INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2018, VOL. 64, NO. 1, PP. 33–38
Manuscript received February 20, 2017; revised January, 2018. DOI: 10.24425/118143

On Secrecy Performance for Energy-Harvesting Multi-Antenna Relaying Networks with a Dual-Use Source

Jiliang Zhang, Gaofeng Pan, and Yiyuan Xie

***Abstract*—This paper studies the secrecy performance of an energy-harvesting relaying system in the presence of a dual-use source node and an eavesdropper. Specifically, the source has dual roles in the dual-hop communication: 1) to transmit confidential information in the first hop; 2) to generate jamming signal to interfere the eavesdropper in the second hop. Moreover, the multi-antenna relay deploys a power-splitting harvesting scheme to coordinate the information receiving and energy harvesting, and adopts maximal ratio combining technique to process the multiple copies of signals. Considering decode-and-forward protocol and transmit antenna selection scheme, we derive an analytical expression for secrecy outage probability, and perform Monte Carlo simulation to validate the analysis. Analytical results show that the SOP performance with the dual-use source node can be effectively improved when the relay-destination channel does not have absolute advantage over the relay-eavesdropper channel.**

***Keywords*—Decode-and-forward, dual-use, energy harvesting, maximal ratio combining, secrecy outage probability**

I. Introduction

Nowadays, cooperative/relaying technique has received increasing interest in the context of physical-layer (PHY) security over wireless communication systems, as it can not only significantly enhance the PHY security from information-theoretic sense but also extend the coverage of information transmission [1], [2]. For example, in [3], considering both randomize-and-forward and decode-and-forward (DF) relaying protocols, a hybrid half-duplex (HD)/full-duplex (FD) relaying system was proposed to enhance the PHY security in terms of secrecy capacity (SC) and average throughput. Taking into account a joint relay and jamming selection scheme, the authors derived the closed-form expressions for connection outage probability, secrecy outage probability (SOP), reliable and secure connection probability, and reliability and security ratio in [4]. In [5], an analytical expression for SOP was derived for a single-input multiple-output relaying system over double Rayleigh fading channels.

Radio-frequency-enabled energy-harvesting (EH) is an efficient technique to prolong the lifetime of energy-constrained systems [7]-[8]. Several works have been reported to investigate EH relaying systems in the context of PHY security [9]-[12]. The authors in [9] presented a thorough literature review on PHY security in EH relaying systems. In [10], an energy-efficient beamforming was proposed to minimize the transmission power for a multiple-input single-output system in the presence of multiple single-antenna eavesdroppers. Assuming both perfect and imperfect channel state information (CSI), a SC maximization problem was formulated under the constraints of transmission power for a multi-antenna amplify-and-forward (AF) relaying system in the presence of multiple multi-antenna harvest-and-jam helpers in [11]. In [12], a joint beamforming vector designing problem at both the source and the relay was investigated to maximize the SC for a multiple-input multiple-output (MIMO) EH relaying system.

To further enhance the PHY security, cooperative jamming (CJ) has been utilized to confuse eavesdropper(s) [1], [13]. Assuming the relay equipped with multiple antennas, an artificial noise (AN) assisted relay beamforming vector was proposed to interfere the eavesdropper for HD and FD modes in [14] and [15], respectively. Later, the work of [14] was extended into a general MIMO scenario, where all nodes including the source, the relay, the destination and the eavesdropper are with multiple antennas in [16]. Taking into account power-splitting (PS) and time-switching (TS) schemes, a robust AN beamforming vector was also proposed to minimize the transmission power subject to the constraints of SC and relaying power in [17]. In the presence of multiple relaying nodes either performing CJ or relaying, a SC maximization issue was investigated by designing optimal and/or suboptimal relaying beamforming vectors under the constraint of relaying power in [18] and through a new joint relay and jammer selection scheme in [19]. References [20] and [21] proposed a destination based dual-use AN signal to interfere the eavesdroppers and to harvest the relays concurrently in the transmission mode of the source. In particular, an optimization problem by jointly designing the PS factor and beamforming vector was studied in [20]. The authors in [21] derived the analytical expression for average secrecy capacity (ASC) when both PS and TS schemes were considered.

It is noted that confusing the eavesdropper(s) is realized by generating AN with the aid of either the node equipped with multiple antennas [14]-[17] or extra helper(s) [18]-[21], which also degrades the system performance of the legitimate destination. Different from the aforementioned works, in this work, we investigates the secrecy performance for a multi-antenna EH relaying system operating in an HD mode with a dual-use source. Specifically, the source has two roles in

This work is supported by the National High-Tech R&D Program of China (No. 2015AA016304) and the Fundamental Research Funds for the Central Universities of China (No. XDJK2016A011).

The authors are with the Key Laboratory of Networks and Cloud Computing Security of Universities in Chongqing, School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, P. R. China (e-mail: gfpan@swu.edu.cn).

the dual-hop communication, i.e. to broadcast information in the first hop and to generate interference to confuse the eavesdropper in the second hop. The difference is two-fold. First, unlike the conventional HD mode, the source utilizes a portion of power to transmit the confidential information in the first hop, and uses the remaining to generate jamming signal to confuse the eavesdropper in the second hop. Assuming no direct link exists between the source and the destination [18], [19], the jamming signal generated by the source only confuses the eavesdropper, and the destination is free from it. Second, most of those works are limited to beamforming vector design or resource allocation, and only a few works evaluate the secrecy performance for multi-antenna EH relaying systems, i.e. Reference [21] investigates the ASC. In this paper, we focus on secrecy performance in terms of SOP. In particular, assuming the PS and DF schemes are employed at the relay, the analytical expression of SOP has been derived. Moreover, the maximal ratio combining (MRC) technique and transmit antenna selection (TAS) scheme at the relay are also considered.

The rest of this paper is structured as follows. In Section II, system model is described. In Section III, the analysis of SOP is presented. In Section IV, numerical results are evaluated. Finally, concluding remarks are presented in Section V.

II. System Model

Consider a DF dual-hop relaying system operating in a HD mode, which consists of a source (S), a relay (R), and a destination (D) in the presence of an eavesdropper (E). It is assumed that the relaying node is equipped with M antennas, and each of the remaining nodes is with a single antenna. A harvest-to-use scheme [22] is considered in this work, in which the relaying node does not have extra energy, and it harvests the energy from the source in the first hop and uses up all the harvested energy to broadcast the information in the second hop. We further assume that the energy consumed in other operations such as information decoding, MRC and TAS is ignored as the energy consumption for transmitting the information is dominant in total energy consumption [21], [23], [24]. Perfect CSI is also assumed to be available at R to perform MRC and TAS. It is assumed that the direct link between S and D is broken due to serious fading [21], [25]. All links between S and each antenna at R are assumed to experience independent and identical Rayleigh fading, all the channels between each antenna at R and D undergo independent and identical Rayleigh distribution, and the remaining channels are with independent but not necessarily identical Rayleigh-distributed. Furthermore, it is also assumed that the channels between S and E in the first and second time slots are independent but not necessarily identical Rayleigh-distributed. This is reasonable in practical scenario as E will adaptively adjust its relative locations to S and R in the dual-hop communication processes to overhear more information. The channel coefficient is denoted as h_b, $b \in \{SR_m, SE_1, RE, SE_2, R_mD\}$ and $m = 1, 2, \cdots, M$. Hence, $|h_b|^2$ is with an exponential distribution and its probability density function (PDF) and cumulative distribution function (CDF) can be denoted as

$$f_{|h_b|^2}(x) = \frac{1}{g_b} \exp\left(-\frac{x}{g_b}\right) \tag{1}$$

and

$$F_{|h_b|^2}(x) = 1 - \exp\left(-\frac{x}{g_b}\right) \tag{2}$$

respectively, where g_b denotes the expectation of channel power gain [26].

In this work, a PS harvesting scheme [27] is considered at each antenna of R to coordinate the energy harvesting and information transmission concurrently. Therefore, a portion of the received energy is fed into the MRC processor for information processing, and the rest is stored in the energy harvester. As a dual-hop relaying scheme with two equal time slots is considered, each slot is assumed to be with a duration of $T/2$. In the first time slot, S uses a portion of the power, $\rho_1 P_s$, where $0 < \rho_1 < 1$ and P_s is the total power at S, to transmit signal to R in the presence of E. The information received and energy harvested at the mth antenna of R are

$$y_{R_m} = \sqrt{1-\rho_2}\left(\sqrt{\rho_1 P_s} h_{SR_m} X_s + n_{R_m a}\right) + n_{R_m c} \tag{3}$$

and

$$E_{R_m} = \rho_2 \rho_1 \eta P_s |h_{SR_m}|^2 T/2 \tag{4}$$

where $0 < \rho_2 < 1$ is the PS factor, X_s is the transmitted symbol at S, η is the energy conversion efficiency, $n_{R_m a}$ denotes the additive white Gaussian noise (AWGN) with zero mean and a variance of N_0, and $n_{R_m c}$ is the processing noise [25], which is also modeled as AWGN with zero mean and a variance of σ^2. After that, all the M received information copies are fed into the MRC processor, which outputs an instantaneous signal-to-noise ratio (SNR) as

$$\gamma_{SR} = \frac{(1-\rho_2)\rho_1 P_s |h_{SR}|^2}{(1-\rho_2)N_0 + \sigma^2} \tag{5}$$

where $|h_{SR}|^2 = \sum_{m=1}^{M} |h_{SR_m}|^2$ with its PDF and CDF denoted as [26]

$$f_{|h_{SR}|^2}(x) = \frac{\lambda_{SR}^M x^{M-1}}{\Gamma(M)} \exp(-x\lambda_{SR}) \tag{6}$$

and

$$F_{|h_{SR}|^2}(x) = \frac{1}{\Gamma(M)} \gamma(M, x\lambda_{SR}) \tag{7}$$

respectively, where $\Gamma(\cdot)$ is the gamma function defined by (8.310.1) in [28], $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function defined by (8.350.1) in [28], and $\lambda_{SR} = \frac{1}{g_{SR}}$. Similarly, the energy harvested at all the M antennas is combined together to output the relaying power at R as

$$P_R = \rho_2 \rho_1 \eta P_s |h_{SR}|^2. \tag{8}$$

The received signal and instantaneous SNR at E are

$$y_{SE} = \sqrt{\rho_1 P_s} h_{SE_1} X_s + n_E \tag{9}$$

and

$$\gamma_{SE} = \frac{\rho_1 P_s |h_{SE_1}|^2}{N_0} \tag{10}$$

respectively, where n_E is also modeled as AWGN with zero mean and a variance of N_0.

In the second time slot, the relay employs TAS scheme to select the best antenna in terms of the largest instantaneous channel gain to transmit the processed information to D while E is overhearing the information. The best antenna is selected based on the information fed back from D. At the same time, S utilizes the rest portion of power to send jamming signal to confuse E. As the link between S and D is broken, D is free from the jamming signal. Hence, the received signal and the instantaneous SNR at D are

$$y_{RD} = \sqrt{P_R} h_{RD} X_s + n_D \tag{11}$$

and

$$\gamma_{RD} = \frac{P_R |h_{RD}|^2}{N_0} \tag{12}$$

respectively, where h_{RD} denotes the largest channel coefficient between all the M antennas of R and D, and its mathematical representation can be expressed as

$$|h_{RD}| = \max_{l=1,2,\dots,M} \{|h_{R_l D}|\} \tag{13}$$

with its CDF and PDF denoted as [29]

$$F_{|h_{RD}|^2}(x) = \left(1 - \exp\left(-\frac{x}{g_{RD}}\right)\right)^M \tag{14}$$

and

$$f_{|h_{RD}|^2}(x) = \frac{M}{g_{RD}} \left[1 - \exp\left(-\frac{x}{g_{RD}}\right)\right]^{M-1} \times \exp\left(-\frac{x}{g_{RD}}\right) \tag{15}$$

respectively.

Next, the received signal at E is

$$y_{RE} = \sqrt{P_R} h_{RE} X_s + \sqrt{(1-\rho_1) P_s} h_{SE_2} X_I + n_E \tag{16}$$

where X_I is the jamming signal from S, and the signal-to-interference-plus-noise ratio (SINR) is obtained as

$$\gamma_{RE} = \frac{P_R |h_{RE}|^2}{(1-\rho_1) P_s |h_{SE_2}|^2 + N_0}. \tag{17}$$

For mathematical simplification, we assume that the interference is dominant, which is also of practical interest [22], [30]. Thus, we have $\gamma_{RE} \approx \frac{P_R |h_{RE}|^2}{(1-\rho_1) P_s |h_{SE_2}|^2}$.

III. Secrecy Outage Analysis

In this section, the derivation of SOP will be presented. The instantaneous SC for the first and second time slots can be obtained as

$$C_{SR} = \left\{\frac{1}{2}\big(\log_2(1+\gamma_{SR}) - \log_2(1+\gamma_{SE})\big)\right\}^+ \tag{18}$$

and

$$C_{RD} = \left\{\frac{1}{2}\big(\log_2(1+\gamma_{RD}) - \log_2(1+\gamma_{RE})\big)\right\}^+ \tag{19}$$

respectively, where $\{x\}^+ = \max\{x, 0\}$. When $\gamma_{RD} \gg 1$ and $\gamma_{RE} \gg 1$, we can have $C_{RD} \approx \{\frac{1}{2}\big(\log_2(\gamma_{RD}) - \log_2(\gamma_{RE})\big)\}^+$. This condition can be satisfied at higher SNR and SINR regimes, which are also of interest for practical communications. The instantaneous SC for S-R-D link is the minimum value of those two hops and it can be expressed as

$$C_s = \min(C_{SR}, C_{RD}). \tag{20}$$

The SOP is defined as the probability when the even that the instantaneous capacity C_s is below a target secrecy rate R_s, i.e. $C_s < R_s$, occurs. Thus, the SOP can be given as

$$\begin{aligned} P_{SOP} &= Pr(C_s < R_s) \\ &= Pr(\min(C_{SR}, C_{RD}) < R_s) \\ &= 1 - Pr(\min(C_{SR}, C_{RD}) \geq R_s) \\ &= 1 - Pr(C_{SR} \geq R_s, C_{RD} \geq R_s) \end{aligned} \tag{21}$$

where

$$\begin{aligned} &Pr(C_{SR} \geq R_s, C_{RD} \geq R_s) \\ &= Pr\left(|h_{SR}|^2 \geq A|h_{SE_1}|^2 + B, |h_{RD}|^2 \geq C\frac{|h_{RE}|^2}{|h_{SE_2}|^2}\right) \\ &= Pr(|h_{SR}|^2 \geq A|h_{SE_1}|^2 + B) Pr(|h_{RD}|^2 \geq Cz) \end{aligned} \tag{22}$$

in which $A = \frac{\beta[(1-\rho_2)N_0 + \sigma^2]}{N_0(1-\rho_2)}$, $B = \frac{(\beta-1)[(1-\rho_2)N_0+\sigma^2]}{(1-\rho_2)\rho_1 P_s}$, $C = \frac{N_0 \beta}{(1-\rho_2)P_s}$, $\beta = 2^{2R_s}$ and $z = \frac{|h_{RE}|^2}{|h_{SE_2}|^2}$.

Making use of (5) and (10), $Pr(|h_{SR}|^2 \geq A|h_{SE}|^2 + B)$ in (22) can be re-expressed as

$$\begin{aligned} &Pr(|h_{SR}|^2 \geq A|h_{SE_1}|^2 + B) \\ &= Pr\left(|h_{SE_1}|^2 \leq \frac{|h_{SR}|^2 - B}{A}\right) \\ &= \int_B^\infty \left[1 - \exp\left(-\lambda_{SE_1}\left(\frac{x-B}{A}\right)\right)\right] f_{|h_{SR}|^2}(x) dx \\ &= 1 - \frac{1}{\Gamma(M)} \gamma(M, \lambda_{SR} B) - I_1 \end{aligned} \tag{23}$$

where

$$I_1 = \int_B^\infty x^{M-1} \exp\left(-\big(\lambda_{SR} + \frac{\lambda_{SE_1}}{A}\big)x\right) dx \times \frac{\lambda_{SR}^M}{\Gamma(M)} \exp\left(\frac{\lambda_{SE_1} B}{A}\right). \tag{24}$$

Using $(3.351.2.^{11})$ in [28], I_1 can be further simplified into

$$I_1 = \frac{\lambda_{SR}^M}{\Gamma(M)} \exp\left(\frac{\lambda_{SE_1} B}{A}\right) \big(\lambda_{SR} + \frac{\lambda_{SE_1}}{A}\big)^{-M} \times \Gamma\left(M, B\big(\lambda_{SR} + \frac{\lambda_{SE_1}}{A}\big)\right) \tag{25}$$

where $\Gamma(\cdot, \cdot)$ is the upper incomplete gamma function defined by $(8.350.2.^{11})$ in [28].

Since both $|h_{RE}|^2$ and $|h_{SE_2}|^2$ are independent and non-negative random variables, the PDF expression of z can be obtained as [29]

$$\begin{aligned} f_z(z) &= \int_0^\infty x f_{|h_{RE}|^2}(xz) f_{|h_{SE_2}|^2}(x) dx \\ &= \lambda_{RE}\lambda_{SE_2} \int_0^\infty x \exp\Big(-(\lambda_{RE} z + \lambda_{SE_2})x\Big) dx \\ &= \frac{\lambda_{RE}\lambda_{SE_2}}{(z\lambda_{RE} + \lambda_{SE_2})^2} \end{aligned} \tag{26}$$

where $\lambda_{RE} = \frac{1}{g_{RE}}$ and $\lambda_{SE_2} = \frac{1}{g_{SE_2}}$.

Next, using (14), (26) and the power series shown in (1.111) in [28], one can re-express $Pr(|h_{RD}|^2 \geq Cz)$ as

$$\begin{aligned} & Pr(|h_{RD}|^2 \geq Cz) \\ &= 1 - Pr(|h_{RD}|^2 < Cz) \\ &= 1 - \int_0^\infty \Big[1 - \exp\big(-\lambda_{RD} C z\big)\Big]^M \\ &\qquad \times \frac{\lambda_{RE}\lambda_{SE_2}}{(z\lambda_{RE} + \lambda_{SE_2})^2} dz \\ &= 1 - \int_0^\infty \sum_{k=0}^{M} \binom{M}{k} (-1)^k \exp\big(-k\lambda_{RD} C z\big) \\ &\qquad \times \frac{\lambda_{RE}\lambda_{SE_2}}{(z\lambda_{RE} + \lambda_{SE_2})^2} dz. \end{aligned} \tag{27}$$

Making use of (3.353.3) in [28], (27) can be further simplified into

$$\begin{aligned} & Pr(|h_{RD}|^2 \geq Cz) \\ &= 1 - \sum_{k=0}^{M} \binom{M}{k} (-1)^k \Bigg[\frac{\lambda_{SE_2}\lambda_{RD} k C}{\lambda_{RE}} \exp\left(\frac{\lambda_{SE_2}\lambda_{RD} k C}{\lambda_{RE}}\right) \\ &\qquad \times E_i\bigg(-\frac{\lambda_{SE_2}\lambda_{RD} k C}{\lambda_{RE}}\bigg) + 1\Bigg] \end{aligned} \tag{28}$$

where $E_i(\cdot)$ is the exponential integral function defined by (8.211.1) in [28] and $\lambda_{RD} = \frac{1}{g_{RD}}$.

Finally, SOP can be obtained by substituting (23) and (28) into (21).

IV. Numerical Results and Discussions

In this section, analytical and simulation results for SOP will be presented and compared. Unless otherwise explicitly specified, the parameters of those results are set as follows: $M = 3$, $P_s/N_0 = 30$ dB, $R_s = 0.1$ bits/s/Hz, $g_{SR} = 1$, $g_{RD} = 1$, $g_{SE_1} = 0.5$, $g_{SE_2} = 0.5$, $\eta = 0.9$, $\rho_1 = 0.5$, $\rho_2 = 0.5$, $N_0 = \sigma^2$, and $\tau = \frac{g_{RD}}{g_{RE}}$.

Fig. 1 shows the SOP performance under various M. It is observed that the SOP performance improves as the value of M increases. This is because a higher value of M means more antennas are equipped at the relay, which in turn can enjoy a joint advantage of larger diversity gains benefited from the MRC and TAS schemes employed at the relay in the first and second hops, respectively. We also observe that both analytical results and Monte Carlo simulation results match with each other, which validates the accuracy of the analytical expression derived.

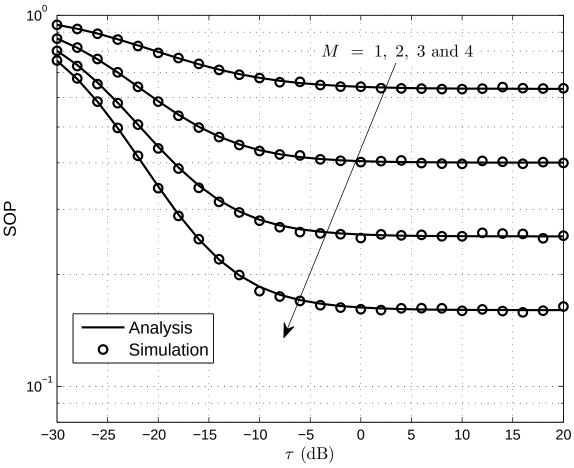

Fig. 1. SOP vs τ for various M.

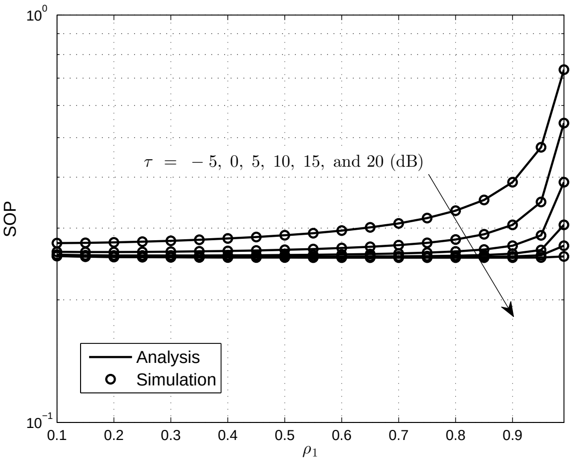

Fig. 2. SOP vs ρ_1 for various τ with $P_s/N_0 = 24$ dB.

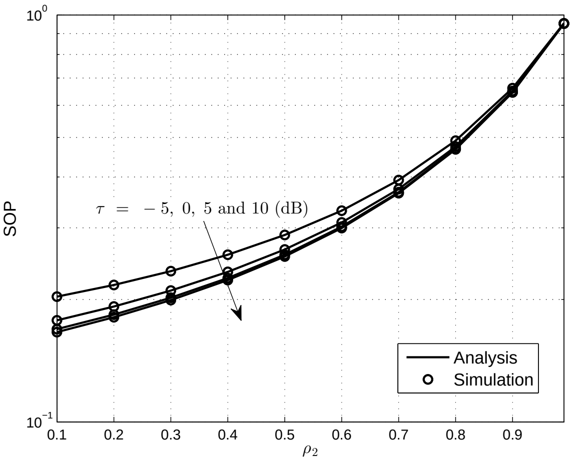

Fig. 3. SOP vs ρ_2 for various τ with $P_s/N_0 = 24$ dB.

The SOP performance against ρ_1 and ρ_2 are presented in Fig. 2 and Fig. 3, respectively. From Fig. 2, one can observe that ρ_1 has little effect on the SOP performance when $\tau \geq 10$ dB, as the channel advantage of R-D link over R-E link is dominated on the SOP performance, and generating jamming signal from S to interfere E has little effect on improving the SOP performance under this certain condition. On the other hand, when τ is small, i.e. $\tau \leq 5$ dB, observed from the trend of the three curves, it is clear to see that the SOP performance when $0 < \rho_1 < 1$ is better than that when $\rho_1 \to 1$. Note that $0 < \rho_1 < 1$ indicates the scenario that there exists a jamming signal generated by the source in the second time slot to interfere the eavesdropper, while $\rho_1 \to 1$ nearly means no jamming signal generated. Hence,we can conclude that our proposed dual-use source model can have better SOP performance than the conventional one without any jamming signal when the R-D link does not have absolute advantage over the R-E link, i.e. $\tau \leq 5$ dB. Moreover, we can also observe that there is no much difference on the SOP performance in a wide range of ρ_1 in all the curves, i.e. ρ_1 goes from 0.1 to 0.6 at $\tau = -5$ dB, which indicates the choice of ρ_1 is flexible. Fig. 3 shows that a higher value of ρ_2 can lead to worse SOP performance as less energy is used for information decoding at the relay. Furthermore, the SOP performance improves as τ increases when $\tau \leq 5$ dB. While $\tau > 5$ dB, the SOP values almost remain unchange as τ increases. This scenario can be explained by the fact that the SC for S-R-D link is the minimum value of the two hops as shown in (20), and increasing τ can only improve the SC in the second hop. When $C_{SR} > C_{RD}$, increasing τ has positive advantage on the SOP performance as $C_s = C_{RD}$. On the other hand, when $C_{SR} < C_{RD}$, τ has little effect on the SOP performance as C_S is dominated by the SC in the first hop, i.e. $C_S = C_{SR}$.

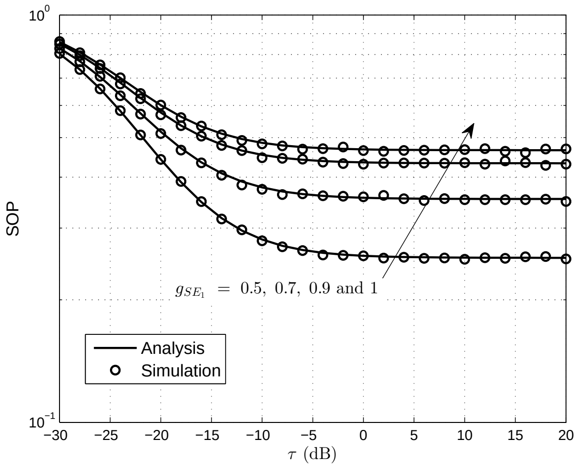

Fig. 4. SOP vs τ for various g_{SE_1}.

Figs. 4 and 5 present the effects of channel gains g_{SE_1} and g_{SE_2} on the SOP performance, respectively. It is noted from Fig. 4 that the SOP performance is worse at a higher value of g_{SE_1}. This is because the channel condition for S-E link in the first hop becomes better at a higher value of g_{SE_1}, and E can overhear more information, which in turn decreases the SOP performance. From Fig. 5, one can see that the SOP performance improves as g_{SE_2} increases when $\tau \leq 5$ dB. This phenomenon can be explained by the fact that a higher channel gain results in a stronger jamming signal at E to degrade its performance. On the other hand, when $\tau > 5$ dB, the SOP values remain unchanged as the value of channel gain g_{SE_2} increases as generating jamming signal has little effect on improving the SOP performance under this certain conditions, which also coincides with those observations in Fig. 2.

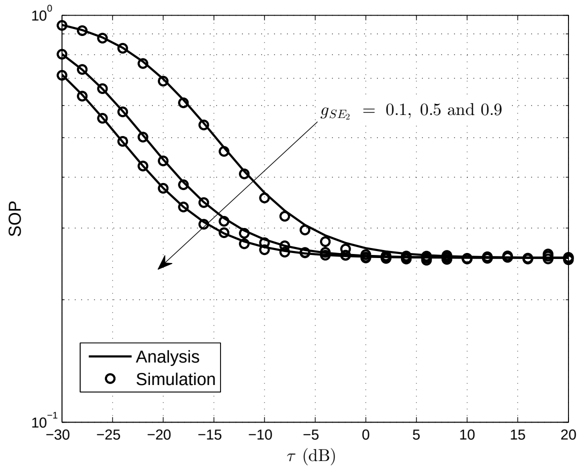

Fig. 5. SOP vs τ for various g_{SE_2}.

V. Conclusion

This paper investigates the secrecy outage performance for a multi-antenna EH relay system when the source plays dual roles in the two-hop communications. Taking into account PS scheme and DF protocol, an analytical expression for SOP has been derived when MRC technique and TAS scheme are performed at the relay in the first and second time slots, respectively. Simulation results show that our proposed model are very effective on improving the SOP performance when the R-D link does not have absolute advantage over the R-E link, i.e. $\tau \leq 5$ dB.

References

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

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Effcient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[3] A. El Shafie, A. Sultan, and N. Al-Dhahir, "Physical-layer security of a buffer-aided full-duplex relaying System," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1856-1859, Sept. 2016.

[4] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259-6274, Aug. 2016.

[5] J. Zhang and G. Pan, "Secrecy outage analysis with Kth best relay selection in dual-hop inter-vehicle communication systems," *AEU-Int. J. Electron. Commun.*, vol. 71, pp. 139-148, Jan. 2017.

[6] T. R. Ramya and S. Bhashyam, "Using delayed feedback for antenna selection in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 6059-6067, Dec. 2009.

[7] S. Sudevalayam and P. Kulkarni, "Energy harvesting sensor nodes: Survey and implications," *IEEE Commun. Surveys & Tutorials*, vol. 13, no. 3, pp. 443-461, Third Quart. 2011.

[8] M.-L. Ku, W Li, Y. Chen, and K. J. R. Liu, "Advances in energy harvesting communications: Past, present, and future challenges," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 3, pp. 1384-1412, Second Quart. 2016.

[9] J. Kang, R. Yu, S. Maharjan, Y. Zhang, X. Huang, S. Xie, H. Bogucka, and S. Gjessing, "Toward secure energy harvesting cooperative networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 114-121, Aug. 2015.

[10] H. Gao, T. Lv, W. Wang, and N. C. Beaulieu, "Energy-efficient and secure beamforming for self-sustainable relay-aided multicast networks," *IEEE Sig. Proc. Lett.*, vol. 23, no. 11, pp. 1509-1513, Nov. 2016.

[11] H. Xing, K.-K Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Sig. Proc.*, vol. 63, no. 24, pp. 6616-6631, Dec. 2015.

[12] G. Zhang, X. Li, M. Cui, G. Li, and L. Yang, "Signal and artificial noise beamforming for secure simultaneous wireless information and power transfer multiple-input multiple output relaying systems," *IET Commun.*, vol. 10, no. 7, pp. 796-804, Jul. 2016.

[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wire. Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[14] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9006-9019, Nov. 2016.

[15] Q. Li, W.-K Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE J. Sel. Areas Commun.*, vol. 10, no. 8, pp. 1359-1374, Dec. 2016.

[16] Q. Li and J. Qin, "Joint source and relay secure beamforming for non-regenerative MIMO relay systems with wireless information and power transfer," *IEEE Trans. Veh. Technol.*, doi: 10.1109/TVT.2016.2633380.

[17] B. Li, Z. Fei, and H. Chen, "Robust artificial noise-aided secure beamforming in wireless-powered non-regenerative relay networks," *IEEE Access*, vol. 4, pp. 7921-7929, Nov. 2016.

[18] H. Xing, K.-K Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Trans. Wire. Commun.*, vol. 15, no. 12, pp. 7971-7984, Dec. 2016.

[19] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, "Power-constrained secrecy rate maximization for joint relay and jammer selection assisted wireless networks," *IEEE Trans. Commun.*, doi: 10.1109/TCOMM.2017.2651066.

[20] M. Zhao, X. Wang, and S. Feng, "Joint power splitting and secure beamforming design in the multiple non-regenerative wireless-powered relay networks," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1540-1543, Sep. 2015.

[21] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025-3038, July 2016.

[22] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447-3461, Oct. 2014.

[23] I. Krikidis, G. Zheng, and B. Ottersten, "Harvest-use cooperative networks with half/full-duplex relaying," in *Proc. IEEE WCNC*, Shanghai, China, Apr. 2013, pp. 4256-4260.

[24] K. Ishibashi, C. K. Ho, and I. Krikidis, "Diversity-multiplexing tradeoff of dynamic harvest-and-forward cooperation," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 633-636, Dec. 2015.

[25] Y. Chen, "Energy harvesting AF relaying in the presence of interference and Nakagami-*m* fading," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1008-1017, Feb. 2016.

[26] J. G. Proakis, *Digital Communications*, 4th Ed., McGraw-Hill, 2001.

[27] G. Pan and C. Tang, "Outage performance on threshold AF and DF relaying schemes in simultaneous wireless information and power transfer systems," *AEU-Int. J. Electron. Commun.*, vol. 71, pp. 175-180, Jan. 2017.

[28] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th Ed., Elsevier, 2007.

[29] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*, 4th Ed., McGraw-Hill, 2001.

[30] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Chanllenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637-1652, Sep. 2014.