

# Heterogeneous Secure Transmissions in IRS-Assisted NOMA Communications: CO-GNN Approach

Linlin Liang, *Member, IEEE*, Zongkai Tian, Haiyan Huang, *Member, IEEE*, Xiaoyan Li, Zhisheng Yin, *Member, IEEE*, Dehua Zhang, Nina Zhang, Wenchao Zhai

**Abstract**—Intelligent Reflecting Surfaces (IRS) enhance spectral efficiency by adjusting reflection phase shifts, while Non-Orthogonal Multiple Access (NOMA) increases system capacity. Consequently, IRS-assisted NOMA communications have garnered significant research interest. However, the passive nature of the IRS, lacking authentication and security protocols, makes these systems vulnerable to external eavesdropping due to the openness of electromagnetic signal propagation and reflection. NOMA's inherent multi-user signal superposition also introduces internal eavesdropping risks during user pairing. This paper investigates secure transmissions in IRS-assisted NOMA systems with heterogeneous resource configuration in wireless networks to mitigate both external and internal eavesdropping. To maximize the sum secrecy rate of legitimate users, we propose a combinatorial optimization graph neural network (CO-GNN) approach to jointly optimize beamforming at the base station, power allocation of NOMA users, and phase shifts of IRS for dynamic heterogeneous resource allocation, thereby enabling the design of dual-link or multi-link secure transmissions in the presence of eavesdroppers on the same or heterogeneous links. The CO-GNN algorithm simplifies the complex mathematical problem-solving process, eliminates the need for channel estimation, and enhances scalability. Simulation results demonstrate that the proposed algorithm significantly enhances the secure transmission performance of the system.

**Index Terms**—Intelligent reflecting surface, non-orthogonal multiple access, secure transmission, graph neural networks.

## I. INTRODUCTION

THE escalating demand for high data capacity and low transmission latency in wireless communication has led

to significant proliferation in recent decades. To address the challenges posed by the frequent and substantial information exchange, non-orthogonal multiple access (NOMA) has garnered widespread attention in both academia and industry due to its superior spectrum efficiency, extensive connectivity, and enhanced user fairness. While NOMA shows promise in strengthening spectral efficiency and user fairness, its vulnerability to passive attacks such as eavesdropping due to the open nature of wireless communication poses a critical challenge in ensuring the security of NOMA transmissions.

Physical layer security (PLS) techniques are specifically designed to enhance the confidentiality and integrity of transmitted information by leveraging the physical attributes of wireless communication channels. In this regard, the intelligent reflecting surface (IRS) has garnered significant attention for its ability to improve the transmission performance and security of NOMA networks. The individual elements on the IRS can manipulate the phase of the incident signal independently, thereby enhancing the received signal from the base station to users and thwarting potential eavesdroppers from intercepting information. As a result of the advantages provided by IRS technology, IRS-enhanced wireless networks are being explored as a viable solution to enhance system transmission and security.

### A. Related Works

Existing studies have conducted in-depth exploration of performance analysis and resource configuration in IRS-assisted-NOMA systems. Sun *et al.* [1] first compared the performance differences between ideal IRS (with continuous phase shifts) and non-ideal IRS (with discrete phase shifts) in NOMA networks, deriving closed-form expressions for outage probability and revealing the critical impact of IRS phase precision on system capacity. Subsequently, researchers employed methods such as alternating optimization (AO) and penalty dual decomposition (PDD) [2]–[4] to jointly optimize BS beamforming and IRS reflection matrices to maximize the system sum rate. Furthermore, some studies utilized a two-stage approach to optimize NOMA power allocation, IRS phase shifts, and other parameters by transforming non-convex problems into convex ones for analysis [5], [6]. For example, Khan *et al.* [5] decoupled the original optimization problem into two subproblems: power allocation and passive beamforming, solved via the inner approximation method and

Linlin Liang, Zongkai Tian, Xiaoyan Li are with the School of Cyber Engineering and Zhisheng Yin is with the School of Telecommunications Engineering, Xidian University, Xi'an, 710071, China (email: liliang@xidian.edu.cn; zktian@stu.xidian.edu.cn; xiaoyanleece@stu.xidian.edu.cn; zsyin@xidian.edu.cn).

Haiyan Huang is with the School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou, 730070, China (email: huanghaiyan@mail.lzjtu.cn).

Wenchao Zhai is with the College of Information Engineering, China Jiliang University, Hangzhou, 310018, China (email: zhaiwenchao@cjl.edu.cn).

Nina Zhang is with the Comprehensive Information Support Center, Shaanxi General Staff of PAP, Xi'an, 710054, China (email: zhangnina0301@yeah.net).

Dehua Zhang is with the School of Artificial Intelligence, Henan University, Zhengzhou, 450046, China (email: dhuazhang@vip.henu.edu.cn).

Manuscript received September xx, 2024. This work was supported by the National Natural Science Foundation of China under Grants 62001359 and 62461032, National basic scientific research of China under Grants JCKY2023110C099, and by the Key Science and Technology Research Project of Henan Province under Grants 232102211059. (*Corresponding author:* Zhisheng Yin and Haiyan Huang.)

convex optimization, respectively. However, existing works predominantly focus on single objectives and fail to jointly optimize heterogeneous resources, relying on traditional convex optimization frameworks that struggle to meet real-time requirements in dynamic eavesdropping scenarios.

With advancements in deep learning technologies, neural networks have gradually been applied to parameter optimization in IRS-NOMA systems. Chandan *et al.* [7] constructed a deep neural network (DNN) to predict outage probability and ergodic rates under hardware impairments while considering residual hardware damage. Ridho *et al.* [8] designed a deep learning model to jointly optimize precoding matrices and IRS phase shifts, but their user pairing strategy remains confined to static scenarios. Gao *et al.* [9] employed long short-term memory, a K-means-based Gaussian mixture model, and deep Q-networks to maximize the sum rate of all users. In reinforcement learning, Chen *et al.* [10] proposed a multi-agent deep reinforcement learning framework to optimize IRS phases and downlink power through information interaction, aiming to maximize overall energy efficiency. Yu *et al.* [11], [12] introduced a Lyapunov-function-based mixed-integer deep deterministic policy gradient algorithm within a multi-agent reinforcement learning framework to enhance communication spectral efficiency. However, these studies do not explore dynamic resource allocation mechanisms tailored for secrecy rate maximization. Although some works combine traditional optimization algorithms, such as AO [13], to reduce complexity, their generalization capabilities remain limited by fixed system models, making them unsuitable for security requirements in heterogeneous links.

To address eavesdropping threats in IRS-NOMA systems, physical layer security techniques have become a research hotspot. Some studies counteract potential eavesdropping through coordinated jamming or artificial noise injection [14]–[17]. Wang *et al.* [14] proposed an IRS-assisted artificial noise scheme to suppress passive eavesdropping by jointly transmitting NOMA signals and jamming signals. Several researchers adopted secrecy outage probability (SOP) as a security metric to analyze system security [18], [19]. Lu *et al.* [20] optimized transmit power and IRS reflect beamforming with SOP as the objective. Additionally, Zhang *et al.* [21] decomposed active and passive beamforming problems using AO to maximize the secrecy rate of primary users but neglected the collaborative attack risks posed by internal and external eavesdroppers. Han *et al.* [22] considered scenarios with both internal and external eavesdroppers, jointly optimizing active and passive beamforming to maximize the secrecy rate while minimizing legitimate users' transmit power and increasing artificial noise power to disrupt eavesdroppers. Furthermore, Guo *et al.* [23] integrated unmanned aerial vehicles (UAVs) with IRS and adopted a double deep Q-network algorithm to learn online UAV trajectory design strategies for maximizing the system secrecy rate. Despite leveraging traditional optimization methods to enhance security performance, existing works heavily depend on precise channel state information (CSI) and suffer from high computational complexity, hindering their applicability in large-scale dynamic network environments.

## B. Motivation and Contributions

Due to the inherent openness of electromagnetic signal propagation and reflection, the passive nature of IRS makes it vulnerable to targeted eavesdropping attacks. Coupled with multi-user signal superposition in NOMA, systems are highly susceptible to both external and internal eavesdropping threats. Despite this, there is a conspicuous dearth of research that comprehensively addresses reliable and secure communication in IRS-assisted NOMA networks that are susceptible to both internal and external eavesdropping in the heterogeneous links, posing a complex challenge. Current literature predominantly focuses on optimizing beamforming at BS and phase shifts of IRS to enhance system transmission or security. However, a power allocation policy based on successive interference cancellation (SIC) holds the potential to significantly enhance both transmission efficiency and security, as evidenced in [9]. Nonetheless, the joint optimization of the heterogeneous resources, including the IRS phase shift matrix, base station beamforming, and user power allocation policy, remains an area of limited exploration. Additionally, while deep learning algorithms have demonstrated remarkable performance gains in deep feature extraction and parameter optimization, their application in enhancing the security performance of IRS-assisted NOMA networks remains an understudied area, indicating a crucial research gap.

Motivated by the aforementioned context, our objective is to obtain the sum secrecy rate in IRS-assisted NOMA networks. The differences between our work and other existing studies are presented in TABLE I. Our contributions are outlined as follows:

- We propose a heterogeneous secure IRS-assisted NOMA transmission system that addresses both internal eavesdroppers and external eavesdroppers of wireless networks. Our research focuses on planning wireless heterogeneous resource configurations amidst the coexistence of internal and external eavesdroppers.
- We propose the Combinatorial Optimization Graph Neural Networks (CO-GNN) algorithm to design a heterogeneous resource configuration approach. This scheme addresses the beamforming, power allocation, and phase shift problems in our model for security analysis. By directly mapping received signals to optimal parameters, CO-GNN eliminates the necessity for explicit mathematical representations and channel estimation, thereby bolstering resilience against attacks.
- Simulation results clearly demonstrate that our CO-GNN scheme consistently achieves the highest sum secrecy rate, thereby validating the effectiveness of our the heterogeneous resource configuration approach. Furthermore, as the transmit power increases, as well as the number of IRS reflecting elements or transmit antennas, the security of our model experiences a noteworthy enhancement. Notably, compared with conventional AO schemes, the CO-GNN achieves superior security performance while maintaining low computational complexity. These findings not only establish the superiority of our proposed method but also highlight its practicality and scalability

TABLE I: Comparisons of proposed and exiting works

CTX	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
$\mathcal{A}$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{B}$	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{C}$			✓	✓	✓	✓	✓	✓			✓				✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	
$\mathcal{D}$			✓	✓	✓		✓		✓			✓				✓	✓	✓	✓	✓	✓			✓	✓	✓	
$\mathcal{E}$					✓	✓	✓				✓	✓				✓										✓	✓
$\mathcal{F}$																	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
$\mathcal{G}$																			✓			✓		✓			
$\mathcal{H}$									✓	✓	✓	✓	✓	✓	✓	✓											✓
$\mathcal{I}$																				✓	✓		✓				

$\mathcal{A}$ : NOMA.  $\mathcal{B}$ : IRS-assisted.  $\mathcal{C}$ : Beamforming-optimized.  $\mathcal{D}$ : Phase-shifts-optimized.  $\mathcal{E}$ : power-allocator-optimized.  $\mathcal{F}$ : External Eve.  $\mathcal{G}$ : Internal Eve.  $\mathcal{H}$ : Neural Networks.  $\mathcal{I}$ : Secrecy rate.

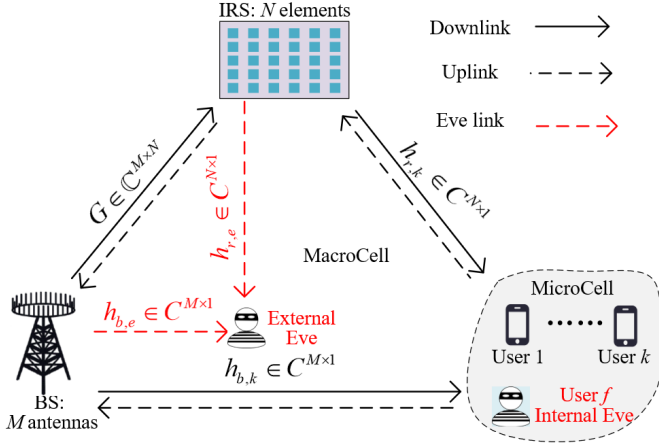


Fig. 1: System Model

in real-world scenarios.

### C. Paper Organization

The rest of the paper is given as follows. Section II proposes the system model, hardware impairments and problem formulation. Section III gives the designed CO-GNN network for joint optimization. Section IV presents the performance results and the analysis and Section V draws the conclusion.

## II. SYSTEM MODEL AND PROBLEM FORMULATION

### A. System Model

In this paper, we investigate an IRS-assisted NOMA communication system depicted in Fig. 1, encompassing downlink, uplink, and eavesdropping links. The uplink and downlink denote signal transmission directions in an IRS-assisted NOMA system: downlink from the base station (BS) or via the IRS to users, and uplink vice versa. Operating under a time division duplex (TDD) system, both the BS and IRS can acquire channel state information (CSI) from users for the downlink. We specifically consider two types of eavesdroppers: external eavesdroppers, unauthorized and not part of NOMA pairing, and internal eavesdroppers within the NOMA pairing, attempting to intercept NOMA signals.

The BS is equipped with  $M$  transmit antennas and communicates with  $K$  single-antenna users, where  $M \geq K$ . Eavesdroppers also deploy single antennas. The reflecting IRS is

equipped with  $N$  low-cost passive reflecting elements capable of digitally controlling phase and amplitude to alter signal propagation directions and effects. Channel gain from the BS to the IRS,  $k$ -th users, and Eves, and from the IRS to the  $k$ -th users and Eves are denoted as  $\mathbf{G} \in \mathbb{C}^{M \times N}$ ,  $\mathbf{h}_{b,k} \in \mathbb{C}^{M \times 1}$ ,  $\mathbf{h}_{b,e} \in \mathbb{C}^{M \times 1}$ ,  $\mathbf{h}_{r,k} \in \mathbb{C}^{N \times 1}$ ,  $\mathbf{h}_{r,e} \in \mathbb{C}^{N \times 1}$ , and  $\mathbf{h}_{f,e} \in \mathbb{C}^{N \times 1}$ , respectively. All channel coefficients experience small-scale fading and path loss, modeled by Rayleigh fading. The CSI of users is obtainable at both the BS and IRS but not at eavesdroppers, who remain silent. The downlink channels from the BS to the user  $k$  can be expressed as

$$\mathbf{h}_{b,k} = \beta_{0,k} \tilde{\mathbf{h}}_{b,k}, \quad (1)$$

where  $\tilde{\mathbf{h}}_{b,k} \sim \mathcal{CN}(0, 1)$ , and  $\beta_{0,k}$  denotes the path loss of the downlink.

The IRS is strategically placed to maintain a downlink line-of-sight (LOS) communication pathway with the BS and the users. Therefore, the channels, represented by  $\mathbf{G}$  and  $\mathbf{h}_{r,k}$ , are characterized using the Rician fading model, expressed as:

$$\mathbf{G} = \beta_1 \left( \sqrt{\frac{\kappa}{1+\kappa}} \tilde{\mathbf{G}}^{LOS} + \sqrt{\frac{\kappa}{1+\kappa}} \tilde{\mathbf{G}}^{NLOS} \right), \quad (2)$$

$$\mathbf{h}_{r,k} = \beta_{2,k} \left( \sqrt{\frac{\kappa}{1+\kappa}} \tilde{\mathbf{h}}_{r,k}^{LOS} + \sqrt{\frac{\kappa}{1+\kappa}} \tilde{\mathbf{h}}_{r,k}^{NLOS} \right), \quad (3)$$

where  $\kappa$  signifies the Rician K-factor. The superscripts 'LOS' and 'NLOS' refer to the line-of-sight and non-line-of-sight components, respectively. The terms  $\beta_1$  and  $\beta_{2,k}$  denote the path loss from the BS to the IRS, and from the IRS to the  $k$ -th user, respectively. The elements within the matrices  $\tilde{\mathbf{G}}^{NLOS}$  and  $\tilde{\mathbf{h}}_{r,k}^{NLOS}$  are modeled as independent and identically distributed (i.i.d.) complex Gaussian random variables with zero mean and unit variance, i.e.,  $[\tilde{\mathbf{G}}^{NLOS}]_{ij} \sim \mathcal{CN}(0, 1)$  and  $[\tilde{\mathbf{h}}_{r,k}^{NLOS}]_i \sim \mathcal{CN}(0, 1)$ .

The LoS component of the channel  $\mathbf{h}_{r,k}$  depends on the positions of the IRS and users. Let  $\phi_{2,k}$  and  $\theta_{2,k}$  represent the azimuth and elevation angles of arrival (AoA) from user  $k$  to the IRS. The LoS channel is given by  $\tilde{h}_{r,k}^{LOS} = \alpha_{IRS}(\phi_{2,k}, \theta_{2,k})$ , where the  $n$ -th element of the IRS steering vector  $\alpha_{IRS}(\phi_{2,k}, \theta_{2,k})$  is defined as [24].

$$[\alpha_{IRS}(\phi_{2,k}, \theta_{2,k})]_n = e^{j \frac{2\pi d_{IRS}}{\lambda c} \{i_1(n) \sin(\phi_{2,k}) \cos(\theta_{2,k}) + i_2(n) \sin(\theta_{2,k})\}} \quad (4)$$

where  $d^{IRS}$  represents the distance between two adjacent elements of the IRS, and  $\lambda_c$  denotes the carrier wavelength. The functions  $i_1(n) = \text{mod}(n-1, 10)$  and  $i_2(n) = \lfloor \frac{n-1}{10} \rfloor$  are defined to facilitate specific calculations. For simplicity, we set  $\frac{2d^{IRS}}{\lambda_c} = 1$ .

Let  $(s_k, y_k, z_k)$  denotes the location of the user  $k$  and  $(x^{IRS}, y^{IRS}, z^{IRS})$  represents the location of the IRS, then

$$\sin(\phi_{2,k}) \cos(\theta_{2,k}) = \frac{y_k - y^{IRS}}{d_k^{IU}}, \quad (5)$$

$$\sin(\theta_{2,k}) = \frac{z_k - z^{IRS}}{d_k^{IU}}, \quad (6)$$

where  $d_k^{IU}$  is the distance between IRS and  $k$ -th user.

Similarly, let  $\phi_0$  and  $\theta_0$  denote the azimuth and elevation angles of arrival at the BS. The BS steering vector can then be formulated as

$$\alpha_{BS}(\phi_0, \theta_0) = \left[ 1, \dots, e^{j \frac{2\pi(M-1)d^{BS}}{\lambda_c} \cos(\phi_0) \cos(\theta_0)} \right], \quad (7)$$

where  $d^{BS}$  is the distance between two adjacent BS antennas, and we assume  $\frac{2\pi d^{BS}}{\lambda_c} = 1$ . Let  $\phi_1, \theta_1$  denote the azimuth and elevation angles of departure(AoD) from the IRS to the BS, then we can obtain

$$\tilde{\mathbf{G}}^{LOS} = \alpha_{BS}(\phi_0, \theta_0) \alpha_{IRS}(\phi_1, \theta_1)^H. \quad (8)$$

From (5) and (6), we can get

$$\cos(\phi_0) \cos(\theta_0) = \frac{x^{IRS} - x^{BS}}{d^{BI}}, \quad (9)$$

$$\sin(\phi_1) \cos(\theta_1) = \frac{y^{BS} - y^{IRS}}{d^{BI}}, \quad (10)$$

$$\sin(\theta_1) = \frac{z^{BS} - z^{IRS}}{d^{BI}}, \quad (11)$$

where  $d^{BI}$  is the distance between the IRS and the BS.

Let  $s_k \in \mathbb{C}$  be the signal intended for transmission from BS to  $k$ -th user. The BS employs a beamforming strategy, utilizing a beamforming vector  $\mathbf{w}_k \in \mathbb{C}^M$ , and encodes the signals for all users simultaneously with the power allocation factor  $\mathbf{a}_k$ . Both the beamforming and power allocation factor must satisfy some constraints:  $\sum_{k=1}^K \|\mathbf{w}_k\|^2 \leq P_t$  and  $\sum_{k=1}^K \mathbf{a}_k = 1$ , where  $P_t$  is the transmission power at BS. The reflection matrix of IRS is denoted as  $\Phi = \text{diag}\{e^{j\theta_1}, \dots, e^{j\theta_n}, \dots, e^{j\theta_N}\}$ , where  $\theta_n$  is the phase shifts at  $n$ -th reconfiguration element. So the received signal at  $k$ -th user is denoted as

$$\mathbf{y}_k = \sum_{i=1}^K (\mathbf{h}_{b,k} + \mathbf{G}\Phi\mathbf{h}_{r,k})^T \mathbf{w}_k \sqrt{P_t \mathbf{a}_k} s_k + n_k, \quad (12)$$

where the  $n_k$  denotes the additive white gaussian noise (AWGN) at user  $k$  with mean power parameter  $\sigma^2$ .

In NOMA systems, users employ the SIC technique for signal decoding. The demodulation order in SIC is established based on the combined channel's equivalent channel gain. We adhere to the principle that the user with the strongest channel

gain is demodulated first, while the users with weaker channel gains receive information directly. The users are ordered as  $\|\mathbf{h}_1\|^2 \geq \|\mathbf{h}_2\|^2 \geq \dots \geq \|\mathbf{h}_K\|^2$ , where the  $k$ -th ordered users corresponds to the  $k$ -th Strongest channels. For the  $k$ -th strongest user, it decodes its signal by treating other weaker users' signals as interference. The signal-to-interference-plus-noise ratio (SINR) for the strongest  $k$ -th user decoding its signal can be expressed as

$$\gamma_k = \frac{\mathbf{a}_k P_t |(\mathbf{h}_{b,k} + \mathbf{G}\Phi\mathbf{h}_{r,k})^T \mathbf{w}_k|^2}{\sum_{i=k+1}^K \mathbf{a}_i P_t |(\mathbf{h}_{b,k} + \mathbf{G}\Phi\mathbf{h}_{r,k})^T \mathbf{w}_i|^2 + \sigma_k^2}. \quad (13)$$

Consequently, the transmission rate for  $k$ -th user can be denoted as

$$R_k = \log_2(1 + \gamma_k). \quad (14)$$

Considering the detrimental effects of the intricate electromagnetic environment on secure communication via exposed radio signals, we examine both external and internal wiretapping scenarios in the heterogeneous links to assess the secrecy performance of IRS-NOMA networks.

An external eavesdropper is unauthorized and not part of the NOMA pairing. The broadcast nature of wireless networks increases the likelihood of unauthorized eavesdroppers intercepting NOMA signals.

1) External Eve: the external Eve is unauthorized and not part of the NOMA pairing. The broadcast nature of wireless networks increases the likelihood of unauthorized eavesdroppers intercepting NOMA signals. To this end, the received signal at Eve can be derived as

$$\mathbf{y}_{EE} = \sum_{i=1}^K (\mathbf{h}_{b,e} + \mathbf{G}\Phi\mathbf{h}_{r,e})^T \mathbf{w}_i \sqrt{P_t \mathbf{a}_i} s_i + n_e, \quad (15)$$

where the  $n_e$  denotes the AWGN at Eve. Referring to the analysis above, the external Eve can decode the information of user  $k$  by applying SIC. So the SINR for  $E$  to wiretap the signal from user  $k$  can be established as

$$\gamma_{e \rightarrow k} = \frac{\mathbf{a}_k P_t |(\mathbf{h}_{b,e} + \mathbf{G}\Phi\mathbf{h}_{r,e})^T \mathbf{w}_k|^2}{\sum_{i=k+1}^K \mathbf{a}_i P_t |(\mathbf{h}_{b,e} + \mathbf{G}\Phi\mathbf{h}_{r,e})^T \mathbf{w}_i|^2 + \sigma_k^2}. \quad (16)$$

Then the transmission rate for external eve can be obtained like (14).

2) Internal Eve: In this scenario, although the distant user  $f$  is a legitimate user, its weaker channel condition urges it to inadvertently overhear transmissions intended for other legitimate users, thus functioning as an internal eavesdropper. Consequently, the signal received at internal Eve  $f$  can be expressed as

$$\mathbf{y}_{IE} = \sum_{i=1}^{K-1} (\mathbf{h}_{b,f} + \mathbf{G}\Phi\mathbf{h}_{r,f})^T \mathbf{w}_i \sqrt{P_t \mathbf{a}_i} s_i + n_f. \quad (17)$$

At this moment, the SINR  $\gamma_{f \rightarrow k, k \neq f}$  for internal eavesdropper  $f$  can be derived like (16) and the transmission rate for  $f$  also can be obtained like (14).

According to the definition of the secrecy rate, for each user, the secrecy rate  $R_k^{\text{sec}}$  can be expressed as

$$R_k^{\text{sec}} = [R_k - R_{\varphi \rightarrow k}]^+ \quad \varphi = e, f. \quad (18)$$

### B. Problem Formulation

Our objective is to jointly optimize the robust BS's beamforming  $\mathbf{w}$  and power allocation matrix  $\mathbf{a}$  based on NOMA protocol and the robust IRS's phase shift matrix  $\Phi$  to maximize the sum secrecy rate. By mapping the received signals directly to the optimized beamforming, power allocation and phase shifts for utility maximization, we can bypass the channel estimation getting the optimized transmission strategy more efficiently.

As a consequence, we can get the optimal beamforming  $\mathbf{w}$ , power allocation  $\mathbf{a}$  and phase shifts  $\Phi$  based directly on the received signals  $\mathbf{Y}$  by a function  $g(\cdot)$ .

$$\begin{aligned} \underset{(\mathbf{w}, \mathbf{a}, \Phi) = g(\mathbf{Y})}{\text{maximize}} \quad & \sum_{k=1}^K R_k^{\text{sec}}(\mathbf{w}, \mathbf{a}, \Phi) \\ & \sum_{k=1}^K \|\mathbf{w}_k\|^2 \leq P_t \\ & \sum_{k=1}^K \mathbf{a}_k = 1 \\ \text{s.t.} \quad & |e^{j\theta_n}| = 1, 0 \leq \theta_n \leq 2\pi \quad \forall n \\ & \|\mathbf{h}_{b1} + \mathbf{h}_{br}\Phi\mathbf{h}_{r1}\|^2 \geq \|\mathbf{h}_{b2} + \mathbf{h}_{br}\Phi\mathbf{h}_{r2}\|^2 \\ & \geq \dots \geq \|\mathbf{h}_{bK} + \mathbf{h}_{br}\Phi\mathbf{h}_{rK}\|^2 \\ & R_{\text{sec}} \geq R_{\min} \end{aligned} \quad (19)$$

The constraint  $R_{\text{sec}} \geq R_{\min}$  guarantees that all legitimate users achieve a secure transmission rate no less than the predefined threshold  $R_{\min}$ . This design effectively prevents users with poor channel conditions from being sacrificed due to unbalanced resource allocation, thereby significantly enhancing the system's service fairness. Specifically, when the equivalent channel gain of a user is detected to be low, the CO-GNN algorithm dynamically adjusts its beamforming vector  $\mathbf{w}_k$  and power allocation factor  $\mathbf{a}_k$  to prioritize compensating its secrecy rate until the  $R_{\min}$  requirement is satisfied.

Due to the non-convex nature of the objective function in the problem (19), solving it computationally presents a significant challenge. To address this issue effectively and circumvent the need for channel estimation, we have developed a deep neural network to visualize the mapping function  $g(\cdot)$  and to train the heterogeneous network parameters using the received signals to achieve best sum secrecy rate.

## III. PROPOSED DEEP LEARNING FRAMEWORK

Solving the optimization problem delineated in (19) poses significant challenges due to its non-convex nature. Traditional optimization methods often encounter computational hurdles, particularly in scenarios requiring channel estimation. Consequently, applying these conventional techniques to devise an efficient secure joint optimization policy in dynamically

changing environments is generally impractical. In response to this optimization challenge posed by (19), we introduce a neural network, CO-GNN, to model the mapping function  $g(\cdot)$ . By employing the proposed CO-GNN, we achieve joint optimization and get the beamforming, power allocation, and phase shifts straightly from the received signals, ultimately maximizing the secrecy network utility. By leveraging the opposite number of the objective function as the loss function for our network, we are able to achieve the joint optimization through the suppression of malicious eavesdroppers, as dictated by the objective function, thereby ensuring that the signal is transmitted in a direction that favors legitimate users while simultaneously mitigating eavesdropping attempts. The comprehensive framework of this approach is depicted in Fig. 2. In the following, we elaborate on the graphical representation, our CO-GNN, and the training procedure.

### A. Graphical Presentation of Users and IRS

To precisely characterize the interplay between nodes and IRS and minimize mutual interference among users, we employ graphs to represent users and IRS, thereby capturing the underlying relationships and mitigating negative interference. To achieve this, we devise a combinatorial optimization graph neural network to jointly optimize beamforming  $\mathbf{w}$ , power allocation factors  $\mathbf{a}$  at BS and the phase shifts  $\Phi$  at the IRS, aiming for superior system performance. Our CO-GNN is apt for communication networks due to its robust learning capacity in capturing interactions between users and IRS and extracting spatial information embedded in the network topology. Moreover, our CO-GNN maintains permutation invariance and permutation equivariance properties for graphs. Specifically, regardless of permutations or shuffles in the input index labels, the GNN network can still generate the correspondingly changing or unchanging output. Here, permutation invariance ensures that phase shifts are agnostic to the ordering of user channels, while permutation equivariance implies that if user channels are rearranged, the beamforming and power allocation vectors will be similarly permuted. The parameters of the GNN can be shared among users, facilitating its generalization to scenarios with varying user counts. Furthermore, the GNN architecture reduces model complexity compared to fully connected neural networks.

We employ a graph to model the interactions between the IRS and user nodes. The IRS is represented by node 0, while the  $K$  users are represented by nodes 1 through  $K$ . Meanwhile, the information of Node  $k$  is associated with a representation vector, denoted as  $\mathbf{r}_k$ , where  $k = 0, 1, \dots, K$ . Within our CO-GNN, the vectors are fed and updated layer by layer, with each update considering the vectors from the previous layer as input. After multiple layers of processing, the vector of each node will contain sufficient information to facilitate the design of beamforming  $\mathbf{w}$ , power allocator  $\mathbf{a}$ , and phase shifts  $\Phi$ . Specifically, the update of each user node's vector is a function of all its neighboring user nodes' vectors as well as the IRS node's vector. This design enables our CO-GNN to learn how to mitigate interference by capturing the relationships between neighboring nodes and the IRS as well as getting the joint

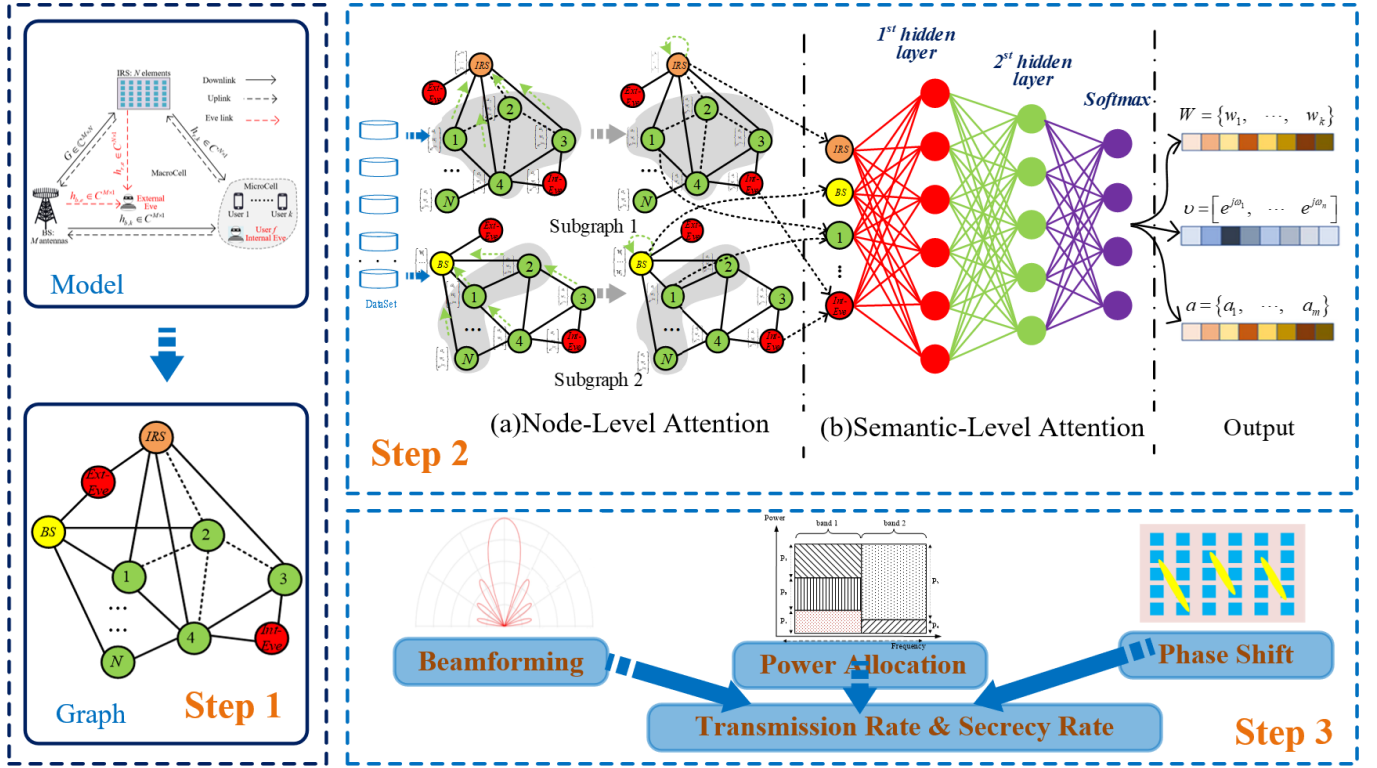


Fig. 2: Proposed Deep Learning Framework: CO-GNN

optimization results for improved secrecy performance. The update of the IRS node is a function of all the user nodes, which enables our CO-GNN to learn to configure the phase shifts on all the channels.

### B. Combinatorial Optimization Graph Neural Networks

We employ CO-GNN to train and jointly optimize the heterogeneous resource configurations, including the beamforming vector  $\mathbf{w}$ , the power allocation vector  $\mathbf{a}$ , and the phase shifts  $\Phi$ . Our CO-GNN specifically focuses on learning the graph representation vector  $r_k$  through a multi-layer architecture consisting of an input layer, two message passing layers, and an output layer. The network ingests the received signals from the user node of the graph, which serve as initial input values for joint optimization. These inputs are then propagated through two message passing layers, which contain the effective aggregation and combination functions, resulting in jointly optimized representations. Finally, an output layer straightly transforms and maps the representations into the optimized beamforming vector  $\mathbf{w}$ , power allocation vector  $\mathbf{a}$ , and phase shifts  $\Phi$  via a fully connected layer. The overall architecture of our CO-GNN is depicted in Fig. 2.

1) **Input Layer:** The input layer receives the feature vectors from the received signals for each user in the graph, denoted as  $\mathbf{Y}_k$  for  $k = 1, \dots, K$ . This is attributed to the fact that the received signal encapsulates ample information pertaining to beamforming, power allocation, and phase shifts, rendering it a valuable input for achieving enhanced outcomes through joint optimization of our CO-GNN. Given that the signal comprises

both real and imaginary components, for the user nodes, we can derive the updated result  $r_k^1$  as follows:

$$r_k^1 = f_{MLP}^1 \left( [(\mathbf{Y}_k).real]^T, [(\mathbf{Y}_k).imag]^T \right), \quad (20)$$

where  $f_{MLP}^1(\cdot)$  denotes a multilayer perceptron (MLP) that comprises two fully connected hidden layers.

For the IRS node, since all signals are reflected via the IRS, it is crucial to ensure that the received signals all contain an equivalent amount of information pertaining to the IRS. Consequently, the  $r_0^1$  can be derived as the mean of all the signals received from the user nodes:

$$r_0^1 = f_{MLP}^1 \left( \frac{1}{K} \sum_{k=1}^K [(\mathbf{Y}_k).real]^T, [(\mathbf{Y}_k).imag]^T \right). \quad (21)$$

2) **Message Passing Layers:** The message passing layers are the pivotal layers in our CO-GNN for joint optimization. These layers leverage neighbor aggregation and combination strategies to extract information from nodes, enabling the generation of a representation vector encompassing beamforming, power allocator and phase shifts for joint optimization. The representation vector are derived by aggregating the characteristics of neighboring nodes and subsequently combining them, effectively amounting to a message passing process [25]. In our implementation of the message passing layer, the aggregation function serves to compile the features of neighboring nodes into a message vector, which can then be relayed to the central node. Conversely, the combination function updates the node's representation at the current instant, integrating

both the current representation of the node and the messages garnered from the aggregation function. A crucial aspect in the design of GNNs lies in the selection of a suitable aggregation function  $f_{\text{aggregate}}(\cdot)$  and a combination function  $f_{\text{combine}}(\cdot)$  that enable the GNN to scale effectively and jointly optimize well. As for user nodes, we choose the aggregation function as

$$f_{\text{aggregate}}^i\left(\{r_j^{i-1}\}_{j \in N(k)}\right) = \Theta\left(\{f_{nn}^i(r_j^{i-1})\}_{j \in N(k)}\right), \quad (22)$$

where  $i$  is  $i$ -th aggregate layer,  $i = 1, \dots, I$ ,  $N(k)$  denotes the set of neighboring nodes of the node  $k$ ,  $\Theta$  is the mean-pooling function, and  $f_{nn}^i$  is a fully connected hidden layer. This aggregation function serves the purpose of gathering information from neighboring nodes and consolidating it for transmission to the central node. Mean-pooling ensures that interference features from all users are equally considered, thereby preventing resource allocation skewness. Its low-variance property not only enhances the model's robustness in dynamic channel conditions but also provides a smooth optimization trajectory for secrecy rate maximization.

As for the user combination function, it integrates the current node representation and the aggregated neighbor messages, as discussed in [25], and is realized through the use of a MLP:

$$f_{\text{combine}}^i(\{r_k^{i-1}\}) = f_{MLP}^i\left(r_k^{i-1}, f_{\text{aggregate}}^i\left(\{r_j^{i-1}\}_{j \in N(k)}\right)\right). \quad (23)$$

With the role of aggregation and combination, the message passing layer for the user can be obtained as

$$r_k^i = f_{MLP}^i\left(f_{MLP}^i(r_0^{i-1}), f_{\text{combine}}^i(\{r_k^{i-1}\})\right), \quad (24)$$

where the IRS node representation vector  $r_0^i$  can be present as

$$r_0^i = f_{MLP}^i\left(\begin{matrix} f_{MLP}^i(r_0^{i-1}), \\ \Delta(f_{MLP}^i(r_1^{i-1}), \dots, f_{MLP}^i(r_K^{i-1})) \end{matrix}\right), \quad (25)$$

where  $\Delta$  represents the max-pooling function, known for its empirical performance and its correspondence to the prevailing notion that multiuser interference is predominantly influenced by the strongest user. Max-pooling pinpoints the user most susceptible to the eavesdropping link and amplifies its feature representation. This compels the IRS phase shifts to prioritize suppressing signal leakage from this user, thereby optimizing the system's secrecy rate.

3) Output layer: After the completion of  $I$  message passing layers, we can generate the joint optimized phase shifts  $\Phi \in \mathbb{C}^N$ , the beamforming  $\mathbf{w} \in \mathbb{C}^{M \times K}$ , and the power allocation factors  $\mathbf{a} \in \mathbb{R}^K$  via the final output layer. Specifically, through the fully connected layer of corresponding size, the power allocation and beamforming are derived from the representation vectors of the user nodes, while the phase shifts are derived from the representation vectors of the IRS nodes.

When dealing with the phase shifts, as we initially separated the real and imaginary parts at the input layer, it is necessary

at this stage to combine them to obtain the phase shifts in complex form.

$$r_\Phi = [f_{nn}^{\text{out}}(r_0^I)(1:N), f_{nn}^{\text{out}}(r_0^I)(N+1:2N)] \in \mathbb{R}^{N \times 2}, \quad (26)$$

$$\Phi_n = \frac{[r_\Phi]_{n,1}}{\sqrt{[r_\Phi]_{n,1}^2 + [r_\Phi]_{n,2}^2}} + j \frac{[r_\Phi]_{n,2}}{\sqrt{[r_\Phi]_{n,1}^2 + [r_\Phi]_{n,2}^2}}. \quad (27)$$

For the beamforming and power allocator, the representation vectors of user nodes are needed to through the fully connected layer.

$$r_w = [f_{nn}^{\text{out}}(r_1^I), \dots, f_{nn}^{\text{out}}(r_K^I)] \in \mathbb{R}^{2M \times K}, \quad (28)$$

$$\mathbf{w} = \frac{r_w}{\|r_w\|}(1:M,:) + j \frac{r_w}{\|r_w\|}(M+1:2M,:). \quad (29)$$

Similarly, we can also get the power allocation vector  $\mathbf{a}$  like (28) which satisfies  $\mathbf{a}_k^{\text{out}} \in [0, 1]$  and  $\sum_1^K \mathbf{a}_k^{\text{out}} = 1$ .

### C. The Training

The loss function of CO-GNN is defined as the negative value of the sum secrecy rate:

$$\mathcal{L} = - \sum_{k=1}^K R_k^{\text{sec}}(\mathbf{w}, \mathbf{a}, \Phi) \quad (30)$$

The optimization process can be formulated as a minimization problem for this non-convex function. Despite the overall non-convexity of the loss function, convergence guarantees are achieved through the following design principles:

First, local convergence of gradient descent. Assuming the learning rate  $\eta$  satisfies the Lipschitz continuity condition, i.e., there exists a constant  $L > 0$  such that:

$$\|\nabla \mathcal{L}(\Theta^{(t+1)}) - \nabla \mathcal{L}(\Theta^{(t)})\| \leq L \|\Theta^{(t+1)} - \Theta^{(t)}\| \quad (31)$$

where  $\Theta$  denotes the model parameters, and the adaptive learning rate adjustment via the Adam optimizer ensures monotonic decrease of the loss function during iterations and convergence to a local minimum.

Second, smoothness of the loss function. Since the message-passing layers in CO-GNN employ continuously differentiable MLPs and pooling operations, the gradient of loss  $\mathcal{L}$  with respect to model parameters  $\Theta$  always exists and is computable, satisfying:

$$\nabla \Theta \mathcal{L} = - \sum_{k=1}^K \nabla \Theta R_k^{\text{sec}}, \quad (32)$$

This guarantees the validity of gradient descent updates.

The proposed training algorithm for CO-GNN is outlined in Algorithm 1. In each training iteration, the loss is iteratively fed back to the network, guiding the optimization of beamforming, power allocation, and phase shifts in a manner that maximizes the transmission rate for legitimate users while minimizing the eavesdropping rate. As the loss value



gradually diminishes, the system's sum secrecy rate performance increase concurrently, culminating in the achievement of jointly optimized parameters and the optimal sum secrecy rate. Moreover, the scenarios involving external and internal eavesdroppers are designated as  $E_{EX}$  and  $E_{IN}$ , respectively.

---

**Algorithm 1** CO-GNN Joint Optimization Training Algorithm

---

**Input:** Graph  $\mathbb{G}$ , input signals  $\mathbf{Y}$ , channel group  $\mathbf{H}$ , designed aggregation functions  $AGGREGATE_i$ , designed combination functions  $COMBINE_i$ , input layer  $MLP_{IN}$ , output layer  $MLP_{OUT}$

**Output:** Optimized  $\mathbf{w}$ ,  $\mathbf{a}$ ,  $\Phi$

Initialize

- 1:  $\mathbf{H}_R, \mathbf{H}_I \leftarrow \text{Channel2real}(\mathbf{H})$
- 2: **repeat**
- 3:   **for** each episode **do**
- 4:      $\mathbf{Y}_{ini} = \mathbf{0}$
- 5:     **for**  $k \in K$  **do**
- 6:        $r_U \leftarrow MLP_{IN}(\mathbf{Y}[k])$
- 7:        $\mathbf{Y}_{ini} = \mathbf{Y}_{ini} + \mathbf{Y}[k]$
- 8:     **end for**
- 9:      $Input_{\Phi} \leftarrow \text{Mean}(\mathbf{Y}_{ini})$
- 10:      $r_{\Phi} \leftarrow MLP_{IN}(Input_{\Phi})$
- 11:     **for**  $i \in I$  **do**
- 12:        $r_U, r_{\Phi} \leftarrow AGGREGATE_i(r_U, r_{\Phi})$
- 13:        $r_U, r_{\Phi} \leftarrow COMBINE_i(r_U, r_{\Phi})$
- 14:     **end for**
- 15:      $\mathbf{w}, \mathbf{a}, \Phi \leftarrow MLP_{OUT}(r_U, r_{\Phi})$
- 16:      $E_{IN}$ : Calculate loss function  $L_{IN}(\mathbf{H}_R, \mathbf{H}_I, \mathbf{w}, \mathbf{a}, \Phi)$  using (18)
- 17:      $E_{EX}$ : Calculate loss function  $L_{EX}(\mathbf{H}_R, \mathbf{H}_I, \mathbf{w}, \mathbf{a}, \Phi)$
- 18:     Update network weights
- 19:   **end for**
- 20: **until** reaches the maximum training process or the loss does not decreased over 30 consecutive epochs
- 21: **return** Optimized  $\mathbf{w}$ ,  $\mathbf{a}$ ,  $\Phi$

---

#### IV. PERFORMANCE RESULTS AND ANALYSIS

In this section, we present a performance evaluation for the proposed CO-GNN to solve the sum secrecy rate optimization problems in IRS-assisted NOMA networks.

##### A. Setting and Benchmarks

The program in this study was developed based on the TensorFlow [26] framework, and all experiments were conducted using an RTX 3090 Ti GPU. And the hyperparameters used in our model are shown in TABLE II. Specifically, our neural network was trained to utilize the Adam optimizer [27] with an initial learning rate  $1 \times 10^{-4}$ . The training process is designed to terminate if it reaches the maximum of 100 epochs or if the loss function does not decrease over 30 consecutive training epochs. During each training epoch, we iterate 100 times to update the parameters of the neural network, with 10000 training samples being used to compute the gradients

TABLE II: Simulation Parameters

System Parameter	Numerical Value
Number of antennas	5
Number of reflecting elements	100
Number of users	2
Number of eavesdropper	1
Number of message passing la	1
The Rician factor	10dBm
Transmit Power	30dBm
Noise power	-100dBm
The coordinates of BS	(0,0,0)
The coordinates of IRS	(rand(20,30),rand(20,30),0)
The coordinates of users	(rand(30,50),rand(30,50),-10)
The coordinates of external eve	(rand(50,100),rand(30,50),-20)
Path loss for $\mathbf{h}_{d,k}$	32.6+36.7lgd
Path loss for $\mathbf{G}$ and $\mathbf{h}_{r,k}$	30.0+22.0lgd
Learning rate	$1 \times 10^{-4}$
Max epochs	100
No-increasing epochs	30
Training samples	10000

in each iteration. In the testing phase, our CO-GNN network is compared against five benchmarks.

The benchmarks we compare the CO-GNN networks with are as follows:

- *Benchmark 1. GNN & Average Power:* To evaluate the effectiveness of joint optimization in CO-GNN, we conduct comparative GNN-based optimization experiments. Specifically, we design a neural network model closely resembling CO-GNN to maximize the sum secrecy rate. The model's configuration restricts optimization variables to beamforming and phase shifts, omitting the power allocation factor. We allocate power evenly between the two users, resulting in a uniform power allocation factor of  $[0.5, 0.5]$ .
- *Benchmark 2. GNN & Random IRS:* Given the random IRS, the GNN network is trained to optimize both the power allocation factor and beamforming to maximize the sum secrecy rate.
- *Benchmark 3. GNN & Omni-beam:* Given the omnidirectional beam, the GNN network is trained to optimize the power allocation factor and phase shifts to maximize the sum secrecy rate.
- *Benchmark 4. Alternating Optimization:* In the alternating optimization approach proposed in [28], we conduct joint optimization in three phases to enhance the secrecy rate. Initially, beamforming is optimized using the weighted minimum mean-squared error (WMMSE) algorithm [29]. Next, phase optimization is performed employing the Riemannian conjugate gradient (RCG) algorithm [30]. Subsequently, the problem simplifies, enabling the application of a genetic algorithm for optimizing the power allocation factors.

##### B. Results and Analysis

To assess the convergence of the CO-GNN algorithm, we conduct several experiments varying the critic learning rates and batch sizes in the external eve scenario, with results



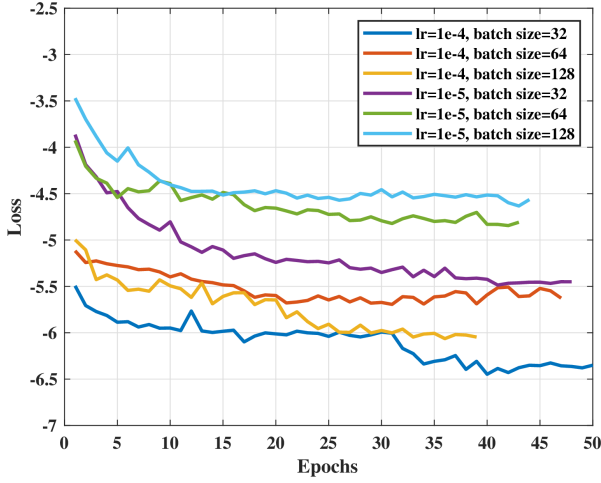


Fig. 3: The convergence of the proposed CO-GNN networks

depicted in Fig. 3. Our focus lies on the impact of critic learning rates, as the performance of CO-GNN algorithms heavily relies on the accuracy of the action-value function approximation. As depicted in Fig. 3, a learning rate of  $1 \times 10^{-4}$  yields lower loss, indicating a higher secrecy rate compared to the learning rate of  $1 \times 10^{-5}$ . Additionally, although a batch size of 32 requires more epochs to converge, it consistently exhibits the lowest loss with the given learning rate. Consequently, we opt for a batch size of 32 and a critic learning rate of  $1 \times 10^{-4}$  in subsequent experiments to achieve optimal optimization results.

Fig. 4 illustrates the sum secrecy rate of various schemes concerning the transmit power  $P_t$  when  $M = 5$ ,  $N = 100$ , and  $K = 2$  in an external eavesdropper scenario. Simulation results demonstrate that the sum secrecy rate monotonically increases with the transmit power  $P_t$ . Remarkably, the proposed CO-GNN scheme achieves the highest secrecy rate among all compared methods, significantly outperforming conventional benchmarks. In scenarios with external eavesdroppers, the sum secure rate of CO-GNN exhibits approximately 40% improvement over the AO scheme. This observation is consistent with conventional multiuser Multiple-Input Single-Output (MISO) systems. Through the joint optimization of transmit beamforming, power allocation, and phase shifts, the co-channel interference can be designed to damage the Eve, leading to performance enhancement with increasing  $P_t$ . Notably, the random IRS scheme exhibits the lowest rate. This underscores the significance of incorporating an IRS and optimizing its parameters to significantly enhance the system's secrecy rate. Moreover, both the 'GNN & Omni-beam' and the 'Alternating Optimization' scheme demonstrate nearly identical performance. This suggests that the similarity in optimization efforts of both algorithms results in their convergence towards the same stationary solution with high probability.

Fig. 5 illustrates the sum secrecy rate as a function of power  $P_t$  under an internal eavesdropping scenario with  $M = 5$ ,  $N = 100$ , and  $K = 2$ . In contrast to external eavesdropping, the secrecy rate exhibits a more pronounced increase in the in-

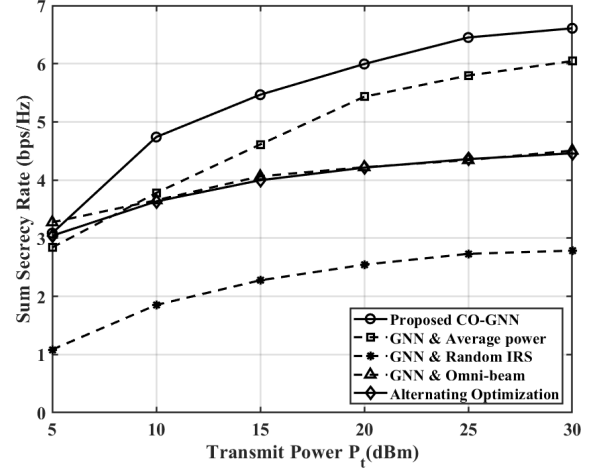


Fig. 4: The sum secrecy rate versus transmit power  $P_t$  under external eavesdropping scenario, with  $M = 5$ ,  $N = 100$ , and  $K = 2$ .

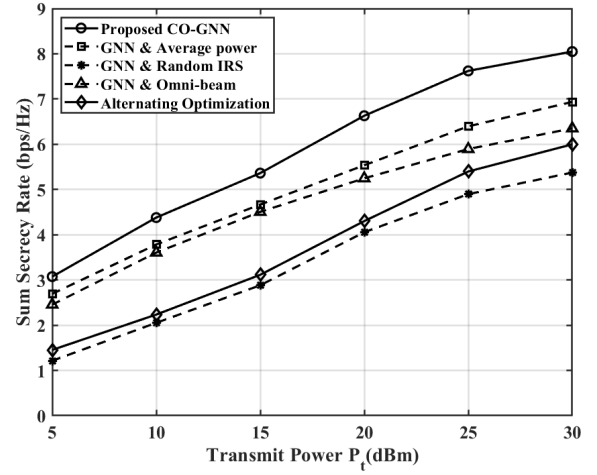


Fig. 5: The sum secrecy rate versus transmit power  $P_t$  under internal eavesdropping scenario, with  $M = 5$ ,  $N = 100$ , and  $K = 2$ .

ternal eavesdropping scenario. We hypothesize that this is due to the node targeted for internal eavesdropping being treated as a legitimate node before in the model. Consequently, the neural network can effectively enhance its link performance. Conversely, when the node is acting as an eavesdropper, the neural network can more effectively suppress its activity, resulting in a higher level of security. Simulation results demonstrate that under internal eavesdropping scenarios, the CO-GNN scheme achieves approximately 30% higher secrecy rate than the conventional AO approach. Additionally, the 'GNN & Random IRS' scheme, despite being the lowest-performing, demonstrates similar effects to the "Alternating Optimization" scheme, highlighting the advantages of employing GNN for optimization in the context of internal eavesdropping scenarios.

Fig. 6 presents a comparison of the sum secrecy rate

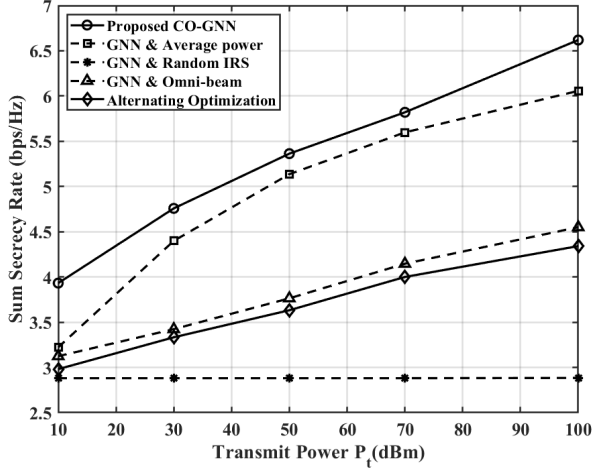


Fig. 6: The sum secrecy rate versus the number of reflecting elements  $N$  under external eavesdropping scenario, with  $M = 5$ ,  $K = 2$ , and  $P_t = 30$ dBm.

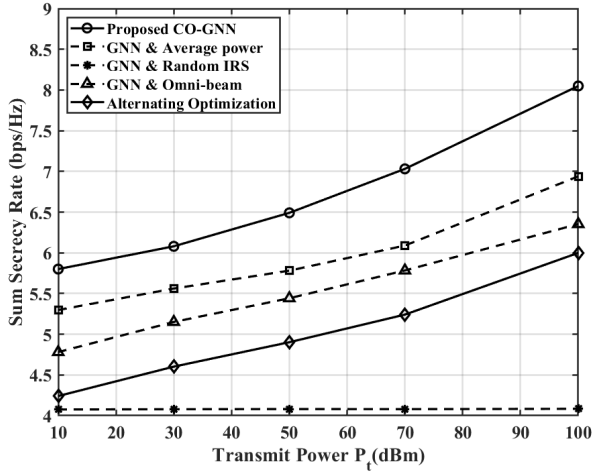


Fig. 7: The sum secrecy rate versus the number of reflecting elements  $N$  under internal eavesdropping scenario, with  $M = 5$ ,  $K = 2$ , and  $P_t = 30$ dBm.

against the number of elements in the IRS  $N$  in an external eavesdropping scenario with  $M = 5$ ,  $K = 2$  and  $P_t = 30$ dBm. It is noticeable that the rate for the 'GNN & Random IRS' scheme remains relatively constant, exhibiting insensitivity to variations in the number of IRS elements, whereas all IRS-assisted schemes achieve remarkable performance gains as  $N$  increases. By deploying an IRS with a greater number of reflecting elements, we can effectively enhance the user links and suppress external eavesdropping, ensuring the security of the two legitimate users.

Fig. 7 elucidates the variation of the sum secrecy rate concerning the number of elements in the IRS  $N$  within an internal eavesdropping scenario with parameters  $M = 5$ ,  $K = 2$  and  $P_t = 30$ dBm. With the exception of the relatively insensitive 'GNN & Random IRS' scheme, all GNN optimization schemes outperform the 'Alternating Optimization'

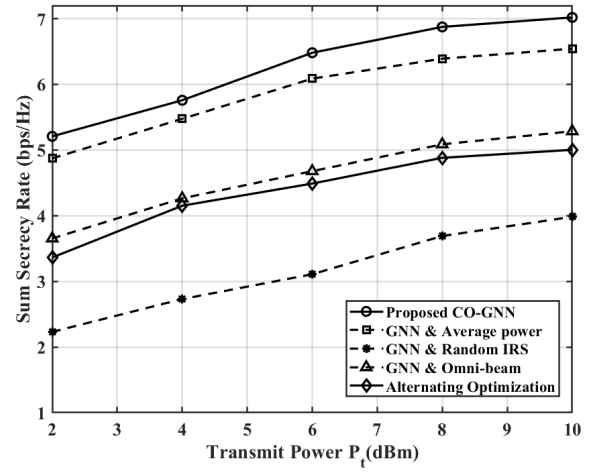


Fig. 8: The sum secrecy rate versus the number of antennas  $M$  under external eavesdropping scenario, with  $K = 2$ ,  $N = 100$  and  $P_t = 30$ dBm.

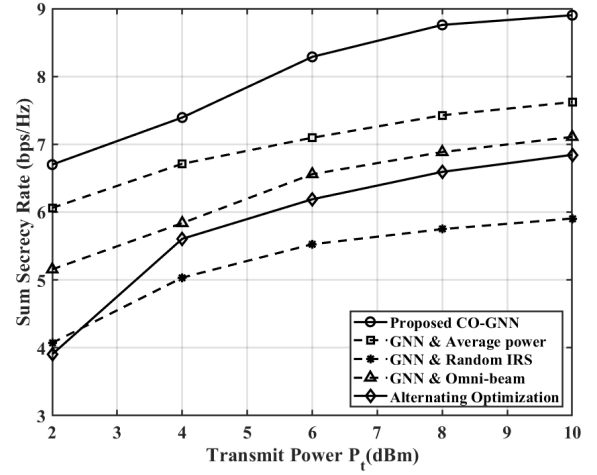


Fig. 9: The sum secrecy rate versus the number of antennas  $M$  under internal eavesdropping scenario, with  $K = 2$ ,  $N = 100$  and  $P_t = 30$ dBm.

scheme, with our proposed CO-GNN demonstrating the highest sum secrecy rate. Furthermore, in the context of internal eavesdropping, the trend observed in this figure closely mirrors the curve depicted in Fig. 5, suggesting a similarity in the effects of power and the number of IRS elements on the sum secrecy rate under internal eavesdropping scenarios.

Fig. 8 and Fig. 9 delineate the influence of the number of transmit antennas  $M$  on the sum secrecy rate under the conditions of  $K = 2$ ,  $N = 100$  and  $P_t = 30$ dBm. These figures reveal a monotonic increase in the sum secrecy rate as the number of transmit antennas increases. It can be attributed to the ability of additional antennas to bolster the strength of the main links and provide a more centralized approach, thereby confounding potential eavesdroppers through optimized beamforming, power allocation, and phase shifts. It is noteworthy that even with a limited number of antennas,

the sum secrecy rate remains high across all experimental scenarios. This resilience is attributed to the combined effect of the specified power level,  $P_t = 30\text{dBm}$ , and the ample number of elements in the IRS,  $N = 100$ , which collectively ensure the robust security of the system.

### C. Interpretation of Optimization of CO-GNN

To substantiate the effectiveness of joint optimization within our proposed CO-GNN framework, we present visualizations demonstrating the optimized outcomes. These visualizations aptly illustrate the refined directions and angles relevant to beamforming and phase shifts. The detailed analysis of these results heavily relies on the angular configurations of each node. Accordingly, we define  $\phi_1, \phi_2$  as the AoD from the IRS to the BS and AoA from the users to the IRS, respectively. The corresponding elevation angles are denoted as  $\eta_1$  and  $\eta_2$ .

From the steering vectors (4), (8), (10) and (11), we can get the array response of IRS as follows:

$$A(\phi_1, \eta_1, \phi_2, \eta_2) = |\Phi^H e^{j\pi(i_1(n)\tau_1 + i_2(n)\tau_2)}|, \quad (33)$$

where  $\tau_1 = \sin(\phi_2)\cos(\eta_2) - \sin(\phi_1)\cos(\eta_1)$  and  $\tau_2 = \sin(\eta_2) - \sin(\eta_1)$ .

To investigate the impact of angles on the array response at varying IRS numbers, we fixed the location of the BS at  $(0,0,0)$  and the IRS at  $(20,30,0)$ . Furthermore, we positioned two users at  $(40,40,-10)$  and  $(40,45,-10)$ . The visualization of this experimental configuration is shown in Fig. 11. We assigned  $(\phi_2, \eta_2)$  values of  $(0.4636, 0.4082)$  and  $(0.6435, 0.3714)$  to these users. Utilizing our trained model with optimized beamforming, power allocation, and phase shifts, we obtain the array response of the IRS. The results are presented in Fig. 10, which comprises a 3D view for  $N = 10, 50, 100$ . From these figures, it is evident that the peak values precisely align with the angles  $\phi_2$  and  $\eta_2$ , corresponding to the two users. Notably, as the number of IRS elements increases, the peaks become more pronounced and concentrated to the angles of both legitimate users. This signifies that a greater number of IRS elements exert higher control over the beamforming, enabling a more focused and directed transmission of signals towards the users, while effectively

mitigating the signal leakage towards the eavesdropper. Hence, our proposed CO-GNN framework effectively integrates joint optimization techniques, leading to maximized sum secrecy rates for both users.

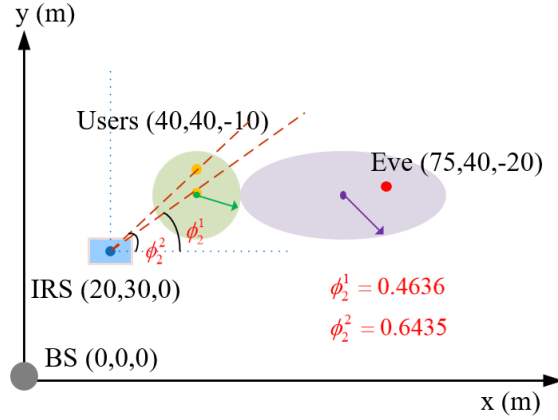


Fig. 11: The visual simulation setup of experimental configuration

### D. Computational Complexity Analysis

This subsection investigates the computational complexity of different schemes. For the GNN-based schemes, since there is no strict time limit at the offline training stage, we only consider the computational complexity at the online test stage in the CPU. The computational complexity analysis of different schemes are as follows.

- For our CO-GNN scheme, the computational complexity is  $O((3 \times 3 + L)d_{MLP}T_R)$ , where  $3 \times 3$  means the number of input and output layers of three optimized parameters,  $L = 8$  is the number of network layers,  $d_{MLP} = 512$  is the dimension of linear embedding and  $T_R$  is the time of calculate sum secrecy rate.
- The computational complexity of *GNN & Average Power*, *GNN & Random IRS*, *GNN & Omni-beam* is  $O((3 \times 2 + L)d_{MLP}T_R'')$  since the optimization goal is two in these schemes. Meanwhile, there are differences

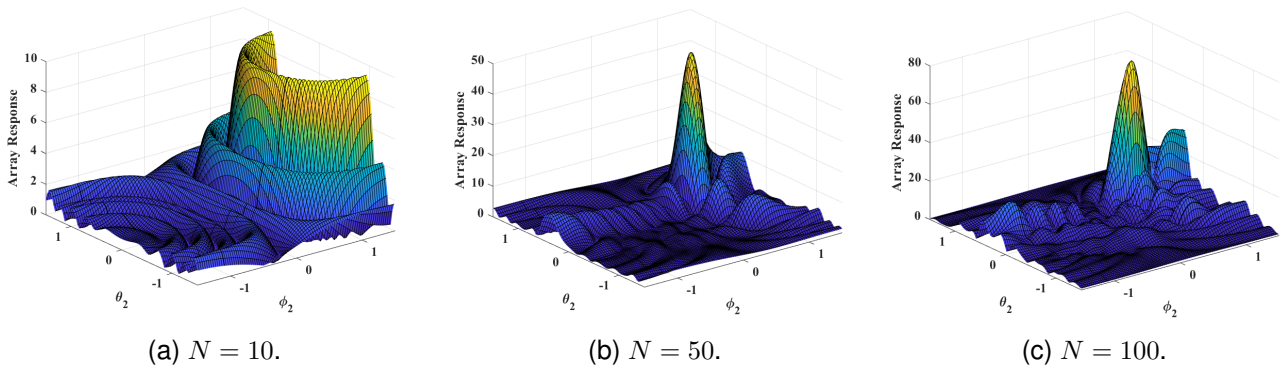


Fig. 10: Array response of IRS obtained from CO-GNN over two users with  $M = 5$ , 3-D view. The optimal  $(\phi_2, \eta_2) = (0.4636, 0.4082), (0.6435, 0.3714)$ .

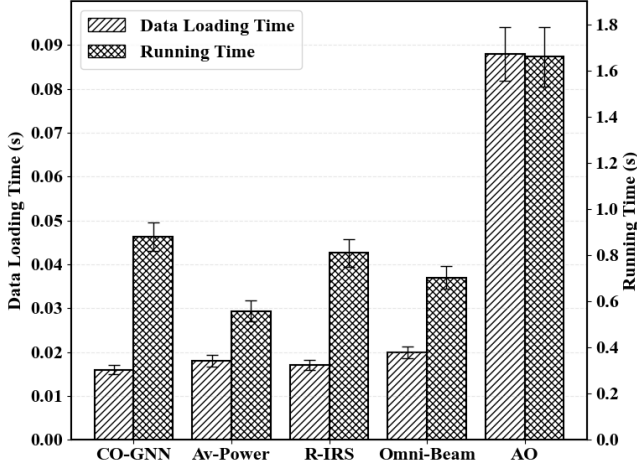


Fig. 12: Computing time of different schemes.

in the  $T_R''$  in these schemes, leading to slight variations in computational complexity.

- As for the AO algorithm, the complexity of the WMMSE algorithm is  $O(I_\lambda I_w K M^3)$ , where  $I_\lambda$  and  $I_w$  are the iteration numbers of searching  $\lambda$  and the three-step updating loop. Meanwhile, the complexity of the RCG algorithm is decided by the Euclidean gradient, which is computed as  $O(K^2 N^2)$ . The complexity of genetic algorithm is depends on the Population size  $P_o$  and evolutionary generations  $t$ . So the total complexity of the alternating optimization is  $O(I_\lambda I_w K M^3 + K^2 N^2 + P_o t)$ .

To intuitively observe the computational complexity across different schemes, Fig. 12 shows the data loading time and the running time of different schemes in the CPU. Notably, the figure reveals that our CO-GNN approach significantly outperforms the AO scheme in both metrics. In terms of data loading time, which encapsulates the duration for importing test data and pre-trained models, the AO algorithm's slightly prolonged model import time contributes to its marginally higher overall loading time compared to other schemes. As for running time, the AO scheme necessitates separate optimization of three parameters, which results in a higher execution time compared to the neural network model, which directly derives the optimized parameters.

## V. CONCLUSION

In this paper, we have developed a secure model for an IRS-assisted NOMA transmission system, accounting for both external and internal eavesdroppers in heterogeneous networks, as well as potential hardware impairments. Furthermore, we introduce a novel joint optimization approach, CO-GNN, which is designed to optimize the heterogeneous resources and obtain the optimized transmit beamforming at BS, power allocation for NOMA users, and phase shifts of IRS, aiming to maximize the sum secrecy rate of legitimate users. Our CO-GNN exhibits a standardized formulation and low implementation complexity, eliminating the need for explicit mathematical representations of wireless systems and

intricate channel estimation procedures. This simplifies the scaling process to accommodate diverse system configurations.

Simulation results underscore the necessity and efficacy of jointly optimizing beamforming, power allocation, and phase shifts. Additionally, as transmit power, the number of IRS reflecting elements, or transmit antennas increase, the security of our model experiences a significant enhancement. Notably, compared with conventional AO schemes, the CO-GNN achieves superior security performance while maintaining low computational complexity. These findings not only establish the superiority of our proposed method but also highlight its practicality and scalability in real-world scenarios.

Future research will extend the current framework by: rigorously validating the theoretical security boundaries of CO-GNN against heterogeneous attack strategies in complex threat scenarios to establish a generalized anti-jamming model; designing real-time sensing-based adaptive IRS reconfiguration algorithms to address practical deployment challenges such as IRS occlusion, mobility, and environmental perturbations, thereby enhancing system resilience under non-ideal channel conditions; and exploring deep integration mechanisms between CO-GNN and physical-layer security techniques, such as artificial noise injection and cryptographic encoding, to construct a cross-layer cooperative optimization framework that maximizes eavesdropper obfuscation through dynamic resource allocation while ensuring quality-of-service for legitimate users. These efforts will systematically bridge the gap between theoretical models and engineering practices, facilitating reliable deployment of secure IRS-NOMA networks in complex heterogeneous environments.

## REFERENCES

- [1] Z. Sun and Y. Jing, "On the performance of multi-antenna ired-assisted noma networks with continuous and discrete ired phase shifting," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 3012–3023, May. 2022.
- [2] J. Zhu, Y. Huang, J. Wang, K. Navaie, and Z. Ding, "Power efficient ired-assisted noma," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 900–913, Feb. 2021.
- [3] Y. Omid, S. M. M. Shahabi, C. Pan, Y. Deng, and A. Nallanathan, "Robust beamforming design for an ired-aided noma communication system with csi uncertainty," *IEEE Trans. Wireless Commun.*, vol. 23, no. 2, pp. 874–889, Feb. 2024.
- [4] X. Mu, Y. Liu, L. Guo, J. Lin, and N. Al-Dhahir, "Exploiting intelligent reflecting surfaces in noma networks: Joint beamforming optimization," *IEEE Trans. Wireless Commun.*, vol. 19, no. 10, pp. 6884–6898, Oct. 2020.
- [5] W. U. Khan, E. Lagunas, A. Mahmood, Z. Ali, M. Asif, S. Chatzinotas, and B. Ottersten, "Integration of noma with reflecting intelligent surfaces: A multi-cell optimization with sic decoding errors," *IEEE Trans. Green Commun.*, vol. 7, no. 3, pp. 1554–1565, Sep. 2023.
- [6] Z. Li, W. Chen, Q. Wu, K. Wang, and J. Li, "Joint beamforming design and power splitting optimization in ired-assisted swipt noma networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 2019–2033, Mar. 2022.
- [7] C. K. Singh, P. K. Upadhyay, J. Lehtomäki, and M. Juntti, "Performance analysis with deep learning assay for cooperative uav-borne ired noma networks under non-ideal system imperfections," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 1065–1083, Jan. 2024.
- [8] R. H. Y. Perdana, T.-V. Nguyen, and B. An, "Adaptive user pairing in multi-ired-aided massive mimo-noma networks: Spectral efficiency maximization and deep learning design," *IEEE Trans. Commun.*, vol. 71, no. 7, pp. 4377–4390, 2023.
- [9] X. Gao, Y. Liu, X. Liu, and L. Song, "Machine learning empowered resource allocation in ired aided miso-noma networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 3478–3492, 2022.

- [10] H. Chen, G. Zhang, X. Li, and P. Zhu, "Multi-agent deep reinforcement learning based resource management in 5g-noma terahertz network," in *2022 IEEE/CIC International Conference on Communications in China (ICCC)*, Aug. 2022, pp. 766–771.
- [11] J. Yu, Y. Li, X. Liu, B. Sun, Y. Wu, and D. H. Tsang, "Energy efficient 5g assisted noma aided mobile edge computing via heterogeneous multi-agent reinforcement learning," in *ICC 2023 - IEEE International Conference on Communications*, May. 2023, pp. 5352–5357.
- [12] J. Yu, Y. Li, X. Liu, B. Sun, Y. Wu, and D. Hin-Kwok Tsang, "5g assisted noma aided mobile edge computing with queue stability: Heterogeneous multi-agent reinforcement learning," *IEEE Trans. Wireless Commun.*, vol. 22, no. 7, pp. 4296–4312, Jul. 2023.
- [13] Q. Sun, H. You, and H. Liu, "Supervised learning-based joint active and passive beamforming for 5g-assisted noma systems," in *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, Aug. 2022, pp. 152–157.
- [14] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and jamming optimization for 5g-aided secure noma networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, Mar. 2022.
- [15] Y. Feng, J. Chen, X. Xue, K. Wu, Y. Zhou, and L. Yang, "Max-min fair beamforming for 5g-aided secure noma systems," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 234–238, Feb. 2022.
- [16] Z. Zhang, L. Lv, Q. Wu, H. Deng, and J. Chen, "Robust and secure communications in intelligent reflecting surface assisted noma networks," *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 739–743, Mar. 2021.
- [17] Y. Han, N. Li, Y. Liu, T. Zhang, and X. Tao, "Artificial noise aided secure noma communications in star-5g networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 1191–1195, Jun. 2022.
- [18] Z. Zhang, J. Chen, Q. Wu, Y. Liu, L. Lv, and X. Su, "Securing noma networks by exploiting intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1096–1111, Feb. 2022.
- [19] C. Gong, X. Yue, X. Wang, X. Dai, R. Zou, and M. Essaidi, "Intelligent reflecting surface aided secure communications for noma networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2761–2773, Mar. 2022.
- [20] L. Lv, Q. Wu, Z. Li, Z. Ding, N. Al-Dhahir, and J. Chen, "Covert communication in intelligent reflecting surface-assisted noma systems: Design, analysis, and optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1735–1750, Mar. 2022.
- [21] J. Zhang, W. Wang, J. Tang, N. Zhao, K.-K. Wong, and X. Wang, "Joint analog and passive beamforming design for 5g-aided secure cognitive noma systems," in *ICC 2023 - IEEE International Conference on Communications*, May. 2023, pp. 4267–4272.
- [22] H. Han, Y. Cao, M. Sheng, N. Zhao, J. Liu, and D. Niyato, "5g-aided secure noma networks against internal and external eavesdropping," *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7536–7548, Nov. 2022.
- [23] L. Guo, J. Jia, J. Chen, and X. Wang, "Secure communication optimization in noma systems with uav-mounted star-5g," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 2300–2314, 2024.
- [24] E. Björnson and L. Sanguinetti, "Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces," *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830–834, Apr. 2021.
- [25] K. Xu, W. Hu, L. Jure, and J. Stefanie, "How powerful are graph neural networks?" in *International Conference on Learning Representations*, 2019.
- [26] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, and M. Devin, "Tensorflow: Large-scale machine learning on heterogeneous distributed systems," *hgpu.org*, 2015.
- [27] D. Kingma and J. Ba, "Adam: A method for stochastic optimization," *Computer Science*, 2014.
- [28] H. Guo, Y.-C. Liang, J. Chen, and E. G. Larsson, "Weighted sum-rate maximization for reconfigurable intelligent surface aided wireless networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3064–3076, May 2020.
- [29] Q. Shi, M. Razaviyayn, Z.-Q. Luo, and C. He, "An iteratively weighted mmse approach to distributed sum-utility maximization for a mimo interfering broadcast channel," *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4331–4340, Sep. 2011.
- [30] N. Boumal, B. Mishra, P.-A. Absil, and R. Sepulchre, "Manopt, a matlab toolbox for optimization on manifolds," *J. Mach. Learn. Res.*, vol. 15, no. 1, p. 1455–1459, Jan. 2014.