Security-Reliability Analysis of Power Beacon-Assisted Multi-hop Relaying Networks Exploiting Fountain Codes with Hardware Imperfection

Dang The Hung *, Tran Trung Duy †, Do Quoc Trinh *, Vo Nguyen Quoc Bao †, and Tan Hanh †
* Le Quy Don Technical University, Vietnam
Email: danghung8384@gmail.com, trinhdq@mta.edu.vn
† Posts and Telecommunications Institute of Technology, Vietnam
Email: {trantrungduy, baovnq, tanhanh}@ptithcm.edu.vn

***Abstract*—In this paper, we consider a multi-hop relaying protocol using beacon-assisted energy harvesting. In the proposed protocol, a source encodes its data by Fountain codes, and sends encoded packets to a destination via intermediate relays. An eavesdropper who appears around the destination attempts to receive the encoded packets for the data recovery. For performance evaluation, we derive exact expressions of outage probability (OP) and intercept probability (IP) over Rayleigh fading channels under impact of hardware impairments. Computer simulations are then performed to verify our derivations.**

***Index Terms*—Fountain Codes, outage probability, intercept probability, multi-hop relaying network, beacon-assisted energy harvesting.**

I. Introduction

Recently, power beacon-assisted energy harvesting (PB-EH) [1]–[8] has gained much attention as an efficient method to solve energy-constrained issue in wireless networks such as wireless sensor networks (WSN), wireless ad-hoc networks, etc. In this method, power beacons are deployed in the network to support energy for wireless devices. In [1], [2], the authors proposed the PB-EH schemes in multi-hop underlay cognitive radio (CR) networks. To enhance the end-to-end outage probability (OP) for PB-EH multi-hop relaying protocols in cluster networks, the authors in [3], [4] proposed various relay selection methods. Published works [5], [6] considered PB-assisted wireless power two-way relaying schemes in which two energy constrained sources harvest the radio frequency (RF) energy from a multi-antenna PB for communicating with each other with the assistance of a relay. In [7], the outage performance of partial and opportunistic relay selection strategies in PB-aided dual-hop CR WSNs under impact of hardware imperfection was evaluated. Published work [8] considered a multi-path multi-hop PB-EH secured communication protocol, where all of the transmitters have to adjust their transmit power so that the eavesdroppers cannot decode the received data successfully.

In Fountain codes (FCs) or rateless codes [9], a limitless sequence of the encoded packets can be generated from a given set of the data packets that were divided from an original data. In addition, the original data can be recovered from any subset of the encoded packets, where the size of the subset is only slightly higher than the number of the data packets. With low complexity encoding and decoding algorithms, the implementation of FCs is simple, and they are suitable for the broadcast transmission [9], [10]. However, security has become a critical issue of wireless networks using FCs due to the broadcast of wireless channel. Indeed, since the eavesdroppers can receive the encoded packets, they easily recover the original data with a sufficient number of the encoded packets. As a result, this motivates researchers to propose secured communication methods for FCs-based wireless systems. In [11], [12], a secured delivery scheme exploiting FCs was analyzed, where security is achieved if the intended receiver can receive enough encoded packets before the eavesdropper does. The authors in [13] considered a secured cooperative scenario using FCs at the application layer and cooperative jamming at the physical layer to enhance security and reliability of the data transmission for industrial WSNs. Similar to [13], the authors in [14] investigated secrecy performance of a FCs-based multiple input single output (MISO) protocol in which transmit antenna selection (TAS) and cooperative jamming techniques are exploited to increase the channel quality of the data links and decrease the channel quality of the eavesdropping links, respectively. Published work [15] proposed a Fountain-encoding scheme in Internet of Things (IoT) multicast systems which can reduce the intercept probability (IP) at the eavesdropper.

Different from [11]–[15], this paper proposes a PB-EH multi-hop relaying scheme employing FCs. In the proposed scheme, a source transmits the encoded packets (or Fountain packets) to a destination via intermediate relay nodes. In this network, an eavesdropper who appears around the destination attempts to decode the encoded packets to recover the original data of the source. The main contributions can be summarized as follows:

- We consider a practical model where the transceiver hardware of all the nodes is imperfect due to phase noise,

978-1-5386-6542-8/18/$31.00 ©2018 IEEE

I/Q imbalance and amplifier non-linearity [16]–[18]. We also investigate the impact of the hardware impairments on the system performance.

- An asymmetric fading channel model is studied, i.e., the data and eavesdropping links are Rician fading while the EH links are Rayleigh fading. It is due to the fact that the nodes on the path between the source and the destination can be strategically located by the operator so that the links between them experience line of sight (LOS) [19], [20].
- We derive exact expressions of outage probability (OP) and intercept probability (IP) to evaluate the trade-off between security and reliability for the proposed scheme.
- Monte Carlo simulations are presented to verify the analyzes.

The rest of this paper is organized as follows. The system model of the proposed protocol is described in Section II. In Section III, expressions of OP and IP are derived. The simulation results are presented in Section IV. Finally, Section V concludes the paper.

II. System Model

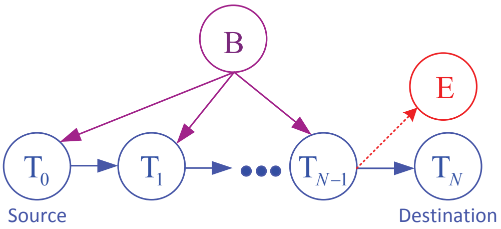

Fig. 1. System model of the proposed protocol.

As presented in Fig. 1, the source (T_0) wants to send its data to the destination (T_N) via $N-1$ relays denoted by T_1, T_2,..., T_{N-1}. We assume that the transmitters such as source and relays are power-constrained wireless devices which have to harvest energy from the power beacon (B). In this network, the eavesdropper (E) appears around the destination so that it can overhear the data sent to this node. Because the eavesdropper is near the destination, we can assume that the node E only receives the data transmitted from the relay T_{N-1}. Assume that all of the terminals have only a single antenna and operate on a half-duplex mode. Therefore, a time division multiple access (TDMA) approach can be employed to send the encoded packets from the source to the destination via N orthogonal time slots.

A. FCs-based multihop relaying protocol

Using FCs, the source first divides its original data into T packets which are used to generate the Fountain packets. Then, the source sends each Fountain packet to the destination with the help of the relay nodes. Let us denote M as the maximum number of the Fountain packets that the source can send to the destination, which is also considered as the allowable delay time in delay-constrained systems. We assume that the source will stop its transmission after sending M encoded packets to the destination. To recover the source data, the destination and the eavesdropper have to successfully receive at least H Fountain packets, where $H = (1+\varepsilon)\,\mathrm{T}$, $H \leq M$, and ε is the decoding overhead which depends on concrete code design [11]–[15]. Let denote L_{D} and L_{E} as the number of Fountain packets that the destination and the eavesdropper can obtain after M time slots, respectively. If $L_{\mathrm{D}} \geq H$, the destination can perfectly recover the original data. Otherwise, i.e., $L_{\mathrm{D}} < H$, an outage event can be stated. For the decoding status at the eavesdropper, if $L_{\mathrm{E}} \geq H$, the source data is intercepted. Otherwise, i.e., $L_{\mathrm{E}} < H$, the data transmission is secure.

B. Formulation of the end-to-end channel capacity

Let us denote τ as the total transmission time of each Fountain packet. Similar to [1]–[8], a duration of $\alpha\tau\,(0 \leq \alpha < 1)$ is used for the source and the relays to harvest energy from the power beacon, and the remaining time $(1-\alpha)\,\tau$ is used for the data transmission. Because the data transmission is split into N time slots, the transmission time of each time slot can be allocated equally by $(1-\alpha)\,\tau/N$.

Next, the energy harvested by the node T_n can be given as

$$Q_n = \eta\alpha\tau P\gamma_{\mathrm{B},n}, \tag{1}$$

where $n = 0, 1, ..., N-1$, $\eta\,(0 \leq \eta \leq 1)$ is energy conversion efficiency, P is transmit power of B, and $\gamma_{\mathrm{B},n}$ is channel gain of the $\mathrm{B} \rightarrow \mathrm{T}_n$ link.

From (1), the average transmit power of T_n can be calculated by

$$P_n = \frac{Q_n}{(1-\alpha)\,\tau/N} = \omega P\gamma_{\mathrm{B},n}, \tag{2}$$

where

$$\omega = \frac{N\eta\alpha}{1-\alpha}. \tag{3}$$

Next, under impact of the hardware impairments, the instantaneous data rate of the $\mathrm{T}_n \rightarrow \mathrm{T}_{n+1}$ link can be given as

$$\begin{aligned} C_n &= \frac{(1-\alpha)\,\tau}{N}\log_2\left(1+\frac{P_n\gamma_{\mathrm{D},n}}{\kappa_{\mathrm{D}}^2 P_n\gamma_{\mathrm{D},n}+\sigma^2}\right) \\ &= \frac{(1-\alpha)\,\tau}{N}\log_2\left(1+\frac{\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}}{\kappa_{\mathrm{D}}^2\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}+1}\right), \end{aligned} \tag{4}$$

where $\gamma_{\mathrm{D},n}$ is channel gain of the $\mathrm{T}_n \rightarrow \mathrm{T}_{n+1}$ link, κ_{D}^2 is total hardware impairment level on all of the data links [16]–[18], σ^2 is variance of Gaussian noises at all of the receivers, and $\Delta = P/\sigma^2$ is transmit signal-to-noise ratio (SNR).

Using decode-and-forward (DF) relaying technique [3], [4], [21], the end-to-end channel capacity of the data link is formulated as

$$C_{\mathrm{D}} = \min_{n=1,2,...,N}(C_n)\,. \tag{5}$$

Similar to (4), the instantaneous data rate of the $\mathrm{T}_{N-1} \rightarrow \mathrm{E}$ link can be given as

$$C_{\mathrm{Eav}} = \frac{(1-\alpha)\tau}{N}\log_2\left(1 + \frac{\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{E}}}{\kappa_{\mathrm{E}}^2\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{E}}+1}\right), \tag{6}$$

where γ_{E} is channel gain of the $\mathrm{T}_{N-1} \rightarrow \mathrm{E}$ link, and κ_{E}^2 is total hardware impairment level on the eavesdropping link.

Also, we can formulate the end-to-end channel capacity of the eavesdropping link as

$$C_{\mathrm{E}} = \min_{n=1,2,\ldots,N-1}\left(C_n, C_{\mathrm{Eav}}\right). \tag{7}$$

Assume that each Fountain packet can be decoded successfully if the end-to-end data rate is higher than a predetermined target rate denoted by C_{th}. Otherwise, the Fountain packet cannot be received correctly. Hence, the probability that the destination cannot correctly receive one encoded packet is given as

$$\rho_{\mathrm{D}} = \Pr\left(C_{\mathrm{D}} < C_{\mathrm{th}}\right). \tag{8}$$

It is worth noting that the probability of the successful decoding of each Fountain packet is $\Pr\left(C_{\mathrm{D}} \geq C_{\mathrm{th}}\right) = 1-\rho_{\mathrm{D}}$. Similarly, the probability that one Fountain packet can be received correctly and incorrectly by the eavesdropper can be given, respectively as

$$\begin{aligned}\rho_{\mathrm{E}} &= \Pr\left(C_{\mathrm{E}} < C_{\mathrm{th}}\right),\\ \Pr\left(C_{\mathrm{E}} \geq C_{\mathrm{th}}\right) &= 1-\rho_{\mathrm{E}}.\end{aligned} \tag{9}$$

C. Channel models

Assume that the EH links experience Rayleigh fading channels because there is non LOS between the power beacon and the transmitters. As a result, the channel gain $\gamma_{\mathrm{B},n}$ is an exponential random variable (RV) whose CDF and PDF are written, respectively as

$$\begin{aligned}F_{\gamma_{\mathrm{B},n}}(x) &= 1-\exp\left(-\lambda_{\mathrm{B},n}x\right),\\ f_{\gamma_{\mathrm{B},n}}(x) &= \lambda_{\mathrm{B},n}\exp\left(-\lambda_{\mathrm{B},n}x\right),\end{aligned} \tag{10}$$

where $\lambda_{\mathrm{B},n}$ is the parameter given as in [21]:

$$\lambda_{\mathrm{B},n} = l_n^{\beta}, \tag{11}$$

where β is path-loss exponent, and l_n is distance between B and T_n.

Because the channel between T_n and T_{n+1} is Rician fading, CDF and PDF of $\gamma_{\mathrm{D},n}$ are given, respectively as in (12):

$$\begin{aligned}&F_{\gamma_{\mathrm{D},n}}(x) = 1-Q_1\left(\sqrt{2K_{\mathrm{D}}}, \sqrt{2\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}x}\right),\\ &f_{\gamma_{\mathrm{D},n}}(x) = \left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}\exp\left(-K_{\mathrm{D}}\right)\\ &\times\exp\left(-\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}x\right)I_0\left(2\sqrt{K_{\mathrm{D}}\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}x}\right),\end{aligned} \tag{12}$$

where $Q_1(.)$ is Marcum-Q function [22], $I_0(.)$ is modified Bessel function of the first kind [23], K_{D} is Rician K-factor of all of the data links, and the parameter $\lambda_{\mathrm{D},n}$ is also modeled as in (11): $\lambda_{\mathrm{D},n} = d_n^{\beta}$, where d_n is distance between T_n and T_{n+1}.

Similarly, CDF and PDF of γ_{E} are written, respectively as

$$\begin{aligned}&F_{\gamma_{\mathrm{D},n}}(x) = 1-Q_1\left(\sqrt{2K_{\mathrm{E}}}, \sqrt{2\left(1+K_{\mathrm{E}}\right)\lambda_{\mathrm{E}}x}\right),\\ &f_{\gamma_{\mathrm{D},n}}(x) = \left(1+K_{\mathrm{E}}\right)\lambda_{\mathrm{E}}\exp\left(-K_{\mathrm{E}}\right)\\ &\times\exp\left(-\left(1+K_{\mathrm{E}}\right)\lambda_{\mathrm{E}}x\right)I_0\left(2\sqrt{K_{\mathrm{E}}\left(1+K_{\mathrm{E}}\right)\lambda_{\mathrm{E}}x}\right),\end{aligned} \tag{13}$$

where K_{E} is Rician K-factor of the $\mathrm{T}_{N-1} \rightarrow \mathrm{E}$ link, $\lambda_{\mathrm{E}} = d_{\mathrm{E}}^{\beta}$, and d_{E} is distance between T_{N-1} and E.

Moreover, with the help of [23, eq. (8.445)], we can express $f_{\gamma_{\mathrm{D},n}}(x)$ in (12) by an infinite series as

$$\begin{aligned}&f_{\gamma_{\mathrm{D},n}}(x) = \exp\left(-K_{\mathrm{D}}\right)\sum_{k=0}^{+\infty}\frac{1}{(k!)^2}\left(K_{\mathrm{D}}\right)^k\\ &\times\left(\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}\right)^{k+1}x^k\exp\left(-\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}x\right).\end{aligned} \tag{14}$$

D. Performance metrics

In this paper, we investigate the outage probability (OP) and intercept probability (IP) for the proposed scheme. As disscussed above, OP and IP can be defined, respectively as

$$\mathrm{OP} = \Pr\left(L_{\mathrm{D}} < H\right),\ \mathrm{IP} = \Pr\left(L_{\mathrm{E}} \geq H\right). \tag{15}$$

III. Performance evaluation

In this section, expressions of OP and IP are derived. At first, we derive the probability ρ_{D} given in (8). Combining (5) and (8), which yields

$$\begin{aligned}\rho_{\mathrm{D}} &= \Pr\left(\min_{n=1,2,\ldots,N}\left(C_n\right) < C_{\mathrm{th}}\right)\\ &= 1-\prod_{n=1}^{N}\left(1-\rho_{\mathrm{D},n}\right),\end{aligned} \tag{16}$$

where $\rho_{\mathrm{D,n}} = \Pr\left(C_n < C_{\mathrm{th}}\right)$. Using (4), we have

$$\begin{aligned}\rho_{\mathrm{D,n}} &= \Pr\left(\frac{\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}}{\kappa_{\mathrm{D}}^2\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n}+1} < \chi\right)\\ &= \Pr\left(\left(1-\kappa_{\mathrm{D}}^2\chi\right)\omega\Delta\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n} < \chi\right),\end{aligned} \tag{17}$$

where

$$\chi = 2^{\frac{NC_{\mathrm{th}}}{(1-\alpha)\tau}}-1. \tag{18}$$

Moreover, from (17), we have

$$\rho_{\mathrm{D},n} = \begin{cases}1, & \text{if } 1-\kappa_{\mathrm{D}}^2\chi \leq 0\\ \Pr\left(\gamma_{\mathrm{B},n}\gamma_{\mathrm{D},n} < \theta_{\mathrm{D}}\right), & \text{if } 1-\kappa_{\mathrm{D}}^2\chi > 0\end{cases} \tag{19}$$

where

$$\theta_{\mathrm{D}} = \frac{\chi}{\left(1-\kappa_{\mathrm{D}}^2\chi\right)\omega\Delta}. \tag{20}$$

Then, from (19), if $1-\kappa_{\mathrm{D}}^2\chi > 0$, $\rho_{\mathrm{D},n}$ can be rewritten by

$$\rho_{\mathrm{D},n} = \int_0^{+\infty}F_{\gamma_{\mathrm{B},n}}\left(\frac{\theta_{\mathrm{D}}}{x}\right)f_{\gamma_{\mathrm{D},n}}(x)\,dx. \tag{21}$$

Substituting (10) and (14) into (21), which yields

$$\rho_{\mathrm{D},n} = 1 - \exp\left(-K_{\mathrm{D}}\right) \sum_{k=0}^{+\infty} \frac{1}{\left(k!\right)^2} \left(K_{\mathrm{D}}\right)^k \left(\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}\right)^{k+1}$$
$$\times \int_0^{+\infty} x^k \exp\left(-\frac{\lambda_{\mathrm{B},n}\theta_{\mathrm{D}}}{x}\right) \exp\left(-\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{D},n}x\right) dx. \quad (22)$$

Next, applying [23, eq. (3.471.9)] for the corresponding integral in (22), we obtain

$$\rho_{\mathrm{D},n} = 1 - \sum_{k=0}^{+\infty} \frac{2}{\left(k!\right)^2} \left(K_{\mathrm{D}}\right)^k \exp\left(-K_{\mathrm{D}}\right)$$
$$\times \left(\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}\right)^{\frac{k+1}{2}}$$
$$\times K_{t+1}\left(2\sqrt{\left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}}\right), \quad (23)$$

where $K_{t+1}\left(.\right)$ is modified Bessel function of the second kind [23].

Combining (16), (19) and (23) together, we can express ρ_{D} as in (24) at the top of the next page, where $\psi_n = \left(1+K_{\mathrm{D}}\right)\lambda_{\mathrm{B},n}\lambda_{\mathrm{D},n}\theta_{\mathrm{D}}$.

Next, with the same derivation method, we can obtain

$$\rho_{\mathrm{E},N} = \Pr\left(C_{\mathrm{Eav}} < C_{\mathrm{th}}\right)$$
$$= \begin{cases} 1, \ \text{if } 1-\kappa_{\mathrm{E}}^2\chi \le 0 \\ 1 - \sum\limits_{k=0}^{+\infty} \frac{2}{(k!)^2}\left(K_{\mathrm{E}}\right)^k \exp\left(-K_{\mathrm{E}}\right)\left(\psi_{\mathrm{E}}\right)^{\frac{k+1}{2}} \\ \qquad \times K_{t+1}\left(2\sqrt{\psi_{\mathrm{E}}}\right), \ \text{if } 1-\kappa_{\mathrm{E}}^2\chi > 0 \end{cases} \quad (25)$$

where

$$\theta_{\mathrm{E}} = \frac{\chi}{\left(1-\kappa_{\mathrm{E}}^2\chi\right)\omega\Delta},$$
$$\psi_{\mathrm{E}} = \left(1+K_{\mathrm{E}}\right)\lambda_{\mathrm{B},N-1}\lambda_{\mathrm{E}}\theta_{\mathrm{E}}. \quad (26)$$

Similar to (16), the probability ρ_{E} can be expressed as

$$\rho_{\mathrm{E}} = \Pr\left(C_{\mathrm{E}} < C_{\mathrm{th}}\right)$$
$$= 1 - \left[\prod_{n=1}^{N-1}\left(1-\rho_{\mathrm{D},n}\right)\right] \times \left(1-\rho_{\mathrm{E},N}\right). \quad (27)$$

Substituting (23) and (25) into (27), an exact expression of ρ_{E} can be obtained. It is worth noting that $\rho_{\mathrm{E}} = 1$ when $1-\kappa_{\mathrm{E}}^2\chi \le 0$. In addition, ρ_{E} depends on the decoding status at the n-th hop ($\rho_{\mathrm{D},n}$), where $n = 1, 2, ..., N-1$.

Next, we evaluate the outage probability (OP) which can be calculated as

$$\mathrm{OP} = \Pr\left(L_{\mathrm{D}} < H\right)$$
$$= \sum_{L_{\mathrm{D}}=0}^{H-1} C_M^{L_{\mathrm{D}}} \rho_{\mathrm{D}}^{L_{\mathrm{D}}} \left(1-\rho_{\mathrm{D}}\right)^{M-L_{\mathrm{D}}}. \quad (28)$$

Equation (28) implies that the destination cannot recover the original data of the source because the number of Fountain packets received is less than H. Also, the intercept probability (IP) can be given as

$$\mathrm{IP} = \Pr\left(L_{\mathrm{E}} \ge H\right)$$
$$= \sum_{L_{\mathrm{E}}=H}^{M} C_M^{L_{\mathrm{E}}} \rho_{\mathrm{E}}^{L_{\mathrm{E}}} \left(1-\rho_{\mathrm{E}}\right)^{M-L_{\mathrm{E}}}. \quad (29)$$

IV. Simulation Results

In this section, we present Monte Carlo simulations to validate the formulas derived in the previous section. We consider a two-dimensional plane xOy in which the coordinates of the node T_n and B are $(n/N, 0)$ and (0.5, 0.5), respectively, where $n = 0, 1, ..., N$. Hence, the source is located at the origin (0,0), while the destination is placed at (1, 0). Because the eavesdropper is near the destination, its position is assumed to be (1, 0.2). In all of the simulations, we fix the values of path-loss exponent (β), the number of Fountain packets required for the data recovery (H), the total transmission time of each time slot (τ), and the energy conversion efficiency (η) by 3, 5, 1, and 1, respectively. Moreover, to present the theoretical results, the infinite series are truncated by 50 first terms.

Figures 2 and 3 present ρ_{D} and ρ_{E} as a function of the transmit SNR (Δ) in dB with various number of hops (N). The results show that ρ_{D} and ρ_{E} decrease with the increasing of Δ and N. As illustrated, the simulation (Sim) and theoretical (Theory) results match very well which validates our derivations in Section III.

In Figs. 4-5, we investigate the trade-off between security and reliability. As we can see, OP in Fig. 4 decreases as increasing the transmit SNR (Δ). However, as shown in Fig. 5, IP rapidly increases with higher Δ values. It is seen in Fig. 5 that when Δ is higher than 6 dB, the original data is almost intercepted, i.e., IP $\approx$ 1. Figures 4 and 5 also present the impact of the fraction of time allocated to the EH phase on the values of OP and IP. Particularly, OP is lowest and highest with $\alpha = 0.3$ and $\alpha = 0.6$, respectively, while the intercept possibility of the eavesdropper is best and worst at $\alpha = 0.3$ and $\alpha = 0.6$, respectively.

Figure 6 presents OP and IP as a function of α with various hardware impairment levels. As observed, there exist values of α so that OP is lowest and IP is highest. For example, when $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0.015$, the best outage performance and the highest intercept possibility can be obtained at $\alpha = 0.175$. We also see in these figures that OP is higher and IP is lower when the hardware impairment levels κ_{D}^2 and κ_{E}^2 increase.

In Fig. 7, we investigate the impact of the number of hops on the values of OP and IP. In this figure, the minimum value of OP is obtained at $N = 4$. We also see that as increasing the value M from 6 to 8, OP significantly decreases. However, increasing the number of time slots used for transmitting the Fountain packets (M) also increases the intercept probability because the eavesdropper has more opportunity to receive sufficient number of packets.

From Figs. 4-7, we can see that the simulation results are in good agreement with the theoretical ones, which again verifies the correction of our derivations.

V. CONCLUSIONS

In this paper, we investigated the trade-off between security and reliability for power beacon-assisted energy harvesting multi-hop relaying networks employing Fountain codes under impact of the hardware impairments. The outage performance can be enhanced by increasing the transmit SNR, selecting the number of hops appropriately and designing the optimal

$$\rho_{\mathrm{D}} = \begin{cases} 1, & \text{if } 1-\kappa_{\mathrm{D}}^2\chi \le 0 \\ 1 - \prod\limits_{n=1}^{N} \left[\sum\limits_{k=0}^{+\infty} \frac{2}{(k!)^2} (K_{\mathrm{D}})^k \exp\left(-K_{\mathrm{D}}\right) (\psi_n)^{\frac{k+1}{2}} K_{t+1}\left(2\sqrt{\psi_n}\right) \right], & \text{if } 1-\kappa_{\mathrm{D}}^2\chi > 0 \end{cases} \tag{24}$$

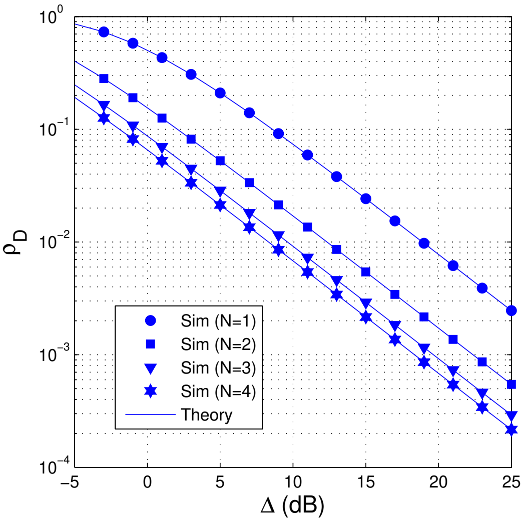

Fig. 2. ρ_{D} as a function of Δ in dB when $K_{\mathrm{D}} = 10$, $K_{\mathrm{E}} = 5$, $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0.01$, $\alpha = 0.25$, and $C_{\mathrm{th}} = 0.5$.

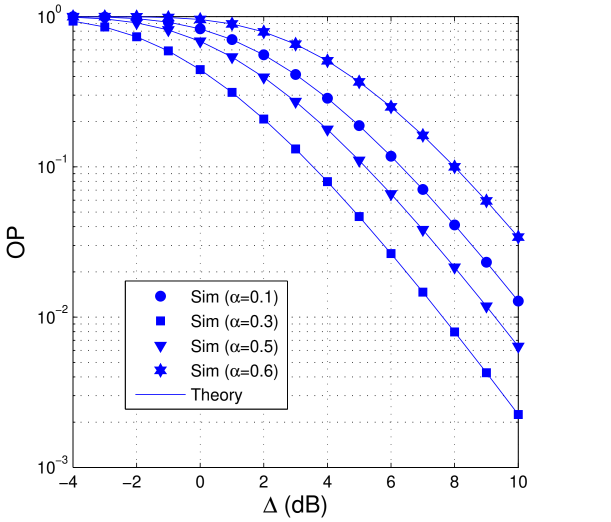

Fig. 4. OP as a function of Δ in dB when $N = 3$, $K_{\mathrm{D}} = 10$, $K_{\mathrm{E}} = 5$, $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0$, $C_{\mathrm{th}} = 1$, $M = 7$, and $H = 5$.

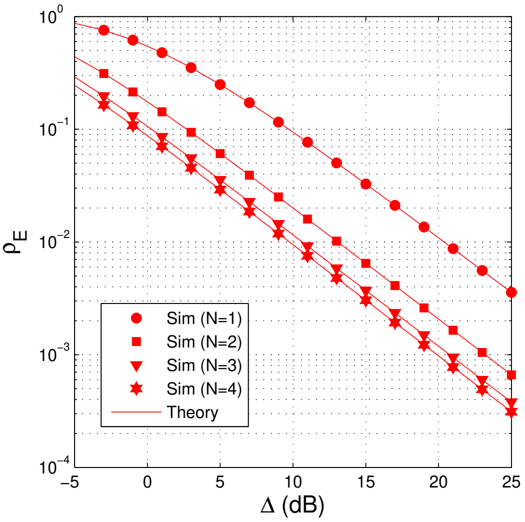

Fig. 3. ρ_{E} as a function of Δ in dB when $K_{\mathrm{D}} = 10$, $K_{\mathrm{E}} = 5$, $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0.01$, $\alpha = 0.25$, and $C_{\mathrm{th}} = 0.5$.

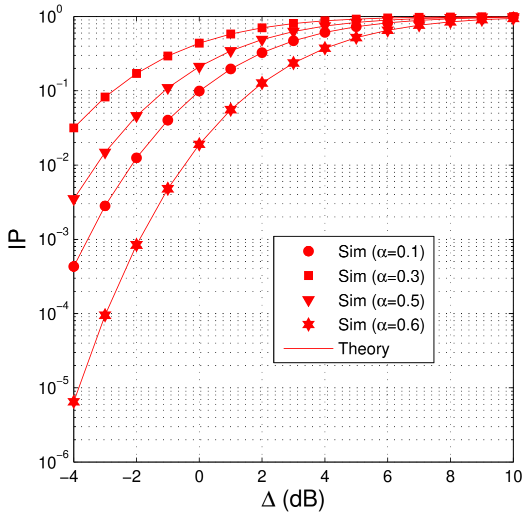

Fig. 5. IP as a function of Δ in dB when $N = 3$, $K_{\mathrm{D}} = 10$, $K_{\mathrm{E}} = 5$, $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0$, $C_{\mathrm{th}} = 1$, $M = 7$, and $H = 5$.

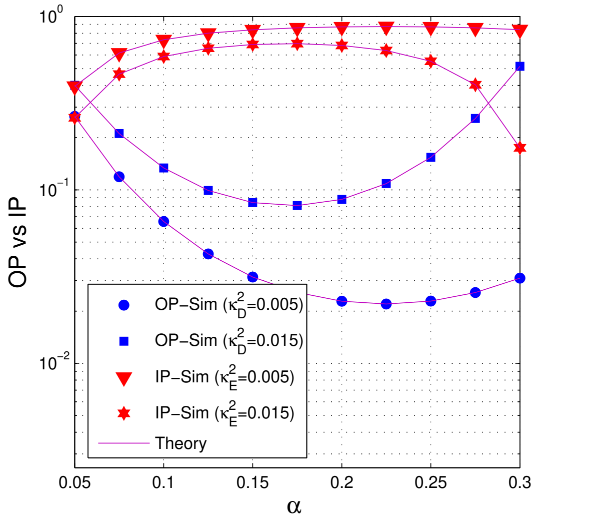

Fig. 6. OP and IP as a function of α when $\Delta = 5$ dB, $N = 4$, $K_{\mathrm{D}} = 20$, $K_{\mathrm{E}} = 1$, $C_{\mathrm{th}} = 1$, $M = 8$, and $H = 5$.

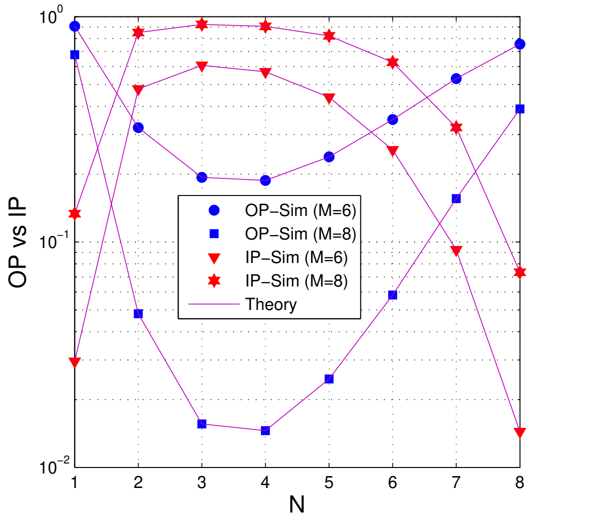

Fig. 7. OP and IP as a function of N when $\Delta = 3$ dB, $K_{\mathrm{D}} = 20$, $K_{\mathrm{E}} = 1$, $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0$, $C_{\mathrm{th}} = 0.9$, $M = 8$, and $H = 5$.

duration for the energy harvesting phase. However, the results also showed that the intercept probability would increase with the decreasing of the outage probability. Therefore, the system parameters should be designed appropriately so that the proposed scheme can obtain the target QoS and the intercept probability is as small as possible.

ACKNOWLEDGE

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2017.317

REFERENCES

[1] C. Xu, M. Zheng, W. Liang, H. Yu, and Y. C. Liang, "Outage performance of underlay multihop cognitive relay networks with energy harvesting," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1148–1151, Jun. 2016.

[2] ——, "End-to-end throughput maximization for underlay multi-hop cognitive radio networks with rf energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3561–3572, Jun. 2017.

[3] N. T. Van, N. T. Do, V. N. Q. Bao, and B. An, "Performance analysis of wireless energy harvesting multihop cluster-based networks over nakgami-m fading channels," *IEEE Access*, vol. 6, pp. 3068–3084, Dec. 2017.

[4] V. N. Q. Bao, N. T. Van, and T. T. Duy, "Exact outage analysis of energy-harvesting multihop cluster-based networks with multiple power beacons over nakagami-m fading channels," in *SigTelCom*, HoChiMinh city, Vietnam, 2018, pp. 1–6.

[5] H. Liang, C. Zhong, H. Lin, H. A. Suraweera, F. Qu, and Z. Zhang, "Optimization of power beacon assisted wireless powered two-way relaying systems under user fairness," in *IEEE Globecom*, Singapore, 2017, pp. 1–6.

[6] C. Zhong, H. Liang, H. Lin, H. A. Suraweera, F. Qu, and Z. Zhang, "Energy beamformer and time split design for wireless powered two-way relaying systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 1–14, Jun. 2018.

[7] T. D. Hieu, T. T. Duy, L. T. Dung, and S. G. Choi, "Performance evaluation of relay selection schemes in beacon-assisted dual-hop cognitive radio wireless sensor networks under impact of hardware noises," *Sensors*, vol. 18, no. 6, pp. 1–24, Jun. 2018.

[8] T. D. Hieu, T. T. Duy, and B.-S. Kim, "Performance enhancement for multi-hop harvest-to-transmit wsns with path-selection methods in presence of eavesdroppers and hardware noises," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 5173–5186, Jun. 2018.

[9] D. J. C. Mackay, "Fountain codes," *IEEE Proc. Commun.*, vol. 152, pp. 1062–1068, 2005.

[10] J. Castura and Y. Mao, "Rateless coding for wireless relay channels," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1638–1642, May 2018.

[11] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 777–780, May 2014.

[12] W. Li, Q. Du, L. Sun, P. Ren, and Y. Wang, "Security enhanced via dynamic fountain code design for wireless delivery," in *IEEE WCNC*, Doha, Quatar, 2016, pp. 1–6.

[13] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 291–300, Feb. 2016.

[14] D. T. Hung, T. T. Duy, D. Q. Trinh, and V. N. Q. Bao, "Secrecy performance evaluation of tas protocol exploiting fountain codes and cooperative jamming under impact of hardware impairments," in *SigTelCom*, HoChiMinh city, Vietnam, 2018, pp. 164–169.

[15] Q. Du, Y. Xu, W. Li, and H. Song, "Security enhancement for multicast over internet of things by dynamically constructed fountain codes," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–11, 2018.

[16] M. Matthaiou and A. Papadogiannis, "Two-way relaying under the presence of relay transceiver hardware impairments," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1136–1139, Jun. 2013.

[17] T. T. Duy, T. Q. Duong, D. da Costa, V. Bao, and M. Elkashlan, "Proactive relay selection with joint impact of hardware impairment and co-channel interference," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1594–1606, May 2015.

[18] P. T. Tin, D. T. Hung, T. T. Duy, and M. Voznak, "Analysis of probability of non-zero secrecy capacity for multi-hop networks in presence of hardware impairments over nakagami-m fading channels," *RadioEngineering*, vol. 25, no. 4, pp. 774–782, Dec. 2016.

[19] H. A. Suraweera, R. H. Y. Louie, Y. Li, G. K. Karagiannidis, and B. Vucetic, "Two hop amplify-and-forward transmission in mixed rayleigh and rician fading channels," *IEEE Commun. Lett.*, vol. 13, no. 4, pp. 227–229, Apr. 2009.

[20] T. Q. Duong, T. T. Duy, M. Matthaiou, T. Tsiftsis, and G. K. Karagiannidis, "Cognitive cooperative networks in dual-hop asymmetric fading channels," in *IEEE Globecom*, Atlanta, GA, 2013, pp. 977–983.

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

[22] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Performance Analysis*. Wiley, 2000.

[23] D. Zwillinger, *Table of integrals, series, and products*. Elsevier, 2014.