Truly Intelligent Reflecting Surface-Aided Secure Communication Using Deep Learning

Yizhuo Song[1], Muhammad R. A. Khandaker[1], Faisal Tariq[2], and Kai-Kit Wong[3]

[1]School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, United Kingdom
[2]James Watt School of Engineering, University of Glasgow, United Kingdom
[3]Department of Electronic and Electrical Engineering, University College London, United Kingdom
Corresponding e-mail: {ys32, m.khandaker}@hw.ac.uk

Abstract—This paper considers machine learning for physical layer security design for communication in a challenging wireless environment. The radio environment is assumed to be programmable with the aid of a meta material-based intelligent reflecting surface (IRS) allowing customisable path loss, multipath fading and interference effects. In particular, the fine-grained reflections from the IRS elements are exploited to create channel advantage for maximizing the secrecy rate at a legitimate receiver. A deep learning (DL) technique has been developed to tune the reflections of the IRS elements in real-time. Simulation results demonstrate that the DL approach yields comparable performance to the conventional approaches while significantly reducing the computational complexity.

I. INTRODUCTION

Security has become a major concern for wireless communication systems with the emergence of high data rate and low latency requirements which, due to inherent vulnerability in their architecture, has limited ability to embed security in the higher layers of communication. Thus physical layer security (PLS) will become an integral part of future communication systems beyond 5G [1]. Despite rapid progress in PLS techniques, the effectiveness of PLS in real scenarios are in doubt due to some major challenges including energy cost incurred in relaying jamming signals and artificial noise as well as computational complexity in beamforming design [2].

With the development of metamaterials technology, intelligent reflecting surface (IRS) has emerged as a promising technique for future wireless communications due its ability to reconfigure the wireless propagation environment by exploiting a large number of low-cost passive reflection units (thus incurs no energy cost for reflecting the signals) which can intelligently adjust the incident signal to improve the system performance [3]. In particular, IRS has great potential in enhancing physical layer security [4] by intelligently tailoring the multipath propagation. By adjusting the phase shift of reflection unit adaptively, the signal reflected by IRS can be enhanced or weakened correspondingly at the receiver, thus strengthening the desired signal and attenuating interference signal [5]. The secrecy rate can be greatly improved by jointly optimizing the beam-forming at the base station and the phase shifts of IRS units. However, generating the optimal phase shifts of IRS elements with acceptable computational complexity remains as the most pressing challenge [3].

In [6], a two phase optimisation approach is adopted in which closed form expression for beamforming design followed by identification of appropriate phase shift in IRS reflector. In [7], secrecy rate maximisation algorithm was developed and a closed form and semi-closed for expressions were obtained for beamforming and phase shift of IRS respectively. In [2], the algorithms of block coordinate descent (BCD) and minorisation maximization (MM) are investigated for small-scale IRSs and large-scale IRSs, respectively. Moreover, the authors of [8] proposed an iterative path-following algorithm. It was shown in [9] that a locally optimal solution can be obtained by using second-order cone programming, which achieves better performance than conventional semidefinite programming (SDP) based algorithms. However, all the above iterative algorithms involve heavily computation-demanding matrix inversions, and their complexity increases exponentially with the number of IRS reflection units. In addition, the alternating optimization algorithms usually require long time to find an apparently optimal solution, which makes the solution less attractive for practical implementation.

Recently, machine learning (ML) and deep learning (DL) techniques have attracted huge interest for addressing wireless communication problems due to their ability to improve system performance and reduce the computational cost [10]. DL exploits the deep neural network (DNN), which completes the training process offline and the trained DNN only includes simple linear and non-linear transformation units. Although the name suggests that IRSs are intelligent, existing works with IRS-assisted communications do not implement any systematic learning approach. While ML/DL has been widely investigated in wireless communications, there is hardly any work that exploits DNN for IRS and to the best of the authors' knowledge, there is no such work that exploits ML for IRS-aided PLS. In this work, DL is applied to design the optimal reflection coefficients of the IRS elements for secure communication. The main contributions of the paper include: (i) a deep learning solution for designing truly intelligent reflecting surface for the secrecy rate maximization problem, and (ii) rigorous performance analysis and comparison with existing optimisation algorithms. The proposed DNN approach provides us real-time IRS reflections thus addressing the implementation challenges of iterative IRS design.

Notations– In this paper, bold lower-case and upper-case

letters represent vectors and matrices, respectively, $\mathbb{C}^{M \times N}$ denotes the space of $M \times N$ complex-valued matrices, $\mathbf{H}^T$ stands for the transpose of matrix $\mathbf{H}$, while $|\cdot|$ and $\|\cdot\|$ denote absolute value and the Euclidean norm, respectively. $\mathrm{diag}(\mathbf{g})$ means a $N \times N$ diagonal matrix with $\mathbf{g} \triangleq [g_1,\ g_2,\ \cdots,\ g_N]$ as the main diagonal and $[\cdot]^+$ denotes $\max(0, x)$.

II. SYSTEM MODEL AND PROBLEM FORMULATION

Fig. 1 illustrates the IRS-assisted wireless system model of interest, which consists of an access point (AP), one legitimate user, one eavesdropper and an IRS. The AP transmits signals to the user in the presence of the eavesdropper. We assume that the AP is equipped with M antennas, while the user and the eavesdropper each with a single antenna. The IRS is deployed in the network between the AP and the user to aid secure data transmission to the user, with N reconfigurable reflecting units programmed by an IRS controller.
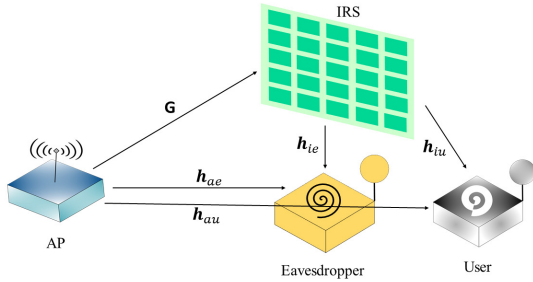

Figure 1. An IRS-assisted wireless communication system.

The channel coefficients between AP and IRS, AP and user, AP and eavesdropper, IRS and user and IRS and eavesdropper are denoted by $\mathbf{G} \in \mathbb{C}^{N \times M}$, $\mathbf{h}_{\mathrm{au}} \in \mathbb{C}^{1 \times M}$, $\mathbf{h}_{\mathrm{ae}} \in \mathbb{C}^{1 \times M}$, $\mathbf{h}_{\mathrm{iu}} \in \mathbb{C}^{1 \times N}$, $\mathbf{h}_{\mathrm{ie}} \in \mathbb{C}^{1 \times N}$, respectively. Consider that all channels in the system experience quasi-static flat-fading and the global channel state information (CSI) is perfectly known at both AP and the IRS controller. n_{U} and n_{E} denote the additive Gaussian noises at the user and the eavesdropper with zero mean and variance σ_{u}^2 and σ_{e}^2, respectively.

The AP transmits confidential message $\mathbf{s}$ with mean value 0 and unit variance to the user through beamforming. The beamforming vector is denoted by $\mathbf{f} \in \mathbb{C}^{M \times 1}$ satisfying the constraint

$$\|\mathbf{f}\|^2 \leq P_{\mathrm{t}}, \tag{1}$$

where P_{t} is the maximum transmit power budget at AP.

The vector of the reflection coefficients by the IRS units is denoted by $\boldsymbol{\varphi} \triangleq [\varphi_1, \varphi_2, \ldots, \varphi_N]^T$, where $\varphi_n = \beta_n e^{j\theta_n}$. β_n and θ_n stand for the amplitude and the phase shift of the nth reflection coefficient, respectively. For simplicity, we assume ideal hardware configuration for the IRS, meaning that the elements are designed for maximum reflection [5], i.e., $\beta_n = 1$ and $\theta_n \in [0, 2\pi)$, for $n = 1, \ldots, N$.

The achievable rates at the user and the eavesdropper are, respectively, given by [11]

$$R_{\mathrm{u}} = \log_2\left(1 + \frac{|(\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{au}})\,\mathbf{f}|^2}{\sigma_{\mathrm{u}}^2}\right), \tag{2}$$

$$R_{\mathrm{e}} = \log_2\left(1 + \frac{|(\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{ae}})\,\mathbf{f}|^2}{\sigma_{\mathrm{e}}^2}\right), \tag{3}$$

where $\boldsymbol{\Phi} \triangleq \mathrm{diag}(\boldsymbol{\varphi})$. With R_{u} and R_{e}, the secrecy rate from AP to the user is given by [11]

$$R_{\mathrm{sec}} = [R_{\mathrm{u}} - R_{\mathrm{e}}]^+. \tag{4}$$

The operator $[\cdot]^+$ will be omitted in the following expressions since the optimal secrecy rate must be nonnegative.

Our objective is to find the optimal phase-shifts of reflectors in the IRS and corresponding beamforming vector for maximizing the secrecy rate (4). Thus, the related optimization problem is formulated as

$$\max_{\mathbf{f},\boldsymbol{\varphi}} \quad \log_2\left(1 + \frac{|(\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{au}})\,\mathbf{f}|^2}{\sigma_{\mathrm{u}}^2}\right)$$
$$- \log_2\left(1 + \frac{|(\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{ae}})\,\mathbf{f}|^2}{\sigma_{\mathrm{e}}^2}\right), \tag{5a}$$

$$\mathrm{s.t.} \quad \|\mathbf{f}\|^2 \leq P_{\mathrm{t}}, \tag{5b}$$

$$|\varphi_n| = 1, \forall n \tag{5c}$$

Constraint (5b) limits the transmission power of the beamforming vector, whereas (5c) guarantees maximum reflection. The objective (5a) is a non-convex function with regard to $\mathbf{f}$ and $\boldsymbol{\varphi}$. It is worth noting that the global optimal solution of non-convex optimization problems with unit modulus constraints is usually hard to find. Therefore, [5] proposed an iterative optimization method.

III. PROPOSED SOLUTION

In this section, we present both the traditional convex optimization based algorithm and the proposed deep learning method to find the optimal phase shifts of IRS units as well as the transmit beamforming vector.

A. Conventional Approach

The basic process of alternating optimization is to find the optimal solution for one variable while keeping the others fixed. In this case, we firstly optimize $\mathbf{f}$ assuming that $\boldsymbol{\varphi}$ is given and then optimize $\boldsymbol{\varphi}$ with given $\mathbf{f}$ iteratively.

1) Optimizing $\mathbf{f}$ with given $\boldsymbol{\varphi}$: The optimization problem (5) with given $\boldsymbol{\varphi}$ reduces to

$$\max_{\mathbf{f}} \quad \frac{\frac{1}{\sigma_u^2}|(\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{au}})\,\mathbf{f}|^2 + 1}{\frac{1}{\sigma_e^2}|(\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{ae}})\,\mathbf{f}|^2 + 1} \tag{9a}$$

$$\mathrm{s.t.} \quad \|\mathbf{f}\|^2 \leq P_{\mathrm{t}}. \tag{9b}$$

Introducing matrix variables $\mathbf{A}$ and $\mathbf{B}$ defined as

$$\mathbf{A} = \frac{1}{\sigma_{\mathrm{u}}^2} \left(\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{au}}\right)^H \left(\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{au}}\right), \quad (10)$$

$$\mathbf{B} = \frac{1}{\sigma_{\mathrm{e}}^2} \left(\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{ae}}\right)^H \left(\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{ae}}\right), \quad (11)$$

the optimization problem (9) can be rewritten as

$$\max_{\mathbf{f}} \quad \frac{\mathbf{f}^H \mathbf{A}\mathbf{f} + 1}{\mathbf{f}^H \mathbf{B}\mathbf{f} + 1} \tag{12a}$$

$$\text{s.t.} \quad \mathbf{f}^H \mathbf{f} \leq P_t. \tag{12b}$$

Assuming that $\mathbf{e}_{\max}$ is the normalized eigenvector corresponding to the maximum eigenvalue of matrix $\mathbf{C}$ defined as

$$\mathbf{C} = \left(\mathbf{B} + \frac{1}{P_t}\mathbf{I}\right)^{-1} \left(\mathbf{A} + \frac{1}{P_t}\mathbf{I}\right), \tag{13}$$

where $\mathbf{I}$ is an identity matrix, the optimal solution for $\mathbf{f}$ is given by [11]

$$\mathbf{f}_{\mathrm{opt}} = \sqrt{P_t}\mathbf{e}_{\max}. \tag{14}$$

2) Optimizing $\boldsymbol{\varphi}$ with given $\mathbf{f}$: From (5), the optimization problem with given $\mathbf{f}$ can be expressed as:

$$\max_{\boldsymbol{\varphi}} \quad \frac{\frac{1}{\sigma_u^2}\left|\left(\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{au}}\right)\mathbf{f}\right|^2 + 1}{\frac{1}{\sigma_e^2}\left|\left(\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} + \mathbf{h}_{\mathrm{ae}}\right)\mathbf{f}\right|^2 + 1} \tag{15a}$$

$$\text{s.t.} \quad |\varphi_n| = 1, \forall n. \tag{15b}$$

It is known that

$$\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} = \boldsymbol{\varphi}^T \operatorname{diag}\left(\mathbf{h}_{\mathrm{iu}}\right)\mathbf{G}, \tag{16}$$

$$\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} = \boldsymbol{\varphi}^T \operatorname{diag}\left(\mathbf{h}_{\mathrm{ie}}\right)\mathbf{G}. \tag{17}$$

Let $\operatorname{diag}\left(\mathbf{h}_{\mathrm{iu}}\right)\mathbf{G} = \mathbf{K}_{\mathrm{u}}$, and $\operatorname{diag}\left(\mathbf{h}_{\mathrm{ie}}\right)\mathbf{G} = \mathbf{K}_{\mathrm{e}}$, equations above can be rewritten as

$$\mathbf{h}_{\mathrm{iu}}\boldsymbol{\Phi}\mathbf{G} = \boldsymbol{\varphi}^T \mathbf{K}_{\mathrm{u}}, \tag{18}$$

$$\mathbf{h}_{\mathrm{ie}}\boldsymbol{\Phi}\mathbf{G} = \boldsymbol{\varphi}^T \mathbf{K}_{\mathrm{e}}, \tag{19}$$

Defining $\mathbf{f}^*\mathbf{f}^T \triangleq \mathbf{F}$, problem (15) is equivalent to

$$\max_{\boldsymbol{\varphi}} \quad f(\boldsymbol{\varphi}) \tag{20a}$$

$$\text{s.t.} \quad |\varphi_n| = 1, \forall n, \tag{20b}$$

where $f(\boldsymbol{\varphi})$ is defined in (21) (at the bottom of the page). Let us now define the variables ν_{U}, ν_{E}, $\boldsymbol{\Gamma}_{\mathrm{U}}$ and $\boldsymbol{\Gamma}_{\mathrm{E}}$ as

$$\nu_{\mathrm{U}} = \frac{\mathbf{h}_{\mathrm{au}}^T \mathbf{F}\mathbf{h}_{\mathrm{au}}^*}{\sigma_{\mathrm{u}}^2}, \quad \nu_{\mathrm{E}} = \frac{\mathbf{h}_{\mathrm{ae}}^T \mathbf{F}\mathbf{h}_{\mathrm{ae}}^*}{\sigma_{\mathrm{e}}^2}, \tag{22}$$

$$\boldsymbol{\Gamma}_{\mathrm{U}} = \frac{1}{\sigma_u^2} \begin{bmatrix} \mathbf{K}_{\mathrm{u}}^T \mathbf{F}\mathbf{K}_{\mathrm{u}}^* & \mathbf{K}_{\mathrm{u}}^T \mathbf{F}\mathbf{h}_{\mathrm{au}}^* \\ \mathbf{h}_{\mathrm{au}}^T \mathbf{F}\mathbf{K}_{\mathrm{u}}^* & 0 \end{bmatrix}, \tag{23}$$

$$\boldsymbol{\Gamma}_{\mathrm{E}} = \frac{1}{\sigma_e^2} \begin{bmatrix} \mathbf{K}_{\mathrm{e}}^T \mathbf{F}\mathbf{K}_{\mathrm{e}}^T & \mathbf{K}_{\mathrm{e}}^T \mathbf{F}\mathbf{h}_{\mathrm{ae}}^* \\ \mathbf{h}_{\mathrm{ae}}^T \mathbf{F}\mathbf{K}_{\mathrm{e}}^* & 0 \end{bmatrix}. \tag{24}$$

By substituting (22) - (24), (20) can be simplified as the following equivalent problem

$$\max_{\mathbf{v}} \quad \frac{\mathbf{v}^H \boldsymbol{\Gamma}_{\mathrm{U}}\mathbf{v} + \nu_{\mathrm{U}} + 1}{\mathbf{v}^H \boldsymbol{\Gamma}_{\mathrm{E}}\mathbf{v} + \nu_{\mathrm{E}} + 1}, \tag{25a}$$

$$\text{s.t.} \quad \mathbf{v}^H \mathbf{U}_n \mathbf{v} = 1, \forall n, \tag{25b}$$

where $\mathbf{v} = \left[\boldsymbol{\varphi}^T, 1\right]^T$ and $\mathbf{U}$ is a three dimensional matrix, with elements of $\mathbf{U}_n$ given by

$$[\mathbf{U}_n]_{i,j} = \begin{cases} 1 & i = j = n \\ 0 & \text{otherwise} \end{cases}. \tag{26}$$

Note that problem (25) is still non-convex. Defining $\mathbf{V} \triangleq \mathbf{v}\mathbf{v}^H$ requires that $\operatorname{rank}(\mathbf{V}) \leq 1$. Ignoring this rank constraint, the semidefinite relaxation technique can be applied to address the non-convex problem [12]. Thus the optimization problem can be reformulated as

$$\max_{\mathbf{V} \succeq \mathbf{0}} \quad \frac{\operatorname{tr}\left(\boldsymbol{\Gamma}_{\mathrm{U}}\mathbf{V}\right) + \nu_{\mathrm{U}} + 1}{\operatorname{tr}\left(\boldsymbol{\Gamma}_{\mathrm{E}}\mathbf{V}\right) + \nu_{\mathrm{E}} + 1} \tag{27}$$

$$\text{s.t.} \quad \operatorname{tr}\left(\mathbf{U}_n \mathbf{V}\right) = 1, \forall n. \tag{28}$$

Then, we can apply Charnes-Cooper transformation [13] to transform it into a convex semidefinite programming (SDP) problem by defining $\mu = 1/\left[\operatorname{tr}\left(\boldsymbol{\Gamma}_{\mathrm{E}}\mathbf{V}\right) + \nu_{\mathrm{E}} + 1\right]$. The equivalent optimization problem is given by

$$\max_{\mu \geq 0, \mathbf{Z} \succeq 0} \quad \operatorname{tr}\left(\boldsymbol{\Gamma}_{\mathrm{U}}\mathbf{Z}\right) + \mu\left(\nu_{\mathrm{U}} + 1\right) \tag{29}$$

$$\text{s.t.} \quad \operatorname{tr}\left(\boldsymbol{\Gamma}_{\mathrm{E}}\mathbf{Z}\right) + \mu\left(\nu_{\mathrm{E}} + 1\right) = 1 \tag{30}$$

$$\operatorname{tr}\left(\mathbf{U}_n \mathbf{Z}\right) = \mu, \forall n, \tag{31}$$

where $\mathbf{Z} = \mu\mathbf{V}$. The problem is now convex and can be efficiently solved by interior-point methods (e.g., CVX) [14]. Gaussian randomization method can be used to cope with the rank constraint and obtain an approximate optimal solution.

B. Proposed Deep Learning Algorithm

While deep learning has played an important role in many applications in recent years, there are a number of challenges facing the design of a DL method for the secure communication scenario under consideration:

- It is difficult to model the input-output relationship of DNN due to the large number of parameters involved in the calculation of secrecy rate.
- Acquisition of training data set, in particular, supervised learning not only needs a lot of channel samples, but also the target outputs mapped with those samples.
- Excepting the transmit power and noise power, all the other parameters are inherently complex; nevertheless, most of the deep neural network technologies are based on real-valued operation and representation.

$$f(\boldsymbol{\varphi}) \triangleq \frac{\frac{1}{\sigma_u^2}\left(\boldsymbol{\varphi}^H \mathbf{K}_{\mathrm{u}}^* \mathbf{F}\mathbf{K}_{\mathrm{u}}^T \boldsymbol{\varphi} + \mathbf{h}_{\mathrm{au}}^* \mathbf{F}\mathbf{K}_{\mathrm{u}}^T \boldsymbol{\varphi} + \boldsymbol{\varphi}^H \mathbf{K}_{\mathrm{u}}^* \mathbf{F}\mathbf{h}_{\mathrm{au}}^T + \mathbf{h}_{\mathrm{au}}^* \mathbf{F}\mathbf{h}_{\mathrm{au}}^T\right) + 1}{\frac{1}{\sigma_e^2}\left(\boldsymbol{\varphi}^H \mathbf{K}_{\mathrm{e}}^* \mathbf{F}\mathbf{K}_{\mathrm{e}}^T \boldsymbol{\varphi} + \mathbf{h}_{\mathrm{ae}}^* \mathbf{F}\mathbf{K}_{\mathrm{e}}^T \boldsymbol{\varphi} + \boldsymbol{\varphi}^H \mathbf{K}_{\mathrm{e}}^* \mathbf{F}\mathbf{h}_{\mathrm{ae}}^T + \mathbf{h}_{\mathrm{ae}}^* \mathbf{F}\mathbf{h}_{\mathrm{ae}}^T\right) + 1} \tag{21}$$

Deep neural network (DNN) is a kind of mathematical framework that realizes the mapping from input to output through a series of data transformation layers. Supervised learning and unsupervised learning are widely used algorithms in machine learning. In this paper, we use supervised learning to train the DNN.

The proposed DNN framework used to obtain the optimal phase shifts of IRS reflection units is shown in Fig. 2, and the beamforming vector $\mathbf{f}$ is computed according to (14). For handling multiple inputs, we use Keras functional API model in this work because of its flexibility in dealing with multi-inputs problem. The proposed neural network includes three modules: input processing module, phase shift calculation module and output processing module.

Figure 2. Proposed DNN framework.

The input processing module has several parallel sets of input lines to take channel coefficients as inputs. The complex channel coefficients are divided into real part and imaginary part since the neural network framework can only perform real-valued operations. After each set of inputs passing through batch normalization layer and flatten layer in turn, they will be concatenated into one set of one-dimensional data that is taken as the input to the phase shift calculation module. In the input processing module, each layer is composed of a fixed number of neurons which is determined by the number of channel coefficients.

The phase shift calculation module includes several dense layers and batch normalization layers. The number of neurons in each dense layer is adjustable. The function of all these dense layers is to establish the logical relationship between the channel coefficients and the phase shifts of IRS units.

The output processing module is composed of one dense layer and two Lambda layers. The dense layer outputs the phase shifts of the IRS units in radians. In the first Lambda layer, the Euler formula is used to convert the phase shift θ_n into complex form φ_n, which also satisfies the constrains defined in (5c), $|\varphi_n| = 1$; the second Lambda layer takes all the channel coefficients, transmit power and φ as inputs to obtain the secrecy rate.

Learning Policy: Fig. 3 shows how DNN based on supervised learning works. The input X will go through several data transformation layers, and the predicted output $\tilde{Y}$ will be generated. The loss function is generated by comparing the output value $\tilde{Y}$ and actual target value Y. Then, the optimizer

will iteratively optimize the weight values in each layer based on the loss value. For supervised learning, there are two dense layers and one batch-normalization layer. We take Adam as the optimizer and choose mean squared error (MSE) as the loss function, given by

$$MSE = \frac{1}{n} \sum_{i=1}^{n} (\tilde{y}_i - t_i)^2 \qquad (32)$$

where $\tilde{y}_i$ is the output of the neural network, t_i is the corresponding training targets, i is the index of data. The channel coefficients and target values are generated by computer simulation using the alternating optimization algorithm in Section III-A.
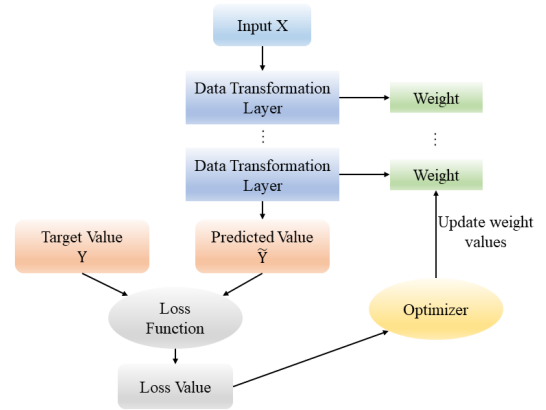

Figure 3. Supervised learning algorithm.

IV. NUMERICAL SIMULATIONS

In this section, we perform numerical simulations to demonstrate the effectiveness of the proposed supervised learning based secrecy rate maximization approach for the proposed scenario of interest. We first demonstrate the learning accuracy of the proposed DL method to determine the optimal hyper parameters for the proposed wiretapping scenario. We then compare the performance of the trained DNN against the alternating optimization algorithm in [5] and two other benchmark schemes as defined below:

- **Optimal AP without IRS**: The optimal beamforming vector $\mathbf{f}$ is computed according to (14) with $\varphi = 0$.
- **AP MEV with IRS**: Firstly, we set beamforming vector $\mathbf{f}$ same as the 'Optimal AP without IRS' scheme, then obtain optimal φ by using the method in section III-A2.
- **Alternating Optimization**: Based on the method in Section III-A.
- **Supervised Learning**: Get training data from the simulation results of alternating optimization. The trained DNN can output reflection phase shifts by taking channel coefficients and transmit power as inputs.

For a fair comparison, we choose parameter settings as in [5] wherever applicable. Accordingly, we set $M = 4$ and $N = 25$, the noise variance at both the eavesdropper and the user are
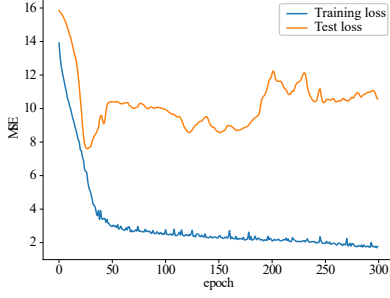
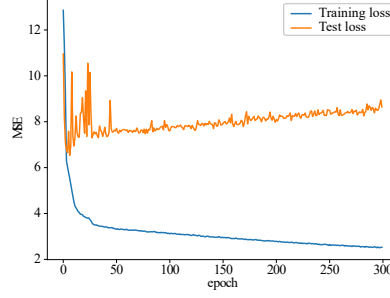Figure 4. Model loss with 100 training sets.
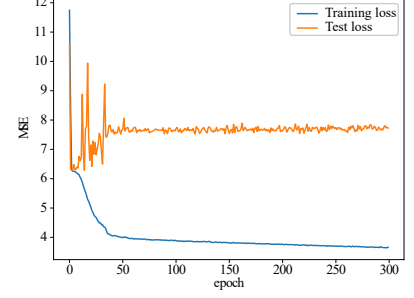

Figure 5. Model loss with 2700 training sets.

Figure 6. Model loss with 9000 training sets.

set to $\sigma_{\mathrm{u}}^2 = \sigma_{\mathrm{e}}^2 = -80$dBm, unless otherwise specified. The AP, eavesdropper and the user are located on the same horizontal line. The distance between AP and eavesdropper, AP and the user and eavesdropper and the user are denoted by d_{ae}, d_{au} and d_{eu}, respectively, and set as $d_{\mathrm{ae}} = 145$m and $d_{\mathrm{au}} = 150$m, thus $d_{\mathrm{eu}} = d_{\mathrm{au}} - d_{\mathrm{ae}} = 5$m. The IRS-eavesdropper, IRS-user and AP-IRS link distances are set as $d_{\mathrm{ie}} = 5$m, $d_{\mathrm{iu}} = \sqrt{\left(d_{\mathrm{ie}}^2 + d_{\mathrm{eu}}^2\right)}$ and $d_{\mathrm{ai}} = \sqrt{\left(d_{\mathrm{ae}}^2 + d_{\mathrm{ie}}^2\right)}$, respectively. Since the AP, eavesdropper and user lie on the same horizontal line, the channels from AP to the user $\mathbf{h}_{\mathrm{au}}$ and to the eavesdropper $\mathbf{h}_{\mathrm{ae}}$ are assumed to experience spatially correlated Rician fading, with Rician factors $K_{\mathrm{au}} = K_{\mathrm{ae}} = 1$ and the spatial correlation matrix $\mathbf{R}$, which is given by $[\mathbf{R}]_{i,j} = r$ where $r = 0.95$. The channel coefficients $\mathbf{h}_{\mathrm{au}}$ and $\mathbf{h}_{\mathrm{ae}}$ can be obtained as $\mathbf{h}_{\mathrm{au}} = \sqrt{\eta_0 \left(d_0/d_{\mathrm{au}}\right)^{\psi_{\mathrm{au}}}} \mathbf{g}_{\mathrm{au}}$, and $\mathbf{h}_{\mathrm{ae}} = \sqrt{\eta_0 \left(d_0/d_{\mathrm{ae}}\right)^{\psi_{\mathrm{ae}}}} \mathbf{g}_{\mathrm{ae}}$, where $\eta_0 = -30$dB is the path loss with reference distance $d_0 = 1$m, and $\psi_{\mathrm{au}} = \psi_{\mathrm{ae}} = 3$ are the corresponding path loss exponents. The other channels $\mathbf{G}$, $\mathbf{h}_{\mathrm{iu}}$ and $\mathbf{h}_{\mathrm{ie}}$ are independent Rician fading with corresponding path loss $\psi_{\mathrm{ai}} = 2.2$ and $\psi_{\mathrm{iu}} = \psi_{\mathrm{ie}} = 3$.

A. Simulation Setup for the Deep Learning Model

For the proposed supervised learning approach, a total of $10,000$ data samples have been generated, of which 90% is used for training and the remaining 10% for testing the performance, unless otherwise specified. The proposed DNN was trained in a GPU server with the following configuration:
- Intel Xeon Scalable Silver 4110 8Core 2.1GHz processor,
- 128 GB DDR4 2666 MHz ECC registered memory.

B. Overfitting Problem

Overfitting is a common problem in deep learning. It refers to the state that only the training data can be well-fitted, but not the data that is not included for training. For supervised learning in particular, over-fitting problem is critical, so we first focus on over-fitting phenomenon in supervised learning and its solutions.

C. Methods to Suppress Overfitting

1) Increasing Training Data: In Fig. 4, we used 100 training sets and 100 test sets. To further improve the generalization ability of DNN, the number of training sets is increased from 100 to 2700 in Fig. 5 and it is tested on 300 data sets. From Fig. 5, it is observed that the training loss curve is smoother and the test loss is slightly lower compared with Fig. 4.

Even though Fig. 5 has some improvement compared with Fig. 4, it still has a large gap between training loss and test loss. Thus, the number of training sets is further increased to 9000. After training it on 9000 data sets and testing it on 1000 data sets, the results are illustrated in Fig. 6. It can be observed that the value of test loss decreased to below 8 and no longer showed an upward trend.

2) Decreasing Hidden Layers: It is known that the DNN architecture in Fig. 4, Fig. 5 and Fig. 6 has 4 hidden layers. After reducing the number of hidden layers from 4 to 3 and 2, the model loss is shown as Fig. 7 and Fig. 8, respectively. It can be observed from Fig. 8 that 2 hidden layers greatly reduce the model loss, thereby effectively suppressing overfitting.

3) Early Stopping: It can be observed that the overfitting in Fig. 8 is slowly increasing with epoch. However, Fig. 9 illustrates the model loss with early stopping at 110 epochs. We can observe from Fig. 9 that the test loss is no longer increasing with epochs.

A comparison between the initial model loss in Fig. 4 and the final model loss in Fig. 9 reveals that overfitting can be effectively suppressed by increasing training data set, decreasing the number of hidden layers stopping early as appropriate.

D. Secrecy Rate Result

Finally, we illustrate the achievable secrecy rate performance of the conventional and supervised learning approaches. All of the simulation results are averaged over 1000 channel realizations.

Fig. 10 and Fig. 11 illustrate the PDF and the CDF, respectively, of the secrecy rates obtained by the schemes. The simulation results are obtained from $1,000$ samples with P_t equal to 20dBm. Again, the alternating optimization yields the best performance and the performance of the 'AP MEV with IRS' is slightly worse than this method. Both the 'Optimal AP without IRS' and 'Supervised Learning' are also comparable. The marginal performance loss is due to insufficient training data. Theoretically, even if supervised learning can
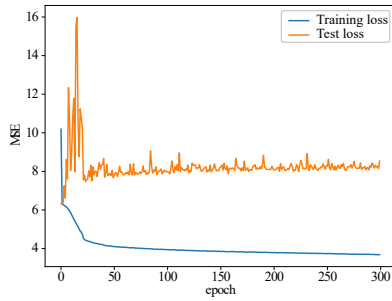
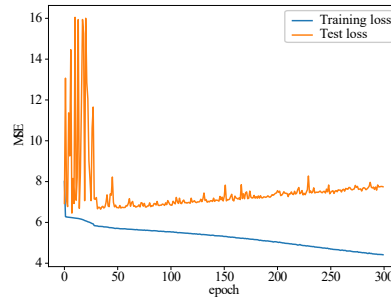Figure 7. Model loss with 3 hidden layers.

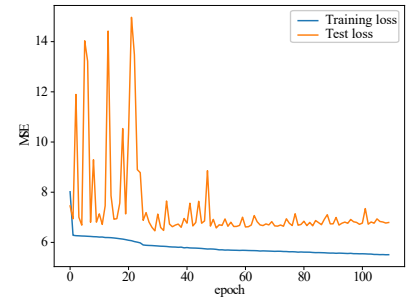Figure 8. Model loss with 2 hidden layers.

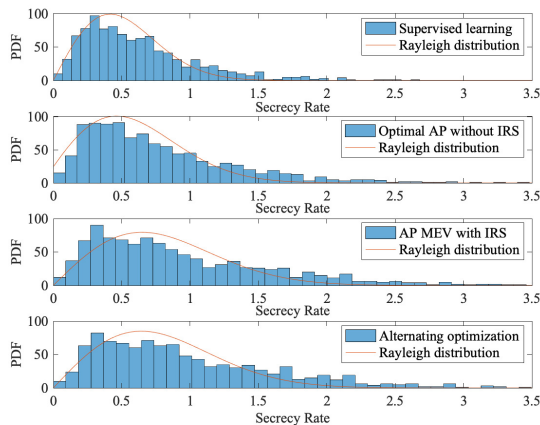Figure 9. Model loss with early stopping.

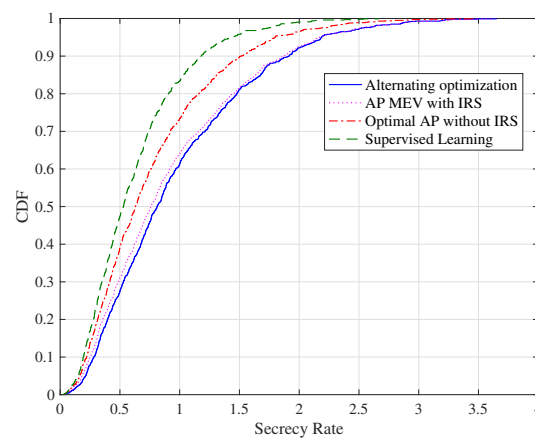Figure 10. PDF of the achievable secrecy rate.

Figure 11. CDF of the achievable secrecy rate.

obtain sufficient training data and time, its performance can not surpass the alternating optimization algorithm. This is because the result of the 'alternating optimization' scheme is the benchmark for the supervised learning scheme. Although the conventional optimization algorithms show higher secrecy rates, these schemes are computationally expensive in practice.

V. Conclusion

The IRS is a cost-effective technology consisting of a large number of low-cost reflection units, which can greatly improve the performance of the physical layer without incurring the high cost and power consumption required for multiple antennas. We have introduced a truly intelligent reflecting surface aided secure communication system. Simulation results demonstrate that the proposed supervised learning approach can achieve comparable performance with the alternating optimization algorithm, and is simpler to implement, shorter in operation time and offers greater flexibility.

References

[1] F. Tariq, M. R. A. Khandaker, K. K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[3] Q. Wu and R. Zhang, "Beamforming optimization for intelligent reflecting surface with discrete phase shifts," in *Proc. IEEE ICASSP*, 2019.

[2] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," *arXiv preprint arXiv:1904.09573*, 2019.

[4] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.*, to appear, 2020.

[5] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, pp. 1410–1414, 2019.

[6] B. Feng, Y. Wu, and M. Zheng, "Secure transmission strategy for intelligent reflecting surface enhanced wireless system," in *Int. Conf. Wireless Commun. Signal Process.*, 2019.

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

[8] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[9] Y. Li, M. Jiang, Q. Zhang, and J. Qin, "Joint beamforming design in multi-cluster MISO NOMA intelligent reflecting surface-aided downlink communication networks," *arXiv preprint arXiv:1909.06972*, 2019.

[10] J. Gao, M. R. A. Khandaker, F. Tariq, K.-K. Wong, and R. T. Khan, "Deep neural network based resource allocation for V2X communications," in *Proc. IEEE 90th Vehicular Technol. Conf. (VTC-Fall)*, 2019.

[11] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME channel," *IEEE Trans. Inf. Theory*, 2008.

[12] M. R. A. Khandaker and K.-K. Wong, "SWIPT in MISO multicasting systems," *IEEE Wireless Commun. Letters*, vol. 3, pp. 277–280, 2014.

[13] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Research*, vol. 9, pp. 181–186, 1962.

[14] I. Pólik and T. Terlaky, "Interior-point methods for nonlinear optimization," in *Nonlinear Optimization*. Springer, 2010, pp. 215–276.