Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8367107, 7 pages
https://doi.org/10.1155/2022/8367107

WILEY | Hindawi

Research Article

Secrecy Performance by Power Splitting in Cooperative Dual-Hop Relay Wireless Energy Harvesting

Nabila Sehito,[1] Shouyi Yang,[1] Abdullh G. Al Harbi,[2] Muhammad Inam Abbasi,[3] Muhammad Abbas Khan,[4] Muhammad Amir Khan,[5] and Mian Muhammad Kamal[1]

[1]*School of Information Engineering, Zhengzhou University, 100, Science Avenue Zhengzhou 450001, China*
[2]*Department of Electrical Engineering, Faculty of Engineering, Jouf University, Sakaka 42421, Saudi Arabia*
[3]*Centre for Telecommunication Research & Innovation (CETRI), Faculty of Electrical and Electronic Engineering Technology (FTKEE), Universiti Teknikal Malaysia Melaka (UTeM), Melaka 76100, Malaysia*
[4]*Department of Electrical Engineering, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta, Pakistan*
[5]*Department of Computer Science, COMSATS University Islamabad Abbottabad Campus, 22060, Pakistan*

Correspondence should be addressed to Shouyi Yang; nabila@gs.zzu.edu.cn
and Muhammad Inam Abbasi; muhammad_inamabbasi@yahoo.com

Received 17 February 2022; Accepted 22 April 2022; Published 14 May 2022

Academic Editor: Abdul Basit

In wireless communication systems, for secure communication between a transmitter and receiver over the communication channel, the physical layer security is widely utilized. The paper presents a dual-hop wireless full-duplex relay (FDR) network with a source relay and destination relay between two nodes and listening devices. The relay and source use energy harvesting to gain energy from power beacon. Two cooperative techniques are utilized to investigate the amplify-forward (AF) and decode-forward (DF) secrecy capacity in the energy harvesting power splitting system. It is shown that the secrecy performance of an AF relay is better than the secrecy performance of a DF relay in the given form. At 40-meter distance between the relay and the eavesdropper in an energy harvesting system, the AF relay outperforms the DF relay. The simulation is performed using the Monte-Carlo method in MATLAB.

1. Introduction

Cooperative techniques (AF and DF) are significant techniques in wireless communication which play a vital role in wireless networks utilized widely in different branches and applications, including green monitoring systems, social networks, Internet of Things (IoT), and banking systems [1–4]. Thus, the physical layer security of cooperative relaying systems has recently become a major research scope of direction. Significant amount of work has been done in physical layer security to improve secure communication and reduce limitations in cooperative relay networks at both indoor and outdoor propagating environments [5–9].

In [5], a radio signal transmission was secured using an optimum design model from source node to destination through the DF network. In [6], a new two-phase protocol was presented for efficient energy transfer and information relaying, in which the relay operates in full-duplex mode with simultaneous energy harvesting. Ref [7] presents cooperative schemes in dual-hop relaying systems with EH over indoor communication channels categorized by log-normal fading. Similarly, in [8], the cooperative systems are considered with joint time allocation and power splitting schemes.

In addition to enhancing spectrum efficiency, wireless nodes also have major issues in cooperative wireless networks, particularly in energy considerations. In [10], the authors investigated EH to improve the system performance and secrecy rate in a jamming system but did not show the full power of the EH system. In [11], the

Table 1: Paper layout.

Section I	Section II
1. Introduction 1.1. Paper organization	2. System model 2.1 Energy harvesting technique 2.1.1. Decode-forward relay scheme 2.1.2 Amplify-forward relay scheme
Section III	Section IV
3. Secrecy capacity performance 3.1. DF scheme 3.2. AF scheme	4. Simulation results and performance
Section V	
5. Conclusions	

performance and the secrecy rate for both TS and PS protocols were investigated, while [12] investigated the outage probability (OP) over the Rayleigh channel for DF and AF schemes in multiple antennas, respectively. Nevertheless, the EH from the interference node is not considered, and no interference is used, such that only EH from the source is analyzed [13, 14].

In [15], a secrecy performance is investigated comprising a single-hop relay system with improvement of EH of 8.89% for the AF relay and of 9.83% for the DF relay between the eavesdropper and the relay. Ref [16] 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. A geometric programmed (GP) method in [17] was implemented on a full duplex relay network for physical secrecy in a dual-hop relay system. The GP program was applied to power allocation problem on the transmitter side. In [18], the secrecy rate performance of nonorthogonal multiple access and backscatter communication is considered. In [19], they investigated physical layer security ambient backscatter nonorthogonal multiple access in channel estimation errors and imperfect successive interference cancellation with emphasis on reliability and security. The authors in [20] investigated three hop relay cooperative communication networks to perform the two schemes AF and DF, improved by 50.55% (AF) and by 44.2% (DF).

In the current study, we have investigated a dual-hop relay cooperative network with a source, relay, eavesdropper, and EH scheme. The goal of this research is to increase the security performance of such a system, using cooperative scheme AF and DF techniques. We have examined the secrecy performance of our proposed model. The contribution of the present work is summarized as follows.

(i) First, we have investigated a dual-hop wireless relay system containing a single source and a single destination relay, along with two nodes and one eavesdropper

(ii) To propose AF and DF schemes and increase the system secrecy performance in the cooperative network

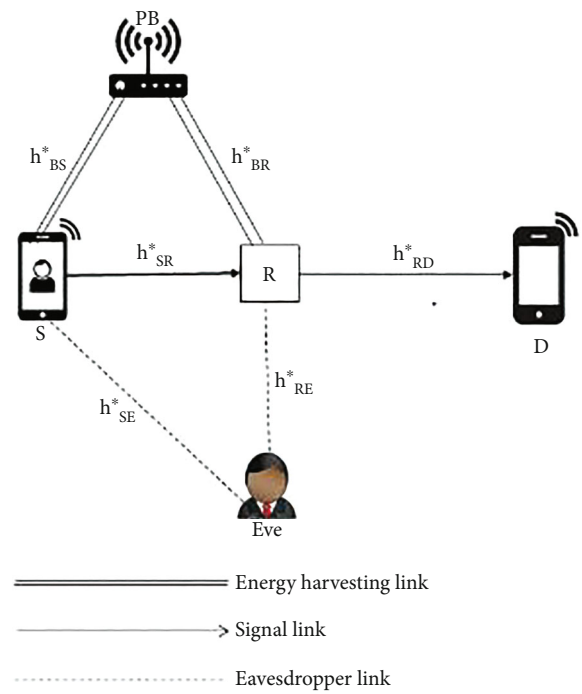

Figure 1: Dual-hop relay network.

(iii) Various parameters, like the time switching protocol, energy harvesting, power splitting ratio, interference relay, and eavesdropper distance, are investigated. The secrecy performance of designed schemes is discussed and compared to the secrecy performance in previous publications

1.1. Paper Organization. The layout of the paper is shown in Table 1.

2. System Model

In this section, we consider a network that relies on a single hop and consists of a relay node (R), source (S), eavesdropper (E), and destination node (D) as presented in Figure 1. It contains power from a beacon (P_B). In Figure 1, $h*_{SR}$, $h*_{RD}$, $h*_{RE}$, and $h*_{SE}$ define the complicated channel gain from P_B to S, while $h*_{BS}$ and $h*_{BR}$ define the

complex channel gain from P_B to R. Additionally, we note that noise is complex. Additive white Gaussian noise (AWGN) at each node has zero mean and variance σ^2 such that no interference is available. Additionally, the relay function is performed with mutual full-duplex relay and half-duplex relay mode techniques.

2.1. Energy Harvesting Technique. In the designed technique, the nodes relay (R) and source (S) harvest energy from the power beacon (P_B). That energy is used to transmit the signals from source S to R and R to D. For high quantities, the time switching- (TS-) based protocol is used for energy harvesting as shown in Figure 2.

The energy harvesting by S and R is given by [17]

$$\begin{aligned} \mathbf{E_S} &= \boldsymbol{\eta}\,\boldsymbol{\alpha}\,\mathbf{P_B}|\mathbf{h}_{\mathbf{BS}}^*|^2\frac{\mathbf{T}}{\mathbf{2}}, \\ \mathbf{E_R} &= \boldsymbol{\eta}\,\boldsymbol{\alpha}\,\mathbf{P_B}|\mathbf{h}_{\mathbf{BR}}^*|^2\frac{\mathbf{T}}{\mathbf{2}}. \end{aligned} \tag{1}$$

The competence coefficient of the proposed method is denoted by $\eta\,(0<\eta<1)$, and the power transmitted by B is denoted by P_B and $0<\alpha<1$. T represents the time taken to transmit the specific block by S and R [17]. Thus, the power transferred by R and S is given by

$$\begin{aligned} P_S &= \eta\,\alpha P_B|h_{BS}^*|^2(1-\alpha), \\ P_R &= \eta\,\alpha P_B|h_{BR}^*|^2(1-\alpha). \end{aligned} \tag{2}$$

2.1.1. Decode-Forward Relay Scheme. This scheme consists of two phases, the first of which is shown in Figure 3. During the initial transmission, the source sends a signal $X(n)$ to the relay and the relay sends the jamming signal $q(2n)$ to the eavesdropper at the same time. In time slot $2n$, the established signal at the R and E is given by [17]

$$Y_R(2n) = \sqrt{\rho P_S}h_{SR}^*x(n) + n_R(2n), \tag{3}$$

$$Y_E(2n) = \sqrt{\rho P_S}h_{SE}^*x(n) + \sqrt{\rho P_{RJ}}h_{RE}^*x(n) + n_E(2n), \tag{4}$$

where the strength of the interference signal from R is given by $n_R(2n)$. In the next time slot, as presented in Figure 4, the R simply sends the already decoded signal to a valid junction and no longer receives the signal. The source at this point sends the jamming signal to the eavesdropper E, and the signal established in time slots $(2n+1)$ at R and D is expressed as [17]

$$Y_R(2n+1) = \sqrt{\rho P_R}\mathrm{h}_{RE}^*x(\mathrm{n}) + \sqrt{\rho P_{SJ}}h_{SE}^*\,qx(n+1) + n_E(2n), \tag{5}$$

$$Y_D(2n+1) = \sqrt{\rho P_R}h_{RD}^*x(n) + n_D(2n+1). \tag{6}$$

2.1.2. Amplify-Forward Relay Scheme. This scenario part has two phases; further, in the first phase, it is the DF scheme. During the initial stages, the signal acquired at R and the eavesdropper E is applied; relay transmits enhanced performance of signals received at the destination in the second phase. The source sends jamming signals to D and E, in the time slot $(2n+1)$, which are received at the same time, given

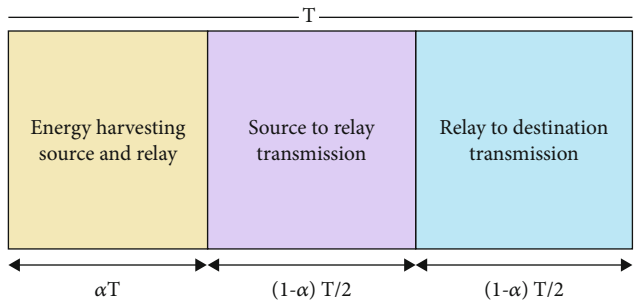

Figure 2: Time switching-based protocol.

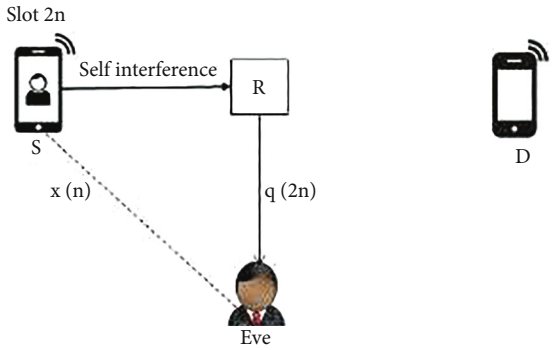

Figure 3: Illustration of the signal transmission for the $2n$ time slot.

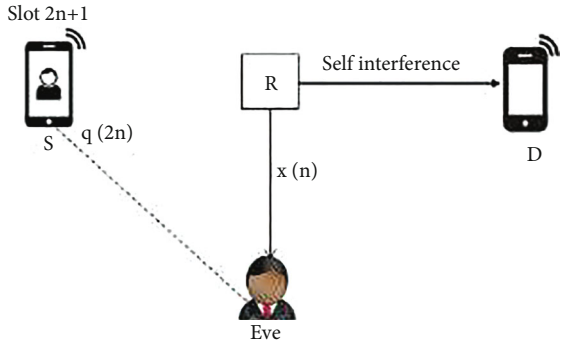

Figure 4: Illustration of the signal transmission in the $(2n+1)$ time slot.

$$Y_D(2n+1) = G\sqrt{\rho P_S}h_{RD}^*Y_R(2n) + n_D(2n+1), \tag{7}$$

$$Y_E(2n+1) = G\sqrt{\rho P_{SJ}}h_{SE}^*\,qx(2n+1) + n_E(2n+1). \tag{8}$$

Here, we defined the scaling factor G. The fluctuation of the channel coefficient is

$$G = \frac{1}{\sqrt{P_{R_1}|h_{SR1}|^2+N_0}}, \tag{9}$$

where N_0 is the AWGN noise variance.

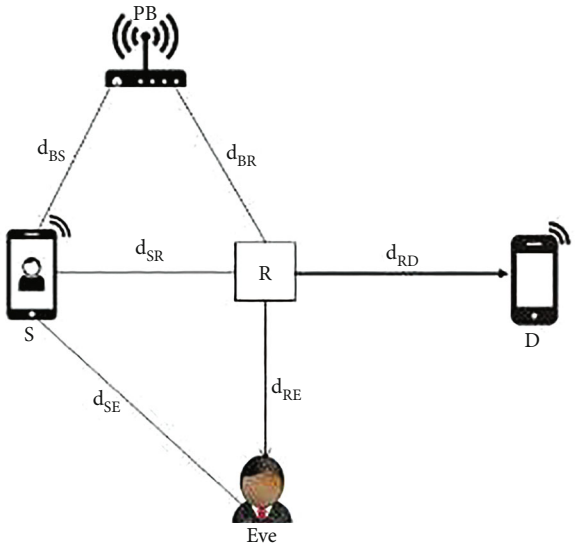

Figure 5: Numerical model.

Table 2: Parameter used for the simulation.

Parameter	Single-relay network
D_{SR}	25 m
D_{RE}	30 m
D_{RD}	15 m
D_{RB}	14 m
RNT	Line of sight (LOS)
PLE	3.5
Number of relay	1
Communicate energy	30 dBm
Make noise power	-40 dBm
α	0.999
ρ	3.5

3. Secrecy Capacity Performance

Further, we present a performance secrecy model in terms of secrecy rate. The signal information that may be transferred over a wireless channel to an eavesdropper is defined as the secrecy rate. The next two sections investigate the secrecy rate in AF and DF cooperative networks.

3.1. DF Scheme. The secrecy capacity at D and E is defined by equations (3)–(6) for a full-duplex relay in [17]. Thus, we obtain

$$R_d = \frac{1}{2}\log_2(1+\rho P_R \alpha_{RD}), \tag{10}$$

$$R_e = \frac{1}{2}\log_2\left(1+\frac{P_S\alpha_{SE}}{1+P_{RJ}\alpha_{RE}}+\frac{\rho P_R\alpha_{RE}}{1+\rho P_{RJ}\alpha_{SE}}\right). \tag{11}$$

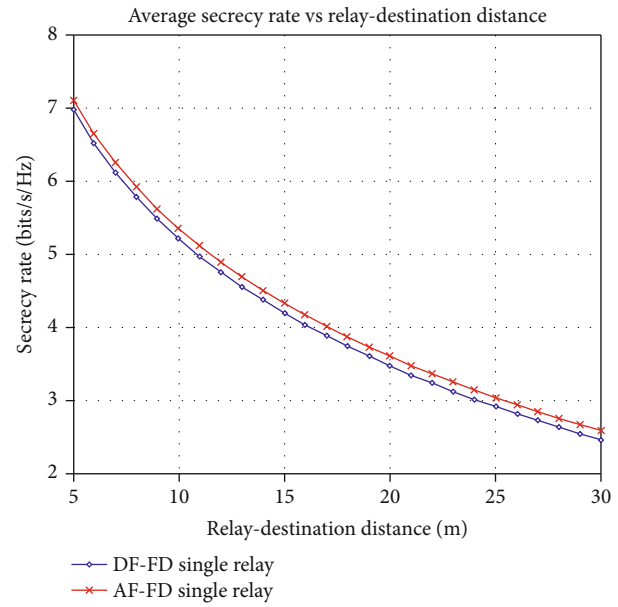

Figure 6: Secrecy rate vs. d_{RD} for the EH system.

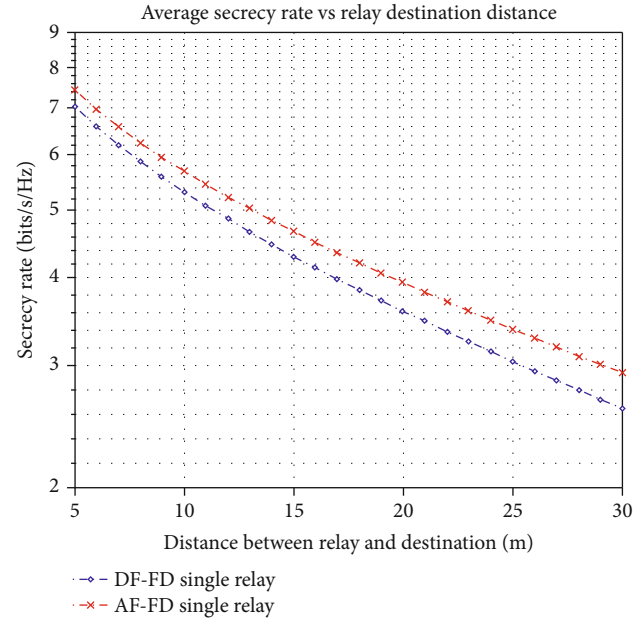

Figure 7: Secrecy rate vs. D_{RD} for the proposed EH and PS system.

Here, we define

$$\alpha_{RD} = \frac{|h_{RD}|^2}{\sigma^2}, \alpha_{SE} = \frac{|H_{SE}|^2}{\sigma^2}, \alpha_{RE} = \frac{|h_{RE}|^2}{\sigma^2}. \tag{12}$$

Using equations (6) and (7), the achievable secrecy rate is given by $R_S = \max\{R_d - R_e, 0\}$, where it is given in

$$R_d - R_e = \frac{1}{2}\log_2\left(\frac{1+\rho P_R\alpha_{RD}}{1+(\rho P_S\alpha_{SE}/(1+\rho P_R\alpha_{RE}))+(P_R\alpha_{RE}/(1+P_{SJ}\alpha_{SE}))}\right). \tag{13}$$

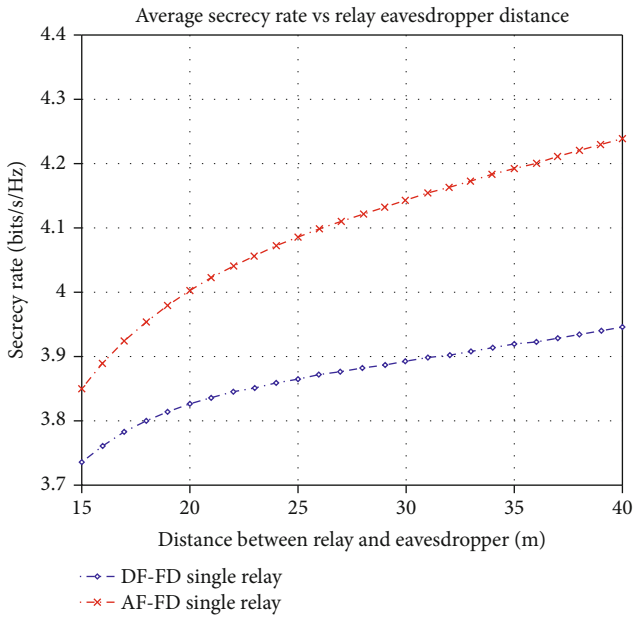

Figure 8: Secrecy rate vs. D_{RE} for the energy harvesting system.

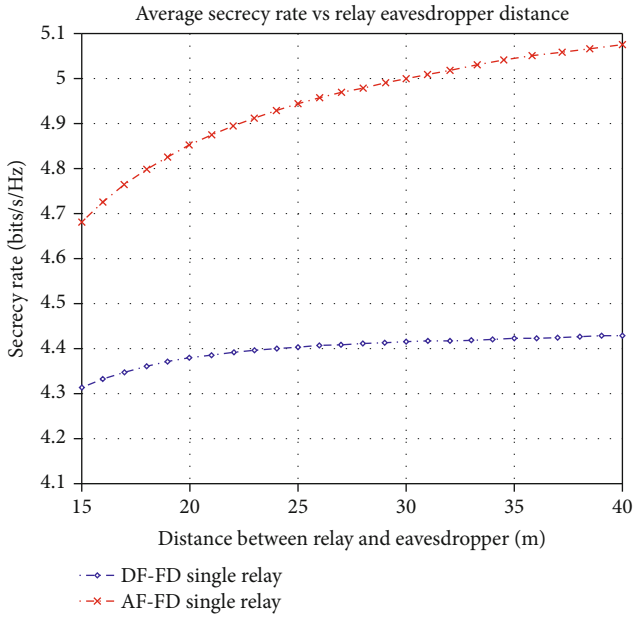

Figure 9: Secrecy rate vs. D_{RE} for the energy harvesting power splitting system.

3.2. AF Scheme. Using further equations (7) and (8) at D and E, the secrecy capacity rate can be obtained from

$$R_d = \frac{1}{2}\log_2\left(1 + G^2\rho P_S \alpha_{RD}\right), \tag{14}$$

$$R_e = \frac{1}{2}\log_2\left(\frac{1+\rho P_S\alpha_{SE}}{1+\rho P_{RJ}\alpha_{RE}} + \frac{G^2\rho P_S\alpha_{RE}}{1+P_{SJ}\alpha_{SE}}\right). \tag{15}$$

The secrecy rate is here obtained as given as $R_S = \max\{R_d - R_e, 0\}$, whereas

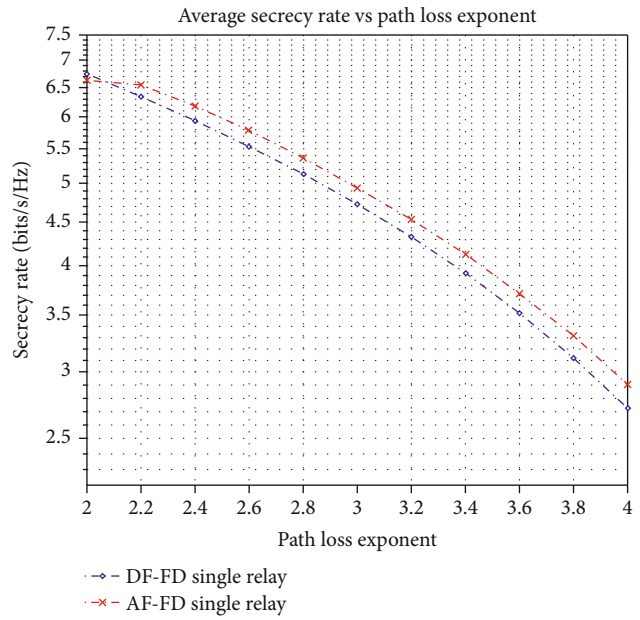

Figure 10: Secrecy capacity rate vs. PLE for the EH system.

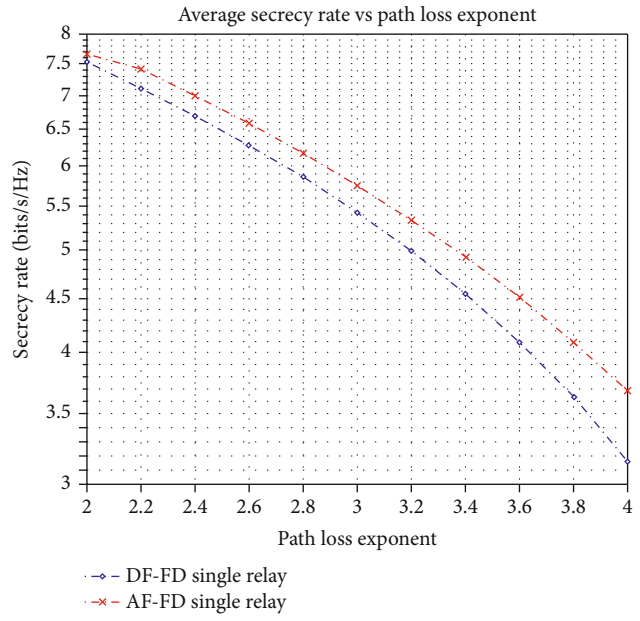

Figure 11: Secrecy capacity rate vs. PLE for the EH PS system.

$$R_d - R_e = \frac{1}{2}\log_2\left(\frac{1+\rho P_R\alpha_{RD}}{1+\left(P_S\alpha_{SE}/\left(1+P_J\alpha_{RE}\right)\right)+\left(G^2\rho P_S\alpha_{RE}/\left(1+P_{SJ}\alpha_{SE}\right)\right)}\right). \tag{16}$$

4. Numerical Results and Performance

This section presents the numerical results for the investigation of the secrecy performance of the proposed system model, in dual-hop EH and AF and DF cooperative scenarios in terms of relay distance. The numerical results based on the simulation model are shown in Figure 5; the S, R, and D are assumed to be the presence of a line of sight (LOS);

Table 3: Performance comparison of the cooperative scheme concerning their secrecy rate.

Reference	Techniques	Cooperative scheme	
		Amplify-forward	Decode-forward
[17]	HADF, FDR, EPA	29.26%	29.26%
[15]	Energy harvesting	8.89%	9.83%
[16]	Energy harvesting and jamming signal	23.63%	30.47%
[21]	AF and DF	11.9%	42.96%
[22]	HDR, AF, and DF	40%	41%
[20]	EH, TS, PS, FDR, SOP	50.5%	44.2%
Present article	EH, PS, AF, DF, single relay, HDR, FDR	65.5%	52.5%

moreover, d_{RD}, d_{RE}, d_{BS}, and d_{BR} indicate the distances between R and S nodes, between D and R, between E and R, between P_B and S, between R and P_B, and between S and R. The distance between S and E nodes can be, respectively, given as

$$d_{SE} = \sqrt{d_{SR}^2 + d_{RE}^2}. \quad (17)$$

Source, relay, and destination are located in the line of sight (LOS). The channel model configuration describes the channel between any two nodes, which is uniformly distributed within $[0, 2\pi]$, with path loss exponent $c = 3.50$ [17].

We assume that the transmission power of the beacon is $P_B = 30$ dBM and the noise power is $N_B = -40$ dBm.

Furthermore, it is assumed that $d_{BS} = id_{BR} = 14$ m. Moreover, $\alpha = 0.999$, $\eta = 1$, and $p = 3.5$.

The parameters used for the simulation of this research are shown in Table 2.

In Figures 6 and 7, we give the plot of the security performance AF and DF dual-hop scheme and distance between relay (R) and destination (D), when $d_{SR} = 25$ m, $d_{BR} = 14$ m , and $d_{RD} = 30$ m in the proposed EH system and PS EH system. The plot of secrecy capacity shows that the secrecy capacity decreases with increasing distance between destination and relay, but at the same time due to the power splitting receiver in the EH system, the secrecy rate is quite high which is good. Also, this figure clearly shows that the AF single-relay scheme gives a better secrecy rate than the DF single-relay scheme.

In Figures 8 and 9, we compare the secrecy rate distance between relay and eavesdropper between the AF and DF schemes, when $d_{SR} = 10$ m and $d_{RD} = 30$ m. The graph shows the secrecy rate in the energy harvesting (EH) system depending on the distance between R and E. In the proposed EH PS system, the secrecy rate is very high for the power splitting receiver. Also, in the AF scheme, the secrecy rate is better than that in the DF Scheme. Therefore, to increase the secrecy rate, it is important to use a share of useful power to relay jamming signals in both AF and DF.

In Figures 10 and 11, we plot the average secrecy rate as a function of the path loss exponent factor in the single-relay AF and DF schemes, when $d_{SR} = 10$ m, $d_{RD} = 15$ m, and $d_{RE} = 15$ m. Path loss plays a vital role in the calculation of the secrecy rate. The graph shows that as we increase the path loss exponent, the secrecy rate decreases gradually in both the existing EH systems and the proposed EH PS system. It is shown that the increment in the path loss exponent degraded the system secrecy capacity in both AF and DF schemes. This implies that self-interference should be minimized.

The comparison of the cooperative proposed techniques with the published literature is shown in Table 3.

5. Conclusions

In this study, we have proposed the energy harvesting single-relay cooperative system, to enhance the performance of secure wireless communications in the existence of one eavesdropper E and relay R. Under a total transmitted power constraint of 30 dBm and noise power of -40 dBm, the secrecy performance of a single-relay wireless cooperative system is investigated, and an innovative single-relay technique has been applied. In the proposed technique, each R transmits a signal to the E and gets a transmission signal at the same time. Two cooperative schemes have been examined: amplify-forward (AF) and decode-forward (DF) in energy harvesting. The results show that secrecy rate performance is improved by AF FDR for single relay to 65.5% and DF FDR for single relay to 52.5% in the energy harvesting power splitting system. Furthermore, we show that an increase in the path loss exponent degrades the performance of the system.

Notations

FDR: Full duplex relay
HADF: Hybrid decode forward
LOS: Line of sight
EPA: Equal power allocation
T: Transmission period of energy harvesting
n_E: Energy conversion efficiency of an eavesdropper
P_{RJ}: Power relay jamming
ρP_R: Signal of power relay
n_D: The energy efficiency of the destination
N_0: Noise variance
G: The fluctuation of the channel coefficient
h_{SR}^*: Channel gain source to relay
A: Time switching factor
P_E: Power signal eavesdropper

P_B: Power Beacon
d_{BR}: Distance beacon relay
R_e: Relay eavesdropper.

Data Availability

All the data have been included in the study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] R. Francesco, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1354–1367, 2012.

[2] F. Jameel, W. U. Khan, M. A. Jamshed, H. Pervaiz, Q. Abbasi, and R. Jäntti, "Reinforcement learning for scalable and reliable power allocation in SDN-based backscatter heterogeneous network," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, 2020.

[3] W. U. Khan, N. Imtiaz, and I. Ullah, "Joint optimization of NOMA-enabled backscatter communications for beyond 5G IoT networks," *Internet Technology Letters*, vol. 4, no. 2, article e265, 2021.

[4] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, Cambridge, United Kingdom, 2011.

[5] F. Jameel, W. U. Khan, S. T. Shah, and T. Ristaniemi, "Towards intelligent IoT networks: reinforcement learning for reliable backscatter communications," in *2019 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Waikoloa, HI, USA, 2019.

[6] Y. Zeng and R. Zhang, "Full-duplex wireless-powered relay with self-energy recycling," *IEEE Wireless Communications Letters*, vol. 4, no. 2, pp. 201–204, 2015.

[7] K. M. Rabie, B. Adebisi, and M. -S. Alouini, "Half-duplex and full-duplex AF and DF relaying with energy-harvesting in log-normal fading," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 4, pp. 468–480, 2017.

[8] J. Shen, Y. Liu, H. Yang, and C. Yan, "Joint time allocation and power splitting schemes for amplify-and-forward relaying network over log-normal fading channel," in *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, Hangzhou, China, 2018.

[9] X. Li, M. Huang, C. Zhang et al., "Security and reliability performance analysis of cooperative multi-relay systems with nonlinear energy harvesters and hardware impairments," *Access IEEE*, vol. 7, pp. 102644–102661, 2019.

[10] T. M. Hoang, T. Q. Duong, N. S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174–177, 2017.

[11] L. Elmorshedy, C. Leung, and S. A. Mousavifar, "RF energy harvesting in DF relay networks in the presence of an interfering signal," in *2016 IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, 2016.

[12] T. Mekkawy, R. Yao, F. Xu, and L. Wang, "Optimal power allocation for achievable secrecy rate in an untrusted relay network with bounded channel estimation error," in *2017 26th Wireless and Optical Communication Conference (WOCC)*, pp. 1–5, Newark, NJ, USA, 2017.

[13] G. Yanju and S. Aissa, "Interference aided energy harvesting in decode-and-forward relaying systems," in *IEEE International Conference on Communications, 2014 (ICC 2014)*, pp. 5378–5382, Sydney, NSW, Australia, 2014.

[14] Y. Alsaba, C. Y. Leow, and S. K. Abdul Rahim, "A game-theoretical modelling approach for enhancing the physical layer security of non-orthogonal multiple access system," *IEEE Access*, vol. 7, pp. 5896–5904, 2019.

[15] P. Jindal and R. Sinha, "Physical layer security with energy harvesting in single hop wireless relaying system," in *International Conference on Information Science and Applications*, pp. 249–256, Changsha, China, 2017.

[16] R. Sinha and P. Jindal, "A study of physical layer security with energy harvesting in single hop relaying environment," in *2017 4th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 530–533, Noida, India, 2017.

[17] P. Jindal and R. Sinha, "Physical layer security with rf energy harvesting protocols for wireless networks," *Pertanika Journal of Science and Technology*, vol. 26, pp. 1677–1692, 2018.

[18] W. U. Khan, J. Liu, F. Jameel, M. T. R. Khan, S. H. Ahmed, and R. Jäntti, "Secure backscatter communications in multi-cell NOMA networks: enabling link security for massive IoT networks," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 213–218, Toronto, ON, Canada, 2020.

[19] X. Li, M. Zhao, M. Zeng et al., "Hardware impaired ambient backscatter NOMA systems: reliability and security," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2723–2736, 2021.

[20] N. Sehito, S. Yang, E. M. Ali et al., "Physical layer secrecy by power splitting and jamming in cooperative multiple relay based on energy harvesting in full-duplex network," *Electronics*, vol. 11, no. 1, 2021.

[21] S. Pal and P. Jindal, "Secrecy performance analysis for multi-hop and single-hop relaying model," in *Optical and Wireless Technologies Proceedings of OWT 2019*, Jaipur, India, 2020.

[22] K. D. Gawtham and P. Jindal, "Analysis of amplify and forward technique to improve secrecy rate in multi-hop relaying system," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 62–64, Bangalore, India, 2016.