_e \Phi f_k)|^2 \right),$$

where $K_k = [h_1 + G\Phi f_1, \ldots, h_{k-1} + G\Phi f_{k-1}, h_{k+1} + G\Phi f_{k+1}, \ldots, h_K + G\Phi f_K]$ is an extended channel matrix that excludes $h_k + G\Phi f_k$. $C_{m,k}$ is achievable at BS when using the receiving vector $w_k^H$. The pessimistic condition is assumed that Eve has enough computing capacity to eliminate interuser interference and gather the power gain of desired signals, such as using joint minimum mean square error (MMSE) and successive interference cancellation (SIC) scheme [11].

B. Secrecy Outage Probability

However, the secrecy rate can not be measured due to the lack of $H_e$ and $G_e$. In this case, PLS usually uses secrecy outage probability as the security metric for PLS coding or optimization algorithms. The secrecy outage probability is defined as the probability that the targeted PLS coding rate of $U_k$ encoder, i.e., $R_k$, is larger than the secrecy rate $C_{s,k}$. From [12, Eq. (38)], the secrecy outage probability can be expressed as

$$P_k(R_k) = P(C_{s,k} \leq R_k | \text{transmission})$$

$$= P(C_{w,k} \geq C_{m,k} - R_k).$$  

Obviously, the priority of solving this problem is to find the expression of $P_k(R_k)$, which is formulated as follows.

Theorem 1 (Expression of secrecy outage probability). The secrecy outage probability of $R_k$ in $U_k$, i.e., $P_k(R_k)$, is expressed as

$$P_k(R_k) = \frac{1}{\Gamma(N_e)} \Gamma\left( N_e, \frac{\phi_k}{1 + \|f_k\|^2} \right),$$

where $\phi_k = \sigma_n^2 (2^{C_{m,k}-R_k} - 1) / \rho_k$, $C_{m,k}$ is defined in Eq. (5), $\Gamma(x)$ is the Gamma function with respect to $x$, and $\Gamma(\epsilon, \eta)$ is the upper incomplete Gamma function defined as follows,

$$\Gamma(\epsilon, \eta) = \int_{\eta}^{\infty} \exp(-z) z^{\epsilon-1} dz.$$  

Proof. See [4] Corollary 2.

C. Problem Formulation

To reduce the secrecy outage probability and guarantee user fairness, the optimization problem is to minimize the maximal secrecy outage probability (the min-max fairness) among the $K$ users, where the phase shift matrix and receiving matrix are jointly optimized, which is formulated as follows.

$$P_1: \min_{\Phi, W} \max_k P_k(R_k),$$

$$\text{s.t. } |\exp(j\theta_n)|^2 = 1, \quad n = 1, \ldots, N_s,$$

$$w_k^H w_k = 1, \quad k = 1, \ldots, K,$$
where $P_k(R_k)$ can be found in Eq. (8). $\Phi$ is the phase shift matrix, and $W \in \mathbb{C}^{K \times N_k}$ is the receiving matrix that combines $w_k^H \forall k$ by row. Eq. (11) corresponds to the unit-modulus requirements of the reflection elements at the IRS and Eq. (12) is the receiving vector constraint.

III. ALTERNATING OPTIMIZATION FOR MIN-MAX SECRECY OUTAGE PROBABILITY

According to Eq. (8), we use an auxiliary value $z_k$ as
\[
  z_k = \frac{\phi_k}{(1 + |\Phi f_k|^2)^2}.
\]
Since $N_e > 0$ and $z_k > 0$, we have
\[
  \frac{\partial \Gamma(N_e, z_k)}{\partial z_k} = -z_k N_e^{-1} \exp(-z_k),
\]
and it is concluded that the optimization objective $P_k(R_k)$ of $P1$ decreases with an increasing $z_k$. Hence, we can transform $P1$ into $P2$ as follows,
\[
P2: \max \min_{w_k} z_k, \quad \text{s.t. Eqs. (11) and (12).}
\]

Obviously, it is difficult to optimize $\Phi$ and $W$ as they are coupled, so we transform $P2$ into two subproblems as $P3$ and $P4$, i.e., the optimization problems of receiving matrix and phase shift matrix as follows,
\[
P3: \max \min_{w_k} z_k, \quad \text{s.t. Eq. (12).}
\]
\[
P4: \max \min_{\Phi} z_k, \quad \text{s.t. Eq. (11).}
\]

In Section III-A we solve $P3$ using the generalized Rayleigh quotient. $P4$ is solved by the SDR approach and generalized Dinkelbach’s algorithm in Section III-B. Then, we use an AO algorithm to find the global results for $\Phi$ and $W$ in Section III-C.

A. RECEIVING VECTOR OPTIMIZATION

For any given phase shift matrix $\Phi$, the secrecy outage probability of each user is independent of others. Hence, the optimization problem of each user is independent. In this case, $P3$ can be equivalently transformed into $P5$ as follows,
\[
P5: \min \max_{k} z_k, \quad \text{s.t. } w_k^H w_k = 1, k = 1, \ldots, K.
\]
To solve $P5$, $z_k$ in Eq. (19) can be transformed into Eq. (21) as follows,
\[
z_k = \frac{\phi_k}{(1 + |\Phi f_k|^2)^2}
\]
\[
  = c_1k \left( \frac{|w_k^H (h_k + G \Phi f_k)|^2}{w_k^H (K_k P_k^H + \sigma_b^2 I_{N_k}) w_k} + c_2k \right)
\]
\[
  = c_1k \left( \frac{|w_k^H (h_k + G \Phi f_k)|^2 (h_k + G \Phi f_k)^H w_k}{w_k^H (K_k P_k^H + \sigma_b^2 I_{N_k}) w_k} + c_2k \right)
\]
\[
  = c_1k \left( \frac{w_k^H A_k w_k}{w_k^H B_k w_k} + c_2k \right).
\]

where
\[
c_1k = \sigma_e^2/[2^{R_k} (1 + |f_k|^2)]
\]
\[
c_2k = \sigma_e^2(1 - 2^{R_k})/(\rho_k 2^{R_k} (1 + |f_k|^2))
\]
\[
A_k = (h_k + G \Phi f_k)(h_k + G \Phi f_k)^H
\]
\[
B_k = (K_k P_k^H + \sigma_b^2 I_{N_k}).
\]

According to Eq. (21), we can transform $P5$ into $P6$ as follows,
\[
P6: \min \max_{k} c_1k \left( \frac{w_k^H A_k w_k}{w_k^H B_k w_k} + c_2k \right),
\]
\[
\text{s.t. } w_k^H w_k = 1, k = 1, \ldots, K.
\]

For each user $k$, the optimal receiving vector, i.e., $w_k^*$ can be found by solving the inner maximization problem of $P6$ as follows,
\[
w_k^* = \arg \max_{w_k} c_1k \left( \frac{w_k^H A_k w_k}{w_k^H B_k w_k} + c_2k \right).
\]

It is obvious that $A_k$ and $B_k$ are Hermitian matrices and $B_k \succ 0$ according to Eqs (24) and (25). Thus, with the property of generalized Rayleigh quotient, the optimal $w_k$ can be derived as follows [13] Pro 2.1.1,
\[
w_k^* = \text{eigvec}_{\lambda_{max}}(B_k^{-1} A_k).
\]

where $\text{eigvec}_{\lambda_{max}}(X)$ means the corresponding eigenvector of the largest eigenvalue of matrix $X$, and $\lambda_{max}$ is the largest eigenvalue of $X$. For each user, we get the optimal receiving vector by Eq. (29), then we have the receiving matrix $W$ for fixed phase shift matrix $\Phi$. It can be said that the subproblem $P3$ is solved optimally.

B. PHASE SHIFT MATRIX OPTIMIZATION

In the IRS-assisted multiple-user model, the change of phase shift matrix $\Phi$ of IRS affects all users. Thus, we cannot consider this problem to be independent for each user as we did with $P3$. According to the Eq. (21), the $P4$ can be transformed into $P7$ as
\[
P7: \max \min_{\Phi} c_1k \left( \frac{|w_k^H (h_k + G \Phi f_k)|^2}{w_k^H (K_k P_k^H + \sigma_b^2 I_{N_k}) w_k} + c_2k \right),
\]
\[
\text{s.t. Eq. (11).}
\]

In order to solve $P7$ conveniently, we make the following mathematical transformations. The phase shift matrix $\Phi$ is
a diagonal matrix and \( f_k \) is a vector, so \( G \Phi \Phi f_k \) can be transformed as follows,

\[
G \Phi \Phi f_k = G \text{diag}(f_k) \text{vec}(\Phi) = E_k q,
\]

where

\[
q = \text{vec}(\Phi), \quad E_k = G \text{diag}(f_k).
\]

The denominator of the optimization objective of P7 can be transformed as follows,

\[
w_k^H (K_k P K_k^H + \sigma_b^2 I_{N_i}) w_k = w_k^H K_k P K_k^H w_k + t
\]

\[
= \sum_{i=1,i \neq k}^K \rho_i (h_i + E_i \hat{q})^H w_k + t
\]

\[
= \sum_{i=1,i \neq k}^K \rho_i (h_i^H w_k w_k^H h_i + h_i^H w_k E_i q + q^H E_i w_k w_k^H E_i q) + t
\]

\[
= \sum_{i=1,i \neq k}^K \rho_i (q^H M_{i,k} \hat{q} + v_{i,k}) + t,
\]

where \( t = w_k^H \sigma_b^2 I_{N_i} w_k \)

\[
M_{i,k} = \begin{bmatrix} E_i^H w_k w_k^H E_i & E_i^H w_k w_k^H h_i \\ h_i^H w_k w_k^H E_i & 0 \end{bmatrix},
\]

\[
v_{i,k} = h_i^H w_k w_k^H h_i,
\]

\[
\hat{q}^H = [\hat{q}^H, I], \quad E_i = G \text{diag}(f_i).
\]

and \( l \) is an auxiliary variable. Similarly, the numerator of the optimization objective of P7 can be transformed as

\[
|w_k^H (h_k + G \Phi f_k)|^2 = q^H M_{k,k} \hat{q} + v_{k,k},
\]

\[
\text{where } M_{k,k} \text{ and } v_{k,k} \text{ have the same structure with Eqs. (35) and (36) by replacing subscript } i \text{ with } k. \text{ According to the Eqs. (34) and (38), P7 can be transformed into P8 as follows.}
\]

\[
P8: \max_{q} \min_{k \neq 1,k} \left( \frac{q^H M_{i,k} \hat{q} + v_{i,k}}{\sum_{i=1,i \neq k}^K \rho_i (q^H M_{i,k} \hat{q} + v_{i,k}) + t} \right) + c_{2k}
\]

s.t. \( |\hat{q}_i|^2 = 1, \forall i = 1, ..., N_s + 1 \),

where \( \hat{q}_i \) is the \( i \)-th element in \( \hat{q} \). Notice that \( q^H M_{i,k} \hat{q} \) is a quadric form. By exploiting the fact that \( \text{tr}(ABC) = \text{tr}(BCA) \), \( q^H M_{i,k} \hat{q} \) can be transformed as follows,

\[
q^H M_{i,k} \hat{q} = \text{tr}(q^H M_{i,k} \hat{q})
\]

\[
= \text{tr}(M_{i,k} q \hat{q}^H)
\]

\[
= \text{tr}(M_{i,k} Q)
\]

where \( Q = \hat{q} \hat{q}^H \). Also, we have \( q^H M_{k,k} \hat{q} = \text{tr}(M_{k,k} Q) \). To address constraint (40), we introduce \( N_s + 1 \) auxiliary matrices \( E_n, n = 1, ..., N_s + 1 \) as follows,

\[
[E_n]_{i,j} = \begin{cases} 1, & i = j = n, \\ 0, & \text{otherwise}, \end{cases}
\]

\[
\text{Algorithm 1: Generalized Dinkelbach's Method for P9}
\]

\[
\text{Input: } G, H, F, P, \sigma_b, N_t, N_s, K, R_k
\]

\[
\text{Output: } Q^*
\]

1. Initialize \( \tau > 0, \lambda = 0; \)
2. do
3. \( Q^* = \arg \max_{Q \in S} \left\{ \min_{1 \leq k \leq K} \left\{ N_k(Q) - \lambda D_k(Q) \right\} \right\}; \)
4. \( F = \min_{1 \leq k \leq K} \left\{ N_k(Q^*) - \lambda D_k(Q^*) \right\}; \)
5. \( \lambda = \min_{1 \leq k \leq K} \frac{N_k(Q^*)}{D_k(Q^*)}; \)
6. while \( F > \tau \)
7. Get result \( Q^*; \)
8. Procedure End

where \( [E_n]_{i,j} \) is the \( (i, j) \)-th element of \( E_n \). With \( E_n, \forall n \), the constraint (40) can be transformed as \( q^H E_n \hat{q} = \text{trace}(E_n Q) = 1, \forall n = 1, ..., N_s + 1 \). Then, P8 can be transformed equivalently as

\[
P9: \max_{Q} \min_{k} \frac{c_{1k} (\text{tr}(M_{k,k} Q) + v_{k,k})}{\sum_{i=1,i \neq k}^K \rho_i (\text{tr}(M_{i,k} Q) + v_{i,k}) + t} + c_{2k},
\]

s.t. \( \text{rank}(Q) = 1 \),

\[
\text{tr}(E_n Q) = 1, \forall n = 1, ..., N_s + 1,
\]

\[
Q \geq 0,
\]

where the constraints in P9 are convex except the rank(\( Q \)) = 1 is a non-convex constraint. Thus, we apply semi-definite relaxation to relax this constraint to get a convex problem. P9 without the rank-one constraint can be regarded as an optimization problem that maximizes the ratios in which both the numerator and the denominator are affine, and generalized Dinkelbach’s algorithm is suitable to solve it. Generalized Dinkelbach’s algorithm belongs to the class of parametric algorithms, which can decompose P9 into a sequence of convex problems and obtain the global solution at a linear convergence rate [14].

In order to execute the generalized Dinkelbach’s algorithm conveniently, we denote the numerator and denominator of the optimization objective in P9 as \( N_k(Q) \) and \( D_k(Q) \),

\[
N_k(Q) = c_{1k} (\text{tr}(M_{k,k} Q) + v_{k,k}) + c_{2k} D_k(Q),
\]

\[
D_k(Q) = \sum_{i=1}^K \rho_i (\text{tr}(M_{i,k} Q) + v_{i,k}) + t.
\]

The constraints of P9 are denoted by a set \( S \) except for the rank-one constraint in Eq. (44) as follows,

\[
S = \{ Q \mid \text{Eqs. (45), (46)} \}.
\]

The procedure of solving P9 by generalized Dinkelbach’s algorithm is described in Algorithm[1] where \( \tau \) is an arbitrarily
small value. In detail, the step 3 in Algorithm 1 can be transformed by introducing an auxiliary value $u$,

\begin{align}
P10: & \max_u u, \\
& \text{s.t. } \mathbf{Q} \in \mathcal{S}, \\
& u \leq N_k(\mathbf{Q}) - \lambda_\alpha D_k(\mathbf{Q}), \forall k = 1, \ldots, K.
\end{align}

P10 is a convex problem, which can be solved by interior-point methods or MATLAB CVX tool.

By generalized Dinkelbach’s algorithm, we can obtain $\mathbf{Q}^*$. If $\text{rank}(\mathbf{Q}^*) = 1$, the optimal $\hat{\mathbf{q}}$, i.e., $\mathbf{q}^*$ can be obtained as follows,

$$
\hat{\mathbf{q}} = \text{eigvec}_{\lambda_{\text{max}}}(\mathbf{Q}^*).
$$

However, when $\text{rank}(\mathbf{Q}^*)$ is not equal to one, the near-optimal $\hat{\mathbf{q}}$ can be obtained by maximum eigenvalue methods or the Gaussian randomization method [15]. Here, we choose the Gaussian randomization method to obtain near-optimal $\hat{\mathbf{q}}$.

C. Alternating Optimization

In previous sections, we use the generalized Rayleigh quotient and generalized Dinkelbach’s algorithm to solve P3 and P4, respectively. Here, we design an AO algorithm for the global results of the receiving matrix and phase shift matrix, as shown in Algorithm 2.

**Algorithm 2: AO Algorithm for Receiving Matrix and Phase Shift Matrix.**

**Input:** $\mathbf{G}, \mathbf{H}, \mathbf{F}, \mathbf{P}, \mathbf{R}, \sigma_b, \sigma_c, N_t, N_s, N_c, R_k$

**Output:** $\mathbf{R}_e^*, \mathbf{W}_o^*$

1. Initialize $\text{iter} = 1$ and the iterating limit is $\text{iter}_{\text{max}}$;
2. Initialize receiving matrix $\mathbf{Q}_0^*$ randomly;
3. do
4. Solve P3 via generalized Rayleigh quotient to obtain $\mathbf{W}_{\text{iter}}^*$;
5. Obtain $\mathbf{Q}_{\text{iter}}^*$ with fixed $\mathbf{W}_{\text{iter}}^*$ by generalized Dinkelbach’s algorithm;
6. Calculate $P_k(R_k), \forall k$ via Eq. (8) and takes the maximum value for each user, i.e., $P_{\text{out}}(\text{iter})$;
7. Update $\text{iter} = \text{iter} + 1$;
8. while $\text{iter} < \text{iter}_{\text{max}} \& \& \{P_{\text{out}}(\text{iter}) - P_{\text{out}}(\text{iter} - 1) \leq \xi\}$
9. $\mathbf{Q}_o^* = \mathbf{Q}_{\text{iter}}^*, \mathbf{W}_o^* = \mathbf{W}_{\text{iter}}^*$;
10. Get $\hat{\mathbf{q}}_o^*$ via Gaussian randomization method of $\mathbf{Q}_o^*$;
11. Procedure End

In Algorithm 2, $\mathbf{Q}_{\text{iter}}^*$ and $\mathbf{W}_{\text{iter}}^*$ are local results with in the $\text{iter}$-th iteration, and $P_{\text{out}}(\text{iter})$ is the min-max secrecy outage probability in the $\text{iter}$-th iteration. We set an arbitrarily small value $\xi$, where the iteration process continues until $P_{\text{out}}(\text{iter}) - P_{\text{out}}(\text{iter} - 1) \leq \xi$. With the iteration, the receiving matrix and phase shift matrix are alternately optimized, and $P_{\text{out}}(\text{iter})$ gradually converges to constants, as do $\mathbf{Q}_{\text{iter}}^*$ and $\mathbf{W}_{\text{iter}}^*$. Then, the iteration terminated. To avoid the endless loop, we set $\text{iter}_{\text{max}}$ as the maximum number of allowed loops.

D. Computational Complexity Analysis

The computational complexity of Algorithm 2 is related to the number of iterations and the complexity of solving two subproblems in steps 4, 5, 10, respectively. According to Eq. (29), we know that step 4 requires $K(3N_t^2 + KN_s^2)$ iterations. Step 5 exploits Algorithm 1 to obtain the phase shift matrix with a linear convergence rate. The complexity of each iteration in Algorithm 1 is in the order of $O(K\ln(1/\epsilon)(KN_s)^4.5]$, where $\epsilon$ is the accuracy requirement of the interior-point method. According to Eq. (8), the computational complexity of step 6 is on the order of $O(K^2N_s^3)$. The computational complexity of step 10 is on the order of $O((I_A(KN_s^3 + K^2N_t^2 + IDK\ln(1/\epsilon)(KN_s)^4.5) + ICKN_s^3)$, where $I_C$ denotes the number of iterations of the Gaussian randomization method. In total, the computational complexity of Algorithm 2 is on the order of $O(I_A(KN_s^3 + K^2N_t^2 + IDK\ln(1/\epsilon)(KN_s)^4.5) + ICKN_s^3)$, where $I_A$ and $I_D$ denote the numbers of iterations of AO algorithm and generalized Dinkelbach’s algorithm, respectively.

IV. SIMULATIONS

In this section, simulation results are provided to test the proposed optimization scheme. The performance of the proposed scheme is tested in different $N_t, N_s$, and $N_c$, and the max-min SINR scheme [8]–[12] as a comparison for our proposed scheme. The number of users $K$ is set to 4 to simulate a multi-user scenario. The power $\rho_k$ is set to the same for all users, so is the PLS coding rate $R_k$.

We first perform a convergence test on the proposed AO algorithm. As shown in Fig. 2, we conducted convergence tests with different $N_s$. Where MM-SOP$^+$ and MM-SOP$^-$ mean the maximum and minimum value in multiple users respectively, with the proposed scheme that minimizes the maximum secrecy outage probability (MM-SOP). MM-SINR means the scheme that maximizes the minimum SINR [8]–[12]. In several independent simulations, our optimization objective, the maximum secrecy outage probability in multi-users, decreases rapidly in the first few iterations and converges to a constant in later iterations. The curve shows a good performance of the proposed AO algorithm. Compared
with the MM-SOP scheme, the secrecy outage probability gap between multi-users using the MM-SINR scheme is larger. In addition, the convergence rate is slower in $N_e = 32$ compared to that of $N_e = 64$. A larger number of IRS elements is more conducive to the system with the proposed scheme.

Fig. 3a shows the impact of $N_e$ on secrecy outage probability. We can find that the secrecy outage probability increases with an increasing $N_e$. In addition, Fig. 3a also shows that more antennas of BS or more IRS reflecting elements can decrease the maximum secrecy outage probability of users, both for MM-SOP and MM-SINR. Fig. 3b shows in more detail the impact of $N_s$ on the maximum secrecy outage probability. With the increase of $N_s$, the maximum secrecy outage probability gradually decreases. Fortunately, the reflecting elements of IRS are low-cost and can be equipped in large quantities. The impact of $N_t$ is shown in Fig. 3c. It can be observed that more BS antennas can reduce the secrecy outage probability and the system is more sensitive to $N_t$ than to $N_e$. Fig. 3a, 3b, and 3c also show that the performance of the MM-SOP scheme is superior than that of the MM-SINR scheme.

V. CONCLUSIONS

This paper focuses on the PLS without the instantaneous CSI of eavesdroppers in IRS-assisted multiple-user uplink channels. We have proposed an AO algorithm to minimize the maximum outage probability with fairness among multiple users. In detail, receiving vector of each user and phase shift matrix are optimized alternately by generalized Rayleigh quotient and generalized Dinkelbach’s algorithm, respectively. Simulation results have shown the excellent convergence performance of the AO algorithm. Moreover, the proposed scheme significantly reduces the maximum secrecy outage probability compared to the max-min SINR method.

REFERENCES

[1] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, “Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey,” IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2283–2314, Fourthquarter 2020.

[2] T. V. Nguyen, T. P. Truong, T. M. T. Nguyen, W. Noh, and S. Cho, “Achievable rate analysis of two-hop interference channel with coordinated IRS relay,” IEEE Trans. Wireless Commun., pp. 1–1, 2022.

[3] B. Zhang, C. You, W. Mei, and R. Zhang, “A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications,” Early Access in IEEE Commun. Surveys Tuts., DOI: 10.1109/COMST.2022.3155305.

[4] Y. Liu, Z. Su, C. Zhang, and H.-H. Chen, “Minimization of secrecy outage probability in reconfigurable intelligent surface-assisted mimo system.” [Online]. Available: https://arxiv.org/abs/2205.00204

[5] S. Xu, Y. Du, J. Liu, and J. Li, “Weighted sum rate maximization in IRS-BackCom enabled downlink multi-cell MISO network,” IEEE Commun. Lett., vol. 26, no. 3, pp. 642–646, Mar. 2022.

[6] L. Dong, H.-M. Wang, and H. Xiao, “Secure cognitive radio communication via intelligent reflecting surface,” IEEE Trans. Commun., vol. 69, no. 7, pp. 4678–4690, Jul. 2021.

[7] S. Asaad, Y. Wu, A. Berehiy, R. R. Muller, R. F. Schaefer, and H. V. Poor, “Secure active and passive beamforming in IRS-aided MIMO systems,” IEEE Trans. Inf. Forensics and Security, vol. 17, pp. 1300–1315, Mar. 2022.

[8] S. Wang and Q. Li, “Distributionally robust secure multicast beamforming with intelligent reflecting surface,” IEEE Trans. Inf. Forensics and Security, vol. 16, pp. 5429–5441, Nov. 2021.

[9] S. Gong, Z. Yang, C. Xing, J. An, and L. Hanzo, “Beamforming optimization for intelligent reflecting surface-aided swipt iot networks relying on discrete phase shifts,” IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8585–8602, 2021.

[10] Q.-U.-A. Nadeem, A. Kamnoum, A. Chaban, M. Debhah, and M.-S. Alouini, “Asymptotic max-min sum rate analysis of reconfigurable intelligent surface assisted mimo systems,” IEEE Transactions on Wireless Communications, vol. 19, no. 12, pp. 7748–7764, 2020.

[11] D. Tse and P. Viswanath, Fundamentals of wireless communication. Cambridge, England: Cambridge university press, 2005.

[12] Y. Liu, W. Wang, H.-H. Chen, F. Lyu, L. Wang, W. Meng, and X. Shen, “Physical layer security assisted computation offloading in intelligently connected vehicle networks,” IEEE Trans. Wireless Commun., vol. 20, no. 6, pp. 3555–3570, Jun. 2021.

[13] M. Absil, R. Mahony, and R. Sepulchre, Optimization algorithms on matrix manifolds. Princeton, New Jersey, US: Princeton University Press, 2009.

[14] A. Zappone and E. Jorswieck, “Energy efficiency in wireless networks via fractional programming theory,” Foundations and Trends in Communications and Information Theory, vol. 11, no. 3–4, pp. 185–396, 2015.

[15] Q. Wu and R. Zhang, “Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming,” IEEE Trans. Wireless Commun., vol. 18, no. 11, pp. 5394–5409, Nov. 2019.