Secrecy Outage Probability Fairness in Intelligent Reflecting Surface Assisted Uplink Channels – Alternating Optimization vs. Deep Learning

Yiliang Liu, Xiangrui Cheng, Zhou Su, Haixia Peng, Tom H. Luan, and Hsiao-Hwa Chen, *Fellow, IEEE*

***Abstract*—This paper explores the fairness issues on physical layer security (PLS) in intelligent reflecting surface (IRS) assisted multiple-user uplink channels. Due to unknown instantaneous eavesdropper channel state information (CSI), it is not possible to acquire exact secrecy rate of a PLS system. In this paper, we introduce secrecy outage probability (SOP) as a security metric, instead of secrecy rate as used in most existing works, and formulate a minimization problem of maximum (min-max) SOP among multiple users. To solve this problem, we propose two independent approaches: one is an alternating optimization (AO) and the other is a deep learning based (DL) scheme. The AO scheme decouples the problem into two sub-problems to alternately optimize phase shift matrix and receiving beamforming vectors, which gives a near-optimal performance but with a high complexity. The DL scheme, on the other hand, works based on neural networks through offline training, which is used for online generation of phase shift matrix and receiving beamforming vectors with a lower complexity. As traditional self-supervised neural networks cannot achieve a good solution to the max-min problem, we design a multiple-stage booster (MSB) framework to solve this problem. Simulations demonstrate that SOP is improved significantly with the proposed schemes compared to benchmark schemes. In particular, AO scheme slightly outperforms DL-based approach at the cost of a relatively high computational complexity.**

***Index Terms*—Physical layer security, intelligent reflecting surface, secrecy outage probability, min-max fairness, deep learning.**

I. INTRODUCTION

With the rapid development of wireless technologies, such as the Internet of Things (IoT) and the 5th-generation (5G) and beyond wireless communications, a large number of devices have been deployed. Due to the broadcast nature of wireless communications, their security has become a widely addressed issue. One of the most promising security technologies in wireless communications is physical layer security (PLS), which works based on the random characteristics of physical channels without any shared keys [1]. PLS leverages the channel difference between legitimate users and eavesdroppers to establish secure communications. To enlarge the capacity difference between the legitimate and eavesdropper channels, many PLS technologies have been developed, including massive multiple-input multiple-output (MIMO), artificial noise (AN), and relaying, etc. [2]–[5].

Recently, intelligent reflecting surfaces (IRS) technology has garnered a significant attention as a promising way to implement the 6th-generation (6G) mobile communications [6]. The IRS, made up of numerous reflecting elements, possesses its unique capability to control the directions of scattering, reflection, and refraction radio waves [7]. Consequently, there has been a surge in the research efforts exploring IRS's potential to enhance coverage, spectral efficiency, and energy efficiency of wireless communications [8]–[11]. Due to its ability to change wireless environment and its relatively low cost, IRS has also been studied to assist PLS in improving secrecy rate or security energy-efficiency of the system [12]–[16]. Next, we will briefly review the works on IRS-assisted PLS to highlight the challenges faced by the existing works.

A. Related Works

1) IRS-assisted PLS and Secrecy Fairness: Numerous IRS-assisted PLS schemes were developed with a primary focus on maximizing secrecy rate through optimization of IRS's phase shift matrix [12]–[14]. In [12], a simple single-user IRS-assisted communication system was considered with a multiple-antenna transmitter, a single-antenna receiver, and a single-antenna eavesdropper. Specifically, the authors proposed an AO scheme by alternately optimizing transmitting beamforming matrix and phase shift matrix of the IRS to maximize secrecy rate. Furthermore, the authors extended IRS-assisted PLS to multiple-user scenarios [13] and invoked fractional programming in the AO scheme to iteratively find the optimal beamforming and phase shift to maximize achievable weighted sum secrecy rate. However, the proposed sum secrecy rate maximization problem is not applicable in multiple-user fairness scenarios. For IRS-assisted multiple-user MISO systems, Li *et al.* proposed a max-min problem to maximize minimum secrecy rate among multiple legitimate users [14], which guarantees the worst-case secrecy rate among multiple users and is fairer than the sum-rate maximization schemes. In addition, IRS was also utilized to improve energy efficiency of secure communications [15], [16]. [15] took secrecy rate as a constraint to minimize transmit power by jointly optimizing phase shift matrix of IRS and transmitting beamforming, while ensuring that secrecy rate of each legitimate user is above

Yiliang Liu (email: liuyiliang@xjtu.edu.cn), Xiangrui Cheng (email: innsdcc@stu.xjtu.edu.cn), Zhou Su (email: zhousu@ieee.org), and Tom H. Luan (email: tom.luan@xjtu.edu.cn) are with the School of Cyber Science and Engineering, Xian Jiaotong University, China. Haixia Peng (email: haixia.peng@xjtu.edu.cn) is with the School of Information and Communications Engineering, Xian Jiaotong University, China. Hsiao-Hwa Chen (email: hshwchen@mail.ncku.edu.tw) is with the Department of Engineering Science, National Cheng Kung University, Taiwan. (Corresponding authors: Zhou Su, Hsiao-Hwa Chen)

a given threshold. Song *et al.* exploited IRS to optimize energy efficiency, i.e., the number of bits securely delivered to a destination per Joule of energy consumption of the communication system in [16]. Considering a multiple-input single-output single-antenna-eavesdropper (MISOSE) scenario as described in [12]–[14], [17] and [18] explored PLS issues with multiple-antenna receiver and multiple-antenna eavesdropper, and proposed AO schemes to maximize secrecy rate and energy efficiency, respectively.

2) Unknown Eavesdropper's CSI Issue: Although numerous results have been obtained in using IRS to achieve a higher secrecy rate, the aforementioned studies assumed that eavesdropper's instantaneous CSI is available to calculate the secrecy rate, which is usually impractical when eavesdroppers are passive and silent. Feng *et al.* simulated a lot of CSI samples as instantaneous eavesdropper's CSI to calculate an approximate secrecy rate and address the unknown eavesdropper's CSI issue [19]. However, simulating a large number of eavesdropper's CSI samples is time-consuming, and it is hard to verify whether the simulated data have the same patterns as real CSI. A traditional method to address the unknown eavesdropper's CSI issue is to derive SOP instead of secrecy rate as a security metric or optimization objective. For example, [20] studied an SOP minimization problem in a multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) IRS-assisted system. Specifically, the authors derived an expression of SOP, and then minimized the SOP with an AO approach.

3) DL-enabled IRS-assisted PLS: The aforementioned studies mainly used numerical optimization methods, such as AO schemes and semi-definite relax (SDR) technique, to optimize IRS phase shift and beamforming. However, optimization algorithms are usually time-consuming. Recently, deep learning (DL) based phase shift matrix optimization method has gained a lot of attention due to its superior computational efficiency compared to traditional methods. [21] used a supervised deep learning scheme to maximize secrecy rate, where beamforming and phase shift labels applied to train neural network were obtained still by numerical optimization algorithms. [22] tried to maximize sum channel capacity in a multiple-user IRS-aided system through an unsupervised neural network, which avoided pre-computation of labels by numerical optimization. Specifically, a loss function was set to a negative value of the sum channel capacity. In [23], the authors tried to optimize phase shift matrix by a deep reinforcement learning-based method to improve downlink signal-to-noise ratio (SNR). [24] maximized sum secrecy rate of multiple users in an IRS-assisted system by DRL and considered the impact of outdated CSI. [25] minimized SOP of an IRS-assisted single-user model via unsupervised learning. Since fixed CSIs are considered in state space, the learning model must be retrained when instantaneous CSI changes. To the best of our knowledge, the fairness issue of IRS-assisted communications/PLS has not been sufficiently investigated by DL-based schemes.

B. Contributions

In general, there are abundant studies on exploring IRS-assisted PLS. However, most current investigations usually considered secrecy rate fairness problem of IRS-assisted multiple-user channels, assuming that eavesdropper's CSI is available. To address this issue, we formulate a min-max fairness problem among multiple users in terms of SOP in uplink channels. The proposed approach involves using convex optimization or deep learning algorithms to minimize the maximum secrecy outage probability among users. The main contributions of this work can be summarized as follows.

1) Considering an IRS-assisted uplink channel, we address a multiple-user fairness problem. As instantaneous CSI of eavesdropper is unknown, we use SOP as a security performance metric instead of secrecy capacity or secrecy rate. Our objective is to minimize the maximum SOP among users by optimization of IRS phase shift and receiving beamforming.
2) As the formulated problem is non-convex, we decompose it into two separate optimization subproblems for receiving beamforming vectors and phase shift matrix. The receiving beamforming vector optimization is solved by generalized Rayleigh quotient approach, while the phase shift matrix optimization is done by generalized Dinkelbach's algorithm. Subsequently, we introduce an AO algorithm to iteratively obtain the global solutions of the optimization problem.
3) A DL-based multiple-stage booster (MSB) scheme is proposed to solve the min-max SOP problem. The MSB scheme can update the phase shift matrix and receiving beamforming vectors with multiple stages through neural networks instead of a time-consuming AO algorithm. In particular, MSB includes three networks. First, we propose a worst-user booster network (WUB-Net) to focus on reducing SOP of the current worst user. Second, we use an overall performance booster network (OPB-Net) to reduce SOP of all users. WUB-Net and OPB-Net update the phase shift matrix jointly. Third, a beamforming (BF) network is used to update the beamforming matrix once the phase shift of IRS is changed.
4) Extensive simulations demonstrate the effectiveness of the proposed AO and DL schemes in reducing the maximum SOP among multiple users. The maximum SOP is reduced significantly with the aid of IRS, and the proposed AO and DL schemes can outperform state-of-the-art schemes. In addition, security performance of the AO scheme has its advantage over DL, but DL is significantly faster than AO. Finally, we also test the sensitivity of DL scheme against parameter settings, to verify the robustness of the proposed DL scheme.

The rest of the paper is outline as follows. In Section II, we introduce the system model and problem formulation. The proposed AO scheme is presented in Section III. Section IV describes the proposed DL scheme. Simulation results are provided in Section V, followed by the conclusions in Section VI.

Notations: Bold uppercase letters, such as $\mathbf{A}$, denote ma-

trices, and bold lowercase letters, such as $\mathbf{a}$, denote column vectors. $\mathbf{A}^{\dagger}$, $\mathbf{A}^{\mathrm{T}}$, and $\mathbf{A}^{\mathrm{H}}$ 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 its mean μ and variance σ^2. $(\mathbf{A})^{-1}$ is the inverse function of $\mathbf{A}$. $|\mathbf{x}|$ is the Euclidean norm of $\mathbf{x}$. diag$(\mathbf{x})$ is the diagonal matrix of $\mathbf{x}$. vec$(\mathbf{A})$ is the vectorization of the diagonal elements of $\mathbf{A}$. $\Re(x)$ and $\Im(x)$ are real and imaginary parts of x, respectively. $a^{(t)}$ is a in the t-th iteration.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

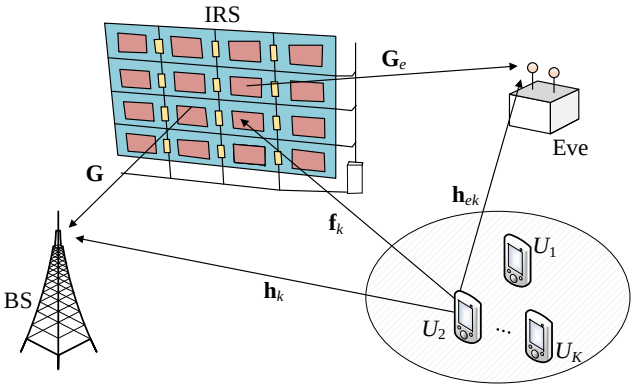


Fig. 1: An IRS-assisted PLS model in multiple-user uplink channels, which consists of K users with single-antenna, an IRS with N_s reflecting elements, a BS N_t antennas, and a passive eavesdropper with N_e antennas.

In the paper, we investigate an IRS-assisted PLS in multiple-user uplink channels, as illustrated in Fig. 1. The model comprises a base station (BS) equipped with N_t antennas, an N_e-antenna eavesdropper (Eve), an IRS with N_s programmable phase shift elements, and K legitimate users denoted as $\mathcal{U} = \{U_1, ...U_K\}$ with single-antenna. Since the location information of Eve is unknown, we consider the worst-case scenario where the path loss in Eve's channel model is assumed to be one. In contrast, the legitimate users' channels experience path loss, making their channel gains lower than that of Eve. Assume that wiretap channels suffer Rayleigh fading, the uplink channel between U_k and Eve is denoted as $\mathbf{h}_{e,k} \sim \mathcal{CN}_{N_e,1}(\mathbf{0}, \mathbf{I}_{N_e})$, and the IRS-to-Eve channel is represented as $\mathbf{G}_e \sim \mathcal{CN}_{N_e,N_s}(\mathbf{0}, \mathbf{I}_{N_e} \otimes \mathbf{I}_{N_s})$. The channels from U_k to BS, IRS to BS, and U_k to IRS are denoted as $\mathbf{h}_k \in \mathbb{C}^{N_t \times 1}$,$\mathbf{G} \in \mathbb{C}^{N_t \times N_s}$, and $\mathbf{f}_k \in \mathbb{C}^{N_s \times 1}$, respectively. It is assumed that $\mathbf{h}_k$,$\mathbf{G}$, and $\mathbf{f}_k$ can be estimated perfectly[1]. The phase shift elements of the IRS are regulated by a phase shift matrix denoted as $\mathbf{\Phi}$, which is an $N_s \times N_s$ matrix defined as follows,

$$\mathbf{\Phi} = \mathrm{diag}\big[\exp(j\theta_1), ..., \exp(j\theta_n), ..., \exp(j\theta_{N_s})\big], \quad (1)$$

and the n-th phase shift element in IRS can control the phase angle $\theta_n, \forall n$ within $[0, 2\pi)$.

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

$$\begin{aligned}\mathbf{y} &= (\mathbf{H} + \mathbf{G}\mathbf{\Phi}\mathbf{F})\mathbf{x} + \mathbf{n} \\ &= (\mathbf{h}_k + \mathbf{G}\mathbf{\Phi}\mathbf{f}_k)x_k + \sum_{i=1, i\neq k}^{K} (\mathbf{h}_i + \mathbf{G}\mathbf{\Phi}\mathbf{f}_i)x_i + \mathbf{n}, \quad (2)\end{aligned}$$

$$\mathbf{y}_e = (\mathbf{H}_e + \mathbf{G}_e\mathbf{\Phi}\mathbf{F})\mathbf{x} + \mathbf{n}_e. \quad (3)$$

The confidential message of U_k is represented as x_k, subject to a power limitation, i.e., $\mathbb{E}(|x_k|^2) = \rho_k$, where ρ_k denotes transmit power of U_k. Vector $\mathbf{x} = [x_1, x_2, ..., x_K]$ represents a message vector, encompassing the messages from all K users. Additionally, $\mathbf{n}_b$ and $\mathbf{n}_e$ correspond to additive white Gaussian noise (AWGN) that obey $\mathcal{CN}_{N_t,1}(0, \sigma_b^2\mathbf{I}_{N_t})$ and $\mathcal{CN}_{N_e,1}(\mathbf{0}, \sigma_e^2\mathbf{I}_{N_e})$, respectively. We define $\mathbf{H} \triangleq [\mathbf{h}_1, \mathbf{h}_2, ..., \mathbf{h}_K], \mathbf{F} \triangleq [\mathbf{f}_1, \mathbf{f}_2, ..., \mathbf{f}_K]$, and $\mathbf{H}_e \triangleq [\mathbf{h}_{e,1}, \mathbf{h}_{e,2}, ..., \mathbf{h}_{e,K}]$. Based on this model, secrecy rate of U_k can be expressed as

$$C_{s,k} = (C_{m,k} - C_{w,k})^+, \quad (4)$$

where $C_{m,k}$ and $C_{w,k}$ are defined as achievable rates for BS and Eve, respectively, to decode data sent by U_k, or

$$C_{m,k} = \log_2(1 + \mathrm{SINR}_k), \quad (5)$$

$$\mathrm{SINR}_k = \frac{\rho_k |\mathbf{w}_k^{\mathrm{H}}(\mathbf{h}_k + \mathbf{G}\mathbf{\Phi}\mathbf{f}_k)|^2}{\mathbf{w}_k^{\mathrm{H}}(\tilde{\mathbf{K}}_k\mathbf{P}\tilde{\mathbf{K}}_k^{\mathrm{H}} + \sigma_b^2\mathbf{I}_{N_t})\mathbf{w}_k},$$

$$\mathbf{P} = \mathrm{diag}(\rho_1, ..., \rho_{k-1}, \rho_{k+1}, ..., \rho_K),$$

$$C_{w,k} = \log_2\left[1 + \frac{\rho_k}{\sigma_e^2}|(\mathbf{h}_{e,k} + \mathbf{G}_e\mathbf{\Phi}\mathbf{f}_k)|^2\right], \quad (6)$$

where extended channel matrix $\tilde{\mathbf{K}}_k$ is defined as $[\mathbf{h}_1 + \mathbf{G}\mathbf{\Phi}\mathbf{f}_1, ..., \mathbf{h}_{k-1} + \mathbf{G}\mathbf{\Phi}\mathbf{f}_{k-1}, \mathbf{h}_{k+1} + \mathbf{G}\mathbf{\Phi}\mathbf{f}_{k+1}, ..., \mathbf{h}_K + \mathbf{G}\mathbf{\Phi}\mathbf{f}_K]$, excluding $\mathbf{h}_k + \mathbf{G}\mathbf{\Phi}\mathbf{f}_k$. Achievable $C_{m,k}$ is attained at BS when employing receiving beamforming vector $\mathbf{w}_k^{\mathrm{H}}$. Under a pessimistic assumption, Eve is assumed to possess sufficient computing resources to remove inter-user interference and collect transmit powers of desired signals [27].

B. Secrecy Outage Probability

As CSI in $\mathbf{H}_e$ and $\mathbf{G}_e$ are not available at users and BS, secrecy rate remains unmeasurable. In such scenarios, PLS commonly employs another performance metric, i.e., SOP, for PLS coding or optimization process. SOP denotes the probability that an intended PLS coding rate of encoder of U_k, denoted as R_k, surpasses secrecy rate $C_{s,k}$. According to [28, Eq. (38)], SOP can be formulated as

$$\begin{aligned}P_k(R_k) &= P(C_{s,k} \leq R_k \big| \text{Correctly decoding}) \\ &= P(C_{w,k} \geq C_{m,k} - R_k), \quad (7)\end{aligned}$$

[1]To estimate direct channel $\mathbf{h}_k$, all IRS elements are turned off so that the incident electromagnetic wave is absorbed completely by IRS instead of being reflected to the receiver. The IRS assisted communication system can be simplified as a conventional communication system without IRS. Hence, $\mathbf{h}_k$ can be estimated by pilot signals. To estimate $\mathbf{G}$, BS should work at a full-duplex mode to transmit pilots to IRS via downlink channel, and then IRS reflects pilots back to BS via uplink channel with a set of pre-designed reflection coefficients. Finally, BS estimates cascaded channel $\mathbf{h}_k + \mathbf{G}\mathbf{\Phi}\mathbf{f_k}$, and then calculates $\mathbf{f}_k$ with given $\mathbf{G}$ and $\mathbf{h}_k$ [26].

which calculates the conditional probability based on correct decoding at BS, under an assumption that rate $C_{m,k}$ is achievable at BS. The primary objective is to find the expression of $P_k(R_k)$.

Following [20, Corollary 2], we can see that SOP of U_k for a given PLS coding rate R_k, i.e., $P_k(R_k)$, can be expressed as

$$P_k(R_k) = \frac{1}{\Gamma(N_e)}\Gamma\Big(N_e, \frac{\phi_k}{1+|\mathbf{\Phi}\mathbf{f}_k|^2}\Big), \tag{8}$$

where $\phi_k = \sigma_e^2(2^{C_{m,k}-R_k}-1)/\rho_k$, $C_{m,k}$ is calculated by Eq. (5), $\Gamma(\epsilon,\eta)$ denotes the upper incomplete Gamma function, or

$$\Gamma(\epsilon,\eta) = \int_{\eta}^{\infty} \exp(-z) z^{\epsilon-1} \mathrm{d}z, \tag{9}$$

and $\Gamma(x)$ is the Gamma function of x.

C. Problem Formulation

To strike a good balance between minimizing SOP and ensuring fairness of multiple users, optimization objective is to minimize the maximum SOP (min-max fairness) among all users. This involves a joint optimization of phase shift matrix and receiving beamforming matrix, and can be expressed as

$$\begin{aligned}
\text{P1:}\ &\min_{\mathbf{\Phi},\mathbf{W}} \max_{k} P_k(R_k), && \text{(10a)}\\
&\text{s.t.}\ |\exp(j\theta_n)|^2 = 1, \quad n = 1,...,N_s, && \text{(10b)}\\
&\mathbf{w}_k^{\mathrm{H}}\mathbf{w}_k = 1, \quad k = 1,...,K, && \text{(10c)}
\end{aligned}$$

where $P_k(R_k)$ is obtained by Eq. (8), $\mathbf{\Phi}$ represents phase shift matrix, and $\mathbf{W} \in \mathbb{C}^{K\times N_t}$ is receiving beamforming matrix that includes $\mathbf{w}_k^{\mathrm{H}}$ for all k. Eqs. (10b) and (10c) denote the power constraints of reflection elements of the IRS and the receiving beamforming, respectively.

III. ALTERNATING OPTIMIZATION FOR MIN-MAX SOP

To transform Eq. (8) into a simpler form, we use an auxiliary value z_k given by

$$z_k = \frac{\phi_k}{(1+|\mathbf{\Phi}\mathbf{f}_k|^2)}. \tag{11}$$

As $N_e > 0$ and $z_k > 0$, we can obtain

$$\frac{\partial \Gamma(N_e, z_k)}{\partial z_k} = -z_k^{N_e-1}\exp(-z_k), \tag{12}$$

and it is concluded that expression $P_k(R_k)$ decreases with an increasing z_k. Therefore, P1 is transformed to P2, or

$$\begin{aligned}
\text{P2:}\ &\max_{\mathbf{\Phi},\mathbf{W}} \min_{k} z_k, && \text{(13a)}\\
&\text{s.t. Eqs. } (10b) \text{ and } (10c). && \text{(13b)}
\end{aligned}$$

Clearly, optimizing $\mathbf{\Phi}$ and $\mathbf{W}$ simultaneously is challenging due to their tight coupling with each other. Therefore, we split P2 into two problems, namely P3 and P4, which correspond to the optimization of receiving beamforming matrix and phase shift matrix, respectively.

$$\begin{aligned}
\text{P3:}\ &\max_{\mathbf{W}} \min_{k} z_k,\\
&\text{s.t. Eq. } (10c).\\
\text{P4:}\ &\max_{\mathbf{\Phi}} \min_{k} z_k,\\
&\text{s.t. Eq. } (10b).
\end{aligned}$$

First, P3 is solved by using the generalized Rayleigh quotient in Section III-A. In Section III-B, we deal with P4 with the help of SDR technique and generalized Dinkelbach's algorithm. In Section III-C, an AO scheme is used to obtain the final outputs of $\mathbf{\Phi}$ and $\mathbf{W}$ after the AO scheme is convergent.

A. Optimization of Receiving Beamforming Matrix

As each user in SOP is independent of others for any given phase shift matrix $\mathbf{\Phi}$, the optimization process of each user becomes independent too. As a result, P3 is equivalently transformed into the following problem, or

$$\begin{aligned}
\text{P5:}\ &\min_{k} \max_{\mathbf{W}} z_k, && \text{(14a)}\\
&\text{s.t. } \mathbf{w}_k^{\mathrm{H}}\mathbf{w}_k = 1,\ k = 1,...,K. && \text{(14b)}
\end{aligned}$$

To deal with P5, z_k in Eq. (14a) is changed by

$$\begin{aligned}
z_k &= \frac{\phi_k}{(1+|\mathbf{\Phi}\mathbf{f}_k|^2)}\\
&= c_{1k}\Big(\frac{|\mathbf{w}_k^{\mathrm{H}}(\mathbf{h}_k+\mathbf{G}\mathbf{\Phi}\mathbf{f}_k)|^2}{\mathbf{w}_k^{\mathrm{H}}(\tilde{\mathbf{K}}_k\mathbf{P}\tilde{\mathbf{K}}_k^{\mathrm{H}}+\sigma_b^2\mathbf{I}_{N_t})\mathbf{w}_k}\Big)+c_{2k}\\
&= c_{1k}\Big(\frac{\mathbf{w}_k^{\mathrm{H}}(\mathbf{h}_k+\mathbf{G}\mathbf{\Phi}\mathbf{f}_k)(\mathbf{h}_k+\mathbf{G}\mathbf{\Phi}\mathbf{f}_k)^{\mathrm{H}}\mathbf{w}_k}{\mathbf{w}_k^{\mathrm{H}}(\tilde{\mathbf{K}}_k\mathbf{P}\tilde{\mathbf{K}}_k^{\mathrm{H}}+\sigma_b^2\mathbf{I}_{N_t})\mathbf{w}_k}\Big)+c_{2k}\\
&= c_{1k}\Big(\frac{\mathbf{w}_k^{\mathrm{H}}\mathbf{A}_k\mathbf{w}_k}{\mathbf{w}_k^{\mathrm{H}}\mathbf{B}_k\mathbf{w}_k}\Big)+c_{2k}, && \text{(15)}
\end{aligned}$$

where

$$\begin{aligned}
c_{1k} &= \sigma_e^2/\big[2^{R_k}(1+|\mathbf{\Phi}\mathbf{f}_k|^2)\big], && \text{(16)}\\
c_{2k} &= \sigma_e^2(1-2^{R_k})/\big[\rho_k 2^{R_k}(1+|\mathbf{\Phi}\mathbf{f}_k|^2)\big], && \text{(17)}\\
\mathbf{A}_k &= (\mathbf{h}_k+\mathbf{G}\mathbf{\Phi}\mathbf{f}_k)(\mathbf{h}_k+\mathbf{G}\mathbf{\Phi}\mathbf{f}_k)^{\mathrm{H}}, && \text{(18)}\\
\mathbf{B}_k &= (\tilde{\mathbf{K}}_k\mathbf{P}\tilde{\mathbf{K}}_k^{\mathrm{H}}+\sigma_b^2\mathbf{I}_{N_t}). && \text{(19)}
\end{aligned}$$

Using Eq. (15), we transform P5 into P6 as

$$\begin{aligned}
\text{P6:}\ &\min_{k} \max_{\mathbf{W}} c_{1k}\Big(\frac{\mathbf{w}_k^{\mathrm{H}}\mathbf{A}_k\mathbf{w}_k}{\mathbf{w}_k^{\mathrm{H}}\mathbf{B}_k\mathbf{w}_k}\Big)+c_{2k}. && \text{(20a)}\\
&\text{s.t. } \mathbf{w}_k^{\mathrm{H}}\mathbf{w}_k = 1, k = 1,...,K. && \text{(20b)}
\end{aligned}$$

To find the optimal receiving beamforming vector $\mathbf{w}_k^*$ for U_k, we need to solve the inner maximization problem of P6, which can be expressed as

$$\mathbf{w}_k^* = \arg\max_{\mathbf{w}_k} c_{1k}\Big(\frac{\mathbf{w}_k^{\mathrm{H}}\mathbf{A}_k\mathbf{w}_k}{\mathbf{w}_k^{\mathrm{H}}\mathbf{B}_k\mathbf{w}_k}\Big)+c_{2k}. \tag{21}$$

Obviously, $\mathbf{A}_k$ is a Hermitian matrix and $\mathbf{B}_k$ is a Hermitian positive-definite matrix based on Eqs. (18) and (19). Therefore, utilizing the generalized Rayleigh quotient, we can derive the optimal $\mathbf{w}_k$ as [29, Proposition 2.1.1]

$$\mathbf{w}_k^* = \mathrm{eigvec}_{\lambda_{\max}}(\mathbf{B}_k^{-1}\mathbf{A}_k), \tag{22}$$

where $\lambda_{\max}$ is the largest eigenvalue of matrix $\mathbf{X}$ and eigvec$\lambda_{\max}(\mathbf{X})$ represents the corresponding eigenvector of $\lambda_{\max}$. Applying Eq. (22) to each user, we obtain the optimal receiving beamforming vectors. Combining these vectors yields the optimal receiving beamforming matrix $\mathbf{W}$ with a fixed phase shift matrix $\mathbf{\Phi}$. Here, P3 is solved optimally.

B. Optimization of Phase Shift Matrix

In the proposed model, adjustment of $\mathbf{\Phi}$ will affect all users' security performance. Therefore, we no longer view P4 as an individual optimization process for each user, in a way similar to that we treated P3. Instead, we resort to another algorithm as follows. With Eq. (15), P4 is transformed by P7 as

$$\text{P7: } \max_{\mathbf{\Phi}} \min_{k} c_{1k}\Big(\frac{|\mathbf{w}_k^{\mathrm{H}}(\mathbf{h}_k+\mathbf{G}\mathbf{\Phi}\mathbf{f}_k)|^2}{\mathbf{w}_k^{\mathrm{H}}(\tilde{\mathbf{K}}_k\mathbf{P}\tilde{\mathbf{K}}_k^{\mathrm{H}}+\sigma_b^2\mathbf{I}_{N_t})\mathbf{w}_k}\Big)+c_{2k}, \tag{23a}$$

$$\text{s.t. Eq. } (10b). \tag{23b}$$

To conveniently solve P7, we perform the following mathematical transformations. Owing to the fact that $\mathbf{f}_k$ is a vector and $\mathbf{\Phi}$ is a diagonal matrix, $\mathbf{G}\mathbf{\Phi}\mathbf{f}_k$ can be transformed as

$$\mathbf{G}\mathbf{\Phi}\mathbf{f}_k=\mathbf{G}\text{diag}(\mathbf{f}_k)\text{vec}(\mathbf{\Phi})=\mathbf{E}_k\mathbf{q}, \tag{24}$$

where $\mathbf{q}=\text{vec}(\mathbf{\Phi})$ and $\mathbf{E}_k=\mathbf{G}\text{diag}(\mathbf{f}_k)$. The bottom part in the brackets of P7 is transformed to

$$\begin{aligned}
&\mathbf{w}_k^{\mathrm{H}}(\tilde{\mathbf{K}}_k\mathbf{P}\tilde{\mathbf{K}}_k^{\mathrm{H}}+\sigma_b^2\mathbf{I}_{N_t})\mathbf{w}_k\\
&=\mathbf{w}_k^{\mathrm{H}}\tilde{\mathbf{K}}_k\mathbf{P}\tilde{\mathbf{K}}_k^{\mathrm{H}}\mathbf{w}_k+t\\
&=\sum_{i=1,i\neq k}^{K}\rho_i|(\mathbf{h}_i+\mathbf{E}_i\mathbf{q})^{\mathrm{H}}\mathbf{w}_k|^2+t\\
&=\sum_{i=1,i\neq k}^{K}\rho_i(\mathbf{h}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{h}_i+\mathbf{h}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{E}_i\mathbf{q}\\
&+\mathbf{q}^{\mathrm{H}}\mathbf{E}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{h}_i+\mathbf{q}^{\mathrm{H}}\mathbf{E}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{E}_i\mathbf{q})+t\\
&=\sum_{i=1,i\neq k}^{K}\rho_i(\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{i,k}\hat{\mathbf{q}}+v_{i,k})+t,
\end{aligned} \tag{25}$$

where

$$t=\mathbf{w}_k^{\mathrm{H}}\sigma_b^2\mathbf{I}_{N_t}\mathbf{w}_k,$$

$$\mathbf{M}_{i,k}=\begin{bmatrix}\mathbf{E}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{E}_i & \mathbf{E}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{h}_i\\ \mathbf{h}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{E}_i & 0\end{bmatrix}, \tag{26}$$

$$v_{i,k}=\mathbf{h}_i^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\mathbf{h}_i, \tag{27}$$

$$\mathbf{E}_i=\mathbf{G}\text{diag}(\mathbf{f}_i),\quad \hat{\mathbf{q}}^{\mathrm{H}}=\begin{bmatrix}\mathbf{q}^{\mathrm{H}}, & l\end{bmatrix}, \tag{28}$$

and l is an auxiliary parameter. Analogously, the top item in the brackets of P7 is expressed as

$$|\mathbf{w}_k^{\mathrm{H}}(\mathbf{h}_k+\mathbf{G}\mathbf{\Phi}\mathbf{f}_k)|^2=\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{k,k}\hat{\mathbf{q}}+v_{k,k}, \tag{29}$$

where structures of $\mathbf{M}_{k,k}$ and $v_{k,k}$ are the same as Eqs. (26) and (27), respectively, with the subscript i replaced by k. Utilizing Eqs. (25) and (29), P7 can be transformed into P8 as

$$\text{P8: } \max_{\hat{\mathbf{q}}} \min_{k} c_{1k}\Big(\frac{\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{k,k}\hat{\mathbf{q}}+v_{k,k}}{\sum_{i=1,i\neq k}^{K}\rho_i(\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{i,k}\hat{\mathbf{q}}+v_{i,k})+t}\Big)+c_{2k}, \tag{30a}$$

$$\text{s.t. } |\hat{q}_i|^2=1, i=1,...,N_s+1, \tag{30b}$$

where $\hat{q}_i$ represents the i-th value of $\hat{\mathbf{q}}$. Notably, $\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{i,k}\hat{\mathbf{q}}$ exhibits as a quadratic formula. We can utilize the property $\text{tr}(\mathbf{AB})=\text{tr}(\mathbf{BA})$ to transform $\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{i,k}\hat{\mathbf{q}}$ into

$$\begin{aligned}
\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{i,k}\hat{\mathbf{q}}&=\text{tr}(\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{i,k}\hat{\mathbf{q}})\\
&=\text{tr}(\mathbf{M}_{i,k}\hat{\mathbf{q}}\hat{\mathbf{q}}^{\mathrm{H}})\\
&=\text{tr}(\mathbf{M}_{i,k}\mathbf{Q}),
\end{aligned} \tag{31}$$

where $\mathbf{Q}=\hat{\mathbf{q}}\hat{\mathbf{q}}^{\mathrm{H}}$. Similarly, we obtain $\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{M}_{k,k}\hat{\mathbf{q}}=\text{tr}(\mathbf{M}_{k,k}\mathbf{Q})$. Constraint (30b) will be addressed by introducing N_s+1 auxiliary matrices, i.e., $\mathbf{E}_n, n=1,...,N_s+1$. The $(i,j)-$th element of $\mathbf{E}_n$ can be expressed as

$$[\mathbf{E}_n]_{i,j}=\begin{cases}1, & i=j=n,\\ 0, & \text{otherwise.}\end{cases} \tag{32}$$

With $\mathbf{E}_n$, constraint (30b) is transformed into $\hat{\mathbf{q}}^{\mathrm{H}}\mathbf{E}_n\hat{\mathbf{q}}=\text{trace}(\mathbf{E}_n\mathbf{Q})=1, n=1,...,N_s+1$. Next, P8 is transformed into P9 as

$$\text{P9: } \max_{\mathbf{Q}} \min_{k} \frac{c_{1k}(\text{tr}(\mathbf{M}_{k,k}\mathbf{Q})+v_{k,k})}{\sum_{i!=k}^{K}\rho_i(\text{tr}(\mathbf{M}_{i,k}\mathbf{Q})+v_{i,k})+t}+c_{2k}, \tag{33a}$$

$$\text{s.t. rank}(\mathbf{Q})=1, \tag{33b}$$

$$\text{tr}(\mathbf{E}_n\mathbf{Q})=1, n=1,...,N_s+1, \tag{33c}$$

$$\mathbf{Q}\succeq 0. \tag{33d}$$

All constraints of P9 are convex, except for constraint $\text{rank}(\mathbf{Q})=1$. To handle this non-convex constraint, this work uses SDR to relax $\text{rank}(\mathbf{Q})=1$, transforming the problem into a convex one. By removing the rank-one constraint, P9 becomes an optimization problem for maximizing the ratios between the numerator and denominator, which can then be solved using generalized Dinkelbach's algorithm, which is a parametric algorithm that decomposes P9 into a series of convex subproblems, to achieve the optimal results within a linear convergence time [30].

To execute this generalized Dinkelbach's algorithm, this work introduces notations $N_k(\mathbf{Q})$ and $D_k(\mathbf{Q})$ for the top and bottom parts of the fraction in the objective function of P9, or

$$N_k(\mathbf{Q})=c_{1k}(\text{tr}(\mathbf{M}_{k,k}\mathbf{Q})+v_{k,k})+c_{2k}D_k(\mathbf{Q}), \tag{34}$$

$$D_k(\mathbf{Q})=\sum_{i!=k}^{K}\rho_i(\text{tr}(\mathbf{M}_{i,k}\mathbf{Q})+v_{i,k})+t. \tag{35}$$

The constraints of P9, excluding the rank-one constraint in Eq. (33b), are represented by a set $\mathcal{S}$ as

$$\mathcal{S}=\big\{\mathbf{Q}\mid \text{Eqs. (33c), (33d)}\big\}. \tag{36}$$

The process of solving P9 using the generalized Dinkelbach's algorithm is outlined in Algorithm 1 with τ being an arbitrarily small parameter. Specifically, by introducing an

Algorithm 1: The generalized Dinkelbach's Algorithm for P9 with SDR.

Input: $\mathbf{H}, \mathbf{F}, \mathbf{G}, \mathbf{W}, N_t, N_s, \sigma_b^2, \sigma_e^2, K,\ R_k, \rho_k, \forall k$
Output: $\mathbf{Q}^*$
Initialize $\lambda = 0$ and $\tau > 0$;
do
  $\mathbf{Q}^* = \arg\max_{\mathbf{Q}\in\mathcal{S}} \{ \min_{1\le k\le K} [N_k(\mathbf{Q}) - \lambda D_k(\mathbf{Q})] \}$;
  $Z = \min_{1\le k\le K} \{ N_k(\mathbf{Q}^*) - \lambda D_k(\mathbf{Q}^*) \}$;
  $\lambda = \min_{1\le k\le K} \frac{N_k(\mathbf{Q}^*)}{D_k(\mathbf{Q}^*)}$;
while $Z > \tau$
Obtain the optimal value $\mathbf{Q}^*$;
Procedure End

auxiliary value u, Step 3 in Algorithm 1 is transformed into P10 as

$$\text{P10: } \max_{\mathbf{Q}} u, \tag{37a}$$

$$\text{s.t. } \mathbf{Q} \in \mathcal{S}, \tag{37b}$$

$$u \le N_k(\mathbf{Q}) - \lambda_n D_k(\mathbf{Q}),\ k = 1, ..., K. \tag{37c}$$

P10 is a convex problem and can be addressed efficiently using interior-point methods or MATLAB CVX toolbox.

Now, we can obtain $\mathbf{Q}^*$ by the generalized Dinkelbach's algorithm. If $\text{rank}(\mathbf{Q}^*) = 1$, the optimal $\hat{\mathbf{q}}^*$ is acquired by

$$\hat{\mathbf{q}}^* = \text{eigvec}_{\lambda_{\max}}(\mathbf{Q}^*). \tag{38}$$

If $\text{rank}(\mathbf{Q}^*) \neq 1$, to obtain a near-optimal $\hat{\mathbf{q}}$ is possible through the maximum eigenvalue method or Gaussian randomization method [31]. In this work, we opt for the Gaussian randomization method since it provides a more accurate result compared to the maximum eigenvalue method.

C. Alternating Optimization Scheme

In Sections III-A and III-B, we obtained the optimal value of either receiving beamforming matrix or phase shift matrix by fixing the other one. Here, we introduce an AO scheme in Algorithm 2 to attain a global optimization outputs for both receiving beamforming and phase shift.

In Algorithm 2, $\mathbf{Q}^*_{\text{iter}}$ and $\mathbf{W}^*_{\text{iter}}$ represent the optimal results within the iter-th iteration, while $P_{\text{out}}(\text{iter})$ indicates the maximum SOP in the iter-th iteration. The iteration process continues until the difference between $P_{\text{out}}(\text{iter})$ and $P_{\text{out}}(\text{iter}-1)$ is smaller than or equal to an arbitrarily small value ξ. Through multiple iterations, receiving beamforming matrix and phase shift matrix are alternatively optimized, resulting in gradual convergence of $P_{\text{out}}(\text{iter})$ to constants. The iteration process terminates once the convergence is achieved. To prevent an endless loop, we set $\text{iter}_{\max}$ as the maximum allowable number of iterations. Successful convergence of the scheme ensures to attain the optimal solutions for all subproblems [32]. At the convergence point, we utilize $\mathbf{Q}^*$ instead of $\mathbf{\Phi}^*$ because P10 yields the optimal result, while the Gaussian randomization method cannot guarantee optimality. Note that the outputs $\mathbf{\Phi}_0^*$ and $\mathbf{W}_0^*$ may not be the stationary points, and therefore they may yield suboptimal system performance [33]–[35]. Despite these limitations, we still chose to employ the conventional AO-based approach as a benchmark in this paper. This allows us to compare security performances between the AO scheme and the DL scheme.

Algorithm 2: AO Algorithm for Optimal Phase Shift and Receiving Beamforming.

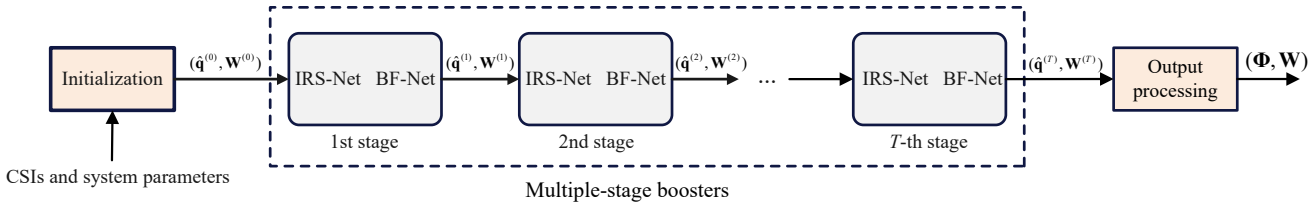
Input: $\mathbf{H}, \mathbf{F}, \mathbf{G}, N_t, N_s, N_e, \sigma_b^2, \sigma_e^2,\ R_k, \rho_k, \forall k$
Output: $\mathbf{\Phi}_{\text{o}}^*, \mathbf{W}_{\text{o}}^*$
Initialize $iter$ = 1, iteration limitation sets $iter_{\max}$;
Initialize $\mathbf{Q}_0^*$ randomly;
do
  Obtain $\mathbf{W}^*_{\text{iter}}$ in P3 by generalized Rayleigh quotient with $\mathbf{Q}^*_{\text{iter-1}}$;
  Solve P10 via generalized Dinkelbach's algorithm to obtain $\mathbf{Q}^*_{\text{iter}}$ with $\mathbf{W}^*_{\text{iter}}$;
  Compute $P_k(R_k), \forall k$ by Eq. (8), take maximum one among them, denoted by $P_{\text{out}}(iter)$;
  Update $iter$ = $iter$ + 1;
while $(iter < iter_{max}) \&\& \{P_{out}(iter) - P_{out}(iter-1) \le \xi\}$
$\mathbf{Q}_{\text{o}}^* = \mathbf{Q}^*_{\text{iter}}, \mathbf{W}_{\text{o}}^* = \mathbf{W}^*_{\text{iter}}$;
Obtain $\hat{\mathbf{q}}_{\text{o}}^*$ via Gaussian randomization with $\mathbf{Q}_{\text{o}}^*$;
Remove the last element of $\hat{\mathbf{q}}_{\text{o}}^*$ to get $\mathbf{q}_{\text{o}}^*$ and calculate $\mathbf{\Phi}_{\text{o}}^* = \text{diag}(\mathbf{q}_{\text{o}}^*)$;
Procedure End

D. Computational Complexity Analysis

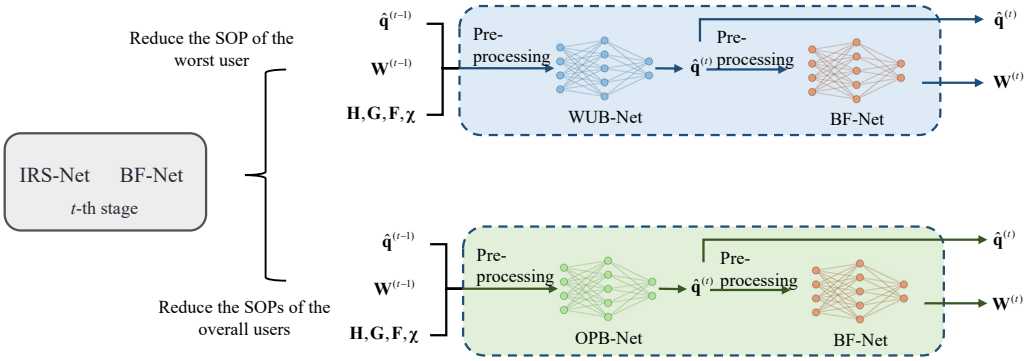
Computational complexity of Algorithm 2 depends on the number of iterations to solve two subproblems in Steps 4 and 5. In particular, Step 4 requires $K(3N_t^3 + KN_t^2)$ iterations, as given by Eq. (22). Step 5 utilizes Algorithm 1 to get the phase shift matrix, where the complexity is approximately $O[K\ln(1/\epsilon)(KN_s)^{4.5}]$, and ϵ represents the accuracy requirement of the interior-point method [36]. Furthermore, as per Eq. (8), the computational complexity of Step 6 is approximately $O(K^2N_s^3)$. Meanwhile, Step 10 has a computational complexity on the order of $O[(N_s)^3 + I_G K N_s^3]$, where I_G represents the number of iterations in the Gaussian randomization method. In conclusion, the computational complexity of Algorithm 2 can be estimated as $O(I_A(KN_t^3 + K^2N_t^2 + I_D K\ln(1/\epsilon)(KN_s)^{4.5}) + I_G K N_s^3)$, where I_A and I_D denote the numbers of iterations in the AO algorithm and generalized Dinkelbach's algorithm, respectively.

IV. DEEP LEARNING BASED APPROACH

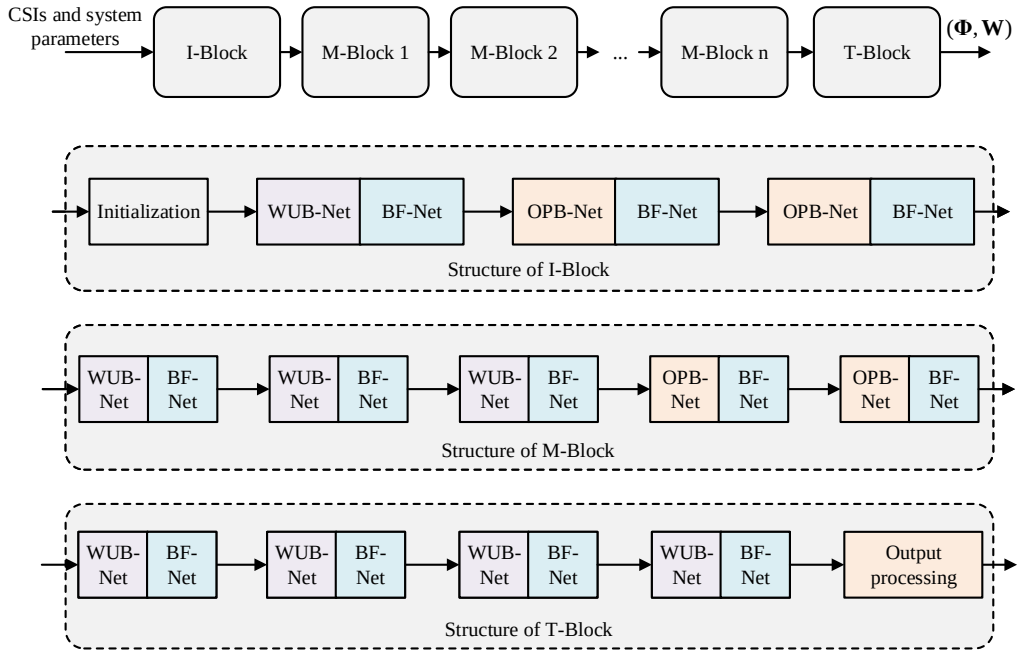
Although the proposed AO scheme can solve problem P1, its high computational complexity is unacceptable in some practical applications. Thanks to the development of deep learning algorithms, trained deep neural networks can generate the results quickly. Therefore, we apply deep neural networks to solve the min-max fairness problem with a relatively low computational complexity in this section. In our early works, we tried to solve this problem using a neural network framework as proposed in [22], [37]–[39], which is a popular DL scheme to solve the min-max fairness problem. With regard to the neural network framework [22], [37]–[39], the loss function of neural networks is designed as $-\min_k z_k$ to maximize the minimum z_k for K users. However, after a lot of experiments, we found that the neural network framework is



(a) The proposed MSB framework with T stages, where the input includes CSI $\{\mathbf{G}, \mathbf{H}, \mathbf{F}\}$ and system parameters $\boldsymbol{\chi} = \{\sigma_b^2, \sigma_e^2, N_t, N_s, N_e, R_k, \rho_k, \forall k\}$. An IRS-Net and a BF-Net are used in each stage to output phase shift vector and receive beamforming matrix, respectively. At the beginning, initial phase shift vector $\hat{\mathbf{q}}^{(0)}$ is generated randomly, and the corresponding receive beamforming matrix $\mathbf{W}^{(0)}$ is obtained by the generalized Rayleigh quotient (as shown in Eq. (22)) or a BF-Net (introduced in Section IV-C). The last stage outputs $(\hat{\mathbf{q}}^{(T)}, \mathbf{W}^{(T)})$, which is transmitted from output processing module and transformed into $\mathbf{W}^{(T)} = \mathbf{W}$ and $\mathbf{\Phi} = \text{diag}(\mathbf{q}^{(T)})$, where $\mathbf{q}^{(T)}$ is the vector $\hat{\mathbf{q}}^{(T)}$ to remove the last element.



(b) There are two different IRS-Nets, namely WUB network (WUB-Net) and OPB network (OPB-Net), to improve the performance of the worst user and overall performance, respectively. Behind each WUB-Net and OPB-Net, a BF-Net is used to generate a receiving beamforming matrix.



(c) Three block diagrams, namely I-Block, M-Block, and T-Block, to form the entire DL model.

Fig. 2: The proposed DL scheme to generate phase shift matrix and receiving beamforming matrix.

not suitable for solving the max-min problem in multiple-user scenarios because it just reflects the features of the minimum z_k but omits many significant features of other users.

Inspired by the proposed AO scheme, this work proposes an MSB scheme to tackle P1. The overview of the MSB framework is shown in Fig. 2a, where each stage consists of an IRS network (IRS-Net) and a receiving beamforming network (BF-Net). Without loss of generality, the t-th stage outputs phase shift vector $\hat{\mathbf{q}}^{(t)}$ and receiving beamforming matrix $\mathbf{W}^{(t)}$ based on the previous stage, respectively. The phase shift matrix $\mathbf{\Phi}$ and receiving beamforming matrix $\mathbf{W}$ in the last stage are the output from the model. Besides, the initial phase shift vector is generated randomly, and the initial receiving beamforming matrix is obtained through the generalized Rayleigh quotient in Eq. (22) or a BF-Net in Section IV-C.

As shown in Fig. 2b, there are two different IRS-Nets, namely worst-user booster network (WUB-Net) and overall performance booster network (OPB-Net). WUB-Net is designed to focus on the worst user (for a maximum SOP) and improves their security performance. Correspondingly, OPB is a network that improves overall performance. Behind each WUB-Net and OPB-Net, a BF-Net is used to generate a receiving beamforming matrix. The proposed multiple-stage framework needs the cooperation of WUB-Net and OPB-Net to minimize the maximum SOP among multiple users effectively. Based on a large number of experiments, we design a DL model with a block structure to employ the MSB framework, as shown in Fig. 2c. The DL scheme consists of one I-Block, several M-Blocks, and one T-Block. The I-Block is at the head of the DL model, and it consists of an initialization phase, a WUB-Net, and two OPB-Nets, where each network is followed by a BF-Net. On the other hand, the T-Block is at the end of the DL model and consists of four WUB-Nets, each of which is followed by a BF-Net. The M-Blcoks are in the middle of the DL model, which includes three WUB-Nets and two OPB-Nets. Also, each network is followed by a BF-Net, where the number of M-Blocks is adjustable. More M-Blocks will make the model perform better, but it will also increase the computation complexity. In the sections followed, we will discuss about the details of WUB-Net, OPB-Net, and BF-Net.

A. Worst-User Booster Network (WUB-Net)

The WUB-Net is a neural network, where the input is not only the CSI and system parameters, but also the receiving beamforming and phase shift vector obtained in the previous stage. The output of WUB-Net is the phase shift vector. Without loss of generality, if we focus on the t-th stage, the input includes $\mathbf{W}^{(t-1)}$ and $\hat{\mathbf{q}}^{(t-1)}$, and the output of WUB-Net is $\hat{\mathbf{q}}^{(t)}$. It is important to note that WUB-Net puts its focus on the worst-case users, which could potentially result in a significant drop in performance for the other users. In order to avoid this issue, we impose some limits on the capabilities of WUB-Net by restricting modifications to the phase shift within a certain range. Further details regarding the WUB-Net will be explained in the sequel.

1) WUB-Net Architecture: The WUB-Net architecture is shown in Fig. 3a, which is made up of 4 fully-connected (FC) layers with $128N_s, 64N_s, 16N_s$, and N_s neurons, respectively. We take LeakyReLU as the activation function of hidden layers. LeakyReLU is an improved version of the ReLU function, which gives a non-zero slope to negative values in ReLU. The output layer is an FC layer with N_s neurons, which corresponds to the number of elements of IRS. To limit the output range, scaled Tanh (sTanh) is taken as an activation function of the output layer, which is defined as

$$\text{sTanh}(\cdot) = \sigma_w \times \text{Tanh}(\cdot), \tag{39}$$

where σ_w is scale factor, and sTanh takes its value in $[-\sigma_w, \sigma_w]$.

2) Inputs: It is intuitive to use the CSI, system parameters, receiving beamforming, and phase shift vector at the previous stage as the input, i.e., $\mathbf{H}, \mathbf{G}, \mathbf{F}$, $\boldsymbol{\chi}$, $\mathbf{W}$, and $\hat{\mathbf{q}}$. However, these inputs should be pre-processed before training process. A multiple-user communication model is complex for neural networks, and raw data is difficult for neural networks to understand. Thus, we designed a feature processing method to enable the WUB-Net to pay a closer attention to the worst-case user, while the effect of the other users on this worst-case user is not ignored. At first, reflected channel and direct channel features are integrated into the tensor $\mathbf{M} \in \mathbb{C}^{K\times K\times(N_s+1)\times(N_s+1)}$ and the matrix $\mathbf{V} \in \mathbb{R}^{K\times K}$. For example, the k-th row and the k-th column of $\mathbf{M}$, i.e., $\mathbf{M}_{k,k} \in \mathbb{C}^{(N_s+1)\times(N_s+1)}$ is the effect of the k-th user's signal on the k-th user's reflected channel, and $\mathbf{M}_{i,k} \in \mathbb{C}^{(N_s+1)\times(N_s+1)}$ is the effect of the i-th user's signal on the k-th user's reflected channel, which are calculated by Eq. (26). Similarly, the k-th row and the k-th column of $\mathbf{V}$, i.e., $v_{i,k}$, is the effect of the i-th user's signal on the k-th user's direct channel, which is calculated by Eq. (27), and so does $v_{k,k}$. Then, IRS phase shift features of the previous stage are integrated into the matrix $\mathbf{C} \in \mathbb{R}^{(N_s+1)\times(N_s+1)}$ and $\mathbf{S} \in \mathbb{R}^{(N_s+1)\times(N_s+1)}$, whose i-th row and j-th column are defined as

$$[\mathbf{C}]_{i,j} = \Re(\hat{q}_i)\Re(\hat{q}_j) + \Im(\hat{q}_i)\Im(\hat{q}_j), \tag{40}$$

$$[\mathbf{S}]_{i,j} = \Im(\hat{q}_i)\Re(\hat{q}_j) - \Re(\hat{q}_i)\Im(\hat{q}_j), \tag{41}$$

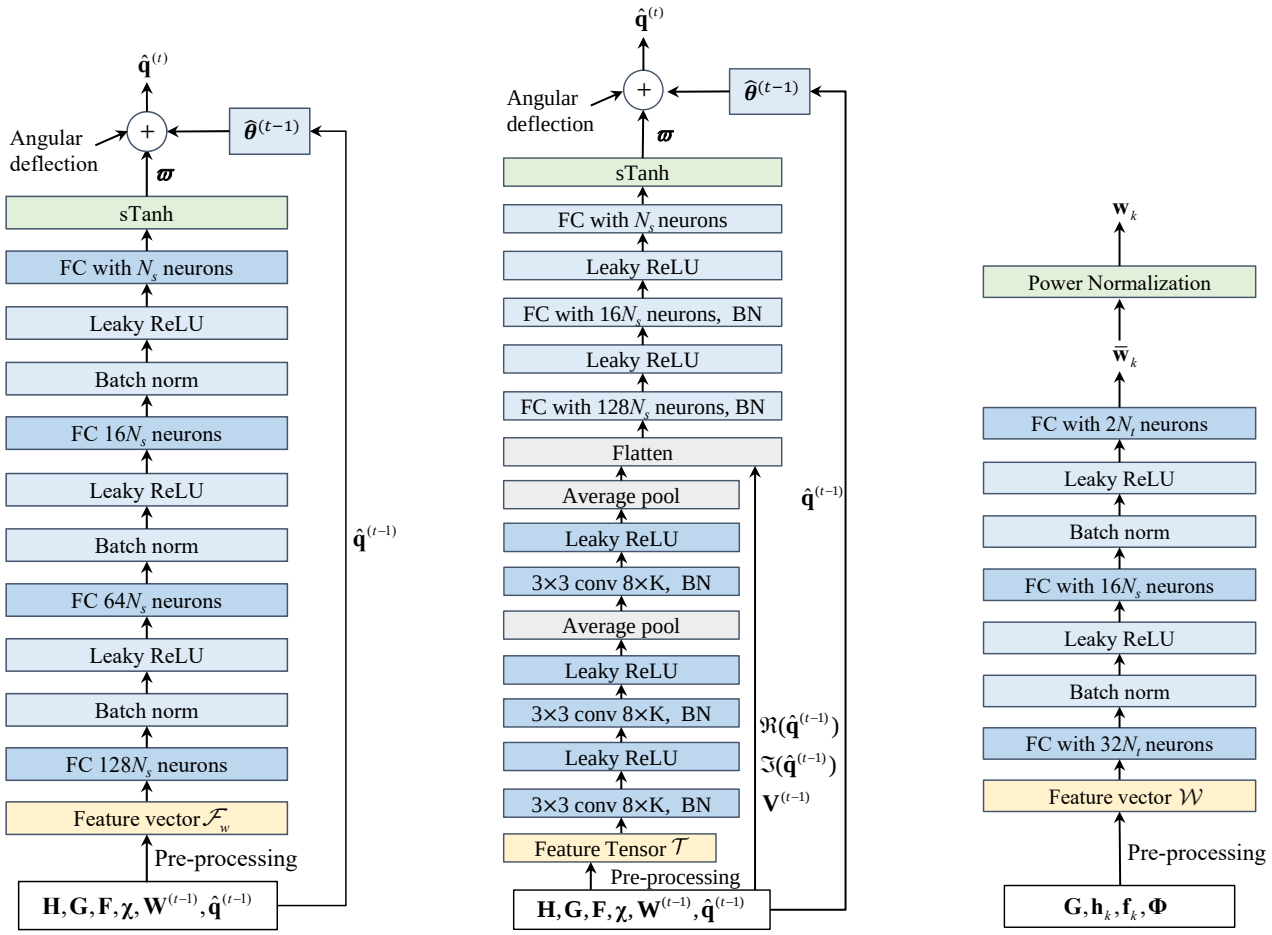
where $\hat{q}_i$ is the i-th element of $\hat{\mathbf{q}}$ of the previous stage, $\Re(x)$ and $\Im(x)$ mean the real and imaginary parts of a complex variable x, respectively. At last, the joint features of channel and IRS phase shift are generated by the tensor $\mathbf{U} \in \mathbb{R}^{K\times K\times(N_s+1)\times(N_s+1)}$ and $\mathbf{D} \in \mathbb{R}^{K\times K\times(N_s+1)\times(N_s+1)}$, which are defined as

$$\mathbf{U}_{i,j} = \Im(\mathbf{M}_{i,j}) \cdot \mathbf{C}, \tag{42}$$

$$\mathbf{D}_{i,j} = \Re(\mathbf{M}_{i,j}) \cdot \mathbf{S}, \tag{43}$$

where $\mathbf{U}_{i,j} \in \mathbb{R}^{(N_s+1)\times(N_s+1)}$ and $\mathbf{D}_{i,j} \in \mathbb{R}^{(N_s+1)\times(N_s+1)}$ are the i-th row and the j-th column of $\mathbf{U}$ and $\mathbf{D}$, respectively. Note that $\mathbf{A} \cdot \mathbf{B}$ represents the dot product of $\mathbf{A}$ and $\mathbf{B}$.

The WUB-Net is designed to improve the SOP of the worst-case user, i.e., the maximum SOP. Thus, assuming that the index of the current worst user is w, we select the features associated with user w, i.e., $\overline{\mathbf{U}}_w, \tilde{\mathbf{U}}_w, \overline{\mathbf{D}}_w$, and, $\tilde{\mathbf{D}}_w$, where $\overline{\mathbf{U}}_w = \mathbf{U}_{w,w}$, and $\overline{\mathbf{D}}_w = \mathbf{D}_{w,w}$. The $\tilde{\mathbf{U}}_w$ and $\tilde{\mathbf{D}}_w$



(a) WUB-Net architecture (b) OPB-Net architecture (c) BF-Net architecture

Fig. 3: The structures of WUB-Net, OPB-Net, and BF-Net.

are interferences generated from the other users, which are expressed as

$$\tilde{\mathbf{U}}_w = \sum_{i=1,i\neq w}^{K} \rho_i \mathbf{U}_{i,w}, \tag{44}$$

$$\tilde{\mathbf{D}}_w = \sum_{i=1,i\neq w}^{K} \rho_i \mathbf{D}_{i,w}. \tag{45}$$

After signal processing on the features, the original features of inputs are flattened into the feature of the worst-case user $\mathcal{F}_w = \text{flatten}(\overline{\mathbf{U}}_w, \tilde{\mathbf{U}}_w, \overline{\mathbf{D}}_w, \tilde{\mathbf{D}}_w, \mathbf{V}_{:,w}, \hat{\mathbf{q}})$, where $\mathbf{V}_{:,w}$ represents the w-th column of the matrix $\mathbf{V}$ and $\text{flatten}(\mathbf{A})$ is to expand the matrix $\mathbf{A}$ to a one-dimensional vector. $\mathcal{F}_w$ is used as the input of WUB-Net.

3) Output and Loss Function: Without loss of generality, let us focus on the t-th stage. The sTanh activation function follows the last FC layer of WUB-Net to limit the range of $(N_s \times 1)$ output vector $\boldsymbol{\varpi}$ at the current stage. With $\boldsymbol{\varpi}$, $\hat{\mathbf{q}}^{(t)}$ can be obtained based on $\hat{\mathbf{q}}^{(t-1)}$ in the previous stage with the skewing of $\boldsymbol{\varpi}$. Specifically, complex vector $\hat{\mathbf{q}}^{(t-1)}$ can be transformed by an angle vector $\hat{\boldsymbol{\theta}}^{(t-1)} = [\theta_1, \theta_2, ..., \theta_{N_s}, 0]$, where $-\pi \leqslant \theta_i \leqslant \pi, \forall i = 1, ..., N_s$. The $\hat{\boldsymbol{\theta}}^{(t)}$ can be obtained as

$$\hat{\boldsymbol{\theta}}^{(t)} = \left\{[(\hat{\boldsymbol{\theta}}^{(t-1)} + \pi) + \hat{\boldsymbol{\varpi}}], \mod 2\pi\right\} - \pi, \tag{46}$$

where $\hat{\boldsymbol{\varpi}} = [\boldsymbol{\varpi}, 0]$. Finally, $\hat{\mathbf{q}}^{(t)}$ can be obtained by

$$\hat{\mathbf{q}}^{(t)} = \exp(j\hat{\boldsymbol{\theta}}^{(t)}). \tag{47}$$

The loss function of WUB-Net is defined as follows,

$$\mathcal{L}_w = -\frac{1}{N}\sum_{n=1}^{N} z_{n,w}, \tag{48}$$

where N is the number of the samples in each batch of a training set, $z_{n,w}$ represents z_w of the worst user U_w screened out at this stage in the n-th sample, and z_w can be calculated by Eq. (11). The loss function reveals how the WUB-Net is designed to improve the performance of the worst-case user.

B. Overall Performance Booster Network (OPB-Net)

The OPB-Net is designed to improve security performance of the entire system, i.e., to reduce the sum of SOPs of all legitimate users. When improving the performance of the worst user in the training process of WUB-Net, the model may fall into a trap in a way that the worst-case user can be switched among a few fixed users, and the overall security performance

may not be improved. This seesaw-like phenomenon is due to the performance of the worst-case user being already close to that of other users during the training process. To solve this problem, we propose the OPB-Net to improve the overall system security.

1) OPB-Net Architecture: OPB-Net needs to pay attention to all legitimate users and has more complex inputs than WUB-Net. Thus, we take a convolutional neural network (CNN) to extract the features. As shown in Fig. 3b, OPB-Net consists of three convolutional (conv) layers and three FC layers. All convolutional layers are designed with $8K$ filters with a size of 3×3. A Leaky ReLU activation function is applied after the first convolutional layer. Each of the second and third convolutional layers is followed by a Leaky ReLU activation function and an average pooling layer. The three FC layers are designed with $128N_s, 16N_s$, and N_s neurons, respectively. To limit the output range, scaled Tanh (sTanh) is also taken as the activation function of the output layer with a scale factor σ_o, which is similar to Eq. (39).

2) Inputs: The pre-processing of OPB-Net's inputs is similar to that of WUB-Net. The input feature $\mathcal{T} \in \mathbb{R}^{4K\times(N_s+1)\times(N_s+1)}$ is a 3-D matrix, which can be viewed as $(N_s+1)\times(N_s+1)$ image data with $4K$ channels, i.e., $\mathcal{T} = \{\tilde{\mathbf{U}}_1, \overline{\mathbf{U}}_1, \tilde{\mathbf{D}}_1, \overline{\mathbf{D}}_1, \cdots, \tilde{\mathbf{U}}_K, \overline{\mathbf{U}}_K, \tilde{\mathbf{D}}_K, \overline{\mathbf{D}}_K\}$. Compared to WUB-Net, the inputs of CNN part are the features of all users instead of the features of the worst user. The 3D-tensor $\mathcal{T}$ is input into the convolutional layers for feature extraction, and then is flattened with other features, i.e., $\mathbf{V}^{(t-1)}$, $\Re(\hat{\mathbf{q}}^{(t-1)})$, and $\Im(\hat{\mathbf{q}}^{(t-1)})$. These three features are generated by the same method in WUB-Net, and serve as the input of the first fully connected layer.

3) Output and Loss Function: The sTanh activation function follows the last FC layer to limit the range of $\boldsymbol{\varpi}$, and $\hat{\mathbf{q}}^{(t)}$ can be obtained by Eqs. (46) and (47).

The loss function of OPB-Net in each stage is designed as follows:

$$\mathcal{L}_o = -\frac{1}{N}\sum_{i=1}^{N}\sum_{k=1}^{K} z_k. \tag{49}$$

The z_k is defined in Eq. (11), which can be calculated using the output of phase shift matrix and receiving beamforming matrix in each training process.

C. Beamforming Optimization Network (BF-Net)

The optimal receive beamforming vector can be obtained by Eq. (22), but $\text{eigvec}_{\lambda_{max}}(\cdot)$ has a high computational complexity. Thus, we use a simple neural network to replace $\text{eigvec}_{\lambda_{max}}(\cdot)$, namely BF-Net. As shown in Fig. 3c, the BF-Net is a simple 3-layer FC network with LeakyReLU as its activation function, and the three FC layers are designed with $32N_t, 16N_t$, and $2N_t$ neurons, respectively. A batch normalization layer is inserted between the FC layers in order to prevent overfitting and improve training efficiency.

The SOP of each user is independent of others with any phase shift matrix, so that the BF-Net can be trained by CSIs $\mathbf{G}, \mathbf{h}_k, \mathbf{f}_k$ and $\boldsymbol{\Phi}$. The original inputs of BF-Net are CSI and $\boldsymbol{\Phi}$ for single user, i.e., $\mathbf{G}, \mathbf{h}_k, \mathbf{f}_k$, and $\boldsymbol{\Phi}$. The feature vector $\mathcal{W}$ can be defined by $\text{flatten}([\Re(\mathbf{B}_k^{-1}\mathbf{A}_k), \Im(\mathbf{B}_k^{-1}\mathbf{A}_k)])$, where $\mathbf{A}_k$ and $\mathbf{B}_k$ are defined in Eq. (18) and Eq. (19), respectively.

The BF-Net outputs $2N_t$ values, where an half of which are used as the real part of $\bar{\mathbf{w}}_k$ and the other half are used as the imaginary part. The details of power normalization are given as

$$\mathbf{w}_k = \frac{\bar{\mathbf{w}}_k}{|\bar{\mathbf{w}}_k|}. \tag{50}$$

The loss function of BF-Net is designed as

$$\mathcal{L}_r = -\frac{1}{N} z_k, \tag{51}$$

where N is the number of samples in each batch of the training set, and z_k is calculated by Eq. (11). After BF-Net is trained, it is straightforward to obtain the entire $\mathbf{W}$ in the test process with CSI of K users.

D. Network Training

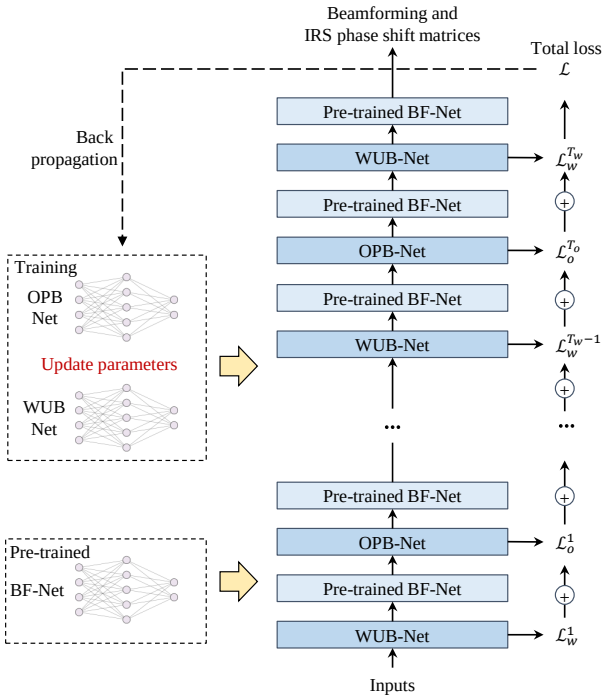


Fig. 4: Training processes for WUB-Net and OPB-Net.

The entire multiple-stage boosting model consists of three sub-models. In order to reduce the coupling between sub-models in training, we divide the process of training into two independent parts, i.e., training of the BF-Net and training of the WUB-Net and OPB-Net.

Training BF-Net: Since BF-Net is designed as an unsupervised model that does not require labels, the cost of dataset generation is quite low. The loss function shows exactly how the neural network is designed to improve the performance of BS signal detection. To update the loss function, BF-Net necessitates to have $\{\mathbf{G}, \mathbf{h}_k, \mathbf{f}_k, \boldsymbol{\Phi}\}$. The optimizer adopts adaptive moment estimation (Adam) with an initial learning rate of 0.01. To avoid oscillation, the learning rate decays by

0.3 when the validation loss does not decrease for 15 consecutive epochs. The batch size is 500. Additionally, early stop with a patience of 20 is implemented to prevent overfitting. Through extensive experiments, the BF-Net model can be used as a stable beamforming solver for pre-training the WUB-Net and OPB-Net.

Training WUB-Net and OPB-Net: The process of training WUB-Net and OPB-Net is shown in Fig. 4. Total loss $\mathcal{L}$ is the sum of the losses in each stage, given by

$$\mathcal{L} = \sum_{t=1}^{T_w} \mathcal{L}_w^{(t)} + \sum_{t=1}^{T_o} \mathcal{L}_o^{(t)}, \tag{52}$$

where T_w and T_o represent the numbers of worst-user booster stages and overall performance booster stages, respectively. The total loss function delineates how each neural network is designed specifically to enhance the performance for the worst-case user and all users. To update the loss function, the WUB-Net and OPB-Net require the inputs of $\{\mathbf{H}, \mathbf{G}, \mathbf{F}, \boldsymbol{\chi}, \mathbf{W}, \hat{\mathbf{q}}\}$. The pre-trained BF-Net does not update parameters, and the batch size is 500. The optimizer uses Adam with a lower initial learning rate of 0.001 compared to BF-Net training.

The training processes were conducted using Python 3.10.6, Cuda 11.3, and PyTorch 1.12.1 on a server equipped with a GeForce GTX 3090 GPU. After BF-Net, WUB-Net, and OPB-Net are trained, we establish a multiple-stage network framework, as shown in Fig. 2, to output the phase shift matrix and beamforming matrix as the solutions of P1. When the neural network has been trained, the parameters are fixed, so that solving the optimization problem P1 becomes simple matrix computations, and the computational complexity of the DL-based approach is approximated as $O(N_s^2 + N_t K N_s)$.

V. SIMULATIONS

In this section, we present simulation results to evaluate the performance of the proposed AO and DL schemes. The performance was tested with different values of N_t, N_s, N_e, SNR, and R_k. To simulate a multiple-user scenario, we set the number of users K to 4. For simplicity, power ρ_k and PLS coding rate R_k were set to be the same for all users. We generated 16,500 CSI samples using MATLAB, with 12,500 samples for training, 2,000 samples for validation, and other 2,000 samples for testing, respectively. The Monte Carlo simulations for non-DL schemes were conducted simultaneously using the 2,000 testing samples.

A log-normal shadowing path loss model was considered with its parameters similar to those used in [11]. The path loss and SNR parameters can be calculated by

$$\begin{aligned} \text{PL} &= -20\log_{10}\left(\frac{\upsilon}{4\pi d_0}\right) + 10\chi\log_{10}\left(\frac{d}{d_0}\right) + \text{L}_{\text{shadow}}, \\ \text{SNR} &= 10\log_{10}(P_{\text{mW}}) - \text{PL} - \text{AWGN}_{\text{dBm}}, \end{aligned} \tag{53}$$

where $\upsilon = 3 \times 10^8/f_c$, f_c is carrier frequency, d_0 is the reference distance, χ is a path loss exponent, L_{shadow} is shadowing fading that is assumed to be a Gaussian variable, P_{mW} is transmit power, AWGN_{dBm} is AWGN that is set to be $-174 + 10\log_{10}(W_b)$, W_b is the bandwidth, and d is the distance between BS and users, which obeys a uniform distribution. These parameters are listed in TABLE I.

TABLE I: Simulation parameters.

Parameters	Value
Carrier frequency	2 GHz
Alice-to-Bob distance	Uniform in [40, 80] m
Reference distance	1 m
Bandwidth size	20 MHz
Path loss exponent	3
Rician factors of legitimate channels	3
Shadowing fading variance	9

The small-scale fading parts of $\mathbf{h}_k$,$\mathbf{G}$, and $\mathbf{f}_k$ obey Rician distributions. For example, $\mathbf{h}_k \sim \mathcal{CN}_{N_t,1}(\sqrt{\kappa_k/(1+\kappa_k)}\mathbf{a}_k, 1/(1+\kappa_k)\mathbf{I}_{N_t})$, where κ_k is Rician factor and $\mathbf{a}_k$ is the line of sight component. $\mathbf{G}$ and $\mathbf{f}_k$ take the same format as $\mathbf{h}_k$.

The performance of the proposed schemes is compared with the following six different schemes in the same scenario.

1) Without IRS: In this scheme, IRS is removed. The receiving beamforming vector of user k is given by $w_k = \text{eigvec}_{\lambda_{max}}((\tilde{\mathbf{K}}_k \mathbf{P} \tilde{\mathbf{K}}_k^{\text{H}} + \sigma_b^2 \mathbf{I}_{N_t})^{-1}(\mathbf{h}_k \mathbf{h}_k^{\text{H}}))$, where $\tilde{\mathbf{K}}_k = [\mathbf{h}_1, ..., \mathbf{h}_{k-1}, \mathbf{h}_{k+1}, ..., \mathbf{h}_K]$ represents interference from other users.

2) Random Phase Shift (Random $\boldsymbol{\Phi}$): Each phase shift, i.e., θ^n in $\boldsymbol{\Phi}$ is generated randomly in $[-\pi, \pi]$, and $\mathbf{w}_k$ will be calculated by random $\boldsymbol{\Phi}$ using Eq. (22).

3) AO Scheme (AO): The AO scheme was proposed in Section III, which initializes $\boldsymbol{\Phi}$ randomly, and then alternately optimizes $\boldsymbol{\Phi}$ and $\mathbf{w}_k$ to reach the optimal solution.

4) Single-loss Neural Networks (Single-loss Net): The two networks generate phase shift matrix and beamforming vectors, respectively [22]. Specifically, the network in the first stage is composed of two convolutional layers and three FC layers. The two convolutional layers have 128 filters with a size of 2×2 and 256 filters with a size of 2×2, respectively. The three FC layers of the first stage are designed with $128N_s, 16N_s,$ and N_s neurons, respectively. The second network is a three-layer FC layer similar to BF-Net. Besides, LeakyReLU is the activation function, and the batch normalization layer is used in each layer. The loss function is set to $-\sum_{i=1}^{N} \min_k z_k, \forall k = 1 \dots K$, where N is the number of the samples in each batch. The similar single-loss functions for min-max or max-min problems can be found in [37]–[39].

5) Proposed MSB with BFNet (MSB-BFNet): The proposed MSB framework is used here, where BFNet is to obtain receiving beamforming vector $\mathbf{w}_k$. Through extensive experiments, 10 M-Blocks are used in this framework.

6) Proposed MSB with Generalized Rayleigh Quotient (MSB-Rayleigh): The proposed MSB framework is used again, where receiving beamforming vector is solved by generalized Rayleigh quotient, i.e., Eq. (22). A closed-form solution is usually better than BFNet approach, but it takes a longer time for eigenvalue decomposition. Also, 10 M-Blocks are used in this framework.

Note that all CSI samples were generated using MATLAB. Python was employed for training and validation processes

with these CSI samples to acquire the trained neural networks. During the testing process, both AO-based and DL-based schemes were executed in MATLAB, where the DL-based schemes were loaded with the trained neural networks.

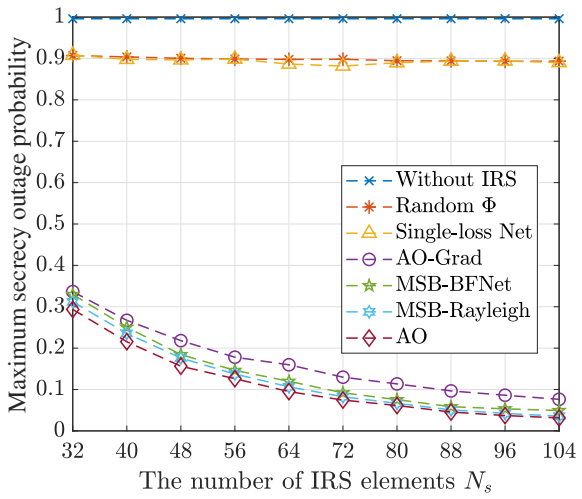


Fig. 5: Impact of N_s, where $N_t = 8$, $N_e = 2$, SNR = 1 dB, and $R_k = 2.5$ bit/s/Hz.

In Fig. 5, we illustrate the impact of the number of IRS elements, denoted as N_s, on the maximum SOP. It is noteworthy that an increase in the number of IRS elements results in a decrease in the maximum SOP. The maximum SOP value in the case without IRS scheme remains to be high consistently. These results indicate a fact that effective configuration of IRS is crucial, and simply increasing the number of elements and configuring them randomly are not effective, leading to a waste of resources. With the increase in the number of IRS elements, a slight decrease in the maximum SOP in the random $\mathbf{\Phi}$ scheme is observed. It is worth noting that Single-loss Net scheme performs similarly to random $\mathbf{\Phi}$ scheme, suggesting that Single-loss Net is not suitable for max-min problem. We can observe a phenomenon in which security performance with $N_s = 80$ is not as good as that with $N_s = 72$. This is caused by the instability and a poor performance of the Single-loss Net scheme. Simulations also demonstrated that Single-loss Net is not well-suited for solving complex max-min problems, despite its wide applications in many scenarios, such as [22], [37]–[39]. Notably, lower four curves in the plot are relatively close, indicating a fact that they are all acceptable schemes for solving P1. Among these schemes, AO scheme is the best as it consistently achieves the lowest maximum SOP. Both DL schemes, namely MSB-BFNet and MSB-Rayleigh schemes, are slightly worse than the AO scheme. The AO-Grad scheme demonstrates the worst performance when compared to the AO and MSB schemes[2]. This shortcoming of DL schemes primarily stems from the limited capacity of neural networks to learn from the extensive features introduced by IRS elements. In the future, we aim to optimize the neural network architecture design, boosting its ability to efficiently tackle the min-max SOP problem in IRS-assisted PLS. Additionally, we also note that MSB-Rayleigh performs slightly better than MSB-BFNet.

[2]The details of AO-Grad scheme based on the smoothing technique [40] and fast iterative shrinkage-thresholding algorithm (FISTA) [41] can be found in https://github.com/yiliangliu1990/liugit_pub/tree/master/fairness_irs.

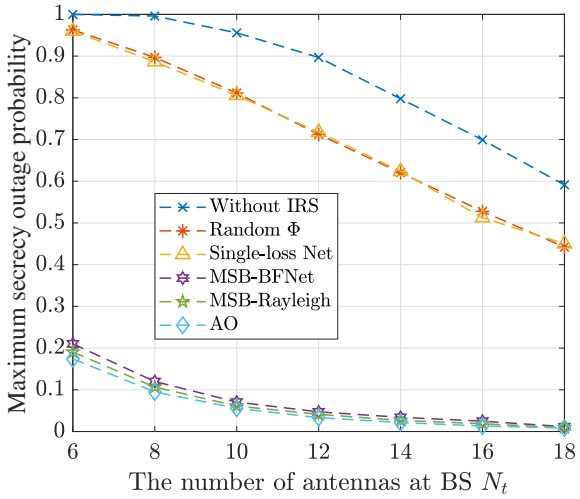


Fig. 6: Impact of N_t, where $N_e = 2$, $N_s = 64$, SNR = 1 dB, and $R_k = 2.5$ bit/s/Hz.

In Fig. 6, we present the impact of the number of BS antennas on the maximum SOP. As expected, an increase in the number of BS antennas leads to a significant improvement in security performance of all schemes. AO, MSB-Rayleigh, and MSB-BFNet schemes, when compared to without IRS and random $\mathbf{\Phi}$ schemes, achieve a substantial reduction in the maximum SOP. Notably, even with a large number of BS antennas, a considerable gap still exists between the without IRS scheme and the IRS-assisted ones, signifying that IRS can effectively enhance PLS performance. In terms of cost-effectiveness, the use of IRS approach may be more effective than increasing the number of BS antennas, as the former is generally cheaper.

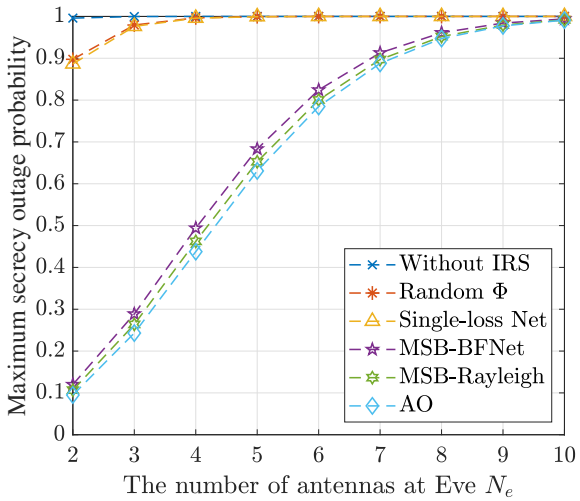


Fig. 7: Impact of N_e, where $N_t = 8$, $N_s = 64$, SNR = 1 dB, and $R_k = 2.5$ bit/s/Hz.

Fig. 7 depicts the impact of the number of eavesdropper antennas on the maximum SOP. It can be observed that as

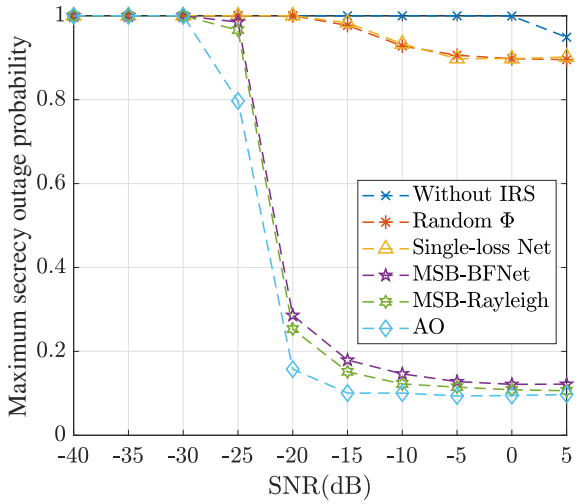


Fig. 8: Impact of SNR, where $N_t = 8, N_s = 64, N_e = 2$, and $R_k = 2.5$ bit/s/Hz.

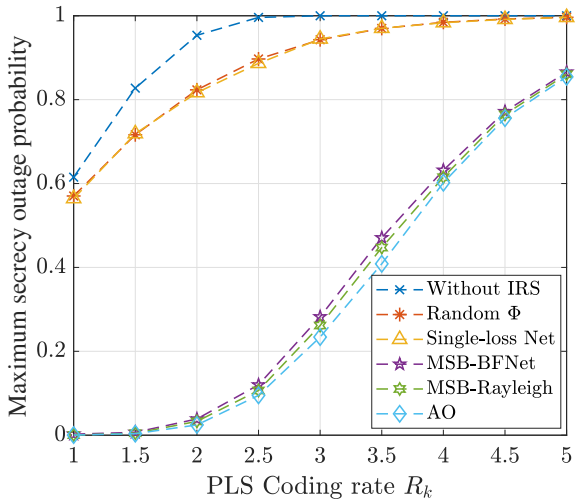


Fig. 9: Impact of R_k, where $N_t = 8, N_s = 64, N_e = 2$, and SNR = 1 dB.

the number of eavesdropper antennas increases, the maximum SOP also increases continuously. This is because an increased number of eavesdropper antennas results in higher gains for the eavesdroppers, ultimately diminishing system security. However, both the proposed AO algorithm and the MSB-based schemes demonstrate their effectiveness in mitigating the impact of increased N_e when compared to without IRS or random $\mathbf{\Phi}$ schemes. Notably, the performances of AO algorithm and MSB-based schemes are closely comparable, similar to what we can observe from Figs. 5 and 6.

Fig. 8 demonstrates the impact of SNR on the system performance. In a low SNR region, all schemes exhibit a high maximum SOP. As SNR increases, the maximum SOP of all schemes decreases. However, the proposed AO and MSB-based schemes significantly outperform without IRS and random $\mathbf{\Phi}$ schemes, with their performances being closely comparable. Simulations also demonstrate the instability and poor performance of Single-loss Net scheme, which is not

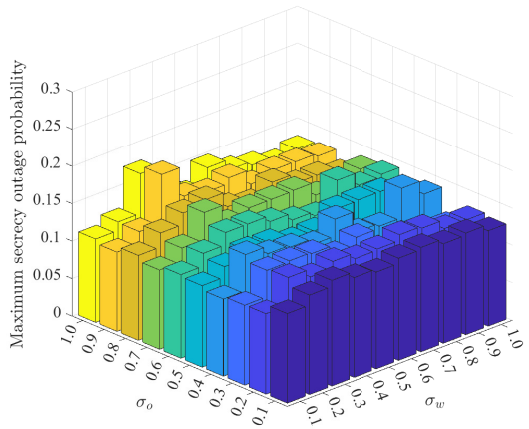


Fig. 10: Parameter sensitivity test, where $N_t = 8, N_s = 64, N_e = 2$, SNR = 1 dB, and $R_k = 2.5$ bit/s/Hz.

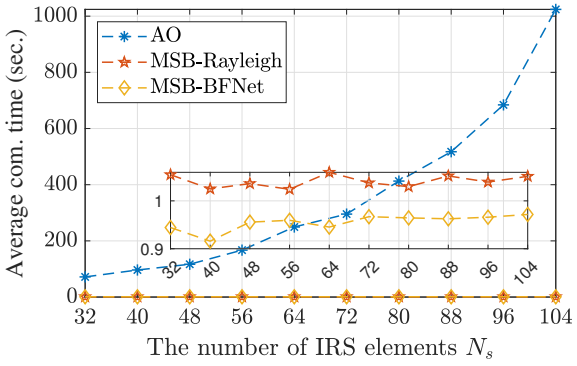


Fig. 11: Impact of N_s on computation time, where $N_t = 8$, $N_e = 2$, SNR = 1 dB, and $R_k = 2.5$ bit/s/Hz.

well-suited for solving complex max-min problems, despite its wide applications in many applications [37]–[39]. Fig. 9 illustrates the impact of PLS coding rate on the maximum SOP. As PLS coding rate increases, the maximum SOP of all schemes increases as well.

Fig. 10 provides the results on sensitivity analysis of the MSB framework with respect to scaled Tanh parameters σ_w and σ_o, which denote the output dynamics of WUB-Net and OPB-Net, respectively, i.e., $[-\sigma_w, \sigma_w]$ and $[-\sigma_o, \sigma_o]$. Here, both σ_w and σ_o are chosen from interval $[0.1, 0.2, \ldots, 1.0]$. As shown in Fig. 10, the proposed model exhibits its robustness to the values of σ_w and σ_o, and slightly degrades its performance only with $\sigma_w = 0.3$ and $\sigma_o = 0.9$.

The impact of N_s on computation time of running a total of 2,000 simulations is illustrated in Fig. 11, from which we can observe that the time taken by AO algorithm increases significantly with an increase in N_s. This is mainly due to the time-consuming nature of solving problem P10 by CXV in AO optimization process, which correlates positively with the number of IRS elements. Moreover, the MSB-based schemes demonstrate significantly lower time consumption compared to AO scheme. Finally, we note that while time consumption of MSB-Rayleigh is similar to that of MSB-

BFNet, the algorithm run time of AO scheme is approximately 100 ms when $N_s = 64$, whereas the deep learning algorithm completes its computations in about 0.5 ms, consistent to many existing investigations [22], [25]. In high-speed environments, channel coherence time is measured on millisecond scale. Consequently, for practical applications of this algorithm, more robust computing resources and more powerful chips will be essential.

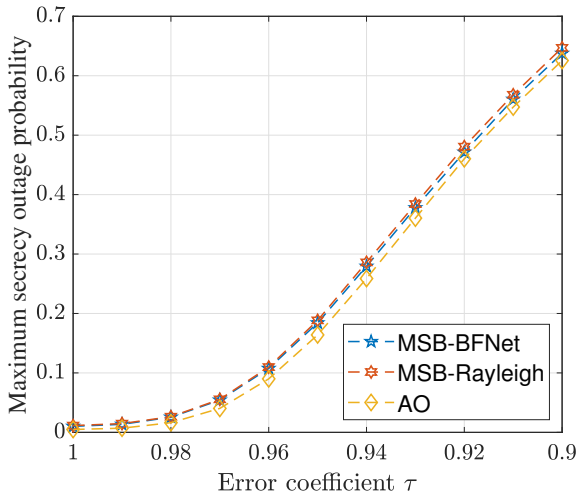


Fig. 12: Impact of channel estimation error, where $N_t = 8$, $N_e = 2$, $N_s = 64$, SNR = 1 dB, and $R_k = 2.5$ bit/s/Hz.

We examine the impact of inaccurate CSI in Fig. 12, where test dataset used inaccurate CSI data. The inaccurate CSI was generated by the following model [42].

$$\begin{aligned}\mathbf{h}_k &= \tau\bar{\mathbf{h}}_k + \sqrt{1-\tau^2}\mathbf{e}, \forall k,\\ \mathbf{f}_k &= \tau\bar{\mathbf{f}}_k + \sqrt{1-\tau^2}\mathbf{e}, \forall k,\\ \mathbf{G} &= \tau\bar{\mathbf{G}} + \sqrt{1-\tau^2}\mathbf{E}, \end{aligned} \tag{54}$$

where $\bar{\mathbf{h}}_k$, $\bar{\mathbf{f}}_k$, and $\bar{\mathbf{G}}$ denote estimated CSI, and $\mathbf{e}$ and $\mathbf{E}$ are random vector and matrix, in which their elements are independent identically distributed (i.i.d.) with $\mathcal{CN}(0,1)$. $\tau = J_0(2\pi f_D T_d)$ is a fading correlation coefficient, where $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind. $f_D = \frac{v}{c} f_c$ is the maximum Doppler spread, where $c = 3 \times 10^8$ m/s is the light speed and f_c is carrier frequency. As depicted in Fig. 12, channel estimation error affects security performance of all schemes, with a larger error leading to an increased SOP. In the future, we will design a robust scheme to reduce the impact of CSI estimation error.

Next, we perform a convergence test on the proposed AO algorithm. As shown in Fig. 13, we conducted convergence tests with different values of N_s. With an increasing number of iterations in AO algorithm, our optimization objective, i.e., the maximum SOP among multiple users, decreases rapidly before the 30th iteration and converges to a constant in the subsequent iterations. The curve shows a good performance of the proposed AO algorithm. The superiority of the proposed DL scheme over MSB framework is demonstrated in Figs. 14 and 15. It is evident that validation loss not only decreases rapidly but also converges swiftly after just a few epochs.

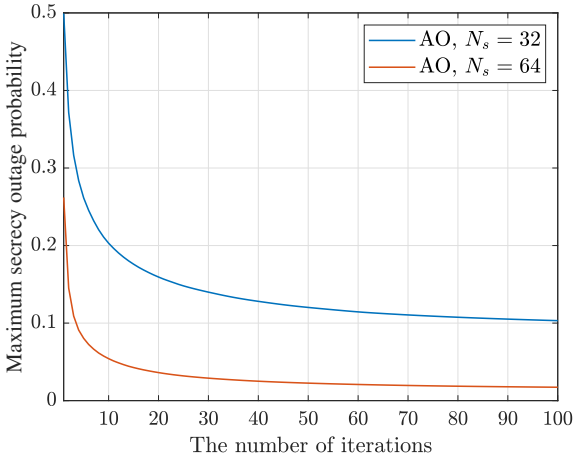


Fig. 13: Convergence test of AO scheme.

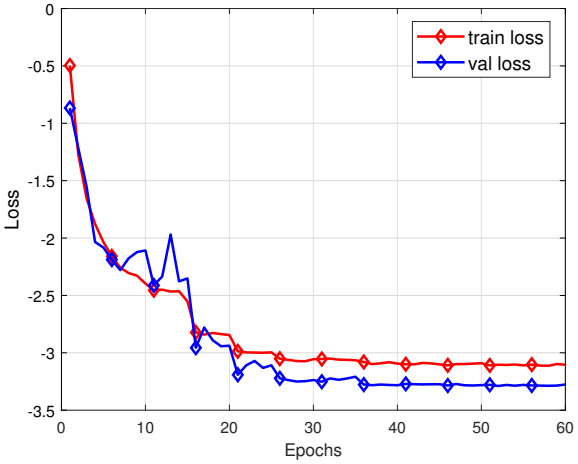


Fig. 14: First 60 epochs for training BF-Net.

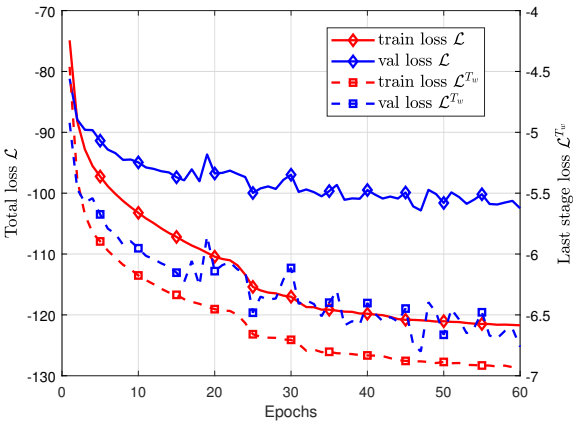


Fig. 15: First 60 epochs for training IRS-Net.

This efficiency is attributed to a high capacity of DL scheme in effectively managing the coupling effect among various antennas, reflecting elements, and users. Fig. 15 shows loss variation in multiple-stage learning, where the total loss on the left-hand side is obtained by summing the losses from multiple stages, and the loss on the right-hand side represents the loss from the final stage only.

VI. CONCLUSIONS

This paper addressed a challenging issue on achieving secure communications in multiple-user uplink channels with IRS-assisted PLS in the absence of instantaneous CSI of eavesdroppers. To this end, we proposed two schemes, i.e., AO scheme and DL scheme, both of which can minimize the maximum SOP independently among multiple users. In particular, the proposed DL scheme achieves a performance comparable to that of the AO scheme with a relatively low computational complexity. In our future works, we aim to do some more experiments to tailor design learning and graph neural networks to reduce the computation complexity with different changing parameters, such as the numbers of antennas, IRS elements, or users.

REFERENCES

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[2] T. Yang, R. Zhang, X. Cheng, and L. Yang, "Secure massive MIMO under imperfect CSI: Performance analysis and channel prediction," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 6, pp. 1610–1623, 2019.

[3] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, 2018.

[4] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40–46, 2015.

[5] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[6] 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. Surv. Tutorials*, vol. 22, no. 4, pp. 2283–2314, Fourthquarter 2020.

[7] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, 2020.

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

[9] 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.*, vol. 21, no. 9, pp. 7055–7071, 2022.

[10] B. Zheng, C. You, W. Mei, and R. Zhang, "A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 2, pp. 1035–1071, 2022.

[11] S. Xu, C. Chen, Y. Du, J. Wang, and J. Zhang, "Intelligent reflecting surface backscatter enabled uplink coordinated multi-cell MIMO network," *IEEE Trans. Wireless Commun.*, vol. 22, no. 8, pp. 5685–5696, 2023.

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

[13] S. Asaad, Y. Wu, A. Bereyhi, R. R. Müller, R. F. Schaefer, and H. V. Poor, "Secure active and passive beamforming in IRS-aided MIMO systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1300–1315, 2022.

[14] J. Li, L. Zhang, K. Xue, Y. Fang, and Q. Sun, "Secure transmission by leveraging multiple intelligent reflecting surfaces in MISO systems," *IEEE Trans. Mob. Comput.*, vol. 22, no. 4, pp. 2387–2401, 2022.

[15] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent reflecting surface aided multi-antenna secure transmission," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 108–112, 2020.

[16] H. Song, H. Wen, J. Tang, P.-H. Ho, and R. Zhao, "Secrecy energy efficiency maximization for distributed intelligent reflecting surfaces assisted MISO secure communications," *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4462–4474, 2022.

[17] A. Mukherjee, V. Kumar, and L.-N. Tran, "Secrecy rate maximization for intelligent reflecting surface assisted MIMOME wiretap channels," in *IEEE Military Communications Conference*, 2021, pp. 261–266.

[18] A. Mukherjee, V. Kumar, D. W. K. Ng, and L.-N. Tran, "On the energy-efficiency maximization for IRS-assisted MIMOME wiretap channels," in *IEEE Vehicular Technology Conference (VTC2022-Fall)*, 2022, pp. 1–6.

[19] B. Feng, Y. Wu, M. Zheng, X.-G. Xia, Y. Wang, and C. Xiao, "Large intelligent surface aided physical layer security transmission," *IEEE Trans. Signal Process.*, vol. 68, pp. 5276–5291, 2020.

[20] Y. Liu, Z. Su, C. Zhang, and H.-H. Chen, "Minimization of secrecy outage probability in reconfigurable intelligent surface-assisted MIMOME system," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 1374–1387, 2023.

[21] Y. Song, M. R. A. Khandaker, F. Tariq, K.-K. Wong, and A. Toding, "Truly intelligent reflecting surface-aided secure communication using deep learning," in *IEEE Vehicular Technology Conference (VTC2021-Spring)*, 2021, pp. 1–6.

[22] H. Song, M. Zhang, J. Gao, and C. Zhong, "Unsupervised learning-based joint active and passive beamforming design for reconfigurable intelligent surfaces aided wireless networks," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 892–896, 2021.

[23] K. Feng, Q. Wang, X. Li, and C.-K. Wen, "Deep reinforcement learning based intelligent reflecting surface optimization for MISO communication systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 745–749, 2020.

[24] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 375–388, 2021.

[25] C. Zhang, Y. Liu, and H.-H. Chen, "Deep learning based joint beamforming design in IRS-assisted secure communications," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16 861–16 865, 2023.

[26] X. Wei, D. Shen, and L. Dai, "Channel estimation for RIS assisted wireless communications—part I: Fundamentals, solutions, and future opportunities," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1398–1402, 2021.

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

[28] 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, 2021.

[29] P.-A. Absil, R. Mahony, and R. Sepulchre, *Optimization algorithms on matrix manifolds*. Princeton, New Jersey, US: Princeton University Press, 2009.

[30] 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.

[31] 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, 2019.

[32] J. C. Bezdek and R. J. Hathaway, "Convergence of alternating optimization," *Neural, Parallel & Scientific Computations*, vol. 11, no. 4, pp. 351–368, 2003.

[33] B. Feng, J. Gao, Y. Wu, W. Zhang, X.-G. Xia, and C. Xiao, "Optimization techniques in reconfigurable intelligent surface aided networks," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 87–93, 2021.

[34] V. Kumar, R. Zhang, M. D. Renzo, and L.-N. Tran, "A novel SCA-Based method for beamforming optimization in IRS/RIS-assisted MU-MISO downlink," *IEEE Wireless Communications Letters*, vol. 12, no. 2, pp. 297–301, 2023.

[35] V. Kumar, M. Chafii, A. L. Swindlehurst, L.-N. Tran, and M. F. Flanagan, "SCA-based beamforming optimization for IRS-enabled secure integrated sensing and communication," in *IEEE Global Communications Conference*, 2023, pp. 5992–5997.

[36] Z. Q. Luo, W. K. Ma, A. M. C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process Mag.*, vol. 27, no. 3, pp. 20–34, 2010.

[37] Y. Zhang, J. Zhang, S. Buzzi, H. Xiao, and B. Ai, "Unsupervised deep learning for power control of cell-free massive MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 9585–9590, 2023.

[38] N. Rajapaksha, K. B. Shashika Manosha, N. Rajatheva, and M. Latva-Aho, "Deep learning-based power control for cell-free massive MIMO networks," in *IEEE International Conference on Communications*, 2021, pp. 1–7.

[39] M. Farooq, H. Q. Ngo, and L. Nam Tran, "A low-complexity approach for max-min fairness in uplink cell-free massive MIMO," in *IEEE Vehicular Technology Conference (VTC2021-Spring)*, 2021, pp. 1–6.

[40] Y. Nesterov, "Smooth minimization of non-smooth functions," *Mathematical programming*, vol. 103, pp. 127–152, 2005.

[41] A. Beck and M. Teboulle, "A fast iterative shrinkage-thresholding algorithm for linear inverse problems," *SIAM journal on imaging sciences*, vol. 2, no. 1, pp. 183–202, 2009.

[42] X. Luo, Y. Liu, H.-H. Chen, and Q. Guo, "PHY security design for mobile crowd computing in ICV networks based on multi-agent reinforcement learning," *IEEE Trans. Wireless Commun.*, vol. 22, no. 10, pp. 6810–6825, 2023.