URSI AP-RASC 2019, New Delhi, India, 09 - 15 March 2019

Physical Layer Security under Accumulated Harvested Energy from RF Source

Shashibhushan Sharma*, Sanjay Dhar Roy, and Sumit Kundu
Dept. of ECE, NIT Durgapur, West Bengal, India
ss.15ec1105@phd.nitdgp.ac.in, s_dharroy@yahoo.com, sumitkundu@yahoo.com

Abstract

In this paper, we have studied the accumulation of harvested energy, at decode and forward (DF) relays over several frames, which is used by the relays to forward the signal in a particular frame in presence of a passive eavesdropper. The source broadcasts the information signal to DF relays in the broadcasting phase. Each relay is assisted with two omnidirectional antennas, while the source and the destination is assisted with a single omnidirectional antenna. The selected relay uses the signal received from one antenna to harvest energy, while it uses the received signal from another antenna to decode the message. At the relay, the harvested energy in each frame of communication might not be sufficient to forward the signal, which requires accumulation of energy. The accumulated energy over several frames becomes sufficient to forward the signal to the destination in a particular frame through a single antenna in the relaying phase, while the eavesdropper tries to eavesdrop the relayed information signal. We evaluate the secrecy outage probability in the proposed network to secure the information signal at the physical layer when the selected relay transmits using accumulated harvested energy. The secrecy performance increases with an increase in transmit power of the source, and the number of the frames used for energy accumulation. A closed-form expression on secrecy outage probability under accumulation of harvested energy is developed which is verified by MATLAB based simulation.

1. Introduction

Due to broadcast nature of the wireless channel by omnidirectional antenna, the information signal is easily received by a suspicious user (termed as eavesdropper) which can eavesdrop the message. Conventional approach of maintaining secrecy involves cryptography which requires complex key exchange and computational complexity. In contrast, secrecy can be maintained at physical layer as demonstrated by Wyner in his pioneer work on wire-tap channel [1]. The physical layer secrecy (PLS) can be measured in terms of the secrecy capacity (SC), which is a difference between legitimate channel capacity and wire-tap channel capacity [2]. The higher value of SC indicates a higher level of secrecy. Further, Secrecy outage probability (SOP) is also used as a metric for characterizing confidentiality of the message which is defined as the probability of secrecy capacity falling below a threshold called a threshold secrecy rate [3].

Cooperative jamming [4] is a promising approach to secure the confidential message. In [4], the destination assisted jamming has been considered to jam the untrusted amplify and forward relays, and the performance of secrecy in terms of ergodic secrecy capacity has been evaluated. In [5], source and destination assisted jamming has been considered to jam the EAV. The authors have evaluated the secrecy rate to observe the performance.

Harvesting of energy from RF signal and ambient sources such as radio frequency (RF) energy, solar energy, and wind energy is utilized to supplement energy to energy constrained wireless nodes [6].

The energy harvester can operate over a large range of frequency and harvest the energy from RF sources [7]. In the energy harvesting from RF energy source, two techniques of energy harvesting are mainly used to harvest the energy, one is power splitting (PS) scheme, and the other is time switching (TS) scheme [7]. It has been observed that the better transformation of energy and information is achieved by the PS scheme as compared to TS scheme [7]. In [8], the authors have analyzed the secrecy performance in terms of the SOP and the ergodic secrecy rate with PS and TS scheme based energy harvesting. Further, in [8], the authors demonstrate that the PS scheme based energy harvesting system provides better secrecy than the TS scheme based energy harvesting.

In the present paper, we analyze the secrecy performance of an energy harvesting relay network. The relay over a single frame of communication may not harvest energy sufficient to transmit the signal. Here, the frame is described as the very small interval of time of communication between the source and the destination. The relay harvests energy from RF source in a single frame, which is very small. Thus, we consider the accumulation of energy over multiple frames. In our proposed model, the relays accumulate the harvested energy in each frame of communication and store in the storage battery. Next, selected relay uses the accumulated harvested energy to forward the information signal to the destination. In the absence of sufficient accumulated energy, the relay carries out communication utilizing energy from other sources such as solar energy, wind energy, and grid supply. The secrecy performance has been analyzed when relay uses the accumulated harvested energy from RF source. The contributions of this work are given below as:

- Energy accumulated through harvesting from RF signal over a number of frames of communication is evaluated.
- An optimal value of the fraction of accumulated power, which is utilize for transmitting information, is investigated at which the SOP is minimum.
- A closed-form expression of the SOP is developed.
- MATLAB based simulation is used to validate our analytical results.

The paper is organized as follow. The system model is described in Section II. The SOP has been evaluated in Section III. The numerical results are described in Section IV, and conclusion is drawn in Section V.

2. System Model

A. Design of System Model and Channel Model

We consider a system model in which the source (S) communicates with the destination (D) via multiple N half-duplex decode and forward (DF) relays (Rs). An eavesdropper (EAV) wants to eavesdrop the message from the information signal that is forwarded by a selected relay (say i^{th} relay (R_i), where $i = 1, 2, 3, ..., N$ and N is the number of relay). The source and the destination are assisted with a single omnidirectional antenna, while all the relays are individually assisted with two antennas. At the relays, the received signal from one antenna is used to accumulate the energy, while that from the other antenna is used to decode the message. The destination and the EAV do not receive the signal directly from the source due to severe fading and shadowing. Thus, communication completes in two-time slots. The first time slot is known as the broadcasting phase, and the other is known as the relaying phase. All relays harvest the energy in the broadcasting phase following PS scheme. Energy is accumulated in storage battery over several frames of communication. Here, the frame is described as the fixed small time slot of communication between the S and D. The accumulated energy from the RF sources is used to forward the signals in relaying phase with a single antenna only.

In the proposed system model, the channel coefficient of links from the S to the first antenna of the R_i, the S to the second antenna of the R_i, the first antenna of the R_i to the D, the second antenna of the R_i to the D, the first antenna of the R_i to the EAV, and the second antenna of the R_i to the EAV are represented by $h_{SR_{i1}}$, $h_{SR_{i2}}$, $h_{R_{i1}D}$, $h_{R_{i2}D}$, $h_{R_{i1}E}$ and $h_{R_{i2}E}$, respectively, which are assumed to be Rayleigh faded. The channel gains of these links are represented by $\phi_{SR_{i1}}$, $\phi_{SR_{i2}}$, $\phi_{R_{i1}D}$, $\phi_{R_{i2}D}$, $\phi_{R_{i1}E}$ and $\phi_{R_{i2}E}$, respectively, which follow the exponential distribution. Further, the mean channel gains of the links are indicated as, $\Omega_{SR_{i1}}$, $\Omega_{SR_{i2}}$, $\Omega_{R_{i1}D}$, $\Omega_{R_{i2}D}$, $\Omega_{R_{i1}E}$ and $\Omega_{R_{i2}E}$, respectively. The channel noise is additive white Gaussian noise (AWGN) with noise power of N_0.

We assume that the channel state information (CSI) is available at the relays and the destination. We also assume that the all channel are independent and identically distributed (i.i.d.) random variables.

In the relaying phase, the relay uses a part of the available energy at the relay to forward the information signal [9] and remaining power is used by the relay to transmit the jamming signal. The destination knows the jamming signal and also the CSI. On the basis of these knowledges, the destination is able to detect the jamming signal and cancel the same from the received signal. The remaining signal is used by the destination to extract the message.

B. Energy Harvesting

The received signal at the i^{th} relay can be expressed as:

$$y_{R_{i1}} = \sqrt{P_S} h_{SR_{i1}} x_S + n_R ; y_{R_{i2}} = \sqrt{P_S} h_{SR_{i2}} x_S + n_R, \quad (1)$$

where $y_{R_{i1}}$ and $y_{R_{i2}}$ are the received signal at the i^{th} relay through the antenna one and two, respectively. The additive white Gaussian noise (AWGN) at the relay is n_R, which has a power N_0. The x_S is the message signal of the source with unit power. The P_S is the transmit power of source. The received signal through the first antenna is used to harvest the energy. All relays harvest energy in broadcasting phase using PS scheme. The harvested energy following PS scheme in one frame can be expressed as [7, 8]:

$$E_{H_i} = \eta P_S \phi_{SR_{i1}} \tfrac{T}{2}, \quad (2)$$

where E_{H_i} is the harvested energy in broadcasting phase in a single frame, T is the total communication time between the S and the D, P_S is the transmit power of the source, and the η is the energy conversion efficiency of the energy harvester circuit. The selected relay uses the harvested energy in a particular frame (say the M^{th} frame) after accumulation of energy. Next, the accumulated harvesting energy up to M^{th} frame is expressed as:

$$E_{H_i} = \eta P_S \tfrac{T}{2} \sum_{j=1}^{M} \phi_{SR_{i1j}}, \quad (3)$$

where $\phi_{SR_{i1j}}$ is the channel gain between the source and the first antenna of the R_i in j^{th} frame, and M is the number of frames. Further, the used power in the relaying phase can be expressed as:

$$P_{H_i} = \frac{\eta P_S \tfrac{T}{2} \sum_{j=1}^{M} \phi_{SR_{i1j}}}{\tfrac{T}{2}} = \eta P_S X, \quad (4)$$

where $X = \sum_{j=1}^{M} \phi_{SR_{i1j}}$.

C. Channel capacities of main link and the EAV link, and the secrecy capacity and Relay Selection

The SNR at the relay in broadcasting phase from Eq. (1) is expressed as:

$$\gamma_{SR_i} = \frac{P_S \phi_{SR_{i2}}}{N_0}, \quad (5)$$

The selected i^{th} relay uses a fraction α $(0 < \alpha \leq 1)$ of power available at the relay to forward the information signal and remaining part of the available power is used to broadcast the jamming signal which is known at the destination. The selected i^{th} relay forwards the encoded information signal to the destination together with jamming signal using the second antenna which are also over hered by the EAV. The received signal at the destination and the EAV can be expressed as:

$$\left.\begin{aligned} y_{D_i} &= \sqrt{\alpha P_{H_i}} h_{R_{i2}D} x_R + \sqrt{(1-\alpha) P_{H_i}} h_{R_{i2}D} x_J + n_D; \\ y_{E_i} &= \sqrt{\alpha P_{H_i}} h_{R_{i2}E} x_R + \sqrt{(1-\alpha) P_{H_i}} h_{R_{i2}E} x_J + n_E \end{aligned}\right\}, \quad (6)$$

where y_{D_i} and y_{E_i} are the received signal at the destination and the EAV, respectively from the R_i. The n_D and n_E are the AWGN with power N_0. The destination easily catches the jamming signal and eliminates from the received signal on basis of the prior knowledge of jamming signal and CSI [8, 9]. The SNR at the D and SINR at the EAV can be expressed as:

$$\gamma_{D_i} = \frac{\alpha P_{H_i} \phi_{R_{i2}D}}{N_0}; \gamma_{E_i} = \frac{\alpha P_{H_i} \phi_{R_{i2}E}}{(1-\alpha) P_{H_i} \phi_{R_{i2}E} + N_0}, \quad (7)$$

where γ_{D_i} and γ_{E_i} are the SNR at the D and SINR at the EAV, respectively. As per DF relay scheme, the end-to-end SNR can be expressed as:

$$\gamma_{SD} = \min\left(\frac{P_S \phi_{SR_{i2}}}{N_0}, \frac{\alpha P_{H_i} \phi_{R_{i2}D}}{N_0} \right). \quad (8)$$

The SNR at the EAV can be approximated as [9]:

$$\gamma_{E_i} = \frac{\alpha}{(1-\alpha) + \frac{N_0}{P_{H_i} \phi_{R_{i2}E}}} \approx \frac{\alpha}{(1-\alpha)}, \quad (9)$$

From Eq. (9), we observe that the average SINR at the EAV is almost constant.

The channel capacity of the main link and EAV link are expressed as:

$$C_{SD} = \tfrac{1}{2} \log_2 (1+\gamma_{SD}); C_{R_iE} = \tfrac{1}{2} \log_2 (1+\gamma_{R_iE}), \quad (10)$$

where C_{SD} and C_{R_iE} are the main and EAV channel capacity, respectively. The positive difference between main channel capacity and EAV channel capacity is known as the secrecy capacity [2]. The secrecy capacity can be expressed as:

$$C_{SD_i}^{\text{Sec}} = \left[\frac{1}{2} \log_2 \left(\frac{1+\gamma_{SD}}{1+\gamma_{R_iE}} \right) \right]^+, \quad (11)$$

where $[x]^+ = \max(0, x)$, and $C_{SD_i}^{\text{Sec}}$ is the secrecy capacity through the R_i.

The criteria of selecting the relay is to maximize the secrecy capacity. Thus, the i^{th} relay, i.e. R_i, is selected which satisfies the following equation:

$$i^* = \arg\max_{1 \leq i \leq N} \left(C_{SD_i}^{\text{Sec}} \right) \quad (13)$$

3. Performance Analysis

The SOP through a multiple half-duplex DF relays can be expressed as:

$$P_{OUT}^{\text{Sec}} = P\left(\max_{1 \leq i \leq N} C_{SD_i}^{\text{Sec}} < R_{TH}^{\text{Sec}} \right), \quad (14)$$

where P_{OUT}^{Sec} is the SOP of the relay network and R_{TH}^{Sec} is the target secrecy rate. The Eq. (14) can be re-expressed as:

$$P_{OUT}^{\text{Sec}} = \left[\underbrace{P\left(C_{SD_i}^{\text{Sec}} < R_{TH}^{\text{Sec}} \right)}_{I} \right]^N, \quad (15)$$

The term I can be expressed as:

$$I = P\left(C_{SD_i}^{\text{Sec}} < R_{TH}^{\text{Sec}} \right) = P(\gamma_{SD} < \delta), \quad (16)$$

where $\delta = 2^{2R_{TH}^{\text{Sec}}} (1+\gamma_{E_i}) - 1$, which is a constant. After some simplification, we obtain the closed-form expression of the term I as:

$$I = 1 - \frac{2\sqrt{(\Phi)^M} K_M \left(2\sqrt{\Phi} \right)}{\Gamma(M) \Omega_{R_{i2}D}} \exp\left(\frac{-\delta N_0}{P_S \Omega_{SR_{i2}}} \right), \quad (17)$$

where $K_M(*)$ is the modified Bessel function of second kind with the order M. Here, number of frame is the order of the Bessel function. Finally, we obtain the closed-form expression of the SOP as:

$$P_{OUT}^{\text{Sec}} = \left[1 - \frac{2\sqrt{(\Phi)^M} K_M \left(2\sqrt{\Phi} \right)}{\Gamma(M) \Omega_{R_{i2}D}} \exp\left(\frac{-\delta N_0}{P_S \Omega_{SR_{i2}}} \right) \right]^N. \quad (18)$$

The detail derivation of the expression (17) is avoided due to space limitation.

4. Numerical Results

We consider the following numerical values for the parameters as mean channel gains $\Omega_{SR_{i1}} = \Omega_{SR_{i2}} = \Omega_{R_{i1}D} = \Omega_{R_{i2}D} = \Omega_{R_{i1}E} = \Omega_{R_{i2}E} = 0.125$, AWGN power $N_0 = 10^{-2}$, target secrecy rate R_{TH}^{Sec} = 0.5, 0.75, 1, 1.5 bit/s/Hz. For Fig. 3 and Fig. 5, R_{TH}^{Sec} =1 bit/s/Hz. The transmit power of source (P_S) are considered as 0, 5, 10, and 15 dBW. Number of relays (N) is 5. The energy conversion efficiency (η) is considered as 0.5, and harvested power (α) is fixed at an optimal value of 0.35 as obtained in Fig. 1.

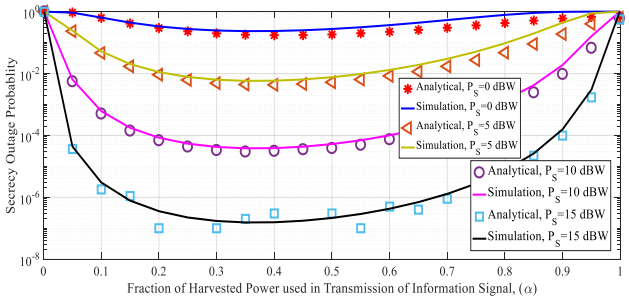

Fig. 1 The SOP vs. fraction of harvested power (α) used in transmission of information signal for different values of transmitting power of source and M =20.

In Fig. 1, the plot of the SOP vs. α has been shown. In this Figure we have consider the number of frame is 20, i.e., M =20. The transmit power of the source spent for transmission of information signal increases as α increase. In this figure, an optimal value of α =0.35, at which the minimum SOP is obtained. Before the optimal value, the increase in transmit power increases the signal strength at the destination, while at the EAV signal strength does not increase with high rate due to jamming effect before the optimal value as per Eq. (9). Thus, the secrecy capacity increases and corresponding the SOP decreases. The decrease in the SOP increases the secrecy performance. On the other side of the optimal value, the signal strength at the destination increases with the same rate as before the optimal value, but the signal strength at the EAV increases with high rate due to the decrease in jamming power. Thus, secrecy capacity decreases and the SOP increases after the optimal value. The increase in the SOP decreases the secrecy performance.

We have also seen that for at any value of α, the SOP decreases when transmit power of the source increases.

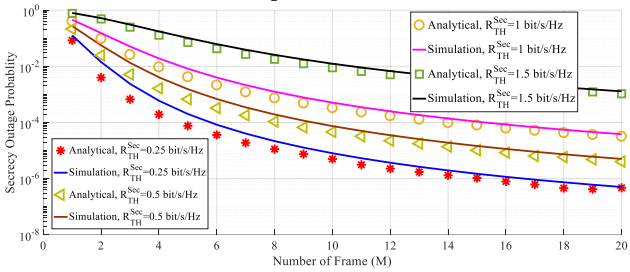

Fig. 2 The SOP vs. number of frame (M) for different value of target secrecy rate.

In Fig. 2, the variation of SOP vs. M has been shown. We have seen that the accumulated harvested energy increases as per Eq. (3) with an increase in a number of frames. Correspondingly more the accumulated harvested energy, more the power which can be used by the selected relay to transmit the information signal as well as jamming signal for a given value of α. For a given value of α the SINR at the EAV becomes almost constant. Thus, the EAV channel capacity becomes also constant. But, the increase in transmit power of the selected relay, due to an increase in accumulated harvested energy, increases the signal strength at the destination. The increment in signal strength increases the secrecy capacity, which decreases the SOP and the secrecy performance improves.

5. Conclusion

We have investigated the secrecy performance of an energy harvesting relays network in terms of the SOP in a particular frame of communication. Accumulation of energy through harvesting from RF signal over several frames is considered. We observe that the accumulation of harvested energy improves the secrecy performance significantly, while harvesting over a single frame may not be sufficient. The secrecy performance increases with increase in transmit power of the source, and number of frames of energy accumulation, while the secrecy performance decreases with increase in the target secrecy rate. Thus, instead of using energy harvested in the current frame to forward the signal, we can use the accumulated harvested energy over several frames and achieve a better secrecy at physical layer.

6. Acknowledgment

This research is supported by the Department of Electronics and Information Technology, Ministry of Communications and IT, Government of India under the Visvesvaraya PhD Scheme administered by Media Lab Asia with Grant number PhD-MLA/4(29)/2015-16.

7. References

[1] A. D. Wyner, “The Wire-Tap Channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian Wire-Tap Channel,” IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] J. Barros and M. D. Rodrigues, “Secrecy Capacity of Wireless Channels,” 2006 IEEE Int. Symp. Inf. Theory, vol. 1, pp. 356–360, Jul. 2006.

[4] L. Sun, T. Zhang, Y. Li, and H. Niu, “Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes,” IEEE Trans. Veh. Technol., vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[5] Y. Liu, J. Li, and A. P. Petropulu, “Destination assisted cooperative jamming for wireless physical-layer security,” IEEE Trans. Inf. Forensics Secur., vol. 8, no. 4, pp. 682–694, Apr. 2013.

[6] S. Sudevalayam and P. Kulkarni, "Energy Harvesting Sensor Nodes: Survey and Implications," in IEEE Communications Surveys & Tutorials, vol. 13, no. 3, pp. 443-461, Third Quarter 2011.

[7] X. Lu, P. Wang, D. Niyato, D. I. Kim and Z. Han, "Wireless Networks With RF Energy Harvesting: A Contemporary Survey," in IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 757-789, Secondquarter 2015.

[8] S. S. Kalamkar and A. Banerjee, "Secure Communication via a Wireless Energy Harvesting Untrusted Relay," in IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2199-2213, March 2017.

[9] L. Dong, H. Yousefi'zadeh and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," 2011 IEEE International Conference on Communications (ICC), Kyoto, 2011, pp. 1-5.