Wireless Personal Communications (2020) 110:2045–2064
https://doi.org/10.1007/s11277-019-06829-6

Two-Way Secure Communication with Multiple Untrusted Half-Duplex AF Relays

Shashibhushan Sharma[1] · Sanjay Dhar Roy[1] · Sumit Kundu[1]

Published online: 18 October 2019

Abstract

In this paper, we analyze the secrecy outage probability (SOP) of a cognitive cooperative radio network in a two-way communication in which two secondary source communicate with each other via multiple untrusted half-duplex amplify and forward relays in the absence of direct link. Due to the cognitive scenario, power is allocated to secondary nodes on the basis of outage constraint of the primary network. In the absence of direct link between two sources, communication completes in two time slots. In the first time slot, both of the sources broadcast the information signal and in the second time slot, a selected relay broadcasts the amplified information signals of both of the sources. Relays being untrusted, they can eavesdrop the message from the information signal. A particular relay, which maximizes the end-to-end secrecy capacity, is selected to broadcast the signal. The selected untrusted relay can only eavesdrop the message and other relays forcefully remain in idle condition. At the untrusted relay, information signals of both of the sources act as a jamming to each other. The selected untrusted relay harvests the energy using a power splitting ratio scheme. We observe the performance of the proposed model in terms of SOP. We find the optimal values of energy harvesting factor at which SOP becomes minimum. Several important parameters such as the impact of number of untrusted relays, primary transmit power, peak transmit power of secondary sources, threshold outage rate of primary receiver and threshold secrecy rate on SOP is indicated. An analytical expression for the SOP has been developed in a single integration form. Numerical results based on analytical expression are verified by MATLAB simulation.

Keywords Physical layer secrecy · Half-duplex amplify and forward relay · Two-way communication · Threshold secrecy rate · Secrecy rate · Secrecy outage

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

[1] Department of Electronics and Communication Engineering, NIT Durgapur, Durgapur, West Bengal 713209, India

1 Introduction

Physical layer security (PLS) [1] is an appealing approach to maintain secrecy of confidential message alternative to cryptography technique. In cryptographic approach, message becomes vulnerable if someone knows the private keys. At physical layer, message may not be secured always in the case, when an eavesdropper is very close to the source. In such case, cooperative jamming helps to improve security at physical layer [2].

1.1 Secrecy Capacity, Secrecy Outage Probability and Cooperative Jamming

The authors in [3] considered the Gaussian wire-tap channel and defined the secrecy capacity which is the difference between legitimate channel capacity and eavesdropper (EAV) channel capacity. For proper secrecy of the information signal, information channel capacity at destination should be greater than that at the EAV. The authors in [4] evaluated the ergodic secrecy capacity (ESC) via multiple untrusted amplify and forward (AF) relays. In the same, relays are assisted with directional antennas. They have found that the multiple untrusted relay does not improve the performance. The authors in [5] also proved that the ESC degrades with increase in number untrusted AF relays. Here relays are assisted with Omni-directional antennas. The authors in [2] have found the secrecy rate under the source and destination assisted jamming via multiple decode and forward (DF) relays.

The authors in [6] have evaluated the SOP in presence of an untrusted energy harvesting AF relay. In the same, to enhance the positive secrecy rate, cooperative destination assisted jamming has been used which is eliminated in the second time slot by the destination. The authors in [7] have evaluated the SOP under the scenario in which an EAV tries to eavesdrop the information signal from selected relay. An optimal relay selection is considered and the SOP is analyzed under such case. The authors in [8] evaluated the SOP in presence of multiple EAVs for a single hop communication. The authors in [9] evaluated the secrecy rate for multiple-input and multiple-output relay network. In the same, authors have used the cooperative jamming to improve positive secrecy rate. In [10], the authors considered a destination assisted jamming in the first time slot under the perfect knowledge of channel state information (CSI). The destination eliminates the known jamming on the basis of perfect knowledge of CSI.

1.2 Energy Harvesting

Intermediate helper nodes like relay or jammer, which are constrained by power, need to harvest energy. They can use this energy to forward the information signal or send the jamming signal. Popular schemes for harvesting energy from radio frequency (RF) signal exist such as power splitting ratio (PSR) based [6, 8, 11] and time switching relay (TSR) [12] or hybrid combination of these two. The authors in [6] power the relay with harvested energy based on power splitting scheme. In [8], all energy harvesters harvest the energy based on power splitting scheme. Power splitting based energy harvesting has been discussed in [11] which uses supplies the harvested power to both of the AF and DF relays. In [12], both of the relays and jammer are powered by harvested energy on the basis of time switching scheme.

1.3 Secrecy in Cognitive Radio Network

Due to multiple nodes in cognitive radio network (CRN), PLS is promising approach to secure the message of primary and secondary network. In [13], PLS has been estimated in terms of secrecy rate and SOP in a cognitive environment. In the same, there are multiple primary users (PUs) and multiple EAVs. Secrecy rate is maximized under the interference constraint of PU receiver (PU-RX). In [14], SOP has been evaluated in a cognitive environment which uses single hop communication. Power is allocated to cognitive nodes under the interference constraint of PU-RX. In the same, authors assume that the primary transmitter (PU-TX) is situated far away from the secondary receiving node. The signal received at destination is not interfered by the transmission of PU-TX. In [15], authors have evaluated the SOP in the CRN with coordinated and uncoordinated EAVs. Power allocation in the CRN is an important issue. Power can be allocated to cognitive nodes on the basis of outage constraint [16] and interference constraint [14].

1.4 Two-Way Communication

Two-way communication via half duplex AF relay increase the efficiency of utilization of bandwidth and also saves the time of communication. In two-way communication, two nodes share their information with the help of intermediate relay(s) which can work in half duplex mode or full duplex mode [12, 17]. In [17], the SOP is affected with number of relays, average signal to interference plus noise ratio (SINR) and average self-interference at full duplex relays. In [18], the SOP and the average secrecy rate have been analyzed for fifth generation network achieving two-way communication via multiple relays under attack of multiple EAVs. Relay has been selected following a low-complexity relay selection criterion. In [19], the secrecy performance has been analyzed using truth-telling mechanism via multiple AF relays under an EAV attack. Relays harvest the energy from RF sources. In [12], ergodic secrecy rate has been analyzed in a two-way communication with and without jammer. In the same, energy is harvested from RF source in the first time slot and in second time slot both the sources forward the information signal and jammer sends the jamming signal to confuse untrusted relay. In the third time slot, relay forwards the scaled version of the signal to both the sources.

1.5 Problem Addressed in the Paper

In the existing literature, as discussed above, secrecy performance of two-way communication via multiple energy harvesting untrusted relays in the cognitive scenario is not addressed to the best of our knowledge. In [6], only a single untrusted relay and only one-way communication is discussed where the relay also harvests energy. In [12], two-way communication is taking place between two sources via a single energy harvesting untrusted relay without considering any cognitive scenario. Thus, there is a need of analyzing the secrecy performance for the two-way communication with the help of multiple energy harvesting untrusted relays in a cognitive scenario which is the theme of this paper.

1.6 Contribution of the Present Paper

We have evaluated the SOP of CCRN in two-way communication via multiple energy harvesting half-duplex untrusted relays. The evaluation of SOP in such environment is our novel contribution. Major contribution of the present paper is outlined below as:

- We evaluate the SOP of the proposed model. Analytical expression of SOP involving a single integration is developed.
- In the considered model, the closed form expression of power allocation to cognitive nodes under the outage constraint of primary user in the first and second time slots have been evaluated.
- Optimal value of fraction of received energy has been evaluated at which SOP becomes minimum.
- Impact of several network parameters such as: outage constraints of primary user, fraction of received energy used for harvesting, primary transmit power, peak transmit power of secondary nodes, and threshold secrecy rate is shown on SOP.
- The diversity in number of relays is seen to improve the secrecy performance in terms of SOP significantly, even if relays are untrusted, in contrast to existing literature where multiple untrusted relay degrades SOP in one-way communication [4, 5].

1.7 Sections Organization

The Sect. 2 describes the system model. In Sect. 3, the performance analysis is presented. The numerical results have been presented and explained in Sect. 4. Finally Sect. 5 concludes the paper.

2 System Model

2.1 CCRN Model

In this system model as shown in Fig. 1, secondary source one (SS_1) communicates with secondary source two (SS_2) via multiple half-duplex untrusted secondary amplify and forward relays (USAFRs) under a cognitive scenario. The relays being untrusted and can eavesdrop the message. But, the messages are eavesdropped by the selected relay only, which is selected to broadcast the information signal. The other non-selected relays forcefully remain in idle condition, i.e., they can not receive and transmit the signal. All secondary nodes (SNs) (i.e., SS_1, SS_2 and USAFRs) are assisted with omnidirectional antennas and thus there is a need of power allocation to SNs depending on outage constraint of primary network. Thus power is allocated to SNs on the basis of outage constraint of primary network. We assume that the SNs are far from the PU-TX, the interference from PU-TX to SNs is negligible [14]. There is no direct link between SS_1 and SS_2. Thus, communication is completed in two time slots as shown in Fig. 2. The relay is selected on the basis of maximizing secrecy rate. After relay selection, both the sources, i.e., SS_1 and SS_2, broadcast their confidential information signal via wireless channel to the selected USAFR in the first time slot. In the second time slot, selected relay broadcasts the amplified version of information signals of SS_1 and SS_2 which are

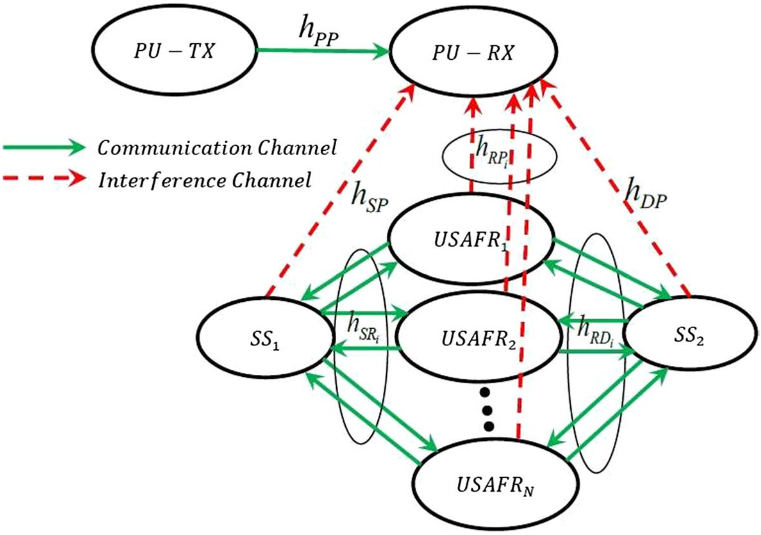

Fig. 1 System model of two-way communication via multiple half-duplex AF relays

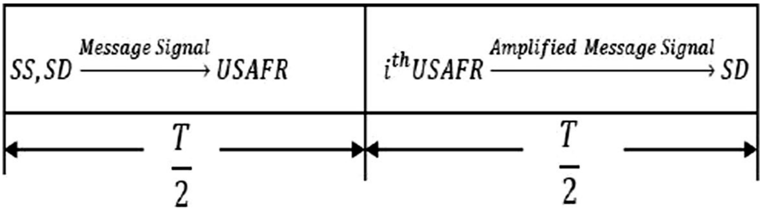

Fig. 2 Time frame structure of complete communication

received at SS_2 and SS_1. Meanwhile, the selected USAFR tries to eavesdrop the message of any one source at a particular time. The selected USAFR can not eavesdrop the messages of both the sources simultaneously at any particular time. Since, information signals of both the sources acts as a jamming to each other at the selected USAFR which degrades the signal strength at the USAFR. In the case of signal transmission with unequal power by both the sources, selected relay is able to eavesdrop the message of the information signal which is being transmitted with comparably higher power. Thus, we consider the signal transmission with equal power which provides signal to interference plus noise ratio (SINR) at the relay receiver almost same for both the senders. This assumption works if both the sources to relay links have independent identically distributed (i.i.d.) fading with same channel mean power.

We also assume that the perfect channel state information (CSI) are available at both the sources [10]. The SS_1 and SS_2 detect their own signal in second time slot on the basis of CSI and delete the same from the received signal as in [10]. The selected relay only tries to eavesdrop the message signal of either source while the message signal of other source acts as a jamming signal. In this way, both the sources decode the message successfully but, due to jamming nature of the signals to each other at the relay position, relay is unable to decode the message properly which leads to maintaining secrecy.

However, the relay's ability to decode the message leads to secrecy outage, the evaluation of probability of which is the main focus of the paper.

2.2 Channel Model

In this model as shown in Fig. 1, let h_{PP}, h_{SS_1P}, h_{RP_i}, h_{SS_2P}, $h_{SS_1R_i}$, $h_{R_iSS_1}$, $h_{R_iSS_2}$ and $h_{SS_2R_i}$ are the channel coefficients of links between *PU-TX* to *PU-RX*, SS_1 to *PU-RX*, $USAFR_i$ to *PU-RX*, SS_2 to *PU-RX*, SS_1 to $USAFR_i$, $USAFR_i$ to SS_1, $USAFR_i$ to SS_2 and SS_2 to $USAFR_i$, respectively. All channels are considered as flat Rayleigh fading.

These channel gains are independent identically distributed (i.i.d.) random variables. Square of the *j*th channel coefficient is the channel gain of that channel and it is expressed as:

$$g_j = \left|h_j\right|^2 \tag{1}$$

The probability distribution function of channel gain is exponential and can be expressed as:

$$f_{g_j}(x) = \frac{1}{\Omega_j} \exp\left(-\frac{x}{\Omega_j}\right); \quad x \geq 0 \tag{2}$$

where the channel mean power of *j*th channel coefficient is Ω_j .Additive white Gaussian noise (AWGN) of channel is circularly symmetry complex Gaussian noise with mean zero and two sided power spectral density of N_0 .Both the sources have the peak transmit power $\left(P_{PK}\right)$.

3 Performance Analysis

In this section, we are evaluating the power allocation to secondary nodes under primary constraint, signal to interference-plus-noise ratio (SINR) at different receiving nodes, global secrecy capacity of two-way communication, and finally SOP of the two-way communication network.

3.1 Power Allocation to Secondary Nodes

In the first time slot of the secondary network, both the sources broadcast the information signal which interfere with the information signal of primary network at the receiver of PU-RX. In this slot, we need to evaluate the maximum limit of the broadcasting power of both the sources. The g_{SS_1P} and g_{SS_2P} are the i.i.d. random variables indicating channel gains of two secondary sources to primary receiver respectively. The outage probability P^P_{Out} of primary network in the duration of first time slot of secondary network is given as:

$$\begin{aligned} P^P_{Out} &= \left[P\left\{\left(1 + \frac{P_P g_{PP}}{P_{M_{SS}}\left(g_{SS_1P} + g_{SS_2P}\right) + N_0}\right) \leq R_P\right\}\right] \leq \Theta \\ &= 1 - \frac{\exp\left(-\frac{\gamma^P_{TH} N_0}{P_P \Omega_{PP}}\right)}{\left(\frac{\gamma^P_{TH} P_{M_{SS}} \Omega_{SS_1P}}{P_P \Omega_{PP}} + 1\right)^2} \leq \Theta. \end{aligned} \tag{3}$$

where $\gamma_{TH}^{P} = 2^{2R_P}$ and P_P is the primary user transmit power, R_P is the threshold outage rate of PU-RX, $P_{M_{SS}}$ is the maximum allowable broadcasting power of SS_1 and SS_2, N_0 is the noise power of AWGN and Θ is the constraint in outage probability of the primary network. On the basis of expression in Eq. (3), we can allocate the power to both of the sources which are in equal values as:

$$P_{M_{SS}} = \frac{P_P \Omega_{PP}}{\gamma_{TH}^{P} \Omega_{SP}} \left[\left\{ \frac{\exp\left(-\frac{\gamma_{TH}^{P} N_O}{P_P \Omega_{PP}}\right)}{1 - \Theta} \right\}^{0.5} - 1 \right], \tag{4}$$

Since both the sources have sufficient amount of available power, they can transmit the signal with assigned maximum allowable broadcasting power $\left(P_{M_{SS}}\right)$ maintaining constraint on primary outage. However, due to purpose of saving the power, they may not transmit the signal with this maximum allowable broadcasting power $\left(P_{M_{SS}}\right)$ estimated above under cognitive constraint. Considering the peak transmit power of secondary nodes (the limitation on peak transmit power arises due to device limitation), the actual assigned power to both the sources can be expressed as:

$$P_S = \min\left(P_{M_{SS}}, P_{PK}\right) \tag{5}$$

where P_S is the assigned power to both the sources. In the second time slot of the secondary network, only the selected relay broadcasts the information signal using harvested energy which interfere with the information signal of primary network at PU-RX. In this time slot also, we can evaluate the maximum amount of broadcasting power with which relay can broadcast the information signal. The outage probability, P_{Out}^{P} of primary network in this second duration is given as:

$$\begin{aligned} P_{Out}^{P} &= P\left\{ log_2\left(1 + \frac{P_P g_{PP}}{P_{M_{SR}} g_{RP} + N_O}\right) \le R_P \right\} \\ &= 1 - \frac{\exp\left(-\frac{\gamma_{TH}^{P} N_0}{P_P \Omega_{PP}}\right)}{\left(\frac{\gamma_{TH}^{P} P_{M_{SR}} \Omega_{RP}}{P_P \Omega_{PP}} + 1\right)} \le \Theta. \end{aligned} \tag{6}$$

The maximum allowable power of the selected ith relay is $P_{M_{SR_i}}$. We leave the subscript i from $P_{M_{SR_i}}$ for ease of notation, i.e., $P_{M_{SR}} = P_{M_{SR_i}}$. The maximum allowable power $\left(P_{M_{SR}}\right)$ of the selected ith relay, to amplify and broadcast the information signal, can be expressed as:

$$P_{M_{SR}} = \frac{P_P \Omega_{PP}}{\gamma_{TH}^{P} \Omega_{RP}} \left[\left\{ \frac{\exp\left(-\frac{\gamma_{TH}^{P} N_O}{P_P \Omega_{PP}}\right)}{1 - \Theta} \right\} - 1 \right]. \tag{7}$$

But, the relay can not always broadcast the information signal with maximum allowable power $\left(P_{M_{SR}}\right)$ under cognitive constraint due to lack of sufficient amount of available power. If ith relay harvests more power which is greater than $P_{M_{SR}}$ then it can broadcast the information signal with $P_{M_{SR}}$, as obtained in Eq. (7), otherwise it broadcasts with maximum available harvesting power. Mathematically, it can be expressed as:

$$P_{SR_i} = \min\left(P_{H_i}, P_{M_{SR}}\right) \tag{8}$$

where P_{H_i} is the harvested power by the ith USAFR which is used by the same in the second time slot and P_{SR_i} is the transmit power of the ith relay.

3.2 Harvesting Energy and SINR Evaluation at Different Receiving Nodes of Secondary Network

AT first, an optimal relay is selected on the basis of maximizing global secrecy capacity as following the approach of maximizing the system secrecy capacity in [7]. The selection scheme of relay has been described in Subsection C of this Section. The SS_1 and SS_2 broadcast their information signal which is received at the selected ith USAFR as:

$$y'_R = \sqrt{P_S}h_{SS_1R_i}x_{SS_1} + \sqrt{P_S}h_{SS_2R_i}x_{SS_2} + n_0 \tag{9}$$

where x_{SS_1} and x_{SS_2} are the messages of the SS_1 and SS_2 with unit power, respectively and n_0 is the AWGN sample. The selected relay harvests the energy using a fraction (β) of the received energy following a PSR scheme [6, 8]. The expression of energy is expressed as:

$$E_{H_i} = \eta\beta P_S\left(g_{SS_1R_i} + g_{SS_2R_i}\right)\frac{T}{2} \tag{10}$$

where E_{H_i} is the harvested energy, β is the fraction of received energy at relay with range $0 < \beta < 1$ and η is the energy conversion efficiency with range $0 < \eta \leq 1$. Harvested power $\left(P_{H_i}\right)$, which is used by the relay in the second time slot to broadcast the information signal, is given as:

$$P_{H_i} = \eta\beta P_S\left(g_{SS_1R_i} + g_{SS_2R_i}\right) \tag{11}$$

The remaining fraction of received power of the information signal is used by the relay for processing the information which is given as:

$$y_R = \sqrt{(1-\beta)P_S}h_{SS_1R_i}x_{SS_1} + \sqrt{(1-\beta)P_S}h_{SS_2R_i}x_{SS_2} + n_0 \tag{12}$$

The relay is being untrusted and tries to eavesdrop the message from the information signal of both the sources. If relay tries to eavesdrop the message from information signal of SS_1 then the information signal of SS_2 acts as a jamming to the ith USAFR and vice versa. The SINRs at the relay in order to eavesdrop the messages from the information signal of SS_1 and SS_2, respectively are expressed as:

$$\left.\begin{aligned} \gamma_{SS_1R_i} &= \frac{(1-\beta)P_S g_{SS_1R_i}}{(1-\beta)P_S g_{SS_2R_i} + N_0}, \\ \gamma_{SS_2R_i} &= \frac{(1-\beta)P_S g_{SS_2R_i}}{(1-\beta)P_S g_{SS_1R_i} + N_0} \end{aligned}\right\} \tag{13}$$

where $\gamma_{SS_1R_i}$ and $\gamma_{SS_2R_i}$ are the SINR at ith USAFR in order to eavesdrop the message of information signal of SS_1 and SS_2, respectively.

The ith USAFR amplifies the signal with a amplification factor $\left(\mu_i\right)$ [10] and broadcasts the information signal via wireless channel. It is clear that the energy of the broadcasting information signal at the relay should not be greater than the energy used by the relay to amplify and broadcast the information signal [10]. Mathematically it can be expressed as:

$$\left.\begin{aligned}\left|\mu_i y_R\right|^2\frac{T}{2} &= P_{SR_i}\frac{T}{2}\\ \left|\mu_i y_R\right|^2 &= P_{SR_i}\end{aligned}\right\} \tag{14}$$

where $\left|\mu_i y_R\right|^2\frac{T}{2}$ is energy of transmitted signal from relay considering an amplification factor μ_i and $P_{SR_i}\frac{T}{2}$ is the energy of transmitted signal from relay considering a transmit power of the relay as P_{SR_i}. An amplification factor of ith USAFR is μ_i and P_{SR_i} is the transmit power of ith relay as defined in Eq. (8), i.e., the selected relay uses the power P_{SR_i} to amplify and broadcast the information signal.

There are two cases of estimating the power of relay to amplify and broadcast the signal as: in case (1), when harvested power $\left(P_{H_i}\right)$ is less than the maximum allowable power $\left(P_{M_{SR}}\right)$ under cognitive constraint to amplify and broadcast the information signal. In case (2), when harvested power is greater or equal to the maximum allowable power $\left(P_{M_{SR}}\right)$ under cognitive constraint to amplify and broadcast the information signal. Mathematically, it can be expressed as:

Case (1), when $P_{H_i} < P_{M_{SR}}$

$$P_{SR_i} = P_{H_i} \tag{15}$$

Case (2), when $P_{H_i} \geq P_{M_{SR}}$

$$P_{SR_i} = P_{M_{SR}} \tag{16}$$

From Eq. (14), amplification factor (μ) can be expressed as:

$$\mu_i = \sqrt{\frac{P_{SR_i}}{(1-\beta)P_S\left(g_{SS_1R_i} + g_{SS_2R_i}\right) + N_0}} \tag{17}$$

In cases (1) and (2), μ_i can be expressed, respectively as:

$$\mu_i = \begin{cases} \sqrt{\frac{P_{H_i}}{(1-\beta)P_S\left(g_{SS_1R_i}+g_{SS_2R_i}\right)+N_0}}; & P_{H_i} < P_{M_{SR}} \\ \sqrt{\frac{P_{M_{SR}}}{(1-\beta)P_S\left(g_{SS_1R_i}+g_{SS_2R_i}\right)+N_0}}; & P_{H_i} \geq P_{M_{SR}} \end{cases} \tag{18}$$

Amplified and broadcasted information signal of relay can be expressed as:

$$x_{R_i} = \mu_i y_R \tag{19}$$

Now, the received signal at the receiver of the both the sources are respectively, given as:

$$\left.\begin{aligned} y_{SS_1} &= \mu_i y_R h_{R_iSS_1} + n_0, \\ y_{SS_2} &= \mu_i y_R h_{R_iSS_2} + n_0 \end{aligned}\right\} \tag{20}$$

At SS_2, to identify the signal and noise part, received information signal can be expressed as:

$$\begin{aligned} y_{SS_2} = {} & \underbrace{\mu_i\sqrt{(1-\beta)P_S}h_{SS_1R_i}h_{R_iSS_2}x_{SS_1}}_{Information\ Signal} + \underbrace{\mu_i\sqrt{(1-\beta)P_S}h_{SS_2R_i}h_{R_iSS_2}x_{SS_2}}_{Self\ interference\ Signal} \\ & + \underbrace{\mu_i n_0 h_{R_iSS_2} + n_0}_{Noise\ signal} \end{aligned} \tag{21}$$

Similarly at SS_1, to identify the signal and noise part, received information signal can be expressed as:

$$y_{SS_1} = \underbrace{\mu_i \sqrt{(1-\beta)P_S} h_{SS_1R_i} h_{R_iSS_1} x_{SS_1}}_{\textit{Self interference Signal}} + \underbrace{\mu_i \sqrt{(1-\beta)P_S} h_{SS_2R_i} h_{R_iSS_1} x_{SS_2}}_{\textit{Information Signal}} + \underbrace{\mu_i n_0 h_{R_iSS_1} + n_0}_{\textit{Noise signal}} \tag{22}$$

Both the sources know the self-interference signal which is detected with the help of perfect knowledge of CSI and can be subtracted [10]. From Eqs. (21) and (22), we can express the SINR at SS_1 and SS_2, respectively as:

$$\left.\begin{aligned} \gamma_{R_iSS_2} &= \frac{\mu_i^2(1-\beta)P_S g_{SS_1R_i} g_{R_iSS_2}}{\mu_i^2 N_0 g_{R_iSS_2} + N_0}, \\ \gamma_{R_iSS_1} &= \frac{\mu_i^2(1-\beta)P_S g_{SS_2R_i} g_{R_iSS_1}}{\mu_i^2 N_0 g_{R_iSS_1} + N_0} \end{aligned}\right\}. \tag{23}$$

Considering case (1) and putting amplification factor in Eq. (23), we re-express it as:

$$\left.\begin{aligned} \gamma_{R_iSS_2} &= \frac{\eta\beta(1-\beta)P_S g_{SS_1R_i} g_{R_iSS_2}}{\eta\beta g_{R_iSS_2} N_0 + (1-\beta)N_0 + \frac{N_0^2}{P_S\left(g_{SS_1R_i} + g_{SS_2R_i}\right)}}, \\ \gamma_{R_iSS_1} &= \frac{\eta\beta(1-\beta)P_S g_{SS_2R_i} g_{R_iSS_1}}{\eta\beta g_{R_iSS_1} N_0 + (1-\beta)N_0 + \frac{N_0^2}{P_S\left(g_{SS_1R_i} + g_{SS_2R_i}\right)}} \end{aligned}\right\}. \tag{24}$$

For low values of N_0, we can make approximation of expressions in Eq. (24) (i.e., SINR at both of the receiving stage of the sources) as:

$$\left.\begin{aligned} \gamma_{R_iSS_2} &\approx \frac{\eta\beta(1-\beta)P_S g_{SS_1R_i} g_{R_iSS_2}}{\eta\beta g_{R_iSS_2} N_0 + (1-\beta)N_0}, \\ \gamma_{R_iSS_1} &\approx \frac{\eta\beta(1-\beta)P_S g_{SS_2R_i} g_{R_iSS_1}}{\eta\beta g_{R_iSS_1} N_0 + (1-\beta)N_0} \end{aligned}\right\}. \tag{25}$$

For evaluating the SOP analytical expression, we utilize the approximated expressions given in Eq. (25).

3.3 Secrecy Capacity, Relay Selection and Secrecy Outage Probability (SOP) of Two-Way Communication

Capacities of links from ith USAFR to SS_2 and SS_1 can be expressed as:

$$\left.\begin{aligned} C_{R_iSS_2} &= \frac{1}{2}\log\left(1 + \gamma_{R_iSS_2}\right), \\ C_{R_iSS_1} &= \frac{1}{2}\log\left(1 + \gamma_{R_iSS_1}\right) \end{aligned}\right\}, \tag{26}$$

where $C_{R_iSS_2}$ and $C_{R_iSS_1}$ are the capacities from ith USAFR to SS_2 and SS_1, respectively. Next, capacities of channel links from sources to ith USAFR in order to eavesdrop the message of SS_1 and SS_2, respectively, can be expressed as:

$$\left.\begin{aligned} C_{SS_1R_i} &= \tfrac{1}{2}\log\left(1+\gamma_{SS_1R_i}\right), \\ C_{SS_2R_i} &= \tfrac{1}{2}\log\left(1+\gamma_{SS_2R_i}\right) \end{aligned}\right\}, \tag{27}$$

where $C_{SS_1R_i}$ and $C_{SS_2R_i}$ are the capacities of channel links from both the sources to ith USAFR in order to eavesdrop the message of SS_1 and SS_2, respectively. Further, secrecy capacity can be defined as the positive difference of capacity of legitimate link and that of ith USAFR link [3]. Mathematically, secrecy capacities of two-way communication can be defined individually as:

$$\left.\begin{aligned} C^{SEC}_{R_iSS_2} &= \tfrac{1}{2}\log\left(1+\gamma_{R_iSS_2}\right) - \tfrac{1}{2}\log\left(1+\gamma_{SS_1R_i}\right), \\ C^{SEC}_{R_iSS_1} &= \tfrac{1}{2}\log\left(1+\gamma_{R_iSS_1}\right) - \tfrac{1}{2}\log\left(1+\gamma_{SS_2R_i}\right) \end{aligned}\right\}, \tag{28}$$

where $C^{SEC}_{R_iSS_2}$ and $C^{SEC}_{R_iSS_1}$ are the secrecy capacities of link from SS_1 to SS_2 and from SS_2 to SS_1, respectively. Further, the above Eq. (28) is re-written as:

$$\left.\begin{aligned} C^{SEC}_{R_iSS_2} &= \left[\tfrac{1}{2}\log\left(\frac{1+\gamma_{R_iSS_2}}{1+\gamma_{SS_1R_i}}\right)\right]^+, \\ C^{SEC}_{R_iSS_1} &= \left[\tfrac{1}{2}\log\left(\frac{1+\gamma_{R_iSS_1}}{1+\gamma_{SS_2R_i}}\right)\right]^+ \end{aligned}\right\}, \tag{29}$$

where $[x]^+ = \max(x, 0)$. In Eq. (29), only individual secrecy capacities corresponding to information signal of SS_1 and SS_2 are defined, respectively. However, in this formulation, if one information is secure, it does not necessarily guarantee security of the other information. So, there is a need of global secrecy capacity which is defined as [18]:

$$C^{SEC}_{G_i} = \min\left(C^{SEC}_{R_iSS_2}, C^{SEC}_{R_iSS_1}\right), \tag{30}$$

where $C^{SEC}_{G_i}$ represents the global secrecy capacity via ith USAFR. The Eq. (30) explains that if minimum secrecy capacity of one of the two links is secure then it ensures that the other link have the comparably maximum secrecy capacity, which is also secured.

Relay selection is based on maximization of global secrecy rate via ith USAFR.

$$i^* = \arg\max_{1\leq i\leq N}\left(C^{SEC}_{G_i}\right), \tag{31}$$

where i^* is the optimal selected relay and N indicates the number of untrusted half-duplex AF relays present in the network. Now, secrecy outage probability (SOP) can be defined as:

$$P^{SEC}_{OUT} = P\left(\max_{1\leq i\leq N} C^{SEC}_{G_i} < R^{SEC}_{TH}\right) \tag{32}$$

where R_{TH}^{SEC} is the threshold secrecy rate of the secondary network. Each of the two-way communication links is i.i.d. Applying order statistics and re-organizing the Eq. (32) becomes:

$$\left.\begin{aligned} P_{OUT}^{SEC} &= P\left[\max_{1\le i\le N}\left\{\min\left(C_{R_iSS_2}^{SEC}, C_{R_iSS_1}^{SEC}\right)\right\} < R_{TH}^{SEC}\right] \\ &= \prod_{i=1}^{N}\left[P\left\{\min\left(C_{R_iSS_2}^{SEC}, C_{R_iSS_1}^{SEC}\right) < R_{TH}^{SEC}\right\}\right] \\ &= \left[1-\left\{1-\underbrace{P\left(C_{R_iSS_2}^{SEC} < R_{TH}^{SEC}\right)}_{I_1}\right\}\times\left\{1-\underbrace{P\left(C_{R_iSS_1}^{SEC} < R_{TH}^{SEC}\right)}_{I_2}\right\}\right]^N \\ &= \left[1-(1-I)^2\right]^N \end{aligned}\right\}, \tag{33}$$

here $I = I_1 = I_2$ due to independent and symmetry about relay. Considering the two cases of power allocation at the ith USAFR, we can estimate the I as:

$$\begin{aligned} I &= P\left(C_{R_iSS_2}^{SEC} < R_{TH}^{SEC}\right) \\ &= \underbrace{P\left\{\left(C_{R_iSS_2}^{SEC} < R_{TH}^{SEC}\right)|\left(P_{H_i} < P_{M_{SR}}\right)\right\}}_{I_3} P\left(P_{H_i} < P_{M_{SR}}\right) \\ &\quad + \underbrace{P\left\{\left(C_{R_iSS_2}^{SEC} < R_{TH}^{SEC}\right)|\left(P_{H_i} \ge P_{M_{SR}}\right)\right\}}_{I_4} P\left(P_{H_i} \ge P_{M_{SR}}\right) \end{aligned} \tag{34}$$

In case (1), when $P_{H_i} < P_{M_{SR}}$ then $P_{SR_i} = P_{H_i}$. Probability of event $P_{H_i} < P_{M_{SR}}$ can be expressed as:

$$P\left(P_{H_i} < P_R\right) = 1-\left(1+\frac{P_R}{\rho\beta P_S \Omega_{R_iSS_2}}\right)\exp\left(-\frac{P_R}{\rho\beta P_S \Omega_{R_iSS_2}}\right), \tag{35}$$

In this case, we assume that the $x = \left|h_{SS_2R_i}\right|^2$ and $y = \left|h_{R_iSS_2}\right|^2$. The I_3 in single integration from can be expressed as [6]:

$$\begin{aligned} I_3 &= P\left\{\left(C_{R_iSS_2}^{SEC} < R_{TH}^{SEC}\right)|\left(P_{H_i} < P_{M_{SR}}\right)\right\} \\ &= P\left\{\frac{1}{2}\log_2\left(1+\frac{\eta\beta(1-\beta)P_S xy}{\eta\beta N_0 y + N_0(1-\beta)}\Big/ 1+\frac{(1-\beta)P_S x}{(1-\beta)P_S y + N_0}\right) \le R_{TH}^{S}\right\} \\ &= P\{\nu(y)x < (\Delta-1)\} = 1-\frac{1}{\Omega_{R_iSS_2}}\int_{\theta_1}^{\infty}\exp\left(-\frac{(\Delta-1)}{\nu(y)\Omega_{SS_1R_i}}-\frac{y}{\Omega_{R_iSS_2}}\right)dy, \end{aligned} \tag{36}$$

where $y = \left|h_{R_iSS_2}\right|^2$, $\Delta = 2^{2R_{TH}^{SEC}}$, $v(y) = (1-\beta)\left\{\frac{\eta\beta P_S y}{\eta\beta y N_0 + N_0(1-\beta)} - \frac{\Delta P_S}{(1-\beta)P_S y + N_0}\right\}$, and $\theta_1 = \frac{\left(\frac{\Delta-1}{1-\beta}\right)+\sqrt{\left(\frac{\Delta-1}{1-\beta}\right)^2+\frac{4\Delta P_S}{N_0\eta\beta}}}{2\left(\frac{P_S}{N_0}\right)}$ In case (2), when $P_{H_i} \geq P_{M_{SR}}$ then $P_{SR_i} = P_{M_{SR}}$. Probability of this event is expressed as:

$$\begin{aligned} P\left(P_{H_i} \geq P_{M_{SR}}\right) &= 1 - P\left(P_{H_i} < P_{M_{SR}}\right) \\ &= \left(1 + \frac{P_{M_{SR}}}{\rho\beta P_S \Omega_{R_iSS_2}}\right)\exp\left(-\frac{P_{M_{SR}}}{\rho\beta P_S \Omega_{R_iSS_2}}\right). \end{aligned} \tag{37}$$

In this case, lower bound of SINR at SS_2, from Eq. (23) and with the help of Eq. (18), can be expressed as [4]:

$$\begin{aligned} &\gamma_{R_iSS_2} = \frac{P_{M_{SR}}}{(1-\beta)P_S + P_{M_{SR}}}\left[\frac{\left\{\frac{(1-\beta)P_S}{N_0}x\right\}\left\{\frac{(1-\beta)P_S+P_{M_{SR}}}{N_0}y\right\}}{1+\left\{\frac{(1-\beta)P_S}{N_0}x\right\}+\left\{\frac{(1-\beta)P_S+P_{M_{SR}}}{N_0}y\right\}}\right] \\ &\gamma_{R_iSS_2} < A_1 \min(Q, R); \gamma_{R_iSS_2} \geq \frac{A_1}{2}\min(Q, R) \\ &\text{where } Q = \frac{(1-\beta)P_S}{N_0}x; R = \frac{(1-\beta)P_S + P_{M_{SR}}}{N_0}y; A_1 = \frac{P_{M_{SR}}}{(1-\beta)P_S + P_{M_{SR}}} \end{aligned} \tag{38}$$

From Eq. (38), we can find the PDF of SINR at SS_2 as:

$$f_{\gamma_{R_iSS_2}}(\tau) \approx \frac{1}{\Omega_D}\exp\left(-\frac{\tau}{\Omega_D}\right); \tau \geq 0, \tag{39}$$

where $\Omega_D = \frac{A_1}{2}T_{QR}$; $A_1 = \frac{P_{M_{SR}}}{(1-\beta)P_S+P_{M_{SR}}}$; $T_{QR} = \frac{T_Q T_R}{T_Q+T_R}$; $T_Q = \frac{(1-\beta)P_S\Omega_{SS_1R_i}}{N_o}$; and $T_R = \frac{\left\{(1-\beta)P_S+P_{M_{SR}}\right\}\Omega_{R_iSS_2}}{N_o}$.

PDF of SINR at the selected *i*th USAFR from Eq. (13) can be expressed as:

$$\begin{aligned} f_{\gamma_{SS_1R_i}}(\upsilon) = \frac{N_0}{(1-\beta)P_S\Omega_{R_iSS_2}} \times &\frac{\exp\left(-\frac{N_0\upsilon}{(1-\beta)P_S\Omega_{R_iSS_2}}\right)}{\upsilon+1} \\ + &\frac{\exp\left(-\frac{N_0\upsilon}{(1-\beta)P_S\Omega_{R_iSS_2}}\right)}{(\upsilon+1)^2}; \ \upsilon \geq 0 \end{aligned} \tag{40}$$

The I_4 in single integration from can be expressed as:

$$
\begin{aligned}
I_4 &= P\left\{ \left(C^{SEC}_{R_i SS_2} < R^{SEC}_{TH} \right) | \left(P_{H_i} \geq P_{M_{SR}} \right) \right\} = P\{\tau < (\Delta(1+\upsilon) - 1)\} \\
&= \int_0^{\infty} \int_0^{(\Delta(1+\upsilon)-1)} f_{\gamma_{D_i}\gamma_{R_i}}(\tau, \upsilon) d\tau d\upsilon = \int_0^{\infty} \left\{ \int_0^{(\Delta(1+\upsilon)-1)} f_{\gamma_{R_i SS_2}}\left(\frac{\tau}{\upsilon}\right) d\tau \right\} f_{\gamma_{SS_1 R_i}}(\upsilon) d\upsilon \qquad , \\
&= \int_0^{\infty} \left[\upsilon \left\{ 1 - \exp\left(-\frac{(\Delta(1+\upsilon)-1)}{\Omega_D \upsilon} \right) \right\} \left\{ A_2 \frac{\exp\left(-A_2 \upsilon\right)}{\upsilon + 1} + \frac{\exp\left(-A_2\upsilon\right)}{(\upsilon+1)^2} \right\} \right] d\upsilon
\end{aligned}
\tag{41}
$$

where $A_2 = \frac{N_O}{(1-\beta)P_S \Omega_{SS_1 R_i}}$. We can evaluate the I from Eqs. (34) (35) and (37), and the expressions of I_3 and I_4 given in Eqs. (36) and (41), respectively. The I of Eq. (33) [this I is also expressed in Eq. (34)] can be expressed as:

$$
\begin{aligned}
I = I_3 &\left\{ 1 - \left(1 + \frac{P_R}{\rho\beta P_S \Omega_{R_i SS_2}} \right) \exp\left(-\frac{P_R}{\rho\beta P_S \Omega_{R_i SS_2}} \right) \right\} \\
+ I_4 &\left\{ \left(1 + \frac{P_R}{\rho\beta P_S \Omega_{R_i SS_2}} \right) \exp\left(-\frac{P_R}{\rho\beta P_S \Omega_{R_i SS_2}} \right) \right\}
\end{aligned}
\tag{42}
$$

where I_3 and I_4 are given in Eqs. (36) and (41), respectively. Next, we plug I in Eq. (33) to obtain final expression of SOP which is given as:

$$
P^{SEC}_{out} = \left[1 - (1 - I)^2\right]^N \tag{43}
$$

The expression of SOP in Eq. (42) is in single integration form which can be solved by numerical method of integration.

Table 1 Name of different network parameters with their symbols and numerical values

Network parameters	Numerical values
Peak transmit power of SNs $\left(P_{PK}\right)$	0 dBW, 5 dBW
Primary transmit power $\left(P_P\right)$	5 dBW
Threshold outage rate of PU-RX $\left(R_P\right)$	0.2 b/s/Hz
Outage probability of PU-RX $\left(P^P_{Out} = \Theta\right)$	0.2
Energy conversion efficiency (η)	0.7
Fraction of received energy (β)	0.65 for $P_{PK} = 0$ dBW and 0.7 for $P_{PK} = 5$ dBW
AWGN power $\left(N_0\right)$	10^{-2}W
Threshold secrecy rate $\left(R^{Sec}_{TH}\right)$	1 b/s/Hz
Channel mean power of all links $\left(\Omega_j\right)$	0.5
Number of relays (N)	5

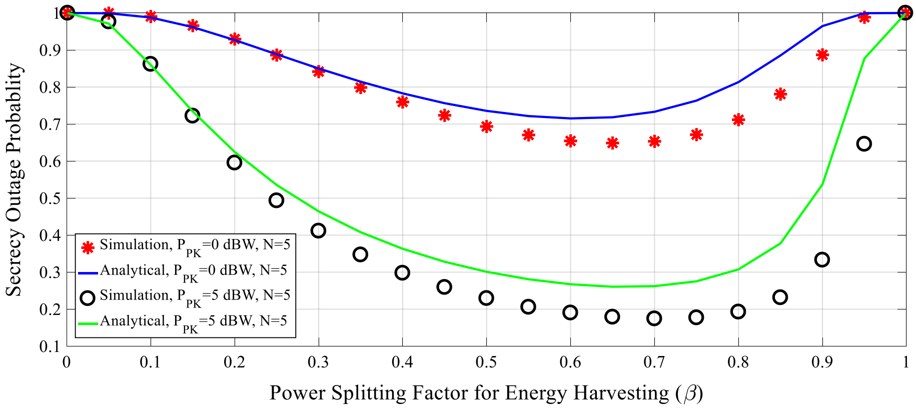

Fig. 3 SOP versus β for different values of P_{PK}. There are different optimal values of β for different values of P_{PK}

4 Numerical Results

In this Section, MATLAB based simulation results has been shown for secured two-way communication via the multiple half-duplex untrusted AF relays. We also have shown the approximated numerical results which closely match with simulated results. Assigned numerical values are given in Table 1.

4.1 Impact of Fraction of Received Energy (β) at Relay on SOP

Figure 3 shows the performance in terms of SOP with respect to β. As β increases, harvested energy increases as per Eq. (10). Harvested power corresponding to harvested energy also increases as per Eq. (11). This increased harvested power increases the signal quality at respective source destination. On the other hand, the information signal available for eavesdropping the message at the untrusted relay becomes poor with increase in β. Thus information signal strength increases at both the source destinations and decreases at the selected untrusted relay with increase in β. This leads to reduction in SOP with increase in β. However, after an optimal value of β, untrusted relay harvests more energy. The high value of harvested power corresponding to harvested energy can not increase the signal quality at the respective source destinations as the received signal strength reduces at the relay due to allocation of higher fraction of signal power for harvesting at relay. Due to more fraction of the information signal used in the harvesting, signal becomes noisy, and after amplification signal becomes comparably noisier which degrades the channel capacity at both the source destinations. Thus, SOP decreases with increase in β after optimal value of it. We obtain the two optimal values of β corresponding to different values of the peak transmit power. It is for as peak transmit power $\left(P_{PK}\right)$ of 0 dBW and 0.7 for P_{PK} of 5 dBW.

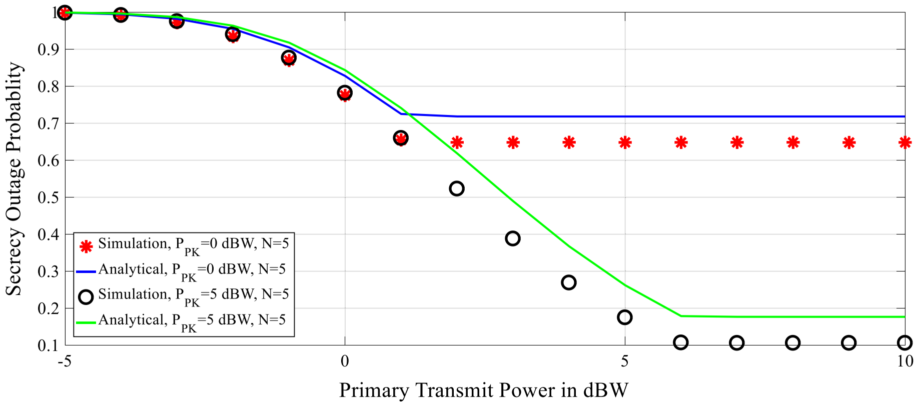

Fig. 4 SOP versus P_P for different values of P_{PK}

4.2 Impact of Transmit Power of Primary Network and Peak Transmit Power of Both of the Secondary Sources on SOP

Figure 4 shows the SOP variation with P_P and P_{PK} . Increase in P_P, assigned power to secondary nodes increases for a given outage constraint of primary network. With increase in signal strength at the selected relay, harvested power also increases for a particular value of β. Combined effect of increase in harvested power and power under cognitive constraint increases the signal strength at the receiving source destination. Thus, SOP decreases with increase in P_P. However, there is no effect on SOP for large value of P_P due to peak transmit power constraint and we obtain the floor. Increase in peak transmit power increases the transmit power of information signal. Thus, SOP also decreases with increase in peak transmit power. For evaluating analytical expression, the lower bound of SINR [as given in Eq. (38)] at the respective source destination is used. Therefore, SOP value in an analytical results for a particular value of P_P is some greater than the SOP value in a simulated results for that particular value of P_P. But, the nature of curves in the graphs are same.

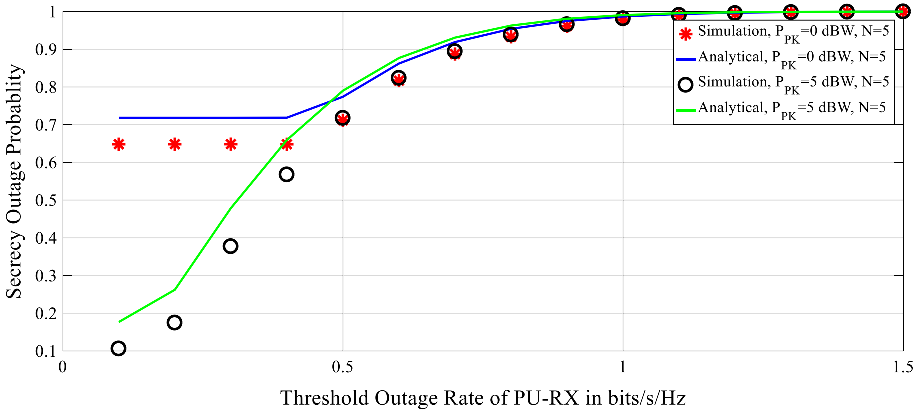

Fig. 5 SOP versus R_P for different values of P_{PK}

4.3 Impact of Threshold Outage Rate of PU-RX on SOP

Figure 5 shows the SOP versus R_P for different values of peak transmit power. Increase in R_P decreases the assigned power to secondary nodes as per Eqs. (4) and (7). Signal with low transmit power is received by relay in poor strength. Corresponding harvested power decreases with increase in R_P. Further, power assigned to relay under cognitive constraint decreases with increase in R_P. Next, combined effect of low harvested power and low assigned power provides the poor channel capacity to respective source destination. Decreasing rate of channel capacities at respective source destination dominates over the decreasing rate of channel capacities at the selected relay. Thus secrecy rate decreases and performance in terms of SOP increases.

4.4 Impact of Number of Relays on SOP

Figure 6 shows the SOP versus number of relays. If number of relay increases then secrecy performance increases even if the relays are untrusted. However it is found in [4] and [5], if number of untrusted relays increases, then performance reduces because all relays are in active stage in first time slot. They can receive the information signal and try to eavesdrop the message. But, in our case, only selected relay is in active stage and all other relays are in idle stage, i.e., non-selected relays do not participate in signal processing, in the first time slot and in the second time slot. In this case diversity in number of relays is preserved and always provide best strength of signal to respective source destination. Thus, secrecy rate increases with increase in number of relays and SOP decreases.

4.5 Imapct of Channel Mean Power of Links Between the Sources and the Selected Relay $\left(\Omega_{SS_1R_i}, \Omega_{SS_2R_i}\right)$ on SOP

Figure 7 shows SOP versus channel mean power of links between the sources and the selected relay $\left(\Omega_{SS_1R_i}, \Omega_{SS_2R_i}\right)$. As the channel mean power increases, strength of the

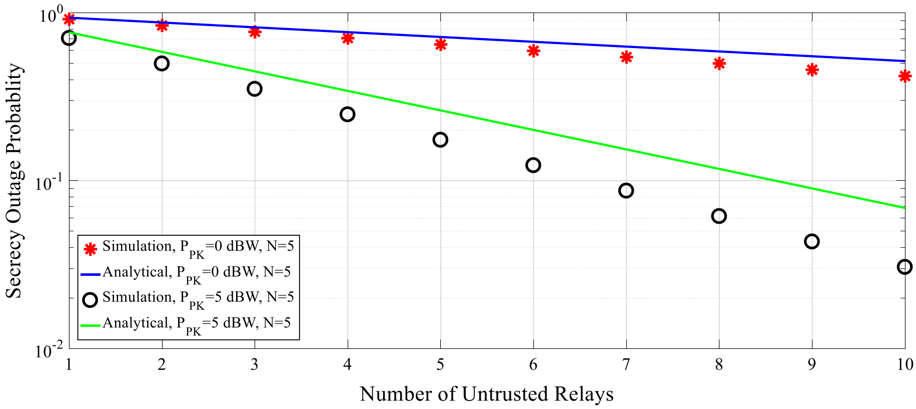

Fig. 6 SOP versus N for different values of P_{PK}

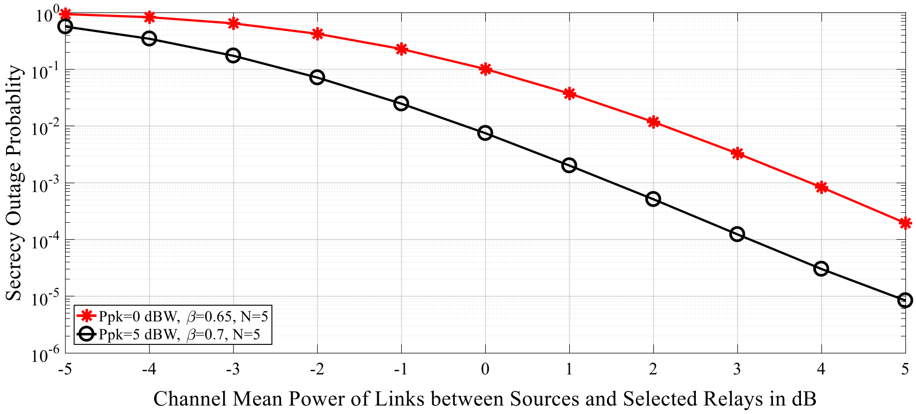

Fig. 7 SOP versus channel mean power of links between the sources and the selected relay $\left(\Omega_{SS_1R_i}, \Omega_{SS_2R_i}\right)$ for different values of P_{PK}

information signals corresponding to both the sources also increases. But due to jamming nature of the information signals to each other at the selected untrusted relay, the selected untrusted relay receives the signal strength with no further improvement. Thus, the selected untrusted relay is unable to eavesdrop the message successfully. On the other hand, after amplification and broadcasting by the selected relay, respective destination sources receive the signal in better strength with increase in channel mean power. Both the sources detects and removes the own signal from the received signal on the basis of CSI. After removal of own signals from the received signal, both the sources are able to decode the information signal of each other.

5 Conclusion

The SOP of CCRN has been evaluated for a two-way communication via multiple half-duplex energy harvesting untrusted AF relays. We obtain optimal values of fraction of received energy at which SOP becomes minimum under a given scenario of primary transmit power and peak transmit power of secondary nodes. For a particular values of outage probability of primary network, SOP decreases with increase in primary transmit power. But, SOP increases with increase in threshold outage rate of PU-RX. Diversity in number of relays provide the benefit in performance even if relays are untrusted. As the number of relays increases, SOP decreases. Next, increase in channel mean power of links between the sources and the selected relay provides better secrecy of the messages. Further, both the sources can share the confidential information via untrusted relays maintaining a desired level of SOP without affecting the quality of service of primary network in terms of outage.

Acknowledgements This research is supported by the Department of Electronics and Information Technology, Ministry of Communications and IT, Government of India under the Visvesvaraya Ph.D. Scheme administered by Media Lab Asia with Grant No. PhD-MLA/4(29)/2015-16.

References

1. Barros, J., & Rodrigues, M. D. (2006) Secrecy capacity of wireless channels. In *2006 IEEE international symposium on information theory* (vol. 1, pp. 356–360).
2. Liu, Y., Li, J., & Petropulu, A. P. (2013). Destination assisted cooperative jamming for wireless physical-layer security. *IEEE Transactions on Information Forensics and Security*, *8*(4), 682–694.
3. Leung-Yan-Cheong, S. K., & Hellman, M. E. (1978). The Gaussian wire-tap channel. *IEEE Transactions on Information Theory*, *24*(4), 451–456.
4. Sun, L., Zhang, T., Li, Y., & Niu, H. (2012). Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes. *IEEE Transactions on Vehicular Technology*, *61*(8), 3801–3807.
5. Sun, L., Ren, P., Du, Q., Wang, Y., & Gao, Z. (2015). Security-aware relaying scheme for cooperative networks with untrusted relay nodes. *IEEE Communications Letters*, *19*(3), 463–466.
6. Kalamkar, S. S., & Banerjee, A. (2017). Secure communication via a wireless energy harvesting untrusted relay. *IEEE Transactions on Vehicular Technology*, *66*(3), 2199–2213.
7. Nguyen, B. V., & Kim, K. (2015). Secrecy outage probability of optimal relay selection for secure AnF cooperative networks. *IEEE Communications Letters*, *19*(12), 2086–2089.
8. Pan, G., Tang, C., Li, T., & Chen, Y. (2015). Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems. *IEEE Transactions on Communications*, *63*(9), 3423–3433.
9. Xiong, J., Cheng, L., Ma, D., & Wei, J. (2016). Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems. *IEEE Transactions on Vehicular Technology*, *65*(9), 7274–7284.
10. Yao, R., Xu, F., Mekkawy, T., & Xu, J. (2016). Optimised power allocation to maximise secure rate in energy harvesting relay network. *Electronics Letters*, *52*(22), 1879–1881.
11. Son, P. N., & Kong, H. Y. (2015). Cooperative communication with energy-harvesting relays under physical layer security. *IET Communications*, *9*(17), 2131–2139.
12. Mamaghani, M. T., Kuhestani, A., & Wong, K. (2018). Secure two-way transmission via wireless-powered untrusted relay and external jammer. *IEEE Transactions on Vehicular Technology*, *67*(9), 8451–8465.
13. Nasr, O., El-Rabaie, S., Sakran, H., El-Azm, A. A., & Shokair, M. (2012). Proposed relay selection scheme for physical layer security in cognitive radio networks. *IET Communications*, *6*(16), 2676–2687.
14. Tang, C., Pan, G., & Li, T. (2014). Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels. *IEEE Wireless Communications Letters*, *3*(6), 609–612.
15. Zou, Y., Li, X., & Liang, Y.-C. (2014). Secrecy outage and diversity analysis of cognitive radio systems. *IEEE Journal on Selected Areas in Communications*, *32*(11), 2222.
16. Tran, H., Zepernick, H. J., & Phan, H. (2013). Cognitive proactive and reactive df relaying schemes under joint outage and peak transmit power constraints. *IEEE Communications Letters*, *17*(8), 1548–1551.
17. Zhong, B., & Zhang, Z. (2017). Secure full-duplex two-way relaying networks with optimal relay selection. *IEEE Communications Letters*, *XX*(X), 1–1.
18. 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 Transactions on Vehicular Technology*, *66*(6), 5462–5466.
19. Khandaker, M. R. A., Wong, K.-K., & Zheng, G. (2017). Truth-telling mechanism for two-way relay selection for secrecy communications with energy-harvesting revenue. *IEEE Transactions on Wireless Communications*, *16*(5), 1–1.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Shashibhushan Sharma He has received his B.E. degree in Electronics and Communication Engineering from University of Rajiv Gandhi Proudyogiki Vishwavidyalaya, India in 2011 and M.Tech. degree in Telecommunication Engineering from the National Institute of Technology, Durgapur, India in 2015. He is Pursuing Ph.D. in Department of Electronics and Communication Engineering, National Institute of Technology Durgapur, India. His research area are Physical layer security, Cognitive radio network, Two-way communication with half and full duplex relay and Energy harvesting.

Dr. Sanjay Dhar Roy (M'07) was born in Balurghat, West Bengal, India, in 1974. He received the B.E. (Hons.) degree in electronics and telecommunication engineering from Jadavpur University, Kolkata, India, in 1997, and the M.Tech. degree in telecommunication engineering and the Ph.D. degree in wireless communications from the National Institute of Technology (NIT) Durgapur, Durgapur, India, in 2008 and 2011, respectively. He was with the Koshika Telecom Ltd., from 1997 to 2000. After that, in 2000, as a Lecturer, he joined the Department of Electronics and Communication Engineering, NIT Durgapur, where he is currently an Assistant Professor. As of today, he has published 100 research papers in various journals and conferences. His research interests include radio resource management, handoff, femtocell, D2D communication, and cognitive radio networks. He is a reviewer of IET Communications, Electronics Letters, and Journal of PIER, IJCS, Wiley.

Dr. Sumit Kundu (SM'13) received the B.E. (Hons.) degree in Electronics and Communication Engineering in 1991 from the National Institute of Technology (NIT), Durgapur, Durgapur, India, and the M.Tech. degree in telecommunication systems engineering and the Ph.D. degree in wireless communication engineering from IIT Kharagpur, Kharagpur, India. Since 1995, he has been with the faculty of the Department of Electronics and Communication Engineering, NIT, Durgapur, where he is currently a Full-Time Professor. As of today, he has published more than 150 research papers in various journals and conferences. His research interests include wireless ad hoc and sensor networks, cognitive radio networks, cooperative communication, energy harvesting, and physical layer security in wireless networks. He is a reviewer of several IEEE and Elsevier journals.