Physical Layer Security in Cooperative Energy Harvesting Networks with a Friendly Jammer

Physical Layer Security in Cooperative Energy Harvesting Networks with a Friendly Jammer

Tiep M. Hoang, Trung Q. Duong, *Senior Member, IEEE*, Nguyen-Son Vo, and Chinmoy Kundu

***Abstract*—In this paper, we consider a cooperative wireless network consisting of a source, multiple intermediate energy harvesting nodes and a destination, in the presence of a passive eavesdropper. First, the intermediate nodes use the time switching-based relaying protocol to harvest energy from the source signal. Then, a pair out of intermediate nodes are selected as a relay and a jammer to transmit confidential and jamming signals to the destination and eavesdropper. Under these assumptions, we evaluate the system performance in terms of secrecy outage probability.**

***Index Terms*—Physical layer security, energy harvesting.**

I. Introduction

Physical layer security (PLS) and energy harvesting (EH) have been attracting a great deal of attention from the researcher community. While the objective of PLS is to guarantee and enhance confidential messages [1]–[4], that of EH is to utilize the harvested energy of wireless received signals for information processing [5]. Although each topic has been well investigated as an individual body of knowledge in literature, it is only recently that their combination has been emerged as an attractive research approach [1]–[4].

In [1], the authors considered a secure network using a multiple-antenna relay which is capable of harvesting energy. In [2], a friendly jammer with the ability of harvesting energy was used to resist eavesdropping. Meanwhile, the authors in [3] designed artificial noise for both interfering with undesired destinations and being cancelable at the intended receiver. Besides, energy harvesting was also discussed in relation to the security of each individual subcarrier in an orthogonal frequency division multiplexing access network as in [4]. Motivated by these work, in this paper, we study the secure performance of a cooperative relaying network which consists of energy harvesting nodes. Different from [1]–[3] which used only one intermediate node, we utilize two intermediate nodes (i.e., a relay and a jammer) for improving the gain of desired channel gain and simultaneously interfering with the eavesdropping channel. In [2] and [4], the authors did not consider the relaying protocol using *time switching-based relaying* (TSR) technique (presented in [5]). Moreover, the simultaneous use of both relay and jammer was not taken into account in these works. To the best of authors' knowledge, the role of such TSR circuitries in both-relay-and-jammer-aided networks is not conducted by any previous work. Note that, although the impact of light-of-sight (LOS) on the harvested energy loss in the context of energy harvesting has recently emerged as one important topic [6], it is not considered in this paper. With many individual aspects of both security and energy harvesting, we choose not to investigate the LOS factor. Instead, we aim to highlight the secure performance when considering intermediate nodes equipped with energy harvesting circuitries. Furthermore, we examine the following two schemes: i) the best relay is chosen for forwarding the retransmitted signal while the jammer is random; ii) the best jammer is chosen for interfering with the eavesdropper while the relay is random. Based on the two schemes of interest, we evaluate the secure performance through the security outage probability (SOP). We demonstrate that the system performance deteriorates in terms of security if the amount of time used for energy harvesting is much larger than that used for information processing and vice versa.

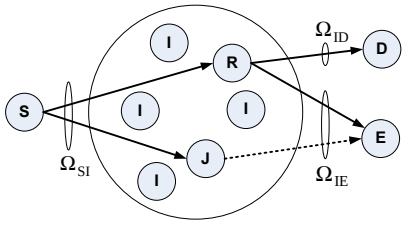

Fig. 1. The system model of interest.

II. System and Channel Model

We consider a cooperative wireless network, which consists of one source S, one destination D, one eavesdropper E, and $M+1$ intermediate nodes I_i, $(i = 1, 2, ..., M+1)$ using decode-and-forward protocol. We assume that the direct link between S and D is not available due to bad conditions and the transmission from S to D is performed by the help of the trusted intermediate nodes $\{I_i\}_{i=1}^{M+1}$. All channels are assumed to undergo Rayleigh fading, and the channel power gain between $X \in \{S, I_i\}$ and $Y \in \{I_i, D, E\} \setminus X$ is denoted by h_{XY}. Then we can say that h_{XY} obeys the exponential distribution with rate $1/\Omega_{XY}$, i.e., $h_{XY} \sim \text{Exp}\left(\frac{1}{\Omega_{XY}}\right)$. For simplicity, we set $\Omega_{SI_i} = \Omega_{SI_j}$ and $\Omega_{I_iE} = \Omega_{I_jE}$ with $i \neq j$.

Among $M+1$ intermediate nodes, we choose a node as a relay R and another node as a jammer J. The relay R will

T. M. Hoang, T. Q. Duong, and C. Kundu are with Queen's University Belfast, Belfast BT7 1NN, UK (e-mail: {mhoang02, trung.q.duong, c.kundu}@qub.ac.uk).

N.-S. Vo is with Duy Tan University, Vietnam (e-mail: vonguyenson@dtu.edu.vn).

This work was supported by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, the Newton Institutional Link under Grant ID 172719890, Royal Society-SERB Newton International Fellowship under Grant ID NF151345, and Royal Society Research Grant under Grant ID RG160302.

transmit confidential signals, while the jammer J will transmit jamming signals. Suppose that D and J cooperate with each other such that the jamming signal can be nulled out at D [7]. In contrast, E has to extract both the confidential information from R and the interference from J.

In the considered network, we employ the TSR protocol presented in [5]. Then, assuming that each I_i harvests energy from S and uses this energy to transmit relaying and jamming signals, we can express the transmit power of I_i as

$$P_{I_i} = \frac{\eta P_S h_{SI_i} \alpha T}{(1-\alpha)T/2} = \frac{2\eta P_S h_{SI_i} \alpha}{(1-\alpha)}, \quad (1)$$

where P_S is the transmit power of S, $\eta \in (0,1)$ is the energy conversion efficiency which depends on the rectification process and the energy harvesting circuitry, T is the block time in which a certain block of information is transmitted from the source node to the destination node, $\alpha \in (0,1)$ is the fraction of the block time in which intermediate nodes harvest energy from the source signal.[1]

A. Best relay and random jammer (bR-rJ)

In this strategy, the jammer J is first randomly selected among $\{I_i\}_{i=1}^{M+1}$. Without loss of the generality, we assume that the $(M+1)$-th intermediate node is the jammer, $J = I_{M+1}$. The relay R^* is then selected among the M remaining intermediate nodes such that the channel power gain of the R^*-D link is largest, i.e.,

$$h_{R^*D} \triangleq \max_{i=1,\ldots,M} h_{I_i D} \quad (2)$$

where $h_{I_i D}$ is the channel power gains of the I_i-D link. Then the instantaneous received SNR at D and E are, respectively, given by

$$\gamma_D^{\text{bR-rJ}} = (P_R/N_0) h_{R^*D} = \xi h_{SR^*} h_{R^*D}, \quad (3)$$

$$\gamma_E^{\text{bR-rJ}} = \frac{P_R h_{R^*E}}{(N_0 + P_J h_{JE})} = \frac{\xi h_{SR^*} h_{R^*E}}{1 + \xi h_{SJ} h_{JE}} \quad (4)$$

where $\xi \triangleq \frac{2\eta\alpha P_S}{(1-\alpha)N_0}$.

B. Random relay and best jammer (rR-bJ)

In this strategy, the relay R is first randomly selected among $\{I_i\}_{i=1}^{M+1}$. Without loss of the generality, we assume that the $(M+1)$-th intermediate node is the relay, $R = I_{M+1}$. The jammer J^* is then selected among the M remaining intermediate nodes such that the channel power gain of the J^*-E link is largest, i.e.,

$$h_{J^*E} = \max_{i=1,\ldots,M} h_{I_i E} \quad (5)$$

where $h_{I_i E}$ is the channel power gains of the I_i-E link. The instantaneous received SNRs at D and E are, respectively, given by

$$\gamma_D^{\text{rR-bJ}} = (P_R/N_0) h_{RD} = \xi h_{SR} h_{RD}, \quad (6)$$

$$\gamma_E^{\text{rR-bJ}} = \frac{P_R h_{RE}}{N_0 + P_J h_{J^*E}} = \frac{\xi h_{SR} h_{RE}}{1 + \xi h_{SJ^*} h_{J^*E}}. \quad (7)$$

[1]Note that αT is the amount of time used for energy harvesting, while the remaining of the block time, $(1-\alpha)T$, is for information processing.

III. Exact Secrecy Outage Probability

In this section, we consider two transmission strategies at the cooperative nodes: i) Best relay and random jammer (bR-rJ) and ii) random relay and best jammer (rR-bJ). To compare the effect of these two strategies on the security performance of our system, we evaluate the SOP which is given by

$$\mathbb{P}_{\text{out}} = \mathbb{P}\{C_s < R\} = \mathbb{P}\{\gamma_D < \beta\gamma_E + (\beta-1)\} \quad (8)$$

where $\gamma_E \in \{\gamma_E^{\text{bR-rJ}}, \gamma_E^{\text{rR-bJ}}\}$, $\gamma_D \in \{\gamma_D^{\text{bR-rJ}}, \gamma_D^{\text{rR-bJ}}\}$, and $\beta = 2^{\frac{2R}{1-\alpha}} \geq 1$ with $R \geq 0$ and $\alpha \in (0,1)$.

A. Best relay and random jammer (bR-rJ)

By substituting Eq. (3) and Eq. (4) into Eq. (8), the SOP can be expressed as

$$\begin{aligned}\mathbb{P}_{\text{out}}^{\text{bR-rJ}} &= \mathbb{P}\left\{\gamma_D^{\text{bR-rJ}} < \beta\gamma_E^{\text{bR-rJ}} + (\beta-1)\right\} \\ &= \int_0^\infty \underbrace{\mathbb{P}\left\{h_{R^*D} \leq \frac{\beta h_{R^*E}}{1+\xi h_{SJ} h_{JE}} + \frac{(\beta-1)}{\xi x}\right\}}_{\triangleq \Phi_1(x)} f_{h_{SR^*}}(x)dx.\end{aligned} \quad (9)$$

Let $\mathcal{V} \triangleq 1 + \xi h_{SJ} h_{JE}$ and $a \triangleq \frac{\beta-1}{\xi}$, we then rewrite the function $\Phi_1(x)$ in Eq. (9) as

$$\Phi_1(x) = \int_1^\infty \underbrace{\left[\int_0^\infty F_{h_{R^*D}}\left(\frac{\beta h}{v} + \frac{a}{x}\right) f_{h_{R^*E}}(h)dh\right]}_{\triangleq \Phi_2(x,v)} f_{\mathcal{V}}(v)dv \quad (10)$$

where the PDF of $\mathcal{V}$ is derived as Eq. (A.2) in Appendix A. The function $\Phi_2(x,v)$ in Eq. (10) can be calculated as

$$\begin{aligned}\Phi_2(x,v) &= \int_0^\infty \left[1 - \exp\left\{-\frac{1}{\Omega_{\text{ID}}}\left(\frac{\beta h}{v} + \frac{\beta-1}{\xi x}\right)\right\}\right]^M \\ &\quad \times (1/\Omega_{\text{IE}}) \exp\{-h/\Omega_{\text{IE}}\} dh \\ &= 1 - \widetilde{\sum} e^{m(1-\beta)/(\xi x \Omega_{\text{ID}})} \frac{v}{v + m\beta(\Omega_{\text{IE}}/\Omega_{\text{ID}})}\end{aligned} \quad (11)$$

where $\widetilde{\sum} = \sum_{m=1}^M \binom{M}{m}(-1)^{m-1}$. Substituting Eq. (11) and Eq. (A.2) into Eq. (10), we obtain

$$\begin{aligned}\Phi_1(x) &= 1 - \widetilde{\sum} \frac{2}{\xi\Omega_{\text{SI}}\Omega_{\text{IE}}} e^{m(1-\beta)/(\xi x \Omega_{\text{ID}})} \\ &\quad \times \int_1^\infty \frac{v}{v + m\beta(\Omega_{\text{IE}}/\Omega_{\text{ID}})} K_0\left(2\sqrt{\tfrac{v-1}{\xi\Omega_{\text{SI}}\Omega_{\text{IE}}}}\right) dv \\ &= 1 - \widetilde{\sum} e^{\frac{m(1-\beta)}{\xi x \Omega_{\text{ID}}}} \left[1 - \frac{4m\beta}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}} S_{-1,0}\left(\frac{2\phi_m}{\sqrt{\xi}}\right)\right]\end{aligned} \quad (12)$$

where $\phi_m \triangleq \sqrt{\frac{1+m\beta(\Omega_{\text{IE}}/\Omega_{\text{ID}})}{\Omega_{\text{SI}}\Omega_{\text{IE}}}}$, $S_{-1,0}(\cdot)$ is the Lommel function [8, Eq. (10.73.4)], and $K_n(\cdot)$ (with $n = 0, 1, \ldots$) is the modified Bessel function of the second kind [9]. It is noted that the last equality is obtained with the help of [9, Eqs. (6.561.16) and (6.565.7)].

Finally, we substitute Eq. (12) into Eq. (9) and arrive at

$$\begin{aligned}\mathbb{P}_{\text{out}}^{\text{bR-rJ}} &= 1 - \widetilde{\sum}\left[1 - \tfrac{4m\beta}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}} S_{-1,0}\left(\tfrac{2\phi_m}{\sqrt{\xi}}\right)\right] \\ &\quad \times \sqrt{\tfrac{4m(\beta-1)}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}}} K_1\left(\sqrt{\tfrac{4m(\beta-1)}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}}}\right).\end{aligned} \quad (13)$$

B. Random relay and best jammer

By substituting Eq. (6) and Eq. (7) into Eq. (8), the SOP can be expressed as

$$\begin{aligned}\mathbb{P}_{\text{out}}^{\text{bR-rJ}} &= \mathbb{P}\left\{\gamma_D^{\text{rRbJ}} < \beta\gamma_E^{\text{rRbJ}} + (\beta-1)\right\} \\ &= \int_0^\infty \underbrace{\mathbb{P}\left\{h_{RD} \le \frac{\beta h_{RE}}{1+\xi h_{SJ^*} h_{J^*E}} + \frac{(\beta-1)}{\xi x}\right\}}_{\triangleq \Psi_1(x)} f_{h_{SR}}(x)dx.\end{aligned} \tag{14}$$

Let $\mathcal{U} \triangleq 1+\xi h_{SJ^*} h_{J^*E}$, we then rewrite the function $\Psi_1(x)$ in Eq. (14) as

$$\Psi_1(x) = \int_1^\infty \underbrace{\left[\int_0^\infty F_{h_{RD}}\left(\frac{\beta h}{u} + \frac{a}{x}\right) f_{h_{RE}}(h)dh\right]}_{\Psi_2(x,u)} f_{\mathcal{U}}(u)du \tag{15}$$

where the PDF of $\mathcal{U}$ is derived as Eq. (B.2) in Appendix B. The function $\Psi_2(x,u)$ in Eq. (15) can be calculated as

$$\begin{aligned}\Psi_2(x,u) &= \int_0^\infty \left[1 - \exp\left\{-\frac{1}{\Omega_{\text{ID}}}\left(\frac{\beta h}{u} + \frac{a}{x}\right)\right\}\right] \\ &\quad \times (1/\Omega_{\text{IE}}) \exp\left\{-h/\Omega_{\text{IE}}\right\} dh \\ &= 1 - e^{(1-\beta)/(\xi x \Omega_{\text{ID}})} \frac{u}{u + \beta\left(\Omega_{\text{IE}}/\Omega_{\text{ID}}\right)}.\end{aligned} \tag{16}$$

Substituting Eq. (16) and Eq. (B.2) into Eq. (15), we obtain

$$\begin{aligned}\Psi_1(x) &= 1 - \widetilde{\sum} \frac{2m}{\xi\Omega_{\text{SI}}\Omega_{\text{IE}}} e^{(1-\beta)/(\xi x\Omega_{\text{ID}})} \\ &\quad \times \int_1^\infty \frac{u}{u+\beta\left(\Omega_{\text{IE}}/\Omega_{\text{ID}}\right)} K_0\left(2\sqrt{\tfrac{m(u-1)}{\xi\Omega_{\text{SI}}\Omega_{\text{IE}}}}\right) du \\ &= 1 - \widetilde{\sum} e^{\frac{(1-\beta)}{\xi x\Omega_{\text{ID}}}} \left[1 - \frac{4m\beta}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}} S_{-1,0}\left(\frac{2\theta_m}{\sqrt{\xi}}\right)\right]\end{aligned} \tag{17}$$

where $\theta_m \triangleq \sqrt{\frac{m(1+\beta(\Omega_{\text{IE}}/\Omega_{\text{ID}}))}{\Omega_{\text{SI}}\Omega_{\text{IE}}}}$ and the last equality is obtained with the help of [9, Eqs. (6.561.16) and (6.565.7)].

Finally, we substitute Eq. (17) into Eq. (14) and arrive at

$$\begin{aligned}\mathbb{P}_{\text{out}}^{\text{rR-bJ}} &= 1 - \widetilde{\sum}\left[1 - \tfrac{4m\beta}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}} S_{-1,0}\left(\tfrac{2\theta_m}{\sqrt{\xi}}\right)\right] \\ &\quad \times \sqrt{\tfrac{4(\beta-1)}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}}} K_1\left(\sqrt{\tfrac{4(\beta-1)}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}}}\right).\end{aligned} \tag{18}$$

IV. Asymptotic Performance Analysis

A. High SNR regime

1) Best relay and random jammer (bR-rJ): The exact expression for the SOP in (13) relies on two special functions, i.e., $S_{-1,0}(\cdot)$ and $K_1(\cdot)$. Therefore, using the identities [8, Eq. (10.73.4)] for $S_{-1,0}(z)$ and [9, Eq. (8.446)] for $K_1(z)$, we can obtain the approximate expressions for $S_{-1,0}(z)$ and $zK_1(z)$ when $z \to 0$ as follows:

$$S_{-1,0}(z) \overset{z\to 0}{\approx} \frac{1}{2}\ln^2\left(\frac{z}{2}\right) + \gamma\ln\left(\frac{z}{2}\right) + \frac{\gamma^2}{2} + \frac{\pi^2}{12} \triangleq S_{\text{asym}}(z) \tag{19}$$

and

$$zK_1(z) \overset{z\to 0}{\approx} 1 + \frac{z^2}{2}\left[\ln\left(\frac{z}{2}\right) + \gamma - \frac{1}{2}\right] \triangleq K_{\text{asym}}(z) \tag{20}$$

where γ is the Euler - Mascheroni constant. $S_{\text{asym}}(z)$ and $K_{\text{asym}}(z)$ respectively are the approximate expressions for $S_{-1,0}(z)$ and $zK_1(z)$ as $z \to 0$. Owing to the relation $\xi = \frac{2\eta\alpha}{1-\alpha}\frac{P_S}{N_0}$, we have $\lim_{P_S/N_0\to 0} \mathbb{P}_{\text{out}}^{\text{bR-rJ}} = \lim_{\xi^{-1}\to 0} \mathbb{P}_{\text{out}}^{\text{bR-rJ}}$. Applying (19) and (20) to (13), we can obtain the asymptotic expression for the SOP at very high ξ (i.e., $1/\xi \to 0$) as follows:

$$\begin{aligned}\mathbb{P}_{\text{asym}}^{\text{bR-rJ}} &= \lim_{\xi^{-1}\to 0} \mathbb{P}_{\text{out}}^{\text{bR-rJ}} \\ &= 1 - \widetilde{\sum} K_{\text{asym}}\left(\sqrt{\tfrac{4m(\beta-1)}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}}}\right)\left[1 - \tfrac{4m\beta}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}} S_{\text{asym}}\left(\tfrac{2\phi_m}{\sqrt{\xi}}\right)\right].\end{aligned} \tag{21}$$

2) Random relay and best jammer (rR-bJ): Applying (19) and (20) to (18), we can obtain the asymptotic expression for the SOP at very high ξ (i.e., $1/\xi \to 0$) as follows:

$$\begin{aligned}\mathbb{P}_{\text{asym}}^{\text{rR-bJ}} &= \lim_{\xi^{-1}\to 0} \mathbb{P}_{\text{out}}^{\text{rR-bJ}} \\ &= 1 - K_{\text{asym}}\left(\sqrt{\tfrac{4(\beta-1)}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}}}\right)\widetilde{\sum}\left[1 - \tfrac{4m\beta}{\xi\Omega_{\text{SI}}\Omega_{\text{ID}}} S_{\text{asym}}\left(\tfrac{2\theta_m}{\sqrt{\xi}}\right)\right].\end{aligned} \tag{22}$$

Remark 1: If $M = 1$, the exact expressions Eq. (13) and Eq. (18) for the SOP are exactly the same. This also applies to the asymptotic expressions Eq. (21) and Eq. (22) when $M = 1$.

B. Special cases of α

1) $\alpha \to 0^+$: In this case, we have $\xi \to 0$ and $\beta \to 2^{2R}$. From (3)-(4) and (6)-(7), the instantaneous SNRs γ_D and γ_E approach 0. As a result, $\mathbb{P}_{\text{out}}$ in (8) is approximated as

$$\lim_{\alpha\to 0} \mathbb{P}_{\text{out}} = \mathbb{P}\left\{0 < 2^{2R} \times 0 + (\beta - 1)\right\} = 1. \tag{23}$$

2) $\alpha \to 1^-$: In this case, we rewrite $\gamma_D = \frac{c_1}{1-\alpha}$ with $c_1 \in \{\frac{2\eta P_S}{N_0} h_{SR^*} h_{R^*D}, \frac{2\eta P_S}{N_0} h_{SR} h_{RD}\}$ from (3)-(4), and have $\gamma_E \to c_2$ with $c_2 \in \left\{\frac{h_{SR^*}h_{R^*E}}{h_{SJ}h_{JE}}, \frac{h_{SR}h_{RE}}{h_{SJ^*}h_{J^*E}}\right\}$ from (6)-(7). Then $\mathbb{P}_{\text{out}}$ in (8) becomes

$$\lim_{\alpha\to 1^-} \mathbb{P}_{\text{out}} = \lim_{\substack{t\triangleq(1-\alpha)^{-1} \\ t\to+\infty}} \mathbb{P}\left\{c_1 < \frac{2^{2Rt}}{t}c_2 - \frac{1}{t}\right\} = 1. \tag{24}$$

V. Numerical Results

In this section, we evaluate the SOP and verify the analysis through the simulation. Common parameters for both Figs. 2 and 3 are as follows: $M = \{1, 10\}$, $\eta = 0.85$, $R = 0.25$ (bits/s/Hz), $\Omega_{\text{SI}} = 2.5$, $\Omega_{\text{ID}} = 1.5$ and $\Omega_{\text{IE}} = 2$. In Fig. 2, we show the SOP as a function of P_S/N_0 with $\alpha = 0.5$. In Fig. 3 and 4, we fix $P_S/N_0 = 15$ dB, then respectively showing the SOP versus $\alpha \in (0,1)$ and $\eta \in (0,1)$. Based on numerical results, we observe that when M increases, the bR-rJ scheme is more efficient than the rR-bJ scheme in terms of security. Moreover, the secure performance can be further improved when M increases.

Finally, Fig. 2 verifies the agreement between the exact analysis and simulation, while the asymptotic analysis is very close to the exact analysis at high P_S/N_0. Besides, Fig. 3 shows that setting $\alpha \to 0^+$ or $\alpha \to 1^-$ is not beneficial to the secure performance. In Fig. 4, the security level of the system increases with η given that the harvested energy also benefits from this parameter.

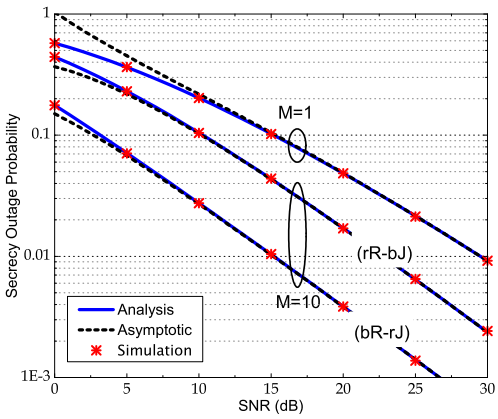

Fig. 2. Secrecy outage probability with $M = \{1, 10\}$, $\eta = 0.85$, $\alpha = 0.5$, $R = 0.25$ (bits/s/Hz), $\Omega_{\rm SI} = 2.5$, $\Omega_{\rm ID} = 1.5$ and $\Omega_{\rm IE} = 2$.

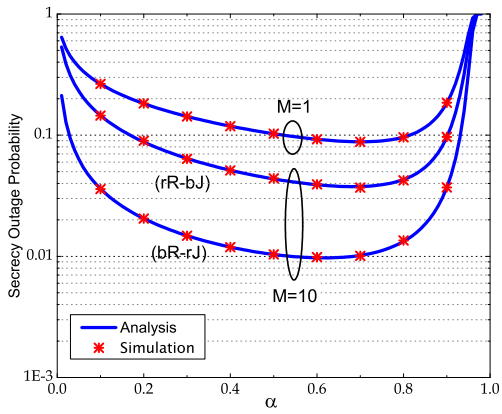

Fig. 3. Secrecy outage probability with $M = \{1, 10\}$, $\eta = 0.85$, $R = 0.25$ (bits/s/Hz), $P_S/N_0 = 15$ dB, $\Omega_{\rm SI} = 2.5$, $\Omega_{\rm ID} = 1.5$ and $\Omega_{\rm IE} = 2$.

VI. Conclusions

This paper has derived exact and asymptotic expressions for the SOP in a cooperative secure network utilizing energy harvesting. Based on analytical and simulation results, we confirm that the security of the proposed system can be further enhanced with increasing number of intermediate nodes and increasing the SNR. More importantly, we show that in the TSR protocol [5], the secure performance deteriorates significantly in two cases: $\alpha \to 0^+$ and $\alpha \to 1^-$. In contrast, the more η becomes, the more secure and harvested energy performance the system gains.

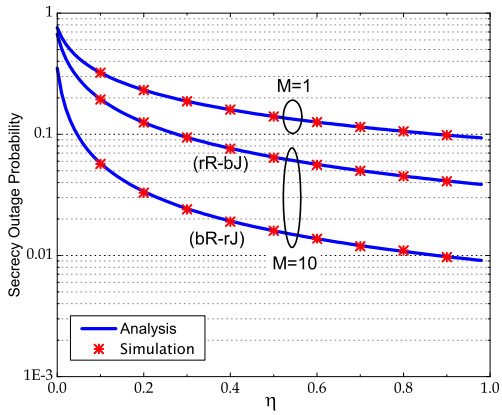

Fig. 4. Secrecy outage probability with $M = \{1, 10\}$, $\alpha = 0.5$, $R = 0.25$ (bits/s/Hz), $P_S/N_0 = 15$ dB, $\Omega_{\rm SI} = 2.5$, $\Omega_{\rm ID} = 1.5$ and $\Omega_{\rm IE} = 2$.

Appendix

A. The distribution of $\mathcal{V} \triangleq 1 + \xi h_{SJ} h_{JE}$

The CDF of $\mathcal{V}$ can be derived as

$$F_{\mathcal{V}}(v) = 1 - 2\sqrt{\tfrac{v-1}{\xi\Omega_{\rm SI}\Omega_{\rm IE}}} K_1\left(2\sqrt{\frac{v-1}{\xi\Omega_{\rm SI}\Omega_{\rm IE}}}\right) \text{ if } v \geq 1, \quad \text{(A.1)}$$

and its PDF is consequently calculated as

$$f_{\mathcal{V}}(v) = \frac{2}{\xi\Omega_{\rm SI}\Omega_{\rm IE}} K_0\left(2\sqrt{\frac{v-1}{\xi\Omega_{\rm SI}\Omega_{\rm IE}}}\right) \text{ if } v \geq 1. \quad \text{(A.2)}$$

B. The distribution of $\mathcal{U} \triangleq 1 + \xi h_{SJ^*} h_{J^*E}$

The CDF of $\mathcal{U}$ can be derived as

$$F_{\mathcal{U}}(u) = 1 - 2\widetilde{\sum}\sqrt{\tfrac{(u-1)m}{\xi\Omega_{\rm IE}\Omega_{\rm SI}}} K_1\left(2\sqrt{\tfrac{(u-1)m}{\xi\Omega_{\rm IE}\Omega_{\rm SI}}}\right) \text{ if } u \geq 1, \quad \text{(B.1)}$$

and its PDF is consequently calculated as

$$f_{\mathcal{U}}(u) = \widetilde{\sum}\tfrac{2m}{\xi\Omega_{\rm SI}\Omega_{\rm IE}} K_0\left(2\sqrt{\tfrac{(u-1)m}{\xi\Omega_{\rm SI}\Omega_{\rm IE}}}\right) \text{ if } u \geq 1. \quad \text{(B.2)}$$

References

[1] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[2] A. E. Shafie, D. Niyato, and N. Al-Dhahir, "Security of rechargeable energy-harvesting transmitters in wireless networks," *IEEE Wirel. Commun. Lett.*, accepted for publication.

[3] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," in *Proc. IEEE ICC*, Sydney, Australia, June 2014, pp. 5413–5418.

[4] M. Zhang and Y. Liu, "Energy harvesting for physical-layer security in OFDMA networks," *IEEE Tran. Infor. Foren. Sec.*, vol. 11, no. 1, pp. 154–162, Jan. 2016.

[5] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, July 2013.

[6] R. Morsi, D. S. Michalopoulos, and R. Schober, "Multiuser scheduling schemes for simultaneous wireless information and power transfer over fading channels," *IEEE Tran. Wireless Commun.*, vol. 14, no. 4, pp. 1967–1982, Apr. 2015.

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

[8] G. N. Watson, *A Treatise on the Theory of Bessel Functions*, 2nd ed. Cambridge, UK: Cambridge University Press, 1944.

[9] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. USA: Academic Press, 2007.