Learning-Based Wireless Powered Secure Transmission

Dongxuan He, Chenxi Liu, *Member, IEEE*, Hua Wang, *Member, IEEE*, and Tony Q. S. Quek, *Fellow, IEEE*

***Abstract*—In this letter, we propose a learning-based wireless powered secure transmission, in which a source utilizes energy harvested from a power beacon to communicate with a legitimate receiver, in the presence of an eavesdropper. In order to confuse the eavesdropper, we assume that the source transmits the artificial noise signals, in addition to the information signals. We first characterize the effective secrecy throughput of our system, showing its dependence on the transmission parameters, including the fraction of time allocated for wireless power transfer, the fraction of power allocated to the information signals, as well as the wiretap code rates. We then leverage the deep feedforward neural network to learn how the optimal transmission parameters that jointly maximize the effective secrecy throughput can be obtained. Through numerical results, we demonstrate that our learning-based scheme can achieve almost the same secrecy performance as the optimal solution obtained from the exhaustive search, while requiring much less computational complexity.**

***Index Terms*—Wireless power transfer, artificial noise, physical layer security, deep feedforward neural network.**

I. Introduction

WIRELESS power transfer has been envisaged as a promising solution to fulfill the ever-increasing demand for energy in the fifth-generation (5G) and beyond wireless networks, since it can harvest energy from the radio frequency signals without relying on the location or the climate [1]. On the other hand, security is another important issue in wireless communications, due to the broadcasting nature of wireless medium. In particular, the decentralized modern wireless networks have introduced significant challenges to traditional key-based cryptographic techniques, such as key generation, distribution, and management. To tackle this problem, physical layer security [2] has been proposed as an alternative for cryptographic techniques, since it can achieve the information-theoretic secure communications without using secret keys.

Recently, wireless powered secure communication has also been receiving an increasing research attention [3]–[5]. In [3], robust beamforming schemes were proposed to maximize the throughput of wireless powered systems with the secrecy constraint, considering that only the imperfect channel state information (CSI) are available at the legitimate system. In [4], the use of artificial noise (AN) was considered to enhance physical layer security in wireless powered systems. The joint design of the power allocation for the AN signals as well as the time fraction between the power transfer (PT) phase and the information transfer (IT) phase under the harvest-then-transmit protocol was examined in [5]. However, these works often require complicated algorithms, which may lead to large latency impact in real-world deployments.

In this letter, we propose a learning-based wireless powered secure transmission, in which we exploit the potential of machine learning in rapidly configuring the wireless powered systems so as to maximize the effective secrecy throughput (EST). In fact, machine learning has been shown to be effective in many wireless network applications with secrecy constraints, such as anti-jamming [6] and secure transmit antenna selection [7]. Compared to these works (e.g., [6] and [7]), our contributions are summarized as follows. First, we focus on the scenario of the wireless powered secure transmission, and characterize the impacts of various transmission parameters on the EST. Second, we show how the deep feedforward neural network (DFNN) can be utilized to efficiently determine the optimal transmission parameters that maximize the EST.

II. System Model and Problem Formulation

We consider a wireless powered secure communication system, which consists of a power beacon (PB), a source (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve). In this system, Alice utilizes energy collected from PB to communicate with Bob in the presence of Eve. We consider that Alice is equipped with N_a antennas, while PB, Bob, and Eve are all equipped with a single antenna. We assume that the CSI between PB and Alice and the CSI between Alice and Bob are perfectly known at PB and Alice, respectively, while only statistical information on Eve's channel is available to the legitimate nodes. We also assume that all the channels are subject to identical and independent distributed (i.i.d) Rayleigh fading. We denote $\mathbf{h}_{ij}$ and d_{ij} as the channel and distance between node i, $i \in \{p, a\}$, and node j, $j \in \{a, b, e\}$, respectively.

A. Wireless Powered Secure Transmission

We now detail the wireless powered secure transmission considered in this letter. The transmission between Alice and Bob consists of two phases, namely, the PT phase and the IT phase. In the PT phase, Alice harvests energy from PB, and

Manuscript received October 3, 2018; accepted November 14, 2018. Date of publication November 19, 2018; date of current version April 9, 2019. This work was supported in part by the China Scholarship Council ([2017] 3109) and in part by the National Natural Science Foundation of China under Grant 61471037, Grant 61771048, and Grant 61201181. The associate editor coordinating the review of this paper and approving it for publication was L. P. Natarajan. *(Corresponding author: Chenxi Liu.)*

D. He and H. Wang are with the School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China (e-mail: hdxbit@bit.edu.cn; wanghua@bit.edu.cn).

C. Liu and T. Q. S. Quek are with the Information Systems Technology and Design Pillar, Singapore University of Technology and Design, Singapore 487372 (e-mail: chenxi_liu@sutd.edu.sg; tonyquek@sutd.edu.sg).

Digital Object Identifier 10.1109/LWC.2018.2881976

then utilizes all the energy harvested in the PT phase to communicate with Bob in the IT phase. We denote τ as the fraction of time allocated to the PT phase. As such, the available transmit power at Alice in the IT phase can be expressed as

$$P_a = \varphi \hat{P}, \tag{1}$$

where $\varphi = \frac{\tau}{(1-\tau)}$, $\hat{P} = \xi P d_{pa}^{-\eta} |\mathbf{h}_{pa}|^2$, $0 < \xi < 1$ denotes the energy harvest efficiency at Alice, P denotes the transmit power at PB, and η denotes the path loss exponent.

In the IT phase, we assume that Alice transmits the AN signals, in addition to the information signals, in order to confuse the eavesdropper. As such, we express the transmitted signal at Alice as

$$\mathbf{x}_{\mathrm{s}} = \mathbf{w} t_{\mathrm{s}} + \mathbf{G}\mathbf{t}_{\mathrm{san}}, \tag{2}$$

where $\mathbf{w}$ and $\mathbf{G}$ denote the $N_a \times 1$ beamforming vector used to transmit the information signal t_{s} and the $N_a \times (N_a - 1)$ beamforming matrix used to transmit the AN signal $\mathbf{t}_{\mathrm{san}}$, respectively. In order to degrade the quality of the received signal at Eve, while maintaining the quality of the received signal at Alice, we choose $\mathbf{w} = \frac{\mathbf{h}_{ab}^{\dagger}}{\|\mathbf{h}_{ab}\|}$ and $\mathbf{G}$ as the projection matrix onto the null space of $\mathbf{h}_{ab}$, respectively [8], [9]. As such, we have $\mathbf{h}_{ab}\mathbf{G} = \mathbf{0}$, and $\mathbf{w}$ and the columns of $\mathbf{G}$ form an orthonormal basis. In addition, we denote α as the fraction of power allocated to the information signals. As such, we have $\mathbb{E}[|t_{\mathrm{s}}|^2] = \alpha P_a$ and $\mathbb{E}[\mathbf{t}_{\mathrm{san}}\mathbf{t}_{\mathrm{san}}^{\dagger}] = \frac{(1-\alpha)P_a}{N_a-1}\mathbf{I}_{N_a-1}$.

Based on (1) and (2), we express the received signal-to-interference-plus-noise ratios (SINRs) at Bob and Eve in the IT phase, respectively, as

$$\gamma_b = \alpha\varphi\overline{\gamma}_b |\mathbf{h}_{ab}|^2, \tag{3}$$

$$\gamma_e = \frac{\alpha\varphi\overline{\gamma}_e |\mathbf{h}_{ae}\mathbf{w}|^2}{\frac{1-\alpha}{N_a-1}\varphi\overline{\gamma}_e \|\mathbf{h}_{ae}\mathbf{G}\|^2 + 1}, \tag{4}$$

where $\overline{\gamma}_b = \hat{P} d_{ab}^{-\eta}/\sigma_b^2$, $\overline{\gamma}_e = \hat{P} d_{ae}^{-\eta}/\sigma_e^2$, σ_b^2 and σ_e^2 denote the variance of the additive white Gaussian noise at Bob and Eve, respectively. According to (3) and (4), the secrecy capacity of our system is expressed as

$$C_s = \{C_b - C_e\}^+, \tag{5}$$

where $\{\cdot\}^+$ denotes $\max\{0, \cdot\}$, $C_b = \log_2(1+\gamma_b)$ and $C_e = \log_2(1+\gamma_e)$ denote the capacity of Bob's channel and the capacity of Eve's channel, respectively.

B. Problem Formulation

In this letter, we employ the well-known Wyner's wiretap code [2] with the parameter pair (R_b, R_e) to perform secure transmissions, where R_b denotes the transmission rate of the wiretap code and R_e denotes the redundancy rate of the wiretap code, representing the cost of preventing eavesdropping. When $R_b > C_b$, the transmitted signal from Alice cannot be reliably decoded at Bob, and the transmission outage occurs. When $R_e \leq C_e$, the information on the transmitted signal is leaked to Eve, and the secrecy outage occurs. Since we assume that $\mathbf{h}_{ab}$ is perfectly known at Alice, we can set $R_b = C_b$. As such, with the aid of [8], the secrecy outage probability of our system can be derived as

$$\begin{aligned} P_{so}(\tau, \alpha, R_e) &= \Pr(\gamma_e > \kappa_e) \\ &= \left(1 + \frac{(1-\alpha)\kappa_e}{\alpha(N_a-1)}\right)^{-(N_a-1)} e^{-\frac{\kappa_e}{\alpha\varphi\overline{\gamma}_e}}, \end{aligned} \tag{6}$$

where $\kappa_e = 2^{R_e} - 1$.

In order to evaluate the secrecy performance of our system, we adopt the modified EST [8], [9] as the performance metric, given by

$$T_s(\tau, \alpha, R_e) = (1-\tau)(R_b - R_e)(1 - P_{so}(\tau, \alpha, R_e)). \tag{7}$$

We can see that the EST in (7) is a function of the fraction of the time allocated to the PT phase τ, the fraction of power allocated to the information signals α, as well as the redundancy rate of the wiretap code R_e. The key goal of this letter is to find the optimal transmission parameter tuple $(\tau^*, \alpha^*, R_e^*)$ that achieves the maximum EST T_s^* per transmission block. Mathematically, this problem can be formulated as

$$\max_{\tau,\alpha,R_e} \quad T_s(\tau, \alpha, R_e), \tag{8a}$$

$$\text{s.t. } 0 < \tau < 1, 0 < \alpha \leq 1, 0 < R_e \leq R_b. \tag{8b}$$

However, the maximization problem in (8) is non-convex. Therefore, it is difficult to analytically obtain the optimal transmission parameter tuple $(\tau^*, \alpha^*, R_e^*)$. Traditionally, (8) can be solved numerically via an exhaustive search, but requiring a high computational complexity. To tackle this problem, we propose a learning-based scheme that is capable of solving (8) in a far more efficient way compared to the exhaustive search.[1]

III. Proposed Learning-Based Scheme

In this section, we present details on our proposed learning-based scheme that solves (8) efficiently.[2] Specifically, we utilize the DFNN to learn the nonlinear mapping from $\mathbf{h}_{ab}$ to the optimal transmission parameter tuple $(\tau^*, \alpha^*, R_e^*)$ that achieves the maximum EST, which can be expressed as

$$(\tau^*, \alpha^*, R_e^*) = f^*(\mathbf{h}_{ab}). \tag{9}$$

We note that the DFNN has shown to be effective in approximating any measurable function to any desired degree of accuracy [11], and thus is an appropriate method to solve (8).[3]

[1]Note that in practice the choice of transmission parameters is finite. We will show in Section IV that, even in such scenarios, our proposed learning-based scheme still outperforms the exhaustive search in terms of the computational complexity.

[2]Besides wireless powered communication systems, our learning-based scheme can also be applied to enhance the security of various communication systems. For example, in secure communication systems with the cooperative jammers (as in [10]), the proposed learning-based scheme can be utilized to determine the optimal power allocation at the cooperative jammers that maximizes the secrecy rate.

[3]We note that the curve fitting method can also be applied to approximate the mapping from $\mathbf{h}_{ab}$ to $(\tau^*, \alpha^*, R_e^*)$. However, it may not achieve the same degree of accuracy as our proposed learning-based scheme.

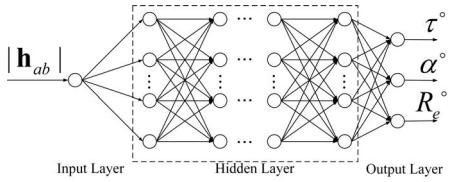


Fig. 1. The structure of the DFNN.

A. Deep Feedforward Neural Network

As shown in Fig. 1, our adopted DFNN consists of three layers, i.e., the input layer, the hidden layer, and the output layer. Specifically, we choose $|\mathbf{h}_{ab}|$ as the input of our DFNN since the input of the neural network must be a real-valued scalar or vector [12]. We also choose $(\tau^\circ, \alpha^\circ, R_e^\circ)$ as the output of our DFNN. We note that there are typically multiple layers in the hidden layer, and the output of one layer is the input of the sequential layer. As such, the output of the *i*-th layer in the hidden layer can be expressed as

$$\mathbf{x}_i = g(\mathbf{W}_i \mathbf{x}_{i-1} + \mathbf{b}_i), \tag{10}$$

where $g(z)$ denotes the activation function of the hidden layer, $\mathbf{W}_i$ and $\mathbf{b}_i$ denote the weight matrix and the bias of the *i*-th layer, respectively. In this letter, we choose the rectified linear unit [13] as the activation function, given by $g(z) = \max\{0, z\}$.

We denote l as the depth of the hidden layer and $\mathbf{W} = [\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_l]$. Then, the mapping relationship between $|\mathbf{h}_{ab}|$ and $(\tau^\circ, \alpha^\circ, R_e^\circ)$ can be expressed as

$$(\tau^\circ, \alpha^\circ, R_e^\circ) = f(|\mathbf{h}_{ab}|, \mathbf{W}). \tag{11}$$

Note that $f(|\mathbf{h}_{ab}|, \mathbf{W})$ in (11) is different from $f^*(\mathbf{h}_{ab})$ in (9). In this letter, the target of our DFNN is to train $\mathbf{W}$ such that $f(|\mathbf{h}_{ab}|, \mathbf{W})$ approaches $f^*(\mathbf{h}_{ab})$. To this end, we adopt the mean squared error (MSE) as the learning performance metric [12]. As such, a well-trained $\mathbf{W}$ should satisfy the following constraint

$$J(\mathbf{W}) = \mathbb{E}_{\mathbf{h}_{ab}}\Big(|f(|\mathbf{h}_{ab}|, \mathbf{W}) - f^*(\mathbf{h}_{ab})|^2\Big) \leq \epsilon. \tag{12}$$

where ϵ denotes the target training error.

B. Training of DFNN

We now detail how our DFNN can be trained to obtain the optimal transmission parameter tuple $(\tau^*, \alpha^*, R_e^*)$ that maximizes the EST of our system. Specifically, the training process of DFNN is performed through two steps: 1) Generate the training set and 2) Use the generated training set to train the DFNN such that $\mathbf{W}$ satisfying (12) is obtained.

1) Training Set Generation: In this step, we generate the training set of *M* training examples. Each training example consists of the channel gain and the corresponding optimal transmission parameter tuple, given by $\mathcal{S}_m = \{|\mathbf{h}_{ab,m}| \rightarrow (\tau_m^*, \alpha_m^*, R_{e,m}^*)\}$, where $m = 1, \ldots, M$. We note that $(\tau_m^*, \alpha_m^*, R_{e,m}^*)$ for each $\mathbf{h}_{ab,m}$ is obtained through the exhaustive search.

2) Training of W: In this step, we use the generated training set $\mathcal{S} = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_M\}$ to train the DFNN such that the weight matrix $\mathbf{W}$ satisfies the constraint in (12). To this end, we adopt the Levenberg-Marquardt method [14], which is suitable for training the neural network when the learning performance metric is the sum of squares of nonlinear functions, to iteratively update $\mathbf{W}$. As such, $\mathbf{W}$ in the $(k+1)$-th update can be expressed as

$$\mathbf{W}^{k+1} = \mathbf{W}^k - \frac{1}{2\mu_k} \nabla F\Big(\mathbf{W}^k\Big), \tag{13}$$

where μ_k is the training parameter and

$$\nabla F\Big(\mathbf{W}^k\Big) = 2\mathbf{J}\Big(\mathbf{W}^k\Big)\mathbf{e}\Big(\mathbf{W}^k\Big). \tag{14}$$

In (14), $\mathbf{J}(\cdot)$ denotes the Jacobian matrix and $\mathbf{e}(\mathbf{W}^k) = [e_1(\mathbf{W}^k), e_2(\mathbf{W}^k), \ldots, e_M(\mathbf{W}^k)]$, where $e_m(\mathbf{W}^k) = |f(|\mathbf{h}_{ab,m}|, \mathbf{W}^k) - f^*(\mathbf{h}_{ab,m})|$.

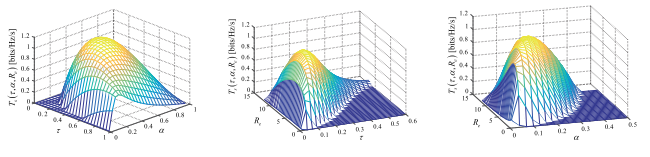
We keep updating $\mathbf{W}$ until the constraint in (12) is satisfied. Then, we can utilize the trained DFNN to determine the optimal transmission parameters that maximize the EST. Specifically, we use a new channel gain $|\mathbf{h}_{ab}|$ as the input of the trained DFNN, then the optimal transmission parameter tuple $(\tau^*, \alpha^*, R_e^*)$ that maximizes the EST can be directly obtained from the output of the DFNN.

IV. Numerical Results

In this section, we present numerical results to validate the effectiveness of our proposed learning-based scheme. Specifically, we first examine the impact of transmission parameters (i.e., τ, α, and R_e) on the EST of our system. We then compare the secrecy performance achieved by our proposed learning-based scheme with that of the optimal solution obtained from the exhaustive search. Finally, we examine the computational demands required by our proposed learning-based scheme and the exhaustive search.

In Fig. 2, we plot $T_s(\tau, \alpha, R_e)$ versus the transmission parameters for $\overline{\gamma}_b = \overline{\gamma}_e = 10$ dB for a realization of $\mathbf{h}_{ab}$. The curves in Fig. 2(a)–2(c) are generated from (7). Fig. 2(a) shows the impacts of τ and α on $T_s(\tau, \alpha, R_e)$ when the optimal R_e^* is selected. We can see that $T_s(\tau, \alpha, R_e)$ first increases then decreases as τ (or α) increases for a given α (or τ), and there is a unique (τ, α) that maximizes $T_s(\tau, \alpha, R_e)$. The same behavior can be observed when examining the impacts of (τ, R_e) and (α, R_e) on $T_s(\tau, \alpha, R_e)$ in Fig. 2(b) and Fig. 2(c), respectively. This demonstrates that there is a unique $(\tau^*, \alpha^*, R_e^*)$ that maximizes $T_s(\tau, \alpha, R_e)$ for each realization of $\mathbf{h}_{ab}$.

In Fig. 3, we plot the average maximum EST, denoted by $\overline{T}_s = \mathbb{E}_{\mathbf{h}_{ab}}[T_s(\tau^*, \alpha^*, R_e^*)]$, versus $\overline{\gamma}_b$ for different values of N_a with the optimal transmission parameter tuple $(\tau^*, \alpha^*, R_e^*)$ being selected for each realization of $\mathbf{h}_{ab}$. In this figure, we consider two schemes, namely, our proposed learning-based scheme and the optimal solution obtained from the exhaustive search. For our proposed learning-based scheme, we use $M = 10^3$ training examples to train the DFNNs. To examine the impact of the depth of the hidden layer (denoted by l) on the performance of the proposed learning-based scheme, we consider three DFNNs with $l = 2$, 4, and 6, respectively. The number of neurons in the hidden layers of these DFNNs is (10, 10), (10, 10, 5, 5), and (10, 10, 10, 10, 5, 5), respectively. We see that, for all the values of N_a, the secrecy



(a) $T_s(\tau, \alpha, R_e)$ versus τ and α for $R_e = R_e^*$. (b) $T_s(\tau, \alpha, R_e)$ versus τ and R_e for $\alpha = \alpha^*$. (c) $T_s(\tau, \alpha, R_e)$ versus α and R_e for $\tau = \tau^*$.

Fig. 2. T_s versus the transmission parameters for $\overline{\gamma}_b = \overline{\gamma}_e = 10$ dB.

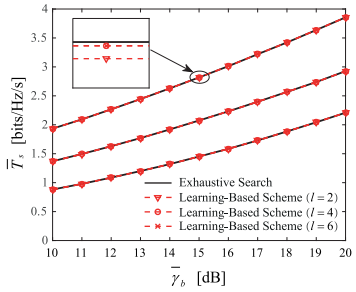


Fig. 3. $\overline{T}_s$ versus $\overline{\gamma}_b$ for different values of N_a.

performance achieved by our proposed learning-based scheme is almost the same as that of the optimal solution obtained from the exhaustive search, demonstrating the effectiveness of our proposed learning-based scheme. We also see that, the DFNN with $l = 2$ achieves a worse performance than the DFNN with $l = 4$, while the DFNN with $l = 6$ achieves almost the same performance as the DFNN with $l = 4$. This indicates that our learning-based scheme can achieve a better trade-off between the performance and the complexity by selecting hyperparameters.

Finally, we evaluate the computational demands of different schemes in Table I.[4] Specifically, we first compare the computational complexities of our proposed learning-based scheme and the exhaustive search. To this end, we define $N_\tau = 1/\delta_\tau$, $N_\alpha = 1/\delta_\alpha$, and $N_R = R_b/\delta_R$, where δ_τ, δ_α, and δ_R denote the search step size for τ, α, and R_e, respectively. We find that the computational complexity of our learning-based scheme (i.e., $\mathcal{O}(1)$) is significantly less than that of the exhaustive search (i.e., $\mathcal{O}(N_\tau N_\alpha N_R)$). This is because a well-trained DFNN only needs finite steps of calculation to obtain the optimal transmission parameter tuple $(\tau^*, \alpha^*, R_e^*)$, while the exhaustive search needs to go through every point in the search space. This finding can be verified by the running times of our learning-based scheme and the exhaustive search on MATLAB on a 6-core 64-bit 2.5 GHz Intel E5-2640 microprocessor with the target training error $\epsilon = 10^{-7}$ and the search step size $\delta_\tau = \delta_\alpha = \delta_R = 10^{-2}$. We see that the running time of our learning-based scheme for a realization of $\mathbf{h}_{ab}$ is much less than that of the exhaustive search for all the values of N_a. We also see that the running time of the exhaustive search increases as N_a increases, while the running time of our learning-based scheme remains relatively the same when N_a varies. These observations indicate that our learning-based scheme can be performed in real-time with negligible latency impact, while the exhaustive search is not practical in real-world deployments.

[4]Since the training phase of our learning-based scheme is completed offline, its computational demands are not included in this table.

TABLE I
COMPLEXITIES AND RUNNING TIMES OF DIFFERENT SCHEMES

	Learning-Based Scheme	Exhaustive Search
	$\mathcal{O}(1)$	$\mathcal{O}(N_\tau N_\alpha N_R)$
$N_s = 2$	1.35×10^{-2} s	4.38 s
$N_s = 3$	1.37×10^{-2} s	5.18 s
$N_s = 4$	1.38×10^{-2} s	5.58 s

V. CONCLUSION

In this letter, we proposed a learning-based wireless powered secure transmission, where the source uses energy collected from a power beacon to communicate with a legitimate receiver, in the presence of an eavesdropper. In our scheme, we assumed that the source transmits the AN signals together with the information signals to confuse the eavesdropper. We characterized the EST of our system, and showed how the EST can be maximized by judiciously selecting the transmission parameters. Furthermore, we exploited the DFNN to learn the nonlinear mapping from Bob's CSI to the optimal transmission parameters that maximize the EST. Compared to the optimal solution obtained from the exhaustive search, we showed that our proposed learning-based scheme can deliver almost the same secrecy performance with much less computational complexity.

REFERENCES

[1] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 117–125, Apr. 2015.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[3] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.
[4] H. Xing, K.-K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 7971–7984, Dec. 2016.
[5] C. Guo, B. Liao, D. Feng, C. He, and X. Ma, "Minimum secrecy throughput maximization in wireless powered secure communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2571–2581, Mar. 2018.
[6] L. Xiao, Y. Li, C. Dai, H. Dai, and H. V. Poor, "Reinforcement learning-based NOMA power allocation in the presence of smart jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3377–3389, Apr. 2018.
[7] D. He, C. Liu, T. Q. S. Quek, and H. Wang, "Transmit antenna selection in MIMO wiretap channels: A machine learning approach," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 634–637, Aug. 2018.
[8] N. Yang *et al.*, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
[9] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.
[10] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495–7505, Aug. 2017.
[11] K. Hornik, M. Stinchcombe, and H. White, "Multilayer feedforward networks are universal approximators," *Neural Netw.*, vol. 2, no. 5, pp. 359–366, 1989.
[12] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
[13] V. Nair and G. E. Hinton, "Rectified linear units improve restricted Boltzmann machines," in *Proc. ICML*, Haifa, Israel, Jun. 2010, pp. 807–814.
[14] M. T. Hagan, H. B. Demuth, and M. Beale, *Neural Network Design*. Boston, MA, USA: PWS, 1995.