

Deep Learning Based Joint Beamforming Design in IRS-Assisted Secure Communications

Chi Zhang, Yiliang Liu, *Member, IEEE*, and Hsiao-Hwa Chen, *Fellow, IEEE*

Abstract—In this article, physical layer security (PLS) in an intelligent reflecting surface (IRS) assisted multiple-input multiple-output multiple antenna eavesdropper (MIMOME) system is studied. In particular, we consider a practical scenario without instantaneous channel state information (CSI) of the eavesdropper and assume that the eavesdropping channel is a Rayleigh channel. To reduce the complexity of currently available IRS-assisted PLS schemes, we propose a low-complexity deep learning (DL) based approach to design transmitter beamforming and IRS jointly, where the precoding vector and phase shift matrix are designed to minimize the secrecy outage probability. Simulation results demonstrate that the proposed DL-based approach can achieve a similar performance of that with conventional alternating optimization (AO) algorithms for a significant reduction in the computational complexity.

Index Terms—Intelligent reflecting surface; Physical layer security; Joint beamforming design; Deep learning.

I. INTRODUCTION

Intelligent reflecting surface (IRS) is a 2-D electromagnetic metasurface composed of a large number of low-cost passive elements that can change wireless propagation environment to improve the performance of wireless communication systems [1]. Physical layer security (PLS) is a type of information security technique that utilizes the randomness of wireless channels to achieve confidential communications [2]. As IRS can improve the quality of legitimate channels while mitigating that of eavesdropped channels, the two techniques combined have a complementary nature of advantages [3].

In [4] and [5], the authors investigated PLS of IRS-assisted single-input single-output (SISO) and multiple-input single-output (MISO) communication systems to maximize secrecy rate of the system by alternating optimization (AO) algorithms. In [6], the authors extended it to a multiple-user case that transmits artificial noise (AN) to enhance the security performance. Moreover, [7] focused on a novel idea of IRS-assisted PLS, in which IRS was deployed to modulate received signal from a transmitter as AN signals. However, the above works were based largely on the assumption that eavesdropper's instantaneous channel state information (CSI) is known. The authors of [8] investigated the PLS by jointly optimizing precoding, IRS phase shift matrix, and AN when the eavesdropper's CSI was unknown, but there was no appropriate metric to evaluate the performance of PLS. The work in [9] used a

large number of random samples instead of eavesdropper's statistical CSI, but the proposed optimization algorithm needs to take into account all random samples, which consumes a lot of computational resources. In [10], the authors investigated the PLS based on eavesdropper's statistical CSI and derived a secrecy outage probability expression as a security metric. However, the complexity of the proposed AO algorithm for the optimization problem of minimizing secrecy outage probability is very high.

To address the CSI issue, we consider an IRS-assisted PLS scenario based on the eavesdropper's statistical CSI. Different from [10], we think the large-scale fading to be non-negligible, so we consider the large-scale fading in the calculation of the secrecy outage probability. Motivated by the machine learning-based research works [12]–[14], we propose a low-complexity deep learning (DL) based approach to design transmitter beamforming and phase shift matrix to minimize the secrecy outage probability, which works based on unsupervised learning and does not need dataset labels.

II. SYSTEM MODEL

Let us consider an IRS-assisted multiple-input multiple-output multiple antenna eavesdropper (MIMOME) system, as shown in Fig. 1, where a transmitter (Alice) equipped with N_t antennas serves an N_r -antenna legitimate user (Bob), assisted by an IRS with N_s reflecting elements. Meanwhile, there is an eavesdropper (Eve) with N_e antennas that receives signals from Alice and IRS. The legitimate channels from Alice to Bob, Alice to IRS, and IRS to Bob are denoted by $\mathbf{H}_b \in \mathbb{C}^{N_r \times N_t}$, $\mathbf{H} \in \mathbb{C}^{N_s \times N_t}$, and $\mathbf{G}_r \in \mathbb{C}^{N_r \times N_s}$, respectively. The wiretap channels from Alice to Eve and IRS to Eve are denoted by $\mathbf{H}_e \in \mathbb{C}^{N_e \times N_t}$ and $\mathbf{G}_e \in \mathbb{C}^{N_e \times N_s}$, respectively. Assume that all channels follow the quasi-static flat-fading channel model, and the legitimate channels \mathbf{H}_b , \mathbf{G}_r , and \mathbf{H} can be perfectly estimated at Alice [15], while the instantaneous CSIs of wiretap channels \mathbf{H}_e and \mathbf{G}_e are unknown to Alice. In addition, we further assume that the wiretap channels obey Rayleigh fading without loss of generality.

Let s be the transmitted single-stream confidential signal following $\mathbb{E}[|s|^2] = 1$. Then, the received signals at Bob and Eve can be expressed as

$$\mathbf{y} = (\mathbf{H}_b + \mathbf{G}_r \mathbf{\Theta} \mathbf{H}) \mathbf{w} s + \mathbf{n}, \quad (1)$$

$$\mathbf{y}_e = (\mathbf{H}_e + \mathbf{G}_e \mathbf{\Theta} \mathbf{H}) \mathbf{w} s + \mathbf{n}_e, \quad (2)$$

where $\mathbf{\Theta} = \text{diag}(e^{j\theta_1}, e^{j\theta_2}, \dots, e^{j\theta_{N_s}})$ denotes a phase shift matrix and θ_n is the phase shift introduced by the n th element of IRS. $\mathbf{w} \in \mathbb{C}^{N_t \times 1}$ is the precoding vector and

C. Zhang (email: maye1998@163.com) is with the School of Electronics and Information Engineering, Harbin Institute of Technology, China. Y. Liu (email: liuyiliang@xjtu.edu.cn) is with the School of Cyber Science and Engineering, Xi'an Jiaotong University, China. Hsiao-Hwa Chen (email: hshwchen@mail.ncku.edu.tw) is with the Department of Engineering Science, National Cheng Kung University, Taiwan.

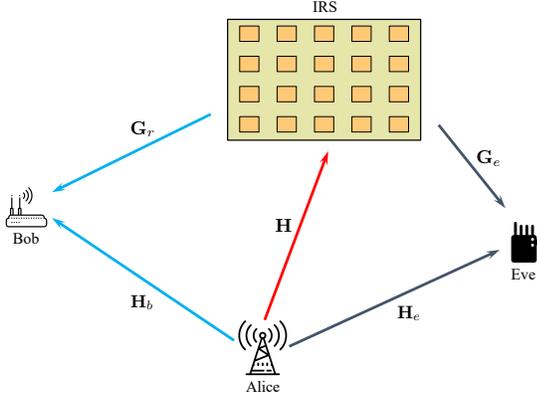


Fig. 1. An IRS-assisted MIMOME system.

satisfies $\|\mathbf{w}\|^2 = P_t$, where P_t is the transmit power of Alice. $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_{N_t})$ and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \sigma_e^2 \mathbf{I}_{N_e})$ are additive white Gaussian noise (AWGN) at Bob and Eve, respectively.

To maximize the signal-noise-ratio (SNR) at Bob, the corresponding received signal vector $\mathbf{w}_r = [(\mathbf{H}_b + \mathbf{G}_r \Theta \mathbf{H}) \mathbf{w}]^H / \|(\mathbf{H}_b + \mathbf{G}_r \Theta \mathbf{H}) \mathbf{w}\|$ is given with the maximum ratio combining (MRC) strategy [2]. We consider a worst-case scenario that Eve has perfect knowledge about \mathbf{H}_e , \mathbf{G}_e , \mathbf{H} , \mathbf{G}_r , Θ , and \mathbf{w} within the coherence time. Then, Eve can also maximize the SNR using the MRC strategy. Accordingly, the channel capacities at Bob and Eve are given by

$$C_m = \log_2 \left[1 + \frac{P_t}{\sigma^2} \|(\mathbf{H}_b + \mathbf{G}_r \Theta \mathbf{H}) \mathbf{b}\|^2 \right], \quad (3)$$

$$C_w = \log_2 \left[1 + \frac{P_t}{\sigma_e^2} \|(\mathbf{H}_e + \mathbf{G}_e \Theta \mathbf{H}) \mathbf{b}\|^2 \right], \quad (4)$$

where C_m and C_w are the main channel capacity and wiretap channel capacity, respectively, and $\mathbf{b} = \mathbf{w}/\sqrt{P_t}$ is the normalized precoding vector.

However, due to the wiretap channels \mathbf{H}_e and \mathbf{G}_e which are unknown, it is not possible to calculate the secrecy capacity C_s , where $C_s = [C_m - C_w]^+$. Therefore, we choose secrecy outage probability as a security metric for PLS, which is defined as the probability that the secrecy capacity C_s is smaller than the target PLS coding rate R_s . The secrecy outage probability is defined as

$$P_{\text{out}}(R_s) = P(C_s \leq R_s \mid \text{Transmission}) \quad (5a)$$

$$= P(\|(\mathbf{H}_e + \mathbf{G}_e \Theta \mathbf{H}) \mathbf{b}\|^2 \geq \phi), \quad (5b)$$

where $\phi = \sigma_e^2 (2^{C_m - R_s} - 1) / P_t$.

Assume that wiretap channels \mathbf{H}_e and \mathbf{G}_e obey Rayleigh fading in this work, i.e., $\mathbf{H}_e = \beta_d \mathbf{Z}$ and $\mathbf{G}_e = \beta_r \mathbf{C}$, where $\mathbf{Z} \sim \mathcal{CN}_{N_e, N_t}(\mathbf{0}, \mathbf{I}_{N_e} \otimes \mathbf{I}_{N_t})$ and $\mathbf{C} \sim \mathcal{CN}_{N_e, N_s}(\mathbf{0}, \mathbf{I}_{N_e} \otimes \mathbf{I}_{N_s})$. Note that \otimes , β_d , and β_r denote the Kronecker products, large-scale fading factors of \mathbf{H}_e and \mathbf{G}_e , respectively.

To derive an expression of the secrecy outage probability, we introduce an auxiliary random variable X as follows.

$$X = \|(\mathbf{H}_e + \mathbf{G}_e \Theta \mathbf{H}) \mathbf{b}\|^2 \quad (6a)$$

$$= \|\beta_d \mathbf{Z} \mathbf{b} + \beta_r \mathbf{C} \Theta \mathbf{H} \mathbf{b}\|^2. \quad (6b)$$

The secrecy outage probability can be given by

$$P_{\text{out}}(R_s) = 1 - F_X(\phi), \quad (7)$$

where $F_X(\cdot)$ is the cumulative distribution function (CDF) of X . With the help of a Gamma distribution [10], [11], we can deduce an approximate expression of secrecy outage probability as¹

$$P_{\text{out}}(R_s) = \frac{1}{\Gamma(N_e)} \Gamma\left(N_e, \frac{\phi}{\beta_d^2 + \beta_r^2 \|\Theta \mathbf{H} \mathbf{b}\|^2}\right), \quad (8)$$

where $\Gamma(m) = \int_0^\infty t^{m-1} e^{-t} dt$ is the Gamma function, and $\Gamma(m, n) = \int_n^\infty t^{m-1} e^{-t} dt$ is the upper incomplete Gamma function.

In this work, we aim to design joint beamforming by optimizing Θ and \mathbf{b} at Alice and IRS to minimize the secrecy outage probability. Moreover, the secrecy outage probability P_{out} decreases as $\phi / (\beta_d^2 + \beta_r^2 \|\Theta \mathbf{H} \mathbf{b}\|^2)$ increases [10]. Thus, the optimization problem can be formulated as

$$\max_{\Theta, \mathbf{b}} \frac{\phi}{\beta_d^2 + \beta_r^2 \|\Theta \mathbf{H} \mathbf{b}\|^2}, \quad (9a)$$

$$\text{s.t. } \mathbf{b}^H \mathbf{b} = 1, \quad (9b)$$

$$|e^{j\theta_n}| = 1, \forall n = 1, \dots, N_s. \quad (9c)$$

It is worth noting that the optimal global solution of the optimization problem with a non-convex unit modulus constraint Eq. (9c) is not available. Therefore, [10] proposed a conventional AO algorithm to solve it, but the computational complexity is very high. In the next section, we will propose a DL-based approach that has a much lower computational complexity.

III. DL-BASED JOINT BEAMFORMING DESIGN

In this section, we propose a low complexity DL-based joint beamforming network (JBFNet) to solve the problem (9). The detailed JBFNet architecture is shown in Fig. 2, which is divided into two parts. One part is named ‘‘PhaseNet’’ for predicting the phase shift matrix Θ of IRS, and the other part is named ‘‘BeamNet’’ for predicting the precoding vector \mathbf{w} . In the following subsections, we discuss the issues on the design of JBFNet in detail.

A. PhaseNet

PhaseNet adopts a multi-layer convolutional neural network (CNN) structure as shown in Fig. 3, which is commonly used in image processing problems and has been proven to be very effective in communication problems like beamforming design and channel estimation [12], [13]. In addition, compared with the commonly used fully connected network (FCN), CNN has a stronger feature extraction capability of 2-D data.

According to [16], the phase shift matrix Θ can be obtained by training the channel data, such that we choose the legitimate channels \mathbf{H}_b , \mathbf{G}_r , and \mathbf{H} as the input to PhaseNet, which are 2-D matrices. In order to improve JBFNet’s capability in feature

¹For the detailed derivation of the Eq. (8), please refer to <https://github.com/MayeZhang/DL-IRSBF-PLS>.

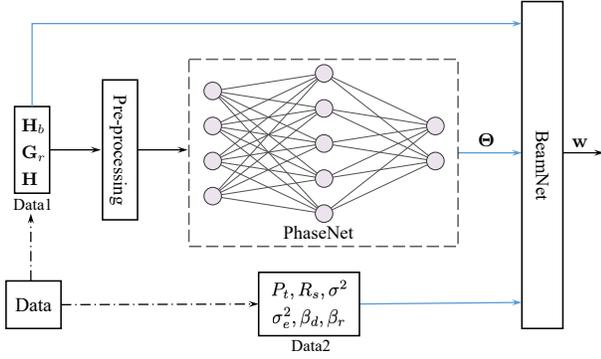


Fig. 2. Proposed JBNNet architecture for joint beamforming design, where data is composed of Data1 and Data2.

extraction, the input $\text{Data1} = \{\mathbf{H}_b, \mathbf{G}_r, \mathbf{H}\}$ needs to be pre-processed. Define $\mathbf{F}_n = \mathbf{g}_{r,n} \mathbf{h}_n^H$, where $\mathbf{g}_{r,n}$ is the n th column of \mathbf{G}_r , and \mathbf{h}_n^H is the n th row of \mathbf{H} . Specifically, \mathbf{F}_n is also the cascaded channel corresponding to the n th element of IRS. Then the channel in Eq. (1) can be rewritten as

$$\mathbf{H}_b + \mathbf{G}_r \Theta \mathbf{H} = \mathbf{H}_b + \sum_{n=1}^{N_s} e^{j\theta_n} \mathbf{F}_n. \quad (10)$$

Specifically, the original data $\mathbf{X} \in \mathbb{C}^{N_r \times N_t \times (N_s+1)}$ can be viewed as a $N_r \times N_t$ image with $N_s + 1$ channels, i.e., $\mathbf{X} = [\mathbf{H}_b; \mathbf{F}_1; \mathbf{F}_2; \dots; \mathbf{F}_{N_s}]$. The input data of the neural network are required to take real values, but the original data \mathbf{X} consisting of CSI are the complex values. To deal with this issue, the real part, imaginary part, and absolute value of each element of \mathbf{X} are extracted to form a new 3-D matrix, i.e., $\bar{\mathbf{X}} = \{\Re(\mathbf{X}), \Im(\mathbf{X}), \text{Abs}(\mathbf{X})\}$. Note that $\Re(\mathbf{X})$, $\Im(\mathbf{X})$, and $\text{Abs}(\mathbf{X})$ are combined according to the CNN channel dimension by default, i.e., $\bar{\mathbf{X}} \in \mathbb{R}^{N_r \times N_t \times 3(N_s+1)}$. In addition, the dimension can be flexibly selected for combination according to the actual parameter settings. For instance, when the number of receiving antennas $N_r = 2$, resulting in a small “image” that is not conducive to the feature extraction, the combination can be done by the first dimension, i.e., $\bar{\mathbf{X}} \in \mathbb{R}^{3N_r \times N_t \times (N_s+1)}$.

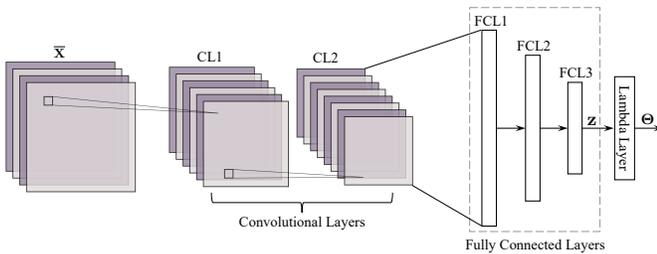


Fig. 3. PhaseNet framework for Θ based on CNN.

As shown in Fig. 3, the preprocessed data $\bar{\mathbf{X}}$ passes through two convolutional layers (CLs) and three fully connected layers (FCLs), and the results are finally outputted by the Lambda layer. We design CL1 with 256 filters of size 2×2 , CL2 with 512 filters of size 2×2 , FCL1 and FCL2 with $64N_s$ and $16N_s$ neurons, respectively. In particular, the number of neurons of FCL3 is set to N_s , which is the same as the number of IRS

reflecting elements. In order to prevent overfitting of the neural network, a batch normalization (BN) layer is inserted between every two layers, and we take rectified linear unit (ReLU) as the activation function except for FCL3. Specifically, FCL3 adopts “Sigmoid” as the activation function, so that the value of the output \mathbf{z} can be compressed between $(0, 1)$. Then, we can get the IRS phase shift matrix as $\Theta = \text{diag}[\exp(j \cdot 2\pi \mathbf{z})]$ through Lambda layer.

B. BeamNet

For any given phase shift matrix Θ , the objective function Eq. (9a) is transformed as

$$\frac{\phi}{\beta_d^2 + \beta_r^2 \|\Theta \mathbf{H} \mathbf{b}\|^2} = c \left(\frac{\mathbf{b}^H (t \mathbf{I}_{N_t} + \mathbf{Q}_1) \mathbf{b}}{\mathbf{b}^H (\beta_d^2 \mathbf{I}_{N_t} + \mathbf{Q}_2) \mathbf{b}} \right), \quad (11)$$

where $c = \sigma_e^2 / (2^{R_s} \sigma^2)$, $t = \sigma^2 (1 - 2^{R_s}) / P_t$, $\mathbf{Q}_1 = (\mathbf{H}_b + \mathbf{G}_r \Theta \mathbf{H})^H (\mathbf{H}_b + \mathbf{G}_r \Theta \mathbf{H})$, and $\mathbf{Q}_2 = \beta_r^2 \mathbf{H}^H \mathbf{H}$. According to the generalized Rayleigh quotient, the optimal \mathbf{b} is given by

$$\mathbf{b}^* = \text{eigvec}_{\lambda_{\max}} \left[(\beta_d^2 \mathbf{I}_{N_t} + \mathbf{Q}_2)^{-1} (t \mathbf{I}_{N_t} + \mathbf{Q}_1) \right], \quad (12)$$

where $\text{eigvec}_{\lambda_{\max}}(\mathbf{X})$ is the eigenvector corresponding to the largest eigenvalue of matrix \mathbf{X} , and λ_{\max} is the largest eigenvalue of \mathbf{X} . Thus, the optimal beamforming vector can be given by $\mathbf{w}^* = \sqrt{P_t} \mathbf{b}^*$.

In summary, BeamNet yields the optimal \mathbf{w}^* by computing Eq. (12) on the basis of the predicted Θ of PhaseNet, Data1, and $\text{Data2} = \{P_t, R_s, \sigma^2, \sigma_e^2, \beta_d, \beta_r\}$.

C. Loss Function

Different from traditional supervised learning, JBNNet adopts unsupervised learning, which does not need additional labels of Θ and \mathbf{b} . In our design, the loss function is related directly to the objective function Eq. (9a)

$$\text{Loss} = -\frac{1}{K} \sum_{k=1}^K \frac{\phi_k}{(\beta_{d,k}^2 + \beta_{r,k}^2 \|\Theta_k \mathbf{H}_k \mathbf{b}_k\|^2)}, \quad (13)$$

where K is the number of the samples in each batch of the training set. Note that the neural network is trained in the direction of minimizing the loss function, which exactly corresponds to an increasing $\phi / (\beta_d^2 + \beta_r^2 \|\Theta \mathbf{H} \mathbf{b}\|^2)$ in Eq. (9a).

D. Network Training

According to PhaseNet and BeamNet, the entire input data of JBNNet is composed of Data1 and Data2, i.e., $\text{Data} = \{\mathbf{H}_b, \mathbf{G}_r, \mathbf{H}, P_t, R_s, \sigma^2, \sigma_e^2, \beta_d, \beta_r\}$. To train JBNNet adequately, we generated 8×10^5 and 2×10^5 data samples for training and validation randomly, respectively. Furthermore, we set the maximum training epochs as 2000 and the batch size as 1000. The optimizer is set to perform adaptive moment estimation (Adam) with an initial learning rate of 0.01. In order to accelerate the convergence and prevent overfitting, the learning rate decays by a factor of 0.3 when the loss on the validation does not decrease for 15 consecutive epochs, and an early stop with patience 20 is applied. All training

processes are implemented with Python 3.8, Cuda 11.1, and PyTorch 1.9.0 on a PC equipped with a GeForce GTX 1080 Ti GPU.

IV. SIMULATION RESULTS

In this section, we give the simulation results of the proposed DL-based method. The simulations adopted the parameters of $N_t = 4$, $N_r = 2$, $N_e = 2$, the noise variances $\sigma^2 = \sigma_e^2$ are normalized to one, and P_t is defined in dB with respect to σ^2 . The legitimate channels \mathbf{H}_b , \mathbf{H} , and \mathbf{G}_r are assumed to be independent Rayleigh fading, and the large-scale fading factors of the wiretap channels β_d and β_r were generated randomly within $(0, 1)$. All simulation results are averaged over 1000 channel realizations, and we compare the performance of the proposed DL-based approach with the following schemes:

- **Without IRS:** The precoding vector \mathbf{w} is given by the maximum ratio transmission (MRT) strategy, i.e., $\mathbf{w} = \sqrt{P_t} \text{eigvec}_{\lambda_{\max}}(\mathbf{H}_b^H \mathbf{H}_b)$. According to Eq. (8), the secrecy outage probability is calculated as $P_{\text{out}}(R_s) = \Gamma(N_e, \phi/\beta_d^2) / \Gamma(N_e)$, where $\phi = \sigma_e^2 (2^{C_m - R_s} - 1) / P_t$ and $C_m = \log_2(1 + P_t \lambda_{\max} / \sigma^2)$.
- **Random phase:** The phase shift θ_n of each element is generated randomly at $[0, 2\pi]$, and then \mathbf{w} is calculated by the random Θ and Eq. (12).
- **AO algorithm:** The optimization problem Eq. (9) is solved by AO-SDR algorithm and AO-Man algorithm, which are proposed in [10].

Fig. 4 shows the secrecy outage probability in terms of different numbers of IRS elements N_s . As we can observe, the proposed JBNNet and two AO algorithms (AO-SDR and AO-Man) reduce the secrecy outage probability as N_s increases, and there is a small gap between JBNNet and the two AO algorithms. Moreover, the secrecy outage probability of the random phase scheme is slightly better than that without IRS. Note that the performance of the random phase scheme does not change significantly as N_s increases, because both Bob and Eve get similar gains from IRS.

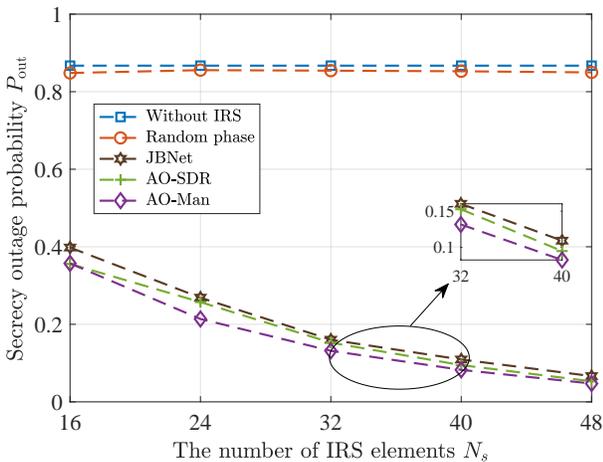


Fig. 4. Secrecy outage probability in terms of N_s when SNR = 10 dB and $R_s = 3.5$ bit/s/Hz.

Fig. 5 illustrates the impact of SNR on the secrecy outage probability. It is interesting to note that the performance

of JBNNet, AO-SDR algorithm, and AO-Man algorithm vary insignificantly in terms of SNR. However, this does not mean that increasing SNR is useless. As SNR increases, slightly increasing secrecy rate can be achieved with a low secrecy outage probability. Moreover, the performance of JBNNet is very close to the two AO algorithms and much better than that without IRS when $N_s = 48$. In particular, there is a lower bound without IRS when $P_t/\sigma_e^2 \rightarrow \infty$, where the proof is given in Appendix.

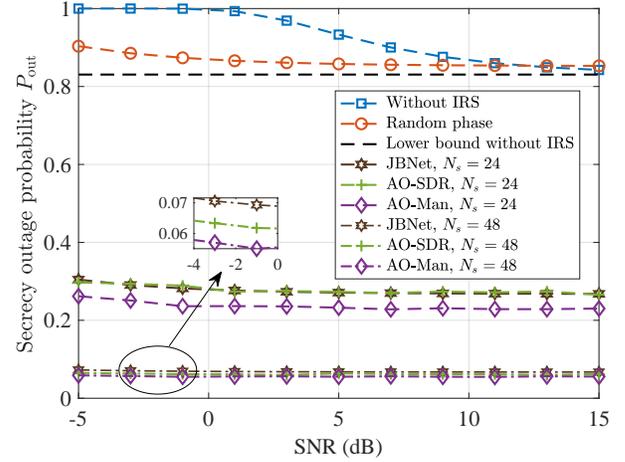


Fig. 5. Secrecy outage probability in terms of SNR when $R_s = 3.5$ bit/s/Hz.

Fig. 6 depicts the impact of the PLS coding rate R_s on the secrecy outage probability. As we can see from the figure, the secrecy outage probability of all schemes rises with an increasing R_s . In this case, some methods can be adopted to improve the PLS coding rate, such as increasing the number of IRS elements N_s , or increasing the numbers of antennas N_t and N_r . For example, Fig. 6 also gives the comparison of simulation curves for $N_s = 24$ and $N_s = 48$.

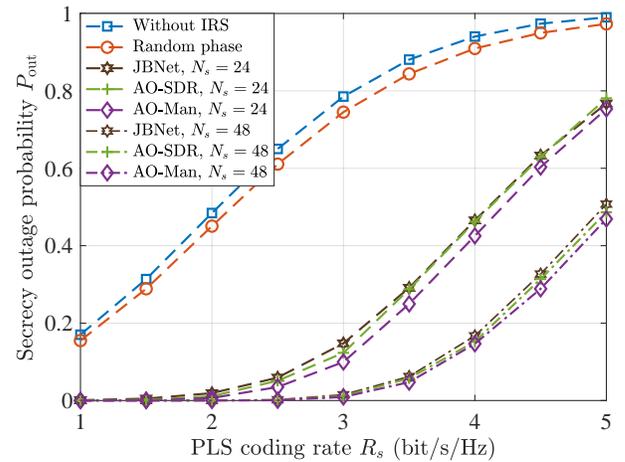


Fig. 6. Secrecy outage probability in terms of R_s when SNR = 10 dB.

Fig. 7 shows the running time of total 20 simulations with different numbers of IRS elements N_s . For a fair comparison, all schemes are executed on the same hardware platform with Intel i5-8259U 2.3GHz CPU. It can be seen that the running

time of the two AO algorithms increases significantly as N_s increases, while the running time of JBNNet remains almost unchanged. Note that $N_s = 16$ has a longer running time than $N_s = 24$, because $N_s = 16$ is the first round of the simulation and the program takes some extra time at startup. According to [10], the computational complexities of AO-SDR algorithm and AO-Man algorithm are $\mathcal{O}(K_{\max}(N_s^{4.5} + N_s^2 N_t + N_t^3))$ and $\mathcal{O}(K_{\max}(N_s^4 + N_s^2 N_t + N_t^3))$, respectively, where K_{\max} is the maximum number of iterations. When the neural network has been trained, the parameters are fixed, so that solving the optimization problem Eq. (9) becomes some simple matrix computation, and the computational complexity of the DL-based approach is approximated as $\mathcal{O}(N_s^2 + N_t N_r N_s)$ [14]. So, the proposed JBNNet has a lower computational complexity.

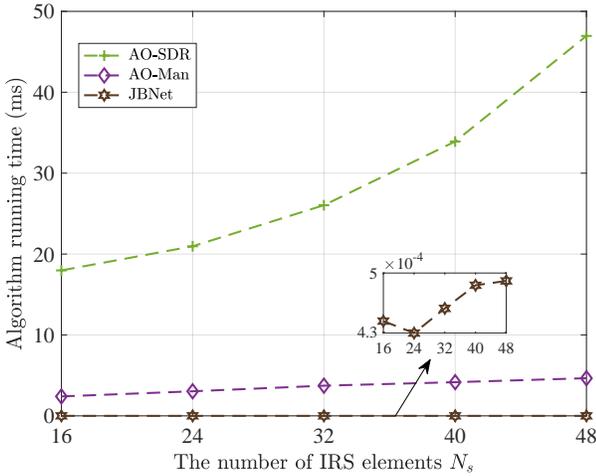


Fig. 7. Running time when SNR = 10 dB and $R_s = 3.5$ bit/s/Hz.

V. CONCLUSION

We derived the expression of secrecy outage probability and proposed a low-complexity DL-based approach for joint beamforming design in an IRS-aided MIMOME system. To reduce the complexity in solving the optimization problem, the data pre-processing method, network structure, and loss function of the neural network have been designed. Simulation results showed that the secrecy performance of the proposed DL-based approach is close to that of the traditional AO algorithms, and the computational complexity is reduced significantly. In the future, we will extend the proposed model to more practical and challenging scenarios, such as IRS with a discrete phase shift, the amplitude and phase coupling, etc.

APPENDIX

In the case of PLS without IRS and $P_t/\sigma_e^2 \rightarrow \infty$, ϕ in Eq. (5a) can be rewritten as

$$\phi = \frac{\sigma_e^2 (2^{C_m - R_s} - 1)}{P_t} \quad (14a)$$

$$= \frac{\sigma_e^2 \|\mathbf{H}_b \mathbf{b}\|^2}{\sigma^2 2^{R_s}} + \frac{\sigma_e^2}{P_t} \left(\frac{1}{2^{R_s}} - 1 \right) \leq \frac{\sigma_e^2 \lambda_{\max}}{\sigma^2 2^{R_s}}, \quad (14b)$$

where λ_{\max} is the largest eigenvalue of \mathbf{H}_b . Therefore, the secrecy outage probability satisfies

$$P_{\text{out}}(R_s) = \frac{1}{\Gamma(N_e)} \Gamma(N_e, \phi/\beta_d^2) \quad (15a)$$

$$\geq \frac{1}{\Gamma(N_e)} \Gamma\left(N_e, \frac{\sigma_e^2 \lambda_{\max}}{\sigma^2 2^{R_s} \beta_d^2}\right). \quad (15b)$$

Note that Eq. (15b) is a lower bound of the secrecy outage probability without IRS as shown in Fig. 5.

REFERENCES

- [1] 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, Jan. 2019.
- [2] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, Firstquarter 2016.
- [3] A. Almohamad, A. M. Tahir, A. Al-Kababji, H. M. Furqan, T. Khattab, M. O. Hasna, and H. Arslan, "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1442–1456, Sep. 2020.
- [4] 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, Sep. 2019.
- [5] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.
- [6] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for secure IRS-assisted multiuser MISO systems," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.
- [7] S. Xu, J. Liu, and Y. Cao, "Intelligent Reflecting Surface Empowered Physical-Layer Security: Signal Cancellation or Jamming?" *IEEE Internet Thing J.*, vol. 9, no. 2, pp. 1265–1275, Jan. 2022.
- [8] H.-M. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Processing Lett.*, vol. 27, pp. 1300–1304, Jul. 2020.
- [9] 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, Sep. 2020.
- [10] Y. Liu, Z. Su, C. Zhang, and H.-H. Chen, "Minimization of Secrecy Outage Probability in Reconfigurable Intelligent Surface-Assisted MIMOME System," *arXiv:2205.00204*, Apr. 2022.
- [11] T. Van Chien, L. T. Tu, S. Chatzinotas, and B. Ottersten, "Coverage probability and ergodic capacity of intelligent reflecting surface-enhanced communication systems," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 69–73, Jan. 2021.
- [12] S. Liu, M. Lei, and M.-J. Zhao, "Deep learning based channel estimation for intelligent reflecting surface aided MISO-OFDM systems," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*. IEEE, 2020, pp. 1–5.
- [13] 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, Mar. 2021.
- [14] A. M. Elbir and S. Coleri, "Federated learning for channel estimation in conventional and RIS-assisted massive MIMO," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4255–4268, Jun. 2022.
- [15] 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, May 2021.
- [16] J. Gao, C. Zhong, X. Chen, H. Lin, and Z. Zhang, "Unsupervised learning for passive beamforming," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1052–1056, May 2020.