

Received 7 February 2025, accepted 6 April 2025, date of publication 11 April 2025, date of current version 18 April 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3559981

RESEARCH ARTICLE

Enhancing Secure Energy Efficiency of SWIPT IoT Network Considering IRS and Artificial-Noise: A Deep Learning Approach

KIMCHHEANG CHHEA¹, AND JUNG-RYUN LEE^{1,2}, (Senior Member, IEEE)

¹Department of Intelligent Energy and Industry, Chung-Ang University, Seoul 156-756, South Korea

²School of Electronics and Electrical Engineering, Chung-Ang University, Seoul 156-756, South Korea

Corresponding author: Jung-Ryun Lee (jrlee@cau.ac.kr)

This work was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation) under Grant IITP-RS-2024-00436248 (50%); and in part by Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government (MOTIE) under Grant RS-2021-KP002504, Convergence Graduate School of Intelligent Energy and Industry.

ABSTRACT Internet of things (IoT) networks connect sensing devices to the Internet for tasks like tracking, monitoring, and data analysis. However, the large data generated, especially in resource-heavy services, challenges energy efficiency (EE) and security. The use of intelligent reflecting surfaces (IRS) in the physical layer security of IoT devices shows promise in improving secrecy performance and EE. This paper addresses IRS and AN-aided secure communication against eavesdroppers, where eavesdroppers are IoT devices equipped with simultaneous wireless information and power transfer (SWIPT) using power splitting policy. Our goal is to maximize secure EE, where the secure EE is defined as the secrecy rate over the power consumption of the user. We aim to jointly optimize phase-shift of IRS, transmit power of jammer and user, to maximize the objective function while ensuring that the secrecy rate is greater than the predefined threshold while allowing the eavesdroppers to harvest energy using SWIPT. We first formulate a joint optimization model of IRS and AN aided secure communication, which is a non-convex optimization problem with linear and non-linear constraints. To solve this problem, we propose a deep neural network (DNN) algorithm that utilizes a loss function derived from Lagrange duality function. The simulation results show that the proposed DNN achieves near-global optimal solutions. In addition, the results also prove the effectiveness of implementing IRS to enhance the secure EE of the user.

INDEX TERMS Internet of Things, IRS, artificial noise, SWIPT, secure energy efficiency, deep learning.

I. INTRODUCTION

With the emergence of the next-generation communications and advancements in the Internet of Things (IoT), wirelessly-connected smart devices and intelligent sensors are finding increasing applications. IoT networks consist of information sensing devices that connect to the Internet in a smart way to communicate and exchange data. IoT networks can perform tasks such as locating, tracking, environment monitoring, surveillance, identifying, and analyzing sensing information for making decisions [1]. However, such tasks produce

large amounts of data in various computationally intensive services and applications, resulting in new challenges related to energy efficiency (EE) and security issues [2]. Eavesdropping attacks present a formidable challenge to the privacy aspects of Industrial IoT infrastructure and operations [3]. As a solution, pre-shared key technique is proposed to ensure message confidentiality, with decryption rendered impossible in the absence of the key. Nonetheless, advanced cryptography techniques require intensive computation and substantial power, posing challenges for resource-constrained IoT sensors unable to handle such demands. This leads to inefficient utilization of energy and processing time [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Ting Yang¹.

Physical layer security (PLS), unlike cryptography, uses the dynamics of fading channels for achieving the highest secrecy capability without the use of encryption keys [5]. Because wireless communication is broadcast in nature, it is highly vulnerable to security threats such as wiretapping. To address this issue, PLS with beamforming and cooperative cognitive radio techniques to reduce the leak of desired signal to malicious nodes has been widely studied [6]. Artificial noise (AN) initially proposed in [7], is an effective technique in which interfering signals are injected for reducing eavesdropper's signal strength while maintaining the intended receiver's signal strength.

Intelligent reflecting surface (IRS) has emerged as a novel and popular paradigm to realize smart and controllable wireless environment systems [8]. An IRS comprises many low-cost passive reflecting elements fixed in meta-surfaces that can be implemented in different areas such as building exteriors and interior walls [9]. The IRS is connected to a controller that controls the phase of each specific reflecting element. The IRS controller is connected to external devices such as a base station or an access point (AP). The IRS does not require transmission via radio frequency links because it acts as a surface for incident wireless signals. Therefore, it has very low energy consumption and, in turn, enhanced the EE [10]. Additionally, IRS phase-shifting can improve the signal of the intended receiver and reduce that of the unintended receiver's, thus improving the security of the intended devices. By installing an IRS in a wireless environment and optimizing its reflection, the signals transmitted and received at both the transmitter's and receiver's end can be optimally reconfigured to achieve the highest system performance [2]. This could critically enable addressing the impairment and interference problems, and thereby realizes new improvements in wireless communication capacity, EE, and PLS.

AN-aided secure communication systems add AN to the transmitted signal to confuse eavesdroppers. However, this AN can degrade the quality of the intended signal received by the legitimate receiver. By using an IRS, the reflected signal can be controlled to enhance the intended signal and suppress the signal received at the eavesdroppers, thereby improving the overall performance of the system. Furthermore, the IRS can improve communication security by reflecting the signal toward the legitimate receiver and away from eavesdroppers through direction control of the reflected signal. Therefore, eavesdroppers will not be able to intercept the signal, and the communication will remain secure. Focusing the signal and directing it toward the legitimate receiver also reduces the power needed for transmission and improves the spectral efficiency.

In recent years, the heterogeneity and complexity in network architectures have increased in recent years, making the optimization problems progressively more complex and challenging to solve. Machine learning, one of the most powerful artificial intelligent tools has been widely applied in various areas of research such as computer vision, signal

processing, behavior analysis, search engine and speech recognition. Machine learning shows flexibility in solving problem such as detecting anomalies, forecasting future scenarios, and identifying patterns that humans overlook [11]. Therefore, the application of machine learning to the next generation wireless networks has attracted huge amount of research attention.

Artificial neural networks with deep architecture have provided a powerful framework for the development of learning-based method. Deep learning algorithm typically involve a hierarchical architecture with many layers, each of which consists of a non-linear information processing unit [12]. Deep neural network (DNN), which employ deep architectures in neural networks, can represent functions with higher complexity if the numbers of layers and units in a single layer are increased. Given enough input datasets, deep learning approaches can help humans to establish mapping functions for operation convenience.

DNNs are crucial in secure communication optimization because they can effectively solve the complex optimization problems involved to maximize performance while ensuring security. Secure communication optimization requires finding the optimal transmission parameters such as the transmit power and reflection coefficients of the IRS. Such optimization problems are complex and dynamic owing to the presence of interference, noise, and changing wireless channel conditions. A DNN can analyze data to learn the complex mapping between the wireless channel conditions and the optimal transmission parameters. Once trained, it can predict the optimal transmission parameters in real-time based on the current channel conditions. This allows for efficient and effective optimization, even in dynamic and complex environments.

To highlight the differences between our work and recent studies, key points are summarized in TABLE 1, and a more detailed discussion is provided in Section II. Although recent works [13], [14], [15], [16] have addressed several key concerns related to PLS and/or IRS, the combined study of AN, IRS, and energy harvesting in systems with multiple eavesdroppers has not been properly investigated. Therefore, this paper aims to improve the secure EE of the intended user while degrading the signal of malicious users through the use of AN to secure transmitted information. In addition, malicious users are allowed to harvest energy via simultaneous wireless information and power transfer (SWIPT). Since malicious users may be located among the IoT nodes, we impose constraint for target secrecy rate while allowing the IoT nodes to harvest some energy using SWIPT. Additionally, we introduce the implementation of IRS to improve the PLS communication signals by effectively controlling and manipulating the wireless environment to meet our objective. Our main contributions are summarized as follows:

- 1) We propose an IRS and AN-aided SWIPT IoT system in the presence of eavesdroppers, where the eavesdroppers are permitted to harvest energy without

TABLE 1. Overview of the state-of-the-art studies.

Paper	Objective	Control Parameters	Artificial Noise	Multiple Eves	Energy Harvesting	IRS
[13]	Maximizing long-term secrecy rate in cognitive radio network	Energy harvesting timeslot and transmit power	✓	✗	✓	✗
[14]	Maximizing downlink secure EE in IRS-assisted Cell-Free Network	Beamforming vector, jamming power vector, and IRS phase-shift	✓	✓	✗	✓
[15]	Maximizing weighted sum rate in multi-IRS scenario	Transmit power, IRS selection, and IRS phase-shift	✗	✓	✗	✓
[16]	Maximizing downlink secure EE in MISO networks	Beamforming vector and IRS phase-shift	✗	✓	✗	✓
Our work	Maximizing uplink secure EE in IoT networks	Transmit power, jamming power vector, and IRS phase-shift	✓	✓	✓	✓

decoding the intended signal. We formulate the secure EE maximization problem, where the secure EE is defined as the secrecy rate over the power consumption of the user. We aim to jointly optimize jamming power vector, transmit power of the user, and phase-shift of IRS, and maximize the objective function while ensuring that eavesdroppers get to harvest some energy without compromising the secrecy of the intended communication.

- 2) We propose a learning approach namely, DNN to solve the secure EE problem, where the input is defined as the channel gains and phase of IRS. The loss function is designed following the Lagrangian dual function. Additionally, we propose an iterative approach using gradient descent (GS) with logarithmic barrier function as benchmark algorithm.
- 3) We validate the effectiveness of our approach through numerical simulations, where the results demonstrate an increase in secure energy efficiency when we increase maximum power constraints and the number of IRS units. In addition, the eavesdropper's rate remains consistently low, which can ensure secure communication.

The rest of this paper is organized as follows. Section II describes the system model and problem formulation for secure EE maximization in IRS and AN aided secure communication. Section III explains the incremental technique for the optimization problem, including exhaustive search (ES) and GS algorithms. Section IV describes the proposed DNN to optimize the transmit power and the phase-shift of IRS. Section V elaborates the results obtained using the ES, GS, and the proposed DNN algorithm. Finally, section VI presents the conclusions of the study.

II. RELATED WORKS

Various use cases of AN in wireless communications for enhancing secrecy performance have been studied in [13], [17], [18], and [19]. In [13], the authors studied the PLS improvement in energy harvesting cognitive radio networks, where deep reinforcement learning is adopted to solve the long-term secrecy rate maximization problem. The simulation results show an improvement in the secrecy rate when

the maximum power and battery capacity were increased. In [17], the authors investigated a general relay-assisted communication system in which the source and the relay are equipped with AN capability. The authors formulated a sum-rate maximization problem and solved it using an exact penalty function method with a parallel stochastic decomposition algorithm. In [18], the authors studied a cooperative non-orthogonal multiple access (NOMA) network in which a source communicates with two multiple-antenna users by using NOMA. To tackle eavesdropping problem, the authors incorporate AN scheme with different relay selection techniques. In [19], the authors proposed a novel secure channel estimation technique in which AN with full-duplex was used to enhance the security from malicious nodes. The simulation results showed the advantage offered by AN in eliminating the eavesdropper's signal.

Several previous works highlight the implementation of IRS as a method to enhance the performance of PLS [14], [15], [16], [20], [21]. In [14], the authors studied the max-min secure EE problem in a cell-free network with multiple eavesdroppers. The optimization problem was deconstructed into two subproblems, and solved using concave-convex and semi-definite programming approaches. The simulation outputs demonstrated the improvement and efficacy of the proposed scheme. In [15], the weight sumrate maximization was studied in the multi-IRS scenario. Inspired from computer-vision and artificial intelligence, the authors used DNN to optimize the beamforming vector and phase-shift of the IRS in a way to maximize the objective function. The results illustrated minimal signal blockage of the signal and low inference time. In [16], a secrecy EE maximization problem in downlink multiple-input single-output (MISO) networks was explored. The author solved the problem using the successive convex approximation technique. The numerical results validated the convergence of the algorithms and show enhanced secrecy in EE. In [20], the authors studied an IRS with Gaussian-aided multiple-input multiple-output wiretap channel. They formulated a secrecy rate maximization problem, and solved it by using the alternative algorithm which jointly optimizes the transmit power and phase-shift of the IRS. In [21], the authors investigated active and passive IRS. They formulated a weighted sum-rate of the

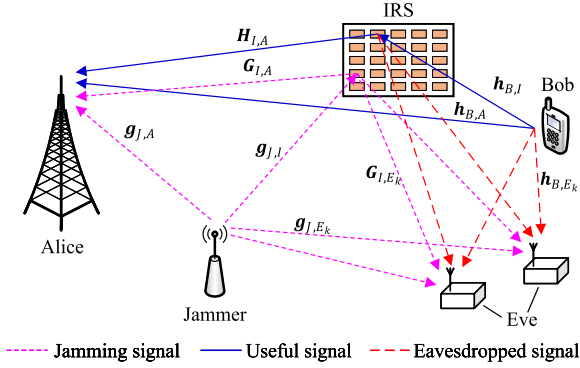


FIGURE 1. System model of IRS and artificial-noise aided secure communication.

uplink and downlink communications, and found that the passive IRS outperforms the active one when the number of reflecting elements is sufficiently large, regardless of whether the communication is downlink or uplink.

The combination of AN techniques with IRS shows promise in improving PLS in IoT networks. However, practical challenges in real systems remain. With the covert nature of passive eavesdroppers, it is challenging to accurately measure and obtain the eavesdroppers' CSI [22]. This can hinder the performance of the AN jammer; thus degrading the security performance of the system. Additionally, the challenge in further enhancing existing AN and IRS systems may relate to hardware costs, i.e., increasing the number of antennas at the jammer, and designing high-quality material and high-precision IRS phase-shift control [23].

III. SYSTEM MODEL

A. COMMUNICATION MODEL

In this system model, we consider that there are one AP (Alice), one user (Bob), and K eavesdroppers (Eve), where Alice and Bob are equipped with M_A antenna and a single antenna, respectively. An IRS has a total of L reflecting elements, and is mounted fixed on a building at height h [24]. We assume that all Eves are suspicious IoT sensor nodes equipped with SWIPT using power splitting policy. From the perspective of Alice and Bob, Eves are untrusted nodes in the communication network. Therefore, to ensure covert communication, Alice and Bob aim to suppress their signal from Eves while allowing the signals to be sufficiently strong for energy harvesting. However, due to the nature of wireless signals, suppressed signals may not guarantee complete covert communication. Therefore, an additional jammer equipped with M_J antennas is considered to send a jamming signal to Eves. This helps to enhance the secrecy of the communication between Alice and Bob by creating additional interference and making it more difficult for Eves to intercept or decode the signals.

The baseband equivalent channel from the Bob to Alice, Bob to IRS, and Bob to Eve are denoted as $\mathbf{h}_{B,A} \in \mathbb{C}^{M_A \times 1}$, $\mathbf{h}_{B,I} \in \mathbb{C}^{L \times 1}$, and $\mathbf{h}_{B,E_k} \in \mathbb{C}^{1 \times 1}$, respectively. The baseband

signal equivalent channel from the jammer to IRS, jammer to Alice, jammer to Eve are denoted as $\mathbf{G}_{J,I} \in \mathbb{C}^{L \times M_J}$, $\mathbf{G}_{J,A} \in \mathbb{C}^{M_A \times M_J}$, and $\mathbf{g}_{J,E_k} \in \mathbb{C}^{1 \times M_J}$, respectively. The baseband signal equivalent channel from the IRS to Alice and Eve can be denoted as $\mathbf{H}_{I,A} \in \mathbb{C}^{L \times M_A}$ and $\mathbf{h}_{I,E_k} \in \mathbb{C}^{L \times 1}$. The transmitted signal from Bob and the jammer are given by

$$x_1 = ps \quad (1)$$

$$x_2 = \mathbf{f}a \quad (2)$$

where $s \sim \mathcal{CN}(0, 1)$ and $a \sim \mathcal{CN}(0, 1)$ are independent information and jamming signals, respectively. $\mathbf{f} \in \mathbb{C}^{1 \times M_J}$ and $p \in \mathbb{C}^{1 \times 1}$ denote jamming vectors and Bob transmit power, respectively. Given $M_A = M_J = M$, the signal received at Alice and Eve k are given by

$$y_A = (\mathbf{h}_{B,A}^H + \mathbf{h}_{B,I}^H \mathbf{\Theta} \mathbf{H}_{I,A})ps + (\mathbf{g}_{J,A}^H + \mathbf{g}_{J,I}^H \mathbf{\Theta} \mathbf{G}_{I,A})\mathbf{f}a + n_B, \quad (3)$$

$$y_{E_k} = (\mathbf{h}_{B,E_k}^H + \mathbf{h}_{B,I}^H \mathbf{\Theta} \mathbf{h}_{I,E_k})ps + (\mathbf{g}_{J,E_k}^H + \mathbf{g}_{J,I}^H \mathbf{\Theta} \mathbf{G}_{I,E_k})\mathbf{f}a + n_{E_k}, \quad (4)$$

where $n_A, n_{E_k} \sim \mathcal{CN}(0, \sigma_0^2)$ is the complex additive white Gaussian noise (AWGN). The signal-to-interference-plus-noise ratio (SINR) at Alice and Eve k are given by

$$\gamma_A = \frac{|\left(\mathbf{h}_{B,A}^H + \mathbf{h}_{B,I}^H \mathbf{\Theta} \mathbf{H}_{I,A}\right)p|^2}{\left|\left(\mathbf{G}_{J,A}^H + \mathbf{G}_{J,I}^H \mathbf{\Theta} \mathbf{H}_{I,A}\right)\mathbf{f}\right|^2 + \sigma^2}, \quad (5)$$

$$\gamma_{E_k} = \frac{|\left(h_{B,E_k}^H + \mathbf{h}_{B,I}^H \mathbf{\Theta} \mathbf{h}_{I,E_k}\right)p|^2}{\left|\left(\mathbf{g}_{J,E_k}^H + \mathbf{G}_{J,I}^H \mathbf{\Theta} \mathbf{h}_{I,E_k}\right)\mathbf{f}\right|^2 + \sigma^2}, \quad (6)$$

For the proposed secure EE in the IRS and AN-aided system, the achievable rate can be defined as

$$R_A = \log_2(1 + \gamma_A), \quad (7)$$

$$R_{E_k} = \log_2(1 + \alpha \gamma_{E_k}), \quad (8)$$

where α is the power splitting ratio of Eve. From (7) and (8), we can express the secure EE as

$$EE(\mathbf{f}, p, \theta) = \frac{R_A - \max_{k \in K} R_{E_k}}{\mathbf{f}^H \mathbf{f} + P_c + p}. \quad (9)$$

where P_c is the circuit power consumption of Bob.

B. PROBLEM FORMULATION

In this subsection, we formulate the problem of maximizing the secure EE in an IRS and AN-aided communication system with a secrecy rate constraint while allowing the eavesdroppers to harvest energy to a certain threshold. The optimization problem can be described by

$$\begin{aligned} & \max_{\mathbf{f}, p, \theta} EE(\mathbf{f}, p, \theta) \\ & \text{s.t. C1: } \mathbf{f}^H \mathbf{f} + p \leq P_{\max}, \\ & \quad \text{C2: } R_A - R_{E_k} \geq R_{\text{Sec}, t \text{ ar}}, \\ & \quad \text{C3: } \gamma_{E_k} \geq \gamma_{EH}, \\ & \quad \text{C4: } 0 \leq \theta \leq 2\pi, \end{aligned} \quad (10)$$

where $R_{sec,tar}$ is the threshold for the target secrecy rate; and γ_{EH} is the minimum SINR for Eve to be able to harvest energy. Notably, the term C1 is the power constraint that limits the total transmit power of Bob and jammer to be less than or equal to maximum allowable transmit power P_{max} . C2 means that the secrecy rate must be greater or equal to the requirement. C3 allows the SINR of Eavesdropper k to be greater than or equal to the minimum energy harvesting threshold. We can notice that the proposed objective function formulated in (10) is a non-convex problem with non linear constraints, making it hard to find a closed-form solution for the optimal transmit power $(\mathbf{f}, p)$ and phase-shift of IRS θ . Therefore, as an alternative method of obtaining the solution of (10), we developed a learning-based approach namely, DNN. In this approach, we train the DNN to learn and approximate the optimal strategy for achieving the secrecy rate in an IRS and AN-aided communication system.

IV. OPTIMIZATION-BASED ITERATIVE METHOD

We explain the application of ES and GS, combined with a constraining factor, to determine the best global and local parameter values for $\mathbf{f}$, p , and θ .

A. EXHAUSTIVE SEARCH

The ES algorithm is a commonly employed approach for locating the optimal solution in optimization problems. While it is a straightforward method, its costs escalate as problem complexity increases. This method reviews all potential options, taking into consideration control parameters such as $\mathbf{f}$, p , and θ , to enhance the objective function while staying within set constraints.

Since implementing the ES incurs significant computational complexity, especially when the number of IRS element increases. We use the search algorithm called GlobalSearch in Matlab to find the global solution of the proposed secure EE problem. GlobalSearch uses a scatter-search mechanism for generating start points. MultiStart uses uniformly distributed start points within bounds, or user-supplied start points. GlobalSearch analyzes start points and rejects those points that are unlikely to improve the best local minimum found so far. MultiStart runs all start points (or, optionally, all start points that are feasible with respect to bounds or inequality constraints).

B. GRADIENT SEARCH

GS, or gradient descent/ascent, is an incremental method for finding local minima/maxima by following the gradient. To handle constraints, we introduce a barrier and use a logarithmic barrier method as a penalty with a parameter $t > 0$, leading to a modified objective function as follows:

$$U(\mathbf{f}, p, \theta) = EE(\mathbf{f}, p, \theta) + f(\mathbf{f}, p, \theta), \quad (11)$$

where the penalty term is

$$f(\mathbf{f}, p, \theta) = \frac{1}{t} \sum_{i=1}^N \left[\ln(P_{max} - \mathbf{f}^H \mathbf{f} - p) + \ln(2\pi - \theta) \right]$$

Algorithm 1 Gradient Search Algorithm

initialize $p, \vec{\mathbf{f}}, \vec{\theta}$ in feasible region

set η_1, η_2, η_3 and ϵ

repeat

$$p_{new} = p_{old} + \eta_1 \times \frac{\partial U}{\partial p}$$

$$\vec{\mathbf{f}}_{new} = \vec{\mathbf{f}}_{old} + \eta_2 \times \frac{\partial U}{\partial \vec{\mathbf{f}}_1}$$

$$\vec{\theta}_{new} = \vec{\theta}_{old} + \eta_3 \times \frac{\partial U}{\partial \vec{\theta}}$$

until $|U_{new} - U_{old}| < \epsilon$

$$\begin{aligned} & + \ln(\theta) + \ln(R_A - R_{E_k} - R_{sec,tar}) \\ & + \ln(p) + \ln(\mathbf{f}^H \mathbf{f}) + \ln(\gamma_{EH} - \gamma_{E_k}) \end{aligned} \quad (12)$$

V. PROPOSED DNN STRUCTURE

Deep learning has proven to be an effective tool for tackling complex, nonconvex optimization challenges in wireless communication systems. This success comes from the universal approximation theorem, which enables DNN to closely approximate optimal solution sets. Researches have demonstrated that deep learning-based methods can achieve performance levels very close to optimal while substantially decreasing computational demands [25], [26].

In this section, we introduce the DNN algorithm designed to predict the optimal solution for the problem described in equation (10). For the training of the proposed DNN structure, we use an unsupervised learning-based training, i.e., the optimal solutions are not provided as label data. The DNN is trained with the goal of minimizing the loss function, which is derived through the utilization of the Lagrange duality technique. Given that our optimization problem involves constraints, we incorporate the Lagrangian to encompass all the constraints in (10) within the loss function. This strategic approach allows for the incorporation of the constraints during the optimization of the DNN. The details of the loss function formulated in the form of Lagrangian will be described later in (17).

In this structure, we set the number of hidden layers to S . Each node in each layer is fully connected to the preceding layer. Fig. 2 provides a visual representation of the proposed DNN model where sigmoid function is the activation function. In practice, the wireless channel experiences significant dynamics due to the exponentially decreasing channel gain with distance, which can negatively affect the training of the DNN structure. To address this, the DNN takes input data where the channel gain is normalized to a mean of zero and a variance of one using batch normalization, ensuring stable convergence during network training [27]. The input data is given as

$$\begin{aligned} \vec{x} = \mathcal{N}(\text{reshape}(\{ & \mathbf{h}_{B,A}^H \mathbf{h}_{B,A} \}, \{ \mathbf{h}_{B,I}^H \mathbf{h}_{B,I} \}, \{ \mathbf{H}_{I,A}^H \mathbf{H}_{I,A} \}, \\ & \{ \mathbf{g}_{J,A}^H \mathbf{g}_{J,A} \}, \{ \mathbf{g}_{J,I}^H \mathbf{g}_{J,I} \}, \{ \mathbf{G}_{I,A}^H \mathbf{G}_{I,A} \}, \\ & \{ \mathbf{G}_{I,E_k}^H \mathbf{G}_{I,E_k} \}, \{ \Theta \} \})), \end{aligned} \quad (13)$$

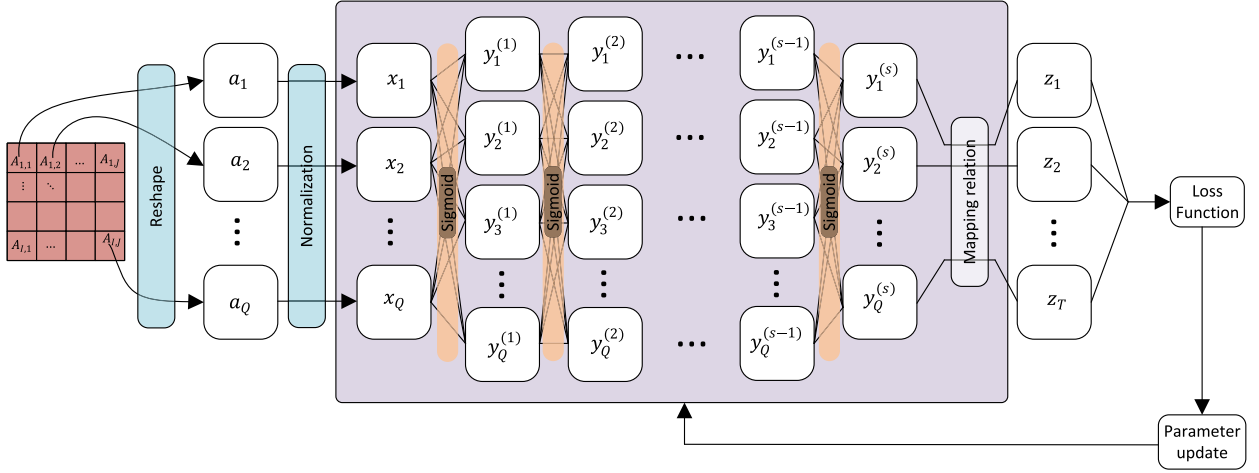


FIGURE 2. Proposed DNN structure.

where $\mathcal{N}(\cdot)$ is the normalization function, respectively. Since each channel matrix has a different dimension, the input is reshaped (flattened and concatenated) from the matrix $\mathbf{A} \in \mathbb{R}^{I \times J}$ to a column vector $\tilde{\mathbf{A}} \in \mathbb{R}^Q$, where $Q = I \times J$, and I and J represent the number of rows and columns, respectively. The s -th hidden layer is configured with a node count of k which corresponds to the size of the reshaped vector $\tilde{\mathbf{A}}$ representing all the channel gains and phase of IRS. Using the input vector, $\tilde{\mathbf{y}}^{(1)} \in \mathbb{R}^{1 \times Q}$ is computed within the nodes of the initial layer, which can be represented as

$$\tilde{\mathbf{y}}^{(1)} = \mathcal{S}(W^{(0)}\tilde{\mathbf{x}}), \quad (14)$$

Here, $\mathcal{S}(\cdot)$ denotes the sigmoid function, defined as $\frac{1}{1+e^{-\cdot}}$, and the weight linked with the initial hidden layer is represented as $W^{(0)}$. Due to the activation of the sigmoid function in each layer, the DNN output spans a range from zero to one. Consequently, it is necessary to create a correlation of the DNN output and the transmit power. The correlation for the transmit power and phase-shift based on DNN output is described as

$$p = (1 - y_{[M+1:M+2]}^{(s)})P_{min} + y_{[M+1:M+2]}^{(s)}P_{max}, \quad (15)$$

$$\theta = 2\pi \times y_{[M+3:M+L+4]}^{(s)}. \quad (16)$$

The transmit power in equation (15) must consistently adhere to the power constraint inequality since $\tilde{\mathbf{y}}^{(s)}$ falls within the range of the sigmoid function output. The same applies to the phase-shift of the IRS. For phase-shift of IRS, because the phase range is $\theta \in [0, 2\pi]$, we multiply the output from the sigmoid function with 2π directly as shown in (16). For adjusting the neural network's weight, we employ the back-propagation technique, known for its effectiveness in minimizing errors. In our study, the loss function is defined as follows

$$\begin{aligned} \mathcal{L}(\mathbf{f}, p, \theta, \lambda, v, \kappa, \tau) \\ = -EE + \lambda(p + \sum_{i=1}^N \mathbf{f} - P_{max}) \end{aligned}$$

$$\begin{aligned} + \sum_{i=1}^L v_i(\theta_i - 2\pi) + \kappa(R_{E_k} + R_{sec,tar} - R_A) \\ + \tau(\gamma_{E_k} - \gamma_{EH}), \end{aligned} \quad (17)$$

where λ , v , κ and τ are the multipliers, where $\tilde{\mathbf{x}}$ is a normalized reshaped vector. In our proposed DNN, the loss function is formulated to ensure that its value increases proportionally when any of the constraints C1-C4 are violated. This is achieved by incorporating penalty terms that reflect the degree of violation of each constraint as written in (17). As a result, when a violation occurs, the corresponding penalty term (i.e., λ , v , κ , τ) amplifies the value of the loss function. This mechanism signals the DNN to adjust its weight parameters through backpropagation and guides the model to satisfy the constraints while minimizing the loss function (maximizing the objective function). This structured approach ensures that the DNN not only maximizes the secure EE but also adheres to the specified constraints C1-C4. The function for updating weights is established by deriving the loss function concerning the transmit power for the jammer, Bob, and the phase-shift for the IRS, which is given by $\nabla_{\mathbf{f}}L(\mathbf{f}, p, \theta, \lambda, v, \kappa, \tau)$, $\nabla_pL(\mathbf{f}, p, \theta, \lambda, v, \kappa, \tau)$ and $\nabla_{\theta}L(\mathbf{f}, p, \theta, \lambda, v, \kappa, \tau)$, respectively. The update procedures are iterated as follows:

$$\begin{aligned} \tilde{l}_{[1:M]}^{(s+1)} &= \nabla_{\mathbf{f}}L(\mathbf{f}, p, \theta, \lambda, v, \kappa, \tau), \\ \tilde{l}_{[M+1:M+2]}^{(s+1)} &= \nabla_pL(\mathbf{f}, p, \theta, \lambda, v, \kappa, \tau), \\ \tilde{l}_{[M+3:M+L+4]}^{(s+1)} &= \nabla_{\theta}L(\mathbf{f}, p, \theta, \lambda, v, \kappa, \tau), \\ \tilde{l}_{[M+L+5:2M+L+6]}^{(s+1)} &= p + \sum_{i=1}^N \mathbf{f} - P_{max}, \\ \tilde{l}_{[2M+L+7:2(M+L)+8]}^{(s+1)} &= \theta_i - 2\pi, \\ \tilde{l}_{[2(M+L)+9:2(M+L)+10]}^{(s+1)} &= R_{E_k} + R_{sec,tar} - R_A, \\ \tilde{l}_{[2(M+L)+11:2(M+L)+12]}^{(s+1)} &= \gamma_{E_k} - \gamma_{EH}. \end{aligned} \quad (18)$$

The update process for the output layer's weight unit is as follows

$$\vec{W}^{(s+1)} \leftarrow \vec{W}^{(s+1)} - \eta_{dnn} S^{(s)} \vec{l}^{(s+1)}. \quad (19)$$

In this context, η_{dnn} symbolizes the learning step, starting at the layer s and spanning to the input layer. Consequently, the cost function for the s -th hidden layer can be formulated as follows:

$$\vec{l}^{(s+1)} = S^{(s)}(1 - S^{(s)})\vec{W}^{(s+1)}\vec{l}^{(s+1)}. \quad (20)$$

Here, we discuss in more detail how the proposed DNN is trained, validated and inferred. The proposed DNN is trained using an unsupervised learning approach, where the optimal values for transmit power, jamming power vector, and IRS phase-shift are independently determined during the training process without relying on labeled data. From (17), the value of the loss function decreases as the secure EE of the system increases while the constraints for transmit power, phase-shift of IRS, secrecy rate requirement and energy harvesting are satisfied. To approximate the optimal solution of (10), the DNN parameters undergo adjustments throughout the training phase to maximize secure EE while ensuring that C1-C4 are met. Additionally, validation is performed during training using 10% of the generated data comprising channel gains and IRS phase shifts, which is separated from the entire dataset. Once training is finished, the transmit power, the jamming power vector, and the IRS phase-shift can be determined by entering the normalized reshaped channel gains and IRS phase-shift as given in (13), into the trained DNN model during the inference stage. In particular, the channel gains and IRS phase-shift are measured by every node (jammer, Alice, Bob, Eves, and IRS controller) and sent to a central controller through the control channel. The central controller utilizes the collected inputs (channel state information and IRS phase-shift) and the trained DNN model to decide on the transmit power, jamming power vector, and IRS phase-shift. The determined transmit power, jamming power vector and IRS phase-shift are transmitted via control channel to Bob, jammer, and IRS controller, respectively.

With the fixed output dimension of the DNN, the changes in the number of users, eavesdroppers, or reflecting elements would also require retraining of the network. Although retraining may require extra time, only the inference process occurs during the implementation stage, which requires minimal computation time due to the DNN structure involving simple matrix calculations and functions (i.e., forward pass). Therefore, the extended training time is unlikely to interfere with real-time operation in a dynamic IoT environment.

VI. RESULTS AND DISCUSSION

In this section, we numerically evaluate the performance of the proposed algorithm. For simulation runs, we set the location of Alice, Bob, IRS, and jammer as (0,5,20), (100,0,1.8), (80,-20,10) and (50,25,20), respectively. We deploy the eavesdroppers in randomly determined location around Bob

Algorithm 2 Proposed DNN Algorithm

Initialize weights using Xavier initialization in [28].

Reshape the input into one column, and normalize it with zero mean and unit variance.

Initialize the Tolerance and learning rate.

repeat

Compute the output of all hidden layers along with DNN output using (14).

Compute the mapping relation of the normalized power and phase-shift as in (15) and (16), respectively.

fix the parameters into loss function (17).

Update the weight of neural network as in (19)

Calculate error as in (20).

until $|\mathcal{L}_{new} - \mathcal{L}_{old}| < \text{Tolerance}$

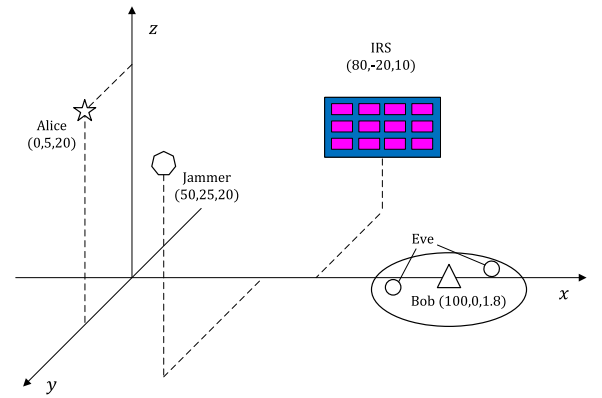


FIGURE 3. Node deployment diagram.

TABLE 2. Simulation parameters.

Parameter	Symbol	Value
Maximum transmit power	P_{max}	10,12,14,...,28 dBm
Minimum power	P_{min}	0 dBm
Number of Eve	K	2
Number of IRS elements	L	6,12,20,30,40,50
Power splitting ratio	α	0.5
Noise power	σ^2	-95 dBm
Number of jammer antenna	M	4
Circuit power consumption	P_c	23 dBm [29]
Learning rate in GS	η_1, η_2, η_3	10^{-4} [30]
Learning rate in DNN	η_{dnn}	3×10^{-4} [31]
Minimum energy harvesting threshold	γ_{EH}	-5 dB [32]
Required secrecy rate	$R_{sec,tar}$	5 bps/Hz

within a 10m radius. Fig. 3 shows the detail of deployment-related parameters. We set the default number of IRS elements in the simulation to 6. The pathloss exponents for IRS-Alice, IRS-Eve, Bob-Eve, Bob-IRS and Bob-Alice are defined as 2.2, 2.2, 2.5, 2.5, and 3.5, respectively. Table 2 lists additional details of the simulation parameters.

We evaluate the performances of GS and ES, for comparison with the proposed algorithm. To evaluate the effectiveness of the ES algorithm, the quantization rate of p, f and θ are configured as 10^3 . For GS, we newly

initialize all the parameters such as controlling parameters, location of Eves, and fading channels for every epoch. We update transmit power, jamming power vector and IRS phase-shift using Algorithm 1 until convergence. Then, we average the solutions for 600 simulation settings for each maximum power constraint and the number of reflecting element. The simulation setup for ES is also applied in a similar way. Concerning the GS algorithm, we configure the regularization factor t to 10^2 . The error threshold ϵ is set to 10^{-4} . The GS learning rate is set as $\eta_1 = \eta_2 = \eta_3 = 10^{-4}$, chosen for its stability in ensuring optimization of control parameters like IRS phase-shift, jamming power vector, and transmit power. For the proposed DNN, we set the learning rate and its tolerance as $\eta_{dnn} = 3 \times 10^{-4}$ and 10^{-4} , respectively. For the dataset, the input for DNN consists of the channel gain of Bob-Alice, Bob-IRS, IRS-Alice, Jammer-Alice, Jammer-IRS, IRS-Alice, IRS-Eve and IRS phase-shift i.e., $\{\mathbf{h}_{B,A}^H \mathbf{h}_{B,A}\}$, $\{\mathbf{h}_{B,I}^H \mathbf{h}_{B,I}\}$, $\{\mathbf{H}_{I,A}^H \mathbf{H}_{I,A}\}$, $\{\mathbf{g}_{J,A}^H \mathbf{g}_{J,A}\}$, $\{\mathbf{g}_{J,I}^H \mathbf{g}_{J,I}\}$, $\{\mathbf{G}_{I,A}^H \mathbf{G}_{I,A}\}$, $\{\mathbf{G}_{I,E_k}^H \mathbf{G}_{I,E_k}\}$, $\{\Theta\}$. To get the dataset, we generated each unique set by randomly varying the Eves' location and setting the IRS phase-shift. We collect this dataset for 10^5 sets, where majority of the dataset, specifically 90% of the total, were allocated for training. The remaining 10% of the samples were set aside to assess the performance of the proposed DNN after it had been trained.

Fig. 4 shows the EE with various maximum power constraint. It is noticeable that the EE shows an increasing trend as the maximum power limit increases. The proposed method performs very close to the global optimal around lower maximum transmit power limits, and further stays near the upper bound for higher maximum power limit. In term of EE, GS shows lower performance than that of DNN for all maximum power limits. At around $P_{max} = 24$ dBm, the EE becomes stable, and the effect of power increase becomes marginal. Fig. 5 shows the secrecy rate and Eve's rate in terms of the maximum power. With all three algorithms, Eve's rate is very low compared to secrecy rate. As the maximum power increases, Eve's rate also increases. However, the increase in Eve's rate is still significantly low for the proposed method compared to that of the GS. We can see the DNN achieves similar result to the ES in lower power constraints at $P_{max} = 10, 12$ dBm. This is because the power being transmitted from Bob to Alice is relatively low, making it hard for Eve to eavesdrop the signal. With the increase in power constraint the Eve's rate increases gradually, but remains relatively low compared to the secrecy rate, thus verifying the energy harvesting constraint in C3 of (10).

In addition, we compare the EE obtained using the GS, ES and DNN algorithms with various number of reflecting elements of IRS and the maximum power limit of $P_{max} = 28$ dBm. As illustrated in Fig. 6, the EE increases for all algorithms as we increase the number of reflecting elements. We can see the DNN outperforms GS while staying relatively near the global optimal for all the number of reflecting element. We can also verify that EE is enhanced considerably when the number of reflecting elements is from

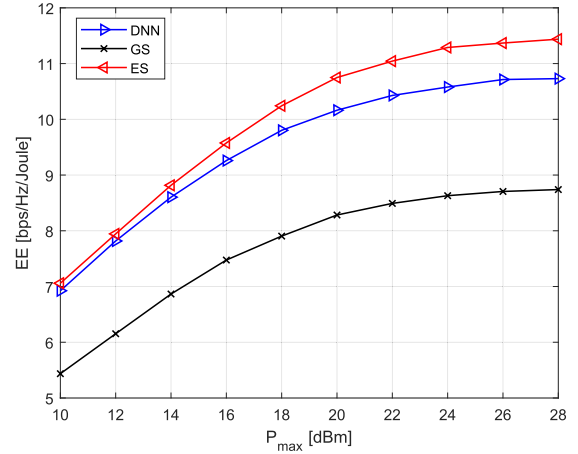


FIGURE 4. Secure EE vs. maximum power.

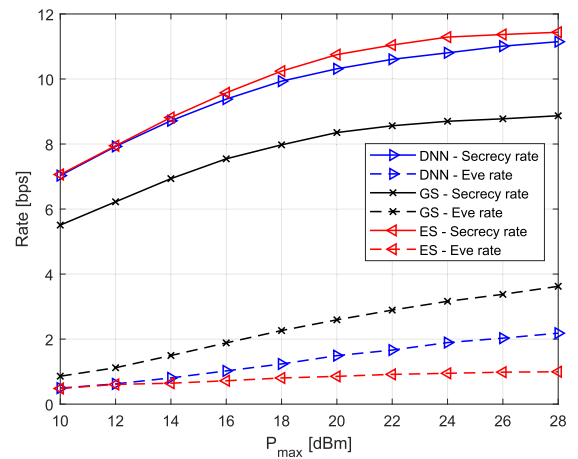


FIGURE 5. Rate vs. maximum power.

around 5 to 30. The EE gradually becomes saturated as the number of reflecting elements is increased further.

Fig. 7 shows the achievable secrecy rate and Eve's rate. The secrecy rate obtained using DNN is close to the upper bound solution compared to obtaining using GS. Eve's rate of DNN is also much lower than that of GS, which shows that IRS results in a larger performance gain in the system as L increases.

Fig. 8 illustrates a numerical result of received AN levels with varying number of reflecting elements. Most notably, the proposed DNN demonstrates better performance than GS in terms of AN reception at Eve and Bob, performing closely to the optimal solution of the ES. Additionally, DNN maintains a consistent gap of approximately 25-30 dBm throughout the increasing number of IRS elements while GS remains at around 15 dBm gap. GS approach exhibits the highest AN reception levels at roughly -34 dBm for Bob and the lowest AN reception levels for Eve at around -22 dBm. Particularly, DNN approach shows marked improvement as the number of reflecting elements increases, with AN levels dropping from around -38 dBm to nearly -45 dBm. Even though the

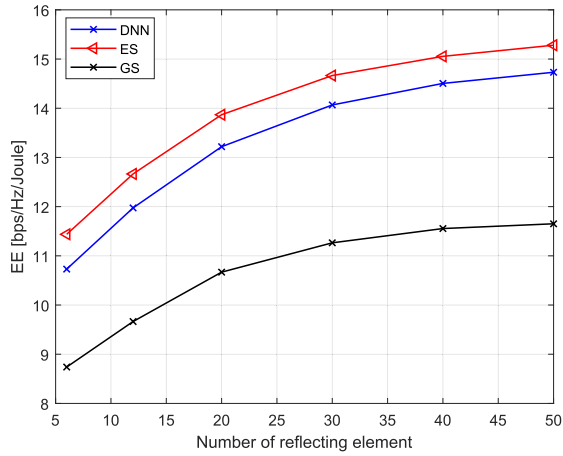


FIGURE 6. Secure EE vs. the number of IRS element.

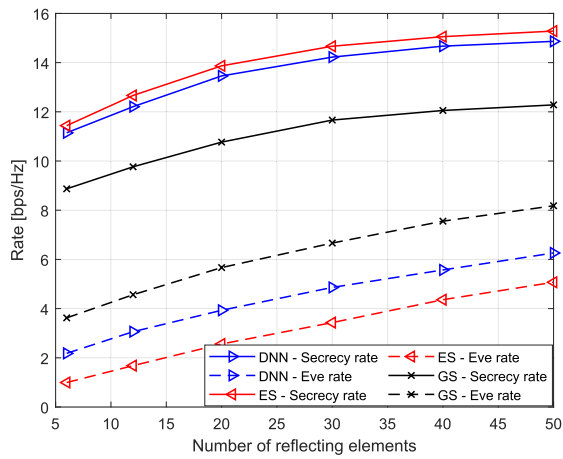


FIGURE 7. Rate vs. the number of IRS element.

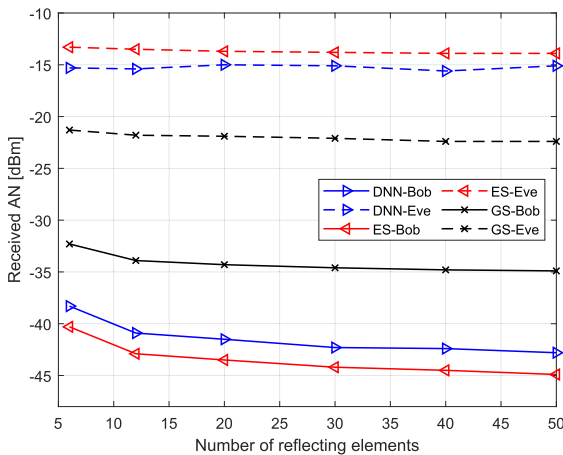


FIGURE 8. Rate vs. the number of IRS element.

AN reception at Eves remains largely unchanged throughout the increasing the number of IRS elements, it decreases slightly at Bob. This is primarily due to the close proximity of Eves to Bob, which causes the AN signals directed toward Eves to create some level of interference, partially affecting

Bob's channel. This indicates that increasing the number of IRS elements can mitigate the AN received by Bob while maintaining a steady level of AN at Eves.

VII. CONCLUSION

In this study, we investigate the application of IRS in the PLS of IoT devices in the aim to enhance the secure EE. We proposed a secure EE maximization problem by jointly considering the phase-shift of IRS, and the transmit powers of the jammer and user with the energy harvesting constraint. To find the optimal phase-shift and transmit power of both the jammer and user, we formulated a non-convex optimization problem with linear and non-linear constraints. We used the DNN algorithm to find a solution for this problem. The loss function of the DNN algorithm was formulated based on the Lagrange duality function, which was then minimized during the training process. We compared the performances of two suboptimal algorithms, namely GS and DNN, with that of ES, which can be considered as the global optimal. The simulation results show that the proposed DNN algorithm performs better than that of the GS in terms of the maximum power constraint and the number of reflection element of IRS, while ensuring sufficient rate of eavesdroppers for energy harvesting. The results highlight the necessity of implementing IRS to improve secure EE.

In future work, we plan to combine the DNN approach with successive convex approximation (SCA) to solve the secure EE problem in multi-IRS systems by using the DNN to initialize the SCA starting point.

REFERENCES

- [1] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.
- [2] A. Almohamad, A. M. Tahir, A. Al-Kababji, H. M. Furqan, T. Khatat, 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, 2020.
- [3] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, "Security of things intrusion detection system for smart healthcare," *Electronics*, vol. 10, no. 12, p. 1375, Jun. 2021.
- [4] H. Chamkhia, A. Erbad, A. Mohamed, A. R. Hussein, A. K. Al-Ali, and M. Guizani, "Stochastic geometry-based physical-layer security performance analysis of a hybrid NOMA-PDM-based IoT system," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 2027–2042, Jan. 2024.
- [5] C. Huang, G. Chen, and K.-K. Wong, "Multi-agent reinforcement learning-based buffer-aided relay selection in IRS-assisted secure cooperative networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4101–4112, 2021.
- [6] W. Jiang, B. Chen, J. Zhao, Z. Xiong, and Z. Ding, "Joint active and passive beamforming design for the IRS-assisted MIMOME-OFDM secure communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10369–10381, Oct. 2021.
- [7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [8] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, May 2021.
- [9] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1546–1577, 3rd Quart., 2021.

- [10] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2283–2314, 4th Quart., 2020.
- [11] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2224–2287, 3rd Quart., 2019.
- [12] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11–26, Apr. 2017.
- [13] R. Lin, H. Qiu, W. Jiang, Z. Jiang, Z. Li, and J. Wang, "Deep reinforcement learning for physical layer security enhancement in energy harvesting based cognitive radio networks," *Sensors*, vol. 23, no. 2, p. 807, Jan. 2023.
- [14] W. Hao, J. Li, G. Sun, C. Huang, M. Zeng, O. A. Dobre, and C. Yuen, "Robust security energy efficiency optimization for RIS-aided cell-free networks with multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 72, no. 12, pp. 7401–7416, Dec. 2024.
- [15] C. Hu, Y. Lu, H. Du, M. Yang, B. Ai, and D. Niyato, "AI-empowered RIS-assisted networks: CV-enabled RIS selection and DNN-enabled transmission," *IEEE Trans. Veh. Technol.*, vol. 73, no. 11, pp. 17854–17858, Nov. 2024.
- [16] Y. Lu, "Secrecy energy efficiency in RIS-assisted networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 9, pp. 12419–12424, Sep. 2023.
- [17] B. Li, M. Zhang, Y. Rong, and Z. Han, "Artificial noise-aided secure relay communication with unknown channel knowledge of eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 3168–3179, May 2021.
- [18] Z. Cao, X. Ji, J. Wang, W. Wang, K. Cumanan, Z. Ding, and O. A. Dobre, "Artificial noise aided secure communications for cooperative NOMA networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 8, no. 2, pp. 946–963, Jun. 2022.
- [19] F. U. Din and F. Labeau, "Artificial noise assisted in-band full-duplex secure channel estimation," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6800–6813, Jul. 2021.
- [20] L. Dong and H.-M. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.
- [21] C. You and R. Zhang, "Wireless communication aided by intelligent reflecting surface: Active or passive?" *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2659–2663, Dec. 2021.
- [22] M. H. Khoshafa, O. Maraqa, J. M. Moualeu, S. Aboagye, T. M. N. Ngatched, M. H. Ahmed, Y. Gadallah, and M. D. Renzo, "RIS-assisted physical layer security in emerging RF and optical wireless communication systems: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, early access, Oct. 28, 2024, doi: 10.1109/COMST.2024.3487112.
- [23] D. Sarkar, Yogita, S. S. Yadav, V. Pal, N. Kumar, and S. K. Patra, "A comprehensive survey on IRS-assisted NOMA-based 6G wireless network: Design perspectives, challenges and future directions," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 2, pp. 2539–2562, Apr. 2024.
- [24] X. Pang, M. Sheng, N. Zhao, J. Tang, D. Niyato, and K.-K. Wong, "When UAV meets IRS: Expanding air-ground networks via passive reflection," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 164–170, Oct. 2021.
- [25] W. Lee and R. Schober, "Deep learning-based resource allocation for device-to-device communication," *IEEE Trans. Wireless Commun.*, vol. 21, no. 7, pp. 5235–5250, Jul. 2022.
- [26] K. Lee and H.-H. Choi, "Transmit power control for secure wireless-powered sensor networks with malicious energy harvester," *IEEE Access*, vol. 11, pp. 103146–103153, 2023.
- [27] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.
- [28] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proc. 13th Int. Conf. Artif. Intell. Statist.*, Mar. 2010, pp. 249–256.
- [29] B. T. Malik, V. Doychinov, A. M. Hayajneh, S. A. R. Zaidi, I. D. Robertson, and N. Somjit, "Wireless power transfer system for battery-less sensor nodes," *IEEE Access*, vol. 8, pp. 95878–95887, 2020.
- [30] K. T. Pauu, Q. Pan, J. Wu, A. K. Bashir, M.-V. Maka, and M. Omar, "IRS-aided federated learning with dynamic differential privacy for UAVs in emergency response," *IEEE Internet Things Mag.*, vol. 7, no. 4, pp. 108–115, Jul. 2024.
- [31] D. Granzio, S. Zohren, and S. Roberts, "Learning rates as a function of batch size: A random matrix theory approach to neural network training," *J. Mach. Learn. Res.*, vol. 23, no. 173, pp. 1–65, Jan. 2020.
- [32] O. Alamu, T. O. Olwal, and K. Djouani, "Achievable rate optimization for space-time block code-aided cooperative NOMA with energy harvesting," *Eng. Sci. Technol., Int. J.*, vol. 40, Apr. 2023, Art. no. 101365.



KIMCHHEANG CHHEA received the B.S. degree from the Department of Electrical and Energy Engineering, Institute of Technology of Cambodia, Phnom Penh, Cambodia, in 2019. He is currently pursuing the integrated M.S. and Ph.D. degrees with the Department of Intelligent Energy and Industry, Chung-Ang University, Seoul, South Korea. His current research interests include energy-efficient networks and machine learning-based wireless networks.



JUNG-RYUN LEE (Senior Member, IEEE) received the B.S. and M.S. degrees in mathematics from Seoul National University, in 1995 and 1997, respectively, and the Ph.D. degree in electrical and electronics engineering from Korea Advanced Institute of Science and Technology (KAIST), in 2006. From 1997 to 2005, he was the Chief Research Engineer with LG Electronics, South Korea. From 2006 to 2007, he was a full-time Lecturer of electronic engineering with the University of Incheon. Since 2008, he has been a Professor with the School of Electrical and Electronics Engineering, Chung-Ang University, South Korea. His research interests include energy-efficient networks and algorithms, bio-inspired autonomous networks, and artificial intelligence-based networking. He is a Regular Member of IEICE, KIISE, and KICS. He received the Excellent Paper Award at ICUFN 2012, the Best Paper Award at ICN 2014, the Best Paper Award at QSHINE 2016, and the Excellent Paper Award at ICTC 2018.

• • •