Received 4 March 2024; accepted 21 March 2024. Date of publication 27 March 2024; date of current version 18 April 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3381951

Deep Learning Aided Secure Transmission in Wirelessly Powered Untrusted Relaying in the Face of Hardware Impairments

VAHID SHAHIRI[1], MOSLEM FOROUZESH[2], HAMID BEHROOZI[1] (Member, IEEE), ALI KUHESTANI[3] (Member, IEEE), AND KAI-KIT WONG[4] (Fellow, IEEE)

[1]Electrical Engineering Department, Sharif University of Technology, Tehran 1458889694, Iran

[2]Faculty of Engineering Technology, Amol University of Special Modern Technologies, Amol 4615664616, Iran

[3]Electrical and Computer Engineering Department, Qom University of Technology, Qom 3718146645, Iran

[4]Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, U.K.

CORRESPONDING AUTHOR: A. KUHESTANI (e-mail: kuhestani@qut.ac.ir).

The work of Ali Kuhestani was supported in part by the INSF under Grant 4022393.

ABSTRACT Limited power and computational resources make the employment of complex classical encryption schemes unrealistic in resource-limited networks, e.g., the Internet of Things (IoT). To this end, physical layer security (PLS) has shown great potential in securing such resource-limited networks. To further combat the power scarcity in IoT nodes, radio frequency (RF) based energy harvesting (EH) is an attractive energy source while relaying can enhance the energy efficiency and extend the range of data transmission. Additionally, due to deploying low-cost hardware, imperfections in the RF chain of IoT transceivers are common. Against this background, in this paper, we investigate an untrusted EH relay-aided secure communication with RF impairments. Specifically, the relay simultaneously receives the desired signal from the source and the jamming from the destination in the first phase. Hence the relay is unable to extract the confidential desired signal. The resultant composite signal is then amplified by the relay in the second phase by using the energy harvested from the composite signal followed by its transmission to the destination. Since the destination is the original source of the jamming, its effect can be readily subtracted from the composite signal to recover the original desired signal of the source. Moreover, in the face of hardware impairments (HWIs) in all nodes, maintaining optimal power management both at the source and destination may impose excessive computations on an IoT node. We solve this problem by deep learning (DL) based optimal power management maximizing the secrecy rate based on the instantaneous channel coefficients. We show that our learning-based scheme can reach the accuracy of the exhaustive search method despite its considerably lower computational complexity. Moreover, we developed an optimization framework for judiciously sharing HWIs across the nodes, so that we attain the maximum secrecy rate. To derive an efficient solution, we utilize a majorization-minimization (MM) algorithm, which is a particular instance in the family of successive convex approximation (SCA) methods. The simulation results show that the proposed HWI aware design considerably improves the secrecy rate.

INDEX TERMS Deep learning, energy harvesting, hardware impairments, majorization-minimization, physical layer security, untrusted relaying.

I. INTRODUCTION

THE POTENTIAL of the Internet of Things (IoT) in revolutionizing smart cities, healthcare, transportation, etc. is widely acknowledged. However, providing connectivity among numerous wireless devices on a massive scale faces significant challenges [1], [2]. To be specific, acquiring a

permanent power source for these devices is not viable, e.g., due to their mobility, hence they tend to depend on batteries. Moreover, frequent recharging and battery replacement would be inappropriate in most applications such as in toxic environments or wireless body area networks, where medical devices are implanted into a patient's body [3]. Accordingly, we have to acquire a sustainable energy source for IoT devices. Another issue is that of the hardware quality in these networks. As the massive deployment of devices is required in most IoT applications, utilizing nodes relying on low-cost hardware becomes inevitable. This leads to relatively high imperfections in the RF chain of the IoT nodes [4]. Another challenge is in the realms of security. Classical encryption schemes are computationally demanding [5] and do not fit well into the low energy-dissipation requirements of IoT devices. Physical layer security (PLS) techniques rely on low-complexity security protocols which fit well into IoT networks [6], [7], [8]. Additionally, the implementation of complex optimization algorithms is quite a challenge owing to the limited resources of IoT networks [9]. Moreover, artificial intelligence (AI) methods, particularly deep learning (DL), are eminently suitable for low-complexity near-real-time resource allocation [10], [11]. In this contribution, we design a security protocol for tackling the aforementioned challenges.

Energy harvesting (EH) is capable of extending the lifetime of energy-constrained wireless nodes [12]. This technique gleans energy from the surrounding radio frequency (RF) signals to recharge the batteries [13], [14]. Very recently, EH applications were studied in numerous use cases, e.g., reconfigurable intelligent surfaces (RIS) [15], multiple input multiple output (MIMO) communications [16], distributed antenna systems [17], relay networks [18], etc. Moreover, in the context of PLS, numerous studies have simultaneously considered the security and energy efficiency of IoT nodes [3], [19], [20], [21]. Specifically, the authors of [3] considered a simultaneous wireless information and power transfer-based (SWIPT-based) amplify and forward (AF) relaying scenario in the presence of an eavesdropper. The relay harvests energy both from the transmitted RF signals of the source and from friendly jammers to glean sufficient power. In [19], the optimal power sharing factor between the source and destination is obtained by maximizing the secrecy rate in a wireless-powered untrusted relaying network, where the untrusted relay is exposed to destination-based jamming. Furthermore, the authors of [20] proposed a wireless-powered two-way cooperative network, wherein the two sources communicate via a wireless-powered untrusted relay. To boost the secrecy performance, an external jammer was relied upon, which was also wirelessly charged by the two sources. In [21], the IoT nodes first harvested energy from the hybrid sink (H-sink) and then transmitted the information to the H-sink and generated interference to confuse the eavesdropper. The sum-throughput maximization problem was formulated to allocate the optimum power to each of the nodes.

In realistic digital communication systems, practical impairments, such as I/Q imbalance, phase noise, amplifier nonlinearities, quantization errors and non-ideal filters inevitably degrade the system performance [22], [23], [24]. Naturally, the level of residual hardware impairments (HWIs) is determined by the quality of the RF transceivers as well as by the analog and digital signal processing techniques adopted [24]. For the sake of analytical tractability, the HWIs may be modeled by additive noise at the transmitter and receiver nodes [22], [23]. This model was confirmed by experiments and it is extensively applied in various use cases in the literature to model the impact of the residual HWIs [25], [26], [27], [28], [29]. Based on this model, several studies have examined the impact of HWIs on the security of diverse communication networks [30], [31], [32], [33], [34]. To be specific, the authors of [30] considered the residual HWIs in a dual-hop untrusted relaying network. Furthermore, the authors of [31] studied a three-hop untrusted relaying network in the presence of HWIs and imperfect channel estimation. Additionally, the authors of [32] have studied physical layer secret key generation (SKG) in direct source-to-destination communication in the presence of a man-in-the-middle adversary, where the legitimate users suffer from HWIs. The same authors [33] also adopted the concept of recurrent neural networks to compensate the HWIs at the legitimate transceivers. Furthermore, in [34], a source intends to transmit its confidential information to a destination in the presence of a group of untrusted AF relays. All the nodes are assumed to have residual HWIs in their transceiver chains, except for the eavesdropper. A sophisticated joint cooperative beamforming, jamming and power allocation policy was proposed to safeguard the confidential information.

DL provides unique advantages in numerous areas, including security. Accordingly, researchers are seeking DL solutions for employment in resource-limited mobile and IoT devices [35]. Some recent PLS studies exploit the ability of deep neural networks (DNNs) to approximate continuous functions for solving resource allocation problems, which are usually non-convex [36], [37], [38], [39], [40], [42], [43]. Specifically, in [36], [37], [38], a transmit power control (TPC) regime was designed for maximizing the system's secrecy rate. An unsupervised DL-assisted approach is proposed for reducing the complexity of the conventional optimization-based techniques and for circumventing their performance erosion due to approximations. EH is also considered in these studies, while the authors of [36] and [38] also take into account the deleterious effects of imperfect channel state information (CSI). Furthermore, the quality-of-security violation probability (QVP) experienced in image transmission is minimized in [39] by utilizing a fully-connected feedforward DNN. The optimal values of the power allocation ratio, the transmit power, the decision threshold on whether to send public or confidential packets and the transmission rate are determined by the DNN. The

authors of [40] leverage a deep feedforward neural network to obtain the optimal fraction of power allocated to the information signal, the redundancy rate and power transfer time that jointly maximize the effective secrecy throughput in a wireless-powered system. The security versus reliability trade-off is considered in [41]. Optimum power allocation coefficient for information and artificial noise power ratio is determined using a feedforward DNN. Additionally, the authors of [42] study a transmit antenna selection (TAS) scheme based on feedforward DNNs in untrusted relay networks. Finally, the authors of [43] propose a specific fully-connected DNN to obtain the optimal precoding matrix, which maximized the secrecy rate in a MIMO Gaussian Wiretap Channel.

Against this background, in this paper, we consider two legitimate nodes in which the source, $\mathcal{S}$, wants to send its confidential information to the destination, $\mathcal{D}$, with the aid of an amplify and forward (AF) relay, $\mathcal{R}$. The relay is powered by the signals gleaned from the environment and it is also assumed to be curious about the information sent from $\mathcal{S}$. Hence $\mathcal{D}$ aims for preventing $\mathcal{R}$ from obtaining the confidential signal by sending jamming during the reception phase of the untrusted relay $\mathcal{R}$. Accordingly, $\mathcal{R}$ simultaneously receives the desired signal from $\mathcal{S}$ and the jamming from $\mathcal{D}$ in the first phase. Hence $\mathcal{R}$ is unable to extract the confidential desired signal. The resultant composite signal is then amplified by $\mathcal{R}$ in the second phase using the energy harvested from the composite signal, followed by its transmission to $\mathcal{D}$. Since $\mathcal{D}$ is the original source of the jamming, its effect can be readily subtracted from the composite signal to recover the original desired signal of the source. Although the energy efficiency of the system suffers, because $\mathcal{D}$ has to dissipate power for jamming transmission and cancellation, this solution assists distant destinations in improving both their reception integrity and confidentiality. Furthermore, we take into account the HWIs of all three nodes. Seeking a light-weight optimization approach, we aim for exploiting the potential of DL in obtaining the optimum power allocation for this scenario.The main contributions of this paper are boldly and explicitly contrasted to the literature in Table 1 and are summarized as follows:

- We first calculate the instantaneous secrecy rate and formulate a secrecy rate optimization problem subject to the individual power constraints of the nodes. We then design a deep neural network (DNN) for addressing the optimization problem formulated. By exploiting the potential of deep learning, we are able to promptly configure the power allocation factors at $\mathcal{S}$ and $\mathcal{D}$ based on the changes in the $\mathcal{S}-\mathcal{R}$ and $\mathcal{R}-\mathcal{D}$ links. Our simulation results show that the proposed deep network approaches the accuracy of the exhaustive search method, despite its substantially reduced complexity.
- To provide further insights on how the available power budget at $\mathcal{S}$ and $\mathcal{D}$ impacts the system model considered, we derive analytical results at high SNRs. Furthermore we discuss the rationale behind our optimal power management problem and discuss the special case in which the secrecy rate becomes equal to zero.
- We develop an optimization framework for finding the optimal sharing of the total HWIs among the nodes for maximizing the secrecy rate. To overcome the non-convexity of this problem, we derive a low-complexity algorithm based on the popular majorization-minimization (MM) method for improving the secrecy rate.
- To gain further insights, a detailed discussion is presented concerning both the impact of HWIs, as well as the energy efficiency and the available power budget at $\mathcal{S}$ and $\mathcal{D}$ on the overall secrecy rate. The impact of these parameters on the power allocation problem considered is also studied in detail.

TABLE 1. Contrasting our contributions to the state-of-the art.

Contributions	**This work**	[36]	[37]	[38]	[39]	[40]	[42]
Untrusted EH Relay	✓						
Hardware Design	✓						
DL-based PLS	✓	✓	✓	✓	✓	✓	✓

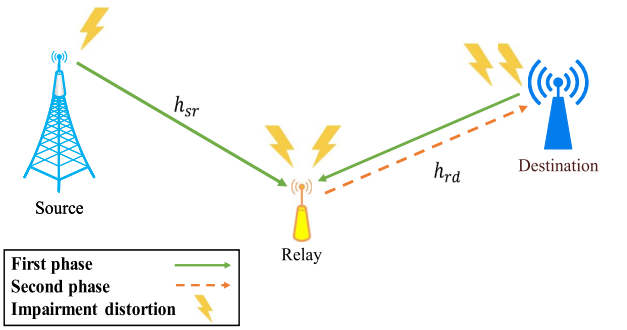


FIGURE 1. System model: An untrusted energy harvesting relay conveys the source signal to the destination in the face of hardware impairments. The destination exploits jamming to disturb the signal reception at the untrusted relay.

The remainder of this paper is organized as follows. In Section II, we introduce our system model and problem formulation. In Section III, we define our approach to solving the optimal power allocation problem by utilizing DL. Accordingly, the structure of our training and test data, activation functions and the loss function are described in detail. To gain further insights, in Section IV, we derive high-SNR expressions of the instantaneous secrecy rate. Based on high-SNR results of Section IV, in Section V, a HWI allocation problem is formulated and solved by applying the MM technique. Finally, in Section VI, our discussions and numerical results are presented, while our conclusions are offered in Section VII.

II. SYSTEM MODEL

We investigate the EH-aided untrusted relay network of Fig. 1, which consists of a source, a destination, and an untrusted AF relay. All the nodes are equipped with a

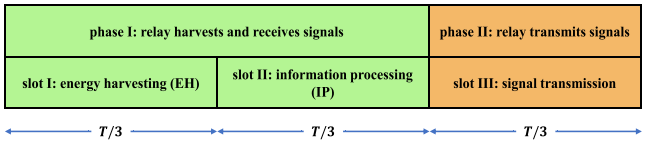


FIGURE 2. Slot allocation for time switching (TS) based energy harvesting in the proposed system model.

single antenna. The transmission is performed in two phases within the time T. In the first phase, the source transmits confidential data to the untrusted relay. Furthermore, to confuse the untrusted relay in this phase, the destination simultaneously emits a jamming signal. In the second phase, the untrusted relay amplifies and retransmits the signal received in the previous phase. Note that the untrusted relay is an essential partner in the proposed system model, but it may also act similar to an eavesdropper and extract confidential data without any permission from the network. Moreover, the untrusted relay considered is able to harvest energy from the signals received in the first phase and consumes it in the second phase. This capability leads to its sustained communication without high-energy batteries. We note that the considered system is equivalent to an IoT sensor (source) which intends to send its sensory data to a central node (destination) with the aid of a third node which acts as a relay and can not be trusted.

Remark 1: Energy harvesting and information transmission have to be appropriately scheduled. In this regard, SWIPT transmission techniques include the time, power, antenna and spatial domains [13]. Here, we consider the time switching (TS) method. As shown in Fig. 2, in this method, the first phase is split into two slots. In the first slot which lasts for $T/3$ seconds, the relay harvests energy from the transmitted signals of source and destination. The second slot is for information processing (IP) which again has the duration of $T/3$. Finally, in the second phase and during the time of $T/3$, the relay transmits the received signal with the harvested energy in the first phase.

Because of the obstacles between the source and destination, the direct link is not available. It is assumed that reciprocity is satisfied by the system model considered. The channels spanning from the source to relay and relay to destination are complex-valued Gaussian with a distribution of $h_{sr} \sim \mathcal{CN}(0, \upsilon_{sr})$ and $h_{rd} \sim \mathcal{CN}(0, \upsilon_{rd})$, respectively. The HWIs in node i (source, relay, destination) are expressed as ξ_i^t and ξ_i^r for the transmission and reception modes, respectively, which are defined as [23]

$$\begin{aligned}
&\xi_S^t \sim \mathcal{CN}\Big(0, p_s {k_S^t}^2\Big), \xi_D^t \sim \mathcal{CN}\Big(0, p_d {k_D^t}^2\Big),\\
&\xi_D^r \sim \mathcal{CN}\Big(0, p_r |h_{rd}|^2 {k_D^r}^2\Big), \xi_R^t \sim \mathcal{CN}\Big(0, p_r {k_R^t}^2\Big),\\
&\xi_R^r \sim \mathcal{CN}\Big(0, {k_R^r}^2\Big(p_s |h_{sr}|^2 + p_d |h_{rd}|^2\Big)\Big),
\end{aligned} \tag{1}$$

where p_s, p_r, and p_d are the transmit powers at the source, relay, and destination, respectively. Moreover, $k_i^t > 0$ and $k_i^r > 0$ are the level of imperfections at the transmitter and receiver hardware, respectively. Note that the additive white noise at node i, $i \in \{\mathcal{R}, \mathcal{D}\}$ is defined as $n_i \sim \mathcal{CN}(0, \sigma_i^2)$, $i \in \{R, D\}$.

A. ENERGY HARVESTING AT THE UNTRUSTED RELAY

In the TS based energy harvesting, the energy E harvested during the first time slot with duration $T/3$ is equal to [20], [44], [45]

$$E = \lambda \frac{T}{3} \left\| \sqrt{p_s} h_{sr} x_s + \sqrt{p_d} h_{rd} x_d \right\|^2, \tag{2}$$

where $\lambda \in [0, 1]$ is the energy conversion efficiency and x_d and x_s are the jamming and information signals with unit power, respectively. The relay uses this energy to transmit the signal in the second phase with the power of

$$p_r = \frac{E}{T/3} = \lambda \left\| \sqrt{p_s} h_{sr} x_s + \sqrt{p_d} h_{rd} x_d \right\|^2. \tag{3}$$

B. IP AT THE UNTRUSTED RELAY

The signal received at the untrusted relay in the second slot of the first phase is given by

$$y_r = \left(\sqrt{p_s} x_s + \xi_S^t\right) h_{sr} + \left(\sqrt{p_d} x_d + \xi_D^t\right) h_{rd} + \xi_R^r + n_R. \tag{4}$$

The received signal-to-interference-plus-noise-ratio (SINR) at the relay is expressed as

$$\Gamma_R = \frac{p_s |h_{sr}|^2}{p_s |h_{sr}|^2 \left({k_S^t}^2 + {k_R^r}^2\right) + p_d |h_{rd}|^2 \left(1 + {k_D^t}^2 + {k_R^r}^2\right) + \sigma_R^2}. \tag{5}$$

C. SIGNAL FORWARDING

In the second phase, the untrusted relay amplifies the received signal y_r by an amplification factor G and then forwards it to the destination. Explicitly, the relay transmits $x_r = G y_r$, where the amplification factor is defined as

$$G = \sqrt{\frac{p_r}{\|y_r\|^2}}. \tag{6}$$

The signal received at the destination is a combination of the *information signal*, *self interference*, *distortion*, and *thermal noise*. After self-interference cancelation, the signal received at the destination is expressed as

$$\begin{aligned}
y_D = &\underbrace{G \sqrt{p_s} h_{sr} h_{rd} x_s}_{\text{Information signal}}\\
&+ \underbrace{G \xi_S^t h_{sr} h_{rd} + G \xi_D^t h_{rd} h_{rd} + G \xi_R^r h_{rd} + \xi_R^t h_{rd} + \xi_D^r}_{\text{Distortion}}\\
&+ \underbrace{G n_R h_{rd} + n_D}_{\text{noise}}.
\end{aligned} \tag{7}$$

It is worth noting that when the relay aims for transmitting data in the second phase, it completely dissipates the total energy harvested in the previous phase, hence, by considering (3) and (6), we have $G \approx \sqrt{\lambda}$.

Remark 2: We note that the approximation $G \approx \sqrt{\lambda}$ is justified, since the term $\sqrt{p_s}h_{sr}x_s + \sqrt{p_d}h_{rd}x_d$ in p_r is way larger than the impairment and noise terms in (4) for practical networks. Otherwise, the end-to-end SNR would be very low. This assumption is widely used in the related literature [46], [47], [48], [49], [50].

We define $k_{R,D}^{t,r\ 2} = k_R^{t\ 2} + k_D^{r\ 2}$ and after some simplifications, the SINR at the destination is given by

$$\Gamma_D = \frac{p_s|h_{sr}|^2}{B}, \tag{8}$$

where we have

$$\begin{aligned} B = {} & p_s|h_{sr}|^2\left(k_S^{t\ 2} + k_R^{r\ 2} + k_{R,D}^{t,r\ 2} + k_{R,D}^{t,r\ 2}k_S^{t\ 2} + k_{R,D}^{t,r\ 2}k_R^{r\ 2}\right) \\ & + p_d|h_{rd}|^2\left(k_D^{t\ 2} + k_R^{r\ 2} + k_{R,D}^{t,r\ 2} + k_{R,D}^{t,r\ 2}k_D^{t\ 2} + k_{R,D}^{t,r\ 2}k_R^{r\ 2}\right) \\ & + \sigma_R^2\left(1 + k_{R,D}^{t,r\ 2}\right) + \sigma_D^2|h_{rd}|^{-2}\lambda^{-1}. \end{aligned} \tag{9}$$

Therefore, the instantaneous secrecy rate at the destination can be expressed as

$$R_s = \left[\log_2(1+\Gamma_D) - \log_2(1+\Gamma_R)\right]^+, \tag{10}$$

where $[\kappa]^+ = \max(\kappa, 0)$. In this paper, our aim is to maximize the secrecy rate by considering realistic power constraints at the source and destination. Hence, we propose the following optimization problem

$$\max_{p_s,p_d} \quad R_s, \tag{11a}$$

$$\text{s.t.: } 0 \le p_s \le P_s^{\max} \tag{11b}$$

$$0 \le p_d \le P_d^{\max}, \tag{11c}$$

where $P_s^{\max}$ and $P_d^{\max}$ are the maximum transmit power available at the source and destination, respectively.

III. DEEP LEARNING BASED OPTIMAL POWER ALLOCATION

In this section, we intend to propose a DNN based solution to solve the optimal power allocation problem. The optimization problem defined in (11) can be rewritten as

$$\max_{\alpha,\beta} \ R_s, \tag{12a}$$

$$\text{s.t.: } 0 \le \alpha \le 1 \tag{12b}$$

$$0 \le \beta \le 1, \tag{12c}$$

where $\alpha = \frac{p_s}{P_s^{\max}}$ and $\beta = \frac{p_d}{P_d^{\max}}$. The above form will later facilitate the design of the neural network to obtain the optimal solution.

However, the above optimization problem is non-convex and complex, hence it is a challenge to find the optimal power allocation coefficients (α^*, β^*) analytically. On the other hand, solving this problem numerically requires substantial processing power and vast memory. Therefore, motivated by the capability of DNNs to solve complex optimization problems, we intend to solve the above problem using a DNN. The following sections show that utilizing DL to solve this optimization problem will significantly reduce the time required for finding the optimal solution compared to the exhaustive search method, when they have the same processing capability.

The primary goal of neural networks is to estimate complex functions using simple operations of the neurons. Here, we will harness this feature of DNNs to obtain a complex mapping between the channel coefficients (h_{sr}, h_{rd}) and optimal power allocation coefficients (α^*, β^*). The result will eventually be able to maximize the ergodic secrecy rate (ESR). This action can be summarized as follows

$$\left(\alpha^*, \beta^*\right) = \Psi^*(h_{sr}, h_{rd}), \tag{13}$$

where Ψ^* represents the complex mapping from (h_{sr}, h_{rd}) to (α^*, β^*). It should be noted that because the channel exhibits fast fading, the coefficients h_{sr} and h_{rd} of the consecutive coherence time intervals will have different values. As such, for each pair of (h_{sr}, h_{rd}), the optimal values of α^* and β^* will be different. Accordingly, performing exhaustive search for each distinct pair of (h_{sr}, h_{rd}) will impose a heavy computational burden on the network, which highlights the need for harnessing a less complex method, such as a DNN. As DNNs can estimate any measurable function up to a desired value [51], we intend to estimate Ψ^* with the required accuracy using our proposed DNN.

A. PROPOSED DEEP NEURAL NETWORK

As shown in Fig. 3, the proposed DNN consists of the input, hidden, and output layers. According to (5), (8) and (10), R_s is a function of $|h_{sr}|^2$ and $|h_{rd}|^2$. Accordingly, instead of using complex values of h_{sr} and h_{rd}, we use $|h_{sr}|^2$ and $|h_{rd}|^2$ as the input of our DNN. This will further simplify its implementation. We also consider the output of the two neurons in the last layer of the DNN as an $(\hat{\alpha}, \hat{\beta})$ pair. Furthermore, we set the number of hidden layers in our DNN to l.

In a DNN, each layer's output is the next layer's input. Therefore, the output of each layer can be written as a function of the input in the same layer formulated as

$$X_i = \Phi(W_i X_{i-1} + b_i), \tag{14}$$

where $\Phi(.)$ is the activation function for the ith layer, and W_i and b_i are the weight and bias matrices of the ith layer, respectively. In this work, we use the rectified linear unit (ReLU) activation function for the hidden layers and the Sigmoid activation function for the output layer, which are defined as

$$\text{ReLU(z)} = \max(0, z), \tag{15}$$

$$\text{Sigmoid(z)} = \frac{1}{1+\text{e}^{-z}}. \tag{16}$$

Using the ReLU function in hidden layers is capable of counteracting the gradient vanishing problem. Moreover, using the Sigmoid function in the output layer can implicitly include constraints (12b) and (12c) in the DNN's optimization problem, since the Sigmoid function always has an output value between 0 and 1.

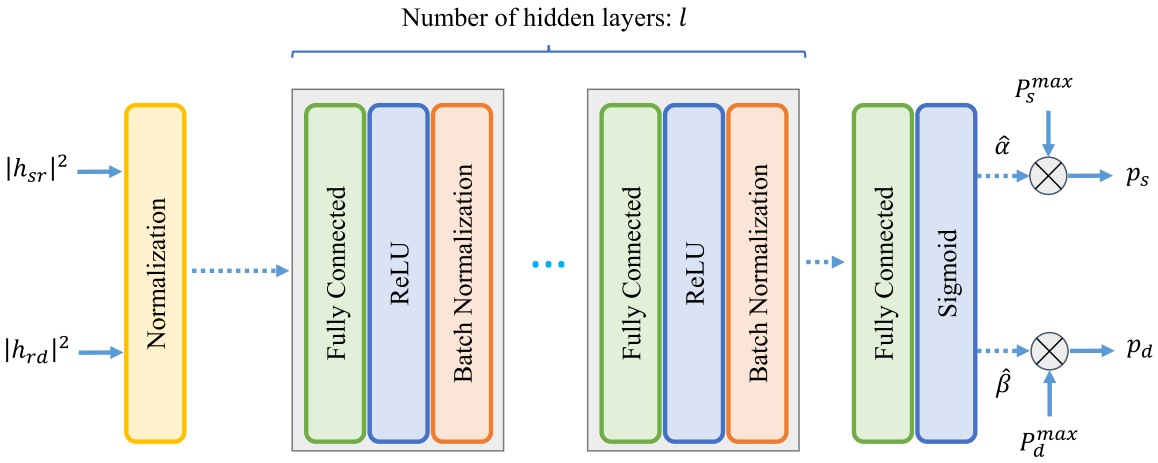


FIGURE 3. Structure of our proposed deep neural network.

B. TRAINING OUR DNN MODEL

This subsection will discuss how to train the proposed DNN to generate optimal power allocation coefficients for maximizing the ESR. To this end, we should first create a dataset to train the DNN for our optimization problem. In the second step, we must define a suitable criterion for the network to enforce its output to get closer to the optimal values of the optimization problem.

1) TRAINING SET GENERATION

To train the DNN, we generate a dataset having M members. Each member of this dataset is an optimal power allocation coefficient as an (α^*, β^*) pair, each obtained for the corresponding $(|h_{sr}|^2, |h_{rd}|^2)$pair, so that we have $\tau_m = \{(|h_{sr}|^2, |h_{rd}|^2) \rightarrow (\alpha^*, \beta^*)\}$, where $m = \{1, \ldots, M\}$. Accordingly, we randomly generate the $(|h_{sr}|^2, |h_{rd}|^2)$ pairs and obtain the corresponding (α^*, β^*) pair using the exhaustive search method.

2) LOSS FUNCTION

To define the Loss Function, we first define $W = [w_1, w_2, \ldots, w_l]$. Accordingly, the mapping between the DNN input and output can be defined as

$$\left(\hat{\alpha}, \hat{\beta}\right) = \Psi\left(|h_{sr}|^2, |h_{rd}|^2, W\right). \tag{17}$$

We remark that the function Ψ^* is a mapping that accepts the channel coefficients at its input and results in the exact value of the optimal power allocation coefficients. At the same time, Ψ is the mapping between the DNN input and output. Our goal is for Ψ and Ψ^* to be as similar as possible. To achieve this, we use the mean square error (MSE) criterion

$$\mathcal{T}(w) = \left|\Psi\left(|h_{sr}|^2, |h_{rd}|^2, W\right) - \Psi^*(h_{sr}, h_{rd})\right|^2. \tag{18}$$

In other words,

$$\mathcal{T}(w) = \left(\alpha - \hat{\alpha}\right)^2 + \left(\beta - \hat{\beta}\right)^2. \tag{19}$$

In Section VI, using the above loss function, we will train our proposed DNN by applying the error back propagation (EBP) algorithm [52].

IV. ASYMPTOTIC HIGH-SNR ANALYSIS

In this section, to provide a better practical insight into the parameters of the scenario studied, we examine the equations obtained in Section II for the asymptotic SNR. To simplify the analysis, we rewrite Eq. (10) as

$$R_s = \left[\log_2 \frac{1+\Gamma_D}{1+\Gamma_R}\right]^+, \tag{20}$$

where the expanded expression for $\frac{1+\Gamma_D}{1+\Gamma_R}$ is presented at the top of the next page with

$$k_1 = k_s^{t^2} + k_R^{r^2} + k_{R,D}^{(t,r)^2} + k_{R,D}^{(t,r)^2} k_s^{t^2} + k_{R,D}^{(t,r)^2} k_R^{r^2}, \tag{21}$$

$$k_2 = k_D^{t^2} + k_R^{r^2} + k_{R,D}^{(t,r)^2} + k_{R,D}^{(t,r)^2} k_D^{t^2} + k_{R,D}^{(t,r)^2} k_R^{r^2}, \tag{22}$$

$$k_3 = \sigma^2\left(1 + k_{R,D}^{(t,r)^2}\right), \tag{23}$$

$$k_4 = \sigma^2 \lambda^{-1}, \tag{24}$$

$$\tau_1 = k_s^{t^2} + k_R^{r^2}, \tag{25}$$

$$\tau_2 = 1 + k_D^{t^2} + k_R^{r^2}, \tag{26}$$

$$\tau_3 = \sigma^2. \tag{27}$$

Additionally, we have assumed equal noise power at all nodes (σ^2) and set $\gamma_{sr} = \frac{p_s|h_{sr}|^2}{\sigma^2}$ and $\gamma_{rd} = \frac{p_d|h_{rd}|^2}{\sigma^2}$.

Corollary 1: If $\gamma_{sr} \rightarrow \infty$ and γ_{rd} has a finite value, then $R_s = 0$.

Proof: According to (20) we can write

$$\lim_{\gamma_{sr}\rightarrow\infty}\left[\log_2 \frac{1+\Gamma_D}{1+\Gamma_R}\right]^+ \overset{(28)}{=} \left[\log_2 \frac{(1+k_1)\tau_1}{k_1(1+\tau_1)}\right]^+. \tag{29}$$

Moreover according to (21) and (25), $\tau_1 \leq k_1$ leading to $\tau_1 + \tau_1 k_1 \leq k_1 + \tau_1 k_1$ so

$$\frac{(1+k_1)\tau_1}{k_1(1+\tau_1)} \leq 1 \rightarrow \log \frac{(1+k_1)\tau_1}{k_1(1+\tau_1)} < 0. \tag{30}$$

Therefore, we have $R_s = 0$.

Corollary 1 states that by increasing the quality of signal reception at the untrusted relay, at some point the rate at the relay exceeds the corresponding rate at the destination. This leads to zero secrecy rate. Moreover, we know that when the transmitter power is zero, $R_s = 0$. Accordingly the optimal value for the transmitted power lays between 0 and ∞. This observation has motivated us to formulate the power allocation problem. ■

Corollary 2: If $\gamma_{rd} \to \infty$ and γ_{sr} has a finite value, then $R_s = 0$.

Proof: According to (20) we can write

$$\lim_{\gamma_{rd}\to\infty}\left[\log_2\frac{1+\Gamma_D}{1+\Gamma_R}\right]^+ \overset{(28)}{=} \left[\log_2 1\right]^+ = 0. \tag{31}$$

Corollary 2 states a completely different result with respect to the ideal hardware case. This is because by increasing γ_{rd} (for example, increasing the level of jamming power sent by the destination), due to the presence of HWIs in the jamming signal transmitted, this node cannot effectively remove the distortion caused by itself, when receiving it again after being forwarded by the relay. This observation is quite different from the ideal hardware mode in which the destination can eliminate the distortion caused by itself. Accordingly, in the ideal hardware case, it will be optimal to use the maximum power of the destination to degrade the quality of the relay's reception. The observation in Corollary 2 was another incentive for us to formulate the optimal power allocation problem. ■

Corollary 3: If $\gamma_{rd} \to \infty$, $\gamma_{sr} \to \infty$ and $\frac{\gamma_{sr}}{\gamma_{rd}} = \nu$, then

$$R_s = \left[\log_2\left[\frac{\nu(1+k_1)+k_2}{\nu k_1+k_2}\cdot\frac{\nu\tau_1+\tau_2}{\nu(1+\tau_1)+\tau_2}\right]\right]^+. \tag{32}$$

Moreover, to have a non-zero secrecy rate, we shall have

$$\nu < \frac{1-k_{R,D}^{(t,r)^2}\left(1+k_D^{t^2}+k_R^{r^2}\right)}{k_{R,D}^{(t,r)^2}\left(1+k_S^{t^2}+k_R^{r^2}\right)}. \tag{33}$$

Proof: According to (20), we can write

$$\lim_{\gamma_{sr},\gamma_{rd}\to\infty}\left[\log_2\frac{1+\Gamma_D}{1+\Gamma_R}\right]^+ \overset{(28)}{=} \left[\log_2\left[\frac{\nu(1+k_1)+k_2}{\nu k_1+k_2}\cdot\frac{\nu\tau_1+\tau_2}{\nu(1+\tau_1)+\tau_2}\right]\right]^+. \tag{34}$$

Additionally, to have non-zero R_s, $\frac{1+\Gamma_D}{1+\Gamma_R}$ has to be strictly positive. Using (32) and (21)–(27) we get the condition in (33).

Corollary 3 highlights three important points of our scenario. Firstly, according to (32), upon increasing the powers at the nodes, the ESR value for this scenario becomes saturated for a given ν. This is due to the HWIs in our scenario and is a fundamental difference with respect to (w.r.t.) the ideal hardware case in which the ESR increases unboundedly upon increasing the power. Secondly, it provides an upper bound on the ratio of $\frac{\gamma_{sr}}{\gamma_{rd}}$, which can be helpful when adjusting the power of the nodes. If the power of $\mathcal{S}$ exceeds a specific level, the rate of the relay will be increased. However, due to the presence of HWIs, $\mathcal{D}$ will not be able to completely contaminate the received signal of the relay. This will eventually lead to zero secrecy rate. Finally, according to (33), for $k_{R,D}^{(t,r)^2}(1+k_D^{t^2}+k_R^{r^2}) \geq 1$ the system will have a zero ESR. This provides us with an upper bound on the worst case HWI values and states that for impairment levels above this upper bound, the ESR will always be zero, regardless of the transmit powers at $\mathcal{S}$ and $\mathcal{D}$. ■

V. OPTIMUM HARDWARE IMPAIRMENT SHARING

The principal motivation behind optimal HWI sharing is to provide a guideline for an overall system design under a total cost constraint [25]. Specifically, the level of HWIs directly depends on the quality of hardware utilized in the RF section of the nodes. These impairments may become excessive in low-cost IoT networks. In such networks, the financial budget and total revenue will eventually determine the quality of RF hardware utilized in each node and the total tolerable HWI levels [25], [30], [31], [53]. In this section we formulate and solve an optimization problem, which determines the optimum sharing of the HWI levels among the nodes. More explicitly, the total tolerable HWIs could be shared in an equitable manner across the three nodes or in an extreme case we could opt for an expensive but high-quality source and low-quality, high-impairment relay and destination.

Accordingly, the optimization problem is formulated using the results of our high-SNR regime in Corollary 3 as

$$\max_{\mathbf{k}} \ \max_{\nu} \log_2\left[\frac{\nu(1+k_1)+k_2}{\nu k_1+k_2}\cdot\frac{\nu\tau_1+\tau_2}{\nu(1+\tau_1)+\tau_2}\right] \tag{35a}$$

$$\text{s.t: } k_1 = k_s^{t^2}+k_R^{r^2}+\left(k_R^{t\,2}+k_D^{r\,2}\right)\left(1+k_s^{t^2}+k_R^{r^2}\right), \tag{35b}$$

$$k_2 = k_D^{t^2}+k_R^{r^2}+\left(k_R^{t\,2}+k_D^{r\,2}\right)\left(1+k_D^{t^2}+k_R^{r^2}\right), \tag{35c}$$

$$\tau_1 = k_s^{t^2}+k_R^{r^2}, \tag{35d}$$

$$\tau_2 = 1+k_D^{t^2}+k_R^{r^2}, \tag{35e}$$

$$k_{S,D}^{tot} = k_S^t+k_D^t+k_D^r, \tag{35f}$$

$$k_R^{tot} = k_R^t+k_R^r, \tag{35g}$$

where $\mathbf{k} = \{k_S^t, k_R^t, k_R^r, k_D^t, k_D^r\}$, $k_{S,D}^{tot}$ is the joint error vector magnitude (EVM) constraint at $\mathcal{S}$ and $\mathcal{D}$, which k_R^{tot} is the

$$\frac{1+\Gamma_D}{1+\Gamma_R} = \frac{\left[(1+k_1)\sigma^2|h_{rd}|^2\gamma_{sr}+k_2\sigma^2|h_{rd}|^2\gamma_{rd}+k_3|h_{rd}|^2+k_4\right]\left[\tau_1\sigma^2\gamma_{sr}+\tau_2\sigma^2\gamma_{rd}+\tau_3\right]}{\left[k_1\sigma^2|h_{rd}|^2\gamma_{sr}+k_2\sigma^2|h_{rd}|^2\gamma_{rd}+k_3|h_{rd}|^2+k_4\right]\left[(1+\tau_1)\sigma^2\gamma_{sr}+\tau_2\sigma^2\gamma_{rd}+\tau_3\right]} \tag{28}$$

maximum tolerable HWIs in $\mathcal{R}$. In our optimization problem we have considered the impairment sharing for the value of ν, which leads to maximizing the instantaneous secrecy rate. This is because when utilizing the system model considered, one intends to adjust the transmit powers of $\mathcal{S}$ and $\mathcal{D}$ in a way, which leads to the maximum secrecy rate and it is in line with the optimization problem in (12). The solution for the optimization problem in (35) is not straightforward, since neither the objective function nor the rational expression inside log(.) are concave w.r.t. the optimization variables. Furthermore, we have non-affine equality constraints in (35b) through (35e). In the following, we intend to solve the above problem using MM by utilizing geometric programming (GP) in each step.

To solve the optimization problem in (35), we consider the joint maximization of the secrecy rate versus the optimization variables ν and $\mathbf{k}$. We can also substitute for k_1, k_2, τ_1 and τ_2 in (35a) to eliminate the non-affine equalities. This yields $\log_2[\frac{N}{D}]$ in the objective function where N and D are defined in (36) and (37) at the bottom of the page. Accordingly, we can rewrite (35) as

$$\max_{\mathbf{k},\nu} \sum_{i=1}^{I} t_i \tag{38a}$$

$$\text{s.t: } t_i D \le p_i, \quad i = 1, \ldots, I, \tag{38b}$$

$$k_{S,D}^{tot} = k_S^t + k_D^t + k_D^r, \tag{38c}$$

$$k_R^{tot} = k_R^t + k_R^r, \tag{38d}$$

where p_i represents each of the monomial terms in (36), t_i represents the slack variables and I is the number of monomials in it ($I = 56$). We have also taken into account the maximization of the rational expression inside the log function, since $\log(x)$ is a monotonically increasing function w.r.t. x. The optimization problem in (38) is in the form of Signomial Programming (SP) and it is still non-convex. However, by applying the following Corollary we can solve it iteratively by converting the SP into a GP in each iteration.

Remark 3: Before proceeding, we need to define the concepts of posynomials and monomials. A monomial is a function $f:\mathbf{R}_{++}^n \to \mathbf{R}$:

$$f(x) = d x_1^{a(1)} x_2^{a(2)}, \ldots x_n^{a(n)}, \tag{39}$$

where the multiplicative constant $d \ge 0$ and the exponential constants $a(j) \in \mathbf{R}$, $j = 1, 2, \ldots, n$. A sum of monomials is called a posynomial [54]. Note that a GP program is the minimization of a posynomial subject to posynomial upper bound inequality constraints and monomial equality constraints. Moreover, since the domain of monomials is the strictly positive real numbers, when a GP is written in terms of monomials, it is implicitly assumed that the optimal variables are greater than zero [54]. A GP is easily converted to a convex program with the change of variables and can be directly defined in MATLAB CVX.

Corollary 4: Let $\{u_i(\mathbf{x})\}$ represent the monomial terms in a posynomial $f(\mathbf{x}) = \sum_i u_i(\mathbf{x})$. A monomial approximation of the posynomial $f(\mathbf{x})$ can be formulated as:

$$\prod_i \left(\frac{u_i(\mathbf{x})}{\alpha_i} \right)^{\alpha_i}, \tag{40}$$

in which α can be chosen as

$$\alpha_i(\mathbf{x}) = u_i(\mathbf{x}) / f(\mathbf{x}), \forall i. \tag{41}$$

Proof: Please see [54]. ■

The objective function in (38a) and the equality constraints in (38c) and (38d) are in posynomial forms. Using Corollary 4, at each iteration of the proposed algorithm, we approximate these posynomial forms with monomials to have a GP program. The resulting monomial is a global lower bound of the corresponding posynomial term and is equal to it at the approximation point [55]. This means that

$$\begin{aligned} N = {} & k_D^{r^2} k_D^{t^4} + 2k_D^{r^2} k_D^{t^2} k_R^{r^2} \nu + 2k_D^{r^2} k_D^{t^2} k_R^{r^2} + 2k_D^{r^2} k_D^{t^2} k_S^{t^2} \nu + k_D^{r^2} k_D^{t^2} \nu + 2k_D^{r^2} k_D^{t^2} + k_D^{r^2} k_R^{r^4} \nu^2 + 2k_D^{r^2} k_R^{r^4} \nu + k_D^{r^2} k_R^{r^4} \\ & + 2k_D^{r^2} k_R^{r^2} k_S^{t^2} \nu^2 + 2k_D^{r^2} k_R^{r^2} k_S^{t^2} \nu + k_D^{r^2} k_R^{r^2} \nu^2 + 3k_D^{r^2} k_R^{r^2} \nu + 2k_D^{r^2} k_R^{r^2} + k_D^{r^2} k_S^{t^4} \nu^2 + k_D^{r^2} k_S^{t^2} \nu^2 + 2k_D^{r^2} k_S^{t^2} \nu \\ & + k_D^{r^2} \nu + k_D^{r^2} + k_D^{t^4} k_R^{t^2} + k_D^{t^4} + 2k_D^{t^2} k_R^{r^2} k_R^{t^2} \nu + 2k_D^{t^2} k_R^{r^2} k_R^{t^2} + 2k_D^{t^2} k_R^{r^2} \nu + 2k_D^{t^2} k_R^{r^2} + 2k_D^{t^2} k_R^{t^2} k_S^{t^2} \nu + k_D^{t^2} k_R^{t^2} \nu \\ & + 2k_D^{t^2} k_R^{t^2} + 2k_D^{t^2} k_S^{t^2} \nu + k_D^{t^2} \nu + k_D^{t^2} + k_R^{r^4} k_R^{t^2} \nu^2 + 2k_R^{r^4} k_R^{t^2} \nu + k_R^{r^4} k_R^{t^2} + k_R^{r^4} \nu^2 + 2k_R^{r^4} \nu + k_R^{r^4} + 2k_R^{r^2} k_R^{t^2} k_S^{t^2} \nu^2 \\ & + 2k_R^{r^2} k_R^{t^2} k_S^{t^2} \nu + k_R^{r^2} k_R^{t^2} \nu^2 + 3k_R^{r^2} k_R^{t^2} \nu + 2k_R^{r^2} k_R^{t^2} + 2k_R^{r^2} k_S^{t^2} \nu^2 + 2k_R^{r^2} k_S^{t^2} \nu + k_R^{r^2} \nu^2 + 2k_R^{r^2} \nu + k_R^{r^2} + k_R^{t^2} k_S^{t^4} \nu^2 \\ & + k_R^{t^2} k_S^{t^2} \nu^2 + 2k_R^{t^2} k_S^{t^2} \nu + k_R^{t^2} \nu + k_R^{t^2} + k_S^{t^4} \nu^2 + k_S^{t^2} \nu^2 + k_S^{t^2} \nu + \nu, \end{aligned} \tag{36}$$

$$\begin{aligned} D = {} & k_D^{r^2} k_D^{t^4} + 2k_D^{r^2} k_D^{t^2} k_R^{r^2} \nu + 2k_D^{r^2} k_D^{t^2} k_R^{r^2} + 2k_D^{r^2} k_D^{t^2} k_S^{t^2} \nu + 2k_D^{r^2} k_D^{t^2} \nu + 2k_D^{r^2} k_D^{t^2} + k_D^{r^2} k_R^{r^4} \nu^2 + 2k_D^{r^2} k_R^{r^4} \nu + k_D^{r^2} k_R^{r^4} \\ & + 2k_D^{r^2} k_R^{r^2} k_S^{t^2} \nu^2 + 2k_D^{r^2} k_R^{r^2} k_S^{t^2} \nu + 2k_D^{r^2} k_R^{r^2} \nu^2 + 4k_D^{r^2} k_R^{r^2} \nu + 2k_D^{r^2} k_R^{r^2} + k_D^{r^2} k_S^{t^4} \nu^2 + 2k_D^{r^2} k_S^{t^2} \nu^2 + 2k_D^{r^2} k_S^{t^2} \nu + k_D^{r^2} \nu^2 \\ & + 2k_D^{r^2} \nu + k_D^{r^2} + k_D^{t^4} k_R^{t^2} + k_D^{t^4} + 2k_D^{t^2} k_R^{r^2} k_R^{t^2} \nu + 2k_D^{t^2} k_R^{r^2} k_R^{t^2} + 2k_D^{t^2} k_R^{r^2} \nu + 2k_D^{t^2} k_R^{r^2} + 2k_D^{t^2} k_R^{t^2} k_S^{t^2} \nu + 2k_D^{t^2} k_R^{t^2} \nu \\ & + 2k_D^{t^2} k_R^{t^2} + 2k_D^{t^2} k_S^{t^2} \nu + k_D^{t^2} \nu + k_D^{t^2} + k_R^{r^4} k_R^{t^2} \nu^2 + 2k_R^{r^4} k_R^{t^2} \nu + k_R^{r^4} k_R^{t^2} + k_R^{r^4} \nu^2 + 2k_R^{r^4} \nu + k_R^{r^4} + 2k_R^{r^2} k_R^{t^2} k_S^{t^2} \nu^2 \\ & + 2k_R^{r^2} k_R^{t^2} k_S^{t^2} \nu + 2k_R^{r^2} k_R^{t^2} \nu^2 + 4k_R^{r^2} k_R^{t^2} \nu + 2k_R^{r^2} k_R^{t^2} + 2k_R^{r^2} k_S^{t^2} \nu^2 + 2k_R^{r^2} k_S^{t^2} \nu + k_R^{r^2} \nu^2 + 2k_R^{r^2} \nu + k_R^{r^2} + k_R^{t^2} k_S^{t^4} \nu^2 \\ & + 2k_R^{t^2} k_S^{t^2} \nu^2 + 2k_R^{t^2} k_S^{t^2} \nu + k_R^{t^2} \nu^2 + 2k_R^{t^2} \nu + k_R^{t^2} + k_S^{t^4} \nu^2 + k_S^{t^2} \nu^2 + k_S^{t^2} \nu. \end{aligned} \tag{37}$$

Algorithm 1 Proposed MM Based Iterative Optimization

Input: $k_{S,D}^{tot}, k_R^{tot}, \Theta$

Output: $k_S^t, k_R^t, k_R^r, k_D^t, k_D^r$

1: **Initialization:**
- $\theta = 0$
- $k_S^t = k_D^t = k_D^r = \frac{k_{S,D}^{tot}}{3}$
- $k_R^t = k_R^r = \frac{k_R^{tot}}{2}$
- $\nu = \frac{1-k_{R,D}^{(t,r)^2}(1+k_D^{t^2}+k_R^{r^2})}{2k_{R,D}^{(t,r)^2}(1+k_S^{t^2}+k_R^{r^2})}$

2: **repeat** (MM Algorithm for $\mathbf{k}$ and ν)

3: Use (41) to convert the posynomials in the objective function and equality conditions into monomials:

(I) $r_i = \frac{t_i}{\sum_{i=1}^{I} t_i}, \quad i = 1, \ldots, I$

(II) $s_1 = \frac{k_S^t}{k_S^t+k_D^t+k_D^r}, s_2 = \frac{k_D^t}{k_S^t+k_D^t+k_D^r}, s_3 = \frac{k_D^r}{k_S^t+k_D^t+k_D^r}$

(III) $q_1 = \frac{k_R^t}{k_R^t+k_R^r}, q_2 = \frac{k_R^r}{k_R^t+k_R^r}$

4: Solve the polynomial time GP:

$$\max_{\mathbf{k},\nu} \prod_{i=1}^{I} \left(\frac{t_i}{r_i}\right)^{r_i}$$

$$\text{s.t: } t_i D \le p_i, \quad i = 1, \ldots, I,$$

$$k_{S,D}^{tot} = \left(\frac{k_S^t}{s_1}\right)^{s_1}\left(\frac{k_D^t}{s_2}\right)^{s_2}\left(\frac{k_D^r}{s_3}\right)^{s_3},$$

$$k_R^{tot} = \left(\frac{k_R^t}{q_1}\right)^{q_1}\left(\frac{k_R^r}{q_2}\right)^{q_2},$$

5: Update $\theta = \theta + 1$.

6: **until** the optimization variables $\mathbf{k}$ and ν reache convergence or $\theta = \Theta$.

the resulting iterative algorithm is MM, and the optimization problem at each step is GP [55]. Accordingly, we start with an arbitrary feasible point in our MM algorithm and apply Corollary 4 to Problem (38) to obtain a standard form GP in each iteration.

Algorithm 1 details our proposed MM algorithm, where Θ is the maximum number of iterations. We have also exploited the upper bound expression in (33) to initialize ν in this algorithm. Our numerical results validate that the proposed algorithm converges rapidly to the optimum point and the approximations are tight.

VI. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we demonstrate the efficiency of our proposed DNN-based power allocation scheme by facilitating Keras Tensorflow [56]. Specifically, we first justify our motivation behind proposing the power allocation problem. Then we will examine the impact of the transmission parameters, namely the power, HWIs and energy efficiency on the ESR. Additionally, by contrasting the outcome of our DNN to the optimum values obtained through exhaustive search, we will evaluate the performance of our DNN. Furthermore, we will run our MM based algorithm to demonstrate the effect of optimum HWI allocation on the ESR. Finally, we will compare the computational cost of our DNN to that of the exhaustive search.

TABLE 2. Parameter Settings

Parameter description	Value
hardware imperfection level	$k = 0.05$
energy conversion efficiency	$\lambda = 1$
search step size	$\zeta_a = \zeta_b = 10^{-2}$
training dataset size	$M = 10000$
batch size	128
initial learning rate	10^{-2}
decay rate	0.9
Number of training epochs	1000
Optimizer	Adam

In our simulations we assume having equal noise power in the receiver nodes, $\sigma_R^2 = \sigma_D^2 = 0.025$. Additionally, unless otherwise stated, we set $\lambda = 1$ and consider the levels of HWIs found in the related literature [24], [34], ${k_S^t}^2 = {k_D^t}^2 = {k_D^r}^2 = {k_R^t}^2 = {k_R^r}^2 = k = 0.05$. Fig. 4 shows the impact of HWIs on the ESR of the scenario studied with different available power constraints in the $\mathcal{S}$ and $\mathcal{D}$ nodes. We can observe that when perfect hardware is considered, regardless of the available power in active nodes, the maximum ESR is obtained upon using the maximum available power in both nodes. However, this is not the case for the scenario of HWIs. We can see that the optimum power allocation factors have to be assigned to the active nodes to reach the maximum ESR and the power allocation factors vary, when the transmit power available at the nodes changes. This observation is the baseline for raising the problem of optimum power allocation. We further note that for all of the cases shown, there is only a single unique optimum point for the maximization of the ESR.

In Fig. 5, we intend to get a better notion of how our optimization problem reacts in the face of different power budgets at $\mathcal{S}$ and $\mathcal{D}$. From an energy harvesting perspective, we expect that the relay will mainly acquire its transmit power by harvesting from the transmit power of $\mathcal{D}$. This is because $\mathcal{D}$ sends a jamming signal, while $\mathcal{S}$ transmits the main message and accordingly, its power boost will directly boost the eavesdropping opportunities of the untrusted relay. This is in line with the trend observed in Fig. 5. Explicitly, we can see in all cases that the maximum ESR is achieved through utilizing the maximum available power at $\mathcal{D}$, $(\beta = 1, \alpha < 1)$, with an exception in the case of $p_s << p_d$. In the latter case to avoid weak reception of the signal at $\mathcal{D}$ and for acquiring sufficient transmit power for $\mathcal{R}$, $\mathcal{S}$ utilizes its maximum power $(\alpha = 1)$. However, due to the presence of HWIs at $\mathcal{D}$, the utilization of the maximum power in this node may deteriorate the quality of signal reception and accordingly, it is not an optimum choice. Furthermore, Fig. 5 confirms our results presented

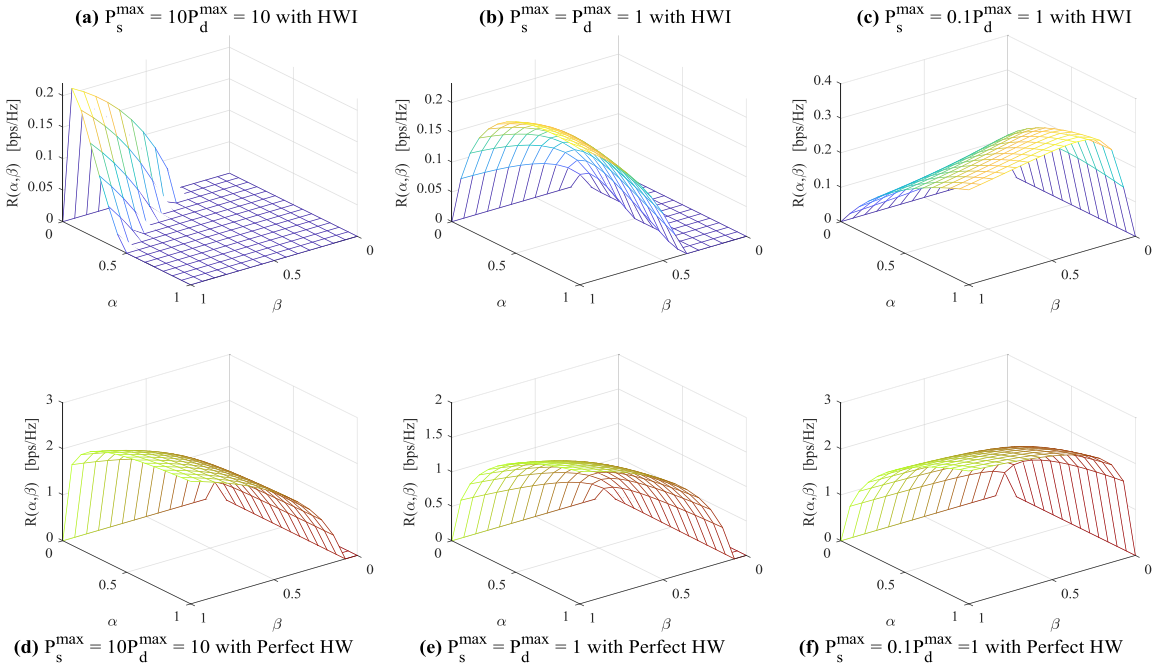


FIGURE 4. Secrecy rate versus power allocation factors α and β for perfect and non-perfect hardware with different available powers in nodes.

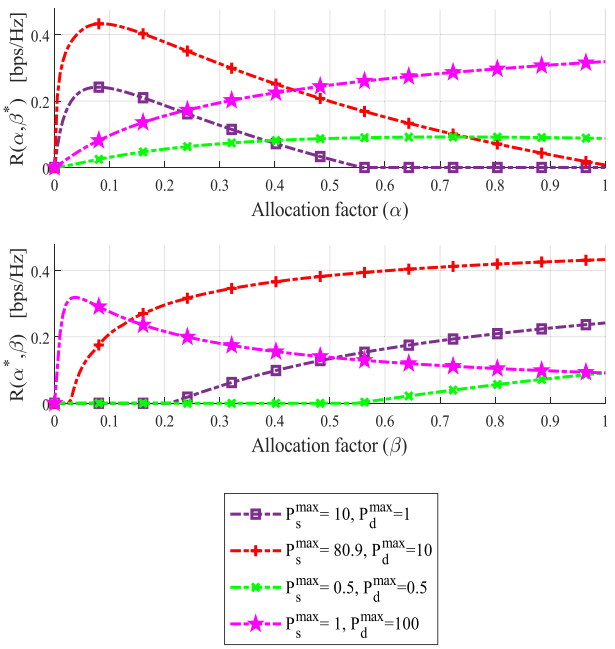


FIGURE 5. Rate versus allocation factors α and β for different available power budgets in nodes.

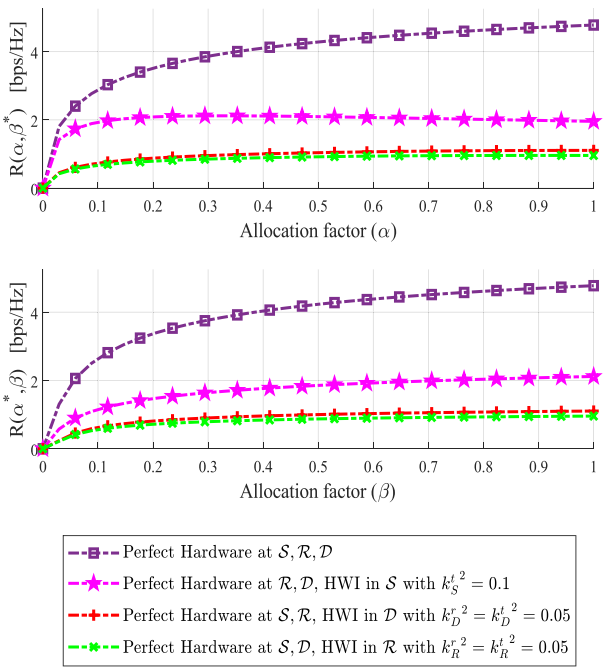


FIGURE 6. Rate versus allocation factors α and β for different distribution of impairments in nodes, $P_s^{max} = P_d^{max} = 10$.

in Corollary 3. This is shown by the ESR versus α curve, in which the transmit powers are set as $P_s^{max} = 80.9$ and $P_d^{max} = 10$. These two values are selected in a way that their ratio meets the condition stated in (33). As expected, when the condition in (33) is met in $\alpha = 1$, the ESR becomes equal to zero.

Fig. 6, demonstrates how the impairment in each of the nodes can affect the ESR. To have a fair comparison, we have assumed equal total impairment levels in each of the nodes and equivalently in each of the curves. Firstly, we can see that the presence of HWIs in every node can severely degrade the ESR. Accordingly, it is vital to take into account the HWIs of nodes in realistic implementations. Additionally, we can observe that the presence of impairments at $\mathcal{R}$ and $\mathcal{D}$ imposes more severe degradation on the ESR than at $\mathcal{S}$.

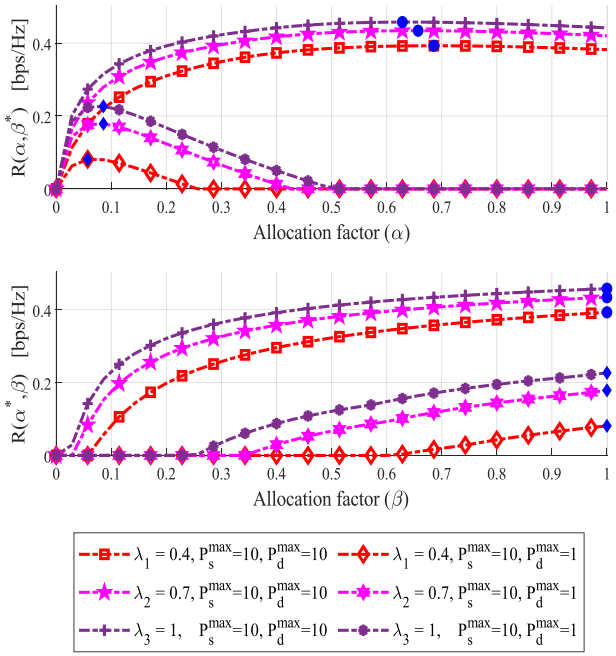


FIGURE 7. Rate versus allocation factors α and β for different values of energy conversion efficiency.

This is because the HWIs of $\mathcal{R}$ and $\mathcal{D}$ are boosted by the transmit power of both $\mathcal{S}$ and $\mathcal{D}$ nodes. However, this is not the case when we only have HWIs in the $\mathcal{S}$ node, where this impairment is introduced to the system only by the transmit power of the source.

Moreover, we can observe that the HWIs at $\mathcal{R}$ lead to more grave degradation than those at the $\mathcal{D}$. Nevertheless, this observation may seem ironic at first sight, since one may expect that in the case of impairments at the untrusted relay, the detection capability of $\mathcal{R}$ degrades, while $\mathcal{D}$ benefits from perfect hardware in support of its detection and accordingly we can get a better ESR. However, in this case, the message transmitted from $\mathcal{S}$ experiences HWIs in both the reception and transmission phases of $\mathcal{R}$. By contrast, when the impairment is only present at $\mathcal{D}$, this only plays a detrimental role once in the reception at $\mathcal{D}$. Care must be taken concerning the transmit power of $\mathcal{S}$ in the latter case, because in the case of $P_s^{\max} >> P_d^{\max}$, $\mathcal{R}$ can efficiently decode the message and the ESR will drop compared to the former case.

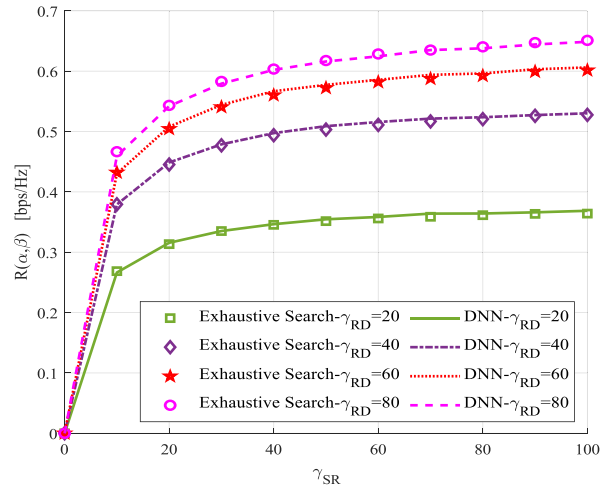
In Fig. 7, we can see the impact of the energy conversion efficiency of our energy harvesting relay imposed on the ESR. The maximum ESR is always obtained when $\lambda = 1$, regardless of the allocation factors. However, for different energy conversion efficiencies, we get different optimum power allocation factors. The trend of change in optimum response with respect to energy conversion efficiency is a function of the power available at $\mathcal{D}$. In Fig. 7, there are two sets of curves, one for $P_d^{\max} = 1$ and the other for $P_d^{\max} = 10$. When there is sufficient power at $\mathcal{D}$ ($P_d^{\max} = 10$), the relay can mainly rely on the transmit power of $\mathcal{D}$ to provide its power. Accordingly, by enhancing the energy efficiency coefficient, the transmit power of $\mathcal{S}$ can be reduced, which leads to reduced information leakage to the untrusted relay. However, this trend does not apply to the scenario, in which the power available at $\mathcal{D}$ is scarce ($P_d^{\max} = 1$). This is because despite the enhancement of the energy efficiency coefficient, the relay is unable to harvest sufficient transmit power from $\mathcal{D}$ and accordingly, it requires more power to be transmitted from $\mathcal{S}$.

Now that we have gained better insights into the impact of the various parameters on the ESR, we intend to solve the optimization problem in (12a) by harnessing a DNN. In the training phase of our DNN, we set $P_s^{\max} = P_d^{\max} = 1$, $k_S^{t^2} = k_R^{r^2} = k_R^{t^2} = k_D^{t^2} = k_D^{r^2} = k = 0.05$ and $\lambda = 1$. The optimum hyper parameters were determined experimentally for our DNN and accordingly we considered a fully-connected neural network having 2 neurons in the input layer and $l = 6$ hidden layers associated with (16, 16, 16, 8, 8, 8) neurons, in addition to output layer consisting of 2 neurons, as shown in Fig. 3. The activation functions for each of these neurons and the corresponding loss function are set in accordance with Section III. We train our DNN with batch sizes of 128 and 1000 training epochs. Moreover, the Adam optimizer having decaying steps is utilized with an initial learning rate of 10^{-2} and decay rate of 0.9. Furthermore, we harness Keras in Python for training and testing our DNN.

We generate a training dataset having $M = 10000$ members. Each optimal power allocation pair (α^*, β^*) is generated through applying exhaustive search based on (12a). Moreover, for each SNR, HWI level and energy conversion efficiency, we generate another dataset independent of the training dataset having $M = 10000$ members to contrast their optimal power allocation obtained by exhaustive search with the output of the trained DNN. Accordingly, in the following figures we average the maximum ESR over 10000 samples formulated by $R_{ave} = \mathbb{E}_{h_{sr},h_{rd}}[R(\alpha^*, \beta^*)]$, for each SNR, HWI level and energy conversion efficiency value.

Fig. 8 characterizes the performance of our trained DNN and compares it to the exhaustive search results for different values of SNRs in the $\mathcal{S}$-$\mathcal{R}$ and $\mathcal{R}$-$\mathcal{D}$ links. The plots prove the robustness of the trained DNN and it can be seen that for some SNRs the performance is slightly better than that of the exhaustive search. This is because the performance of the exhaustive search is limited by its search step size, while the sigmoid activation function at the output allows the DNN to produce any arbitrary number between 0 and 1. Additionally, we can observe that the ESR versus γ_{sr} curves saturate at lower SNRs compared to the ESR versus γ_{rd} curves. This is in line with our previous deductions, since increasing the power of $\mathcal{S}$ will lead to better reception quality at the untrusted relay, which may lead to the degradation of the ESR.

We note that when deployed in practice, we need to fine-tune the trained DNN with the channel samples of the wireless medium [57]. This is because, due to the impairments or channel variations, the channel samples



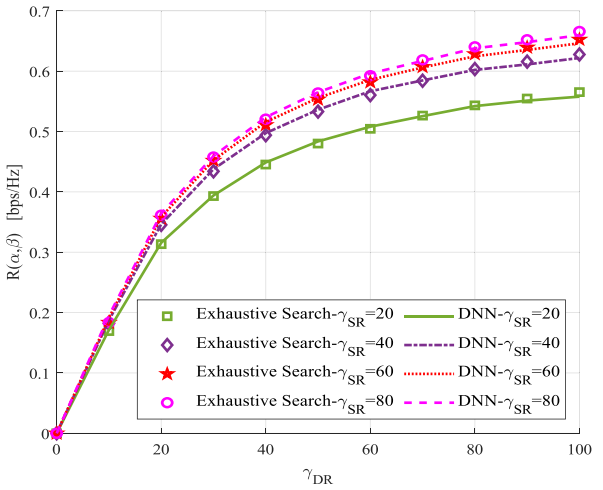


FIGURE 8. ESR versus γ_{SR} and γ_{RD} for $k = 0.05$ and $\lambda = 1$.

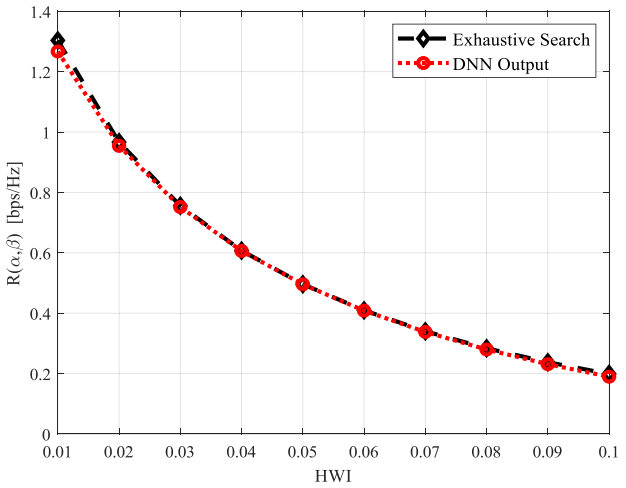


FIGURE 9. Maximum ESR versus HWI level (k) obtained with DNN and applying exhaustive search.

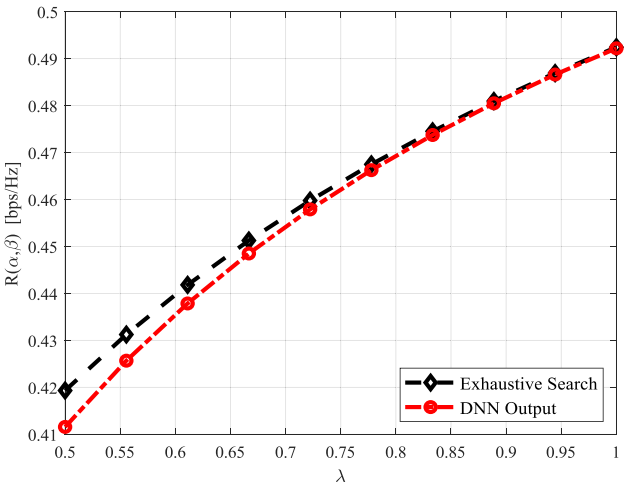


FIGURE 10. Maximum ESR versus energy conversion efficiency obtained with DNN and applying exhaustive search.

generated in simulation may vary from the samples in practice and lead to non-optimal power values [57]. Another method to acquire the channel samples is to deploy generative adversarial networks (GANs). In this method, no assumption is made about the wireless channel model. Specifically, a GAN is trained to mimic the wireless environment based on the measured channel samples [58], [59]. Deploying GANs to acquire the training dataset of the DNN will be considered in our future study.

In Fig. 9, we observe the impact of HWIs on the maximum ESR, which may significantly degrade the ESR. Additionally, the performance of our trained DNN is shown for different values of HWI levels. The ESR attained by the DNN is very close to that of the exhaustive search. This shows that despite being trained on optimum values obtained by $k = 0.05$, our DNN can generate near-optimal results for the entire range of HWIs.

In Fig. 10, one can observe how the energy conversion efficiency affects the maximum ESR. As expected, enhancing the energy conversion efficiency will boost the ESR. Again, we can observe that despite being trained on $\lambda = 1$, our trained DNN generates allocation factors very close to those generated by the exhaustive search for the entire range of energy conversion efficiencies.

Fig. 11 demonstrates how the optimal impairment distribution between the nodes can enhance the secrecy rate. Again, we have considered the equal HWI sharing among the nodes as $k_S^{t^2} = k_R^{r^2} = k_R^{t^2} = k_D^{t^2} = k_D^{r^2} = k = 0.05$ to contrast it with the results obtained by our proposed MM algorithm. Accordingly, we set $k_{S,D}^{tot} = 0.67$ and $k_R^{tot} = 0.45$ and by running Algorithm 1 using MATLAB CVX, we get the optimal values of HWIs in the nodes as $k_S^{t^2} = 0.09$, $k_R^{r^2} = 0.06, k_R^{t^2} = 0.04, k_D^{t^2} = 0.06, k_D^{r^2} = 0.01$. It takes four iterations for the algorithm to converge and accordingly the time required to run the algorithm is short. In Fig. 11 we can observe that the optimal impairment sharing among

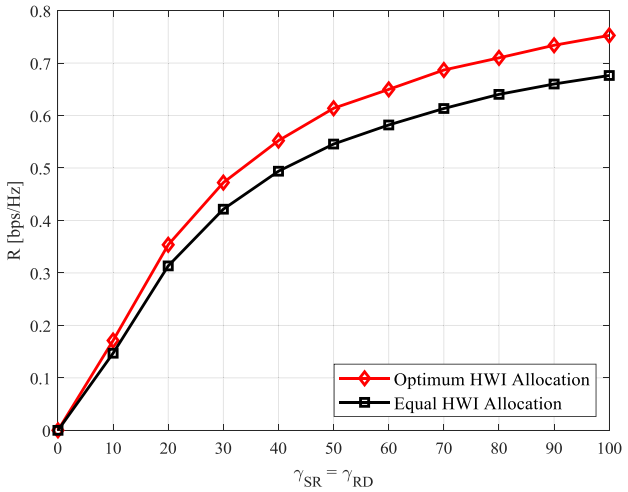


FIGURE 11. The impact of optimal HWI allocation obtained by Algorithm 1 on the ESR.

the nodes can significantly mitigate the deleterious effect of HWIs and enhance the secrecy rate.

The output of Algorithm 1 can give us useful insights in designing the impairment of the scenario considered. We can observe that a considerable share of $k_{S,D}^{tot}$ is allocated to the $\mathcal{S}$. This is in line with our observations in Fig. 6, namely that the presence of HWIs in $\mathcal{S}$ will lead to lower degradation of the ESR compared to that in $\mathcal{D}$. Additionally, we observe that $k_D^{t^2} > k_D^{r^2}$. This is because the higher share of impairment in the transmitter block of $\mathcal{D}$ can lead to higher distortion power at $\mathcal{R}$, hence degrading the reception capability of $\mathcal{R}$. Moreover, the algorithm allocates much of the k_R^{tot} to the receiver block compared to the transmitter block of $\mathcal{R}$. This setting can again degrade the reception quality of $\mathcal{R}$.

Finally, we contrast the computational requirements of the exhaustive search to that of the learning-based method. Accordingly, we define $N_\alpha = 1/\zeta_\alpha$ and $N_\beta = 1/\zeta_\beta$, where ζ_α and ζ_β denote the search step size for α and β in our exhaustive search algorithm. To elaborate further, we quantize α and β with N_α and N_β equally spaced values. Then, by substituting all possible combinations, we can find the maximizing α and β. We note that the computational complexity of DNN-based power allocation is on the order of $\mathcal{O}(1)$, which is significantly lower than that of the exhaustive search $\mathcal{O}(N_\alpha N_\beta)$. This is because when a DNN is utilized, we need just finite steps of arithmetic calculations to get the optimum power allocation factors, while in the exhaustive search we have to go through every point in the search space. We validate these results by contrasting the time taken to obtain the optimum solution by the two methods upon running them on PYTHON using a dual core 2.2 GHz Intel Xeon microprocessor having search step sizes of $\zeta_\alpha = \zeta_\beta = 10^{-2}$. The running time of the learning-based method is as low as 73 microseconds, while for the exhaustive search this is 4.6 milliseconds. This shows about two orders of magnitude difference between the running time of the learning-based method and the exhaustive search. However, recall from Fig. 8, that the DNN performs better at some SNRs than the exhaustive search for the search step sizes assumed. This means that to get an identical performance to the DNN, we even have to make ζ_α and ζ_β smaller for the full search, leading to much more time for obtaining the solution. These observations show that the exhaustive search method may become infeasible in practical cases and that the learning-based method is more suitable in real-time applications.

VII. CONCLUSION

In this paper, we studied a wirelessly powered cooperative communication scheme, while considering the presence of HWIs for all nodes. We provided analytical results for the system model in the high-SNR regime to obtain better insights on how the power available at the source and destination can affect the secrecy rate. Furthermore, an optimization problem associated with individual power constraints was formulated for maximizing the secrecy rate. Accordingly, a DNN was designed and trained to get the optimum power allocation factors at the source and destination. We showed that the proposed DNN succeeds in matching the secrecy rate performance of the exhaustive search, while its complexity is considerably lower. This makes the DNN designed an attractive choice for real-time applications. Finally, we formulated an optimization problem for optimally sharing the HWIs among the nodes and proposed an MM-based algorithm to solve it. It was shown that the optimal distribution of HWIs can substantially enhance the secrecy rate of our system model across the entire range of SNRs. For our future work, we will consider the deleterious effect of channel estimation error (CEE) in the self-interference cancellation phase for a two-way relaying system. Moreover, considering a multi-node and interference-limited scenario with exponential complexity in the corresponding optimization problem, we will deploy unsupervised deep learning or deep reinforcement learning (DRL) to obtain the optimum power values. Devising deep denoising autoencoders to compensate for the deleterious effects of HWIs and CEEs is another intriguing future research direction. Finally, we note that we have assumed a linear relationship between the hardware cost and quality in our HWI sharing problem. However, the connection between the hardware cost and quality can be nonlinear in practice. A deeper examination of the relationship between the cost and hardware quality for optimum HWI sharing is another interesting research direction.

REFERENCES

[1] X. Chen, D. W. K. Ng, W. Yu, E. G. Larsson, N. Al-Dhahir, and R. Schober, "Massive access for 5G and beyond," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 3, pp. 615–637, Mar. 2021.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[3] T. N. Nguyen et al., "Security-reliability tradeoff analysis for SWIPT-and AF-based IoT networks with friendly jammers," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21662–21675, Nov. 2022.

[4] S. Gong, J. Wang, X. Zhao, S. Ma, and C. Xing, "A framework for hardware impairments-aware multi-antenna transceiver design in IoT systems via majorization–minimization," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 417–433, Jan. 2023.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[6] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138406–138446, 2020.

[7] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[8] X. Zhao, Y. Zhao, J. Huang, W. Zhao, and J. Sun, "Physical layer security for indoor hybrid PLC/VLC networks with NOMA," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 872–884, 2024, doi: 10.1109/OJCOMS.2024.3353385.

[9] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 1–24, Jan. 2022.

[10] S. O. Olatinwo and T.-H. Joubert, "Deep learning for resource management in Internet of Things networks: A bibliometric analysis and comprehensive review," *IEEE Access*, vol. 10, pp. 94691–94717, 2022.

[11] R. Li et al., "Intelligent 5G: When cellular networks meet artificial intelligence," *IEEE Wireless Commun.*, vol. 24, no. 5, pp. 175–183, Oct. 2017.

[12] M. Xia and S. Aissa, "On the efficiency of far-field wireless power transfer," *IEEE Trans. Signal Process.*, vol. 63, no. 11, pp. 2835–2847, Aug. 2015.

[13] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 104–110, Nov. 2014.

[14] J. Hu, K. Yang, G. Wen, and L. Hanzo, "Integrated data and energy communication network: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3169–3219, 4th Quart., 2018.

[15] V. Sharma, J. Yaswanth, S. K. Singh, S. Biswas, K. Singh, and F. Khan, "A pricing-based approach for energy-efficiency maximization in RIS-aided multi-user MIMO SWIPT-enabled wireless networks," *IEEE Access*, vol. 10, pp. 29132–29148, 2022.

[16] B. Clerckx, J. Kim, K. W. Choi, and D. I. Kim, "Foundations of wireless information and power transfer: Theory, prototypes, and experiments," *Proc. IEEE*, vol. 110, no. 1, pp. 8–30, Jan. 2022.

[17] Z. Masood, H. Park, H. S. Jang, S. Yoo, S. P. Jung, and Y. Choi, "Optimal power allocation for maximizing energy efficiency in DAS-based IoT network," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2342–2348, Jun. 2021.

[18] G. Si, Z. Dou, Y. Lin, L. Qi, and M. Wang, "Relay selection and secure connectivity analysis in energy harvesting multi-hop D2D networks," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1245–1248, Jun. 2022.

[19] R. Yao, F. Xu, T. Mekkawy, and J. Xu, "Optimised power allocation to maximise secure rate in energy harvesting relay network," *Electron. Lett.*, vol. 52, no. 22, pp. 1879–1881, May 2016.

[20] M. T. Mamaghani, A. Kuhestani, and K. Wong, "Secure two-way transmission via wireless-powered untrusted relay and external jammer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8451–8465, Sep. 2018.

[21] S. Zhang, S. Kong, K. Chi, and L. Huang, "Energy management for secure transmission in wireless powered communication networks," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1171–1181, Jan. 2022.

[22] T. Schenk, *RF Imperfections in High-Rate Wireless Systems: Impact and Digital Compensation.* Dordrecht, The Netherlands: Springer, 2008.

[23] C. Studer, M. Wenk, and A. Burg, "MIMO transmission with residual transmit-RF impairments," in *Proc. ITG/IEEE Workshop Smart Antennas*, Feb. 2010, pp. 189–196.

[24] V. Shahiri, A. Kuhestani, and L. Hanzo, "Short-packet amplify-and-forward relaying for the Internet-of-Things in the face of imperfect channel estimation and hardware impairments," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 20–36, Mar. 2022.

[25] M. Kazemi, A. Mohammadi, and T. M. Duman, "Analysis of DF relay selection in massive MIMO systems with hardware impairments," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6141–6152, Jun. 2020.

[26] Y. Xu, H. Xie, and R. Q. Hu, "Max–min beamforming design for heterogeneous networks with hardware impairments," *IEEE Commun. Lett.*, vol. 25, no. 4, pp. 1328–1332, Apr. 2021.

[27] E. Björnson, J. Hoydis, M. Kountouris, and M. Debbah, "Massive MIMO systems with non-ideal hardware: Energy efficiency, estimation, and capacity limits," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7112–7139, Nov. 2014.

[28] E. Björnson, A. Papadogiannis, M. Matthaiou, and M. Debbah, "On the impact of transceiver impairments on AF relaying," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, May 2013, pp. 4948–4952.

[29] J. Zhu, D. W. K. Ng, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 2001–2016, Mar. 2017.

[30] A. Kuhestani, A. Mohammadi, K. Wong, P. L. Yeoh, M. Moradikia, and M. R. Khandaker, "Optimal power allocation by imperfect hardware analysis in untrusted relaying networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4302–4314, Jul. 2018.

[31] M. Letafati, A. Kuhestani, and H. Behroozi, "Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things," *IEEE Trans. Inf. Forenics Security*, vol. 15, pp. 2856–2868, 2020.

[32] M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "Hardware-impaired PHY secret key generation with man-in-the-middle adversaries," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 856–860, Apr. 2022.

[33] M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "Deep learning for hardware-impaired wireless secret key generation with man-in-the-middle attacks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[34] M. Moradikia, H. Bastami, A. Kuhestani, H. Behroozi, and L. Hanzo, "Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments," *IEEE Access*, vol. 7, pp. 116942–116964, 2019.

[35] T. Zhao et al., "A survey of deep learning on mobile devices: Applications, optimizations, challenges, and research opportunities," *Proc. IEEE*, vol. 110, no. 3, pp. 334–354, Mar. 2022.

[36] W. Lee, K. Lee, and T. Q. S. Quek, "Deep-learning-assisted wireless-powered secure communications with imperfect channel state information," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 11464–11476, Jul. 2022.

[37] K. Lee, J.-P. Hong, and W. Lee, "Deep learning framework for secure communication with an energy harvesting receiver," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10121–10132, Oct. 2021.

[38] W. Lee and K. Lee, "Deep learning-based transmit power control for wireless-powered secure communications with heterogeneous channel uncertainty," *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 11150–11159, Oct. 2022.

[39] M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "On learning-assisted content-based secure image transmission for delay-aware systems with randomly-distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1125–1139, Feb. 2022.

[40] D. He, C. Liu, H. Wang, and T. Q. S. Quek, "Learning-based wireless powered secure transmission," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 600–603, Apr. 2019.

[41] T. M. Hoang, D. Liu, T. V. Luong, J. Zhang, and L. Hanzo, "Deep learning aided physical-layer security: The security versus reliability trade-off," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 442–453, Jun. 2022.

[42] R. Yao, Y. Zhang, S. Wang, N. Qi, N. I. Miridakis, and T. A. Tsiftsis, "Deep neural network assisted approach for antenna selection in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 1644–1647, Dec. 2019.

[43] X. Zhang and M. Vaezi, "Deep learning based precoding for the MIMO Gaussian wiretap channel," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.

[44] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[45] M. T. Mamaghani, A. Mohammadi, P. L. Yeoh, and A. Kuhestani, "Secure two-way communication via a wireless powered untrusted relay and friendly jammer," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.
[46] D. Wang, R. Zhang, X. Cheng, L. Yang, and C. Chen, "Relay selection in full-duplex energy-harvesting two-way relay networks," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 2, pp. 182–191, Jun. 2017.
[47] D. Wang, R. Zhang, X. Cheng, and L. Yang, "Relay selection in two-way full-duplex energy-harvesting relay networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.
[48] Y. Zhang, J. Ge, J. Men, F. Ouyang, and C. Zhang, "Joint relay selection and power allocation in energy harvesting AF relay systems with ICSI," *IET Microw. Antennas Propag.*, vol. 10, no. 15, pp. 1656–1661, Dec. 2016.
[49] J. Men, J. Ge, C. Zhang, and J. Li, "Joint optimal power allocation and relay selection scheme in energy harvesting asymmetric two-way relaying system," *IET Commun.*, vol. 9, no. 11, pp. 1421–1426, Jul. 2015.
[50] S. Xu, X. Song, Z. Xie, J. Cao, and J. Wang, "Secure transmission for energy harvesting relay networks with the destination self-protection mechanism," *Phys. Commun.*, vol. 40, Jun. 2020, Art. no. 101075. [Online]. Available: https://doi.org/10.1016/j.phycom.2020.101075
[51] K. Hornik, M. Stinchcombe, and H. White, "Multilayer feedforward networks are universal approximators," *Neural Netw.*, vol. 2, no. 5, pp. 359–366, 1989.
[52] I. J. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
[53] M. Ragheb, A. Kuhestani, M. Kazemi, H. Ahmadi, and L. Hanzo, "RIS-aided secure millimeter-wave communication under RF-chain impairments," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 952–963, Jan. 2024.
[54] M. Chiang, "Geometric programming for communication systems," *Found. Trends Commun. Inf. Theory*, vol. 2, nos. 1–2, pp. 1–154, 2005. doi: 10.1561/0100000005.
[55] G. Scutari and Y. Sun, "Parallel and distributed successive convex approximation methods for big-data optimization," in *Multi-Agent Optimization*. New York, NY, USA: Springer-Verlag, Nov. 2018, pp. 141–308.
[56] *Keras Documentation: About Keras*. 2020. [Online]. Available: https://keras.io/about
[57] V. Raj and S. Kalyani, "Backpropagating through the air: Deep learning at physical layer without channel models," *IEEE Commun. Lett.*, vol. 22, no. 11, pp. 2278–2281, Nov. 2018.
[58] H. Xiao, W. Tian, W. Liu, and J. Shen, "ChannelGAN: Deep learning-based channel modeling and generating," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 650–654, Mar. 2022.
[59] T. Erpek, T. J. O'Shea, Y. E. Sagduyu, Y. Shi, and T. C. Clancy, "Deep learning for wireless communications," in *Development and Analysis of Deep Learning Architectures*. Cham, Switzerland: Springer, 2020, pp. 223–266.

VAHID SHAHIRI received the B.Sc. degree in electrical engineering from the University of Zanjan and the M.Sc. degree in electrical engineering from the Amirkabir University of Technology, Iran. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, Sharif University of Technology, Tehran. His current research interests include massive MIMO and RIS-aided communications, integrated sensing and communications, applications of deep and deep reinforcement learning in wireless networks and physical layer security techniques for 6G wireless networks including both keyless and key-based methods.

MOSLEM FOROUZESH received the M.Sc. and Ph.D. degrees in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2016 and 2020, respectively. His current research interests include non-orthogonal multiple access, radio resource allocation in wireless networks, physical-layer security, and covert communication.

HAMID BEHROOZI (Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Tehran, Tehran, Iran, in 2000, the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, in 2003, and the Ph.D. degree in electrical engineering from Concordia University, Montreal, QC, Canada, in 2007. From 2007 to 2010, he was a Postdoctoral Fellow with the Department of Mathematics and Statistics, Queen's University, Kingston, ON, Canada. He is currently an Associate Professor with the Department of Electrical Engineering, Sharif University of Technology. His research interests include information theory, joint source-channel coding, artificial intelligence in signal processing and data science, and cooperative communications. He was the recipient of several academic awards, including the Ontario Postdoctoral Fellowship awarded by the Ontario Ministry of Research and Innovation, Quebec Doctoral Research Scholarship awarded by the Government of Quebec, Hydro Quebec Graduate Award, and Concordia University Graduate Fellowship.

ALI KUHESTANI (Member, IEEE) received the Ph.D. degree in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 2017. From 2018 to 2019, he was a Postdoctoral Researcher with the Department of Electrical Engineering, Sharif University of Technology, Tehran. He has authored and coauthored more than 20 journals in prestigious publication avenues (e.g., the IEEE and IET) and more than ten papers in major conference proceedings. His research interests include physical-layer security of wireless communications, Internet of Things, millimeter-wave communication, massive MIMO system, and space-time coding. He was a recipient of the Iran's National Elites Foundation Award for outstanding students in 2017. He was a Reviewer of the IEEE transactions/journals and conferences.

KAI-KIT WONG (Fellow, IEEE) received the B.Eng., M.Phil., and Ph.D. degrees in electrical and electronic engineering from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. After graduation, he took up academic and research positions with the University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group of Stanford University, and the University of Hull, U.K. He is the Chair of wireless communications with the Department of Electronic and Electrical Engineering, University College London, London, U.K. His research focuses on 5-G and beyond mobile communications. He was a corecipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2000 IEEE VTS Japan Chapter Award at the IEEE Vehicular Technology Conference in Japan in 2000, and a few other international Best Paper Awards. He is a Fellow of *Institution of Engineering and Technology* and is also on the Editorial Board of several international journals. In 2020, he was the Editor-in-Chief of IEEE WIRELESS COMMUNICATIONS LETTERS.