sensors

MDPI

Article

Security–Reliability Analysis of AF Full-Duplex Relay Networks Using Self-Energy Recycling and Deep Neural Networks

Tan N. Nguyen [1], Bui Vu Minh [2,*], Dinh-Hieu Tran [3], Thanh-Lanh Le [3], Anh-Tu Le [4], Quang-Sang Nguyen [5] and Byung Moo Lee [6,*]

1 Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam; nguyennhattan@tdtu.edu.vn
2 Faculty of Engineering and Technology, Nguyen Tat Thanh University, 300A-Nguyen Tat Thanh, Ward 13, District 4, Ho Chi Minh City 754000, Vietnam
3 Department of Technology, Dong Nai Technology University, Bien Hoa 76000, Vietnam; tdh@dntu.edu.vn (D.-H.T.); lethanhlanh@dntu.edu.vn (T.-L.L.)
4 Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava, 17. Listopadu 2172/15, 70800 Ostrava, Czech Republic; tule.iuh@gmail.com
5 Science and Technology Application for Sustainable Development Research Group, Ho Chi Minh City University of Transport, Ho Chi Minh City 70000, Vietnam; sang.nguyen@ut.edu.vn
6 Department of Intelligent Mechatronics Engineering, and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, Republic of Korea
* Correspondence: bvminh@ntt.edu.vn (B.V.M.); blee@sejong.ac.kr (B.M.L.)

Abstract: This paper investigates the security–reliability of simultaneous wireless information and power transfer (SWIPT)-assisted amplify-and-forward (AF) full-duplex (FD) relay networks. In practice, an AF-FD relay harvests energy from the source (S) using the power-splitting (PS) protocol. We propose an analysis of the related reliability and security by deriving closed-form formulas for outage probability (OP) and intercept probability (IP). The next contribution of this research is an asymptotic analysis of OP and IP, which was generated to obtain more insight into important system parameters. We validate the analytical formulas and analyze the impact on the key system parameters using Monte Carlo simulations. Finally, we propose a deep learning network (DNN) with minimal computation complexity and great accuracy for OP and IP predictions. The effects of the system's primary parameters on OP and IP are examined and described, along with the numerical data.

Keywords: physical layer security (PLS); self-energy recycling; full duplex (FD); outage probability (OP); intercept probability (IP); deep learning network (DNN)

Citation: Nguyen, T.N.; Minh, B.V.; Tran, D.-H.; Le, T.-L.; Le, A.-T.; Nguyen, Q.-S.; Lee, B.M. Security–Reliability Analysis of AF Full-Duplex Relay Networks Using Self-Energy Recycling and Deep Neural Networks . *Sensors* **2023**, *23*, 7618. https://doi.org/10.3390/s23177618

Academic Editor: He Fang

Received: 23 June 2023
Revised: 31 August 2023
Accepted: 1 September 2023
Published: 2 September 2023

1. Introduction

The Internet of Things (IoT) is the term employed to describe the interconnection of all physical items with the Internet through information sensing devices for the purpose of information exchange, i.e., the way in which physical objects communicate with one another to accomplish intelligent identification and administration. The future beyond 5G (B5G) IoT and massive machine-type communication (mMTC) will face difficult issues due to massively networked smart gadgets [1]. This is mostly due to the varied quality of service (QoS) provided by the enormous number of such devices for 5G-enabled big IoT networks. As a result of the huge IoT, wireless communication networks will face a variety of issues, including fundamental energy consumption, the use of high-frequency resources, and more [2].

Many approaches have been suggested to boost spectral efficiency (SE) performance. Full-duplex (FD) relaying techniques can, among others, roughly quadruple the SE compared to half-duplex (HD) relaying [3–7]. Additionally, the authors in [8] used

orthogonal frequency division multiple access (OFDMA) technology to expand FD relaying into a multi-user scenario. Recent developments in antenna and transceiver design in FD have demonstrated a high potential for eliminating the self-interference (SI) channel up to the receiver noise floor [9]. By utilizing the physical isolation and separation of the transmitter and receiver, the SI channel can lessen passive cancelation. The SI signal in the received transmission is actively suppressed [10]. The FD relay broadcasts information, and the broadcast characteristics of the wireless medium offer a tremendous problem in guaranteeing secure and reliable communications in the face of adversaries [11,12]. As a result, secure transmission becomes a critical problem that cannot be overlooked. Several transmission techniques for enhancing the secrecy rate were presented [13–16] to prevent secret communications from being eavesdropped in FD relay networks. In [17], the authors investigated a communication network in which a source seeks to interact with an FD destination while being overheard by an eavesdropper. The author in [18] studied the secrecy outage probability (SOP) of the multiple FD decode and forward (DF) relay networks under imperfect channel state information (CSI). In this case, relay selection was applied, which proved to be better than the HD-based strategy. An overview of physical layer security (PLS) schemes for FD co-operative systems was presented in [19]. Furthermore, in a situation with untrusted relays, a source-based jamming strategy was presented, in which the source sends a composite signal comprising the secret and jamming signals to increase secrecy. The authors in [20] examined the scenarios involving different relays and the effects of antenna designs and jamming signals on security. In [21], the authors presented the SOP of an FD jamming relay method, where the source sends data to the relay while sending the jamming signals to the eavesdroppers. Furthermore, the authors in [22] studied a two-hop FD-DF relaying scheme with secrecy rates and optimal power allocation. Finally, Moya. et al. proposed a co-operative network where the FD destination transmits the jamming signal to several amplify-and-forward (AF) untrusted relays in [23].

Energy harvesting (EH) is a workable solution to the problem of limited operation time [24–29]. EH can extend the life of the IoT network or even make it self-sufficient by harvesting energy from the environment, such as vibration, solar, and wind [30]. Since it can harvest energy from radio frequency (RF) signals, providing a more reliable energy supply, wireless power transfer (WPT) offers a more realistic solution to the limited period of operation problem [31–33]. Researchers have further incorporated the WPT properties into wireless communication systems, known as simultaneous wireless information and power transfer (SWIPT), by taking into account the fact that RF signals may transport both information and energy [34–36]. For instance, Chen et al., in [37], investigated limited feedback multi-antenna systems, wherein the trade-off between wireless energy and information transfer was considered. In addition, the authors maximized energy harvesting by using adaptive energy beamforming according to instantaneous CSI. The two protocols for EH, which are time switching (TS) and power splitting (PS), were explored in [38,39], respectively. A part of the time or power of the received signal is utilized for energy harvesting in TS or PS protocols, whereas the remainder is used for information processing. The PLS in the SWIPT network has attracted a lot of researchers, as in [40–42]. The secrecy performance of a single-input multiple-output (SIMO) SWIPT system was explored in [40], in which the base station broadcasts information to the receiver while simultaneously transferring energy to numerous energy-harvesting receivers. The authors in [41] presented a strong, secure transmission system for multiple-input single-output (MISO) SWIPT networks. In [42], the authors offered an effective transmission solution for multiple-input multiple-output (MIMO) wiretap channels, in which the non-concave issue was first turned into a convex optimization and then solved by dealing with its dual problem.

Deep learning has recently evolved as a strong data-driven strategy to solve a variety of complex issues, such as image processing, pattern recognition, and wireless communication applications [43]. The authors in [44] designed a deep neural network (DNN) model to forecast coverage probability in random wireless networks. It should be highlighted that

the DNN model outperforms the mathematical method, which is only appropriate for oversimplified network settings. Moreover, in [45], the authors employed a DNN model to predict the SOP and demonstrate the shortest running time for SOP prediction across simulation and analytical findings in unmanned aerial vehicle networks. Zheng et al., in [46], studied the combination of adjusted, deep deterministic policy gradient (A-DDPG) and convex optimization to optimize the long-term secondary throughput in RF-powered ambient backscatter-assisted hybrid underlay cognitive radio networks.

1.1. Related Work and Motivation

A lot of the current literature has studied the PLS in co-operative relaying networks. In [47], the authors studied the problem of security in untrusted FD relaying using the AF protocol system by applying a source-jamming scheme. However, the author did not consider EH to help improve the lifetime of the device. The authors in [48] investigated security performance in an AF relaying FD system in the presence of a passive eavesdropper. In [49], the authors investigated reliability and security in an AF relaying system in the presence of an eavesdropper. Furthermore, the authors considered friendly jammers to improve the security of the system. However, the authors in [48,49] did not consider FD in co-operative relaying to improve the SE of the system. In addition, the authors of [47–49] did not apply a DNN in order to reduce the overall energy consumption through an offline training process. In addition, Table 1 shows a comparison of our work with related works.

Motivated by the challenges described above, we consider the security–reliability of a SWIPT-assisted FD relay in IoT networks. The FD relay harvests energy based on the PS protocol. In particular, the FD relay is also assumed to have the ability for self-energy recycling to increase the average transmittance power. In addition to harvesting the energy from the source's broadcast signal, the self-interference energy can be recovered and reused [50]. In addition, we apply the DNN method to predict the security–reliability of the proposed system.

Table 1. Comparison of our work with the related work.

	Our Work	**[47]**	**[48]**	**[49]**	**[50]**	**[51]**
Co-operative AF relaying network	√	√	√	√	√	√
FD	√				√	
EH	√			√	√	
PLS	√	√	√	√		√
DNN	√					

1.2. Contributions

The main contributions of this paper are listed as follows:

- We propose a novel SWIPT-assisted AF-FD relay network to evaluate security and reliability trade-offs. In particular, in order to increase EH, the relay can harvest energy from the source and reuse the self-interference channel based on the PS protocol to attain battery-free operation;
- We derive the approximate OP for legitimate communications and the approximate IP for the eavesdropper's channel. The asymptotic expressions for the OP and IP are also examined to give some insight into the system configuration under consideration. In order to verify the derived expressions, Monte-Carlo simulation is adopted;
- The suggested DNN performs almost as well as the simulation while drastically lowering the computing complexity. In comparison to existing machine learning-based regression models for OP/IP prediction, our suggested DNN technique has the lowest root mean square error (RMSE) and takes the shortest time to execute. When

system attributes and channel circumstances vary, the data rate of the considered system can be customized based on the estimated OP/IP.

1.3. Organization

Section 2 describes the system model. Section 3 expresses the performance analysis. Section 4 shows the asymptotic analysis. Section 5 proposes the DNN network. Section 6 presents numerical results. Finally, a conclusion for the obtained results is presented in Section 7.

2. System Model

The proposed system model for wireless communication, in which one source node, S, communicates with one destination node, D, via the help of one FD relay node, R, in the presence of an eavesdropper node, E, that wants to take the information from both R and S is shown in Figure 1. In order to enhance the performance at D, we assumed that S could transmit its signal directly to D and via the relay R. Because of the limited energy, R will need to harvest wireless energy from S and employ the self-energy recycling technique, as seen in [50], and then adopt the total harvested energy to transmit the source data to D using the AF mode. In the AF mode, R amplifies and then forwards the received signal from S to D. Moreover, Table 2 shows the main parameters of our paper.

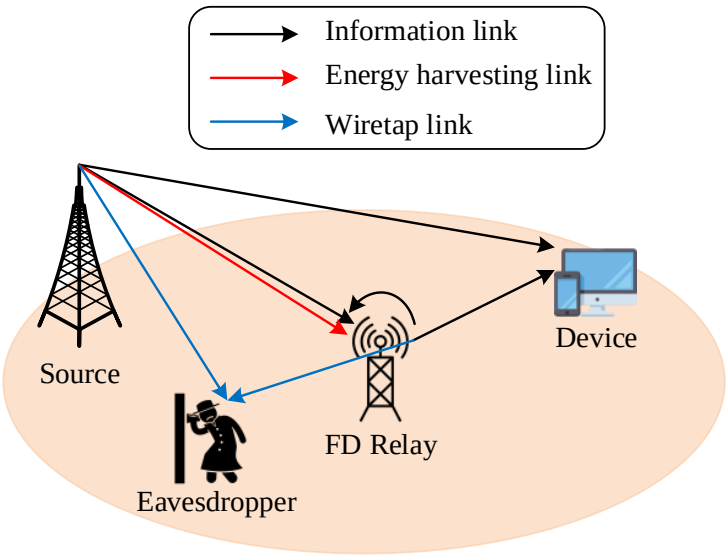

Figure 1. System model.

2.1. Energy Harvesting Model

In the energy harvesting phase, in order to implement self-energy recycling (S-ER), the total harvested energy at R can be expressed as [50]

$$\mathrm{E_R} = \eta\rho\mathrm{T}(P_\mathrm{S}\gamma_\mathrm{SR} + P_\mathrm{R}\gamma_\mathrm{RR}). \tag{1}$$

Then, the transmit power of R can be formulated as

$$P_\mathrm{R} = \frac{\mathrm{E_R}}{\mathrm{T}} = \frac{\eta\rho P_\mathrm{S}\gamma_\mathrm{SR}}{1-\eta\rho\gamma_\mathrm{RR}}. \tag{2}$$

It is worth noting from (2) that $P_\mathrm{R} = 0$ when $\gamma_\mathrm{RR} \geq \frac{1}{\eta\rho}$. In practice, γ_RR is much less than 1 due to passive interference cancellation (IC), such as from antenna isolation, so the denominator in (2) is positive [52].

2.2. Fading Channel Model

Let us denote h_{SD}, h_{SR}, h_{SE}, h_{RD}, and h_{RE} as the channel coefficients of the direct link from source node S to destination node D, and $S \to R, S \to E, R \to D, R \to E$ links, respectively. We also denote h_{RR} as the self-interference coefficient between the transmit and receive antennas of relay node R. Assume that h_X ($X \in \{SD, SR, SE, RD, RE\}$) are Rayleigh fading channels; channel gains $\gamma_X = |h_X|^2$ are exponential random variables (RVs) for which the cumulative distribution function (CDF) is given as

$$F_{\gamma_X}(x) = 1 - \exp(-\lambda_X x). \tag{3}$$

Table 2. Main Parameters.

Notation	Definition
P_S	The transmit power at S
P_R	The transmit power at R
x_S	The transmit signal at S with $\mathbb{E}\{x_S^2\} = P_S$
x_R	The transmit signal at R with $\mathbb{E}\{x_R^2\} = P_R$
η	The conversion efficiency with $0 < \eta \leqslant 1$
ρ	The PS ratio with $0 < \rho < 1$
R_{th}	The target rate
n_R, n_D^1, n_D^2, n_E^1, n_E^2	The AWGN with variance N_0
ω	The path loss exponent
d_{SD}	The distance from S to D
d_{SR}	The distance from S to R
d_{SE}	The distance from S to E
d_{RD}	The distance from R to D
d_{RE}	The distance from R to E
$\mathbb{E}\{\bullet\}$	The expectation operator
$K_\nu(\bullet)$	The modified Bessel function of the second kind with ν-th order:

To take into account the simple path loss model, the parameters can be formulated as follows:

$$\lambda_X = (d_X)^\omega. \tag{4}$$

The RV h_{RR} is also modeled as complex Gaussian RV, and hence $\gamma_{RR} = |h_{RR}|^2$ is also an exponential RV. Then, its CDF is given by

$$F_{\gamma_{RR}}(x) = 1 - \exp(-\lambda_{RR} x). \tag{5}$$

Then, the probability density function (PDF) of γ_Y is given by

$$f_{\gamma_Y}(x) = \xi \exp(-\xi x), \tag{6}$$

where $\xi \in \{\lambda_{SR}, \lambda_{SD}, \lambda_{RD}, \lambda_{SE}, \lambda_{RE}, \lambda_{RR}\}$.

2.3. Transmission Model

In the information transmission phase, the received signal at R is given as follows:

$$y_R = \sqrt{1-\rho} h_{SR} x_S + \sqrt{1-\rho} h_{RR} x_R + n_R. \tag{7}$$

Moreover, in this phase, the received signal at D and E are respectively given by:

$$y_D^1 = h_{RD} x_R + n_D^1, \tag{8}$$

$$y_E^1 = h_{RE} x_R + n_E^1. \tag{9}$$

In our proposed system, the AF protocol is applied. Hence, after receiving the information from S, R will amplify this information to D and E by the given amplification factor β, as follows:

$$\beta = \frac{x_R}{y_R} = \sqrt{\frac{\mathbb{E}\{|x_R|^2\}}{\mathbb{E}\{|y_R|^2\}}} = \sqrt{\frac{P_R}{(1-\rho)\gamma_{SR}P_S+(1-\rho)\gamma_{RR}P_R+N_0}}. \tag{10}$$

By combining (7), (8), (9), and (10), we obtain the received signal at D and E as follows:

$$\begin{aligned} y_D^1 &= h_{RD}\beta\left[\sqrt{1-\rho}h_{SR}x_S + \sqrt{1-\rho}h_{RR}x_R + n_R\right] + n_D^1 \\ &= \underbrace{h_{RD}\beta\sqrt{1-\rho}h_{SR}x_S}_{signal} + \underbrace{h_{RD}\beta\sqrt{1-\rho}h_{RR}x_R}_{interference} + \underbrace{h_{RD}\beta n_R + n_D^1}_{noise}, \end{aligned} \tag{11}$$

and

$$y_E^1 = \underbrace{h_{RE}\beta\sqrt{1-\rho}h_{SR}x_S}_{signal} + \underbrace{h_{RE}\beta\sqrt{1-\rho}h_{RR}x_R}_{interference} + \underbrace{h_{RE}\beta n_R + n_E^1}_{noise}. \tag{12}$$

The received signal-to-interference plus noise ratio (SINR) at D and E in this phase can be, thus, calculated using the following expressions:

$$\gamma_D^1 = \frac{\mathbb{E}\{|signal|^2\}}{\mathbb{E}\{|noise|^2\}} = \frac{\gamma_{SR}\gamma_{RD}\beta^2(1-\rho)P_S}{\gamma_{RR}\gamma_{RD}\beta^2(1-\rho)P_R+\gamma_{RD}\beta^2N_0+N_0}, \tag{13}$$

and

$$\gamma_E^1 = \frac{\mathbb{E}\{|signal|^2\}}{\mathbb{E}\{|noise|^2\}} = \frac{\gamma_{SR}\gamma_{RE}\beta^2(1-\rho)P_S}{\gamma_{RR}\gamma_{RE}\beta^2(1-\rho)P_R+\gamma_{RE}\beta^2N_0+N_0}. \tag{14}$$

By substituting (2) into (13) and (14) and then carrying out some algebra, the SINR at D and E can be rewritten as

$$\gamma_D^1 = \frac{\gamma_{SR}\gamma_{RD}\eta\rho(1-\eta\rho\gamma_{RR})\Psi}{\gamma_{SR}\gamma_{RD}\eta^2\rho^2\Psi\gamma_{RR}-\eta\rho\gamma_{RR}+1}, \tag{15}$$

$$\gamma_E^1 = \frac{\gamma_{SR}\gamma_{RE}\eta\rho(1-\eta\rho\gamma_{RR})\Psi}{\gamma_{SR}\gamma_{RE}\eta^2\rho^2\Psi\gamma_{RR}-\eta\rho\gamma_{RR}+1}, \tag{16}$$

where $\Psi = \frac{P_S}{N_0}$ denotes the average transmited signal-to-noise ratio (SNR).

In our proposed model, the direct link is considered. Hence, in the broadcast phase, D can be received, and the direct signal from S and E can overhear this signal when S broadcasts to R and D. As a result, the received signal at D and E can be thus expressed by

$$y_D^2 = h_{SD}x_S + n_D^2, \tag{17}$$

$$y_E^2 = h_{SE}x_S + n_E^2. \tag{18}$$

The SNR at D and E in this phase can be computed respectively by

$$\gamma_D^2 = \Psi\gamma_{SD}, \tag{19}$$

$$\gamma_E^2 = \Psi\gamma_{SE}. \tag{20}$$

Finally, by adopting the selection-combining (SC) technique at the receiver, the end-to-end SNR at D and E can be respectively claimed as

$$\gamma_D = \max\left(\gamma_D^1, \gamma_D^2\right), \tag{21}$$

$$\gamma_E = \max\left(\gamma_E^1, \gamma_E^2\right). \tag{22}$$

3. Performance Analysis

In this section, the performance of the proposed system is studied. In particular, the closed-form outage probability (OP) and intercept probability (IP) are derived.

3.1. Outage Probability Analysis

The OP of the system can be expressed by

$$\mathrm{OP} = \Pr(\gamma_D \leqslant \gamma_{th}), \tag{23}$$

where $\gamma_{th} = 2^{R_{th}} - 1$ is the threshold, and R_{th} is the target rate. From (21) and (23), the OP can be rewritten as

$$\begin{aligned}
\mathrm{OP} &= \Pr\left(\max\left(\gamma_D^1, \gamma_D^2\right) \leqslant \gamma_{th}\right) \\
&= \Pr\left(\max\left(\frac{\gamma_{SR}\gamma_{RD}\eta\rho(1-\eta\rho\gamma_{RR})\Psi}{\gamma_{SR}\gamma_{RD}\eta^2\rho^2\Psi\gamma_{RR} - \eta\rho\gamma_{RR} + 1}, \Psi\gamma_{SD}\right) \leqslant \gamma_{th}\right) \\
&= \underbrace{\Pr(\Psi\gamma_{SD} \leqslant \gamma_{th})}_{Y_1} \underbrace{\Pr\left(\frac{\gamma_{SR}\gamma_{RD}\eta\rho(1-\eta\rho\gamma_{RR})\Psi}{\gamma_{SR}\gamma_{RD}\eta^2\rho^2\Psi\gamma_{RR} - \eta\rho\gamma_{RR} + 1} \leqslant \gamma_{th}\right)}_{Y_2}.
\end{aligned} \tag{24}$$

Based on (24), Y_1 can be figured out as

$$Y_1 = \Pr(\Psi\gamma_{SD} \leqslant \gamma_{th}) = \Pr\left(\gamma_{SD} \leqslant \frac{\gamma_{th}}{\Psi}\right) = 1 - \exp\left(-\frac{\lambda_{SD}\gamma_{th}}{\Psi}\right). \tag{25}$$

Next, Y_2 can be, thus, computed by

$$\begin{aligned}
Y_2 &= \Pr\left(\frac{\gamma_{SR}\gamma_{RD}\eta\rho(1-\eta\rho\gamma_{RR})\Psi}{\gamma_{SR}\gamma_{RD}\eta^2\rho^2\Psi\gamma_{RR} - \eta\rho\gamma_{RR} + 1} \leqslant \gamma_{th}\right) \\
&= \Pr\left(\gamma_{SRD} < \frac{\gamma_{th}(1-\eta\rho\gamma_{RR})}{\eta\rho(1-\eta\rho\gamma_{RR})\Psi - \gamma_{th}\eta^2\rho^2\Psi\gamma_{RR}}\right),
\end{aligned} \tag{26}$$

where $\gamma_{SRD} = \gamma_{SR}\gamma_{RD}$. From (26), there are two cases to calculate Y_2. In the first case, when $\gamma_{RR} \leqslant \frac{1}{\eta\rho(1+\gamma_{th})}$, we obtain $Y_2 = \Pr\left(\gamma_{SRD} < \frac{\gamma_{th}(1-\eta\rho\gamma_{RR})}{\eta\rho(1-\eta\rho\gamma_{RR})\Psi - \gamma_{th}\eta^2\rho^2\Psi\gamma_{RR}}\right)$. In the second case, when $\gamma_{RR} > \frac{1}{\eta\rho(1+\gamma_{th})}$, we obtain $Y_2 = 1$. Then, in case $\gamma_{RR} \leqslant \frac{1}{\eta\rho(1+\gamma_{th})}$, Y_2 can be calculated as

$$Y_2 = \int_{\frac{1}{\eta\rho(1+\gamma_{th})}}^{+\infty} f_{\gamma_{RR}}(y)dy + \int_0^{\frac{1}{\eta\rho(1+\gamma_{th})}} F_{\gamma_{SRD}}\left[\frac{\gamma_{th}(1-\eta\rho y)}{\eta\rho(1-\eta\rho y)\Psi - \gamma_{th}\eta^2\rho^2\Psi y}\right] f_{\gamma_{RR}}(y)dy. \tag{27}$$

In order to find Y_2, first, we have to derive the CDF of γ_{SRD}. As a result, we claim

$$\begin{aligned}
F_{\gamma_{SRD}}(x) &= \Pr(\gamma_{SRD} < x) = \Pr\left(\gamma_{SR} < \frac{x}{\gamma_{RD}}\right) \\
&= \int_0^{+\infty} F_{\gamma_{SR}}\left(\frac{x}{y}\right) f_{\gamma_{RD}}(y)dy \\
&= 1 - \int_0^{+\infty} \lambda_{RD} \exp\left(-\frac{\lambda_{SR}x}{y} - \lambda_{RD}y\right)dy.
\end{aligned} \tag{28}$$

By applying [53] (Eq. 3.324.1), we obtain

$$F_{\gamma_{\mathrm{SRD}}}(x) = 1 - 2\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}x}K_1\left(2\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}x}\right), \tag{29}$$

where $K_\nu(\bullet)$ is the modified Bessel function of the second kind with ν-th order. From (26) and (29), Y_2 can be found as

$$\mathrm{Y}_2 = 1 - 2\lambda_{\mathrm{RR}}\int_0^{\frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}} \sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\Lambda(y)}\exp(-\lambda_{\mathrm{RR}}y)K_1\left(2\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\Lambda(y)}\right)dy, \tag{30}$$

where $\Lambda(y) = \frac{\gamma_{\mathrm{th}}(1-\eta\rho y)}{\eta\rho(1-\eta\rho y)\Psi - \gamma_{\mathrm{th}}\eta^2\rho^2\Psi y}$. Unfortunately, the integral in Y_2 presents a tough task in terms of finding a closed-form expression. Therefore, we apply the Gaussian-Chebyshev quadrature in [54] to approximate this. As a result, Y_2 can be obtained by

$$\begin{aligned}\mathrm{Y}_2 \approx 1 - \frac{\pi\lambda_{\mathrm{RR}}}{N\eta\rho(1+\gamma_{\mathrm{th}})}\sum_{n=1}^{N}\sqrt{1-\varphi_n^2}\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\Lambda\left(\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)} \\ \times\exp\left(-\lambda_{\mathrm{RR}}\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)K_1\left(2\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\Lambda\left(\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)}\right),\end{aligned} \tag{31}$$

where $\varphi_n = \cos\left(\frac{2n-1}{2N}\pi\right)$. Finally, by substituting (25) and (31) into (23), the OP can be, thus, obtained as

$$\begin{aligned}\mathrm{OP} \approx \left\{1-\exp\left(-\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Psi}\right)\right\}\left\{1 - \frac{\pi\lambda_{\mathrm{RR}}}{N\eta\rho(1+\gamma_{\mathrm{th}})}\sum_{n=1}^{N}\sqrt{1-\varphi_n^2}\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\Lambda\left(\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)}\right. \\ \left.\times\exp\left(-\lambda_{\mathrm{RR}}\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)K_1\left(2\sqrt{\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\Lambda\left(\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)}\right)\right\}.\end{aligned} \tag{32}$$

3.2. Intercept Probability Analysis

The considered system will be wiretapped if E can successfully decode the received signals from the source and relay [55,56]. Therefore, the IP is given by

$$\begin{aligned}\mathrm{IP} &= \Pr(\gamma_{\mathrm{E}} \geqslant \gamma_{\mathrm{th}}) = 1 - \Pr(\gamma_{\mathrm{E}} < \gamma_{\mathrm{th}}) \\ &= 1 - \{\Pr(\Psi\gamma_{\mathrm{SE}} < \gamma_{\mathrm{th}})\}\left\{\Pr\left(\frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RE}}\eta\rho(1-\eta\rho\gamma_{\mathrm{RR}})\Psi}{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RE}}\eta^2\rho^2\Psi\gamma_{\mathrm{RR}} - \eta\rho\gamma_{\mathrm{RR}} + 1}\right) < \gamma_{\mathrm{th}}\right\}.\end{aligned} \tag{33}$$

As a similar proof for OP, the IP can be achieved by

$$\begin{aligned}\mathrm{IP} \approx 1 - \left\{1-\exp\left(-\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Psi}\right)\right\}\left\{1 - \frac{\pi\lambda_{\mathrm{RR}}}{N\eta\rho(1+\gamma_{\mathrm{th}})}\sum_{n=1}^{N}\sqrt{1-\varphi_n^2}\sqrt{\lambda_{\mathrm{SR}}\lambda\Lambda\left(\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)}\right. \\ \left.\times\exp\left(-\lambda_{\mathrm{RR}}\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)K_1\left(2\sqrt{\mathrm{SR}\lambda_{\mathrm{RE}}\Lambda\left(\frac{(1+\varphi_n)}{2\eta\rho(1+\gamma_{\mathrm{th}})}\right)}\right)\right\},\end{aligned} \tag{34}$$

where $\Lambda(y) = \frac{\gamma_{\mathrm{th}}(1-\eta\rho y)}{\eta\rho(1-\eta\rho y)\Psi - \gamma_{\mathrm{th}}\eta^2\rho^2\Psi y}$.

4. Asymptotic Analysis

In this section, we develop the asymptotic equations for OP as the transmitted SNR approaches infinity, i.e., $\Psi \to +\infty$, to give us more insights into the performance analysis of the network under consideration.

4.1. Op Analysis

When $\Psi \to +\infty$, γ_D can be rewritten as

$$\gamma_D^{\Psi \to +\infty} \approx \max\left(\Psi \gamma_{SD}, \frac{1}{\eta \rho \gamma_{RR}} - 1\right). \tag{35}$$

Then, the OP can be obtained by

$$\begin{aligned} OP^{\Psi \to +\infty} &= \Pr\left(\gamma_D^{\Psi \to +\infty} < \gamma_{th}\right) \\ &= \Pr\left(\gamma_{SD} < \frac{\gamma_{th}}{\Psi}\right) \Pr\left(\gamma_{RR} > \frac{1}{\eta \rho (1 + \gamma_{th})}\right) \\ &= \left[1 - \exp\left(-\frac{\lambda_{SD} \gamma_{th}}{\Psi}\right)\right] \exp\left(-\frac{\lambda_{RR}}{\eta \rho (1 + \gamma)}\right). \end{aligned} \tag{36}$$

4.2. Ip Asymptotic Analysis

As a result, in this case, the IP also can be obtained by

$$IP^{\Psi \to +\infty} = \exp\left(-\frac{\lambda_{SE} \gamma_{th}}{\Psi}\right)\left[1 - \exp\left(-\frac{\lambda_{RR}}{\eta \rho (1 + \gamma_{th})}\right)\right]. \tag{37}$$

5. Dnn Network

In this section, we propose a DNN to predict the OP and IP without relying on the statistical model, whereas the traditional analysis and Monte Carlo simulations need an accurate statistical model. In addition, when the system model is complicated, and it is difficult to use the mathematical derivation technique, the DNN model, which is a data-driven approach, becomes an alternate answer. Therefore, the DNN will help the proposed system to achieve a short run time.

5.1. the DNN Design Description

First, we create a DNN model as a regression issue. As illustrated in Figure 2, the DNN model consists of an input layer, numerous hidden layers, and an output layer. The following is a summary of how each layer contributes to training the DNN model:

- Data is sent to the input layer so that the DNN model may determine how the system parameters relate to the relevant OP/IP. The number of neurons in the input layer is, therefore, equal to the number of parameters and does not serve as an activation function;
- The number of hidden layers primarily determines the relationship between the input and output data. In order to accurately calculate the relationship, each connection in each hidden neuron has a separate weight and bias. In order to enhance computational effectiveness, each hidden neuron also has a nonlinear activation function;
- The output layer combines the findings of various hidden layers to predict OP/IP. As a result, there is just one neuron in the output layer. The neuron in the output layer lacks an activation function, much like the input layer.

Furthermore, we have 10 neurons corresponding to 10 parameters, as shown in Table 3 for the input layer. In the hidden layers, each layer k with $k = 1, \ldots, D_{hidden}$ has D_{neu} neurons, and it employs the exponential linear unit (ELU) activation function, which can be given as [57,58]

$$ELU(z) = \begin{cases} \varphi(\exp(z) - 1), & \text{If}: \quad z < 0 \\ z, & \text{If}: \quad z \geqslant 0 \end{cases} \tag{38}$$

where φ denotes the constant value initialized to 1. Since the regression problem tries to estimate an output value without additional conversion, the output layer comprises one neuron that uses the linear activation function to produce the predicted OP/IP value, Out.

Table 3. Theparameters for DNN training and testing.

Input	Value	Input	Value
ω	2	λ_{RR}	[2,4]
d_{SD}	1.5	η	0.8
d_{SR}	1	ρ	0.25
d_{RD}	0.5	γ	[0.5,1]
d_{RE}	1	Ψ	[−5,25]

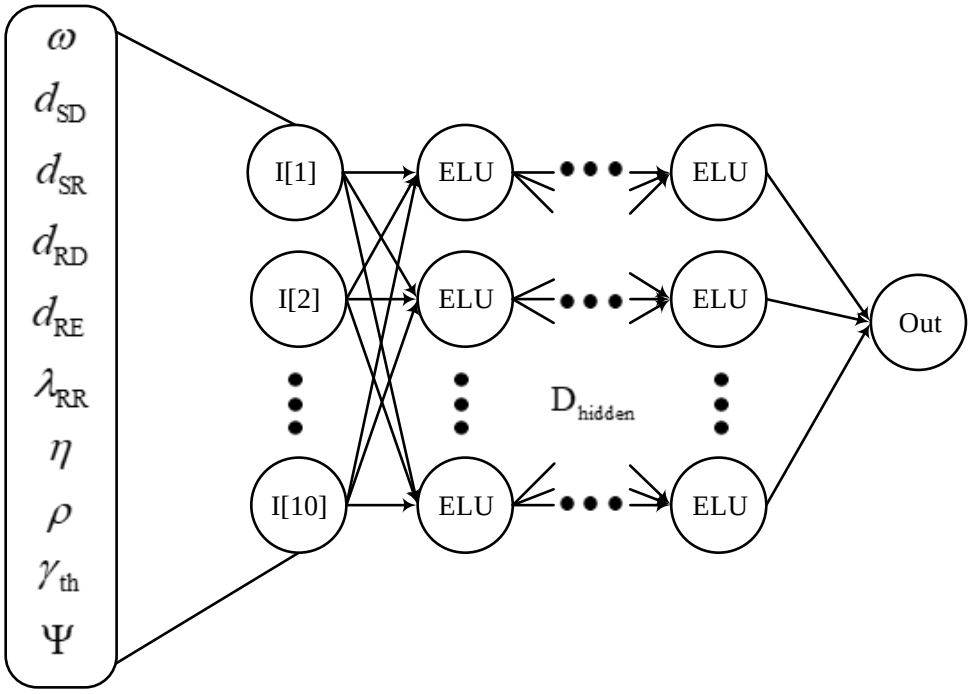

Figure 2. A diagram of the DNN architecture.

5.2. Dataset Setup

In this subsection, we generate dataset $\mathcal{D}$ as a row vector for each sample i, i.e., Data $[k] = [\mathbf{I}[k], \text{Out}_{\text{Sim}}]$, where $\mathbf{I}[k]$ is the feature vector containing all the inputs from the parameters listed in Table 3. Each feature $\mathbf{I}[k]$ is utilized to produce real-value OP/IP sets from (23) and (33); this is input into the simulation, and a unique matching Out_{Sim} is returned. In conclusion, we built the dataset by generating 10^5 samples, concatenating them, and then dividing this into a new dataset with 80% for training ($\mathcal{D}_{\text{train}}$), 10% for validation ($\mathcal{D}_{\text{vali}}$), and 10% for testing ($\mathcal{D}_{\text{test}}$). Moreover, we set the DNN model to have four hidden layers and 128 hidden neurons, which is implemented in Python 3.11.4 using Keras 2.8.0 and TensorFlow 2.8.0. Furthermore, the DNN model is trained in 100 epochs. The deep model is specifically constructed using hardware with an AMDRyzen Threadripper 3970X 32-core CPU and an Nvidia GeForce RTX-2070 super GPU for rapid training and experiment simulations.

The estimation accuracy of the DNN model is calculated using the mean-square error (MSE), which is formally stated as $\text{MSE} = \frac{1}{\mathcal{D}_{\text{test}}} \sum_{k=0}^{\mathcal{D}_{\text{test}}-1} [\text{Out}_{\text{Pre}} - \text{Out}_{\text{Sim}}]$. Furthermore, the appropriate weights and biases for each connection are determined by applying the Adam optimizer [59]. The difference between the natural and predicted OP/IP values

throughout the full test set, which is specified as RMSE $= \sqrt{\text{MSE}}$, is measured by using the RMSE in the OP/IP prediction.

6. Numerical Results

In this section, we provide the analysis findings to evaluate the proposed system in terms of OP and IP, as well as the simulation results, by using the Monte Carlo approach, as per [60,61], to validate our analytical derivations. The main parameter can be shown in Table 3, except for some specific cases.

In Figure 3, we utilize the validation set to evaluate the accuracy of the training. As can be observed, when increasing the epoch and number of hidden layers, the MSE decreased. Moreover, the MSE in the four hidden layers is the best case. Although the DNN model contains four hidden layers that may generalize the dataset and improve network capacity, the second and third hidden layers are unable to learn the intricate patterns in a high-dimensional dataset, resulting in a large MSE.

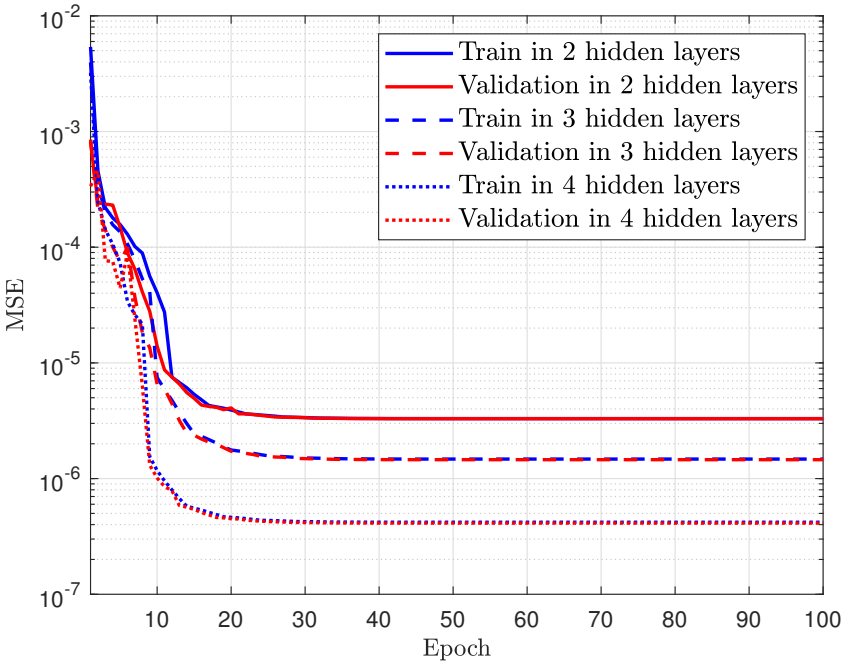

Figure 3. MSE convergence in training and evaluating the DNN with varying the hidden layers.

Figures 4 and 5 show the OP and IP versus Ψ(dB) with different γ_{th}. As observed, the OP and IP curves correspond exactly to the Monte Carlo simulation results. By looking at Figure 4, the OP performance decreases if the Ψ increases. When Ψ is large, the SINR will significantly improve, and this will make the OP performance better. In Figure 5, it can be observed that as Ψ increases, the IP performance also increases. This is expected because an eavesdropper is more likely to overhear the message when the transmission power at S is higher. At a high SNR, i.e., $\Psi \to \infty$, it can be seen that the asymptotic OP and IP curves closely match the actual findings. Specifically, the IP converges to the asymptotic value when $\Psi = 15$(dB), whereas the OP converges to the asymptotic value at a higher Ψ ($\Psi > 25$(dB), which cannot be seen in Figure 4). In addition, it can be shown that the DNN-based prediction results are very similar to the simulation and analysis results for OP and IP, demonstrating the superior prediction capabilities of the DNN.

In Figures 6 and 7, we plot the OP and IP versus λ_{RR} with different η. In Figure 6, increasing the λ_{RR} between the transmitting and receiving antennas at the relay decreases the OP. It can be explained by the fact that increasing λ_{RR} will make the γ_{D}^{1} in (15) larger; hence, the OP will be better. Moreover, when increasing energy efficiency η, the average transmit power at R will be higher, and this will then lead to an improvement in OP.

Furthermore, when increasing λ_{RR} and η, the SINR at E becomes larger. Thus, the possibility of E eavesdropping on information from S and R is also very high. So, the problem is that we have to trade-off between security and reliability in terms of OP and IP. This means that if the system wants to operate well, we must accept high eavesdropping information and vice versa.

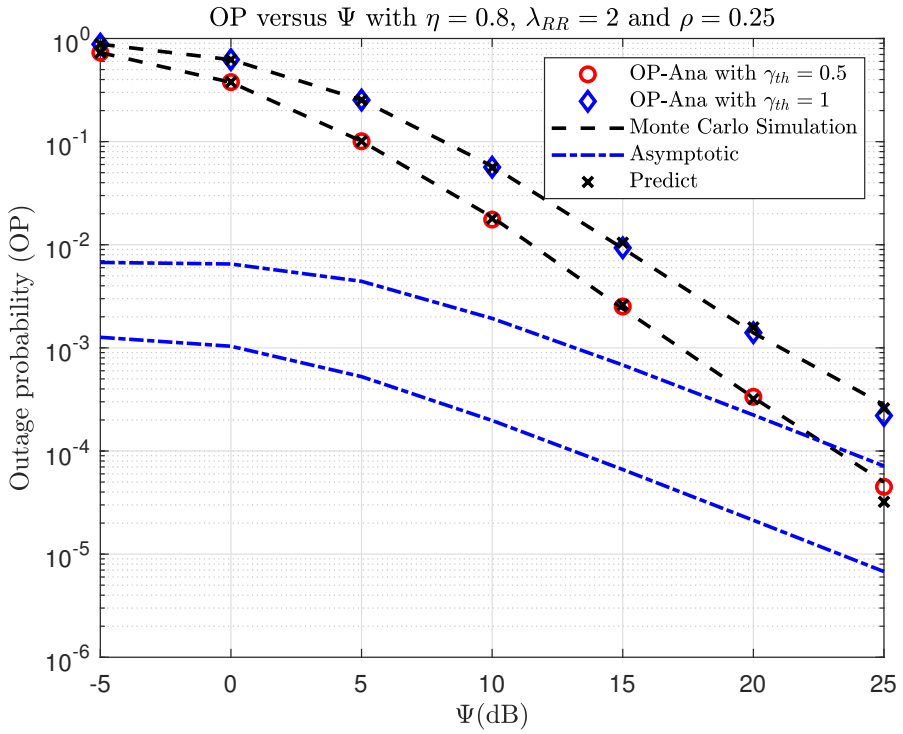

Figure 4. TheOP versus Ψ(dB) when varying γ_{th} with $\eta = 0.8$, $\lambda_{RR} = 2$, and $\rho = 0.25$.

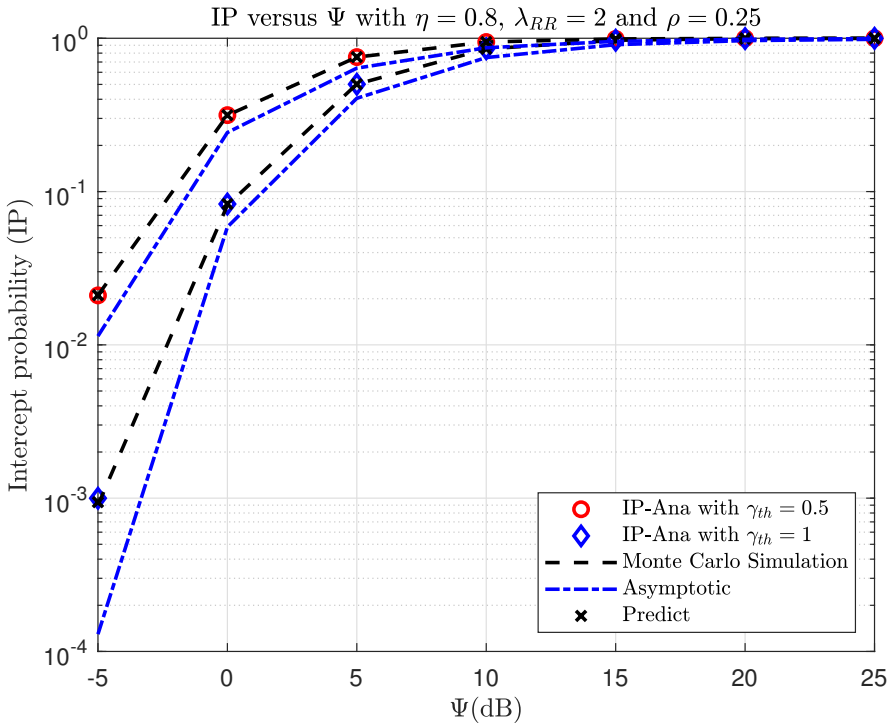

Figure 5. TheIP versus Ψ(dB) when varying γ_{th} with $\eta = 0.8$, $\lambda_{RR} = 2$, and $\rho = 0.25$.

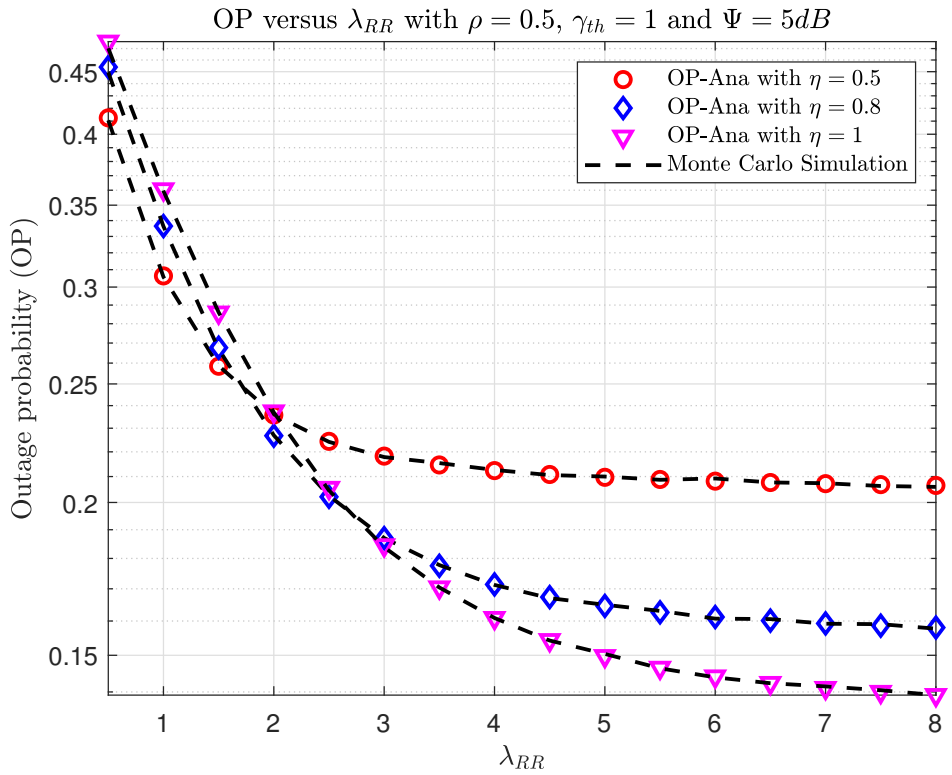

Figure 6. The OP versus λ_{RR} when varying η with $\rho = 0.5$, $\gamma_{th} = 1$, and $\Psi = 5$(dB).

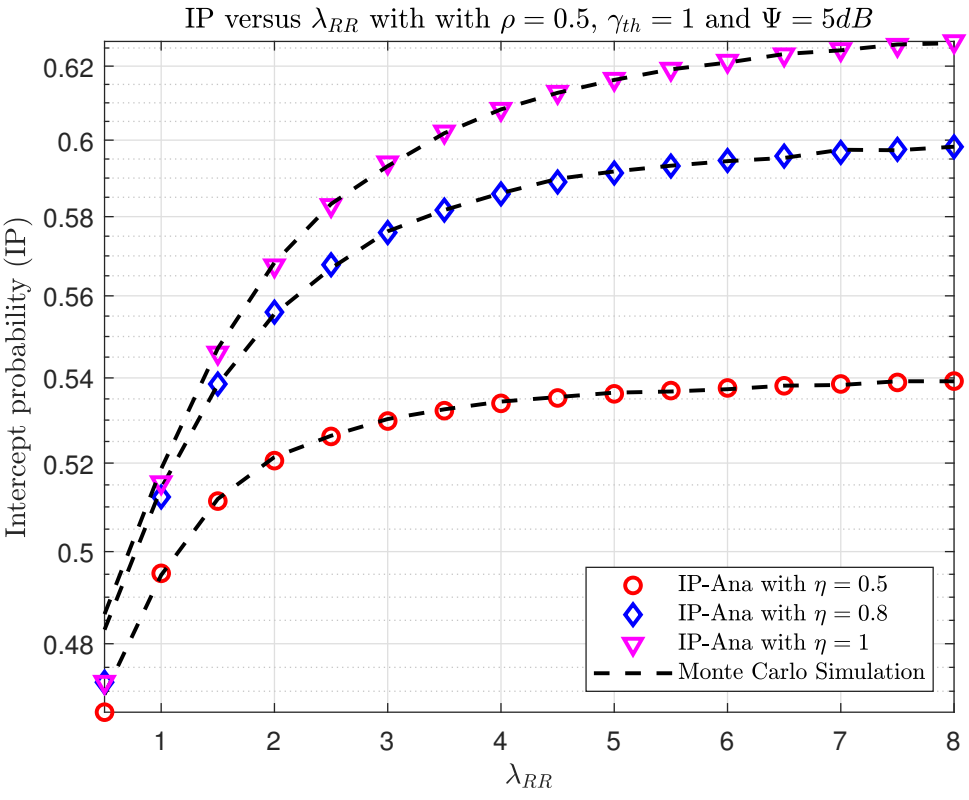

Figure 7. The IP versus λ_{RR} when varying η with $\rho = 0.5$, $\gamma_{th} = 1$, and $\Psi = 5$(dB).

In Figures 8 and 9, we plot the OP and IP versus Ψ(dB) with different PS factors, ρ. First, The higher the Ψ value in Figure 8, the better the OP. This is explained by the fact that

the higher the Ψ value, the more the transmitted power of source S is assigned. Second, it is easy to observe that the OP decreases when the PS factor increases. Third, it can be seen that for a small Ψ (Ψ < 5(dB)), the use of a large PS factor is more beneficial. Reversely, at higher Ψ, the smaller ρ is better. The reason is as follows. For the high-noise environment case, higher transmitted power at the relay is needed to guarantee successful communication. That means more energy needs to be harvested at the relay, so a larger ρ is better. On the other hand, if Ψ is large, then the decoding of the message at the relay is more important. That means we should select the smaller ρ. As can be observed in Figure 9, the intercept performance improves when Ψ increases. This is expected because the eavesdropper has a better chance of overhearing the communication with a greater source transmit power, S. When Ψ is large enough, the IP can converge to one. The eavesdropper's IP increases as the PS factor increases, which is due to the high transmitted power of relay R.

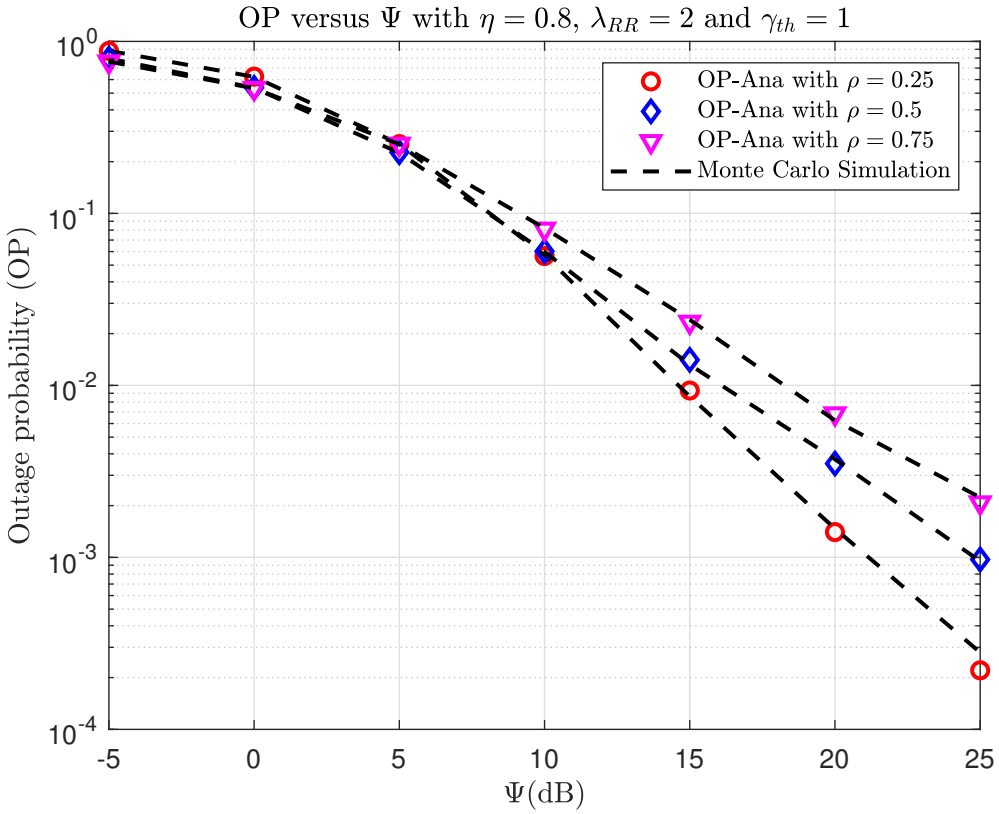

Figure 8. TheOP versus Ψ(dB) when varying ρ with $\eta = 0.8$, $\lambda_{RR} = 2$, and $\gamma_{th} = 1$.

Figures 10 and 11 show the OP and IP versus ρ with different γ_{th}, respectively. The ρ value is significant since it determines not only the quantity of gathered energy at the relay but also the data transfer. First, we can observe in Figure 10 that increasing the target data required leads to an increase in OP. Second, when $0.4 < \rho < 0.5$, the system achieves the best OP performance. In addition, when ρ increases the interception, performance increases, and when increasing γ_{th}, this will decrease the interception performance, similar to Figure 5.

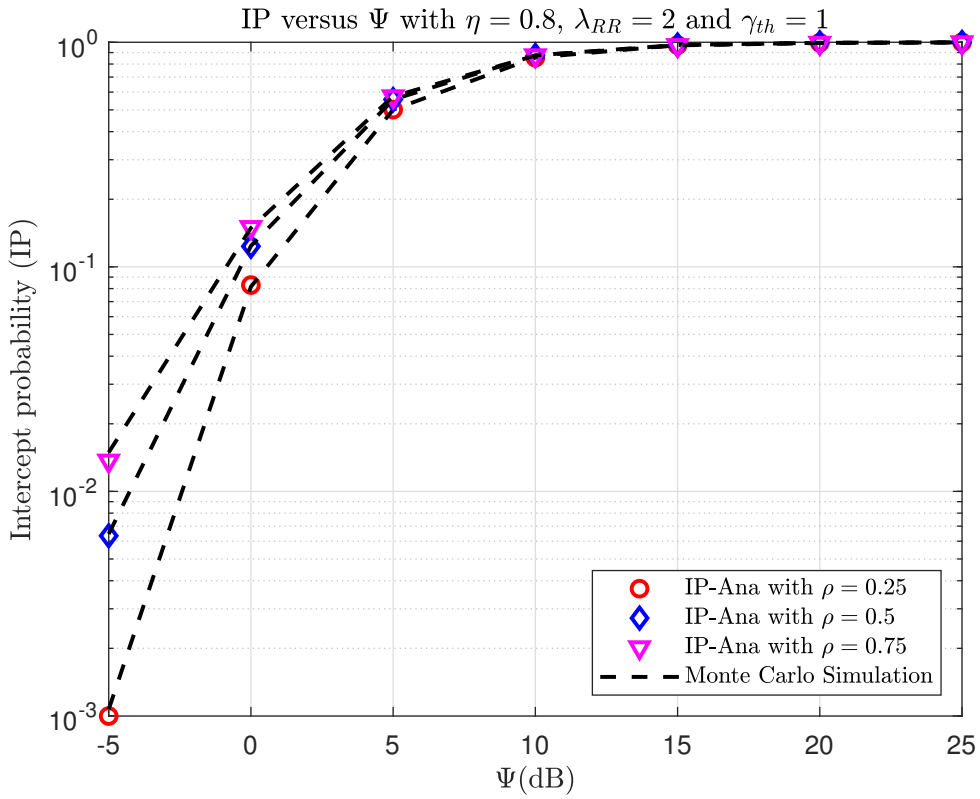

Figure 9. TheIP versus Ψ(dB) when varying ρ with $\eta = 0.8$, $\lambda_{RR} = 2$, and $\gamma_{th} = 1$.

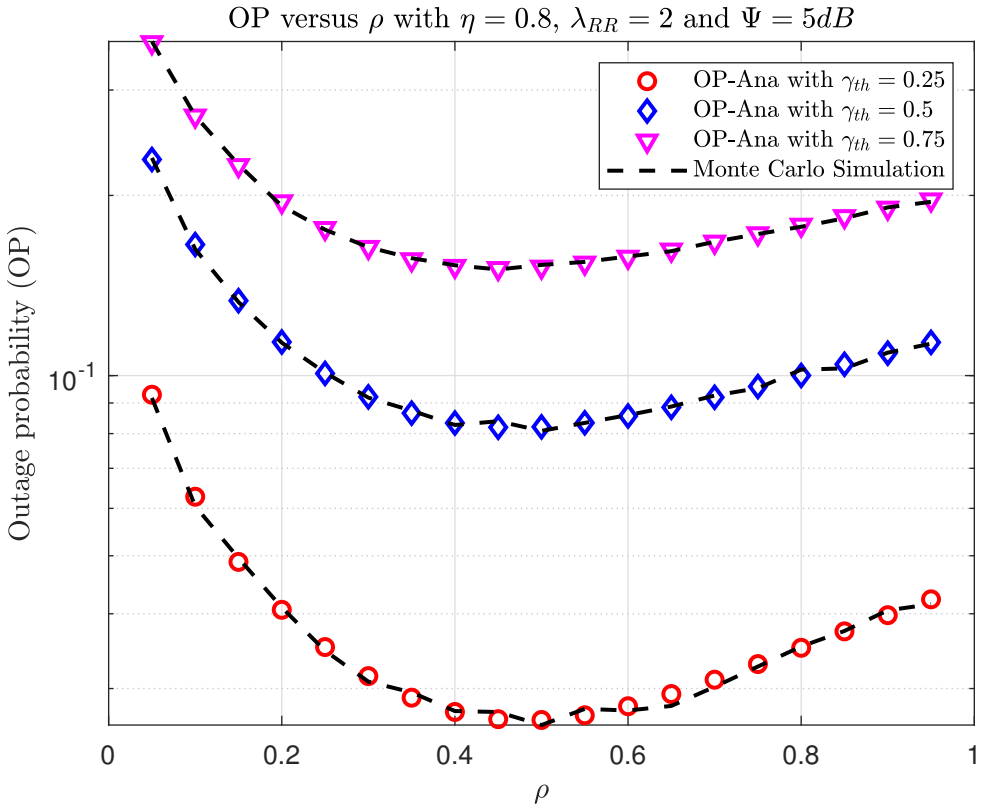

Figure 10. TheOP versus ρ when varying γ_{th} with $\eta = 0.8$, $\lambda_{RR} = 2$, and $\Psi_{th} = 5$(dB).

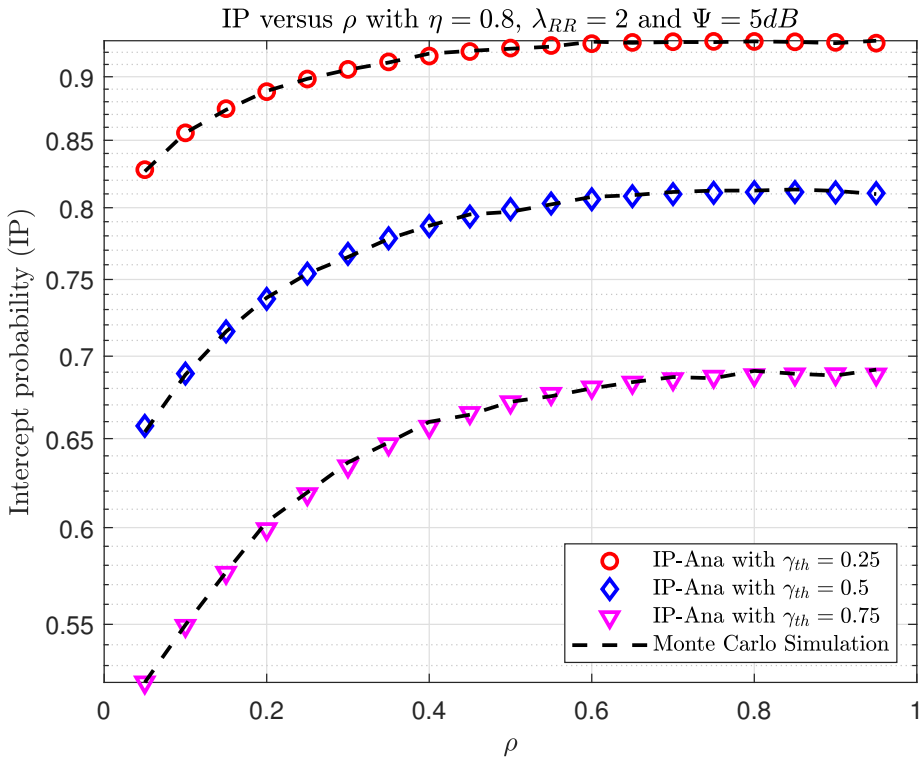

Figure 11. The IP versus ρ when varying γ_{th} with $\eta = 0.8$, $\lambda_{RR} = 2$, and $\Psi_{th} = 5$(dB).

7. Conclusions

We investigated the security and reliability of SWIPT-assistance and self-energy recycling in an AF-FD relay network consisting of an EH relay and a destination in the presence of an eavesdropper. We also evaluated the performance of the security–reliability trade-offs in terms of the OP and IP. Furthermore, Monte Carlo simulation was utilized to verify and examine the influence of the system settings on network performance, as well as the accuracy of the analytical formulations. The OP/IP asymptotic analysis was also performed to offer some insight into the system characteristics. Deep learning was developed as a novel method for predicting the system's OP and IP with minimal computing complexity and good accuracy, which has not been investigated previously. The numerical findings demonstrated that when utilizing DNN prediction, the OP and IP outcomes were almost identical to the Monte-Carlo simulation and analysis results. As a result, deploying a DNN as a black box might be viewed as a potentially promising and effective technique for evaluating system performances via a low-latency inference procedure that avoids the derivation of complicated closed-form expressions in actual network contexts.

Author Contributions: Q.-S.N. and B.M.L. conceived the study idea. A.-T.L. and T.N.N. derived the mathematical framework and proofread the manuscript. B.V.M. performed data curation and software. D.-H.T. and T.-L.L. investigated the system model. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Korean government (MSIT) under Grant NRF-2023R1A2C1002656 and supported by the MSIT (Ministry of Science and ICT), Korea under Grant IITP-2023-RS-2022-00156345 (ICT Challenge and Advanced Network of HRD Program).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jacob, S.; Menon, V.G.; Joseph, S.; Vinoj, P.; Jolfaei, A.; Lukose, J.; Raja, G. A novel spectrum sharing scheme using dynamic long short-term memory with CP-OFDMA in 5G networks. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *6*, 926–934. [CrossRef]
2. Chinnadurai, S.; Yoon, D. Energy efficient MIMO-NOMA HCN with IoT for wireless communication systems. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 17–19 October 2018 ; pp. 856–859.
3. Wei, Z.; Zhu, X.; Sun, S.; Huang, Y.; Dong, L.; Jiang, Y. Full-duplex versus half-duplex amplify-and-forward relaying: Which is more energy efficient in 60-GHz dual-hop indoor wireless systems? *IEEE J. Sel. Areas Commun.* **2015**, *33*, 2936–2947. [CrossRef]
4. Razlighi, M.M.; Zlatanov, N. Buffer-aided relaying for the two-hop full-duplex relay channel with self-interference. *IEEE Trans. Wirel. Commun.* **2017**, *17*, 477–491. [CrossRef]
5. Nguyen, B.C.; Pham, T.Q.; Thang, N.N.; Hoang, T.M.; Tran, P.T. Improving the performance of wireless half-duplex and full-duplex relaying networks with intelligent reflecting surface. *J. Frankl. Inst.* **2023**, *360*, 3095–3118. [CrossRef]
6. Nguyen, T.T.; Hoang, V.T.; Tran, M.H.; Le, T.T.H.; Tran, X.N. Secrecy performance analysis of UAV-based full-duplex two-way relay NOMA system. *Perform. Eval.* **2023**, *161*, 102352. [CrossRef]
7. Nguyen, T. L.; Nguyen, T. L.; Nguyen, V. V., Phu, T. T.; Outage Performance of Full-Duplex Unmanned Aerial Vehicle-aided co-operative Non-orthogonal Multiple Access. *Adv. Electr. Electron. Eng.* **2023**, *21* , 1–8.
8. Ng, D.W.K.; Lo, E.S.; Schober, R. Dynamic resource allocation in MIMO-OFDMA systems with full-duplex and hybrid relaying. *IEEE Trans. Commun.* **2012**, *60*, 1291–1304. [CrossRef]
9. Mohammadi, M.; Shi, X.; Chalise, B.K.; Ding, Z.; Suraweera, H.A.; Zhong, C.; Thompson, J.S. Full-Duplex Non-Orthogonal Multiple Access for Next Generation Wireless Systems. *IEEE Commun. Mag.* **2019**, *57*, 110–116. [CrossRef]
10. Chen, X.; Liu, G.; Ma, Z.; Zhang, X.; Fan, P.; Chen, S.; Yu, F.R. When Full Duplex Wireless Meets Non-Orthogonal Multiple Access: Opportunities and Challenges. *IEEE Wirel. Commun.* **2019**, *26*, 148–155. [CrossRef]
11. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
12. Wang, D.; Bai, B.; Chen, W.; Han, Z. Achieving High Energy Efficiency and Physical-Layer Security in AF Relaying. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 740–752. [CrossRef]
13. Shim, K.; Do, T.N.; Nguyen, T.V.; da Costa, D.B.; An, B. Enhancing PHY-Security of FD-Enabled NOMA Systems Using Jamming and User Selection: Performance Analysis and DNN Evaluation. *IEEE Internet Things J.* **2021**, *8*, 17476–17494. [CrossRef]
14. Lim, J.T.; Kim, T.; Bang, I. Impact of Outdated CSI on the Secure Communication in Untrusted In-Band Full-Duplex Relay Networks. *IEEE Access* **2022**, *10*, 19825–19835. [CrossRef]
15. Hoang, T.M.; Dung, L.T.; Nguyen, B.C.; Tran, X.N.; Kim, T. Secrecy Outage Performance of FD-NOMA Relay System With Multiple Non-Colluding Eavesdroppers. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12985–12997. [CrossRef]
16. Li, X.; Jiang, J.; Wang, H.; Han, C.; Chen, G.; Du, J.; Hu, C.; Mumtaz, S. Physical Layer Security for Wireless-Powered Ambient Backscatter Cooperative Communication Networks. *IEEE Trans. Cogn. Commun. Netw.* **2023**, *9*, 927–939. [CrossRef]
17. Zheng, G.; Krikidis, I.; Li, J.; Petropulu, A.P.; Ottersten, B. Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers. *IEEE Trans. Signal Process.* **2013**, *61*, 4962–4974. [CrossRef]
18. Ding, Q.; Liu, M.; Deng, Y. Secrecy Outage Probability Analysis for Full-Duplex Relaying Networks Based on Relay Selection Schemes. *IEEE Access* **2019**, *7*, 105987–105995. [CrossRef]
19. Nguyen, B.V.; Jung, H.; Kim, K. Physical Layer Security Schemes for Full-Duplex Cooperative Systems: State of the Art and Beyond. *IEEE Commun. Mag.* **2018**, *56*, 131–137. [CrossRef]
20. Lv, L.; Zhou, F.; Chen, J.; Al-Dhahir, N. Secure Cooperative Communications With an Untrusted Relay: A NOMA-Inspired Jamming and Relaying Approach. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3191–3205. [CrossRef]
21. Chen, G.; Gong, Y.; Xiao, P.; Chambers, J.A. Physical Layer Network Security in the Full-Duplex Relay System. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 574–583. [CrossRef]
22. Elsaid, L.; Jiménez-Rodríguez, L.; Tran, N.H.; Shetty, S.; Sastry, S. Secrecy Rates and Optimal Power Allocation for Full-Duplex Decode-and-Forward Relay Wire-Tap Channels. *IEEE Access* **2017**, *5*, 10469–10477. [CrossRef]
23. Moya Osorio, D.P.; Benitez Olivo, E.E.; Alves, H. Secrecy Performance for Multiple Untrusted Relay Networks Using Destination-Based Jamming with Direct Link. In Proceedings of the 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, Italy, 9–12 September 2018 ; pp. 1–5.
24. Saeed, N.; Celik, A.; Al-Naffouri, T.Y.; Alouini, M.S. Localization of energy harvesting empowered underwater optical wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 2652–2663. [CrossRef]
25. Ha, D.H.; Nguyen, T.N.; Tran, M.H.Q.; Li, X.; Tran, P.T.; Voznak, M. Security and Reliability Analysis of a Two-Way Half-Duplex Wireless Relaying Network Using Partial Relay Selection and Hybrid TPSR Energy Harvesting at Relay Nodes. *IEEE Access* **2020**, *8*, 187165–187181. [CrossRef]

26. Tin, P.T.; Dinh, B.H.; Nguyen, T.N.; Ha, D.H.; Trang, T.T. Power Beacon-Assisted Energy Harvesting Wireless Physical Layer Cooperative Relaying Networks: Performance Analysis. *Symmetry* **2020**, *12*, 106. [CrossRef]
27. Nguyen, T.N.; Tran, P.T.; Vozňák, M. Power splitting–based energy-harvesting protocol for wireless-powered communication networks with a bidirectional relay. *Int. J. Commun. Syst.* **2018**, *31*, e3721. [CrossRef]
28. Nguyen, T.N.; Tran, M.; Nguyen, T.L.; Ha, D.H.; Voznak, M. Multisource Power Splitting Energy Harvesting Relaying Network in Half-Duplex System over Block Rayleigh Fading Channel: System Performance Analysis. *Electronics* **2019**, *8*, 67. [CrossRef]
29. Liu, X.; Xu, B.; Wang, X.; Zheng, K.; Chi, K.; Tian, X. Impacts of Sensing Energy and Data Availability on Throughput of Energy Harvesting Cognitive Radio Networks. *IEEE Trans. Veh. Technol.* **2023**, *72*, 747–759. [CrossRef]
30. Hou, L.; Tan, S.; Zhang, Z.; Bergmann, N.W. Thermal energy harvesting WSNs node for temperature monitoring in IIoT. *IEEE Access* **2018**, *6*, 35243–35249. [CrossRef]
31. Tin, P.T.; Nguyen, T.N.; Tran, D.H.; Voznak, M.; Phan, V.D.; Chatzinotas, S. Performance Enhancement for Full-Duplex Relaying with Time-Switching-Based SWIPT in Wireless Sensors Networks. *Sensors* **2021**, *21*, 3847. [CrossRef]
32. Li, X.; Wang, Q.; Liu, M.; Li, J.; Peng, H.; Piran, M.J.; Li, L. Cooperative Wireless-Powered NOMA Relaying for B5G IoT Networks With Hardware Impairments and Channel Estimation Errors. *IEEE Internet Things J.* **2021**, *8*, 5453–5467. [CrossRef]
33. Zhang, R.; Ho, C.K. MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 1989–2001. [CrossRef]
34. Nguyen, H.N.; Dang, H.P.; Le, S.P.; Le, T.D.; Do, D.T.; Voznak, M.; Zdralek, J. Enabling D2D transmission mode with energy harvesting and information transfer in heterogeneous networks. *Adv. Electr. Electron. Eng.* **2018**, *16*, 178–184. [CrossRef]
35. Phan, V.D.; Nguyen, T.L.; Phu, T.T.; Nguyen, V.V. Reliability-Security in Wireless-Powered Cooperative Network with Friendly Jammer. *Adv. Electr. Electron. Eng.* **2023**, *20*, 584–591. [CrossRef]
36. Sun, W.; Song, Q.; Zhao, J.; Guo, L.; Jamalipour, A. Adaptive Resource Allocation in SWIPT-Enabled Cognitive IoT Networks. *IEEE Internet Things J.* **2022**, *9*, 535–545. [CrossRef]
37. Chen, X.; Yuen, C.; Zhang, Z. Wireless energy and information transfer tradeoff for limited-feedback multiantenna systems with energy beamforming. *IEEE Trans. Veh. Technol.* **2013**, *63*, 407–412. [CrossRef]
38. Huynh, T.P.; Son, P.N.; Voznak, M. Exact Throughput Analyses of Energy-Harvesting Cooperation Scheme with Best Relay Selections Under I/Q Imbalance. *Adv. Electr. Electron. Eng.* **2017**, *15*, 585–590. [CrossRef]
39. Nguyen, T.N.; Duy, T.T.; Tran, P.T.; Voznak, M. Performance evaluation of user selection protocols in random networks with energy harvesting and hardware impairments. *Adv. Electr. Electron. Eng.* **2016**, *14*, 372–377. [CrossRef]
40. Pan, G.; Tang, C.; Li, T.; Chen, Y. Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems. *IEEE Trans. Commun.* **2015**, *63*, 3423–3433. [CrossRef]
41. Feng, R.; Li, Q.; Zhang, Q.; Qin, J. Robust secure transmission in MISO simultaneous wireless information and power transfer system. *IEEE Trans. Veh. Technol.* **2014**, *64*, 400–405. [CrossRef]
42. Wu, W.; Wang, B. Efficient transmission solutions for MIMO wiretap channels with SWIPT. *IEEE Commun. Lett.* **2015**, *19*, 1548–1551. [CrossRef]
43. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
44. El Hammouti, H.; Ghogho, M.; Zaidi, S.A.R. A machine learning approach to predicting coverage in random wireless networks. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018 ; pp. 1–6.
45. Bao, T.; Zhu, J.; Yang, H.C.; Hasna, M.O. Secrecy outage performance of ground-to-air communications with multiple aerial eavesdroppers and its deep learning evaluation. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1351–1355. [CrossRef]
46. Zheng, K.; Jia, X.; Chi, K.; Liu, X. DDPG-Based Joint Time and Energy Management in Ambient Backscatter-Assisted Hybrid Underlay CRNs. *IEEE Trans. Commun.* **2023**, *71*, 441–456. [CrossRef]
47. Saman, A.; Nathan, R.; Yindi, J.; Malin, P. Source-Based Jamming for Physical-Layer Security on Untrusted Full-Duplex Relay. *IEEE Commun. Lett.* **2019**, *23*, 842–846.
48. Pandey, A.; Yadav, S. Physical layer security in cooperative amplify-and-forward relay networks over mixed Nakagami-m and double Nakagami-m fading channels: performance evaluation and optimisation. *IET Commun.* **2020**, *14*, 95–104. [CrossRef]
49. Nguyen, T.N.; Tran, D.H.; Van Chien, T.; Phan, V.D.; Voznak, M.; Tin, P.T.; Chatzinotas, S.; Ng, D.W.K.; Poor, H.V. Security–reliability tradeoff analysis for SWIPT-and AF-based IoT networks with friendly jammers. *IEEE Internet Things J.* **2022**, *9*, 21662–21675. [CrossRef]
50. Nguyen, T.N.; Duy, T.T.; Tran, P.T.; Voznak, M.; Li, X.; Poor, H.V. Partial and full relay selection algorithms for AF multi-relay full-duplex networks with self-energy recycling in non-identically distributed fading channels. *IEEE Trans. Veh. Technol.* **2022**, *71*, 6173–6188. [CrossRef]
51. Lee, D. Secrecy Analysis of Relay-User Selection in AS-AF Systems Over Nakagami Fading Channels. *IEEE Trans. Veh. Technol.* **2021**, *70*, 2378–2388. [CrossRef]
52. Liu, H.; Kim, K.J.; Kwak, K.S.; Poor, H.V. Power splitting-based SWIPT with decode-and-forward full-duplex relaying. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 7561–7577. [CrossRef]
53. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*; Academic Press: Cambridge, MA, USA, 2014.

54. Wei, L.; Wang, K.; Pan, C.; Elkashlan, M. Secrecy Performance Analysis of RIS-Aided Communication System With Randomly Flying Eavesdroppers. *IEEE Wirel. Commun. Lett.* **2022**, *11*, 2240–2244. [CrossRef]
55. Li, X.; Zhao, M.; Liu, Y.; Li, L.; Ding, Z.; Nallanathan, A. Secrecy Analysis of Ambient Backscatter NOMA Systems Under I/Q Imbalance. *IEEE Trans. Veh. Technol.* **2020**, *69*, 12286–12290. [CrossRef]
56. Nguyen, T.N.; Chien, T.V.; Tran, D.H.; Phan, V.D.; Voznak, M.; Chatzinotas, S.; Ding, Z.; Poor, H.V. Security-Reliability Trade-Offs for Satellite-Terrestrial Relay Networks with a Friendly Jammer and Imperfect CSI. *IEEE Trans. Aerosp. Electron. Syst.* **2023**, 1–16. [CrossRef]
57. Vu, T.H.; Nguyen, T.V.; Kim, S. Cooperative NOMA-Enabled SWIPT IoT Networks With Imperfect SIC: Performance Analysis and Deep Learning Evaluation. *IEEE Internet Things J.* **2022**, *9*, 2253–2266. [CrossRef]
58. Clevert, D.A.; Unterthiner, T.; Hochreiter, S. Fast and Accurate Deep Network Learning by Exponential Linear Units (ELUs). *arXiv* **2016**, arXiv:1511.07289.
59. Kingma, D.P.; Ba, J. Adam: A method for stochastic optimization. *arXiv* **2014**, arXiv:1412.6980.
60. Van Chien, T.; Tu, L.T.; Chatzinotas, S.; Ottersten, B. Coverage Probability and Ergodic Capacity of Intelligent Reflecting Surface-Enhanced Communication Systems. *IEEE Commun. Lett.* **2021**, *25*, 69–73. [CrossRef]
61. Hoang, T.M.; Huyen, L.T.T.; Tran, X.N.; Hiep, P.T. Outage Probability of Aerial Base Station NOMA MIMO Wireless Communication With RF Energy Harvesting. *IEEE Internet Things J.* **2022**, *9*, 22874–22886. [CrossRef]