




Secrecy outage probability of a two-way cooperative network with an energy harvesting untrusted AF relay

Shashibhushan Sharma¹  · Anurag Kumar¹ · Sanjay Dhar Roy¹ · Sumit Kundu¹

Received: 21 May 2018 / Accepted: 7 June 2018 / Published online: 6 July 2018
© CSI Publications 2018

Abstract In this paper, we analyze the secrecy outage probability (SOP) of a two-way cooperative communication network aided by an energy harvesting untrusted half-duplex amplify and forward relay which conveys information between two legitimate users. The whole communication completes in two time slots. The relay receives signal from both users simultaneously in the first time slot meanwhile it harvests energy based on power splitting ratio scheme. In the second time slot, the relay amplifies and forwards the signal to both users as well as it eavesdrops the message. The relay works as an eavesdropper where signal from one user acts as a jamming signal for the signal of other user. An analytical expression of SOP involving a numerical integration has been derived in single integration form. We verify our analytical results with the simulated results.

Keywords Two-way communication · Energy harvesting · Amplify-and-forward relaying · Secrecy outage probability

1 Introduction

In the past few years, increase in utilization of bandwidth insecure the message at physical layer, if neighbour users known the private key to decode the message. In such cases, there is a need of physical layer security.

Relay nodes working in decode and forward (DF) and, amplify and forward (AF) mode are used for unidirectional

information transfer [1, 2]. Recently two-way relaying has attracted significant interest for exchange of information between two nodes [3]. In [4], the authors have proposed a two-way relaying, where they have shown that the two-way half-duplex relaying overcomes the spectral loss associated with one-way relaying working either in AF or DF mode. Further in [4], the sum rate of two-way communication via half-duplex relay provides the rate equal to the rate of one way full duplex AF or DF relaying. In [5], outage probability has been evaluated in two-way communication with multiple AF relays under a relay selection scheme.

Security of a network is analyzed in [6] where an untrusted energy harvesting relay node (based on power splitting protocol and time switching protocol) relays the information between source and destination and it is shown that an optimal power splitting factor as well as an optimal energy harvesting time factor exist which maximizes the secrecy performance in terms of minimizing the secrecy outage probability (SOP) and maximizing the ergodic secrecy rate. Further friendly jamming by the destination node or a helping node is incorporated to secure the communication through an untrusted relay node [6]. In [7] source and destination based jamming signals are used to jam the untrusted relays which eavesdrop the information signal. Besides these, SOP has been evaluated in multiple full-duplex two-way DF relaying network under optimal relay selection scheme [8].

In [9], the authors study the SOP and average secrecy rate of a two-way communication network with multiple half-duplex AF relays in presence of multiple EAVs. In [10], the authors have derived the performance in terms of ergodic secrecy sum rate (ESSR) and intercept probability a in two-way communication with half-duplex untrusted AF relay with and without friendly jammer (FJ). Intercept probability has been found under a multiple user decoding

✉ Shashibhushan Sharma
ss.15ec1105@phd.nitdgp.ac.in

¹ Department of ECE, NIT Durgapur, Durgapur,
West Bengal 713209, India

scheme in which relay decodes the message signal of both sources. The relay harvests energy in time switching mode. The power outage at relay is also derived which indicates the failure of harvesting circuit in the event of receiving power below a minimum level. Next, the authors in [11], have derived the performance in terms of sum-secrecy rate in a two-way communication as in [10].

However, analysing of secrecy performance is not addressed in terms of SOP in a model as we considered. We evaluate the SOP of two-way relaying network with an energy harvesting half-duplex untrusted AF relay without external jamming. If the two users cooperate in such a way (for example, transmitting at equal power) which reduce the eavesdropping at the relay, the need of an external jammer can be eliminated resulting in significant saving of power. If untrusted relay wants to decode the signal of any one user only at any time, then signal of other user acts as a jamming to prevent eavesdropping by the UAFR. The average received power from both of the users are nearly same which maintains a constant value of SINR at the relay and the secrecy capacity is improved significantly. Analyzing secrecy outage for the above scheme and development of analytical expression for SOP is our novel contribution in this paper.

More precisely, we highlight our contributions of this work as follows:

- Analysing secrecy performance of a two-way communication system with an energy harvesting half-duplex untrusted AF relay (UAFR) in terms of secrecy outage probability.
- Impact of several important physical parameters such as energy harvesting parameter, transmit power of system and channel mean power between users and relay on SOP is indicated.
- We obtain optimal values of energy harvesting factors for which SOP is minimum.
- Impact of energy conversion efficiency on the SOP has been analysed.
- An analytical expression of SOP for the above scenario is obtained in a single integral form which can easily be solved by numerical method of integration.

The remaining part of this paper is organized as follows. In Sect. 2, we describe system model. In Sect. 3, analytical framework for evaluating secrecy performance has been described. Section 4 shows the simulation and numerical results based on our formulation. We conclude this paper in Sect. 5.

2 System model

The user1 (U1) and user2 (U2) share their information via an energy harvesting half-duplex UAFR node as shown in Fig. 1a. We consider that the relay is placed at nearly midpoint between U1 and U2 to remove the extra jamming device as consider in [11]. The jamming device also require extra power to send the jamming signal. All nodes operate in a half-duplex mode and are assisted with a single omnidirectional antenna. There is no direct link between U1 and U2 due to severe shadowing and the communication completes in two hops as in Fig. 1b. In the first time slot, relay harvests the energy from the received signal on the basis of power splitting ratio scheme. The relay amplifies the received signal in the first time slot and forwards it in the second time slot to U1 and to U2, simultaneously. The relay is being untrusted and eavesdrops the message from the information signal of any one user at a time during information sharing between the users. The information signals of both of the users act as a jamming to each other at the untrusted relay [11]. The wireless channel of both hops are flat and slow Rayleigh faded. The channel coefficient between nodes m and n is indicated by h_{mn} . In this model, we assume that the channel are reciprocal [6] and $h_{mn} = h_{nm}$. The channel gain $|h_{mn}|^2$ is exponential distributed random variable with channel mean power Ω_{mn} between nodes m and n and where $m, n \in (U1, U2, R)$. The channel has also additive white Gaussian noise (AWGN) with common distribution $\mathcal{CN}(0, N_0)$. We consider that the perfect channel state information (CSI) is available at the users’ transmitters. Next, we consider the channel coefficients are identically and independent distributed (i.i.d.) random variables.

Figure 1b shows the time frame of complete communication between users. The total communication time T is divided into the two time slots each of equal duration $T/2$. In the first time slot, both of the users transmit the information signal to the relay with power P_{U1} and P_{U2} , respectively. As no external energy source is provided to



(a)

First Time Slot (T/2)	Second Time Slot (T/2)
Information Processing U1, U2→UAFR	Information Processing UAFR→U1, U2
Energy Harvesting and Eavesdropping	

(b)

Fig. 1 a System model of two-way communication and b time frame structure complete communication

the relay, it harvests energy using β fraction of the total received power under power splitting ratio (PSR) scheme and uses $(1 - \beta)$ fraction of received power for information processing following the PSR scheme [6, 11]. In the second time slot, UAFR amplifies and forwards the combined information signal present at the input to both the of users. From the received signal, each user subtracts its own transmitted signal on the basis of perfect knowledge of CSI and thereby receives the signal from the other user. The relay ‘R’ being untrusted tries to eavesdrop the information from each user. However, as the relay eavesdrops signal transmitted by U1, signal from U2 acts as a jamming signal and vice versa.

3 Analytical framework for evaluating secrecy performance

3.1 PSR scheme of energy harvesting by relay

The relay has received the information signal of both user simultaneously in first time slot which can be expressed as:

$$Y'_R = \sqrt{P_{U1}}h_{U1R}x_{U1} + \sqrt{P_{U2}}h_{U2R}x_{U2} + n_r \tag{1}$$

where n_j is the AWGN random variable with common distribution $\mathcal{CN}(0, N_0)$ at j th node ($j \in R, U1, U2$), i.e., AWGN is a circularly symmetric complex Gaussian random variables with mean zero and variance N_0 . The transmitted power of users (user U1 and user U2) are P_{U1} and P_{U2} , respectively. The message signals transmitted by i^{th} user ($i \in 1, 2$) are x_{Ui} having unity power.

A fraction β of the total received signal at the relay is used to harvest the energy under PSR scheme. The AWGN noise part does not contribute any significant power for harvesting energy due to low value and hence it is neglected. The harvested energy, E_H , at the relay and the corresponding power, P_H , in the second time slot are expressed as [6, 11]:

$$\left. \begin{aligned} E_H &= \eta\beta \left(P_{U1}|h_{U1R}|^2 + P_{U2}|h_{U2R}|^2 \right) \frac{T}{2} \\ P_H &= \eta\beta \left(P_{U1}|h_{U1R}|^2 + P_{U2}|h_{U2R}|^2 \right) \end{aligned} \right\} \tag{2}$$

where η is the energy conversion efficiency of the energy harvester and the energy harvesting factor is β .

The remaining received signal (Y_R), after harvesting the energy, is used for information processing at the relay in the first time slot which is expressed as:

$$Y_R = \sqrt{(1 - \beta)P_{U1}}h_{U1R}x_{U1} + \sqrt{(1 - \beta)P_{U2}}h_{U2R}x_{U2} + n_r \tag{3}$$

At the untrusted relay, when the relay decodes information of message signal sent by U1, the other signal sent by U2

acts as a jamming signal and vice versa. Relay is being untrusted and does not get service to subtract the jamming nature of another signal when it decodes the information signal of another user [11]. Thus, the SINRs at relay, corresponding to signal is transmitted by U1 and U2, are respectively given as:

$$\gamma_{U1R} = \frac{(1 - \beta)P_{U1}|h_{U1R}|^2}{(1 - \beta)P_{U2}|h_{U2R}|^2 + N_0} \tag{4}$$

$$\gamma_{U2R} = \frac{(1 - \beta)P_{U2}|h_{U2R}|^2}{(1 - \beta)P_{U1}|h_{U1R}|^2 + N_0} \tag{5}$$

In the second time slot, the relay amplifies the combined received signal Y_R by an amplification factor ξ , thus the transmitted signal, Y_R^{Tx} , of relay is given as:

$$Y_R^{Tx} = \xi Y_R \tag{6}$$

where $\xi = \sqrt{\frac{P_H}{(1-\beta)P_{U1}|h_{U1R}|^2 + (1-\beta)P_{U2}|h_{U2R}|^2 + N_0}}$.

Now, the received signal at the U1 in the second time slot is given by Eq. (7) as:

$$Y_{U1} = h_{RU1}Y_R^{Tx} + n_0 \tag{7}$$

where n_{U1} is also the AWGN sample with power N_0 . Each user, knowing its own signal, subtracts it from the received signal on the basis of perfect knowledge of CSI. The SINR γ_{RU1} at U1 is given as:

$$\gamma_{RU1} = \frac{\xi^2(1 - \beta)P_{U2}|h_{U2R}|^2|h_{RU1}|^2}{(\xi^2|h_{RU1}|^2 + 1)N_0} \tag{8}$$

Substituting the value of ξ from Eq. (6), in Eq. (8) and neglecting the term $\frac{N_0^2}{P_{U1}|h_{U1R}|^2 + P_{U2}|h_{U2R}|^2}$ in the denominator of the Eq. (8) for the low value of N_0 .

Next, using channel reciprocity on the relay-users links [6] $|h_{U1R}|^2 = |h_{RU1}|^2$ and $|h_{U2R}|^2 = |h_{RU2}|^2$, and assuming equal transmit power of both users in order to relay does not eavesdrop the message of any signal more due to jamming nature of each other, i.e., $P_{U1} = P_{U2} = P$, we write γ_{RU1} and γ_{U2} as:

$$\gamma_{RU1} = \frac{\eta\beta(1 - \beta)P|h_{U2R}|^2|h_{RU1}|^2}{\eta\beta|h_{RU1}|^2N_0 + N_0(1 - \beta)} \tag{9}$$

Similarly the SINR γ_{RU2} at U2 is given as:

$$\gamma_{RU2} = \frac{\eta\beta(1 - \beta)P|h_{U2R}|^2|h_{RU1}|^2}{\eta\beta|h_{U2R}|^2N_0 + N_0(1 - \beta)} \tag{10}$$

where γ_{RU1} and γ_{RU2} represent the SINR at U1 and U2, respectively. The use of equal transmit powers remove the extra jamming as used in [10, 11] in which extra power is needed in generation of jamming signal.

3.2 SOP of two-way communication via an untrusted relay

The channel capacities of each one-way communication at the relay and the respective destination can be expressed as:

$$\left. \begin{aligned} C_{U1R} &= \frac{1}{2} \log_2(1 + \gamma_{U1R}); C_{RU2} = \frac{1}{2} \log_2(1 + \gamma_{RU2}) \\ C_{U2R} &= \frac{1}{2} \log_2(1 + \gamma_{U2R}); C_{RU1} = \frac{1}{2} \log_2(1 + \gamma_{RU1}) \end{aligned} \right\} \tag{11}$$

where C_{U1R} , C_{RU2} , C_{U2R} and C_{RU1} are the U1 to relay, relay to U2, U2 to relay and relay to U1 channel capacities, respectively. The secrecy capacities of each one-way communication can be expressed as:

$$\left. \begin{aligned} C_{U1U2}^{Sec} &= \max\{C_{RU2} - C_{U1R}, 0\}; \\ C_{U2U1}^{Sec} &= \max\{C_{RU1} - C_{U2R}, 0\}; \end{aligned} \right\} \tag{12}$$

where C_{U1U2} and C_{U2U1} are the secrecy capacities of transmission links from U1 to U2 and U2 to U1, respectively. The Eq. (12) can be re-expressed as:

$$\left. \begin{aligned} C_{U1U2}^{Sec} &= \max\left\{\frac{1}{2} \log_2\left(\frac{1 + \gamma_{RU2}}{1 + \gamma_{U1R}}\right), 0\right\} \\ C_{U2U1}^{Sec} &= \max\left\{\frac{1}{2} \log_2\left(\frac{1 + \gamma_{RU1}}{1 + \gamma_{U2R}}\right), 0\right\} \end{aligned} \right\} \tag{13}$$

Now, the effective secrecy capacity, C_S , of the network is given as the minimum of the secrecy capacities of the two links in worst case.

$$C_S = \min(C_{U1U2}^{Sec}, C_{U2U1}^{Sec}) \tag{14}$$

A communication network is in secrecy outage if the effective secrecy capacity, C_S , of the network is less than some predefined target secrecy rate R_{TH} . Thus SOP, P_{Out}^{Sec} , of the network model is given as [2]:

$$P_{Out}^{Sec} = P(C_S < R_{TH}) \tag{15}$$

Using Eq. (14) in Eq. (15) and apply order statistics, the Eq. (15) can be re-expressed as:

$$P_{Out}^{Sec} = 1 - \left\{ 1 - \underbrace{P(C_{U1U2}^{Sec} < R_{TH})}_{I_1} \right\} \left\{ 1 - \underbrace{P(C_{U2U1}^{Sec} < R_{TH})}_{I_2} \right\} \tag{16}$$

We have considered the equal transmit power of users and considered that the both of channel coefficients are i.i.d. random variables. In such cases, $I_1 = I_2$, say it as: $I_1 = I_2 = I$ and the P_{Out}^{Sec} can be expressed as:

$$P_{Out}^{Sec} = 1 - (1 - I)^2 \tag{17}$$

We consider the calculation of I_1 . Once, I_1 is evaluated, P_{Out}^{Sec} is also evaluated. Here, I_1 can be expressed as [6, eq. (15)]:

$$I_1 = 1 - \frac{1}{\Omega_{RU1}} \int_{T_1}^{\infty} \left\{ \exp\left(\frac{-(\Delta - 1)}{w(z)\Omega_{U2R}} - \frac{z}{\Omega_{RU1}}\right) \right\} dz \tag{18}$$

where $z = |h_{RU1}|^2$, $\Delta = 2^{2R_{TH}}$, $T_1 = \frac{\left(\frac{\Delta-1}{1-\beta}\right) + \sqrt{\left(\frac{\Delta-1}{1-\beta}\right)^2 + \frac{4\Delta P}{N_0\eta\beta}}}{2\left(\frac{P}{N_0}\right)}$ and

$w(z) = (1 - \beta) \left\{ \frac{\eta\beta Pz}{\eta\beta z N_0 + N_0(1-\beta)} - \frac{\Delta P}{(1-\beta)Pz + N_0} \right\}$. Finally, using Eqs. (17) and (18), SOP can be expressed as:

$$P_{Out}^{Sec} = 1 - \left[\frac{1}{\Omega_{RU1}} \int_{T_1}^{\infty} \left\{ \exp\left(\frac{-(\Delta - 1)}{w(z)\Omega_{U2R}} - \frac{z}{\Omega_{RU1}}\right) \right\} dz \right]^2 \tag{19}$$

3.3 Asymptotic analysis

In Eq. (19), if we consider the $P \rightarrow \infty$ then $T_1 \rightarrow 0$, $w(z) \rightarrow \infty$ and $I_1 \rightarrow 0$. In this case P_{Out}^{Sec} is expressed as:

$$P_{Out}^{Sec} \rightarrow 0 \tag{20}$$

The increased power of both of the users (with high power transmission) increase only the legitimate channel capacity not increase or decrease the eavesdropper channel capacity under perfect knowledge of CSI and i.i.d. channel condition assumption. Thus, $P_{Out}^{Sec} \rightarrow 0$ with $P \rightarrow \infty$. The given final numerical expression for SOP in Eq. (19) is presented in integration form which can be easily evaluated by numerical integration. The expression for SOP is a novel expression for a two-way communication network via an untrusted AF relay considering energy harvesting from RF signals of both users.

4 Simulation and numerical results

Analytical results of SOP given in Eq. (19) have been obtained using numerical method of integration which are validated by MATLAB simulation results.

We have considered the following values system parameters for numerical results which are given in Table 1.

Figures 2 and 3 show the effect of energy harvesting factor (β) on SOP. In Fig. 2, four curves for four different

Table 1 Values of different physical parameters

Physical parameters	Numerical values
Transmit power of users (P)	- 5, 0, 5, 10 dBW
Channel mean power ($\Omega_{U1R} = \Omega_{U2R}$)	- 4, - 2, 0, 2 dB
AWGN power	10^{-2} W
Target secrecy rate (R_{TH})	1 bits/s/Hz
Energy harvesting factor (β)	0.5, 0.6, 0.7, 0.75
Energy conversion efficiency (η)	0.7

values of user transmit power as $P = -5, 0, 5, 10$ dBW and 0 dB channel mean power are presented. But in Fig. 3, four curves for four different values of channel mean power as $\Omega_{U1R} = \Omega_{U2R} = -4, -2, 0, 2$ dB and 5 dBW transmit power of users are presented. In Fig. 2, for a particular value of $P = 10$ dBW, SOP first decreases up to an optimal value of β then further increases with increase in β . In Fig. 2, the optimal values corresponding to different powers is obtained as $P = -5$ dB, $\beta = 0.5$; $P = 0$ dB, $\beta = 0.6$; $P = 5$ dB, $\beta = 0.7$ and $\beta = 0.75$. In Figs. 2 and 3, initial decrease in SOP is due to increase in β , the harvested energy of relay increases, which increases the transmit power of relay, thereby improving the SINR at the

corresponding destination. Next, increase in β reduces the information signal reception at the relay, which reduces SINR at the relay and thereby the capacity of the eavesdropping link. This justifies the initial decrease in SOP curve up to an optimal point. Beyond the optimal point, increase in β causes very poor signal at the relay for the information processing, which on amplification becomes more noisy. This decrement in signal strength for information processing at the relay is not compensated by using harvested energy and amplification factor of relay. Accordingly, the received signal strength at the receiver (U1 or U2) decreases, SOP increases and performance degrades beyond optimal point. However, we get the acceptable performance over a large range of energy harvesting factor. We also observe that for particular value of β , the performance improves with increase in transmit power of both users. From Figs. 2 and 3, we observe that the optimal point changes with change in transmit power. But it does not change with change in channel mean power.

Figure 4 depicts SOP versus the user to relay channel mean power of both the links, $\Omega_{U1R} = \Omega_{U2R}$. There are four curves for four different values of user transmit power as $P_{U1} = P_{U2} = P = -5, 0, 5, 10$ dB. As the Ω_{U1R} increases, channel capacities between the users and the relay

Fig. 2 SOP versus power splitting factor for energy harvesting for different values of transmit power of users and 0 dB channel mean power of both of the links

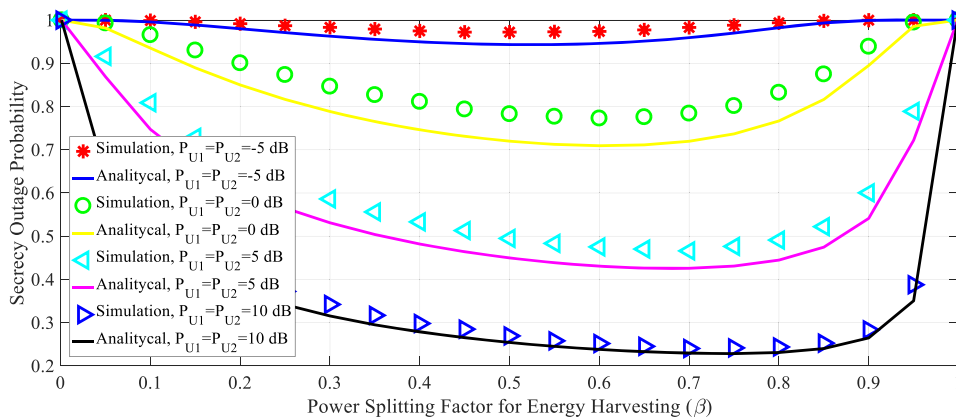


Fig. 3 SOP versus power splitting factor for energy harvesting for different values of channel mean power and 5 dBW transmit power of both of the users

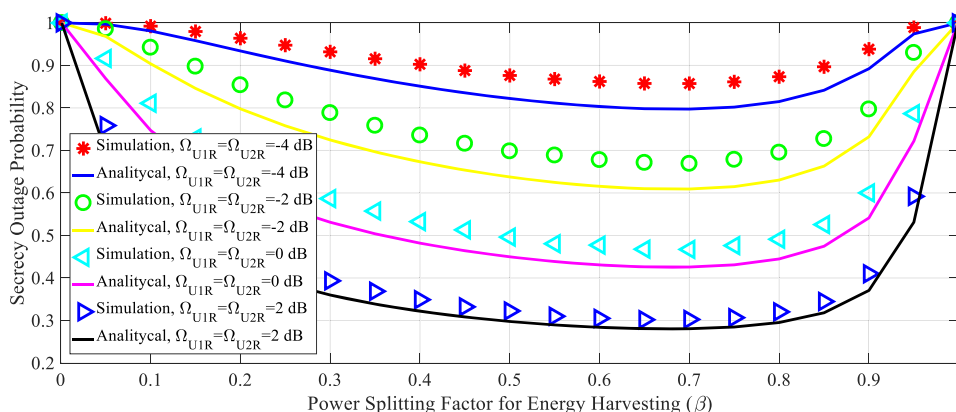


Fig. 4 SOP versus channel mean power of both link in dB for different values of transmit power of users

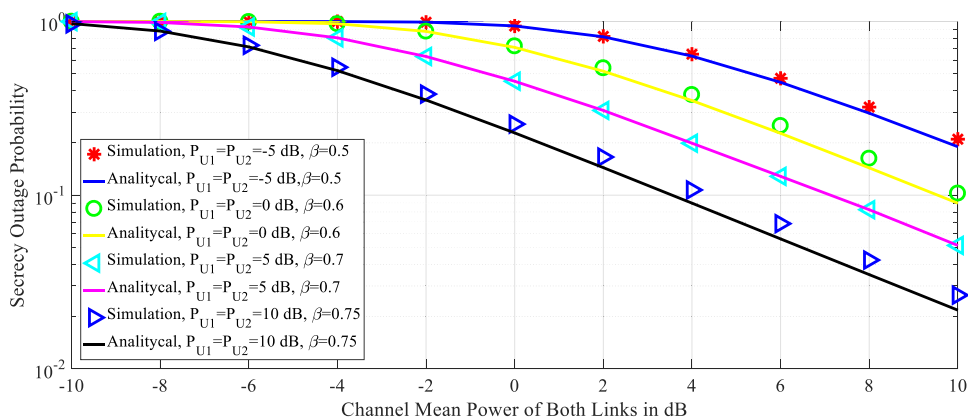
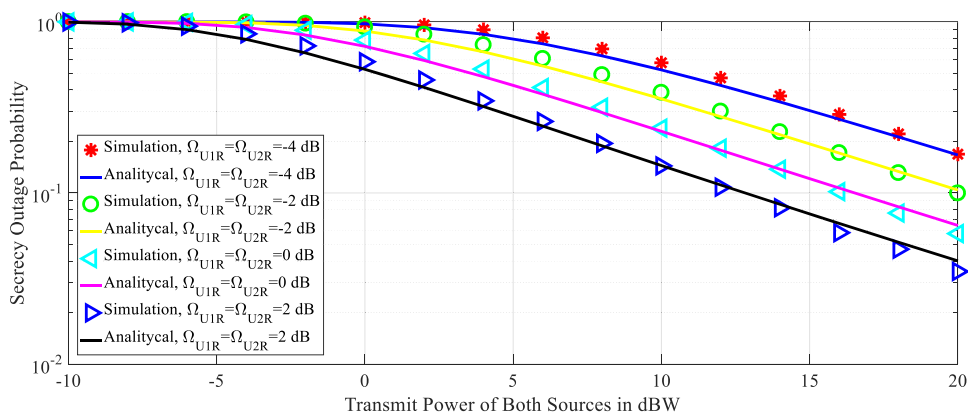


Fig. 5 SOP versus equal transmit power of both users in dB for different values of channel mean power of links with $\beta = 0.7$



increases, enhancing signal quality at the relay which in turn increases SINR at destination user. Due to equal transmit power of users and due to equal channel mean power of both link, SINR of signal of any desired user at the relay does not increase due to jamming nature to each other. Thus, eavesdropping capacity at the UAFR is not enhanced. This combined effect increases secrecy capacity of the users and justifies the continuous decreasing nature of SOP curve. We also observe that for a particular value of channel mean power, SOP reduces with increase in transmit power of users which shows the improvement in performance in terms of SOP. Detailed explanation of this is given in Fig. 5.

Figure 5 shows that increase in transmit power of the users reduces SOP. In this figure, four values of channel mean powers as $\Omega_{U1R} = \Omega_{U2R} = -4, -2, 0, 2$ dB and 5 dBW users transmit power are considered. With increase in transmit power, signal strength at the relay increases which on amplification further increases the SINR at the destination. At the relay though strength of the desired signal increases, increase in strength of signal from other user increases the jamming effect, thus accounting for no improvement of SINR at relay. As a result effective

secrecy capacity increases which reduces the SOP. Further, we observe that for a particular value of transmit power of users, SOP reduces with increase channel mean power. In Fig. 5, we observe that the SOP decreases with increase in user transmit power. It is also proof as in Eq. (20) that as $P \rightarrow \infty$, $SOP, P_{Out}^{Sec} \rightarrow 0$.

Figure 6 shows the impact of energy conversion efficiency on the SOP with 0 dB channel mean power. As the energy conversion efficiency increases, the harvested energy increases which improves the signal strength at the corresponding receiving users. But there is no impact of η on the relay channel capacities. Relay channel capacities are constant and the receiving users' channel capacities at the users increase due to increase in harvesting energy with increase in η . Thus, secrecy capacity increases and SOP decreases. The energy conversion efficiency is different for different harvesting circuits.

Figure 7 shows the SOP vs. target secrecy rate with 0 dB channel mean power. There is more chance of secrecy outage with increase in target secrecy rate. However, performance is better when target secrecy rate is below the 1 bits/s/Hz.

Fig. 6 SOP versus energy conversion efficiency for the different values of transmit power of the users and 0 dB channel mean power

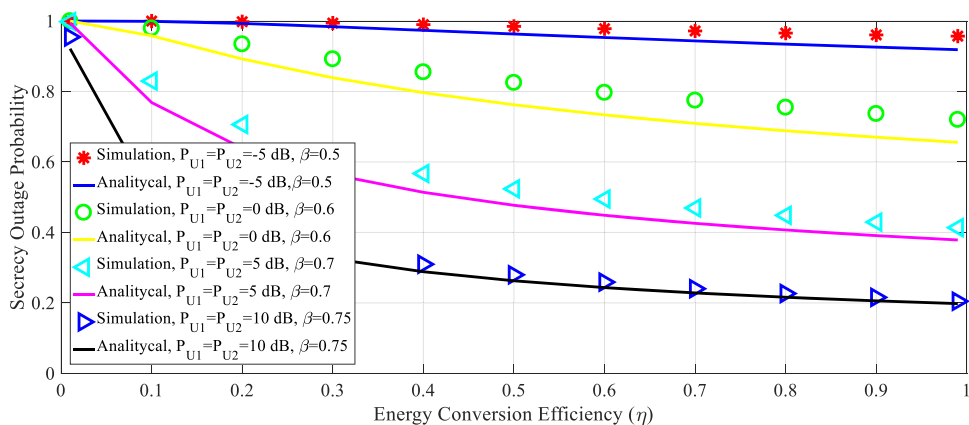
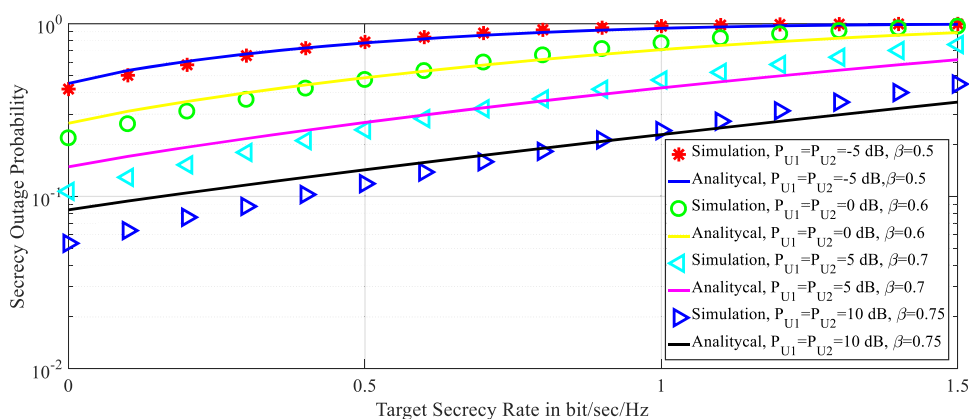


Fig. 7 SOP versus target secrecy rate for the different values of transmit power of the users and 0 dB channel mean power



5 Conclusion

Secrecy performance in terms of SOP of our proposed two way communication model has been studied under several parameters such as power splitting factor, channel mean power and user transmit power. An analytical expression for SOP involving a single integration is derived which can be evaluated numerically. An optimal value of energy harvesting factors are observed depending on other parameters which minimizes the SOP. The optimal values of energy harvesting factor are different for different values of transmit power of users but these are constant for different values of channel mean power. It is also observed that increase in channel mean power as well as user transmit power is beneficial to secure the two-way communication even if the relay is untrusted. The best harvesting circuit provides the best performance in terms of SOP. Further, SOP increases with increase in target secrecy rate. Moreover, this model is beneficial to secure information although there is no jamming device.

Acknowledgements 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.

References

1. Liu Y, Li J, Petropulu AP (2013) Destination assisted cooperative jamming for wireless physical-layer security. *IEEE Trans Inf Forensics Secur* 8(4):682–694
2. Nguyen BV, Kim K (2015) Secrecy outage probability of optimal relay selection for secure AnF cooperative networks. *IEEE Commun Lett* 19(12):2086–2089
3. Liu Y, Elkashlan M, Duong TQ, Nallanathan A (2014) Two-way relaying networks with wireless power transfer: policies design and throughput analysis. In: 2016 IEEE global communications conference, pp 4030–4035
4. Rankov B, Wittneben A (2005) Spectral efficient signaling for half-duplex relay channels. In: Conference record of the thirty-ninth asilomar conference on signals, systems and computers, 2005, pp 1066–1071
5. Jan N, Arbab WA, Khan G (2011) Outage probability and relay selection in bidirectional AF relay networks. In: 2011 7th international conference on wireless communications and networking and mobile computing, pp 1 – 3
6. Kalamkar SS, Banerjee A (2017) Secure communication via a wireless energy harvesting untrusted relay. *IEEE Trans Veh Technol* 66(3):2199–2213

7. Sun L, Ren P, Du Q, Wang Y, Gao Z (2015) Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *IEEE Commun Lett* 19(3):463–466
8. Zhong B, Zhang Z (2017) Secure full-duplex two-way relaying networks with optimal relay selection. *IEEE Commun Lett* 21(5):1123–1126
9. Zhang C, Ge J, Li J, Gong F, Ding H (2017) Complexity-aware relay selection for 5G large-scale secure two-way relay systems. *IEEE Trans Veh Technol* 66(6):5462–5466
10. Mamaghani MT, Kuhestani A, Wong K-K (2017) Energy harvesting based secure two-way communication using an untrusted relay, pp 1–12. 21 Aug 2017. [arXiv:1708.06437v1](https://arxiv.org/abs/1708.06437v1) [cs.CR]
11. Gupta V, Kalamkar SS, Banerjee A (2017) On secure communication using RF energy harvesting two-way untrusted relay, pp 1–7. [arXiv:1708.07989v1](https://arxiv.org/abs/1708.07989v1) [cs.IT]