A Study of Physical Layer Security with Energy Harvesting in Single Hop Relaying Environment

Rupali Sinha
Dept. of Electronics and Communication
National Institute of Technology
Kurukshetra, India
rupalisinha468@gmail.com

Poonam Jindal
Dept. of Electronics and Communication
National Institute of Technology
Kurukshetra, India
poonamjindal81@nitkkr.nic.in

***Abstract*— This paper investigates the secrecy performance of single hop relaying network with Energy Harvesting (EH) and also shows that the system with EH outperforms the conventional system in terms of secrecy rate and energy efficiency. In the proposed system, the source transmits the information signal to the destination via a relay in the presence of an eavesdropper and the source and relay utilizes time switching EH technique to obtain power from a power beacon. This paper compares the secrecy rate of two cooperative schemes: decode-and-forward (DF), and amplify-and-forward (AF) for both proposed system with EH and the conventional system. The system with EH provides higher secrecy rate than that of the conventional system by 30.47 % for DF cooperative scheme and by 23.63 % for AF relay at a distance of 40 m between the eavesdropper and the relay. The resulting analysis also shows that the secrecy rate of the AF relay is higher than that of the DF relay in both considered system with EH and conventional system.**

Keywords—Energy harvesting; full duplex relay; jamming; physical layer security; secrecy rate

I. INTRODUCTION

Transmission of information is not secure in wireless environment due to its broadcast nature. Physical layer security (PLS) helps in providing secure communication by exploiting the physical characteristics of the wireless medium [1]. Various relaying techniques are there to enhance PLS, and among these, two are most commonly used: DF and AF [2]. In conventional networks, the nodes are powered up by placing individual batteries inside them. However, in some cases, it is not favorable to replace or recharge those batteries [3]. This issue can be solved by EH technique [4]-[6]. It also helps in providing benefits to reliability and low maintenance monitoring. Also, as the there is increase in number of communicating devices, it is required to move in favor of energy efficient systems. Hence, EH protocols [7] e.g. time switching based relaying protocol (TSR) and power splitting based relaying (PSR) protocol is gaining attention nowadays.

This paper investigates the secrecy performance of a single hop relaying system with energy harvesting, in which a power beacon provides power to source and relay to perform their respective roles. It is also assumed that self interference is perfectly canceled at each node. The secrecy rate of this system is analyzed for both AF and DF relaying schemes.

The rest of this paper is organized as follows. Section II shows system model considered in this work and explains EH protocol used in this paper. Section III describes the expressions of secrecy rate that can be achieved. Section IV gives the numerical results. The paper is concluded in section V.

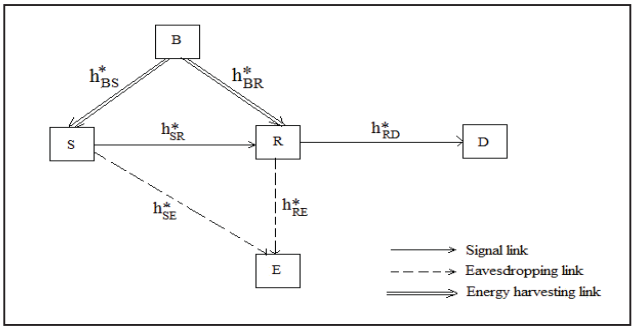

Fig. 1. Proposed relaying system utilizing EH.

II. SYSTEM MODEL

The system model is shown in Fig. 1. It consists of a power beacon *B*, a source *S*, a relay *R*, a destination *D*, and an eavesdropper *E*. Let h^*_{BS}, h^*_{BR}, h^*_{SR}, h^*_{RD}, h^*_{SE} and h^*_{RE} indicate complex channel gains from *B* to *S*, from *B* to *R*, from *S* to *R*, from *R* to *D*, from *S* to *E* and from *R* to *E*, respectively. At each node, the noise is assumed to be complex additive white guassian noise (AWGN) with variance σ^2 and mean zero. Further, the relay utilizes both full and half duplex operation [8] in this system.

A. Energy Harvesting Technique

In this proposed system, *R* and *S* harvests energy from *B* and use this energy for signal transmission. In this paper, the time switching based EH protocol is employed due to its high throughput as shown in Fig. 2. The expressions representing harvested energy at *S* and *R*, respectively are [9]

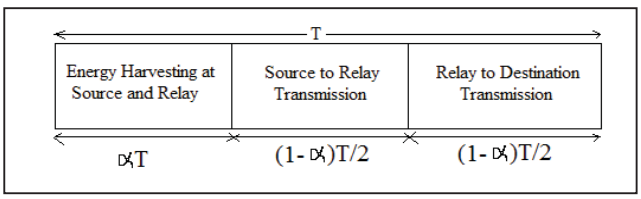

Fig. 2. Time Switching Based Relaying Protocol [7].

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

$$E_R = \eta P_B \alpha T \left| h_{BR}^* \right|^2 . \quad (2)$$

where, the efficiency of this technique of energy conversion is given by $0 < \eta < 1$, the power sent by beacon node is given by P_B and $0 < \alpha < 1$. T represents time duration to transmit a particular block from S to D. Nodes S and R harvest energy from B for time period of αT. Power transmitted by S and R in this proposed system are represented by [9]

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

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

1) DF Scheme: It does its work in two steps. The first step is shown in Fig. 3, where the source sends the signal $x(n)$ to the relay. The relay provides jamming signal $q(2n)$ to the eavesdropper, at the same instant. The signals obtained at nodes R and E, in the time slot 2n are given by [10]

$$y_R(2n) = \sqrt{P_S} h_{SR}^* x(n) + n_R(2n),$$
$$y_E(2n) = \sqrt{P_S} h_{SE}^* x(n) + \sqrt{P_{RJ}} h_{RE}^* q(2n) + n_E(2n) , \quad (5)$$

where, the jamming signal power of R is given by P_{RJ} and AWGN at R and E are represented by $n_R(2n)$ and $n_E(2n)$, respectively.

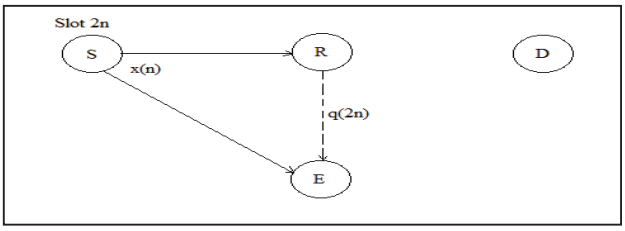

Fig. 3. Illustration of the signals sent in the 2nth time slot.

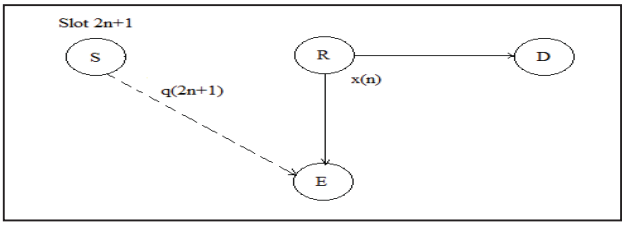

Fig. 4. Illustration of the signals sent in the (2n+1)th time slot.

The second step is shown in the Fig. 4, where the relay sends the previously decoded signal to the destination. Further, in this step, source sends jamming signal to the eavesdropper. The signals obtained at E and D in the time slot (2n+1) are denoted as [10]

$$y_E(2n+1) = \sqrt{P_R} h_{RE}^* x(n) + \sqrt{P_{SJ}} h_{SE}^* q(2n+1) + n_E(2n+1),$$
$$y_D(2n+1) = \sqrt{P_R} h_{RD}^* x(n) + n_D(2n+1), \quad (6)$$

where, the power of the jamming signal of S is represented by P_{SJ} and $n_D(2n+1)$ represents the AWGN at D.

2) AF Scheme: It also has two stages, similar to DF technique. The first step is same like the DF technique as shown in Fig. 3. The signals obtained at nodes R and E in the first time slot 2n are given by (5).

The second stage involves amplification of the received signal by the source and forwarding of this amplified signal to the destination. Also, jamming signal is sent by the source to the eavesdropper as shown in Fig. 4. The signals obtained at D and E in the (2n+1)th time slot can be given as [11]

$$y_D(2n+1) = G\sqrt{P_S}\, h_{RD}^*\, y_R(2n) + n_D(2n+1),$$
$$y_E(2n+1) = G\sqrt{P_S}\, h_{RE}^*\, y_R(2n) + \sqrt{P_{SJ}} h_{SE}^* q(2n+1) + n_E(2n+1), \quad (7)$$

where, the scaling factor is given by $G = \frac{1}{\sqrt{P_S \left| h_{SR} \right|^2 + N_o}}$ [11] and the variance of noise is denoted by N_o.

III. Achievable Secrecy Rate

A. DF Sheme

Using (5) and (6), the rates at D and E is given by [10]

$$R_d = \frac{1}{2}\log_2(1 + P_R \alpha_{RD}) \quad (8)$$

$$R_e = \frac{1}{2}\log_2\left(1 + \frac{P_S \alpha_{SE}}{1 + P_{RJ}\alpha_{RE}} + \frac{P_R \alpha_{RE}}{1 + P_{SJ}\alpha_{SE}}\right) \quad (9)$$

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 (8) and (9), the secrecy rate that can be achieved is represented as $R_S = \max\{R_d - R_e, 0\}$, where

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

(10)

B. AF Scheme

Utilizing (5) and (7), At D and E, the rates can be represented as [10]

$$R_d = \frac{1}{2}\log_2(1 + G^2 P_S \alpha_{RD}) \quad (11)$$

$$R_e = \frac{1}{2}\log_2\left(1 + \frac{P_S \alpha_{SE}}{1 + P_{RJ}\alpha_{RE}} + \frac{G^2 P_S \alpha_{RE}}{1 + P_{SJ}\alpha_{SE}}\right). \quad (12)$$

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

$$R_d - R_e = \frac{1}{2}\log_2\left(\frac{1+G^2P_S\alpha_{RD}}{1+\frac{P_S\alpha_{SE}}{1+P_{RJ}\alpha_{RE}}+\frac{G^2P_S\alpha_{RE}}{1+P_{SJ}\alpha_{SE}}}\right) \quad (13)$$

IV. Numerical Evaluation

In this section, numerical results are presented to investigate secrecy rate of the proposed system utilizing EH for both DF and AF relaying schemes. It is considered that the source S, relay R and destination D are located in a line [2] as shown in Fig. 5, where, d_{BS}, d_{BR}, d_{SR} , d_{RE} and d_{RD} show the distance between B and S, between B and R, between S and R, between R and E and between R and D. The distance between E and S can be represented as $d_{SE} = \sqrt{d_{SR}^2 + d_{RE}^2}$, respectively. The channel used is the line-of-sight (LOS) channel model $d^{-\frac{c}{2}}e^{j\theta}$, where d is the distance between the nodes, θ denotes the random phase that is having uniform distribution within $[0, 2\pi)$, and $c = 3.5$ gives the path loss exponent [2].

It is assumed that P_B = 30 dBm, the noise power = -40 dBm and $d_{BS} = d_{BR}$= 7 m. Further, $\alpha = 0.999$ and $\eta = 0.9$.

Fig. 6. and 7. shows the variation of secrecy rates of AF and DF cooperative schemes with the distance between eavesdropper and relay, d_{RE} when $d_{BS} = d_{BR}$ = 7 m, d_{SR} = 10 m, d_{RD} = 15 m in the considered system utilizing EH and in the conventional system without EH. As there is an increase in d_{RE}, the secrecy rate also increases for both DF and AF cooperative schemes.

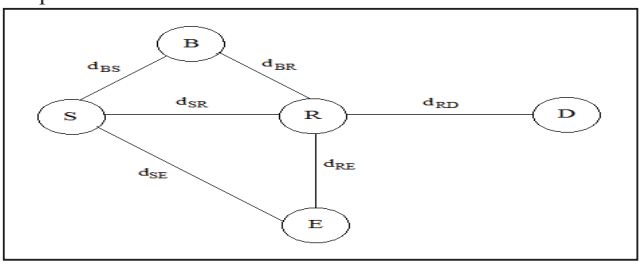

Fig. 5. Illustration of the proposed EH simulation model.

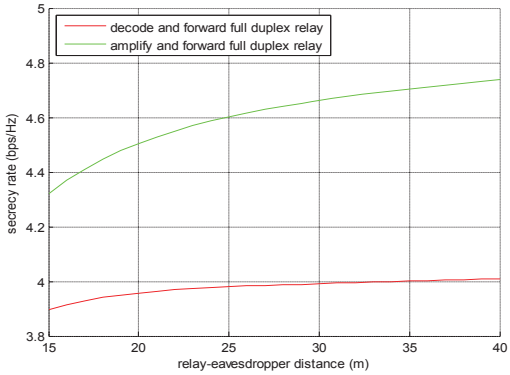

Fig. 6. Secrecy rate versus d_{RE} when d_{SR} = 10 m, d_{RD} = 15 m, d_{BS} = 7 m and d_{BR} = 7 m in proposed system with EH.

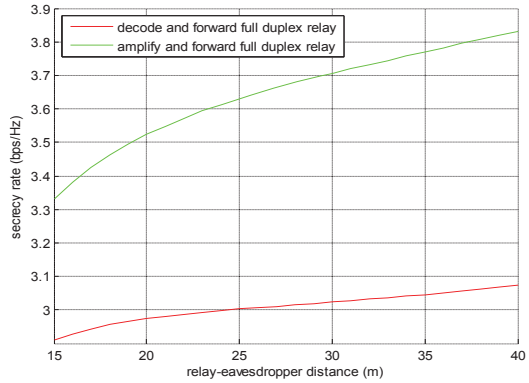

Fig. 7. Secrecy rate versus d_{RE} when d_{SR} = 10 m, d_{RD} = 15 m in the conventional system without EH.

Fig. 8. and 9. represents the plot between secrecy rate and relay-destination distance d_{RD} when $d_{SR} = 10$ m, $d_{RE} = 15$ m in the proposed system with EH and in the conventional system without EH for AF and DF relaying technique. As the distance between R and D, there is decrease in secrecy rate in both cooperative techniques.

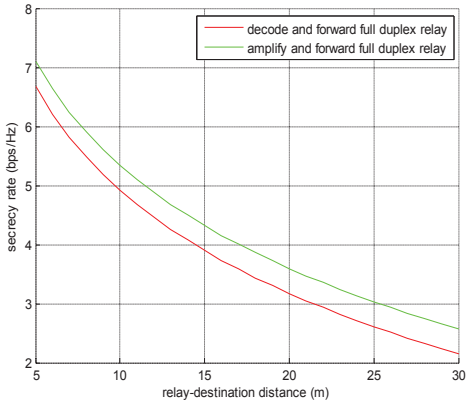

Fig. 8. Secrecy rate versus d_{RD} when d_{SR} = 10 m, d_{RE} = 15 m, d_{BS} = 7 m and d_{BR} = 7 m in proposed system with EH.

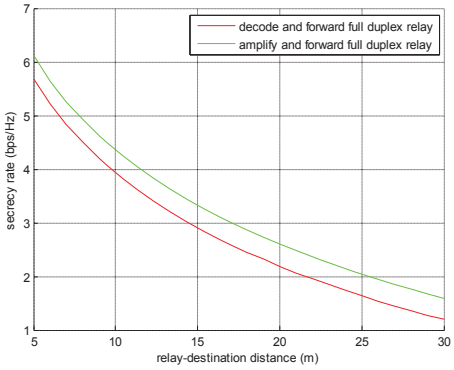

Fig. 9. Secrecy rate versus d_{RD} when d_{SR} = 10 m, d_{RE} = 15 m in the conventional system without EH.

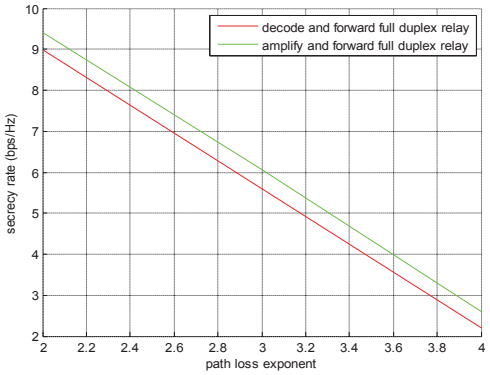

Fig. 10. Secrecy rate versus path loss exponent when d_{SR} = 10 m, d_{RE} = 15 m, d_{RD} = 15 m, d_{BS} = 7 m and d_{BR} = 7 m in proposed system with EH.

Fig. 10. shows the plot of secrecy rate versus path loss exponent when $d_{SR} = 10$ m, $d_{RE} = 15$ m, d_{RD} = 15 m and $d_{BS} = d_{BR}$ = 7 m in the proposed system. With the increase in the path loss exponent, the degradation of the medium also increases and therefore, secrecy rate decreases.

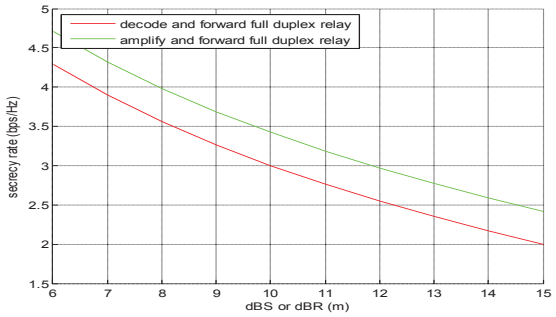

Fig. 11. Secrecy rate versus d_{BS} or d_{BR} when d_{SR} = 10 m, d_{RE} = 15 m, d_{RD} = 15 m in proposed system with EH

Fig. 11. shows the plot of secrecy rate versus beacon-source or beacon-relay distance i.e. d_{BS} or d_{BR}, when $d_{SR} = 10$ m, $d_{RE} = 15$ m, d_{RD} = 15 m and in the proposed system. As the distance between the beacon and the source or relay increases, secrecy rate also decreases.

V. Conclusion

This paper proposes a single hop network, in which relay and source get energy from a node known as power beacon with the help of time switching EH scheme. The secrecy rate of the considered system is analyzed for two relaying schemes: DF and AF. The proposed system utilizing EH scheme provides greater energy efficiency and secrecy rate as compared to the conventional system. The system with EH provides higher secrecy rate than that of the conventional system by 30.47 % for DF cooperative scheme and by 23.63 % for AF relay at a distance of 40 m between the eavesdropper and the relay. The resulting analysis indicates that the performance of AF scheme is better than that of the DF scheme in terms of secrecy rate. Also, it is shown that when the path loss exponent of the channel increases i.e. as the channel becomes worse, the transmission of information becomes less secure.

References

[1] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, Oct. 1955.

[2] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[3] R. Zhang and C. K. Ho, "MIMO broadcasting for simulations wireless information and power transfer," IEEE Trans. Wireless Commun., vol. 12, no. 5, pp. 1989-2001, May 2013.

[4] C. Yuen, M. Elkashlan, Y. Qian, T. Q. Duong, L. Shu, and F. Schmidt, "Energy harvesting communications: Part 1 [Guest Editorial]," IEEE Commun. Mag., vol. 53, no. 4, pp. 68-69, Apr. 2015.

[5] C. Yuen, M. Elkashlan, Y. Qian, T. Q. Duong, L. Shu, and F. Schmidt, "Energy harvesting communications: Part 2 [Guest Editorial]," IEEE Commun. Mag., vol. 53, no. 6, pp. 54-55, Jun. 2015.

[6] C. Yuen, M. Elkashlan, Y. Qian, T. Q. Duong, L. Shu, and F. Schmidt, "Energy harvesting communications: Part III [Guest Editorial]," IEEE Commun. Mag., vol. 53, no. 8, pp. 90-91, Aug. 2015.

[7] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying Protocols for wireless energy harvesting and information processing," IEEE Trans. Wireless Commun., vol. 12, no. 7, pp. 3622-3636, Jul. 2013.

[8] G. Chen, Y. Gong, P. Xiao and J. A. Chambers, "Physical layer network security in the full–duplex relay system," IEEE Trans. Inf. Forensics security, vol. 10, no. 3, pp. 574-583, Mar. 2015.

[9] N. P. Ngyuyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, L. Shu, "Secure 5G wireless communications: A joint relay selection and wireless power transfer approach," IEEE access, vol. 4, pp. 3349-3359, 2016.

[10] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," IEEE Commun. Lett., vol. 19, no. 4, pp. 525-528, Apr. 2015.

[11] N. Kumar and V. Bhatia, "Performance analysis of amplify-and-forward cooperative networks with best-relay selection over weibull fading channels," Springer Wireless Pers. Commun (2015) 85 : 641-653.