Pertanika J. Sci. & Technol. 26 (4): 1677 - 1692 (2018)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Physical Layer Security with RF Energy Harvesting Protocols for Wireless Networks

Jindal, P.* and Sinha, R.

Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra-136119, India

ABSTRACT

In this paper, the secrecy performance of two energy harvesting (EH) protocols, known as, time switching (TS) and power splitting (PS) is analyzed for a single hop relaying network, in which the sender sends the data to legitimate destination using a relay in the presence of an eavesdropper. In the considered network, the relay and source are powered up by using energy harvesting techniques. The performance of the systems with EH is compared with that of the conventional physical layer security model, where nodes are powered up by individual battery sources. The secrecy rates with the two different types of EH protocols and conventional system are analyzed for two relaying schemes: decode-and-forward (DF), and amplify-and-forward (AF). Resulting analysis shows that the TS EH system has higher secrecy rate as compared to conventional system and the secrecy rate of the conventional system is higher than that of PS EH protocol.Further, the simulation results show that AF relays outperforms DF relays in all the scenarios.

Keywords: Amplify and forward, energy harvesting, jamming, physical layer security, secrecy rate

INTRODUCTION

Physical layer security (PLS) and energy harvesting have been gaining a phenomenal growth and attention from the research community. PLS guarantees and enhance confidentiality of the transmitted information (Wyner, 1975), whereas EH utilizes the harvested energy for information processing (Hoang, Duong, Vo, & Kundu, 2017). Although an in-depth investigation of both technologies as an individual body of knowledge has been done in the literature, but the combination of both has been recently recurred as an attractive research paradigm. Physical layer

ARTICLE INFO

Article history:
Received: 30 August 2017
Accepted: 27 June 2018
Published: 24 October 2018

E-mail addresses:
poonamjindal81@nitkkr.ac.in (Jindal, P.)
rupalisinha468@gmail.com (Sinha, R.)
* Corresponding author

ISSN: 0128-7680
e-ISSN: 2231-8526

security helps in providing secure data transmission by using physical characteristics of the wireless medium.

Various techniques are used to support PLS such as jamming, full duplex operations, interference cancellation, relaying schemes such as DF and AF (Dong, Han, Petropulu, & Poor, 2010). Conventionally, nodes in the wireless networks perform their respective roles using individual battery sources. However, in some situations, it is not possible to recharge or replace these batteries (Zhan, & Ho, 2013).

Sometimes, especially in wireless sensor networks, it is hazardous to replace these batteries. Moreover, it is the need of the hour to adopt energy efficient systems as a concern towards environment and conserve energy as much as much as possible as disposal of batteries is also not environment friendly. Different sectors of information and communication technologies (ICT) greatly contribute in CO_2 emission and huge energy consumption. In 2012, about 4.7% of world's electrical energy was consumed by ICT (approx. 920 TWh, 1 TWh=10^{12} Watt hour) and releasing around 1.7% of total carbon emission into the atmosphere. Saving energy to prolong the lifetime of energy constrained nodes, maintaining the parameter metric i.e. secrecy rate, throughput, outage probability, optimize the power allocation to nodes, maintaining the confidentiality, authentication during transmission between legitimate nodes are some of the critical issues in wireless networks.

EH techniques helps in solving energy issues to some extent (Yuen, Elkashlan, Qian, Duong, Shu, & Schmidt, 2015 Part I-III). The two commonly used EH protocols are PS and TS (Nasir, Zhou, Durrani, & Kennedy, 2013). Recently, EH technique has gained considerable attention, especially in energy-constrained networks. This technique involves conversion of the received radio frequency (RF) signal into electricity. It helps wireless devices so that it can harvest energy from RF signals for processing and transmission of information simultaneously. Concept of simultaneous wireless information power transfer (SWIPT) has attracted researchers to replenish energy limited devices. Radio frequency (RF) signal can carry information and energy simultaneously and thus motivating green communication for energy scavenging. Hence, green communication has emerged as latest technology to power next generation wireless networks.

PLS provides the confidentiality to the information. When it combines with the cooperative schemes, enhances the signal coverage along with secrecy. Further, when both of the techniques are combined with RF EH technology, enhances the lifetime of battery-constrained devices. The combination of three techniques; providing information security while maintaining the energy of wireless nodes is considered in this paper. Therefore, the scenario of PLS with energy deprived relay nodes is taken into consideration. The beacon node allocates energy to source and relay node. TS and PS protocols are used to evaluate the secrecy rate of system. In TS, time switching factor is decided to perform energy

harvesting (EH) and information processing (IP). In PS, some portion of received power is used for EH, while remaining power for IP by the relay. Further, EH techniques have been implemented using AF and DF relaying techniques. The performance of systems employing EH techniques is compared with that of the conventional system in terms of secrecy rate, the rate at which information can be sent securely from sender to the intended receiver. An in-depth analysis of different energy harvesting protocols with physical layer security in different cooperative scenarios makes this paper different from the existing work, as the existing literature does not present such a deep insight and an extensive comparative analysis of the problem under study.

Related Work

Some recent studies have investigated the protocols used in EH for transferring confidential information through PLS. For secure communication, power splitting receivers are used for evaluating performance of DF and AF protocols using secrecy outage probability (Son, & Kong, 2015). EH based AF multi antenna, HD relay network with EH relaying protocols: TSR, PSR and IRR in presence of passive eavesdropper is studied. The expression for ergodic secrecy capacity is derived and factors affecting secrecy capacity are investigated. Time switching ratio and power splitting factor for TS and PS are further calculated. (Salem, A., Hamdi, & Rabie, 2016). Two-phase communication protocol for wireless powered cooperative jammer is proposed where energy is harvested by signal transmitted by source. High SNR and antenna regime are considered for increasing throughput with fixed rate transmission.Throughput maximization is done by optimal time allocation for PS and TS protocols. (Liu, Zhou, Durrani, & Popovski, 2016). Wireless power transfer schemes for source, destination and joint destination and source are analyzed. Further, two suboptimal strategies for WPT are proposed to maximize information throughput (Zhang, & Chen, 2017). FD information source capable of self energy recycling, powered by energy source for transmitting confidential information is given (Wu, Wang, Deng, & Zhang, 2017).

Need of Cooperative Physical Layer Security with RF Energy Harvesting

The area under study has a number of real time applications. The upcoming wireless networks including IoTs, 5G networks are based on sensor nodes. Extensive amount of sensitive information is collected and transmitted from wireless sensor nodes that are powered up by individual battery source and their energy is depleted with the passage of time. The proposed schemes are beneficial in extending the battery lifetime while maintaining the information security. The work presented in this paper is beneficial in the military applications where, the soldiers work at hard to reach places and cooperative physical layer security with energy harvesting provides the secure signal transmission with improved coverage and unbreakable connection between the headquarters and the

soldiers. Further, the present era has completely shifted towards the wireless technologies, where there is a huge demand for low cost devices. With the help of RF EH, it is possible to obtain energy from the RF signals, resulting in efficient use of available energy. RF EH techniques are used in wireless body networks, wireless sensor networks, wireless-charging systems etc. Several commercial products are also available in the market based on the EH technique such as power caster and cota system. Due to various advantages of RF EH techniques, it can be collaborated with several types of networks such as cognitive radio networks (CRNs), heterogeneous networks and cellular networks for improving the energy efficiency of the system.

Physical Layer Security Model

The system model for the conventional system is shown in Figure 1. It consists of a source S, a destination D, a relay R, in presence of an eavesdropper E. The complex channel gains from S to R, from S to E, from R to D, and from R to E are denoted by h^*_{SR}, h^*_{SE}, h^*_{RD}, and h^*_{RE}, respectively. For the EH technique, the system model is shown in Figure 2. It is similar as that of the conventional system, except the beacon node, which is absent in the conventional system. Let h^*_{BR} and h^*_{BS} represents the complex channel gains from B to R and from B to S, respectively. It is assumed that the noise is additive white Gaussian noise (AWGN) with mean zero and variance σ^2 and self-interference is perfectly cancelled. Moreover, the relay switches between half and full duplex operations (Sinha, & Jindal, 2016). Full duplex relay (FDR) is able to receive and transmit signal at the same time.

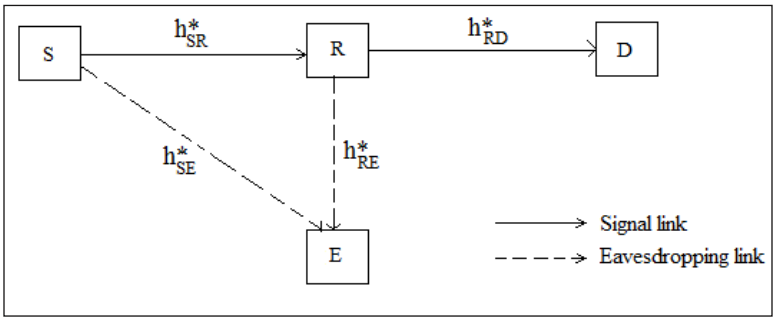

Figure 1. System model with single relay of conventional system

Energy Harvesting Protocol

In literature there are mainly three protocols used for EH system, TSR, PSR, IRR (ideal relay receiver).Among these TSR and PSR are most popularly used to replenish energy to deprived nodes during transmission.In two-phase communication the total time allotted to relay is divided between power transfer (PT) and information transmission (IT) time in TSR. On the other hand, total power is divided into two portions depending on power

splitting ration in PSR for PT and IT. Therefore, time allocation between PT and IT must be carefully designed to improve the throughput.In this paper, two energy harvesting protocols including time switching and power splitting have been analyzed.

A wireless communication system is developed, where legitimate nodes i.e. source S and destination D share confidential information with the aid of intermediate node. Beacon node B is used to allocate power to S and R for harvesting energy. The model has been implemented with the assumptions that there is no direct communication between S and D, relay node assist in between. Only one relay node is considered for simplicity. Relay and source nodes are energy constrained nodes and these nodes first harvest energy from beacon node and then use the harvested energy using TSR and PSR protocol. Amongst various relaying protocols, AF and DF are used and compared based on secrecy rate. Further, it is assumed that channel state information (CSI) is available.

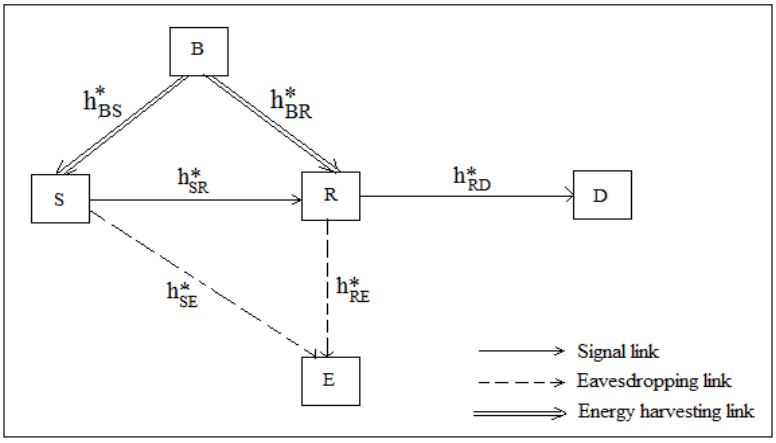

Figure 2. System model with single relay employing EH

Time Switching EH Protocol

Time switching protocol is shown in Figure 3, where T represents the total time required to transmit certain block of information from source to destination. As shown in Figure 3, the source and relay harvests energy from the beacon for duration of αT and $0 \leq \alpha \leq 1$. Data is transmitted from source to relay for half of the remaining time, and from relay to destination in remaining time duration (Sinha, & Jindal, 2017).

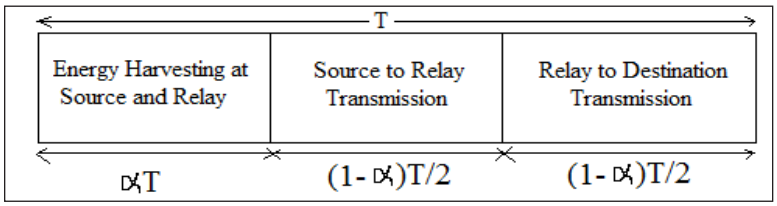

Figure 3. Time Switching EH Protocol

The harvested energy by S and R is given by (Nguyen, Duong, Ngo, Hadzi-Velkov, & Shu, 2016):

$$E_S = \eta P_B \alpha T \left| h_{BS}^* \right|^2 \quad [1]$$

$$E_R = \eta P_B \alpha T \left| h_{BR}^* \right|^2 \quad [2]$$

where, η represents efficiency of energy conversion technique, P_B denotes power of the beacon and α is the time fraction.

Therefore, the transmit power of S and R is given by (Nguyen, Duong, Ngo, Hadzi-Velkov, & Shu, 2016).

$$P_S = \frac{2\eta P_B \left| h_{BS}^* \right|^2 \alpha}{1-\alpha} \quad [3]$$

$$P_R = \frac{2\eta P_B \left| h_{BR}^* \right|^2 \alpha}{1-\alpha} \quad [4]$$

Power Splitting EH Protocol

Figure 4. showsPS EH protocol. As shown in the Figure 4, T represents time required to send a given block of information from sender to intended receiver. This duration is divided into two parts. During the first half, energy is harvested by source and relay, a portion of the signal is utilized for EH and rest of the signal is utilized for communication between source and relay. During the next half, relay sends the data to intended destination.

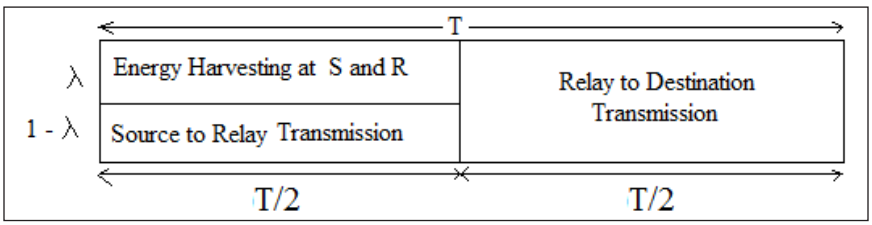

Figure 4. Power Splitting EH Protocol

The harvested energy by S and R is given by (Nasir, Zhou, Durrani, & Kennedy, 2013) as:

$$E_S = \eta \lambda P_B \left| h_{BS}^* \right|^2 (T/2) \quad [5]$$

$$E_R = \eta \lambda P_B \left| h_{BR}^* \right|^2 (T/2) \quad [6]$$

where, λ is the fraction of the signal used for EH.

Therefore, power transmitted by S and R is given by (Nasir, Zhou, Durrani, & Kennedy, 2013) as:

$$P_S = \eta\lambda P_B \left|h_{BS}^*\right|^2 \quad [7]$$

$$P_R = \eta\lambda P_B \left|h_{BR}^*\right|^2 \quad [8]$$

Cooperative Schemes

In this paper, two cooperation schemes amplify-and-forward and decode-and-forward have been analyzed with TS and PS EH protocols. The signal transmission with AF and DF schemes are detailed below:

Decode-and-Forward (DF) Scheme

It consists of two stages. The first stage involves transmission of information signal *x(n)* from source to relay and transmission of jamming signal *q(n)* by relay to the eavesdropper, simultaneously as shown in Figure 5.

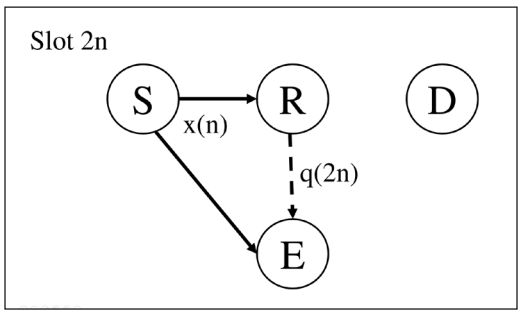

Figure 5. Signals transmitted in 2nth time slot

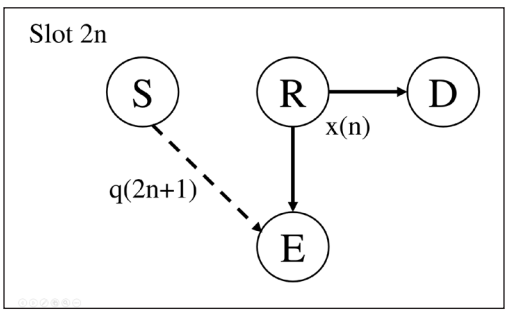

Figure 6. Signals transmitted in (2n+1)th time slot

Signals received by R and E during 2nth time slot are given by (Lee, 2015) as:

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

$$y_E(2n) \aleph \sqrt{\rho P_S}\, h_{SE}^* x(n) \quad \sqrt{\rho P_{RJ}}\, h_{RE}^* q(2n) \quad n_E(2n) \quad [9]$$

where, P_{RJ} denotes the jamming power of relay and $n_R(2n)$ and $n_E(2n)$ represents AWGN at relay and eavesdropper. Also, $\rho = 1$, for TS EH and $\rho = 1 - \lambda$, for PS EH.

In the second stage, relay first decode the received encoded signal, then re-encode it, and finally, transmits the re-encoded signal to destination. At the same time, source sends the jamming signal to the eavesdropper as shown in Figure 6.

Signals received by E and D in (2n+1)th time slot are given by (Lee, 2015):

$$y_E(2n+1) = \sqrt{P_R}\, h_{RE}^{*} x(n) + \sqrt{P_{SJ}}\, h_{SE}^{*} q(2n+1) + n_E(2n+1),$$
$$y_D(2n+1) = \sqrt{P_R}\, h_{RD}^{*} x(n) + n_D(2n+1) \quad [10]$$

where, P_{SJ} represents the jamming signal power of the source and n_D (2n + 1)denotes AWGN at D.

Amplify-and-Forward (AF) Scheme

This scheme also consists of two stages similar to that of DF scheme. Stage 1 is same as that of the DF scheme. Signals obtained at R and E during first stage is given by [9]. In second stage, relay sends amplified version of signal received to the destination. At the same instant, source sends jamming signal to destination. Signals received by D and E in time slot (2n+1) are given by:

$$y_D(2n+1) = G\sqrt{P_S}\, h_{RD}^{*} y_R(2n) + n_D(2n+1),$$
$$y_E(2n+1) = G\sqrt{P_S}\, h_{RE}^{*} y_R(2n) + \sqrt{P_{SJ}}\, h_{SE}^{*} q(2n+1) + n_E(2n+1) \quad [11]$$

Where, scaling factor (Kumar & Bhatia, 2015) is represented by $G = \frac{1}{\sqrt{P_S |h_{SR}|^2 + N_o}}$ and N_o represents variance of noise.

Achievable Secrecy Rate

Performance analysis has been done in terms of secrecy rate. Secrecy rate is defined as the amount of information that can be securely transmitted over the wireless medium in the presence of eavesdropper. The achievable secrecy rate with both AF and DF cooperation schemes is given follows:

DF Scheme. Using equations [9] and [10], the rates at *D* and *E* is given by

$$R_d = \frac{1}{2}\log_2(1 + P_R \alpha_{RD}) \quad [12]$$

$$R_e \aleph \frac{1}{\ddot{u}} \log_2\left(1 \quad \frac{\rho P_{\ddot{u}} \alpha}{+ \aleph P_{RJ} \quad _{RE}} \quad \frac{P_{\ddot{u}} \alpha}{+ P_{SJ} \quad _{SE}}\right) \quad [13]$$

where, $\alpha_{RD} = \frac{|h_{RD}|^2}{\sigma^2}$, $\alpha_{SE} = \frac{|h_{SE}|^2}{\sigma^2}$ and $\alpha_{RE} = \frac{|h_{RE}|^2}{\sigma^2}$. Using equations [12] and [13], the secrecy rate is given by $R_S = \max\{R_d - R_e, 0\}$, where

$$R_d - R_e = \frac{1}{2}\log_2\left(\frac{1+P_R\alpha_{RD}}{1+\frac{\rho P_S\alpha_{SE}}{1+\rho P_{RJ}\alpha_{RE}}+\frac{P_R\alpha_{RE}}{1+P_{SJ}\alpha_{SE}}}\right) \quad [14]$$

AF Scheme. Using equations [9] and [11], the rates at D and E are represented as in (Lee, 2015):

$$R_d = \frac{1}{2}\log_2(1+G^2P_S\alpha_{RD}) \quad [15]$$

$$R_e = \frac{1}{2}\log_2\left(1+\frac{\rho P_S\alpha_{SE}}{1+\rho P_{RJ}\alpha_{RE}}+\frac{G^2P_S\alpha_{RE}}{1+P_{SJ}\alpha_{SE}}\right) \quad [16]$$

The secrecy rate is given by $R_S = \max\{R_d - R_e, 0\}$, where

$$R_d - R_e = \frac{1}{2}\log_2\left(\frac{1+G^2P_S\alpha_{RD}}{1+\frac{\rho P_S\alpha_{SE}}{1+\rho P_{RJ}\alpha_{RE}}+\frac{G^2P_S\alpha_{RE}}{1+P_{SJ}\alpha_{SE}}}\right) \quad [17]$$

RESULTS AND DISCUSSION

Numerical results are presented for investigating secrecy rate of system utilizing both TS and PS EH using AF and DF relaying techniques. The performance of the system employing EH is compared with the conventional system in terms of secrecy rate. It is assumed that the source *S*, destination *D* and relay *R* and are located in a line (Sinha, & Jindal, 2016) as shown in Figure 7, where, d_{BS}, d_{BR}, d_{SR}, d_{RE} and d_{RD} show *B*-*S*, *B*-*R*, *S*-*R*, *R*-*E* and *R*-*D* distance. The distance between *E* and *S* can be represented as $d_{SE} = \sqrt{d_{SR}^2 + d_{RE}^2}$, respectively. The channel used between the nodes is the line-of-sight (LOS) channel $d^{-\frac{c}{2}}e^{j\theta}$, where *d* represents node to node distance, θ is the phase that is having uniform distribution within [0, 2π, and the path loss exponent is given by c=3.5 (Dong, Han, Petropulu, & Poor, 2010).

The performance of EH system is affected by many factors like, distance between relay and eavesdropper node, distance between relay and destination node, beacon power etc. Keeping these factors into consideration, the simulation is conducted to analyze the performance of communication system. The figure of merit of this work is secrecy rate comparison of conventional and EH-TSR, PSR system. All the nodes in experimental setup are deployed to investigate the system performance as shown in Table 1.

Table 1
Distance between communication nodes in all cases of experimental setup

Cases	Conventional and EH system					
	$\mathbf{d_{SR}}$	$\mathbf{d_{RE}}$	$\mathbf{d_{RD}}$	$\mathbf{d_{SE}}$	$\mathbf{d_{BS}}$	$\mathbf{d_{BR}}$
I	10m	15-40m	15m	18.02m-41.23m	7m	7m
II	10m	15m	5-30m	18.02m	7m	7m
III	10m	15m	15m	18.02m	7m	7m
IV	10m	15m	15m	18.02m	6-15m	6-15m

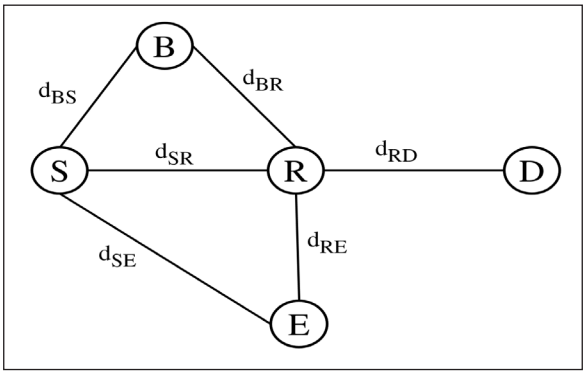

Figure 7. Simulation Model

For the conventional system, it is assumed that the system functions under the constraint of total transmit power of 30 dBm and noise power is -70 dBm. For the system with EH, it is assumed that P_B = 30 dBm, the noise power = -70 dBm and d_{BS}= d_{BR}= 7 m. Further, η =1 for both EH schemes. For TS EH scheme, it is assumed that α=0.999 and for PS EH, it is assumed that λ =0.99. Moreover, the nodes utilize equal power allocation scheme.

The conventional system and EH are investigated for both TSR and PSR protocol using AF and DF methods. To evaluate the performance of wireless system there are many parameters such as secrecy rate, throughput, secrecy outage probability (SOP), ergodic secrecy capacity (ESC) and secrecy rate used in the literature. Here, secrecy rate is considered as parameter metric as it is a measure to ensure the authentication, confidentiality and integrity during data transmission without increased complexity.

The following cases depict various simulation results:

CASE 1: Secrecy Rate versus Relay-Eavesdropper Distance

(a) For Conventional System: Figure 8.shows the plot of secrecy rate versus relay-eavesdropper distance for the conventional system using AF and DF schemes. Secrecy rate increases with increase in distance between relay and eavesdropper.
(b) For TS EH System: Figure 9.shows the plot of secrecy rate versus relay eavesdropper

distance for the system employing TS EH for AF and DF techniques. The plot indicates that with increase in distance between relay and eavesdropper, secrecy rate also increases.

(c) For PS EH System: Figure 10 shows the plot of secrecy rate versus relay-eavesdropper distance for system employing PS EH for AF and DF cooperative schemes. This plot also shows that as the eavesdropper shifts away from the relay, the transmission becomes more secure.

The numerical values for the variation in secrecy rate when the distance between the relay and eavesdropper is 40m have been observed. It is observed that secrecy rate for TS EH is 11% more but for PS EH is 44% less as compared to conventional system (without applying EH technique) with AF cooperative scheme. Further, secrecy rate for TS EH is 11% more but for PS EH is 52% less as compared to conventional system for DF cooperative scheme. The secrecy rate obtained with TS EH is 44% and 57% more as compared to PS EH in AF and DF respectively. Further, the secrecy rate obtained for the conventional physical layer security system with AF is 8.16% more as compared to system with DF.

CASE 2: Secrecy Rate versus Relay-Destination Distance

(a) For Conventional System: Figure 11 shows the plot of secrecy rate versus relay destination distance for the conventional system using AF and DF cooperative schemes. The plot shows that, with increase in the distance between relay and destination, the secrecy rate decreases.

(b) For TS EH System: Figure 12 shows the plot of secrecy rates versus relay-destination distance for the system employing TS EH. The plot indicates that secrecy rate decreases as the distance between the relay and destination increases.

(c) For PS EH System: The plot of secrecy rates versus relay-destination distance for the system employing PS EH is shown in Figure 13. The plot shows that, secrecy rate decreases with increase in distance between relay and destination.

CASE 3: Secrecy Rate versus Path Loss Exponent

(a) For Conventional System: Figure 14 represents the plot of secrecy rate versus path loss exponent for conventional system. It is indicated by the plot that with increase in the path loss exponent, channel become worse and hence the transmission becomes less secure.

(b) For TS EH System: Figure 15 represents the plot of secrecy rate with respect to path loss exponent for system employing TS EH for DF and AF cooperative schemes. The plot shows that secrecy rate decreases with increase in the path loss exponent.

(c) For PS EH System: Figure 16 shows the plot of secrecy rate with respect to path loss exponent for PS EH system. The communication becomes less secure with increase in the pass loss exponent.

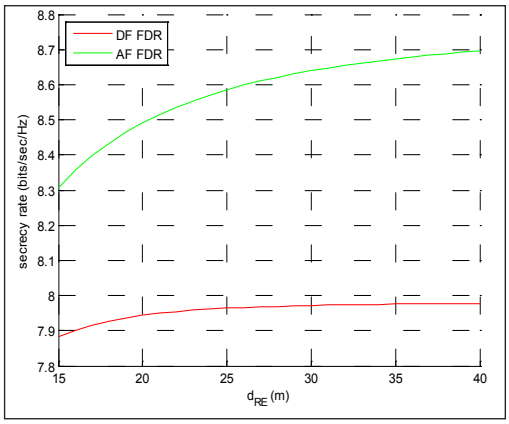

Figure 8. Secrecy rate with respect to d_{RE} for conventional system without EH, where d_{SR}= 10 m, d_{RD}= 15 m

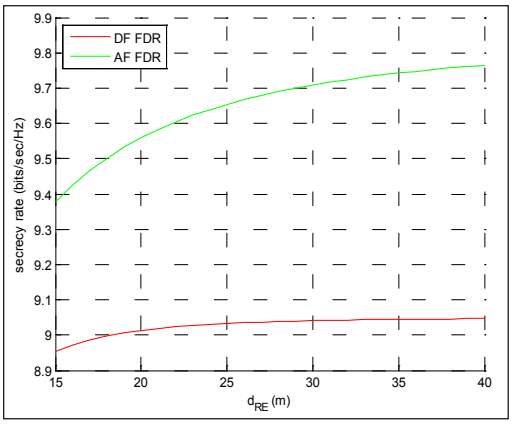

Figure 9. Secrecy rate with respect to d_{RE} for system with TS EH, where d_{SR}= 10 m, d_{RD}= 15 m, d_{BS}= 7 m and d_{BR} = 7 m

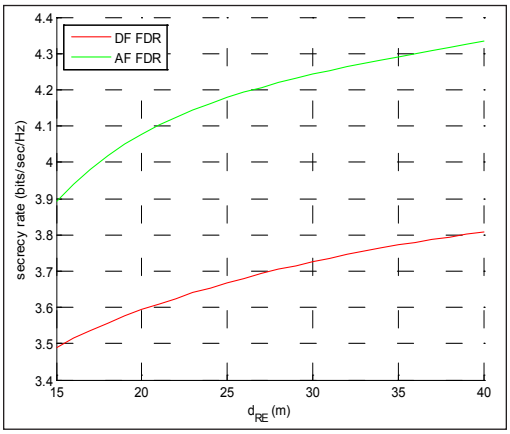

Figure 10. Secrecy rate with respect to d_{RE} for system with PS EH, where d_{SR}= 10 m, d_{RD}= 15 m, d_{BS}= 7 m and d_{BR} = 7 m

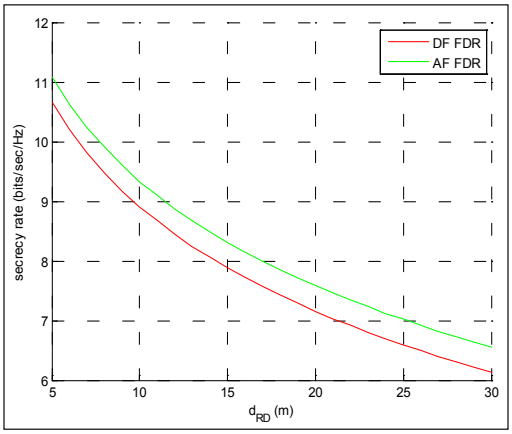

Figure 11. Secrecy rate with respect to d_{RD} for conventional system without EH, where d_{SR}= 10 m, d_{RE}= 15 m

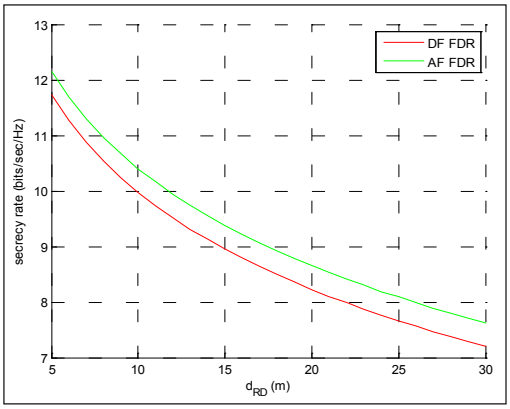

Figure 12. Secrecy rate with respect to d_{RD} for system with TS EH, where d_{SR}= 10 m, d_{RE}= 15 m d_{BS}= 7 m and d_{BR} = 7 m

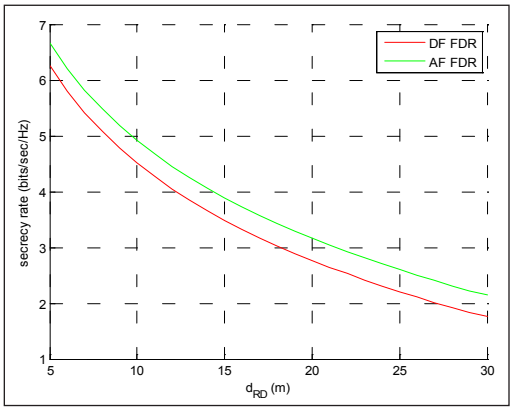

Figure 13. Secrecy rate with respect to d_{RD} for system with PS EH, where d_{SR}= 10 m, d_{RE}= 15 m d_{BS}= 7 m and d_{BR} = 7 m

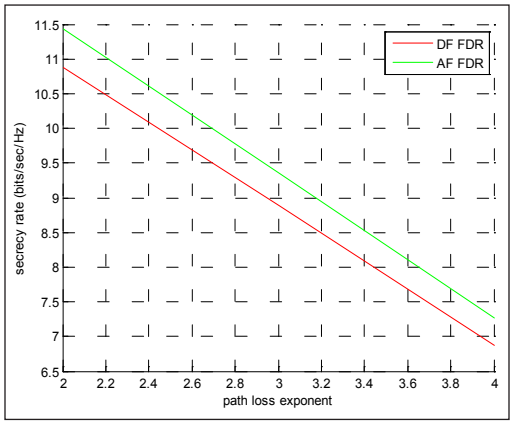

Figure 14. Secrecy rate with respect to path loss component for conventional system, where d_{SR}= 10 m, d_{RE}= 15 m, d_{RD}= 15 m

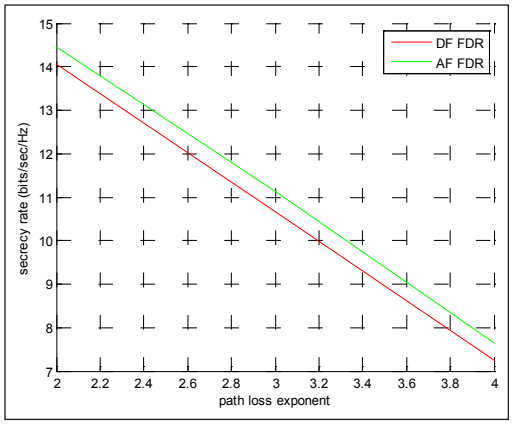

Figure 15. Secrecy rate with respect to path loss exponent for system with TS EH, where d_{SR}= 10 m, d_{RE}= 15 m, d_{RD}= 15 m, d_{BS}= 7 m and d_{BR} = 7 m

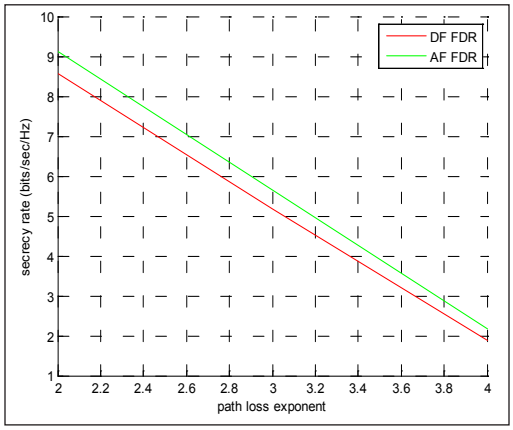

Figure 16. Secrecy rate with respect to path loss exponent for system with PS EH, where d_{SR}= 10 m, d_{RE}= 15 m, d_{RD}= 15 m, d_{BS}= 7 m and d_{BR} = 7 m

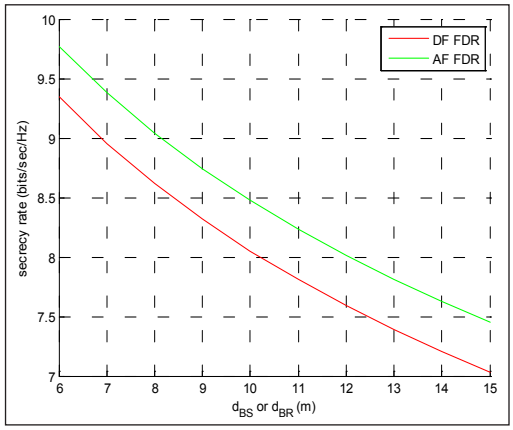

Figure 17. Secrecy rate versus d_{BS}or d_{BR} when d_{SR}= 10 m, d_{RE}= 15 m, d_{RD}= 15 m in system with TS EH

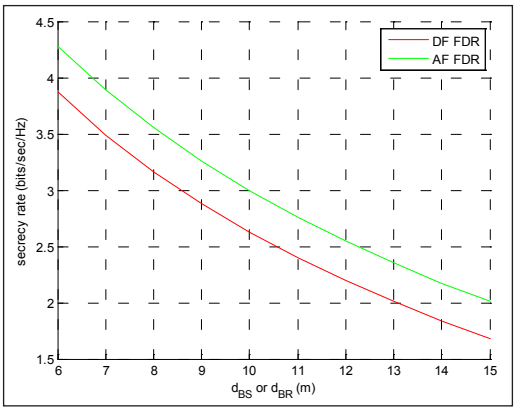

Figure 18. Secrecy rate with respect to d_{BS}or d_{BR} for system with PS EH, where d_{SR}= 10 m, d_{RE}= 15 m, d_{RD}= 15 m

CASE 4: Secrecy Rate versus Beacon Distance

(a) For TS EH System: Figure 17 shows the plot of secrecy rate versus beacon-source or beacon-relay distance in the system with TS EH. The plot shows that secrecy rate decreases as the beacon moves away from the source and relay.

(b) For PS EH System: The plot of secrecy rate versus beacon-source or beacon-relay distance in the system with PS EH is shown in Figure 18. It is represented in the plot that when the beacon moves away from source and relay, secrecy rate decreases.

All the plots clearly show that the performance of the system with TS EH is better than that of the conventional system and the performance with conventional system is better than that of the system with PS EH in the given condition. The reason is that, in case of TS EH system the whole signal strength is used by the nodes for harvesting energy and transmission of information, whereas in case of PS EH, the signal strength is divided into two parts, one for energy harvesting and the other for data transmission. Moreover, it has been observed that, in all network scenarios, the AF cooperative scheme outperforms the DF cooperative scheme.

CONCLUSION

In this paper, we have studied and presented a deep insight of the combination of three technologies; energy harvesting, physical layer security and cooperative communication. The work presented in this paper demonstrates that how energy harvesting along with providing secure communication prolonged the lifetime of energy constrained devices. We have observed the numerical values for the variation in secrecy rate when the distance between the relay and eavesdropper is 40m. It is observed that secrecy rate for TS EH is 11% more but for PS EH is 44% less as compared to conventional system (without applying EH technique) with AF cooperative scheme. Further, secrecy rate for TS EH is 11% more but for PS EH is 52% less as compared to conventional system for DF cooperative scheme. The secrecy rate obtained with TS EH is 44% and 57% more as compared to PS EH in AF and DF respectively. Further, the secrecy rate obtained for the conventional physical layer security system with AF is 8.16% more as compared to system with DF. The performance analysis presented herein may be used as reference for selecting the particular energy harvesting protocol with cooperative scheme for given applications as required. An in-depth comparative analysis of different energy harvesting protocols with physical layer security in different cooperative scenarios makes this paper different from the existing work as the existing literature does not present such an extensive comparative analysis of the problem under study.

Further, implementation of RF-EH in multi-user environment, implementations of multi relay nodes to select an efficient relay and jammer algorithms for improved system performance, implementation of multiple antennas at relay node for improving transmission efficiency, redesigning of conventional schemes and protocols to optimise power consumption in existing protocols while maintaining secrecy constraints of the cooperative network are some open research problems in the area under study.

REFERENCES

Chen, G., Gong, Y., Xiao, P., & Chambers, J. A. (2015). Physical layer network security in the full-duplex relay system. *IEEE Transactions on Information Forensics and Security*, *10*(3), 574-583.

Dong, L., Han, Z., Petropulu, A. P., & Poor, H. V. (2010). Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing*, *58*(3), 1875-1888.

Hoang, T. M., Duong, T. Q., VO, N. S., & Kundu, C. (2017). Physical layer security in cooperative energy harvesting networks with a friendly jammer. *IEEE Wireless Communications Letters*, *6*(2), 174-177.

Jindal, P., & Sinha, R. (2017, March). Physical layer security with energy harvesting in single hop wireless relaying system. In *International Conference on Information Science and Applications* (pp. 249-256). Singapore: Springer.

Kumar, N., & Bhatia, V. (2015). Performance analysis of amplify-and-forward cooperative networks with best-relay selection over Weibull fading channels. *Wireless Personal Communications*, *85*(3), 641-653.

Lee, J. H. (2015). Full-duplex relay for enhancing physical layer security in multi-hop relaying systems. *IEEE Communications Letters*, *19*(4), 525-528.

Liu, W., Zhou, X., Durrani, S., & Popovski, P. (2016). Secure communication with a wireless-powered friendly jammer. *IEEE Transactions on Wireless Communications*, *15*(1), 401-415.

Nasir, A. A., Zhou, X., Durrani, S., & Kennedy, R. A. (2013). Relaying protocols for wireless energy harvesting and information processing. *IEEE Transactions on Wireless Communications*, *12*(7), 3622-3636.

Nguyen, N. P., Duong, T. Q., Ngo, H. Q., Hadzi-Velkov, Z., & Shu, L. (2016). Secure 5G wireless communications: A joint relay selection and wireless power transfer approach. *IEEE Access*, *4*, 3349-3359.

Salem, A., Hamdi, K. A., & Rabie, K. M. (2016). Physical layer security with RF energy harvesting in AF multi-antenna relaying networks. *IEEE Transactions on Communications*, *64*(7), 3025-3038.

Sinha, R., & Jindal, P. (2016, November). Performance analysis of cooperative schemes under total transmit power constraint in single hop wireless relaying system. *2nd International Conference* in *Communication Control and Intelligent Systems (CCIS), 2016* (pp. 28-31). Mathura, India.

Wyner, A. D. (1975). The wire-tap channel. *Bell Labs Technical Journal*, *54*(8), 1355-1387.

Yuen, C., Elkashlan, M., Qian, Y., Duong, T. Q., Shu, L., & Schmidt, F. (2015). Energy harvesting communications: Part 2 [Guest Editorial]. *IEEE Communications Magazine*, *53*(6), 54-55.

Yuen, C., Elkashlan, M., Qian, Y., Duong, T. Q., Shu, L., & Schmidt, F. (2015). Energy harvesting communications: Part 1 [guest editorial]. *IEEE Communications Magazine*, *53*(4), 68-69.

Yuen, C., Elkashlan, M., Qian, Y., Duong, T. Q., Shu, L., & Schmidt, F. (2015). Energy harvesting communications: Part III [Guest Editorial]. *IEEE Communications Magazine*, *53*(8), 90-91.

Zhang, C., & Chen, Y. (2017). Wireless Power Transfer Strategies for Cooperative Relay System to Maximize Information Throughput. *IEEE Access*, *5*, 2573-2582.

Zhang, R., & Ho, C. K. (2013). MIMO broadcasting for simultaneous wireless information and power transfer. *IEEE Transactions on Wireless Communications*, *12*(5), 1989-2001.

Son, P. N., & Kong, H. Y. (2015). Cooperative communication with energy-harvesting relays under physical layer security. *IET Communications*, *9*(17), 2131-2139.

Wu, W., Wang, B., Deng, Z., & Zhang, H. (2017). Secure beamforming for full-duplex wireless powered communication systems with self-energy recycling. *IEEE Wireless Communication Letters, 6*(2), 146-149.