Secure Energy Harvesting Communications with Partial Relay Selection over Nakagami-m Fading Channels

Cheng Yin, Xiangyu He, Nam-Phong Nguyen(✉), and Emiliano Garcia-Palacios

Queen's University Belfast, Belfast, UK
{cyin01,xhe07,pnguyen04}@qub.ac.uk, e.garcia@ee.qub.ac.uk

Abstract. In this paper, a secure energy harvesting relay communication system with partial relay selection over Nakagami-m fading channels is proposed. A power beacon can provide wireless energy for the source and relay. A time-switching-based (TS) radio frequency energy harvesting technique is deployed at the power beacon. An eavesdropper is able to wiretap to the signal transmitted from the source and the relays. The exact closed-form expression of secrecy outage probability is derived. The results show that with increasing number of relays the system performs better in terms of secrecy outage probability (SOP). In addition, the energy harvesting duration has a significant effect on the secrecy outage probability. There exist an optimal energy harvesting duration that can achieve the lowest SOP and therefore this parameter should be carefully designed.

Keywords: Physical layer security · Energy harvesting
Relay networks · Nakagami-m fading

1 Introduction

Human activities are considered the main reason for climate change. A large amount of energy is consumed in wireless communication because of the increasing number of mobile devices and base stations. Therefore, a sustainable network approach has been widely studied [1–3]. Energy harvesting appeals as a promising solution. In conventional terms, renewable energy involves energy like for example solar, wind, vibration or piezoelectric. However, in recent years, RF (radio frequency) [4] energy harvesting (EH) has emerged as a new approach. Radio transmitters around the world can broadcast signals which carry wireless information and can be utilized for power transfer (SWIPT) [5]. Apart from the environmental benefits, energy harvesting is a promising way to prolong the lifetime in energy-constrained networks. There is low maintenance monitoring and no need for replacing or recharging batteries. RF signals can carry information and energy at the same time. In this way, nodes can receive energy for harvesting and also process information [6].

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018
Y. Chen and T. Q. Duong (Eds.): INISCOM 2017, LNICST 221, pp. 100–110, 2018.
https://doi.org/10.1007/978-3-319-74176-5_10

Wireless energy harvesting also brings significant benefits to a cooperative relaying network where the source can transmit information to the destination with the help of relays. This is because energy-constrained relays can harvest energy from a power beacon to stay active [7]. In [8], the authors consider a full-duplex energy harvesting network with time-switching (TS) protocol which allows the relays to harvest energy to forward information from the source to the destination. The authors in [4] propose a relay system where both the source and the relay are energy-constrained, and a power beacon with multi-antenna can provide energy for them.

The deployment of relays to establish longer range communications is desirable for many applications. Although increasing the transmit power can increase the range, it can also bring significant interference which is difficult to prevent. In this context, the relay network is a promising way to extend the coverage of a system. There are two protocols that can be deployed at the relays, i.e., amplify-and-forward (AF) and decode-and-forward (DF) [9]. In AF, the signal will be amplified first then transmitted to the destination, the problem is that the unwanted interference will also be amplified. In DF, the signal is decoded and then forwarded to the destination. Compared with AF, DF has lower interference but the system is complex and high-cost. In addition, relay selection schemes can also enhance relay networks. In [10], the authors investigate a cognitive radio network with best relay selection scheme. The authors in [11] propose a cognitive radio network with buffer-aided relay selection where the relay selected is the one with the highest signal-to-interference (SIR) from all relay nodes.

Another important issue to consider in future communications is security. Due to the broadcast nature of wireless communications, information is vulnerable to be wiretapped by eavesdroppers. Therefore, the security of wireless transmissions has attracted increasing interest. The traditional way to secure wireless communications is deploying upper layer cryptographic techniques. However, cryptographic protocols have been utilized at higher-layers on the unrealistic condition that there are no errors at the physical layer [12]. Other major drawbacks are that cryptographic methods are extremely complex to implement and that when used to encrypt and decrypt data they result in significant energy consumption. Therefore, in recent years, physical layer security (PLS) has emerged as an attractive way to enhance the secrecy performance of a system.

Wyner firstly proposed the classical wiretap channel model in 1975 which recently has been studied with different fading channels such as Rayleigh and Nakagami-m to evaluate the secrecy performance of a system [13]. In PLS networks, most research consider two cooperation techniques: cooperative relaying and cooperative jamming. In [14], an intermediate jammer which can transmit signals to confuse an eavesdropper is considered. Cooperative relaying has been utilized widely in the presence of eavesdroppers [15–24]. Relay selection schemes can be proposed to enhance the performance. In [23], the authors proposed three criteria to select the best relay. In [12], the authors considered outdated relay selection to enhance the performance.

In the research context discussed above energy harvesting has never been considered. However in [18], the combination of energy harvesting, cooperative relaying and PLS in a wireless network is studied over Rayleigh fading. In our research, we extend their work by considering Nakagami-m fading.

Motivated by their research, the secrecy performance of an energy harvesting network with multiple relays in the presence of an eavesdropper over Nakagami-m fading channels is investigated. The contributions of this paper are summarized as follows:

- Partial relay selection is considered to secure the network.
- The exact-closed form expressions of secrecy outage probability (SOP) is derived.
- The results have shown that increasing the number of relays significantly enhances the security performance of the considered system. In addition, the EH duration shows a huge effect on SOP of the considered system. There is optimal point of EH duration in our example which can achieve minimum SOP of the considered system.

The remainder of the paper is organized as follows. System and channel models are described in Sect. 2. Performance analysis with exact closed-form expressions is developed in Sect. 3, while numerical results based on Monte-Carlo simulations to validate the correctness of our analyses is presented in Sect. 4. Finally, the paper is concluded in Sect. 5.

2 System and Channel Models

Consider an energy harvesting network consisting of a power beacon B , an information source S, K DF relays R_k, $k = \{1, ..., K\}$, a destination D and an eavesdropper E , as shown in Fig. 1. The power beacon B, S, R_k, E, and D are equipped with single antenna.The additive white Gaussian noise (AWGN) at R_k and D has zero mean and variance N_0. Assuming all the channels are Nakagami-m fading, and the channel power gains $|h_X|^2$ are gamma distributed with mean power λ_X, and severity parameters m_X, where $X \in \{SR, SE, BS, BR, RE, RD\}$. The cumulative distribution function (CDF) and probability function (PDF) of the random variable X can be written as

$$F_X(x) = 1 - \exp\left(-\frac{x}{\theta_X}\right) \sum_{i=0}^{m_X-1} \frac{1}{i!} \left(\frac{x}{\theta_X}\right)^i, \tag{1}$$

$$f_X(x) = \frac{x^{m_X-1}}{\Gamma(m_X)\theta_X^{m_X}} \exp\left(-\frac{x}{\theta_X}\right). \tag{2}$$

where $\theta_X = \frac{\lambda_X}{m_X}$, and $\Gamma(\cdot, \cdot)$ is the incomplete gamma function [25, Eq. (8.352.6)].

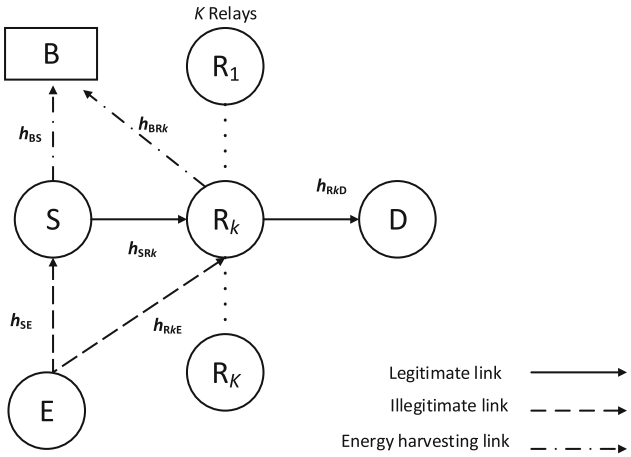

Fig. 1. System model.

2.1 Energy Harvesting Scheme

In the proposed system, S and R_k can harvest energy from B, and then transmit signals with the energy. The power beacon can provide wireless energy to S and R_{k^*}, where the R_{k^*} is the selected aiding relay to forward information. In the paper, time switching (TS) policy based energy harvesting is used, as shown in Fig. 2. In a transmission block time T, S and R_{k^*} harvest energy for αT seconds. Then both $\mathsf{S} \rightarrow \mathsf{R}_{k^*}$ and $\mathsf{R}_{k^*} \rightarrow \mathsf{D}$ transmissions spend $(1-\alpha)T/2$ equally to forward information, where α is the EH time fraction and $0 < \alpha < 1$. Therefore, the harvested energy at S and R_{k^*} are

$$E_{\mathsf{S}} = \eta \mathcal{P}_{\mathsf{B}} \alpha T |h_{\mathsf{BS}}|^2, \tag{3}$$

$$E_{\mathsf{R}} = \eta \mathcal{P}_{\mathsf{B}} \alpha T |h_{\mathsf{BR}_{k^*}}|^2, \tag{4}$$

where η is the efficiency coefficient and $0 < \eta < 1$. $\mathcal{P}_{\mathsf{B}}$ is the transmit power of power beacon B. $|h_{\mathsf{BS}}|^2$ and $|h_{\mathsf{BR}_{k^*}}|^2$ are channel links from power beacon B to source S and B to selected aiding relay R_{k^*}. Assuming the processing energy at S and R_{k^*} can be ignored. Therefore, the transmit power of S and R_{k^*} are

$$\mathcal{P}_{\mathsf{S}} = \frac{2\eta \mathcal{P}_{\mathsf{B}} |h_{\mathsf{BS}}|^2 \alpha}{(1-\alpha)}, \tag{5}$$

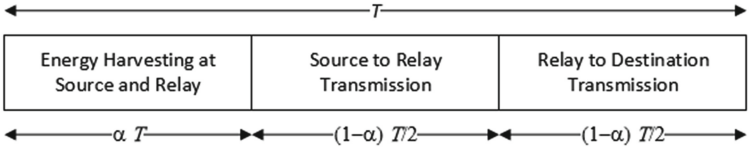

Fig. 2. Time switching based protocol

$$\mathcal{P}_{\mathsf{R}} = \frac{2\eta\mathcal{P}_{\mathsf{B}}|h_{\mathsf{BR}_{k^*}}|^2\alpha}{(1-\alpha)}. \tag{6}$$

2.2 Security Scenarios

In the considered system, E can eavesdrop information during the $\mathsf{S} \rightarrow \mathsf{R}_{k^*}$ and $\mathsf{R}_{k^*} \rightarrow \mathsf{D}$ transmissions. We assume that there is no direct link from $\mathsf{B} \rightarrow \mathsf{E}$. Therefore, the energy harvesting at S and R_{k^*} can not be disturbed in the presence of E. Decode-and-forward (DF) technique and different code books are used in order to enhance the performance of considered system. The secrecy capacity of the considered system is written as

$$C_s = \min(C_{1s}, C_{2s}), \tag{7}$$

where C_{1s} and C_{2s} are the achievable secrecy rate of the first hop and the second hop, they can be expressed as follows:

$$C_{1s} = \frac{1-\alpha}{2}\left[\log_2\left(\frac{1+\gamma_{1\mathsf{M}}}{1+\gamma_{1\mathsf{E}}}\right)\right]^+ = \epsilon\left[\log_2\left(\frac{1+\gamma_{1\mathsf{M}}}{1+\gamma_{1\mathsf{E}}}\right)\right]^+, \tag{8}$$

$$C_{2s} = \frac{1-\alpha}{2}\left[\log_2\left(\frac{1+\gamma_{2\mathsf{M}}}{1+\gamma_{2\mathsf{E}}}\right)\right]^+ = \epsilon\left[\log_2\left(\frac{1+\gamma_{2\mathsf{M}}}{1+\gamma_{2\mathsf{E}}}\right)\right]^+, \tag{9}$$

where $\epsilon = \frac{1-\alpha}{2}$ accounts for the fact that during a block time T, both the first hop and second hop spends $(1-\alpha)T/2$ equally to forward information, and $[x]^+ = \max(x, 0)$. $\gamma_{1\mathsf{M}}$ is the SNR at the first link $\mathsf{S} \rightarrow \mathsf{R}_{k^*}$, $\gamma_{2\mathsf{M}}$ is the SNR at the second link $\mathsf{R}_{k^*} \rightarrow \mathsf{D}$, $\gamma_{1\mathsf{E}}$ is the SNR at $\mathsf{S} \rightarrow \mathsf{E}$ and $\gamma_{2\mathsf{E}}$ is the SNR at $\mathsf{R}_{k^*} \rightarrow \mathsf{E}$. The SNR of the first hop $\gamma_{1\mathsf{M}}$ is given as

$$\gamma_{1\mathsf{M}} = \frac{\mathcal{P}_{\mathsf{S}}|h_{\mathsf{SR}_{k^*}}|^2}{N_0} = \frac{2\eta\alpha\mathcal{P}_{\mathsf{B}}|h_{\mathsf{BS}}|^2|h_{\mathsf{SR}_{k^*}}|^2}{N_0(1-\alpha)} = \xi\gamma_{\mathsf{M}}|h_{\mathsf{BS}}|^2|h_{\mathsf{SR}_{k^*}}|^2, \tag{10}$$

where $\gamma_{\mathsf{M}} = \frac{\mathcal{P}_{\mathsf{B}}}{N_0}$, $\xi = \frac{2\eta\alpha}{(1-\alpha)}$, and $|h_{\mathsf{SR}_{k^*}}|^2$ is the channel power gain of $\mathsf{S} \rightarrow \mathsf{R}_{k^*}$ link. Similarly, $\gamma_{2\mathsf{M}}$, $\gamma_{1\mathsf{E}}$, and $\gamma_{2\mathsf{E}}$ can be written as

$$\gamma_{2\mathsf{M}} = \gamma_{\mathsf{M}}\xi|h_{\mathsf{BR}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2, \tag{11}$$

$$\gamma_{1\mathsf{E}} = \gamma_{\mathsf{E}}\xi|h_{\mathsf{BS}}|^2|h_{\mathsf{SE}}|^2, \tag{12}$$

$$\gamma_{2\mathsf{E}} = \gamma_{\mathsf{E}}\xi|h_{\mathsf{BR}_k}|^2|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2, \tag{13}$$

where $|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2$, $|h_{\mathsf{SE}}|^2$, and $|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2$ are the channel power gains of $\mathsf{R}_{k^*} \rightarrow \mathsf{D}$, $\mathsf{S} \rightarrow \mathsf{E}$, and $\mathsf{R}_{k^*} \rightarrow \mathsf{E}$ links. $\gamma_{\mathsf{E}} = \frac{\mathcal{P}_{\mathsf{B}}}{N_{\mathsf{E}}}$, and N_{E} is the variance of the AWGN at E. In some networks, it is not possible to know the full knowledge of channel state information (CSI) of all the links. Therefore, in this paper, we consider a partial relay selection (PRS) that only need to know CSI of the first hop $\mathsf{S} \rightarrow \mathsf{R}_k$. The best link is selected when the first hop has the maximum SNR, and can be expressed as

$$k^* = \arg\max_{k=1,\ldots,K}(|h_{\mathsf{SR}_k}|^2). \tag{14}$$

Therefore, according to (14), the SNR of the first hop given by (10) can be rewritten as

$$\gamma_{1\mathsf{M}} = \gamma_{\mathsf{M}}\xi|h_{\mathsf{BS}}|^2 \max_{k=1,\ldots,K}(|h_{\mathsf{SR}_{k^*}}|^2), \tag{15}$$

The achievable secrecy rates of PRS scheme in the considered system is written as

$$C_{\mathsf{PRS}} = \epsilon\left[\log_2 \min\left(\frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{BS}}|^2|h_{\mathsf{SR}_{k^*}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{BS}}|^2|h_{\mathsf{SE}}|^2}, \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{BR}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{BR}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2}\right)\right]^+. \tag{16}$$

3 Secrecy Outage Probability

In this section, the closed-form expressions of secrecy outage probability (SOP) for PRS is provided to evaluate the security performance of the considered system. In a communication system, the security outage probability is defined by the probability that the instantaneous mutual information is below a rate R_{th}, and can be expressed as

$$P(C < R_{th}) = P(\gamma < \beta) = F_{\gamma_{\mathsf{PRS}}}(\beta), \tag{17}$$

where $C = \log_2(1+\gamma)$, γ is the SNR of the considered system, and $\beta = 2^{\frac{R_{th}}{\epsilon}}$.

From (16) and(17), we have

$$P(C_{\mathsf{PRS}} < R_{th}) = P(\gamma_{\mathsf{PRS}} < \beta) = F_{\gamma_{\mathsf{PRS}}}(\beta), \tag{18}$$

where

$$\gamma_{\mathsf{PRS}} = \min\left(\frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{BS}}|^2|h_{\mathsf{SR}_{k^*}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{BS}}|^2|h_{\mathsf{SE}}|^2}, \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{BR}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{BR}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2}\right). \tag{19}$$

$F_{\gamma_{\mathsf{PRS}}}(\beta)$ is the cumulative distribution function (CDF) of γ_{PRS}. From (18), we have the following Lemma.

Lemma 1. *The SOP of the considered system in partial relay selection scheme is formulated as follows:*

$$\begin{aligned}
F_{\gamma_{\mathsf{PRS}}}(\beta) = 1 + \sum_{k=1}^{k}\sum_{v=0}^{l}\sum_{l=0}^{k(m_{\mathsf{SR}}-1)}\sum_{i=0}^{m_{\mathsf{RD}}-1}\sum_{j=0}^{i}\binom{k}{k}\binom{l}{v}\binom{i}{j}(-1)^k(\beta-1)^{l-v+i-j}(\gamma_{\mathsf{E}}\beta)^{v+j} \\
\times \frac{w(l,k,m_{\mathsf{SR}})}{i!\gamma_{\mathsf{M}}^{l+i}\xi^{l-v+i-j}\theta_{\mathsf{SR}}^{l}\theta_{\mathsf{RD}}^{i}\Gamma(m_{\mathsf{SE}})\theta_{\mathsf{SE}}^{m_{\mathsf{SE}}}\Gamma(m_{\mathsf{BS}})\theta_{\mathsf{BS}}^{m_{\mathsf{BS}}}\Gamma(m_{\mathsf{RE}})\theta_{\mathsf{RE}}^{m_{\mathsf{RE}}}\Gamma(m_{\mathsf{BR}})\theta_{\mathsf{BR}}^{m_{\mathsf{BR}}}} \\
\times \Gamma(v+m_{\mathsf{SE}})\left(\frac{k\beta}{\theta_{\mathsf{SR}}}+\frac{1}{\theta_{\mathsf{SE}}}\right)^{-(v+m_{\mathsf{SE}})}\Gamma(v+m_{\mathsf{RE}})\left(\frac{\beta\gamma_{\mathsf{E}}}{\gamma_{\mathsf{M}}\theta_{\mathsf{RD}}}+\frac{1}{\theta_{\mathsf{RE}}}\right)^{-(j+m_{\mathsf{RE}})} \\
\times 4\times\left(\frac{k\theta_{\mathsf{BS}}(\beta-1)}{\theta_{\mathsf{SR}}\gamma_{\mathsf{M}}\xi}\right)^{\frac{m_{\mathsf{BS}}-l+v}{2}}\left(\frac{\theta_{\mathsf{BR}}(\beta-1)}{\theta_{\mathsf{RD}}\gamma_{\mathsf{M}}\xi}\right)^{\frac{m_{\mathsf{BR}}-i+j}{2}}\mathbf{K}_{m_{\mathsf{BS}}-l+v}\left(2\sqrt{\frac{k(\beta-1)}{\theta_{\mathsf{SR}}\theta_{\mathsf{BS}}\gamma_{\mathsf{M}}\xi}}\right) \\
\times \mathbf{K}_{m_{\mathsf{BR}}-i+j}\left(2\sqrt{\frac{\beta-1}{\theta_{\mathsf{RD}}\theta_{\mathsf{BR}}\gamma_{\mathsf{M}}\xi}}\right)
\end{aligned} \tag{20}$$

where $\mathbf{K}_1(\cdot)$ *defined in* [25, Eq. (3.471.9)] *is the modified Bessel function of the second kind and* $w(\cdot,\cdot,\cdot)$ *function is derived as*

$$w(l,k,m_{\mathsf{SR}}) = \begin{cases} \left(\frac{1}{l!}\right)^k, & \text{if } l=0 \\ \frac{k}{l!}, & \text{if } l=1 \\ \frac{1}{l}\sum_{q=1}^{l}(qk-l+q)\frac{1}{q!}w(l-q,k,m_{\mathsf{SR}}), & \text{if } 2 \leqslant l \leqslant (m_{\mathsf{SR}}-1) \\ \frac{1}{l}\sum_{q=1}^{m_{\mathsf{SR}}-1}(qk-l+q)\frac{1}{q!}w(l-q,k,m_{\mathsf{SR}}), & \text{if } m_{\mathsf{SR}} \leqslant l < k(m_{\mathsf{SR}}-1) \end{cases} \tag{21}$$

Proof. The proof is given in Appendix A.1.

4 Numerical Results

In this section, the simulation results using Monte Carlo method are provided to validate the accuracy of the above secrecy outage probability analysis. In this section, the following parameters are fixed: γ_{E}=10 dB, $R_{th}=0.2$ bits/s/Hz, $\eta=0.8$. The parameters of channel links are fixed: $m_{\mathsf{BS}}=2$, $\theta_{\mathsf{BS}}=10$, $m_{\mathsf{BR}}=2$, $\theta_{\mathsf{BR}}=10$, $m_{\mathsf{SR}}=2$, $\theta_{\mathsf{SR}}=10$, $m_{\mathsf{RD}}=2$, $\theta_{\mathsf{RD}}=10$. The parameters of the eavesdropping links are designed: $m_{\mathsf{SE}}=2$, $\theta_{\mathsf{SE}}=2$, $m_{\mathsf{RE}}=2$, $\theta_{\mathsf{RE}}=2$.

In Fig. 3, the analysis match the simulation very well. In this setup, $\alpha=0.01$. This is because in Fig. 4, $\alpha=0.01$ seems as an optimal point that has the lowest SOP. The result shows that the number of relays has significant effect on the secrecy outage probability of PRS scheme. More specifically, when K increases, the system performs better in terms of SOP.

Figure 4 investigates the effect of energy harvesting time in a transmission block time on the secrecy outage probability. In the considered system, $k=3$,

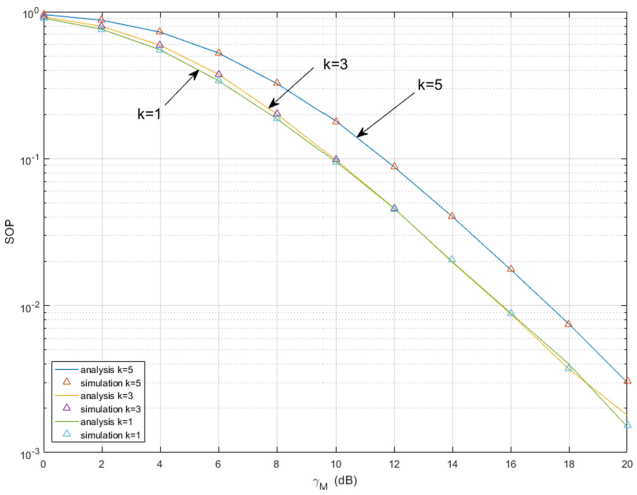

Fig. 3. SOP in PRS scheme with different number of relays

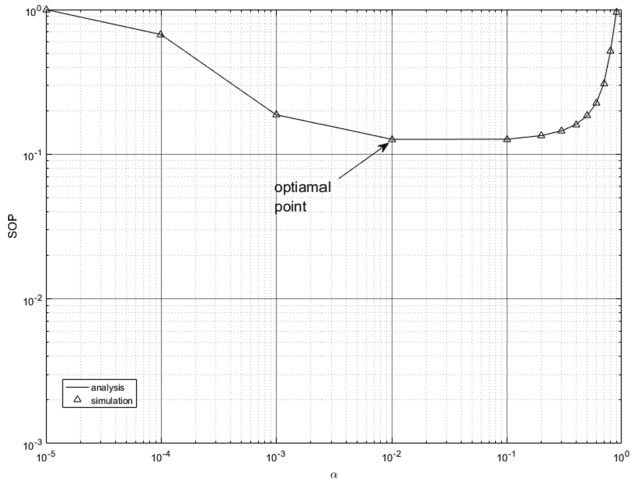

Fig. 4. SOP in PRS scheme is plotted as a function of α

$\gamma_{\mathsf{M}} = 10\,\mathrm{dB}$. The SOP is very large when α is too small or too high. This is because when the energy harvesting time is too long, S and R_{k^*} do not have sufficient time to forward information and when the transmission duration is too long, there is little time for the nodes to harvest energy. In both two cases, the SOP will be extremely large. The results also show that the SOP has an optimal point at $\alpha = 10^{-2}$ in PRS scheme. Specifically, there is very little difference of SOP when α is between 10^{-2} and 10^{-1}. In general, α has a significant effect on the performance of the considered system. Therefore, the EH duration should be mindfully determined in order to secure the communication.

5 Conclusions

In this paper, a system with multiple DF relays and a power beacon with single antenna in the presence of an eavesdropper has been investigated. Partial relay selection has been proposed in order to enhance the performance of the considered system. The exact closed-form expressions of SOP has been derived. The results show that with the increasing number of relays, the security performance can be enhanced. Finally, the EH duration has huge impact on the system performance and should be carefully designed. In our examples, there is an optimal point at α=10^{-2}.

A Appendices

A.1 Proof of Lemma 1

The SNR of first hop and second hop in PRS scheme can be written as

$$\gamma_{1\mathsf{PRS}} = \frac{1 + \gamma_{\mathsf{M}}\xi|h_{\mathsf{BS}}|^2|h_{\mathsf{SR}_{k^*}}|^2}{1 + \gamma_{\mathsf{E}}\xi|h_{\mathsf{BS}}|^2|h_{\mathsf{SE}}|^2}, \tag{A.1}$$

$$\gamma_{2\mathsf{PRS}} = \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{BR}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{BR}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2}. \tag{A.2}$$

The CDF of $\gamma_{1\mathsf{PRS}}$ is expressed as

$$\begin{aligned} P(\gamma_{1\mathsf{PRS}} < x) = 1 + \sum_{k=1}^{K}\sum_{v=0}^{l}\sum_{l=0}^{k(m_{\mathsf{SR}}-1)} \binom{K}{k}\binom{v}{l}(-1)^k(x-1)^{l-v}(\xi)^{v-l}\left(\gamma_{\mathsf{E}}x\right)^v \\ \times \frac{\Gamma(v+m_{\mathsf{SE}})}{\Gamma(m_{\mathsf{SE}})\theta_{\mathsf{SE}}^{m_{\mathsf{SE}}}} \frac{w(l,k,m_{\mathsf{SR}})}{\theta_{\mathsf{SR}}^{l}\gamma_{\mathsf{M}}^{l}} \frac{1}{\Gamma(m_{\mathsf{BS}})\theta_{\mathsf{BS}}^{m_{\mathsf{BS}}}} \left(\frac{\theta_{\mathsf{SR}}\gamma_{\mathsf{M}}\theta_{\mathsf{SE}}}{k\gamma_{\mathsf{E}}x\theta_{\mathsf{SE}}+\theta_{\mathsf{SR}}\gamma_{\mathsf{M}}}\right)^{v+m_{\mathsf{SE}}} \\ \times \mathbf{K}_{m_{\mathsf{BS}}-l+v}\left(2\sqrt{\frac{k(x-1)}{\theta_{\mathsf{SR}}\theta_{\mathsf{BS}}\gamma_{\mathsf{M}}\xi}}\right) \times 2 \times \left(\frac{k(x-1)\theta_{\mathsf{BS}}}{\theta_{\mathsf{SR}}\gamma_{\mathsf{M}}\xi}\right)^{\frac{m_{\mathsf{BS}}-l+v}{2}} \end{aligned} \tag{A.3}$$

The CDF of $\gamma_{2\mathsf{PRS}}$ is expressed as

$$\begin{aligned} P(\gamma_{2\mathsf{PRS}} < x) = 1 - \sum_{i=0}^{m_{\mathsf{RD}}-1}\sum_{j=0}^{i}\binom{i}{j}\frac{1}{i!}\frac{(x-1)^{i-j}(\gamma_{\mathsf{E}}x)^j}{\gamma_{\mathsf{M}}^i\xi^{i-j}\theta_{\mathsf{RD}}^i} \frac{\Gamma(v+m_{\mathsf{RE}})}{\Gamma(m_{\mathsf{RE}})\theta_{\mathsf{RE}}^{m_{\mathsf{RE}}}\Gamma(m_{\mathsf{BR}})\theta_{\mathsf{BR}}^{m_{\mathsf{BR}}}} \\ \times \left(\frac{x\gamma_{\mathsf{E}}}{\gamma_{\mathsf{M}}\theta_{\mathsf{RD}}}+\frac{1}{\theta_{\mathsf{RE}}}\right)^{-(v+m_{\mathsf{RE}})} \mathbf{K}_{m_{\mathsf{BR}}-i+j}\left(2\sqrt{\frac{x-1}{\theta_{\mathsf{RD}}\theta_{\mathsf{BR}}\gamma_{\mathsf{M}}\xi}}\right) \\ \times 2 \times \left(\frac{\theta_{\mathsf{BR}}(x-1)}{\theta_{\mathsf{RD}}\gamma_{\mathsf{M}}\xi}\right)^{\frac{m_{\mathsf{BR}}-i+j}{2}} \end{aligned} \tag{A.4}$$

The SOP of the considered system in PRS scheme is formulated as follows:

$$F_{\gamma_{\mathsf{PRS}}}(\beta) = 1 - [(1 - F_{\gamma_{1\mathsf{PRS}}}(\beta))(1 - F_{\gamma_{2\mathsf{PRS}}}(\beta))] \tag{A.5}$$

After performing some mathematical manipulations, (20) can be achieved with the help of [25, Eq. (3.471.9)].

References

1. Yuen, C., Elkashlan, M., Qian, Y., Duong, T.Q., Shu, L., Schmidt, F.: Energy harvesting communications: Part 1 [Guest Editorial]. IEEE Commun. Mag. **53**(6), 54–55 (2015)
2. Yuen, C., Elkashlan, M., Qian, Y., Duong, T.Q., Shu, L., Schmidt, F.: Energy harvesting communications: Part 2 [Guest Editorial]. IEEE Commun. Mag. **53**(6), 54–55 (2015)
3. Yuen, C., Elkashlan, M., Qian, Y., Duong, T.Q., Shu, L., Schmidt, F.: Energy harvesting communications: Part 3 [Guest Editorial]. IEEE Commun. Mag. **53**(6), 54–55 (2015)
4. Zhong, C., Zheng, G., Zhang, Z., Karagiannidis, G.: Optimum wirelessly powered relaying. IEEE Signal Process. Lett. **22**(10), 1–1 (2015)
5. Zhou, X., Zhang, R., Ho, C.K.: Wireless information and power transfer: Architecture design and rate-energy tradeoff. IEEE Trans. Commun. **61**(11), 4754–4767 (2013)

6. Nasir, A.A., Zhou, X., Durrani, S., Kennedy, R.A.: Relaying protocols for wireless energy harvesting and information processing. IEEE Trans. Wirel. Commun. **12**(7), 3622–3636 (2013)
7. Michalopoulos, D.S., Suraweera, H.A., Schober, R.: Relay selection for simultaneous information transmission and wireless energy transfer: A tradeoff perspective. IEEE J. Sel. Areas Commun. **33**(8), 1 (2015)
8. Mohammadi, M., Chalise, B.K., Suraweera, H.A., Zhong, C., Zheng, G., Krikidis, I.: Throughput analysis and optimization of wireless-powered multiple antenna full-duplex relay systems. IEEE Trans. Commun. **64**(4), 1769–1785 (2016)
9. Rankov, B., Wittneben, A.: Spectral efficient protocols for half-duplex fading relay channels. IEEE J. Sel. Areas Commun. **25**(2), 379–389 (2007)
10. Bao, V.N.Q., Duong, T.Q., da Costa, D.B., Alexandropoulos, G.C., Nallanathan, A.: Cognitive amplify-and-forward relaying with best relay selection in non-identical Rayleigh fading. IEEE Commun. Lett. **17**(3), 475–478 (2013)
11. Chen, G., Tian, Z., Gong, Y., Chambers, J.: Decode-and-forward buffer-aided relay selection in cognitive relay networks. IEEE Trans. Veh. Technol. **63**(9), 4723–4728 (2014)
12. Yang, M., Guo, D., Huang, Y., Duong, T.Q., Zhang, B.: Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-m fading channels. IEEE Trans. Wireless Commun. **15**(12), 8009–8024 (2016)
13. Fan, L., Lei, X., Yang, N., Duong, T.Q., Karagiannidis, G.K.: Secrecy cooperative networks with outdated relay selection over correlated fading channels. IEEE Trans. Veh. Technol. **66**(8), 7599–7603 (2017)
14. Hoang, T.M., Duong, T.Q., Vo, N.S., Kundu, C.: Physical layer security in cooperative energy harvesting networks with a friendly jammer. IEEE Wirel. Commun. Lett. **6**(2), 174–177 (2017)
15. Fan, L., Lei, X., Yang, N., Duong, T.Q., Karagiannidis, G.K.: Secure multiple amplify-and-forward relaying with cochannel interference. IEEE J. Sel. Topics Signal Process. **10**(8), 1494–1505 (2016)
16. Duong, T.Q., Hoang, T.M., Kundu, C., Elkashlan, M., Nallanathan, A.: Optimal power allocation for multiuser secure communication in cooperative relaying networks. IEEE Wirel. Commun. Lett. **5**(5), 516–519 (2016)
17. Huang, Y., Wang, J., Zhong, C., Duong, T.Q., Karagiannidis, G.K.: Secure transmission in cooperative relaying networks with multiple antennas. IEEE Trans. Wireless Commun. **15**(10), 6843–6856 (2016)
18. Nguyen, N.P., Duong, T.Q., Ngo, H.Q., Hadzi-Velkov, Z., Shu, L.: Secure 5G wireless communications: A joint relay selection and wireless power transfer approach. IEEE Access **4**, 3349–3359 (2016)
19. Fan, L., Yang, N., Duong, T.Q., Elkashlan, M., Karagiannidis, G.K.: Exploiting direct links for physical layer security in multiuser multirelay networks. IEEE Trans. Wireless Commun. **15**(6), 3856–3867 (2016)
20. Hoang, T.M., Duong, T.Q., Suraweera, H.A., Tellambura, C., Poor, H.V.: Cooperative beamforming and user selection for improving the security of relay-aided systems. IEEE Trans. Wireless Commun. **63**(12), 5039–5051 (2015)
21. Rodriguez, L.J., Tran, N.H., Duong, T.Q., Le-Ngoc, T., Elkashlan, M., Shetty, S.: Physical layer security in wireless cooperative relay networks: State of the art and beyond. IEEE Commun. Mag. **53**(12), 32–39 (2015)
22. Wang, L., Kim, K.J., Duong, T.Q., Elkashlan, M., Poor, H.V.: Security enhancement of cooperative single carrier systems. IEEE Trans. Inf. Forensics Secur. **10**(1), 90–103 (2015)

23. Fan, L., Lei, X., Duong, T.Q., Elkashlan, M., Karagiannidis, G.K.: Secure multiuser communications in multiple amplify-and-forward relay networks. IEEE Trans. Commun. **62**(9), 3299–3310 (2014)
24. Wang, L., Elkashlan, M., Huang, J., Tran, N.H., Duong, T.Q.: Secure transmission with optimal power allocation in untrusted relay networks. IEEE Wirel. Commun. Lett. **3**(3), 289–292 (2014)
25. Gradshteyn, I.S., Ryzhik, I.M.: Table of Integrals, Series, and Products, 7th edn. Academic press, San Diego (2007)