electronics

MDPI

Article

Physical Layer Secrecy by Power Splitting and Jamming in Cooperative Multiple Relay Based on Energy Harvesting in Full-Duplex Network

Nabila Sehito [1], Shouyi Yang [1,*], Esraa Mousa Ali [2], Muhammad Abbas Khan [3], Raja Sohail Ahmed Larik [4], Inam Bari [5], Mian Muhammad Kamal [1], Salahuddin Khan [6], Mohammad Alibakhshikenari [7,*] and Ernesto Limiti [8]

1 School of Information Engineering, Zhengzhou University, 100, Science Avenue, Zhengzhou 450001, China; nabila.fiza@gmail.com (N.S.); mmkamal@gs.zzu.edu.cn (M.M.K.)
2 Faculty of Aviation Sciences, Amman Arab University, Amman 11953, Jordan; esraa_ali@aau.edu.jo
3 Electrical Engineering Department, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta 87300, Pakistan; Muhammad.Abbas@buitms.edu.pk
4 School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China; dr.rajalarik@njust.edu.cn
5 Department of System Engineering, Military Technological College, Muscat 111, Oman; inam.bari@mtc.edu.om
6 Department of Electrical Engineering, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia; khanheu@gmail.com
7 Department of Signal Theory and Communications, Universidad Carlos III de Madrid, Leganés, 28911 Madrid, Spain
8 Electronic Engineering Department, University of Rome "Tor Vergata", Via del Politecnico 1, 00133 Rome, Italy; limiti@ing.uniroma2.it
* Correspondence: iesyyang@zzu.edu.cn (S.Y.); mohammad.alibakhshikenari@uc3m.es (M.A.)

Citation: Sehito, N.; Yang, S.; Ali, E.M.; Khan, M.A.; Larik, R.S.A.; Bari, I.; Kamal, M.M.; Khan, S.; Alibakhshikenari, M.; Limiti, E. Physical Layer Secrecy by Power Splitting and Jamming in Cooperative Multiple Relay Based on Energy Harvesting in Full-Duplex Network. *Electronics* **2022**, *11*, 40. https://doi.org/10.3390/electronics11010040

Academic Editor: Imran Shafique Ansari

Received: 23 November 2021
Accepted: 18 December 2021
Published: 23 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: In this article, we investigated the secrecy performance of a three-hop relay network system with Power Splitting (PS) and Energy Harvesting (EH). In the presence of one eavesdropper, a signal is transferred from source to destination with the help of a relay. The source signal transmits in full-duplex (FD) mood, jamming the relay transfer signals to the destination. The relay and source employ Time Switching (TS) and Energy Harvesting (EH) techniques to obtain the power from the power beacon. In this study, we compared the Secrecy Rate of two Cooperative Schemes, Amplify and Forward (AF) and Decode and Forward (DF), for both designed systems with the established EH and PS system. The Secrecy Rate was improved by 50.5% in the AF scheme and by 44.2% in the DF scheme between the relay and eavesdropper at 40 m apart for the proposed system in EH and PS. This simulation was performed using the Monto Carlo method in MATLAB.

Keywords: energy harvesting (EH); power splitting; cooperative communication; amplify-and-forward (AF); decode-and-forward (DF); full-duplex relay

1. Introduction

Due to the broadcast nature of wireless communication, information transmission is not secure. By utilizing the physical properties of the wireless communication, physical layer security (PLS) aids in ensuring secure communication [1]. There are several relaying schemes that can be employed to improve PLS, but two of the most popular are Cooperative Schemes DF and AF in wireless communication techniques [2,3]. The nodes in communication networks are powered by putting separate batteries inside them; however, in some circumstances, replacing or recharging those batteries is not recommended [4]. The Energy-Harvesting (EH) approach [5–7] can be used to solve this problem. It also contributes to the improved reliability and low-maintenance monitoring of the system. Additionally, as the number of communication devices grows, it is necessary to shift toward more energy-efficient systems.

In [8], a scheme was presented to check the secrecy level in a cooperative compressed sensing amplify and forward (CCS-AF) wireless network in the presence of eavesdroppers and receive radio frequency signals consisting of Power Splitting Relaying (PSR). Similarly, in [9], the physical layer secrecy efficiency of Radio Frequency Energy Harvesting (RF-EH) in the Rayleigh fading environment was investigated. While the preceding work focuses on two-hop relaying systems, it is worth looking at secure communication in multi-hop relaying systems with more than two hops.

In this work, the authors investigate a three-hop relaying system with a single relay active at each individual hop, where one source–destination pair tries to communicate securely in the presence of one eavesdropper. Each relay node operates using cooperative communication between AF and DF, and each node has a single antenna. Due to propagation loss, each relay and the destination only hear their previous nearby nodes in the standard multi-hop relaying paradigm in [10,11]. This was further analyzed by various authors in a two-way relay network to improve the Secrecy Rate versus eavesdropping attack [12–15].

Ref [12] investigated the secrecy performance of a proposed Single-Hop Relay system and found an improvement in the performance of EH of 8.89% for the AF relay and of 9.83% for the DF Relay between the eavesdropper and the relay. Ref [13] investigated the secrecy performance of a Single-Hop Relay Network, and observed a performance improvement of 30.47% for the DF Cooperative Scheme and of 23.63% for the AF Cooperative Scheme between the eavesdropper and the relay. Ref [14] investigated the secrecy performance of a Single-Hop Relay Network, and the results were an 11.9% improvement for the AF Single-Hop Relay Network and of 42.86% for the DF Single-Hop Relay Network. Ref [15] investigated the secrecy performance of a Wireless Relay Network and found 40% performance improvement for DF in the Half-Duplex Relay (HDR) Network and 41% for the AF Half-Duplex Relay (HDR) Network. However, in our study, the results included an improvement in the secrecy performance of the three-hop wireless relay system, with EH and PS being improved by 50.5% for the AF Cooperative Scheme and by 44.2% for DF between the eavesdropper and R_1 and R_2 in full duplex mood.

The authors conducted a review of various studies focused on the secrecy of wireless communication transmission to eavesdroppers in the relaying node, where the cooperative communication schemes used in the DF and AF relaying protocols were analyzed and equated with different systems. The proposed cooperative jamming in [16] was based on an analysis of the Secrecy Rate, where a number of relays were authorized to communicate with each other and prevent the eavesdropper from attacking. The cooperation of multi-users was employed to examine the physical layer security by using the proposed noise-forwarding scheme. In [17], a full-duplex relay network was presented to improve the physical layer security in the multi-hop relaying system, and a geometric programming (GP) method was applied to solve the transmitted power allocation problem. In summary, the contributions of the paper are as follows.

- This paper presents an investigation of a three-hop relaying system with a single relay active at each individual hop, where one source–destination pair tries to communicate securely in the presence of one eavesdropper.
- Each relay node operates in the AF and DF modes, and each node has a single antenna. Due to propagation loss, each relay and the destination only hear their previous nearby nodes in the standard multi-hop relaying paradigm.
- The Secrecy Rates of two Cooperative Schemes, Amplify and Forward (AF) and Decode and Forward (DF), for both proposed systems are compared with those of the conventional Energy-Harvesting System, including an examination of the performance of the Outage Probability for proposed EH system.
- In calculation, we extract accurate Secrecy Outage Probability (SOP) in a one-integral format and the closed-format asymptotic SOP for higher average Signal Noise Ratio (SNR).

1.1. Paper Organization

This article is organized into various sections; all the sections are divided into different portions and each section contains subsections. Table 1 summarizes paper flow.

Table 1. The following table shows the paper's contents.

Section 1	**Section 2**
Section 1. Introduction Section 1.1. Organization of Paper	Section 2. System Model Section 2.1. Power Splitting and Energy Harvesting Technique Section 2.2. Full Duplex Decoding and Forward (DF) Relay Scheme
Section 3	**Section 4**
Section 3. Achievable Secrecy Rate Section 3.1. DF Relaying Scheme Section 3.2. AF Relaying Scheme	Section 4. Analysis of Outage Probability
Section 5	**Section 6**
Section 5. Numerical Evaluation and Results	Section 6. Conclusions

2. System Model

Figure 1 shows the three-hop relay network with a single eavesdropper (E) utilizing EH. It consists of a source S, Relay R_1, R_2, Distention node D and an eavesdropper E. This three hop relay network is powered up by a power beacon (B). Let $H \times SR_1$, $H \times R_1E$, $H \times R_2E$, $H \times R_2D$, $H \times BR_1$, and $H \times BR_2$ represent the Complex Channel acquired from the network shown in Figure 1. The noise in the network shown in Figure 1 is supposed to be complex additive white Gaussian noise (AWGN) with a mean of zero, the variance σ^2 and no Self-Interference Signal (SIC). Further, the relay exhibits Full Duplex (FD) mood in the designed model. Each relay performs in the AF and DF modes to amplify and decode the signal from the previous node and forward the re-encoded signal to the next node.

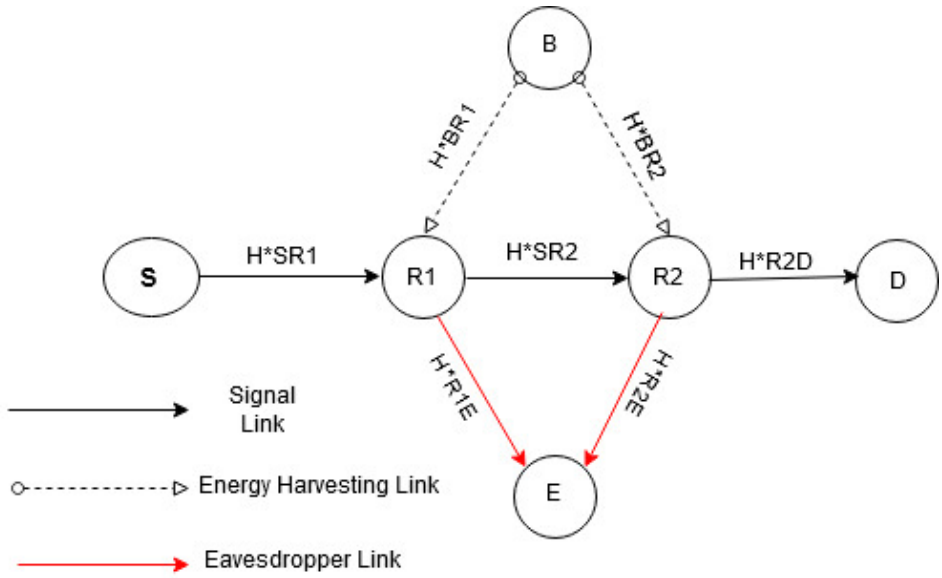

Figure 1. System model of the secrecy relay network.

2.1. Power Splitting and Energy Harvesting Technique

In the present-design system, S, R_1 and R_2 harvest energy from the power beacon and send it to D, where it is used for signal transmission. Figure 2 illustrates Power Switching and Energy Harvesting Schemes; whereas T is the time duration divided into

two parts. The transmitted signal splits into two parts during the first slot and depends on the power splitting ratio of the power. The first phase is transferred by the source for Energy-Harvesting purposes and the second phase is applied to transfer signal to the source. The second time slot is used for transmitting the signal to destination *D*.

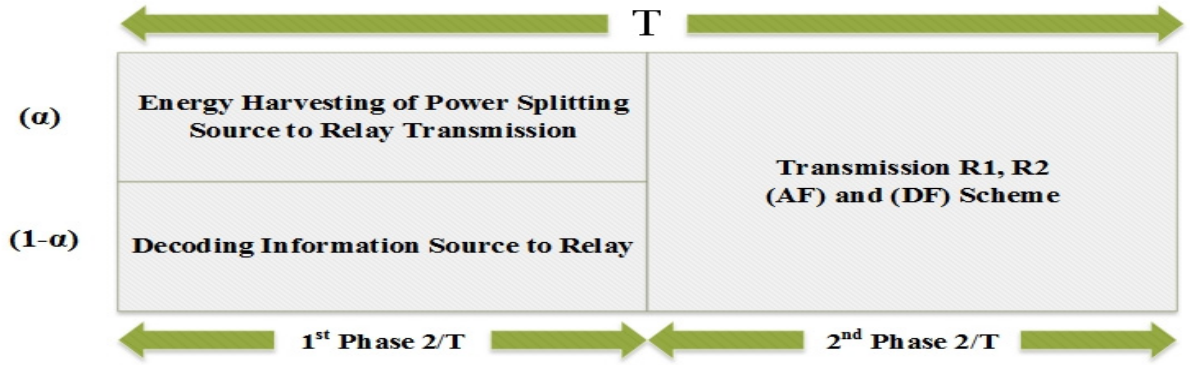

Figure 2. Power-splitting-, Energy-Harvesting- and time-switching-based relaying protocol.

In this equation, the energy harvested from R_1 and R_2 is expressed as.

$$E_{R_1} = \eta\alpha\rho P_B \left| h \times \frac{BR_1|^2\, T}{2} \right. \tag{1}$$

$$E_{R2} = \eta\alpha\rho P_B \left| h \times \frac{BR_2|^2\, T}{2} \right. \tag{2}$$

where α represents the signal portion for EH. Thus, the power transferred by R_1 and R_2 is represented by:

$$P_{R1} = \frac{\eta\ \alpha\rho\ P_B |h \times BR_2|^2}{(1-\alpha)} \tag{3}$$

$$P_{R2} = \frac{\eta\ \alpha\rho\ P_B |h \times BR_2\ |^2}{(1-\alpha)} \tag{4}$$

whereas the efficiency of the coefficient of this process in terms of energy transference is represented by $0 < \eta < 1$, and the power sent through beacon node is represented by P_B and $0 < \alpha < 1$. T represents the time taken to transmit the specific block S to D. The source S, and R_1 and R_2, harvest energy for a B time duration of $\alpha\ T$. The power transmitted via S, R_1 and R_2 in this proposed system is embodied by [11].

2.2. Full Duplex Decode and Forward (DF) Relay Scheme

This section involves work performed in a pair of steps. The Full-Duplex Relay transmits the jamming signal when it receives the required signal from the preceding node. The first occurrence of this is illustrated in Figure 3. We assumed that the FDR Self-Interference Signal (SIC) is canceled completely in the first time slot. In the next time slot, at the $2n$th time slot, S sends a jamming signal $x(n)$ to R_1, R_2 sends the previous $x(n-1)$ to the D $2n$th time slot, and E obtains the jamming signal through the R_1 and R_2 data signals. As such, the received signals derived at R_1, E and D are expressed as:

$$y_{R_1}(2n) = \sqrt{\rho P_s} h^*_{SR_1} x(n) + n_{R_1}(2n) \tag{5}$$

$$y_E(2n) = \sqrt{\rho P_{R_2}} h^*_{R_2E} x(n) + \sqrt{\rho P_{R_1J}} h^*_{R_1E} q(2n) + n_E(2n) \tag{6}$$

$$y_D(2n) = \sqrt{\rho P_{R_2}} h^*_{R_2D} x(n-1) + n_D(2n) \tag{7}$$

where $x(n)$ represents the carried data symbol with the Unit Power, denoted as P_s and P_{R_2} which are the transmitting powers of source S and relay R_2 ; $q(2n)$ is the unit power of the jamming signal, and P_{R_1J} is the relay R_1 of the jamming signal. In addition, $n_{R_1}(2n)$, $n_D(2n)$ and $n_E(2n)$, corresponding to R_1, D, and E, respectively, represent the additive white Gaussian noise (AWGN). ρ is the ratio of the Energy Harvesting power splitting technique.

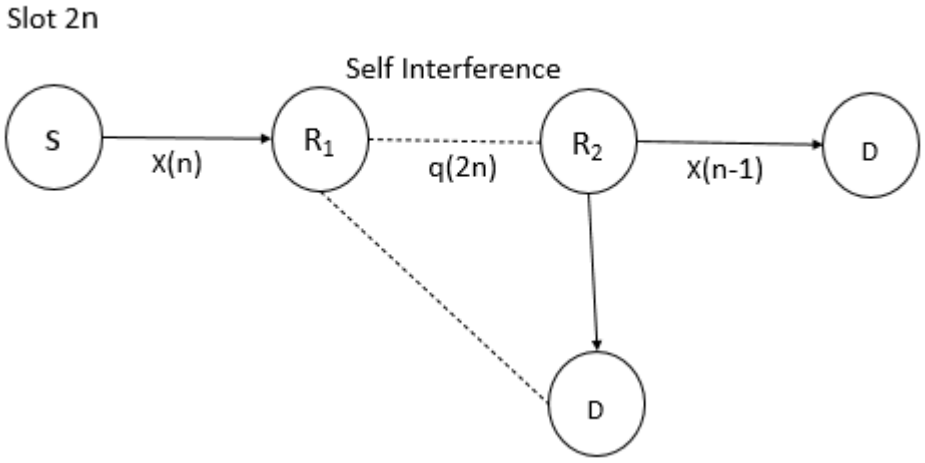

Figure 3. Transmission of signals in 2nth time slot.

In the second phase, according to Figure 3, the $x(n)$ signal from the source is sent and received by the destination. The secrecy is calculated according to the graph. We suspect that in the next time slot, R_1 effectively decodes the signal $x(n)$ and transmits re-encoded signals. The $(2n + 1)$th receiving the signal at R_2 and E in the time slot is obtained as follows:

$$y_{R_2}(2n+1) = \sqrt{(1-\rho)P_{R_1}}h^*_{R_1R_{2J}}x(n) + n_{R_2}(2n+1) \tag{8}$$

$$y_E(2n+1) = \sqrt{(1-\rho)P_{R_1}}h^*_{R_1E}x(n) + \sqrt{(1-\rho)P_{R_2J}}h^*_{R_2E}qx(2n+1) + n_E(2n+1) \tag{9}$$

where P_{R_2J} signifies the jamming signal power of R_2 and P_{R_1} is the transmitted power of R_1. Here, eavesdropper E performs maximum ratio combining (MRC) to decode $x(n)$, with $y_E(2n+1)$ and $y_E(2n+2)$. This is shown in Figures 4 and 5.

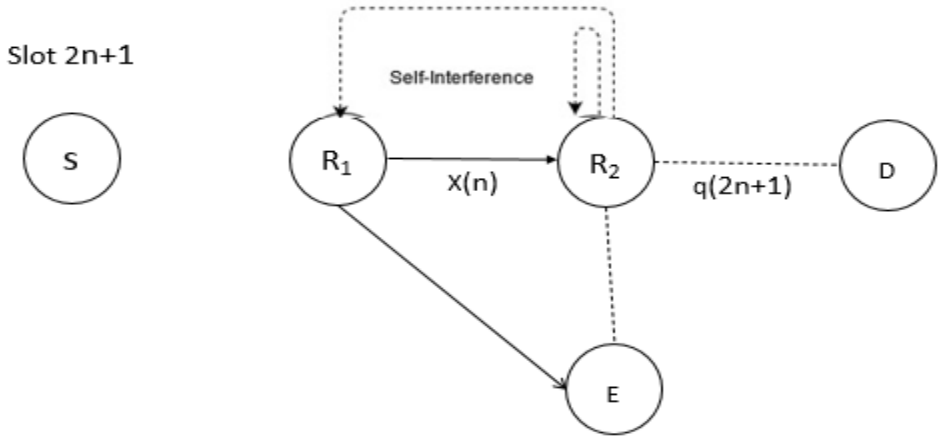

Figure 4. Transmission of signals in the 2$(n + 1)$th time slot.

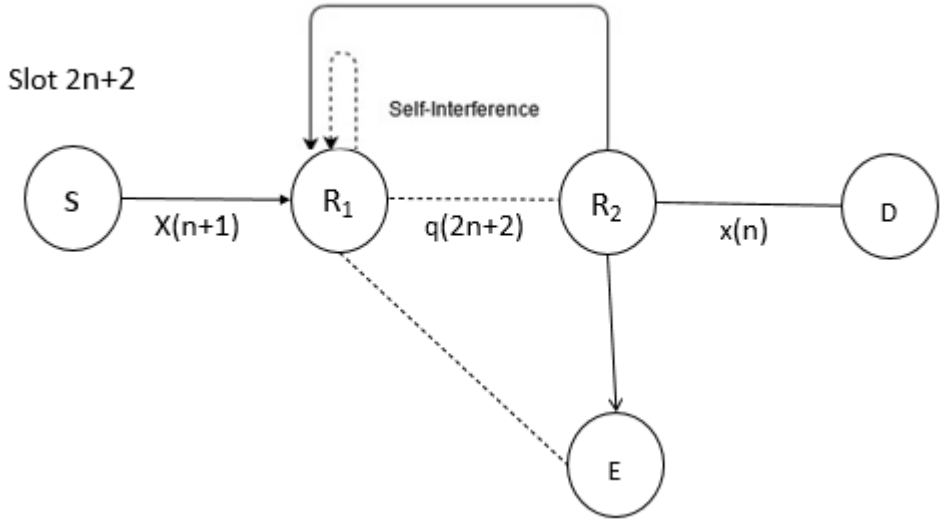

Figure 5. Signal transmission in the 2(n+2)th time slot.

2.3. Amplify and Forward (AF) Relaying Scheme

This involves two phases: the first phase is the same as the DF scheme as demonstrated in Figure 3; in the 2nth time slot, the R_1, R_2, and E signals are received, and the relevant equations are represented by (5)–(7). In the next time slot, the relay sends the amplified signals to the destination using the Amplify and Forward Scheme and by jamming the signal source to the eavesdropper. Therefore, in the (2n + 1)th time slot, the signal received R_2 and E as follows:

$$y_{R_2}(2n+1) = G\sqrt{(1-\rho)P_{R_1}}h^*_{R_1R_2}x(n) + n_{R_2}(2n+1) \tag{10}$$

$$\begin{aligned} y_E(2n+1) = \quad & G\sqrt{(1-\rho)P_{R_1}}h^*_{R_1E}x(n) + \sqrt{(1-\rho)P_{R_2J}}h^*_{R_2E}q(2n+1) \\ & + n_E(2n+1) \end{aligned} \tag{11}$$

whereas the scaling factor [11] is assessed by $G = \frac{1}{\sqrt{P_{R_1}|h_{SR_1}|^2 + N_o}}$ and the noise variance is indicated by the N_o.

3. Achievable Secrecy Rate

3.1. DF Scheme

In (5)–(9), the Secrecy Rate values at D and E are given [11]:

$$R_d = \frac{1}{2}log_2\left(1 + \rho P_{R_2}\alpha_{R_2D}\right) \tag{12}$$

$$R_e = \frac{1}{2}log_2\left(1 + \frac{(1-\rho)P_{R_1}\alpha_{R_1E}}{1 + P_{R_2J}\alpha_{R_2E}} + \frac{(1-\rho)P_{R_2}\alpha_{R_2E}}{1 + P_{R_1J}\alpha_{R_1E}}\right) \tag{13}$$

where, $\alpha_{R_2D} = \frac{|hR_2D|^2}{\sigma^2}$,$\alpha_{R_1E} = \frac{|hR_1E|^2}{\sigma^2}$ and $\alpha_{R_2E} = \frac{|hR_2E|^2}{\sigma^2}$.

It is possible to use secrecy rate obtained in Equations (12) and (13) and the achievable Secrecy Rate can be represented as Rs = max $\{R_d - R_e, 0\}$:

$$R_d - R_e = \frac{1}{2}log_2\left[\frac{1 + \rho P_{R_2}\alpha_{R_2D}}{1 + \frac{(1-\rho)P_{R_1}\alpha_{R_1E}}{1+P_{R_2J}\alpha_{R_2E}} + \frac{(1-\rho)P_{R_2}\alpha_{R_2E}}{1+P_{R_1J}\alpha_{R_1E}}}\right] \tag{14}$$

3.2. AF Scheme

In (10) and (11), the Secrecy Rate values at D and E are given [11]:

$$R_d = \frac{1}{2} log_2\left(1 + G^2 \rho P_{R_2} \alpha_{R_2 D}\right) \tag{15}$$

$$R_e = \frac{1}{2} log_2(1 + \frac{(1-\rho) P_{R_1} \alpha_{R_1 E}}{1 + P_{R_2 J} \alpha_{R_2 E}} + \frac{G^2 (1-\rho) P_{R_2} \alpha_{R_2 E}}{1 + P_{R_1 J} \alpha_{R_1 E}} \tag{16}$$

The secrecy rate is obtained in Equations (15) and (16) as $Rs = \max\{R_d - R_e, 0\}$, whereas

$$R_d - R_e = \frac{1}{2} log_2 \left[\frac{1 + G^2 \rho P_{R_2} \alpha_{R_2 D}}{1 + \frac{(1-\rho) P_{R_1} \alpha_{R_1 E}}{1 + P_{R_2 J} \alpha_{R_2 E}} + \frac{G^2 (1-\rho) P_{R_2} \alpha_{R_2 E}}{1 + P_{R_1 J} \alpha_{R_1 E}}} \right] \tag{17}$$

4. Analysis of Outage Probability

Here, the analytical expressions of the OP for the Energy-Harvesting system performance in the AF and DF Schemes are derived. In addition, the exact accurate Secrecy Outage Probability (SOP) is expressed in a one-integral format and the closed-format asymptotic (CFA) is used for higher averaged SNRs. Throughout the work, the secrecy event usually happens when the achievable secrecy capacity of Rs is below the secrecy capacity of the target Rt, as follows:

$$P\text{out}\,(Rt) = Pr\,[Rs < Rt] \tag{18}$$

where $Rt = 2^{2Rt-1}$ and Rt denote the data rate of the target, and the probability of event A is Pr (A).

4.1. Decode and Forward Scheme

The DF Relaying Scheme's Outage Probability (OP) can be calculated as:

$$P_{out}^{DF}(R_t) = (\max\{R_s, \max\min\{R_d R_e\} < R_t\}) \tag{19}$$

The complete proof of Equation (19) given in Appendix A.

Theorem 1. *A methodological formulation can be given for the DF relaying scheme (OP).*

$$P_{out}^{DF}(R_t) = \Omega \sum_{m=1}^{M} \ominus_m \prod_{k=1}^{K} \left[1 - \lambda_{R_{ek}} \int_{\mu}^{\infty} e^{-y\lambda R_{ek} - \frac{R_t \lambda_{R_k} d_m}{\beta_y}} d_y \right] \tag{20}$$

where $A_{DF_{Scheme}} = \int_{\mu}^{\infty} e^{-y\lambda R_{ek} - \frac{R_t \lambda_{R_k} d_m}{\beta_y}} d_y$.

To the best of the authors' knowledge, the integral $A_{DF_{Scheme}}$ in Equation (20) cannot be condensed. The below lemma based on the Maclaurin series allows the generation of a tractable format from the result shown in Theorem 1.

Lemma 1. *For* $\theta, \xi > 0$, *integral* $\mathrm{A} \triangleq \int_{\mu}^{\infty} \mathrm{e}^{-\theta \mathrm{x} - \frac{\xi}{\mathrm{x}}} \mathrm{dx}$ *could be presented as*

$$\begin{aligned} A \approx \tfrac{e^{-\mu\theta}}{\theta} - \quad & \xi\, \Gamma(0, \mu\theta) \\ & + \sum_{u=2}^{\infty} \tfrac{(-1)^u\, \xi^u}{u!} \\ & \times \left[e^{-\mu\theta} \sum_{v=1}^{u-1} \tfrac{(v-1)!(-\theta)^{u-v-1}}{(u-1)!\mu^v} - \tfrac{(-\theta)^{u-1}}{(u-1)!} E_i(-\mu\theta) \right] \end{aligned} \tag{21}$$

where $\Gamma(\,,\,)$ *is the Gamma function of upper incomplete,*$E_i(\,)$ *is an exponential type of integral function.*

Proof. Using the Maclaurin series of the term $e^{-\frac{\xi}{x}=\sum_{u=1}^{\infty}\frac{(-1)^u\,\xi^u}{u!x^u}}$ and after some algebraic analysis, the solution can be obtained using Formula (21).

Applying Lemma 1, an approximate closed-form expression for the DF Scheme, using the DF relaying operation, can be obtained as:

$$\begin{aligned} P_{out,approx}^{DF} = \quad & \Omega \sum_{m=1}^{M} \ominus_m \prod_{k=1}^{K} \Bigg[1 \\ & -\theta_1 \Bigg[\frac{e^{-\mu\theta}}{\theta} - \xi\, \Gamma(0, \mu\theta) \\ & + \sum_{u=2}^{\infty} \frac{(-1)^u\, \xi^u}{u!} \Bigg[e^{-\mu\theta} \sum_{v=1}^{u-1} \frac{(v-1)!(-\theta)^{u-v-1}}{(u-1)!\mu^v} \\ & - \frac{(-\theta)^{u-1}}{(u-1)!} E_i(-\mu\theta) \Bigg] \Bigg] \Bigg] \end{aligned} \tag{22}$$

where $\theta_1 = \lambda R_{ek}$ and $\xi_1 = \frac{\gamma_{th}\lambda_{R_k} d_m}{\beta}$. □

4.2. AF Strategy for Relaying

From Equations (10)–(20), assuming AF relaying, the AF Scheme's OP can be provided by

$$P_{out}^{AF}(R_t) = (\max\{R_s, \max\{R_d R_e\} < R_t\}) \tag{23}$$

The complete proof of Equation (23) given in Appendix B.

Theorem 2. *A methodological formulation for AF Scheme OP utilizing AF relays may be derived as:*

$$P_{out}^{AF}(R_t) = \Omega \sum_{m=1}^{M} \ominus_m \prod_{k=1}^{K} \left[1 - \lambda_{R_{ek}} \times \int_{\mu}^{\infty} e^{-y\lambda R_{ek} - \frac{\alpha R_t y + (R_t)\lambda_{R_k} d_m}{(\alpha y - R_t)\beta y}} d_y \right] \tag{24}$$

where $\Psi_{AF_{Scheme}} = \int_{\mu}^{\infty} e^{-y\lambda R_{ek} - \frac{\alpha R_t y + (R_t)\lambda_{R_k} d_m}{(\alpha y - R_t)\beta y}} d_y$.

It should be noted that the integral of $\Psi_{AF_{Scheme}}$ in Equation (24) does not have an expression in a closed-form. Here, for two real non-negative numbers, it is possible to obtain $b\frac{ab}{a+b+1} \approx \frac{ab}{a+b}$ when a and b are large enough. The end of the SNR R_e^{AF} in (16) can therefore be computed by:

$$R_e^{AF} \approx \frac{R_1 E R_2 E}{R_1 E + R_2 E} = \max_{1 \le k \le K} \frac{R_1 E R_2 E}{R_1 E + R_2 E} \tag{25}$$

Plugging (25) into (23) and then performing the steps set out in Appendix B, the integration of the $\Psi_{AF_{Scheme}}$ in (24) can be computed by.

$$\Psi_{AF_{Scheme}} \approx \int_{\mu}^{\infty} e^{-y\lambda R_{ek} - \frac{\alpha R_t \lambda_{R_k} d_m}{(\alpha y - R_t)\beta y}} dy \tag{26}$$

5. Numerical Evaluation and Results

This section describes the investigated secrecy performance of the designed system utilizing (EH) for both the DF and AF full-duplex Cooperative Schemes, as illustrated in Figure 6. The source (S), the relays (R_1 and R_2) and the destination (D) are considered in a line [2]. Here, d_{SR1}, d_{R1R2}, d_{R2D}, d_{R1E} and d_{R2E} represent the distance between the Source and Relay1, Relay1 and Relay2, Relay2 and the Destination, Relay1 and the Eavesdropper,

and Relay2 and the Eavesdropper, respectively. Moreover, the distance between jamming relay R_1 and Eavesdropper E is calculated as:

$$d_{R_{1_E}} = \sqrt{d_{R_{1E}}^2 + d_{R_{2E}}^2} \tag{27}$$

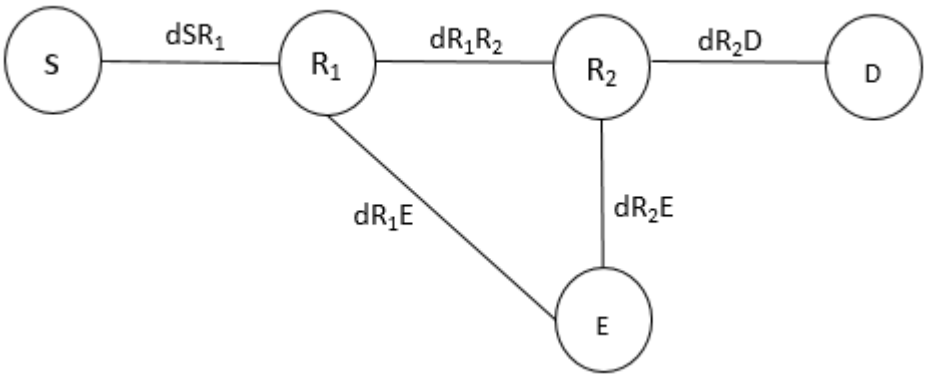

Figure 6. Illustration of PS EH Simulation.

Sight (LOS) channel model uses "$d - c/2ej\theta$" and is followed by channels between any two nodes, whereas d is the space between nodes and θ, which is uniformly distributed in a random phase in the [0, 2π] range, and the path loss exponent c = 3.50. The assumption is that P_B = 30 dBm and the noise power or variance (N_o) = −40 dBm, d_BR1 = d_BR2 = 7 m, $\alpha = 0.99$ η = 0.9 and $\rho = 0.5$.

In Figures 7 and 8, a graph is plotted for the Secrecy Rate and the distance between Relay2 (R_2) and the Destination (D), with the AF and DF strategies, when d_{R1R2} = 10 m, d_{R2E} = 15 m. The graph shows the decreasing Secrecy Rate with the increasing of the distance between Relay2 and the Destination (D), but at the same time, due to power splitting receiver in the Energy Harvesting (EH) system, the Secrecy Rate in the DF Scheme becomes 7, and becomes 7.5 in the AF Scheme, which is considered good. In addition, from Figures 7 and 8, it can be seen that AF Scheme gives a better Secrecy Rate than the DF Scheme.

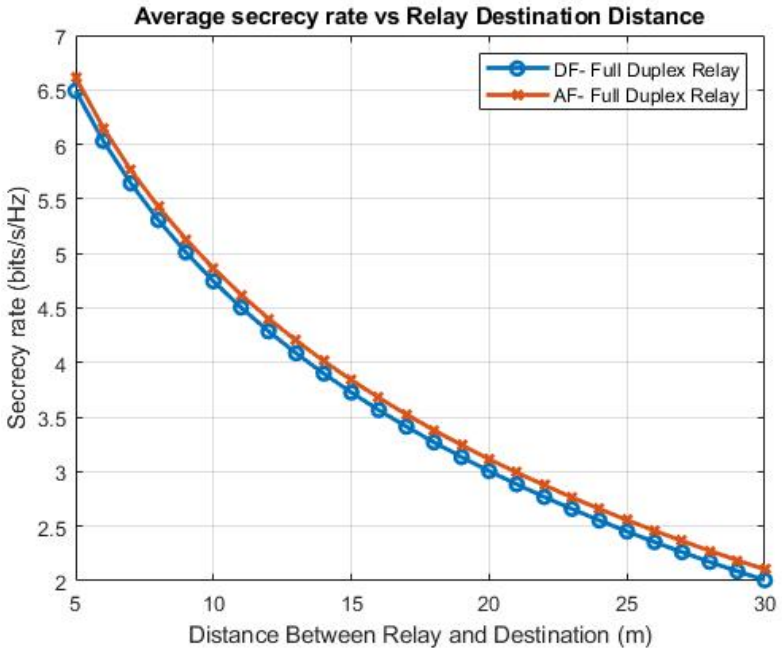

Figure 7. Secrecy Rate vs. d_{R2D} for the EH System.

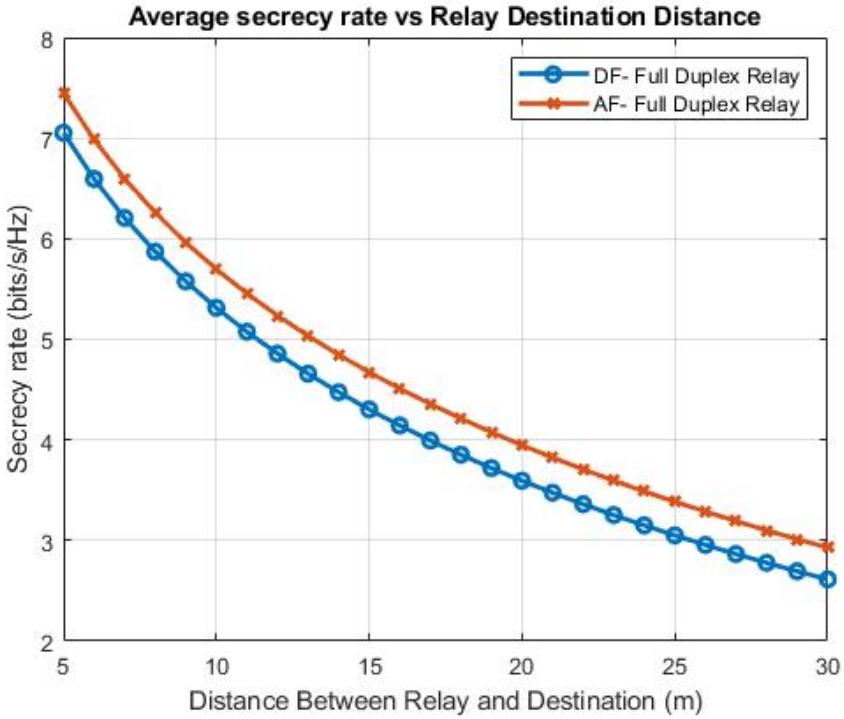

Figure 8. Secrecy Rate vs. d_{R2D} for the proposed EH PS System.

In Figures 9 and 10, graphs are plotted for the Secrecy Rate and the distance between Relay2 (R_2) and the Eavesdropper (E) with the AF and DF Strategies, when d_{R1R2} = 10 m and d_{R2D} = 15 m. The graph shows that the Secrecy Rate increases with the increasing of the distance between (R_2) and (E) in the Energy-Harvesting System. The highest value of the Secrecy Rate in the Energy Harvesting (EH) System with AF Scheme is 4.23, and with the DF Scheme, this value is 3.95. In the proposed Energy Harvesting Power Splitting System, the Secrecy Rate is better in both the schemes because of the Power Splitting Receiver, and the values of Secrecy rate become 5.08 with the AF Scheme and 4.42 with the DF Scheme. Therefore, to increase the Secrecy Rate, it is important to use a share of the useful power to relay the jamming signals when applying both the AF and DF Strategies.

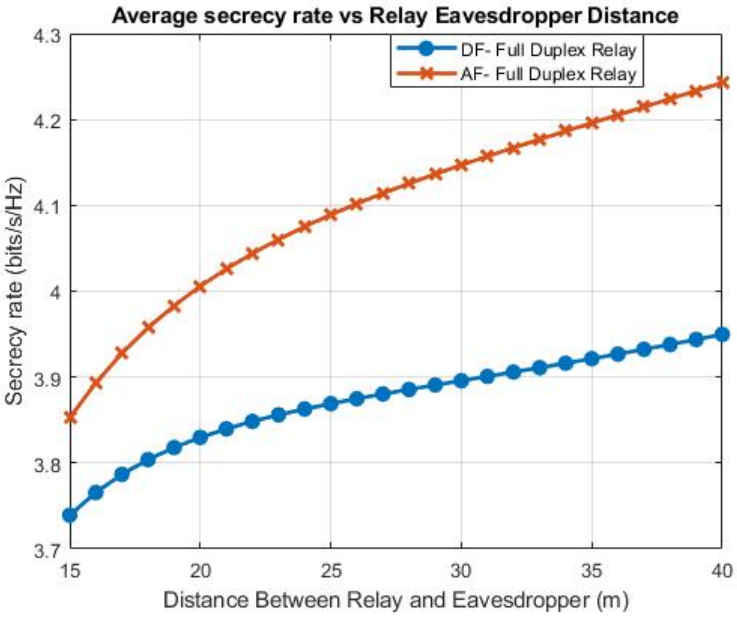

Figure 9. Secrecy Rate vs. d_{R2E} for the EH System.

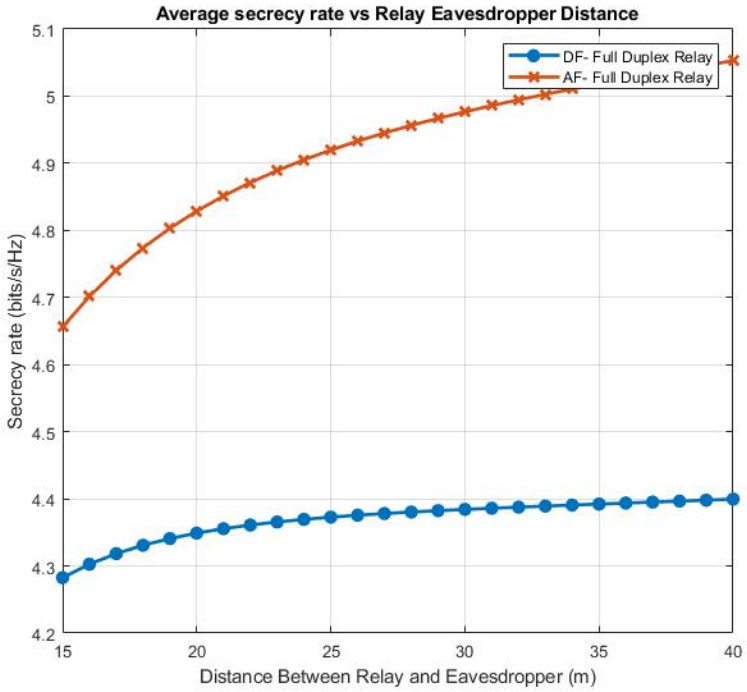

Figure 10. Secrecy Rate vs. d_{R2E} for the EH PS System.

In Figures 11 and 12, graphs are plotted for the Secrecy Rate and the path loss exponent factor with both AF and DF Strategies, when d_{R1R2} = 10 m, d_{R2D} = 15 m and d_{R2E} = 15 m. Path loss plays a vital role in the calculation of the Secrecy Rate. The graph shows that as the path loss exponent is increased from 2 to 4, the Secrecy Rate decreases gradually, in both EH systems, from 6.5 to 2.9, and in the proposed EH PS system, it decreases from 7.6 to 3.6. This shows that the increment in the path loss exponent degrades the system Secrecy Rate in both the AF and DF Schemes, implying that the self-interference between the relays should be minimized so that the Secrecy Rate does not decrease with the increase in path loss exponent factor.

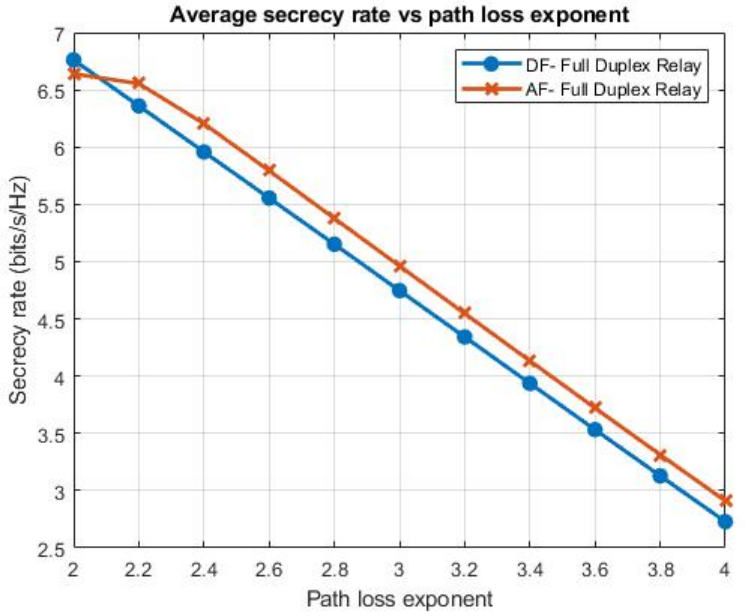

Figure 11. Secrecy Rate vs. Path Loss Exponent for the EH System.

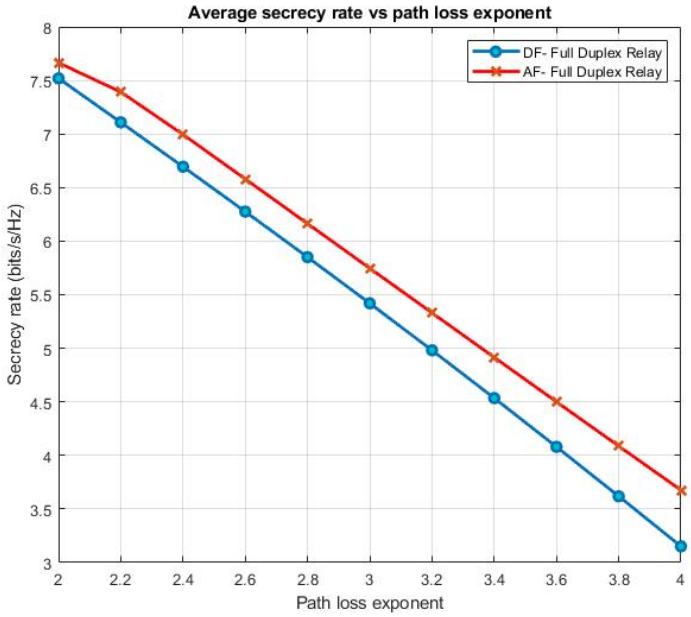

Figure 12. Secrecy Rate vs. Path Loss Exponent.

In Figure 13, a graph is plotted depicting the Outage Probability vs the transmitted SNR with the power splitting ratio $\rho = 0.5$ for the AF and DF Schemes using exact, approximate and asymptotic results. According to our Proposed System Model, the number of destinations (D) is 1 and the number of relays is 2. The curve behavior is similar to a trending curve as the splitting ratio is the same for the DF and AF schemes. In our proposed work, the SNR limit is -10 to 20 dBm, but as the SNR limit increases, the Outage Probability becomes better because the higher SNR value indicates that the Signal power is larger than the Noise power. From the results, it can be clearly seen that from SNR -10 to 15 dBm, DF-approx. and AF-approx. give better Outage Probability values than DF-exact and AF-exact. In addition, in all three scenarios, DF-asymptotic and AF-asymptotic give the highest Outage Probabilities as compared to the other four scenarios.

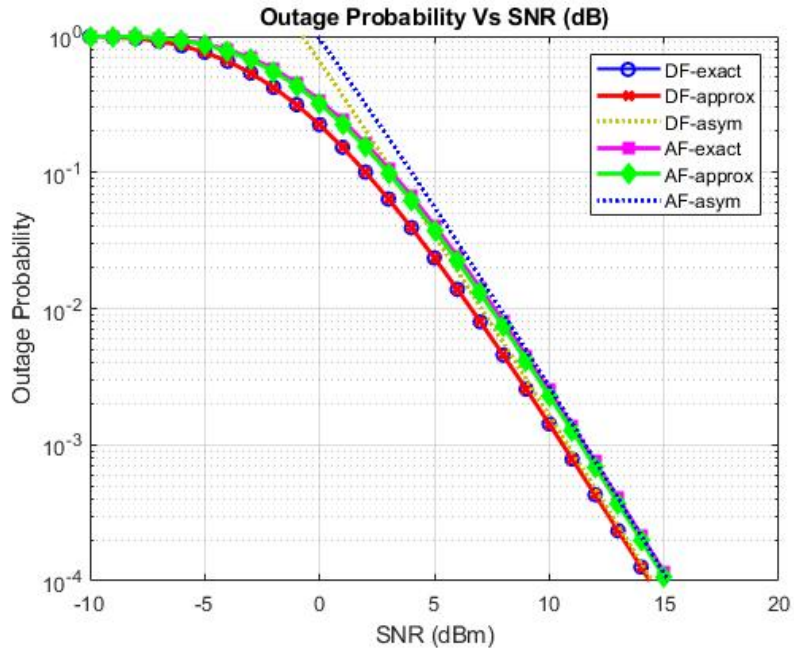

Figure 13. Outage Probability vs. SNR.

In Figure 14, a graph is plotted depicting the Outage Probability and transmitted SNR for different relays with $\rho = 0.5$, for both the AF and DF Schemes, using the exact solution. Generally, the outage Pout (Rt) at end-to-end SNR falls under a few threshold values. When the destination and relay are both 1, then the slope of the curve is almost the same for the AF Scheme and the DF Scheme, but when the destination is 1 and relay is 2, then the slope varies for both the AF and DF Schemes. This shows that as the number of Relays grows, the graph shows increased diversity. Table 2 shows a comparison of the proposed work with the published literature.

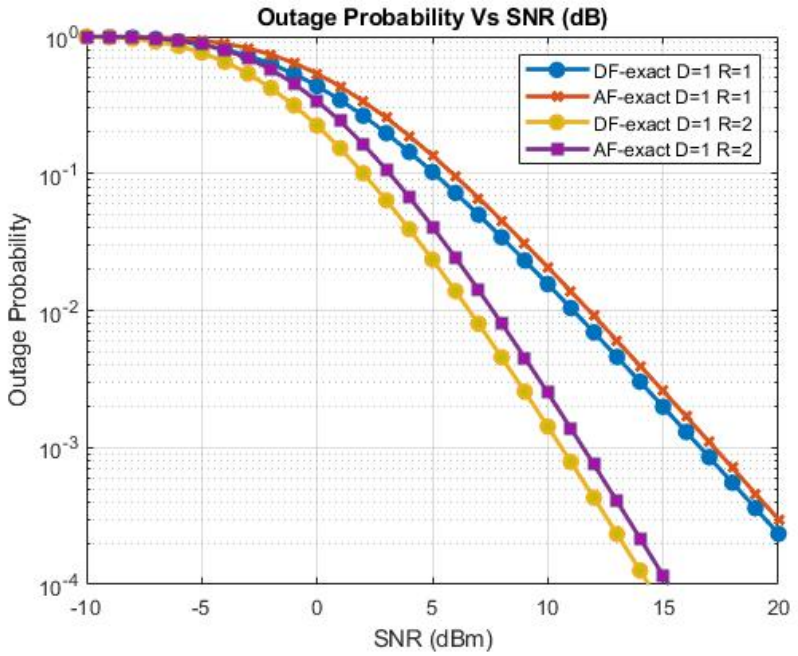

Figure 14. Outage Probability vs. SNR at different K values.

Table 2. Comparison table.

Reference	Investigation	Technique	Cooperative Scheme	
			AF Scheme	DF Scheme
[12]	Single-Hop Relay Network	Energy Harvesting	8.89%	9.83%
[13]	Single-Hop Relay Network	Energy Harvesting and Jamming Signal	23.63%	30.47%
[14]	Single-Hop Relay Network	Physical Layer Security	11.9%	42.86%
[15]	Half-Duplex Relay Network	Amplify and Forward (AF) and Decode and Forward (DF)	40%	41%
Proposed	Multiple-Relay Cooperative System.	Energy Harvesting, Power Splitting, Time Switching, Full Duplex Mode, Secrecy Outage Probability	50.5%	44.2%

6. Conclusions

In this paper, we investigated a three-hop relay network system model, in which the source and relay obtained energy by means of the power beacon with the help of a time-switching EH Scheme. The system's Secrecy Rate considers two cooperative relay schemes: DF and AF. The new techniques use EH, while PS guarantees greater energy efficiency and confidentiality values relative to the conventional EH process. Through the use of the Power Splitting Scheme, the Secrecy Rate is improved by 50.5% in the AF Scheme and by 44.2% in the DF Scheme between the eavesdropper and the relay, which, in the proposed system (Energy Harvesting), are 40 m apart. The resulting analysis shows that the system with PS and EH allows a higher Secrecy Rate than the Conventional EH System

in the AF Cooperative Communication Scheme but not in the DF Scheme. It is shown from the system model that when the channel's path loss exponent increases, the transmission of the information becomes less secure because of self-interference (SIC) between the relays. The compressed sensing multi-hop DF and AF relaying scheme in Energy Harvesting will require further attention in the future.

Author Contributions: Conceptualization, N.S., S.Y., E.M.A., M.A.K., R.S.A.L. and M.A.; methodology, N.S., S.Y., I.B., M.M.K. and M.A.; software, I.B., S.Y., R.S.A.L. and M.A.K.; validation, N.S., S.Y., E.M.A., R.S.A.L., M.A.K., M.M.K., S.K., M.A. and E.L.; formal analysis, S.Y., M.A.K., R.S.A.L., I.B., M.M.K. and M.A.; investigation, N.S., S.Y., E.M.A., R.S.A.L., M.M.K. and M.A.; resources, N.S., S.Y., E.M.A., M.A.K., R.S.A.L., M.M.K., S.K., M.A. and E.L.; data curation, N.S., S.Y., M.A.K., R.S.A.L., I.B. and M.M.K.; writing—original draft preparation, N.S.; writing—review and editing, N.S., S.Y., E.M.A., M.A.K., R.S.A.L., I.B., M.M.K., S.K., M.A. and E.L.; visualization, N.S., S.Y., E.M.A., R.S.A.L., M.M.K., M.A. and E.L.; supervision, S.Y.; project administration, S.Y., M.A. and E.L.; funding acquisition, S.Y., E.M.A., S.K., M.A. and E.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Science and Technology Innovation Project of Zhengzhou 2019CXZX0037, the Special Project for Inter-Government Collaboration of State Key Research and Development Program 2016YFE0118400, and NSFC U1604159. In addition, this project has received funding from the Universidad Carlos III de Madrid and the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie Grant 801538. Furthermore, it received partial funding from the Researchers Supporting Project number RSP-2021/58, King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: All data are included within the manuscript.

Acknowledgments: The authors appreciate the financial support from the Science and Technology Innovation Project of Zhengzhou 2019CXZX0037, the Special Project for Inter-Government Collaboration of State Key Research and Development Program 2016YFE0118400, and NSFC U1604159. Furthermore, the funding from the Universidad Carlos III de Madrid and the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie Grant 801538 is appreciated. Additionally, the partially supported from the Researchers Supporting Project number (RSP-2021/58), King Saud University, Riyadh, Saudi Arabia, is acknowledged.

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

Nomenclature

Acronym	Definition
AF	Amplify-and-Forward
DF	Decode-and-Forward
α	Time-Switching Factor
FDR	Full Duplex Relay
DN	Destination Node
RN	Relay Network
SN	Source Node
T	Transmission Period
ρr	Power Harvest at Relay
R_e	Relay Eavesdropper
ξ	Radio Frequency Energy Harvesting
SWIPT	Simultaneous Wireless Information and Power Transmission
TSR	Time-Switching Relay-Oriented Protocol
PSR	Power-Splitting-Oriented Relay Protocol
AWGN	Additive White Gaussian Noise
PLS	Physical Layer Security
RF	Radiofrequency
RN	Relay Node

P_B	Power Beacon
R_d	Relay Destination
D_{R_1R2}	Distance Between Relay1 and Relay2
ρ	Power
η	Energy Conversion efficiency
N_o	Noise power or variance
P_J	Jamming Signal of power
R_e^{AF}	Relay Eavesdropper AF

Appendix A

The complete Outage probability Theorem 1 given proof Equation (19) can be expressed as:

$$P_{out}^{DF}(R_t) = P_r\left(R_{s_b} < R_t\right) \sum_{m=1}^{M} P_r(D_b = D_m) \times \prod_{k=1}^{K} P_r\left(\min\left\{\alpha\left|h_{R_kE}\right|^2 \beta\left|h_{R_kE}\right|^2 \left|h_{R_kD_m}\right|^2\right\} < R_t\right) \tag{A1}$$

The reader can easily understand by Lemma 1 $P_r\left(R_{s_b} < R_t\right)$.

Lemma 2. *Let* $|\mathrm{h_b}|^2 \max_{1\le \mathrm{l} \le \mathrm{L}}\left\{|\mathrm{h_l}|^2\right\}, \mathrm{l} \in \{1, 2, \ldots . \mathrm{L}\}$, *where* $|\mathrm{h_b}|^2 \in \left\{\left|\mathrm{h_{R_bD}}\right|^2, \left|\mathrm{h_{R_bE}}\right|^2\right\}$, $|\mathrm{h_l}|^2 \in \left\{\left|\mathrm{h_{R_mD}}\right|^2, \left|\mathrm{h_{R_mE}}\right|^2\right\}$, $L \in \{\mathrm{M}, \mathrm{K}\}$.

The cumulative division function (CDF), $F_{|h_b|^2}(z)$, and the Outage probability compactness function (PDF), $F_{|h_b|^2}(z)$, of $|h_b|^2$ can be expressed as follows:

$$F_{|h_b|^2}(z) = 1 + \sum_{l=1}^{L}(-1)^l \sum_{q_1=1}^{L} \ldots\ldots \sum_{q_l=1}^{L} e^{-z\sum_{t=1}^{l}\lambda_{qt}} \tag{A2}$$

$$q_1 < \ldots < q_l$$

$$F_{|h_b|^2}(z) = \sum_{l=1}^{L}(-1)^{l+1} \sum_{q_1=1}^{L} \ldots\ldots \sum_{q_l=1}^{L} \left(\sum_{t=1}^{l}\lambda_{qt}\right) e^{-z\sum_{t=1}^{l}\lambda_{qt}} \tag{A3}$$

$$q_1 < \ldots < q_l$$

Proof. Since $|h_l|^{2\prime}s$ are random variables that are independent of one another and the CDF of $|h_b|^2$ can be shown by $F_{|h_b|^2}(z) = \prod_{l=1}^{L} P_r\left(|h_l|^2 < z\right)$, using the following the multinomial expansion identity

$$\prod_{l=1}^{L}(1 - x_1) = \sum_{l=0}^{L}(-1)^l \sum_{q1=1}^{L} \ldots \sum_{q_l}^{L} \prod_{t=1}^{l} x_{q_t} \tag{A4}$$

$$q_1 < \ldots < q_l$$

and a few subsequent algebraic steps, $F_{|h_b|^2}$ can be obtained via (A1). Taking the derivative of the right-hand side of (A1), the PDF of $|h_b|^2$ can be obtained using Equation (A2). The complete proof of Lemma 2 is given below. Invoking Lemma 2, the probability $P_r\left(R_{s_b} < R_t\right)$ can be given by

$$\Omega = 1 + \sum_{l=1}^{M}(-1)^l \sum_{q_1}^{M} \ldots \sum_{q_l}^{M} e^{-\frac{R_t}{\gamma}\sum_{t=1}^{l}\lambda_{R_{s}qt}} \tag{A5}$$

Next, $\ominus_m$ in Equation (A1) part is derived in the following lemma. □

Lemma 3. *Let* $\ominus_m \hat{=} \mathrm{P_r}(\mathrm{d_b} = \mathrm{d_m})$ *and* $\Gamma_\mathrm{k}\mathrm{P_r}(\mathrm{R_b} = \mathrm{R_k})$. $\ominus_m$ *and* Γ_k, *respectively, given as follows:*

$$\ominus_m = 1 + \sum_{\substack{l=1 \\ l \neq m}}^{M} (-1)^l \sum_{q_1=1,\neq m}^{M} \cdots \sum_{q_l=1,\neq m}^{M} \frac{\lambda_{R_{sm}}}{\lambda_{R_{sm}} + \sum_{t=1}^{l} \lambda_{R_{sqt}}} \tag{A6}$$

$$q_1 < \ldots < q_l$$

$$\Gamma_k = 1 + \sum_{\substack{l=1 \\ l \neq k}}^{K} (-1)^l \sum_{q_1=1,\neq k}^{K} \cdots \sum_{q_l=1,\neq k}^{K} \frac{\lambda_{R_kE}}{\lambda_{R_kE} + \sum_{t=1}^{l} \lambda_{R_{qt}E}} \tag{A7}$$

$$q_1 < \ldots < q_l$$

Proof. Obtaining the multinomial expansion identity is (A3)–(A6) is straightforward using a similar technique. The proof for Lemma 3 is now completed.

The remaining equation part of (A1) will be worked on in the following manner. If $Y\left|h_{R_kE}\right|^2$ and it is specified that $Y = y$, A can be given as:

$$A = \int_0^\infty \left[1 - P_r(\alpha y \geq R_t) P_r\left(\beta y \left|h_{R_kD_m}\right|^2 \geq R_t\right)\right] f_Y(y) dy \tag{A8}$$

where $f_Y(y)$ shows the PDF value of Y. Since $Y = \left|h_{R_e}\right|^2$ and $\left|h_{R_kD_m}\right|^2$ follow exponential division with the rate parameters λ_{R_kE} and $\lambda_{R_kD_m}$, respectively, A can be obtained as:

$$A = 1 - \lambda_{R_kE} \int_\mu^\infty e^{-y\lambda_{R_kE} - \frac{R_t \lambda_{R_kD_m}}{\beta y}}.$$

By plugging (A7) and (A4) into Equation (A1), and invoking Lemma 3, Equation (20) can be used to obtain. □

Appendix B

The complete AF Relying Scheme Theorem 2 is given by Outage Probability, $P_{out}^{AF}(R_t)$ in Equation (23) can be expressed as

$$P_{out}^{AF}(R_t) = P_r\left(R_{s_b} < R_t < R_t\right) \sum_{m=1}^{M} P_r(D_b = D_m) \times \prod_{k=1}^{K} P_r\left(\frac{\alpha\left|h_{R_kE}\right|^2 \beta \left|h_{R_kE}\right|^2 \left|h_{R_kD_m}\right|^2}{\alpha\left|h_{R_kE}\right|^2 + \beta\left|h_{R_kE}\right|^2 \left|h_{R_kD_m}\right|^2 + 1}\right) < R_t \tag{A9}$$

Next, conditioning on $\left|h_{R_kE}\right|^2 = x$, B in the (A8) can be shown as follows:

$$B = \int_0^\infty \left[P_r((\alpha x - R_t)\beta y \left|h_{R_kD_m}\right|^2 < \alpha R_t x + R_t\right] f_{\left|h_{R_kE}\right|^2}(x) dx \tag{A10}$$

if $x \in \left[0, \frac{R_t}{\alpha}\right]$, the probability in Equation (A9) is always 1. Thus, (A9) can be shown as follows:

$$B = \int_0^\mu fX(x) dx + \int_\mu^\infty P_r\left(\left|h_{R_kD_m}\right|^2 < \frac{\alpha R_t x + R_t}{(\alpha x - R_t)\beta x}\right) f_X(x) dx \tag{A11}$$

where $\mu = \frac{R_t}{\alpha}$. Since $\left|h_{R_kE}\right|^2$ and $\left|h_{R_kD_m}\right|^2$ follow the exponential divisions with rate parameters λ_{R_kE} and $\lambda_{R_kD_m}$, respectively, and after the manipulation of algebraic steps, B can be shown as follows:

$$B = 1 - \lambda_{R_kE} \int_{\mu}^{\infty} e^{-y\lambda_{R_kE} - \frac{(\alpha R_t y + R_t)\lambda_{R_kD_m}}{(\alpha y - R_t)\beta y}} dy \tag{A12}$$

Plugging (A4), (A5) and (A11) into (A8), Equation (24) can be given. This is the complete Theorem 2 proof.

References

1. Li, X.; Zheng, Y.; Khan, W.U.; Zeng, M.; Li, D.; Ragesh, G.K.; Li, L. Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1066–1076. [CrossRef]
2. Waqar, O.; Tabassum, H.; Adve, R.S. Secure beamforming and ergodic secrecy rate analysis for amplify-and-forward relay networks with wireless powered jammer. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3908–3913. [CrossRef]
3. Nawaz, M.; Khan, W.U.; Ali, Z.; Ihsan, A.; Waqar, O.; Sidhu, G.A.S. Resource Optimization Framework for Physical Layer Security of Dual-Hop Multi-Carrier Decode and Forward Relay Networks. *IEEE Open J. Antennas Propag.* **2021**, *2*, 634–645. [CrossRef]
4. Shim, Y.; Park, H.; Shin, W. Joint time allocation for wireless energy harvesting decode-and-forward relay-based IoT networks with rechargeable and nonrechargeable batteries. *IEEE Internet Things J.* **2020**, *8*, 2792–2801. [CrossRef]
5. Nguyen, T.N.; Tran, P.T.; Voznak, M. Wireless energy harvesting meets receiver diversity: A successful approach for two-way half-duplex relay networks over block Rayleigh fading channel. *Comput. Netw.* **2020**, *172*, 107176. [CrossRef]
6. Atapattu, S.; Ross, N.; Jing, Y.; He, Y.; Evans, J.S. Physical layer security in full-duplex multi-hop multi-user wireless network with relay selection. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1216–1232. [CrossRef]
7. Phan, V.-D.; Nguyen, T.N.; Le, A.V.; Voznak, M. A Study of Physical Layer Security in SWIPT-Based Decode-and-Forward Relay Networks with Dynamic Power Splitting. *Sensors* **2021**, *21*, 5692. [CrossRef] [PubMed]
8. Chang, S.; Li, J.; Fu, X.; Zhang, L. Energy Harvesting for Physical Layer Security in Cooperative Networks Based on Compressed Sensing. *Entropy* **2017**, *19*, 462. [CrossRef]
9. Truong, T.-V.; Vo, N.-V.; Ha, D.-B.; Tran, D.-D. Secrecy performance analysis of energy harvesting wireless networks with multiple power transfer stations and destinations in the presence of multiple eavesdroppers. In Proceedings of the 2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS), Danang, Vietnam, 14–16 September 2016; pp. 107–112. [CrossRef]
10. Shen, H.; Wang, J.; Levy, B.; Zhao, C. Robust optimization for amplify-and-forward MIMO relaying from a worst-case perspective. *IEEE Trans. Signal Process.* **2013**, *61*, 5458–5471. [CrossRef]
11. Gong, S.; Wang, S.; Chen, S.; Xing, C.; Hanzo, L. Robust energy efficiency optimization for amplify-and-forward MIMO relaying systems. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 4326–4343. [CrossRef]
12. Jindal, P.; Sinha, R. Physical layer security with energy harvesting in single hop wireless relaying system. In Proceedings of the International Conference on Information Science and Applications, Changsha, China, 21–23 July 2017; Springer: Singapore, 2017; pp. 249–256.
13. Sinha, R.; Jindal, P. A study of physical layer security with energy harvesting in single hop relaying environment. In Proceedings of the 2017 4th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2–3 February 2017; pp. 530–533. [CrossRef]
14. Pal, S.; Jindal, P. Secrecy Performance Analysis for Multi-hop and Single-Hop Relaying Model. *Opt. Wirel. Technol. Proc. OWT 2019* **2020**, *648*, 437.
15. Gawtham, K.D.; Jindal, P. Analysis of amplify and forward technique to improve secrecy rate in multi-hop relaying system. In Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 20–21 May 2016; pp. 62–64.
16. Zhou, N.; Wan, B.; Gong, L. Secrecy rate maximisation for non-linear energy harvesting relay networks with cooperative jamming and imperfect channel state information. *ET Commun.* **2020**, *14*, 923–929. [CrossRef]
17. Ding, H.; Ge, J.; da Costa, D.B.; Jiang, Z. A new efficient lowcomplexity scheme for multi-source multi-relay cooperative networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 716–722. [CrossRef]