Journal of Engineering Science and Technology
Vol. 13, No. 12 (2018) 4039- 4052

SECURE PERFORMANCE ANALYSIS OF ADAPTIVE ENERGY HARVESTING ENABLED RELAYING NETWORKS

NGUYEN XUAN VIET[1], DAO THI THU THUY[2], LE SI PHU[3],
NGUYEN HONG NHU[3], NGO TIEN HOA[1],
DINH-THUAN DO[2,*], MIROSLAV VOZNAK[3]

[1]Faculty of Electrical and Electronics Engineering,
Ho Chi Minh City University of Technology and Education, Vietnam
[2]Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Vietnam
[3]VSB Technical University of Ostrava, Ostrava, Poruba, Czech Republic
*Corresponding Author: dodinhthuan@iuh.edu.vn

Abstract

In this paper, the impact of the jamming signal on the secrecy performance of Energy Harvesting (EH) enabled dual-hop amplify-and-forward relaying network is investigated. First, the security outage probability analysis is studied for conventional networks under a single passive eavesdropper attack. Then, the outage performance analysis in two cases regarding energy harvesting is investigated. Moreover, the proposed work enhances Physical Layer (PHY) security performance of two-hop relaying model using Cooperative Jamming Dual-Hop Techniques (CJDH). For this purpose, new closed-form expressions are derived for the outage probability of CJDH model in the presence of interference over Rayleigh fading channels. A power allocation optimization problem for energy harvesting protocol is formulated and solved for enhancing the system security. The derived analytical formulas herein are supported by numerical and simulation results to clarify the main contributions of the paper.

Keywords: Cooperative jamming dual hop, Outage probability, Physical layer (PHY), Security.

1. Introduction

The advantage from the joint advantages of relaying technique and information-theoretic security by describing the features of physical channels in wireless communication, Physical-Layer (PHY) security in relaying has attracted attention significantly in literature. Sending jamming signals to prevent the eavesdroppers with the help of extra cooperative relays is an effective way to ensure dependable communication. This is also referred to Cooperative Jamming (CJ) [1-4]. We assume the situation that relays either help to transfer useful information or to broadcast jamming signals to prevent eavesdroppers, a closed-form expression for SOP is derived by the authors in [1] as well as two relays and jammer selection schemes for SOP minimization are suggested.

As explained by Ding et al. [2], opportunistic CJ and relay chatting networks were suggested by using OP as the metric for performance judging. According to Luo et al. [3], the secrecy rate was proposed for optimal jamming noise structure. Wang et al. [4] presented a two-way relay network with a single antenna, which offered a novel hybrid cooperative beamforming and jamming scheme to guarantee the PHY security when an eavesdropper intends to be overhearing the information. Artificial Noise (AN), which is used to only interfere the eavesdroppers [5], can be created by the systems equipped with multiple antennas to degrade the decoding capability of eavesdroppers [5-9] when cooperative relays are unavailable. Based on a study by Liu et al. [6], a lower bound on the ergodic secrecy capacity for AN scheme was presented for a Multiple-Input Multiple-Output (MIMO) system when perfect channel state information is available at the transmitter and the receiver, respectively.

We assume that a multi-tier variety cellular system in which, the positions of the base stations, the authorized users and the eavesdroppers are built as a Poisson point process. Wang et al. [7] investigated the PHY security in terms of an offered mobile association policy, connection and secrecy probabilities of the AN-aided secrecy transmission, the network-wide secrecy throughput and secrecy throughput minimization for each user. Wang et al. [8] proposed a framework for AN, which was assisted to secure MIMO system in the existing of an eavesdropper with multiple antennas and then a closed-form analytical expression is derived for ergodic secrecy rate. According to Wang et al. [9], the definition of the secrecy outage zone was introduced and then derived the analytical expression for SOP in AN-aided secure transmission networks with a massive-antenna transmitter through Rician fading channels.

Energy harvesting in wireless cellular networks is a basis of emerging 5G cellular networks pointing to "cut the last wires" of the available wireless devices [10-13]. In particular, energy harvesting has a significant role to attract subscribers since it assists mobility and connectivity anywhere and anytime, which is one of the key visions of rising 5G networks. Until now, energy harvesting for wireless communication systems mainly considered surrounding energy sources (e.g., solar, motion and vibration, temperature, wind, thermoelectric effects, interference from Radio Frequency (RF) sources, etc.

According to Kalamkar and Banerjee [14], it inspired by the advantage of CJDH system model and novel results, which motivate us to show comparison study with non-energy harvesting case and this paper further studies secure outage and throughput performance.

2. System Model

2.1. Destination-assisted jamming and channel model information broadcast

As shown in Fig. 1, this CJDH including a source (*S*) communicates with a destination (*D*) through an AF energy harvesting relay (*R*). Despite information cooperation of the relay, the source and destination nodes wish to keep the information from the relay secretly. The destination broadcasts a jamming signal to the relay while the source is transmitting the information to the relay to maintain the confidentiality of the source information. Each node operates in a half-duplex mode and has a single antenna. There is no direct link between *S* and *D*. Let us denote the coefficient of the channel between nodes a and b by g_{ab}. We assume a quasi-static block-fading Rayleigh channel between two nodes. That is, the channel remains constant over a slot-duration of T during which, *S* transmits to *D* via *R*. The gain of channel power is given by $|g_{ab}|^2$, which has an exponential distribution with mean Ω_{ab} , i.e.:

$$f_{|g_{ab}|^2}(x) = \frac{1}{\Omega_{ab}} e^{-\frac{x}{\Omega_{ij}}}, \quad x > 0, \tag{1}$$

In this work, the source is considered to have no Channel State Information (CSI), while the CSI of S-R and R-D channels are available at the relay and destination, respectively.

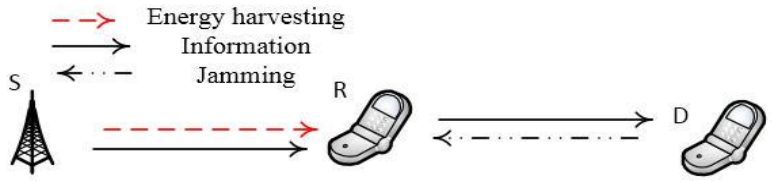

Fig. 1. System model including a source (*S*) and a destination (*D*) via an energy harvesting untrusted relay (*R*) with destination-assisted jamming.

2.2. Energy harvesting and information processing model

The energy, which was harvested by the untrusted relay from the received RF signals uses to forward the source's information to the destination. The received power must be greater than the minimum threshold power γ_H to kick off the energy harvesting circuitry at the relay. Assuming that the relay has no other energy source and it uses the harvested energy completely for the transmission. Moreover, the harvested energy considered as the power consumed by transmit or receive circuitry of the relay is compared to the power, which was required for the transmission. We start using two different receiver architectures based policies at the relay to separate harvest energy from the received RF signals and process the information.

- Power Splitting (PS) policy: The relay utilizes a part of the received power to harvest the energy and the residual part for the information processing.
- Time Switching (TS) policy: The relay switches between the energy harvesting and the information processing, meaning that the relay uses a fraction of the time of a slot to harvest the energy and the residual time for the information processing and relaying.

Notice that the relay may try to decode the source information with the power, which was used for the information processing.

3. Power Splitting Policy based Relaying

Figure 2 illustrates the PS policy based relaying protocol, where the communication in source-to-destination occurs in a slot of duration *T*. Two phases of equal duration T/2 separate the slot. In the first phase, the source transfers information to the relay with power P_S. At the same time, the destination broadcasts a jamming signal with power P_D to the relay to keep the confidentiality of the source information from the relay. The relay uses a fraction of the received power for energy harvesting and the rest $(1-\beta_i),\ i=1,2$ part for information processing, where $0 \le \beta_i \le 1$. By using the harvested energy, in the second phase, the relay forwards the received information to the destination after amplification.

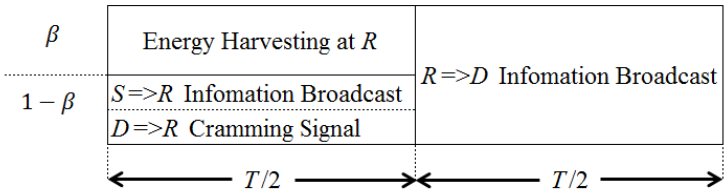

Fig. 2. Adaptive power splitting policy for the secure communication via an energy harvesting untrusted relay.

3.1. Energy harvesting at relay

In the above PS policy, the relay harvests energy E_H given as

$$E_H = E_1 + E_2, \tag{2}$$

where $E_1 = \eta\beta_1 P_S|g_{SR}|^2(T/2), E_2 = \eta\beta_2 P_S|g_{SR}|^2(T/2)$ and η denotes the energy conversion efficiency factor with $0 < \eta \le 1$, which depends on the energy harvesting circuitry of the relay. The terms of $P_S|g_{SR}|^2$ and $P_D|g_{DR}|^2$ in Eq. (2) define the power obtained at the relay due to the information signal from the source and the jamming signal from the destination, respectively. In the second phase of duration *T*/2, the transmit power of relay, which forwards the information to destination is given as:

$$P_H = \frac{E_H}{T/2} = \eta(\beta_1 P_S|g_{SR}|^2 + \beta_2 P_D|g_{DR}|^2) \tag{3}$$

3.2. Information processing and relaying protocol

In the first phase, the received signal y_R for the information processing at the relay can be expressed as:

$$y_R = \sqrt{(1-\beta_1)P_S}g_{SR}x_S + \sqrt{(1-\beta_2)P_D}g_{DR}x_D + w_R \tag{4}$$

where x_S defines the source information with unit power, x_D defines the unit power of the jamming signal sent by the destination and w_R is the Additive White Gaussian Noise (AWGN) at the relay. We assume that the power splitting does not affect the noise power. Based on the received signal y_R in Eq. (4), the relay may try to decode the source message x_S. We have the SNR expression at the relay as:

$$SNR_R = \frac{(1-\beta_1)P_S|g_{SR}|^2}{(1-\beta_2)P_D|g_{DR}|^2+\sigma^2}, \tag{5}$$

where σ^2 is the noise power of AWGN w_R.

In the second phase, the relay amplifies the received signal by a factor ξ and the transmit signal at *R* and such amplified factor is expressed respectively by:

$$x_R = Gy_R \tag{6}$$

$$G = \sqrt{\frac{P_H}{(1-\beta_1)P_S|g_{SR}|^2+(1-\beta_2)P_D|g_{DR}|^2+\sigma^2}} \tag{7}$$

Then, we replace Eq. (4) in Eq. (6) and then use Eq. (6) to express the received signal $y_D^{'}$ at the destination as:

$$\begin{aligned} y_D^{'} &= g_{RD}x_R + w_D \\ &= G\sqrt{(1-\beta_1)P_S}g_{SR}g_{RD}x_S \\ &\qquad +G\sqrt{(1-\beta_2)P_D}g_{RD}g_{DR}x_D + Gg_{RD}w_R + w_D, \end{aligned} \tag{8}$$

where w_D denotes the AWGN at the destination with power σ^2. Since x_D denotes the jamming signal sent by the destination itself to the relay in the first phase, the destination can eliminate the term $G\sqrt{(1-\beta_2)P_D}g_{RD}g_{DR}w_D$ from Eq. (8) and decodes the source information from the rest of the received signal. Thus, the resultant received signal y_D at the destination changes into:

$$y_D = G\sqrt{(1-\beta_1)P_S}g_{SR}g_{RD}x_S + Gg_{RD}w_R + w_D \tag{9}$$

Finally, we replace P_H from Eq. (3) in Eq. (7) and then use ξ from Eq. (7) in Eq. (9), we get:

$$\begin{aligned} y_D = &\frac{\sqrt{\eta\beta_1P_S\left((1-\beta_1)P_S|g_{SR}|^2+(1-\beta_2)P_D|g_{DR}|^2\right)}g_{SR}g_{RD}x_S}{\sqrt{(1-\beta_1)P_S|g_{SR}|^2+(1-\beta_2)P_D|g_{DR}|^2+\sigma^2}} \\ &+\frac{\sqrt{\eta(\beta_1P_S|g_{SR}|^2+\beta_2P_D|g_{DR}|^2)}g_{RD}w_R}{\sqrt{(1-\beta_1)P_S|g_{SR}|^2+(1-\beta_2)P_D|g_{DR}|^2+\sigma^2}}+w_D \end{aligned} \tag{10}$$

The first term on the right-hand side of Eq. (10) represents the signal part, while the second and third terms equal to the entire received noise at the destination. Then, the approximate SNR at the destination at high SNR can be written as

$$SNR_D = \frac{\eta\beta_1P_S|g_{SR}|^2|g_{RD}|^2}{\eta\beta_1|g_{RD}|^2\sigma^2+\sigma^2(1-\beta_1)} \tag{11}$$

3.3. Secure communication via an untrusted relay

When the relay is assumed as the unreliable channel, we have the immediate secrecy rate R_{sec} of the relay-assisted communication as:

$$\begin{aligned} R &= \frac{1}{2}[log_2(1+SNR_D) - log_2(1+SNR_R)]^+ \\ &= \tfrac{1}{2}\left[log_2\left(\frac{1+SNR_D}{1+SNR_R}\right)\right]^+ \end{aligned} \tag{12}$$

where $[x]^+ = max(x, 0)$. The coefficient $\frac{1}{2}$ is the effective communication time between the source and the destination.

Secrecy outage probability:

The secrecy outage probability is an essential measure of the secrecy performance. For the rest of the next step, we consider $P_S = P_D = P$ for a simple analytical result.

It controls directly the probability of getting a target secrecy rate. By giving the energy harvesting circuitry of the relay is active, we can express the secrecy outage probability as

$$OP_{out} = Pr(Rth_{sec}()) \tag{13}$$

where $Pr(.)$is the probability, R_{sec} is the instantaneous secrecy rate given by Eq. (12) and R_{th} represents the target secrecy rate. Then, replacing SNR_R from Eq. (5) and SNR_D from (11), we can rewrite Eq. (13) as

$$OP_{out} = Pr\left(\frac{1+SNR_D}{1+SNR_R} < 2^{2R_{th}}\right) \tag{14}$$

It can be further expressed the secrecy outage probability in analytics (14) as given in Proposition 1. For simplicity, it can be assumed that $\beta_1 = \beta_2 = \beta$

Theory 1. The secrecy outage probability for PS policy can be approximately expressed at high SNR as [14].

$$OP_{out} \approx 1 - \frac{1}{\Omega_{RD}} \int_0^{\infty} e^{-\frac{\varepsilon-1}{Q\Omega_{SR}} - \frac{x}{\Omega_{RD}}} dx, \tag{15}$$

where $\varepsilon = 2^{2R_{th}}$ and

$$Q = \frac{(1-\beta)\eta\beta x}{\frac{\sigma^2}{P}(\eta\beta x + (1-\beta))} - \frac{\varepsilon}{x}. \tag{16}$$

Proof: (See Appendix A).

Equation (15) is obtained by using the high SNR approximation of the received SNR at the destination, which can be given as:

$$SNR_D \approx \frac{\eta\beta(1-\beta)P|g_{SR}|^2|g_{RD}|^2}{\sigma^2(\eta\beta|g_{RD}|^2 + (1-\beta))}. \tag{17}$$

As aforementioned in Section 2.2, the received power at the relay must be greater than the minimum power threshold γ_H to activate the energy harvesting circuitry. By using channel reciprocity on the relay-destination connection, we can express the received power P_R at the relay as:

$$P_R = (P|g_{SR}|^2 + P|g_{RD}|^2). \tag{18}$$

If the received power P_R is smaller than the power threshold γ_H, the energy harvesting circuitry at the relay will remains inactive, leading to the power outage. The next opinion gives the expression for the power outage probability $Pr(P_R < \gamma_H)$.

Theory 2. We have the power outage probability $OP_{p,out}$as follows:

$$OP_{p,out} = \begin{cases} 1 - \frac{\Omega_{SR}}{\Omega_{SR}-\Omega_{RD}} e^{-\frac{\gamma_H}{P\lambda_{SR}}} \\ -\frac{\Omega_{RD}}{\Omega_{RD}-\Omega_{SR}} e^{-\frac{\gamma_H}{P\lambda_{RD}}}, & \text{if } \Omega_{SR} \neq \Omega_{RD} \\ \Phi\left(2, \frac{\gamma_H}{P\Omega_{SR}}\right), & \text{if } \Omega_{SR} = \Omega_{RD}, \end{cases} \quad (19)$$

where $\Phi(a,t) = \int_0^t x^{a-1}e^{-x}dx$ represents the lower incomplete Gamma function.

Proof: (See Appendix B)

For a constrained energy unreliable relay, a secrecy outage can also happen if the power received by the relay is not enough to operate the energy harvesting circuitry. Thus, combining with Eq. (15), we get the overall secrecy outage probability OP_{out}^{S} as:

$$OP_{out}^{S} = OP_{p,out} + \left(1 - OP_{p,out}\right)OP_{out}, \quad (20)$$

where OP_{out} is given by Eq. (15).

The secrecy throughput can be expressed as:

$$T = (1 - OP_{out}^{S})R \quad (21)$$

To investigate the optimal power splitting coefficients, the optimal problem can be solved as:

$$\min_{\alpha} OP_{out}^{S} = argmin\, O\, P_{out}^{S} = \alpha^{*} \quad (22)$$

Unfortunately, the closed-form expression for the optimal fraction is hard to obtain and we look for an optimal value in the simulation section.

4. Non-Energy Harvesting at Relay

To find a benchmark for energy harvesting scheme presented in the previous section, we further examine the scenario when relay has individual power without harvesting wireless energy. It is expected that strong power leads to better outage performance. In this section, we consider two-hop relaying in case of non-Energy Harvesting (non-EH) at the relay, refer to Fig. 3.

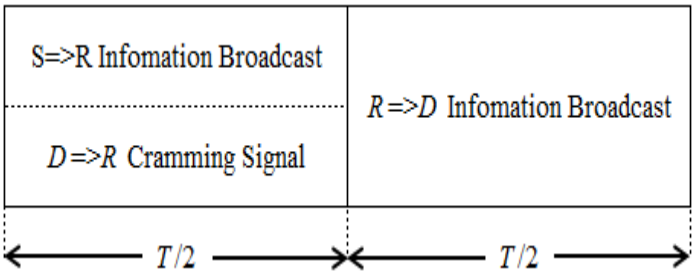

Fig. 3. Two-way relaying with non-EH.

The received signal at the relay *R* in phase 1 can be expressed by:

$$y_R = \sqrt{P_S}g_{SR}x_S + \sqrt{P_D}g_{DR}x_D + w_R \quad (23)$$

In this scenario, the SNR at *R* can be formulated as:

$$SNR_R = \frac{P_S|g_{SR}|^2}{P_D|g_{DR}|^2+\sigma^2} \tag{24}$$

with $\sigma^2$is noise power following AWGN of w_R

Next, the transmit signal at node *R* in phase 2:

$$x_R = G.y_R \tag{25}$$

with the amplifying factor is denoted as $G = \sqrt{\frac{P_R}{P_S|g_{SR}|^2+P_D|g_{DR}|^2+\sigma^2}}$

The received signal at node *D* in phase 2 can be shown as:

$$\begin{aligned} y_D^{'} &= g_{RD}x_R + w_D \\ &= g_{RD}Gy_R + w_D \\ &= G\sqrt{P_S}g_{SR}g_{RD}x_S + G\sqrt{P_D}g_{RD}g_{DR}x_D \\ &\qquad + Gg_{RD}w_R + w_D \end{aligned} \tag{26}$$

Similarly, the received signal $y_D$at *D* will become

$$y_D = G\sqrt{P_S}g_{SR}g_{RD}x_S + Gg_{RD}w_R + w_D \tag{27}$$

Substituting *G* into the above expression, we obtain:

$$\begin{aligned} y_D &= \frac{\sqrt{P_SP_R}g_{SR}g_{RD}x_S}{\sqrt{P_S|g_{SR}|^2 + P_D|g_{DR}|^2 + \sigma^2}} \\ &+ \frac{\sqrt{P_R}g_{RD}w_R}{\sqrt{P_S|g_{SR}|^2+P_D|g_{DR}|^2+\sigma^2}} + w_D \end{aligned} \tag{28}$$

It can be derived SNR at *D* as:

$$SNR_D = \frac{P_SP_R|g_{SR}|^2|g_{RD}|^2}{P_R|g_{RD}|^2\sigma^2+P_S|g_{SR}|^2\sigma^2+P_D|g_{DR}|^2\sigma^2+\sigma^4} \tag{29}$$

The secure rate, in this case, can be computed as:

$$\begin{aligned} &R\frac{1}{2}[log_2(1+SNR_D) - log_2(1+SNR_R)]^+_{sec} \\ &= \frac{1}{2}\left[log_2\left(\frac{1+SNR_D}{1+SNR_R}\right)\right]^+, \end{aligned} \tag{30}$$

Thus, the secure outage probability can be computed by:

$$OP_{out} = Pr\left(\frac{1+\frac{P_SP_R|g_{SR}|^2|g_{RD}|^2}{P_R|g_{RD}|^2\sigma^2+P_S|g_{SR}|^2\sigma^2+P_D|g_{DR}|^2\sigma^2+\sigma^4}}{1+\frac{P_S|g_{SR}|^2}{P_D|g_{DR}|^2+\sigma^2}} < 2^{2R_{th}}\right) \tag{31}$$

5. Simulation Results

In this section, we discover the secrecy performance of source-destination link under the help of an untrusted wireless powered relay. It can be shown that the impact of various system parameters on the secrecy outage probability is examined.

We set up the source power and destination jamming signal power, $P_S = P_D = P = 35\ dBm$ for Figs. 4 and 6, energy conversion efficiency $\eta = 0.8$ energy harvesting circuitry activation threshold, θ_h = 30 dBm and noise power, $\sigma^2 = 10^{-4}$. The distances between source and relay and that between relay and destination is normalize unit. The mean channel power gains and equal to 1.

As can be seen that Fig. 4 exhibits the effects of the power splitting ratio under PS policy on the secrecy outage probability performance. It is intuitively that if we increase in β, the secrecy outage probability primarily decreases to a minimum value. The optimal value of β so-called minimum secrecy outage probability, it is nearly 0.98. In constrast, increasing β further outside the optimal value, the secrecy outage probability will be worse. Also, the increased β reduces the received signal strength at the relay, which degrades the received SNR at the relay. This enhances the secrecy rate of the communication, which reduces the secrecy outage probability. It is required to careful calcuation β for remain secrecy performance. Similar trend can be observed in Fig. 5 as considering SOP performance versus the transmit power together with varying $\beta$with 3 cases $\beta = 0.4, 0.6, 0.8$. It worth noting that we set $R_{th} = 0.5$ (bps/Hz). It is also confirmed that increasing $\beta$the SOP will be improved.

The next experiment as an illustration in Fig. 6 displays the effects of the threshold SNR in the case of the non-EH relay for evaluation of the secrecy outage probability performance. It is natural that if we increase the threshold SNR, the secrecy outage probability will be primarily worse. It is shown that increasing the transmit power the secrecy performance can be enhanced. Furthermore, Fig. 7 concludes that non-EH scheme is always better than EH scheme due to using individual power.

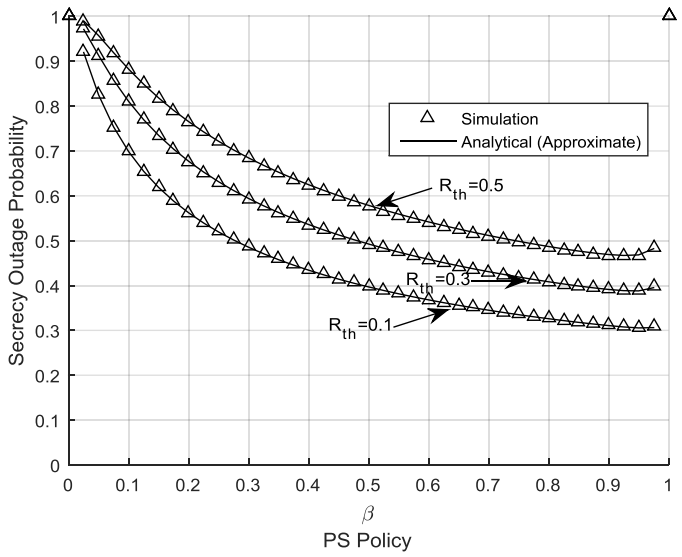

Fig. 4. SOP performance versus β in PS scheme.

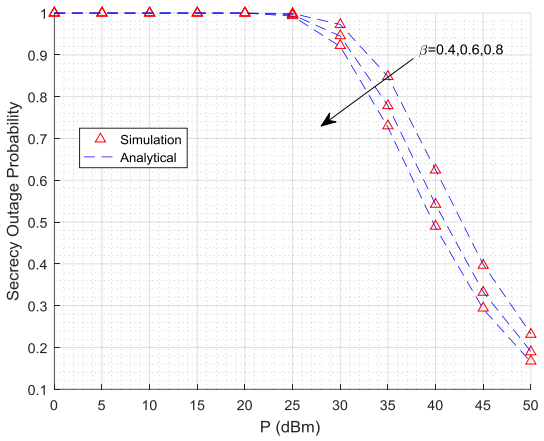

Fig. 5. SOP performance versus transmit power in PS policy.

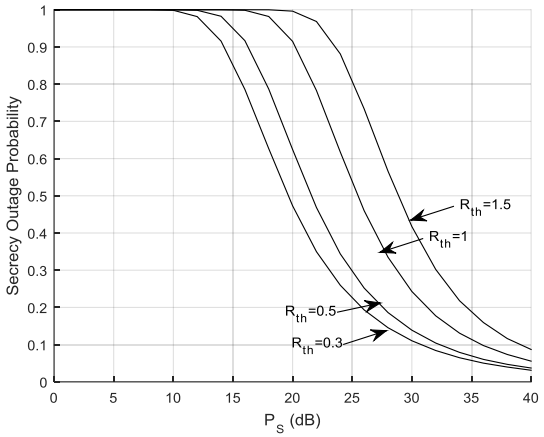

Fig. 6. SOP performance in non-EH case.

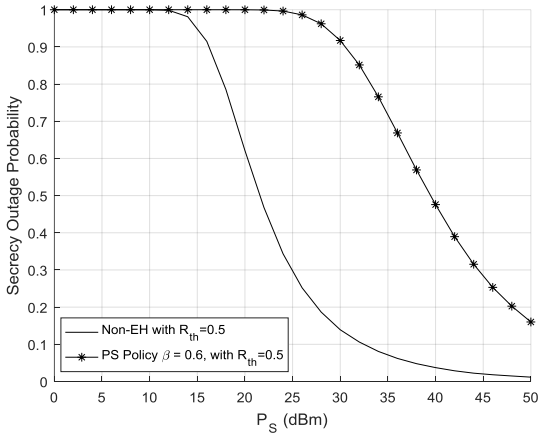

Fig. 7. SOP performance comparison between EH scheme and non-EH scheme.

6. Conclusions

This paper has studied the secrecy performance of simultaneous wireless information and power transfer system. By considering that energy-harvesting receivers may play as eavesdroppers and overhear the information delivery between the source and information receiver, the physical layer security performance such as secrecy outage has been studied. We have derived the closed-form analytical expressions for the exact secrecy outage probability. The validity of the proposed analytical expressions have been confirmed by Monte-Carlo simulations. More importantly, the better performance in case of the non-EH assisted relay can be observed compared with EH scheme. The main reason is that small amount of power can be harvested by EH policy. Our proposed analytical models can be readily applied to practical secrecy wireless powered systems design such as varying power splitting coefficient related to energy harvesting, reasonable selection of fixed rate.

Nomenclatures

D	Destination
E_H E_H	Relay harvests energy
$f_{\|g_{ab}\|^2}(x)$	Probability density function of random variable $\|g_{ab}\|^2 \|g_{ab}\|^2$
G	Relay amplify factor
$\|g_{ab}\|^2$	Gain of channel power
g_{ab} g_{ab}	Coefficient of the channel between nodes a and b
OP_{out}	Secrecy outage probability
P_D P_D	Power of destination
P_H	Transmit power of relay, which forwards information to destination
P_S P_S	Power of source
R	Relay
R_{sec} R_{sec}	Immediate secrecy rate
R_{th} R_{th}	Target secrecy rate
S	Source
x_D x_D	Jamming signal
w_i w_i	Additive white Gaussian noise at note i (i = D, R)
x_S x_S	Source message
y_i y_i	Received signal at i node (i = D, R)

Greek Symbols

β_i	Energy harvesting factor,
γ_H	Minimum threshold power
η	Energy conversion efficiency factor
σ^2	Noise power of AWGN w_i.
Ω_{ab}	Mean of $\|g_{ab}\|^2$

Abbreviations

AN	Artificial Noise
AWGN	Additive White Gaussian Noise
CJDH	Cooperative Jamming Dual-Hop Techniques
CSI	Channel State Information
EH	Energy Harvesting
MIMO	Multiple-Input Multiple-Output
PHY	Physical Layer
PS	Power Splitting
RF	Radio Frequency
SNR	Signal-to-Noise
SOP	Secrecy Outage Probability
TS	Time Switching

References

1. Hui, H.; Swindlehurst, A.L.; Li, G.; and Liang, J. (2015). Secure relay and jammer selection for physical layer security. *IEEE Signal Processing Letters*, 22(8), 1147-1151.
2. Ding, Z.; Leung, K.K.; Goeckel, D. L.; and Towsley, D. (2011). Opportunistic relaying forsecrecy communications: Cooperative jamming vs. relay chatting. *IEEE Transactions on Wireless Communications*, 10(6), 1725-1729.
3. Luo, S.; Li, J.; and Petropulu, A.P. (2013). Uncoordinated cooperative jamming for secret communications. *IEEE Transactions on Information Forensics and Security*, 8(7), 1081-1090.
4. Wang, H.-M.; Luo, M.; Yin, Q.; and Xia, X.-G. (2013). Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. *IEEE Transactions on Information Forensics and Security*, 8(12), 2007-2020.
5. Goel, S.; and Negi, R. (2008). Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6), 2180-2189.
6. Liu, S.; Hong, Y.; and Viterbo, E. (2015). Guaranteeing positive secrecy capacity for MIMOME wiretap channels with finite-rate feedback using artificial noise. *IEEE Transactions on Wireless Communications*, 14(8), 4193-4203.
7. Wang, H.-M.; Zheng, T.-X.; Yuan, J.; Towsley, D.; and Lee, M.H. (2016). Physical layer security in heterogeneous cellular networks. *IEEE Transactions on Communications*, 64(3), 1204-1219.
8. Wang, H.-M.; Wang, C.; and Ng, D.W.K. (2015). Artificial noise assisted secure transmission under training and feedback. *IEEE Transactions on Signal Processing*, 63(23), 6285-6298.
9. Wang, J.; Lee, J.; Wang, F.; and Quek, T.Q.S. (2015). Jamming-aided secure communication in massive MIMO Rician channels. *IEEE Transactions on Wireless Communications*, 14(12), 6854-6868.
10. Do, D.-T.; and Nguyen, H.-S. (2016). A tractable approach to analyze the energy-aware two-way relaying networks in presence of co-channel interference. *EURASIP Journal on Wireless Communications and Networking*, 271, 10 pages.

11. Nguyen, H.-S.; Bui, A.-H.; Do, D.-T.; and Voznak, M. (2016). Imperfect channel state information of AF and DF energy harvesting cooperative networks. *China Communications*, 13(10), 11-19.
12. Luan, N.T.; and Do, D.-T. (2017). A new look at AF two-way relaying networks: Energy harvesting architecture and impact of co-channel interference. *Annals of Telecommunications*, 72(11-12), 669-678, 2017.
13. Nguyen, X.-X.; and Do, D.-T. (2017). Maximum harvested energy policy in full-duplex relaying networks with SWIPT. *International Journal of Communication Systems (Wiley)*, 30(17), 1-16.
14. Kalamkar, S.S.; and Banerjee A. (2017). Secure communication via a wireless energy harvesting untrusted relay. *IEEE Trans on Vehicular Technology*, 66(3), 2199-2213.

Appendix A

Derivation of Eq. (15)

At high SNR, using the channel reciprocity between relay and destination and substituting SNR_R from Eq. (5) and SNR_D from Eq. (17) in Eq. (12) and then using Eqs. (12) and (13), we can write the secrecy outage probability for PS policy as

$$OP_{out} = Pr\left(\frac{1+\frac{\eta\beta(1-\beta)PXY}{\sigma^2(\eta\beta Y+(1-\beta))}}{1+\frac{(1-\beta)PY}{(1-\beta)PY+\sigma^2}} < \delta\right), \quad \text{(A.1)}$$

where $|g_{SR}|^2 = X, |g_{DR}|^2 = Y$ and we denote

$$Q = \frac{(1-\beta)\eta\beta Px}{\sigma^2(\eta\beta x+(1-\beta))} - \frac{(1-\beta)P\delta}{P(1-\beta)x+\sigma^2}. \quad \text{(A.2)}$$

Based on the sign of *Q*, we obtain new formula

$$OP_{out} = \Pr\left(|g_{SR}|^2 < \frac{\varepsilon-1}{Q}\right)\Pr(Q \geq 0) \quad \text{(A.3)}$$

Also, at high SNR it can be show that $Q \geq 0$

And, we can write the outage probability as:

$$OP_{out} = \int_0^\infty \left(1 - e^{-\frac{\varepsilon-1}{Q\Omega_{SR}}}\right) f_x(x)dx \quad \text{(A.4)}$$

Substituting $f_x(x) = \frac{1}{\Omega_{RD}} e^{-\frac{x}{\Omega_{RD}}}$ in the third integral of (A.3), we reach the required expression of OP_{out} as in Eq. (15).

Appendix B

Derivation of Theory 2

We can write the power outage probability as Eq. (14):

$$\begin{aligned} OP_{p,out} &= Pr(P_R < \gamma_H) = Pr(P(|g_{SR}|^2 + |g_{RD}|^2) < \gamma_H) \\ &= Pr\left((|g_{SR}|^2 + |g_{RD}|^2) < \frac{\gamma_H}{P}\right) \end{aligned} \quad \text{(B.1)}$$

Let $= (|g_{SR}|^2 + |g_{RD}|^2)$. Sine $|g_{SR}|^2$and $|g_{RD}|^2$ are exponentially distributed random variables with means Ω_{SR} and Ω_{RD} we can write the probability density function of A as [14]:

$$f_A(A) = \begin{cases} \frac{e^{-\frac{A}{\Omega_{SR}}}}{\Omega_{SR}-\Omega_{RD}} + \frac{e^{-\frac{A}{\Omega_{RD}}}}{\Omega_{RD}-\Omega_{SR}}, & if\ \Omega_{SR} \neq \Omega_{RD} \\ \left(\frac{1}{\Omega_{SR}}\right)^2 A\, e^{-\frac{A}{\Omega_{SR}}}, & if\ \Omega_{SR} = \Omega_{RD}. \end{cases} \quad \text{(B.2)}$$

Note that A can take only non-negative values as it is the sum of two exponential random variables. Therefore, we can write:

$$OP_{p,out} = Pr\left(A < \frac{\gamma_H}{P}\right) = \int_0^{\frac{\gamma_H}{P}} f_A(A)\, dA. \quad \text{(B.3)}$$

Evaluating the integral in (B.3), we get the required expression for the power outage probability as in Eq. (19).