# Performance Enhancement for Multi-hop Harvest-to-Transmit WSNs With Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises

**Article** *in* IEEE Sensors Journal · June 2018

DOI: 10.1109/JSEN.2018.2829145

**3 authors**, including:

Hieu Tran-Dinh

University of Luxembourg

**27** PUBLICATIONS **129** CITATIONS

SEE PROFILE

Tran Trung Duy

Institute of Technology Telecommunications

**135** PUBLICATIONS **1,284** CITATIONS

SEE PROFILE

# Performance Enhancement for Multi-hop Harvest-to-Transmit WSNs With Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises

Tran Dinh Hieu, Tran Trung Duy *Member*, *IEEE* Byung-Seo Kim *Senior Member*, *IEEE*

***Abstract*—Energy-harvesting-based physical layer security (PLS) has become a promising technique, as it not only secures information from eavesdropping without upper layer data encryption, but it also improves the energy efficiency of wireless networks. However, it imposes new challenges, as adversary parties can overhear the transmission of confidential information between the source and destination via a relay. Therefore, the transmit power of the signals must be large enough for energy harvesting, but it must also be small enough to avoid eavesdropping. This is even more challenging with multi-hop multi-path wireless networks. Motivated by these observations, this paper proposes three innovative protocols, namely, the shortest path selection (SPS) protocol, random path selection (RPS) protocol, and best path selection (BPS) protocol. These will enhance the security of multi-hop multi-path randomize-and-forward (RF) cooperative wireless sensor networks (WSNs) under the presence of eavesdroppers and hardware impairment, wherein the source node and relay nodes are capable of harvesting energy from beacon for data transmission. Furthermore, we derive exact closed-form expressions and the asymptotic outage probability for each protocol under multiple eavesdropping attacks. The simulation results validate the theoretical results.**

***Index Terms*—Energy harvesting, power beacon, wireless sensor networks, physical-layer security, randomize-and-forward (RF), multi-hop multi-path networks, path selection, hardware impairments, outage probability.**

## I. Introduction

In the past two decades, wireless sensor networks (WSNs) are one of the most promising emerging technologies and they are widely utilized in many areas such as military, agriculture and industrial applications. A survey on different attributes and applications of WSNs is given in [1]. More specifically, the authors gave a comprehensive description of numerous applications of WSNs in urban environments, i.e., power system monitoring, temperature monitoring, traffic monitoring, gas monitoring, underground monitoring, tsunami detection, healthcare applications, transportation applications, ... Moreover, they listed all the papers related to each application and included many examples that sufficiently fit the scenario.

Since it is usually very difficult to replace or recharge batteries and even be prohibitive, i.e., in the battlefield environments. Therefore, a lot of researches for energy efficiency and energy harvesting in WSNs are developed [2]–[4]. In [2], Akhtar et al. surveyed all the potential renewable energy sources (i.e., solar, vibration, heat, wind, ...) along with their characteristics and applications in WSNs. Besides that, this study also discussed about techniques used for scavenging, storage method, and deployment architecture. A stability-aware geographic routing for reliable data transmissions in energy-harvesting wireless sensor networks (EH-WSNs) to provide a reliable routes selection method and potentially achieve an unlimited network lifetime are proposed in [3]. Specifically, to investigate the network performance, the authors considered not only residual energy and harvested energy but also estimated packet reception rate of wireless link and location information to select routing paths from a source node to a sink node. Based on Hilbert Space Filling Curve, Ghafoor et al. [4] proposed a novel approach for mobile sink trajectory in WSNs in which the curve order changed according to node density.

Besides energy harvesting (EH) from solar, piezoelectric shoe inserts, small vibration microwave ovens, thermoelectricity, and acoustic noise, radio frequency (RF) EH has recently emerged as a promising technique due to its capability of carrying both information and energy simultaneously [5]–[9]. Moreover, the RF EH technique can improve the network performance by providing a perpetual energy supply for energy-constrained devices, such as wireless sensors. However, it is difficult for practical circuits to harvest and decode the information from the same signals. To make theoretical progress, the authors in [10]–[12] proposed some practical receiver designs for simultaneous wireless information and power transfer (SWIPT). For EH wireless sensor networks (WSNs), cooperative communication protocols [13] can be used efficiently to reduce error rates, to extend coverage and to prolong the network lifetime. In particular, in [14], a cooperative clustered WSNs was proposed, where the relay nodes harvest energy from the ambient RF signals to forward the source data to the intended destinations. The authors in [15] designed a cooperative cognitive protocol to solve the power and spectrum issues in WSNs. Meanwhile, the published work [16] proposed a novel cooperative SWIPT scheme to maximize energy efficiency for wirelessly powered sensor networks.

T. D. Hieu is with the Department of Radio and Communication Engineering, Chungbuk National University, Republic of Korea (e-mail: trandinhhieu1989@gmail.com).

T. T. Duy is with Posts and Telecommunications Institute of Technology, Vietnam (e-mail: trantrungduy@ptithcm.edu.vn).

B. S. Kim is with Department of Computer and Information Communication Engineering, Hongik University, Korea (e-mail: jsnbs@hongik.ac.kr).

To improve the system performances of energy-constrained networks further, multi-hop relay methods were also proposed and analyzed in [17]–[20]. The authors in [17] evaluated the performance of the EH-based multi-hop networks using amplify-and-forward (AF) and decode-and-forward (DF) techniques. In [18], a virtual multiple-input multiple-output (MIMO) model for multi-hop, multi-path networks were considered, where all the nodes rely on EH for data transmission. Different from [17] and [18], the EH nodes in [19] harvest energy from both the data transmission and the energy links from nearby routers to compensate for the energy shortage. In [20], a cooperative multi-hop scenario in which intermediate relays are capable of harvesting energy from co-channel interferences to forward the data was proposed. In [21] and [22], the authors analyzed the system performance of underlay multi-hop cognitive radio (CR) networks, where secondary users harvest energy from a beacon [21] or from a primary transmitter [22].

Due to the broadcast nature of wireless channels, the unauthorized parties can overhear the confidential information transmitted by the authorized nodes, and hence security has become a critical issue for wireless communication systems. However, with numerous sensor nodes in the networks, the deployment of cryptographic methods can be too complex and costly. Recently, physical-layer security (PLS) [23], [24] has emerged as a promising technique to enable the security of data transmission. Again, cooperative relay protocols can be used efficiently to enhance the secrecy performance of the secured communication. In [25] and [26], the authors proposed relay selection strategies to improve the secrecy performance at the cooperative phase (second phase). In [27], both DF and AF protocols were studied. Different from the DF technique, the source and relay nodes in the RF one would generate random codebooks to prevent eavesdroppers from combining the overheard data using maximal ratio combining (MRC). In [28] and [29], multiple eavesdropper models were proposed, where eavesdroppers can share their received data together to decode the overheard information. The authors in [30] proposed a joint relay and destination selection scheme to enhance the secrecy performances in the presence of active eavesdroppers.

More recently, the published works [31]–[35] were concerned with secured communication in various EH wireless networks. In particular, the authors in [31] solved the optimal problem of maximizing aggregate harvested power among all users while satisfying the secrecy rate requirement. Moreover, this paper also used the power splitting (PS) method to prevent eavesdroppers from retrieving information from an orthogonal frequency division multiplexing access (OFDMA) system. In [32], secure transmission in the SWIPT system where a source node transmits the information to a full-duplex destination in the presence of a passive eavesdropper was investigated. The authors in [33] proposed and evaluated the secrecy performances for CR SWIPT networks. In [34], wireless-powered cooperative CR networks were investigated, where secondary users are potential eavesdroppers. Lei et al. [35] studied the secrecy outage performance of optimal and suboptimal antenna selection schemes for MIMO underlay CR networks in which a secondary transmitter is powered via the RF signals from a primary source. In [36] and [37], researchers proposed cooperative jamming methods using jammer nodes that harvest energy to generate artificial noises for eavesdroppers.

All the above works have provided useful guidance regarding the performance of EH-based PLS to help system designers make precise decisions. However, most only focus on dual-hop relay networks. In energy-constrained WSNs, multi-hop relay protocols can be used to lower power consumption and extend coverage. Conventionally, direct transmission is employed at each hop to forward the data to the next hop [38], [39]. To improve the performance for multi-hop relay systems over fading channels, the authors in [40] and [41] proposed cooperative routing protocols in which intermediate relays on the primary route can cooperate together to exploit spatial diversity. In [42] and [43], path-selection based multi-hop DF protocols were proposed and analyzed, where the best path between the source and destination nodes is selected, following a max-min selection criterion. Particularly, in [44], the authors proposed a novel protocol to enhance the outage performance of multi-hop multi-path EH cooperative CR networks in the presence of the eavesdropper.

Until now, almost all published works have assumed that the hardware transceivers of wireless devices are perfect. However, physical transceivers of low-cost sensor nodes often suffer from impairments due to phase noises, amplifier-amplitude non-linearity and I/Q imbalance (IQI) [45]–[47]. The results in [45]–[47] presented that the hardware imperfection significantly degrades the performance of wireless networks. In [48], the authors investigated the effects of IQI on the secrecy rate of OFDMA systems. Meanwhile, the published work [49] evaluated the probability of a non-zero secrecy capacity for multi-hop relay networks in the presence of hardware noises over Nakagami-$m$ fading channels. In [50] and [51], the authors proposed EH-based relay methods to compensate for the impact of hardware impairments.

In this paper, we consider multi-path, multi-hop WSNs in the presence of active eavesdroppers, where the source and intermediate relay nodes harvest energy from a beacon to forward data to a destination. The main motivation and contributions of this paper can be summarized as follows:

- We propose path-selection methods such as random path selection (RPS), shortest path selection (SPS), and best path selection (BPS). In RPS, the source selects randomly a path to communicate with the destination. In SPS, the path with the lowest number of hops is chosen. Next, to obtain the optimal outage performance, the BPS method selects the path that provides the highest end-to-end channel capacity.
- We consider a practical WSN application, where all hardware transceivers suffer from impairments.
- The RF technique is employed by the source and relay nodes to prevent the eavesdroppers from combining the source data received over multiple hops. Moreover, these authorized transmitters can adjust their transmit power to reduce the channel capacity obtained on the eavesdropping links.

- Both non-colluding and colluding eavesdropping scenarios are considered in this paper.
- We derive closed-form expressions of outage probability (OP) over a Rayleigh fading channel. Monte Carlo simulations are then presented to verify our derivations.

The paper is organized as follows. Section II describes the system model used in this paper. The performance evaluation is shown in Section III. The simulation results are shown in Section IV. Finally, the paper is concluded in Section V.

## II. System model

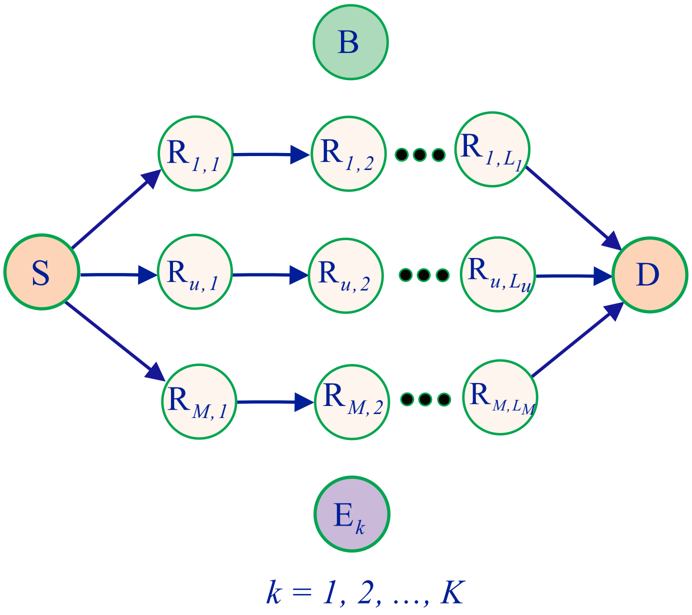


Fig. 1: System model of harvest-to-transmit multi-hop networks in presence of eavesdroppers.

In Fig. 1, we present a system model of the proposed protocol, in which the source S communicates with the destination D via the multi-hop fashion. Moreover, there are $M$ available paths between the source and the destination, and one is selected to serve the source-destination communication. Let us denote $L_u$ as the number of relay nodes (denoted by $\mathrm{R}_{u,1}$, $\mathrm{R}_{u,2}$, ..., $\mathrm{R}_{u,L_u-1}$ and $\mathrm{R}_{u,L_u}$) on the $u$th path, where $u = 1, 2, ..., M$ and $L_u \geq 1$. Moreover, there exist $K$ active eavesdroppers (i.e., $\mathrm{E}_1$, $\mathrm{E}_2$, ..., $\mathrm{E}_{K-1}$ and $\mathrm{E}_K$) attempting to overhear the data transmitted by the source and the relay nodes. To prevent the eavesdroppers from combining the received data with the MRC combiner, the RF strategy [27] is employed at each hop on the selected path. Assume that all the transmitters, including the source and relays, are energy-constrained devices; hence, they have to harvest the RF energy from the beacon B deployed in the network. It is also assumed that all of the terminals are low-cost sensor nodes that are equipped with a single antenna and that operate in a half-duplex mode. As a result, the data transmission is realized by time division multiple access (TDMA) over orthogonal time slots.

Assume that the $u$th path is selected for the data transmission which is split into $L_u$ + 1 orthogonal time slots. In particularly, in the $(j+1)$th time slot, the node $\mathrm{R}_{u,j}$ transmits the source data $s$ to the node $\mathrm{R}_{u,j+1}$, where $j = 0, 1, 2, ..., L_u$. Moreover, we note that $\mathrm{R}_{u,0} \equiv \mathrm{S}$ and $\mathrm{R}_{u,L_u+1} \equiv \mathrm{D}$ for all $u$. In the presence of hardware impairments, the received signal of the transmission $\mathrm{R}_{u,j} \to \mathrm{R}_{u,j+1}$ and $\mathrm{R}_{u,j} \to \mathrm{E}_k$ can be expressed, respectively, as

$$\begin{aligned} y_{\mathrm{R}_{u,j}\mathrm{R}_{u,\mathrm{j}+1}} &= \sqrt{P_{\mathrm{R}_{u,j}}} h_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}} \left(s + \eta_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}}\right) \\ &\quad + \mu_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}} + \nu_{\mathrm{R}_{u,j}\mathrm{R}_{u,\mathrm{j}+1}}, \\ y_{\mathrm{R}_{u,j}\mathrm{E}_k} &= \sqrt{P_{\mathrm{R}_{u,j}}} h_{\mathrm{R}_{u,j}\mathrm{E}_k} \left(s + \eta_{\mathrm{R}_{u,j}\mathrm{E}_k}\right) + \mu_{\mathrm{R}_{u,j}\mathrm{E}_k} \\ &\quad + \nu_{\mathrm{R}_{u,j}\mathrm{E}_k}, \end{aligned} \tag{1}$$

where $P_{\mathrm{R}_{u,j}}$ denotes the transmit power of the transmitter $\mathrm{R}_{u,j}$, $h_{\mathrm{XY}}$ is the channel coefficient of the $\mathrm{X} \to \mathrm{Y}$ link, where $\mathrm{X}, \mathrm{Y} \in \{\mathrm{R}_{u,j}, \mathrm{R}_{u,j+1}, \mathrm{E}_k\}$, $\eta_{\mathrm{XY}}$ and $\mu_{\mathrm{XY}}$ denote noises caused by the hardware impairments at the transmitter X and the receiver Y, respectively, and $\nu_{\mathrm{XY}}$ are additive white Gaussian noises (AWGNs) modeled as Gaussian random variables (RVs) with zero mean and variance $N_0$.

Let us denote $\gamma_{\mathrm{XY}} = |h_{\mathrm{XY}}|^2$ as the channel gain. Assume that the channels are Rayleigh fading; the channel gain $\gamma_{\mathrm{XY}}$ is an exponential RV, whose cumulative distribution function (CDF) and probability density function (PDF) are given, respectively as

$$\begin{aligned} F_{\gamma_{\mathrm{XY}}}(x) &= 1 - \exp\left(-\lambda_{\mathrm{XY}} x\right), \\ f_{\gamma_{\mathrm{XY}}}(x) &= \lambda_{\mathrm{XY}} \exp\left(-\lambda_{\mathrm{XY}} x\right), \end{aligned} \tag{2}$$

where $\lambda_{\mathrm{XY}}$ is the parameter of $\gamma_{\mathrm{XY}}$ and defined as $\lambda_{\mathrm{XY}} = 1/\mathcal{E}\left\{\gamma_{\mathrm{XY}}\right\}$ and $\mathcal{E}\left\{.\right\}$ is an expected operator. To take path-loss into account, $\lambda_{\mathrm{XY}}$ can be modeled as in [13]:

$$\lambda_{\mathrm{XY}} = d_{\mathrm{XY}}^{\beta}, \tag{3}$$

where $d_{\mathrm{XY}}$ is link distance between X and Y, and $\beta$ $(2 \leq \beta \leq 6)$ is path-loss exponent.

**Remark 1:** Similar to [45]–[47], we can model the distortion noises $\eta_{\mathrm{XY}}$ and $\mu_{\mathrm{XY}}$, as circularly-symmetric complex Gaussian distribution with zero-mean and variance $\left(\sigma_{\mathrm{XY}}^{\mathrm{t}}\right)^2 P_{\mathrm{X}}$, and $\left(\sigma_{\mathrm{XY}}^{\mathrm{r}}\right)^2 P_{\mathrm{X}} \gamma_{\mathrm{XY}}$. In order to simplify the system model, it is also assumed that all of the nodes have the same structure so that the hardware impairment levels are the same, i.e., $\left(\sigma_{\mathrm{XY}}^{\mathrm{t}}\right)^2 = \sigma_a^2$, $\left(\sigma_{\mathrm{XY}}^{\mathrm{r}}\right)^2 = \sigma_b^2$. [1]

Therefore, the instantaneous signal-to-noise ratio (SNR) of the $\mathrm{R}_{u,j} \to \mathrm{R}_{u,j+1}$ and $\mathrm{R}_{u,j} \to \mathrm{E}_k$ links can be written as

$$\begin{aligned} \psi_{\mathrm{R}_{u,j}\mathrm{R}_{u,\mathrm{j}+1}} &= \frac{P_{\mathrm{R}_{u,j}} \gamma_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}}}{\kappa P_{\mathrm{R}_{u,j}} \gamma_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}} + N_0}, \\ \psi_{\mathrm{R}_{u,j}\mathrm{E}_k} &= \frac{P_{\mathrm{R}_{u,j}} \gamma_{\mathrm{R}_{u,j}\mathrm{E}_k}}{\kappa P_{\mathrm{R}_{u,j}} \gamma_{\mathrm{R}_{u,j}\mathrm{E}_k} + N_0}, \end{aligned} \tag{4}$$

where $\kappa = \sigma_a^2 + \sigma_b^2$.

Let T denote the total block duration (or the end-to-end delay constraint). Again, we consider the data transmission at the $(j+1)$th time slot on the $u$th path with duration of $\tau_u$ $(\tau_u = \mathrm{T}/\left(L_u + 1\right))$. In this time slot, the time switching-based

[1] In practice, with knowledge of impairment transceiver levels, we should select the transceivers with similar impairment levels, to optimize the system performance (see, Corollary 3 [45]).

technique is used, i.e., the node $\mathrm{R}_{u,j}$ harvests the energy from the beacon B during the time of $\alpha\tau_u$, where $\alpha$ $(0 < \alpha < 1)$ is a designed parameter. Similar to [21], the energy harvested by $\mathrm{R}_{u,j}$ can be given as

$$\mathrm{EH}_{\mathrm{R}_{u,j}} = \eta\alpha\tau_u P\gamma_{\mathrm{BR}_{u,j}}. \tag{5}$$

where $0 < \eta < 1$ is the energy conversion efficiency, $P$ is the transmit power of the power beacon B, and $\gamma_{\mathrm{BR}_{u,j}}$ is channel gain of the B → $\mathrm{R}_{u,j}$ link. Also, we assume that the channel between B and $\gamma_{\mathrm{BR}_{u,j}}$ is Rayleigh fading, and the CDF and PDF of $\gamma_{\mathrm{BR}_{u,j}}$ can be obtained as in (2).

The remaining time $(1-\alpha)\tau_u$ is used for transmitting the data. As a result, the transmit power of $\mathrm{R}_{u,j}$ obtained from the energy harvesting is calculated by

$$P^{\max}_{\mathrm{R}_{u,j}} \le \frac{\mathrm{EH}_{\mathrm{R}_{u,j}}}{(1-\alpha)\tau_u} \triangleq Z_{\mathrm{BR}_{u,j}}, \tag{6}$$

where $Z_{\mathrm{BR}_{u,j}} = \chi P\gamma_{\mathrm{BR}_{u,j}}$ with $\chi = \eta\alpha/(1-\alpha)$.

**Remark 2:** The frequency bands used for the data transmission and the energy harvesting are different, in order to avoid the interference. Moreover, at each time slot, all the nodes (i.e., $\mathrm{R}_{u,j}$) spend the same time $(\alpha\tau_u)$ to harvest energy, and then use it to transmit the data.

Since the eavesdroppers are active, it is assumed that the transmitter $\mathrm{R}_{u,j}$ can obtain the channel state information (CSI) of the eavesdropping links (i.e., $\mathrm{R}_{u,j} \to \mathrm{E}_k$), and hence it can adjust the transmit power to reduce the quality of these links. Let us denote $P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}$ as the transmit power of $\mathrm{R}_{u,j}$, which is adjusted in accordance with the eavesdropping CSIs, the channel capacity between $\mathrm{R}_{u,j}$ and $\mathrm{E}_k$ is calculated by

$$C_{\mathrm{R}_{u,j}\mathrm{E}_k} = (1-\alpha)\tau_u\log_2\left(1 + \frac{P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\gamma_{\mathrm{R}_{u,j}\mathrm{E}_k}}{\kappa P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\gamma_{\mathrm{R}_{u,j}\mathrm{E}_k} + N_0}\right). \tag{7}$$

If the eavesdroppers do not collude, the wiretap data rate at the $u$th time slot is calculated by the channel capacity of the best eavesdropper among all the existing ones (see [52]):

$$\begin{aligned} C^{\mathrm{tot}}_{\mathrm{R}_{u,j}\mathrm{E}_k} &= \max_{k=1,2,\ldots,K}\left(C_{\mathrm{R}_{u,j}\mathrm{E}_k}\right) \\ &= (1-\alpha)\tau_u\log_2\left(1 + \frac{P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\varphi_{\mathrm{R}_{u,j}\max}}{\kappa P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\varphi_{\mathrm{R}_{u,j}\max} + N_0}\right), \end{aligned} \tag{8}$$

where

$$\varphi_{\mathrm{R}_{u,j}\max} = \max_{k=1,2,\ldots,K}\left(\gamma_{\mathrm{R}_{u,j}\mathrm{E}_k}\right). \tag{9}$$

Next, we define the outage probability (OP) which is the probability that the data rate obtained at the intended receiver is below a target rate (denoted by $C_{\mathrm{th}}$).

To avoid eavesdroppers from the successful decoding, we have the following condition: $C^{\mathrm{tot}}_{\mathrm{R}_{u,j}\mathrm{E}_k} \le C_{th}$ or

$$P^{\mathrm{EV}}_{\mathrm{R}_{u,j}} \le \frac{\rho_u N_0}{\varphi_{\mathrm{R}_{u,j}\max}(1-\kappa\rho_u)},\ (\kappa < 1/\rho_u) \tag{10}$$

where

$$\rho_u = 2^{C_{\mathrm{th}}/(1-\alpha)\tau_u} - 1. \tag{11}$$

From (6) and (10), the maximum transmit power of the transmitter $\mathrm{R}_{u,j}$ is written as

$$P^{\max}_{\mathrm{R}_{u,j}} = \begin{cases} Z_{\mathrm{BR}_{u,j}}; & \text{if}\kappa \ge 1/\rho_u \\ \min\left(Z_{\mathrm{BR}_{u,j}}, \frac{\rho_u N_0}{\varphi_{\mathrm{R}_{u,j}\max}(1-\kappa\rho_u)}\right); & \text{if}\kappa < 1/\rho_u \end{cases} \tag{12}$$

Therefore, the channel capacity of the $\mathrm{R}_{u,j} \to \mathrm{R}_{u,j+1}$ link can be expressed by

$$C_{\mathrm{R}_{u,j},\mathrm{R}_{u,j+1}} = \begin{cases} (1-\alpha)\tau_u\log_2\left(1 + \frac{\Delta_{1,u,j}}{\kappa\Delta_{1,u,j}+N_0}\right); & \text{if}\kappa > 1/\rho_u \\ (1-\alpha)\tau_u\log_2\left(1 + \frac{\Delta_{2,u,j}}{\kappa\Delta_{2,u,j}+N_0}\right); & \text{if}\kappa \le 1/\rho_u \end{cases} \tag{13}$$

where

$$\begin{aligned} \Delta_{1,u,j} &= Z_{\mathrm{BR}_{u,j}}\gamma_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}}, \\ \Delta_{2,u,j} &= \min\left(Z_{\mathrm{BR}_{u,j}}, \frac{\rho_u N_0}{\varphi_{\mathrm{R}_{u,j}\max}(1-\kappa\rho_u)}\right)\gamma_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}}. \end{aligned} \tag{14}$$

Then, the end-to-end channel capacity of the $u$th path is computed by

$$\begin{aligned} C^{\mathrm{e2e}}_u &= \min_{j=1,2,\ldots,L_u+1}\left(C_{\mathrm{R}_{u,j},\mathrm{R}_{u,j+1}}\right) = \\ &\begin{cases} (1-\alpha)\tau_u\log_2\left(1 + \min\limits_{j=1,2,\ldots,L_u+1}\left(\frac{\Delta_{1,u,j}}{\kappa\Delta_{1,u,j}+N_0}\right)\right); \\ \qquad \text{if}\kappa > 1/\rho_u \\ (1-\alpha)\tau_u\log_2\left(1 + \min\limits_{j=1,2,\ldots,L_u+1}\left(\frac{\Delta_{2,u,j}}{\kappa\Delta_{2,u,j}+N_0}\right)\right); \\ \qquad \text{if}\kappa \le 1/\rho_u \end{cases} \end{aligned} \tag{15}$$

Now, we consider the case where the eavesdroppers collaborate to decode the data received at the $u$th time slot. Similar to [28], [29], the total channel capacity obtained on the eavesdropping links is formulated as

$$\begin{aligned} C^{\mathrm{tot}}_{\mathrm{R}_{u,j}\mathrm{E}_k} &= (1-\alpha)\tau_u\log_2\left(1 + \frac{\sum\limits_{k=1}^{K} P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\gamma_{\mathrm{R}_{u,j}\mathrm{E}_k}}{\kappa\sum\limits_{k=1}^{K} P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\gamma_{\mathrm{R}_{u,j}\mathrm{E}_k} + N_0}\right) \\ &= (1-\alpha)\tau_u\log_2\left(1 + \frac{P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\varphi_{\mathrm{R}_{u,j}\mathrm{sum}}}{\kappa P^{\mathrm{EV}}_{\mathrm{R}_{u,j}}\varphi_{\mathrm{R}_{u,j}\mathrm{sum}} + N_0}\right), \end{aligned} \tag{16}$$

where

$$\varphi_{\mathrm{R}_{u,j}\mathrm{sum}} = \sum_{k=1}^{K}\gamma_{\mathrm{R}_{u,j},\mathrm{E}_k}. \tag{17}$$

Similar to (12), the transmit power of $\mathrm{R}_{u,j}$ in this case can be obtained by

$$P^{\max}_{\mathrm{R}_{u,j}} = \begin{cases} Z_{\mathrm{BR}_{u,j}}; & \text{if}\kappa \ge 1/\rho_u \\ \min\left(Z_{\mathrm{BR}_{u,j}}, \frac{\rho_u N_0}{\varphi_{\mathrm{R}_{u,j}\mathrm{sum}}(1-\kappa\rho_u)}\right); & \text{if}\kappa < 1/\rho_u \end{cases} \tag{18}$$

From (18), we write the channel capacity of the $w$th hop as

$$C_{\mathrm{R}_{u,j},\mathrm{R}_{u,j+1}} = \begin{cases} (1-\alpha)\tau_u\log_2\left(1 + \frac{\Delta_{1,u,j}}{\kappa\Delta_{1,u,j}+N_0}\right); & \text{if}\kappa > 1/\rho_u \\ (1-\alpha)\tau_u\log_2\left(1 + \frac{\Delta_{3,u,j}}{\kappa\Delta_{3,u,j}+N_0}\right); & \text{if}\kappa \le 1/\rho_u \end{cases} \tag{19}$$

where

$$\Delta_{3,u,j} = \min\left( Z_{\mathrm{BR}_{u,j}}, \frac{\rho_u N_0}{\varphi_{\mathrm{R}_{u,j}} sum \left(1 - \kappa \rho_u\right)} \right) \gamma_{\mathrm{R}_{u,j}\mathrm{R}_{u,j+1}}. \quad (20)$$

Then, the end-to-end channel capacity of the $u$th path is computed as follows

$$C_u^{\mathrm{e2e}} = \min_{j=1,2,\ldots,L_u+1} \left( C_{\mathrm{R}_{u,j},\mathrm{R}_{u,j+1}} \right) = \\ \begin{cases} \left(1-\alpha\right)\tau_u \log_2\left(1 + \min\limits_{j=1,2,\ldots,L_u+1}\left(\frac{\Delta_{1,u,j}}{\kappa\Delta_{1,u,j}+N_0}\right)\right); \\ \hfill \mathrm{if} \kappa \geq \rho_u \\ \left(1-\alpha\right)\tau_u \log_2\left(1 + \min\limits_{j=1,2,\ldots,L_u+1}\left(\frac{\Delta_{3,u,j}}{\kappa\Delta_{3,u,j}+N_0}\right)\right); \\ \hfill \mathrm{if} \kappa < \rho_u \end{cases} \quad (21)$$

In the following, we introduce proposed path selection methods:

In the first proposed protocol, namely, random path selection (RPS), the source randomly selects one of the available paths to transmit its data to the destination. In this protocol, the end-to-end outage probability (OP) can be formulated as

$$\mathrm{OP}_{\mathrm{RPS}} = \frac{1}{M} \sum_{u=1}^{M} \Pr\left( C_u^{\mathrm{e2e}} < C_{\mathrm{th}} \right). \quad (22)$$

where the factor $1/M$ indicates probability that the $u$th path ($u = 1, 2, ..., M$) is chosen for the communication.

Although the implementation of the RPS protocol is simple, it may not provide high outage performance due to the random selection. Because of the delay constraint, it is obvious that reducing the number of hops on the selected path increases the end-to-end data rate. Motivated by this, we propose the second protocol named shortest path selection (SPS). In the SPS method, the path having the lowest number of hops is selected. Hence, the end-to-end OP of this protocol is expressed as

$$\mathrm{OP}_{\mathrm{SPS}} = \Pr\left( C_a^{\mathrm{e2e}} < C_{\mathrm{th}} \right), \quad (23)$$

where the $a$th path is the shortest one, i.e., $a \in \{1, 2, ..., M\}$ and $L_a = \min\limits_{u=1,2,\ldots,M} \left(L_u\right)$.

**Remark 3:** If more than one path has the same shortest number of hops, the source randomly selects one of them for forwarding the data. Therefore, the outage performance of the RPS and SPS protocols are identical when all of the paths have the same number of hops.

Finally, to optimize the system performance, we propose the best path selection protocol (BPS) in which the chosen path is the one providing the highest end-to-end channel capacity. Mathematically speaking, we write

$$C_b^{\mathrm{e2e}} = \max_{n=1,2,\ldots,M} \left( C_u^{\mathrm{e2e}} \right), \quad (24)$$

where $b \in \{1, 2, ..., M\}$.

Similar to (23), OP of the BPS scheme is given as

$$\mathrm{OP}_{\mathrm{BPS}} = \Pr\left( C_b^{\mathrm{e2e}} < C_{\mathrm{th}} \right). \quad (25)$$

## III. Performance Evaluation

To provide further insight into the end-to-end transmission for multi-hop multi-path relay networks formed by energy-harvesting devices, we analyze specifically the OP performance of the SPS, RPS, and BPS in the multi-hop RF cooperative system with $M$ parallel cooperative paths between the source and destination. From (23), (24), (25) we can see that the OP of the RPS and BPS can be easily obtained from the OP of the SPS. Therefore, we will analyze the OP of the SPS first.

### A. The eavesdroppers do not cooperate

*1) The SPS Protocol:* The outage probability of the SPS protocol is given as

$$\begin{aligned} \mathrm{OP}_{\mathrm{SPS}} &= \Pr\left( C_a^{\mathrm{e2e}} < C_{\mathrm{th}} \right) \\ &= \begin{cases} \Pr\left( \min\limits_{j=1,2,\ldots,L_a+1} \left( \frac{\Delta_{1,a,j}}{\kappa\Delta_{1,a,j}+N_0} \right) < \rho_a \right); \mathrm{if} \kappa \geq 1/\rho_a \\ \Pr\left( \min\limits_{j=1,2,\ldots,L_a+1} \left( \frac{\Delta_{2,a,j}}{\kappa\Delta_{2,a,j}+N_0} \right) < \rho_a \right); \mathrm{if} \kappa < 1/\rho_a \end{cases} \\ &= 1 - \prod_{j=1}^{L_a+1} \left(1 - \mathrm{OP}_{j,a}\right), \end{aligned} \quad (26)$$

where $\mathrm{OP}_{j,a}$ is the outage probability at the $j$th hop on the shortest path, expressed by

$$\mathrm{OP}_{j,a} = \begin{cases} \Pr\left( \frac{\Delta_{1,a,j}}{\kappa\Delta_{1,a,j}+N_0} < \rho_a \right); \mathrm{if} \kappa \geq 1/\rho_a \\ \Pr\left( \frac{\Delta_{2,a,j}}{\kappa\Delta_{2,a,j}+N_0} < \rho_a \right); \mathrm{if} \kappa < 1/\rho_a \end{cases} \quad (27)$$

*Lemma 1:* Exact closed-form expression of $\mathrm{OP}_{j,a}$ can be given as in (28), where $K_1(.)$ is modified Bessel function of the second kind [53, eq. (8.432.6)]:

$$\mathrm{OP}_{j,a} = \\ \begin{cases} 1; & \mathrm{if} \kappa \geq 1/\rho_a \\ 1 - \left[ \begin{array}{l} 2\Phi_{1,a,j}\Theta_{1,a,j} + \\ 2\sum\limits_{k=1}^{K} \left(-1\right)^k C_K^k \Phi_{2,a,j}\Theta_{2,a,j} \end{array} \right]; & \mathrm{if} \kappa < 1/\rho_a \end{cases} \quad (28)$$

where

$$\begin{aligned} \Phi_{1,a,j} &= \sqrt{\frac{\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \Omega_{\mathrm{BR}_{a,j}} \rho_a N_0}{\left(1 - \kappa\rho_a\right)}}, \\ \Phi_{2,a,j} &= \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} N_0 \\ &\times \sqrt{\frac{\Omega_{\mathrm{BR}_{a,j}}}{k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}\left(1 - \kappa\rho_a\right)^2 + \rho_a N_0 \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \left(1 - \kappa\rho_a\right)}}, \\ \Theta_{1,a,j} &= K_1\left( 2\sqrt{\frac{\Omega_{\mathrm{BR}_{a,j}} \rho_a N_0 \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}{1 - \kappa\rho_a}} \right), \\ \Theta_{2,a,j} &= K_1\left( 2\sqrt{\frac{\Omega_{\mathrm{BR}_{a,j}}}{1 - \kappa\rho_a} \left( \begin{array}{c} k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}\left(1 - \kappa\rho_a\right) \\ +\rho_a N_0 \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \end{array} \right)} \right). \end{aligned} \quad (29)$$

*Proof 1:* See Appendix A.

Substituting (28) into (26), we can obtain $\mathrm{OP_{SPS}}$ as follows:

$$\mathrm{OP_{SPS}}=\begin{cases}1;\ \mathrm{if}\kappa\geq 1/\rho_a\\ 1-\prod\limits_{j=1}^{L_a+1}\left[\begin{array}{l}2\Phi_{1,a,j}\Theta_{1,a,j}+\\ 2\sum\limits_{k=1}^{K}(-1)^k C_K^k\Phi_{2,a,j}\Theta_{2,a,j}\end{array}\right];\\ \quad \mathrm{if}\kappa<1/\rho_a\end{cases} \tag{30}$$

Due to the significant influence of transmit power of the beacon to the harvested energy at source and relay nodes, we give out the following corollary to definitely show the impact of $P$ on the outage performance.

*Corollary 1:* At high transmit power of the beacon, i.e., $P\to+\infty$, the asymptotic OP of the SPS protocol can be obtained as

$$\mathrm{OP_{SPS}}\overset{P\to+\infty}{\approx}\\ \begin{cases}1; & \mathrm{if}\kappa\geq 1/\rho_a\\ 1-\prod\limits_{j=1}^{L_a+1}\left(1-\sum\limits_{k=1}^{K}C_K^k(-1)^{k+1}\frac{\Phi_{3,a,j}}{\Phi_{3,a,j}+k\Theta_{3,a,j}}\right); & \\ & \mathrm{if}\kappa<1/\rho_a\end{cases} \tag{31}$$

where

$$\begin{aligned}\Phi_{3,a,j}&=\lambda_{\mathrm{R}_{a,j}R_{a,j+1}}\rho_a N_0,\\ \Theta_{3,a,j}&=\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a).\end{aligned} \tag{32}$$

*Proof 2:* See Appendix B.

*2) The RPS Protocol:* Using the result obtained from (30), we can calculate the outage probability $\Pr\left(C_u^{\mathrm{e2e}}<C_{th}\right)$ by

$$\Pr\left(C_u^{\mathrm{e2e}}<C_{\mathrm{th}}\right)=\\ \begin{cases}1; & \mathrm{if}\kappa\geq 1/\rho_u\\ 1-\prod\limits_{j=1}^{L_u+1}\left[\begin{array}{l}2\Phi_{1,u,j}\Theta_{1,u,j}+\\ 2\sum\limits_{k=1}^{K}(-1)^k C_K^k\Phi_{2,u,j}\Theta_{2,u,j}\end{array}\right]; & \\ & \mathrm{if}\kappa<1/\rho_u\end{cases} \tag{33}$$

Substituting (33) into in (22), we obtain an closed-form expression of outage probability for the RPS protocol.

Moreover, similar to (31), we have

$$\Pr\left(C_u^{\mathrm{e2e}}<C_{\mathrm{th}}\right)\overset{P\to+\infty}{\approx}\\ \begin{cases}1; & \mathrm{if}\kappa\geq 1/\rho_u\\ 1-\prod\limits_{j=1}^{L_u+1}\left(1-\sum\limits_{k=1}^{K}C_K^k(-1)^{k+1}\frac{\Phi_{3,u,j}}{\Phi_{3,u,j}+k\Theta_{3,u,j}}\right); & \\ & \mathrm{if}\kappa<1/\rho_u\end{cases} \tag{34}$$

Combining (22) and (34), we obtain an asymptotic OP of the RPS protocol at high $P$ region.

*3) The BPS Protocol:* The end-to-end outage probability of the BPS protocol can be computed exactly as

$$\begin{aligned}\mathrm{OP_{BPS}}&=\Pr\left(\max_{u=1,2,\ldots,M}\left(C_u^{\mathrm{e2e}}\right)<C_{\mathrm{th}}\right)\\ &=\prod_{u=1}^{M}\Pr\left(C_u^{\mathrm{e2e}}<C_{\mathrm{th}}\right).\end{aligned} \tag{35}$$

Therefore, substituting (33) and (34) into (35), we can obtain exact and asymptotic closed-form expressions of $\mathrm{OP_{BPS}}$.

### *B. The eavesdroppers cooperate to decode the data overhead*

*1) The SPS Protocol:* Similar to (26), the outage probability of the SPS protocol on the selected path $a$ is given as

$$\mathrm{OP_{SPS}}=1-\prod_{j=1}^{L_a+1}\left(1-\mathrm{OP}_{j,a}\right), \tag{36}$$

where $\mathrm{OP}_{j,a}$ can be written by

$$\mathrm{OP}_{j,a}=\begin{cases}\Pr\left(\frac{\Delta_{1,a,j}}{\kappa\Delta_{1,a,j}+N_0}<\rho_a\right);\mathrm{if}\kappa\geq 1/\rho_a\\ \Pr\left(\frac{\Delta_{3,a,j}}{\kappa\Delta_{3,a,j}+N_0}<\rho_a\right);\mathrm{if}\kappa<1/\rho_a\end{cases} \tag{37}$$

*Lemma 2:* Exact closed-form expression of $\mathrm{OP}_{j,a}$ can be formulated as

$$\mathrm{OP}_{j,a}=\\ \begin{cases}1; & \mathrm{if}\kappa\geq 1/\rho_a\\ 1-\left[2\Phi_{1,a,j}\Theta_{1,a,j}-2\sum\limits_{k=0}^{K-1}\Phi_{4,a,j}\Theta_{4,a,j}\right]; & \mathrm{if}\kappa<1/\rho_a\end{cases} \tag{38}$$

where

$$\begin{aligned}\Phi_{4,a,j}&=\frac{\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\rho_a N_0}{k!}\left[\Omega_{\mathrm{R}_{u,j}\mathrm{E}_k}(1-\kappa\rho_a)\right]^k\\ &\times\left[\frac{\Omega_{\mathrm{BR}_{u,j}}}{\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)^2+\rho_a N_0\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}(1-\kappa\rho_a)}\right]^{\frac{k+1}{2}},\\ \Theta_{4,a,j}&=\\ K_{-k-1}&\left(2\sqrt{\Omega_{\mathrm{BR}_{a,j}}\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}+\frac{\Omega_{\mathrm{BR}_{a,j}}\rho_a N_0\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}{1-\kappa\rho_a}}\right).\end{aligned} \tag{39}$$

*Proof 3:* See Appendix C.

Substituting (38) into (36), we can obtain $\mathrm{OP_{SPS}}$ as follows:

$$\mathrm{OP_{SPS}}=\begin{cases}1; & \mathrm{if}\kappa\geq 1/\rho_a\\ 1-\prod\limits_{j=1}^{L_a+1}\left[2\Phi_{1,a,j}\Theta_{1,a,j}-2\sum\limits_{k=0}^{K-1}\Phi_{4,a,j}\Theta_{4,a,j}\right]; & \\ & \mathrm{if}\kappa<1/\rho_a\end{cases} \tag{40}$$

*Corollary 2:* At high transmit $P$ values, the asymptotic OP of the SPS protocol can be obtained as

$$\mathrm{OP_{SPS}}\overset{P\to+\infty}{\approx}\\ \begin{cases}1; & \mathrm{if}\kappa\geq 1/\rho_a\\ 1-\prod\limits_{j=1}^{L_a+1}\left(1-\sum\limits_{k=0}^{K-1}\Phi_{5,a,j}\Theta_{5,a,j}\right); & \mathrm{if}\,\kappa<1/\rho_a\end{cases} \tag{41}$$

where

$$\begin{aligned}\Phi_{5,a,j}&=\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\rho_a N_0\left[\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)\right]^k,\\ \Theta_{5,a,j}&=\left(\frac{1}{\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)+\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\rho_a N_0}\right)^{k+1}.\end{aligned} \tag{42}$$

*Proof 4:* See Appendix D.

*2) The RPS Protocol:* From (40) and (41), the exact and asymptotic closed-form expressions of $\Pr\left(C_u^{\mathrm{e2e}} < C_{th}\right)$ can be given, respectively by

$$\Pr\left(C_u^{\mathrm{e2e}} < C_{\mathrm{th}}\right) = \left\{ \begin{array}{ll} 1; & \mathrm{if} \kappa \geq 1/\rho_u \\ 1 - \prod\limits_{j=1}^{L_u+1} \left[ 2\Phi_{1,u,j}\Theta_{1,u,j} - 2\sum\limits_{k=0}^{K-1} \Phi_{4,u,j}\Theta_{4,u,j} \right]; & \\ & \mathrm{if} \kappa < 1/\rho_u \end{array} \right. \tag{43}$$

$$\Pr\left(C_u^{\mathrm{e2e}} < C_{\mathrm{th}}\right) \overset{P \rightarrow +\infty}{\approx} \left\{ \begin{array}{ll} 1; & \mathrm{if} \kappa \geq 1/\rho_u \\ 1 - \prod\limits_{j=1}^{L_u+1} \left( 1 - \sum\limits_{k=0}^{K-1} \Phi_{5,a,j}\Theta_{5,a,j} \right); & \mathrm{if}\ \kappa < 1/\rho_u \end{array} \right. \tag{44}$$

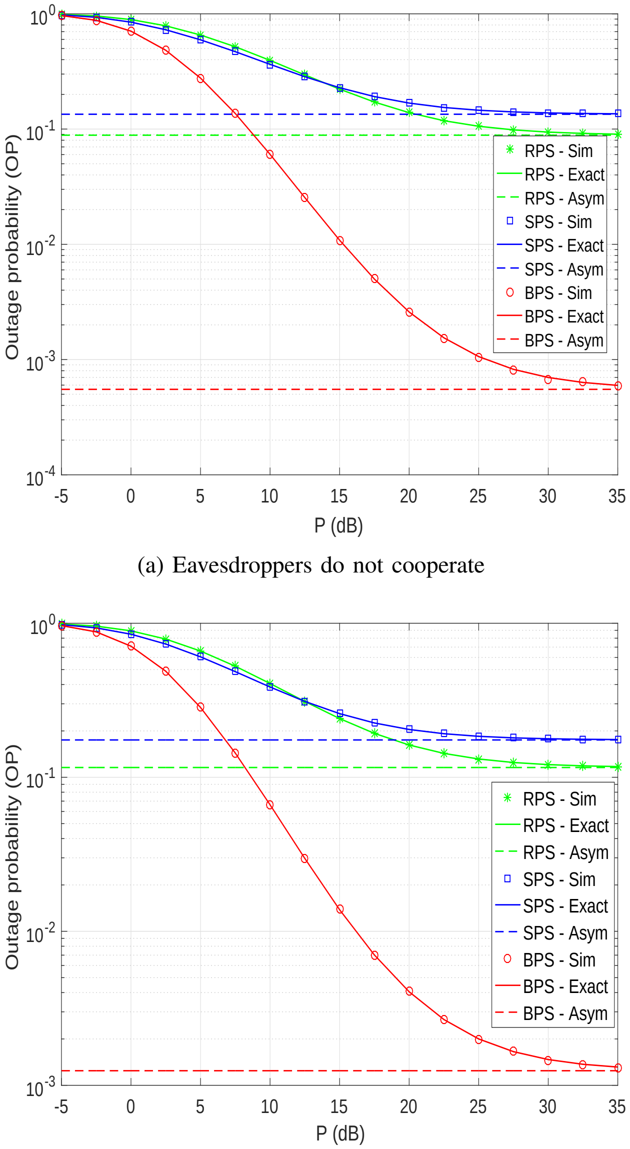
Combining (22), (43) and (44), we obtain the exact and asymptotic closed-form expressions of outage probability for the RPS protocol.

*3) The BPS Protocol:* In this protocol, by substituting (43) and (44) into (35), the exact and asymptotic closed-form expressions of $\mathrm{OP}_{\mathrm{BPS}}$ can be obtained.

## IV. Simulation results

In this section, we provide Monte-Carlo simulations to verify the theoretical derivations. The simulation results are obtained by using MATrix LABoratory (MATLAB R2016a). To obtain the end-to-end outage probability for the proposed protocols, we perform $10^6$ independent trials and in each trial, we create Rayleigh channel coefficients for all of the links. In the simulation environment, we consider a two-dimensional plane in which the coordinates of the source, the relays, the destination, the beacon and the eavesdroppers are (0,0), $\left(\frac{j}{L_k+1}, 0\right)$, (1,0), ($x_{\mathrm{B}}$, $y_{\mathrm{B}}$), and ($x_{\mathrm{E}}$, $y_{\mathrm{E}}$), respectively. The path-loss exponent $\beta$ and the variance of noise equal to 3 and 1, respectively. In all simulations, we present the simulation results, the exactly theoretical results, and the asymptotically theoretical results by markers, solid lines, and dash lines, respectively.

In Fig. 2, we investigate the impact of the transmit power of beacon $P$ (dB) on the value of OP in the case that the eavesdroppers do not cooperate and cooperate together by setting $L = [2, 3, 4]$, $R = 0.5$, $\kappa = 0.1$, $K = 2$, $(x_{\mathrm{B}}, y_{\mathrm{B}}) = (0.5, 0.1)$, $(x_{\mathrm{E}}, y_{\mathrm{E}}) = (0.5, 1)$, $\eta = 0.1$, $\alpha = 0.1$. As shown, there is a good agreement between the theoritical and the simulation results. It is observed that, when $P$ (dB) is small, i.e., $P$ (dB) equal -5dB, OP approaches 1 and when the value of $P$ (dB) increases, OP values decrease. This means that increasing the transmit $P$ can enhance the physical layer security against eavesdropping attacks. Furthermore, comparing the SPS, the RPS, and the BPS protocols, Fig. 2 illustrates that the outage probability value of the BPS protocol is always lower than that of the RPS protocol which further outperforms the SPS protocol. In other words, the BPS protocol achieves the best outage probability performance, further confirming the advantage of proposed best path selection over shortest path selection and random path selection. Moreover, the outage performance of three protocols converges to a positive constant at high transmit $P$. Therefore, we can conclude that the system obtains the zero-diversity order.

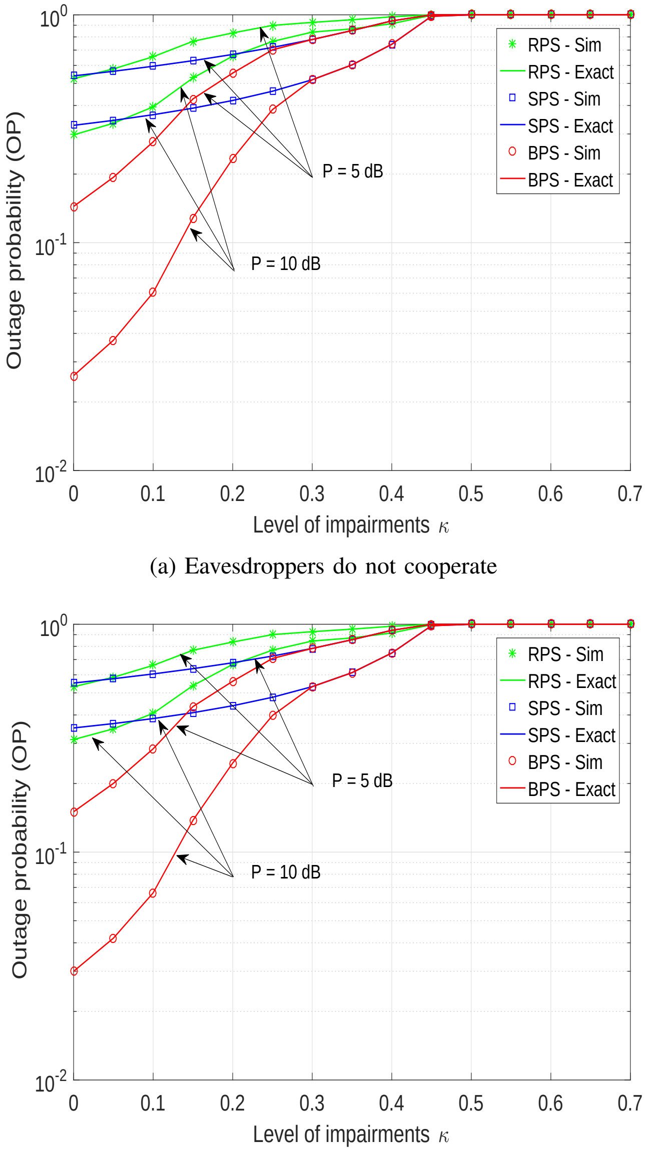


(a) Eavesdroppers do not cooperate

(b) Eavesdroppers cooperate

Fig. 2: Outage probability as a function of the transmit power $P$ in dB in the case (a) eavesdroppers do not cooperate and (b) eavesdroppers cooperate together when $L = [2, 3, 4]$, $R = 0.5$, $\kappa = 0.1$, $K = 2$, $(x_{\mathrm{B}}, y_{\mathrm{B}}) = (0.5, 0.1)$, $(x_{\mathrm{E}}, y_{\mathrm{E}}) = (0.5, 1)$, $\eta = 0.1$, $\alpha = 0.1$.

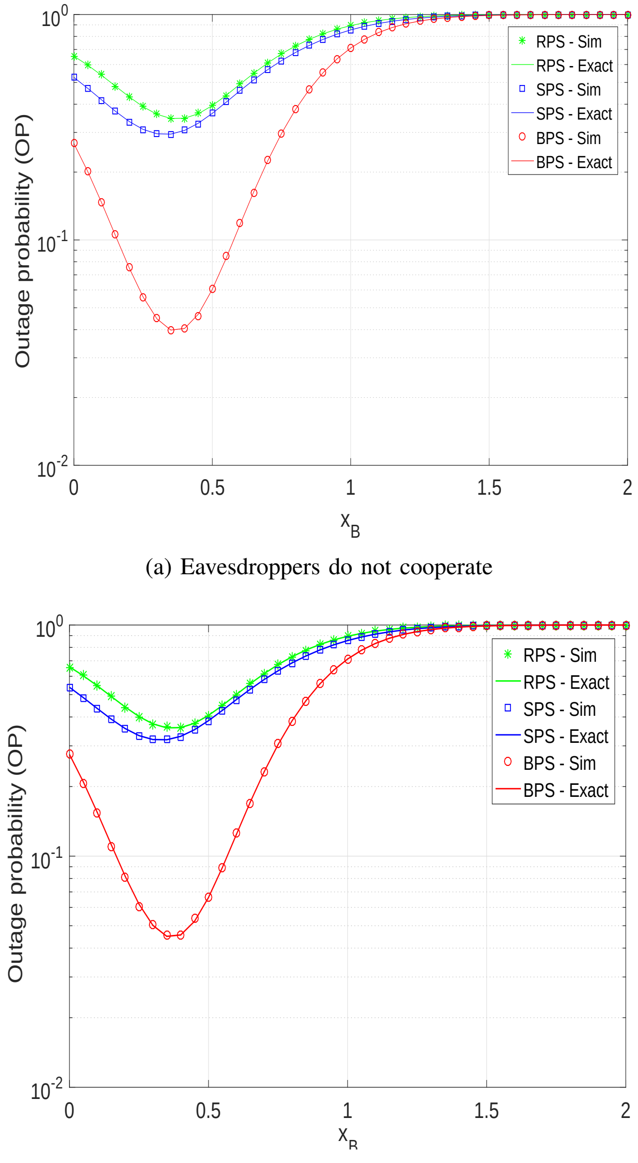
Fig. 3 presents OP as a function of the level of impairments $\kappa$ at two different transmit power of beacon $P$, i.e., $P$ = 5 dB and $P$ = 10 dB, in the case that the eavesdroppers do not cooperate, and eavesdroppers cooperate. The following parameters are employed: $L = [2, 3, 4]$, $R = 0.5$, $K = 2$, $(x_{\mathrm{B}}, y_{\mathrm{B}}) = (0.5, 0.1)$, $(x_{\mathrm{E}}, y_{\mathrm{E}}) = (0.5, 1)$, $\eta = 0.1$, $\alpha = 0.1$. It can be observed from this figure that the OP value of BPS, RPS, and SPS protocols increases with the increasing of $\kappa$. When the level of impairments less than 0.3, the BPS protocol still outperforms RPS and SPS. However, the OP



(a) Eavesdroppers do not cooperate

(b) Eavesdroppers cooperate

Fig. 3: Outage probability as a function of the level of impairments $\kappa$ in the case (a) eavesdroppers do not cooperate and (b) eavesdroppers cooperate together when $L = [2, 3, 4]$, $R = 0.5,\ K = 2,\ (x_{\rm B}, y_{\rm B}) = (0.5, 0.1)\,,\ (x_{\rm E}, y_{\rm E}) = (0.5, 1)\,,\ \eta = 0.1,\ \alpha = 0.1.$



(a) Eavesdroppers do not cooperate

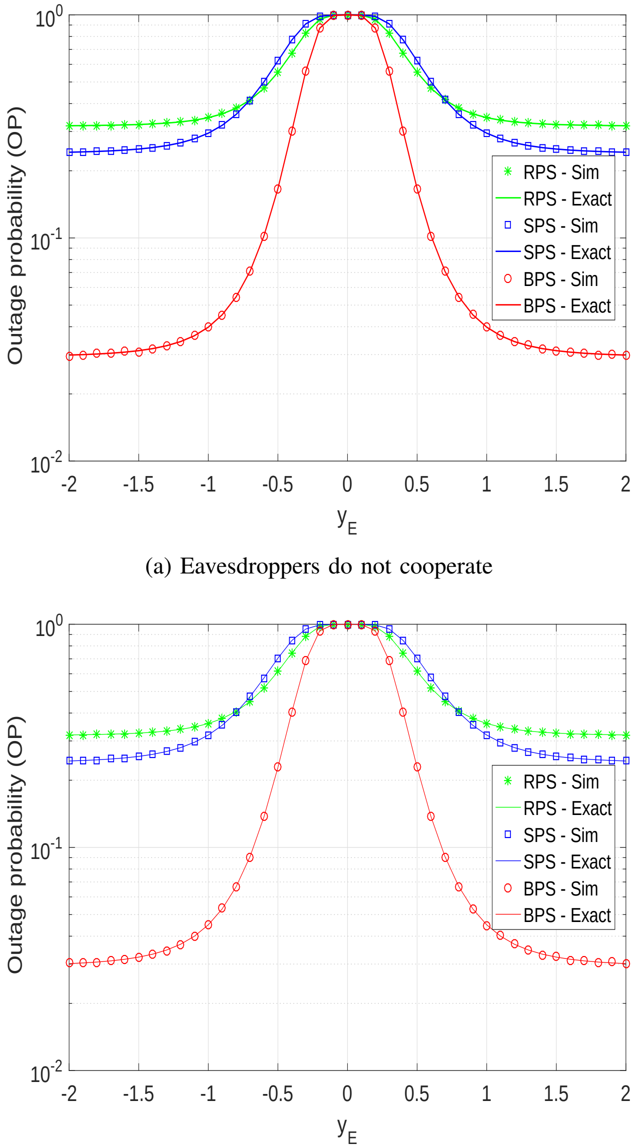
(b) Eavesdroppers cooperate

Fig. 4: Outage probability as a function of $x_B$ in the case (a) eavesdroppers do not cooperate and (b) eavesdroppers cooperate together when $L = [2, 3, 4]$, $R = 0.5,\ \kappa = 0.1,\ K = 2,\ (x_{\rm B}, y_{\rm B}) = (0.5, 0.1)\,,\ (x_{\rm E}, y_{\rm E}) = (0.5, 1)\,,\ \eta = 0.1,\ \alpha = 0.1.$

of BPS and SPS rises to the same value at high level of impairments, i.e., $\kappa \geq 0.3$. Moreover, the OP of all protocols converges toward 1 at high $\kappa$ regions, i.e., $\kappa \geq 0.45$, which agree with the results in the previous section. Figures also shows that the BPS protocol is more robust to hardware impairment compared with RPS and SPS, thus, it can operate better with device has poor hardware quality.

In Fig. 4, the outage probability is plotted as a function of $x_{\rm B}$ in the case that the eavesdroppers do not cooperate and cooperate together, when $L = [2, 3, 4]$, $R = 0.5$, $\kappa = 0.1,\ \ K = 2,\ (x_{\rm B}, y_{\rm B}) = (0.5, 0.1)\,,\ (x_{\rm E}, y_{\rm E}) = (0.5, 1)\,,$ $\eta = 0.1,\ \alpha = 0.1$. It is clearly observed that the outage performance of the propose protocols increases to optimal value with increasing $x_{\rm B}$ value is about 0.35 and after that, it decreases. From this figure, we can determine the position of beacon where the OP reach the optimal value. For example, the OP of BPS and SPS is minimized when $x_{\rm B}$ is about 0.35 or 0.4, the OP of RPS is minimized when is about 0.3 or 0.35.

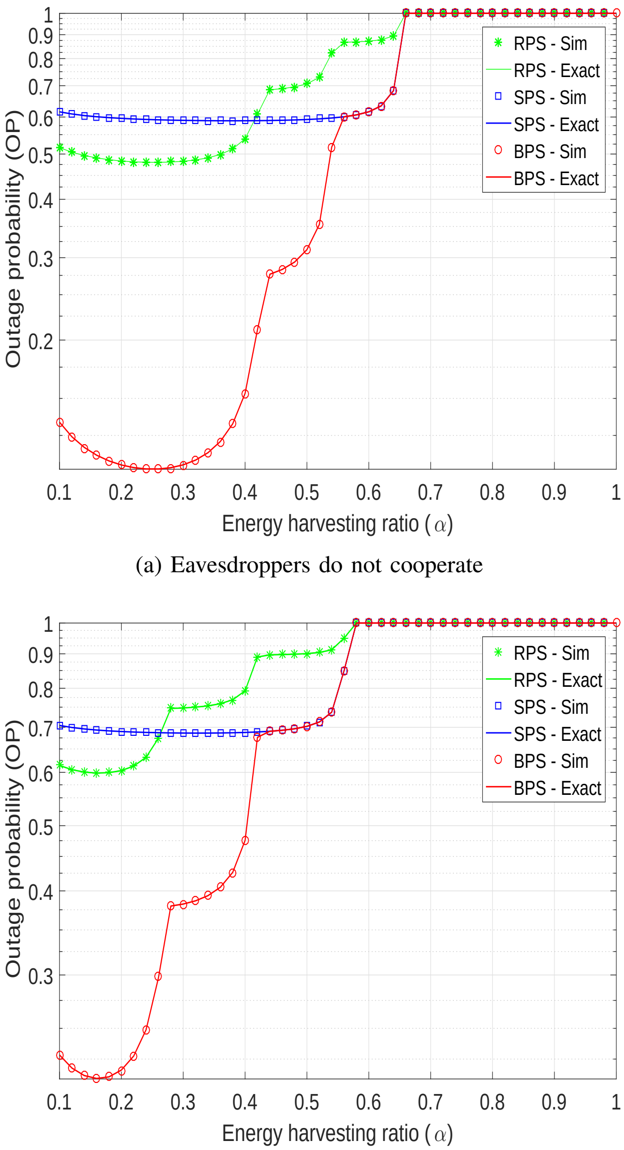
In Fig. 5, we investigate the impact of $y_{\rm E}$ on the OP in the case that the eavesdroppers do not cooperate and cooperate together, respectively, when $L = [2, 3, 4]$, $R = 0.5,\ \kappa = 0.1,$ $K = 2,\ (x_{\rm B}, y_{\rm B}) = (0.5, 0.1)\,,\ x_{\rm E} = 0.5,\ \eta = 0.1,\ \alpha = 0.1.$ and $x_B$ is set at optimal value 0.35. As shown in Fig. 5a and Fig. 5b, the outage performance increases when the eaves-



(a) Eavesdroppers do not cooperate

(b) Eavesdroppers cooperate

Fig. 5: Outage probability as a function of $y_E$ in the case (a) eavesdroppers do not cooperate and (b) eavesdroppers cooperate together when $L = [2, 3, 4]$, $R = 0.5$, $\kappa = 0.1$, $K = 2$, $(x_{\mathrm{B}}, y_{\mathrm{B}}) = (0.5, 0.1)$ , $x_{\mathrm{E}} = 0.5$, $\eta = 0.1$, $\alpha = 0.1$.



(a) Eavesdroppers do not cooperate

(b) Eavesdroppers cooperate

Fig. 6: Outage probability as a function of energy harvesting ratio $\alpha$ in the case (a) eavesdroppers do not cooperate and (b) eavesdroppers cooperate together when $L = [2, 3, 4]$, $R = 0.5$, $\kappa = 0.1$, $K = 2$, $(x_{\mathrm{B}}, y_{\mathrm{B}}) = (0.5, 0.1)$ , $(x_{\mathrm{E}}, y_{\mathrm{E}}) = (0.5, 1)$ , $\eta = 0.1$, $\alpha = 0.1$.

droppers move far away from the data route. Consequently, OP get the worst results at $y_{\mathrm{E}} = 0$ since distance between the eavesdroppers and the source S or the relays $\mathrm{R}_{u,j}$ is shortest.

In Fig. 6, the OP is depicted as a function of energy harvesting ratio $\alpha$ in the case that the eavesdroppers do not cooperate and cooperate together. Herein, the energy harvesting ratio $\alpha$ plays a key role in the energy harvesting process since it affects not only the received power at the best relay path but also the transmit power of the source and the relay nodes, which agree with the results in (6). It can be seen from these figures that there exists an optimal value of $\alpha$ at which the OP is minimized. It can be explained as follows, the higher value of $\alpha$ is, more energy can be harvested from beacon. Consequently, the higher energy that the relay nodes can be used for forwarding the information from the source to the destination. However, the higher value of $\alpha$ is, the less effective communication time, $(1 - \alpha)\,\tau_u$, between the source to the relay or the relay to the relay is. Therefore, when $\alpha$ reaches optimal value, we can obtain the best outage performance. For example, as observed from Fig. 6b, the optimal value of $\alpha$ of BPS equals to 0.16 in the case that the eavesdroppers cooperate to decode the signals.

## V. Conclusions

In this paper, we proposed three novel path selection methods, namely, SPS protocol, RPS protocol, and BPS protocol to investigate the impact of EH and hardware impairments on the outage performance of multi-hop multi-path cooperative WSNs. Moreover, we derive exactly and asymptotically the outage probabilities of three proposed protocols under the presence of one beacon, multiple eavesdropping attacks, and over i.i.d. Rayleigh block fading, where the source S and relaying nodes can harvest the RF signals from the beacon. The simulation results verified that the employment of BPS together with multi-hop multi-path schemes can enhance significantly the secure performance of the considered EH and hardware impairment system. In particular, BPS is more robust to hardware impairment than RPS and SPS; thus, it can operate better with device that have a poor hardware quality. Finally, the performance can be improved by placing the beacon at the appropriate position and choosing a suitable energy-harvesting ratio $\alpha$.

## Acknowledgments

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (no. 2018R1A2B6002399) and in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2015R1D1A1A01059186).

## Appendix A: Proof of Lemma 1

- $Case\ 1 : \kappa \geq 1/\rho_a$.

We can present $\mathrm{OP}_{j,a}$ by the following formula:

$$\begin{aligned}\mathrm{OP}_{j,a} &= \Pr\left(\frac{\Delta_{1,a,j}}{\kappa\Delta_{1,a,j} + N_0} < \rho_a\right)\\ &= \Pr\left(\Delta_{1,a,j}(1-\kappa\rho_a) < \rho_a N_0\right)\\ &= 1. \end{aligned} \tag{A.1}$$

- $Case\ 2 : \kappa < 1/\rho_a$.

Firstly, $\mathrm{OP}_{j,a}$ can be formulated as

$$\begin{aligned}\mathrm{OP}_{j,a} &= \Pr\left(\Delta_{2,a,j} < \frac{\rho_a N_0}{1-\kappa\rho_a}\right)\\ &= \Pr\left(X < \frac{\rho_a N_0}{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}(1-\kappa\rho_a)}\right)\\ &= \int_0^{+\infty} F_X\left(\frac{\rho_a N_0}{y(1-\kappa\rho_a)}\right) f_{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}(y)\,dy, \end{aligned} \tag{A.2}$$

where $X = \min\left(Z_{\mathrm{B}R_{a,j}}, \frac{\rho_a N_0}{\varphi_{\mathrm{R}_{a,j}\ \max}(1-\kappa\rho_a)}\right)$, $F_X(.)$ is the CDF of $X$, and $f_{\gamma_{\mathrm{R}_{a,j},\mathrm{R}_{a,j+1}}}(.)$ is the PDF of $\gamma_{\mathrm{R}_{a,j},\mathrm{R}_{a,j+1}}$.

To attain (A.2), the CDF $F_X(x)$ is required, we have

$$\begin{aligned}F_X(x) &= \Pr\left(\min\left(Z_{\mathrm{B}R_{a,j}}, \frac{\rho_a N_0}{\varphi_{\mathrm{R}_{a,j}\ \max}(1-\kappa\rho_a)}\right) < x\right)\\ &= 1 - \left(1 - F_{Z_{\mathrm{BR}_{a,j}}}(x)\right) F_{\frac{\varphi_{\mathrm{R}_{a,j}\ \max}(1-\kappa\rho_a)}{\rho_a N_0}}\left(\frac{1}{x}\right). \end{aligned} \tag{A.3}$$

Using the CDF of the exponential RV given in (2), we obtain

$$F_{Z_{\mathrm{BR}_{a,j}}}(x) = 1 - \exp\left(-\Omega_{\mathrm{BR}_{a,j}} x\right). \tag{A.4}$$

where

$$\Omega_{\mathrm{BR}_{a,j}} = \frac{\lambda_{\mathrm{BR}_{a,j}}}{\chi P}. \tag{A.5}$$

Using integral table [53, eq. (1.111)], the CDF of RV $\frac{\varphi_{\mathrm{R}_{a,j}\ \max}(1-\kappa\rho_a)}{\rho_a N_0}$ is obtained as

$$\begin{aligned}&F_{\frac{\varphi_{\mathrm{R}_{a,j}\ \max}(1-\kappa\rho_a)}{\rho_a N_0}}(y)\\ &= \Pr\left(\max_{k=1,2,\ldots K}\left(\frac{\gamma_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)}{\rho_a N_0}\right) < y\right)\\ &= \left(F_{\frac{\gamma_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)}{\rho_a N_0}}(y)\right)^K = \left(1 - \exp\left(-\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k} y\right)\right)^K\\ &= 1 + \sum_{k=1}^{K} C_K^k (-1)^k \exp\left(-k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k} y\right). \end{aligned} \tag{A.6}$$

where

$$C_K^k = \frac{K!}{k!(K-k)!}, \Omega_{\mathrm{R}_{a,j}\mathrm{E}_k} = \frac{\lambda_{\mathrm{R}_{a,j}\mathrm{E}_k}\rho_a N_o}{1-\kappa\rho_a}. \tag{A.7}$$

Combining (A.4)-(A.6), yields

$$\begin{aligned}F_X(x) &= 1 - \exp\left(-\Omega_{\mathrm{BR}_{a,j}} x\right)\\ &- \sum_{k=1}^{K} C_K^k (-1)^k \exp\left(-\Omega_{\mathrm{BR}_{a,j}} x - \frac{k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}}{x}\right). \end{aligned} \tag{A.8}$$

Substituting (A.8) and $f_{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}(y) = \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \exp\left(-\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} y\right)$ into (A.2), we obtain

$$\mathrm{OP}_{j,a} = 1 - (I_1 + I_2). \tag{A.9}$$

where $I_1$ and $I_2$ can be expressed as in (A.10).

Using integral table [53, eq. (3.324.1)], $\int\limits_0^\infty \exp\left(-\frac{\beta}{4x} - \gamma x\right)dx = \sqrt{\frac{\beta}{\gamma}} K_1(\sqrt{\beta\gamma})$, after calculating the integrals, $I_1$ and $I_2$ are easily calculated as in (A.11).

Substituting (A.11). into (A.9), we finish the proof.

## Appendix B: Proof of Corollary 1

We consider the outage performance at high transmit power $P$ , i.e., $P \to +\infty$. Indeed, at high $P$ region, we can obtain (B.1) from (12) as

$$P_{\mathrm{R}_{a,j}}^{\max} \overset{P\to+\infty}{\approx} \begin{cases} Z_{\mathrm{BR}_{a,j}}; & \mathrm{if}\kappa \geq 1/\rho_a \\ \frac{\rho_a N_0}{\varphi_{\mathrm{R}_{a,j}\ \max}(1-\kappa\rho_a)}; & \mathrm{if}\kappa < 1/\rho_a \end{cases} \tag{B.1}$$

- $Case\ 1 : \kappa \geq 1/\rho_a$.

Similar to (A.1), we easily obtain $\mathrm{OP}_{j,a} = 1$.

- $Case\ 2 : \kappa < 1/\rho_a$.

Using (B.1) and (A.2) to calculate the outage probability at the $j$th hop on the shortest path, we obtain the following result:

$$\begin{aligned}\mathrm{OP}_{j,a} &\overset{P\to+\infty}{\approx} \Pr\left(X < \frac{\rho_a}{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}(1-\kappa\rho_a)}\right)\\ &\overset{P\to+\infty}{\approx} \int_0^{+\infty} F_X\left(\frac{\rho_a N_0}{y(1-\kappa\rho_a)}\right) f_{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}(y)\,dy, \end{aligned} \tag{B.2}$$

$$
\begin{aligned}
&I_1 = \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \int_0^{+\infty} \exp\left(-\tfrac{\Omega_{\mathrm{BR}_{a,j}}\rho_a N_0}{y(1-\kappa\rho_a)}\right) \exp\left(-\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} y\right) dy,\\
&I_2 = \sum_{k=1}^{K} C_K^k (-1)^k \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \int_0^{+\infty} \exp\left(-\tfrac{\Omega_{\mathrm{BR}_{a,j}}\rho_a N_0}{y(1-\kappa\rho_a)}\right) \exp\left(-\left(\tfrac{k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)}{\rho_a N_0} + \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\right) y\right) dy.
\end{aligned}
\tag{A.10}
$$

$$
\begin{aligned}
I_1 =& 2\sqrt{\frac{\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\Omega_{\mathrm{BR}_{a,j}}\rho_a N_0}{1-\kappa\rho_a}} K_1\left(2\sqrt{\frac{\Omega_{\mathrm{BR}_{a,j}}\rho_a N_0 \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}{1-\kappa\rho_a}}\right),\\
I_2 =& 2\sum_{k=1}^{K} C_K^k (-1)^k \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \rho_a N_0 \sqrt{\frac{\Omega_{\mathrm{BR}_{a,j}}}{k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)^2 + \rho_a N_0 \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}(1-\kappa\rho_a)}}\\
&\times K_1\left(2\sqrt{\frac{\Omega_{\mathrm{BR}_{a,j}}}{(1-\kappa\rho_a)}\left(k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a) + \rho_a N_0 \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\right)}\right).
\end{aligned}
\tag{A.11}
$$

where

$$
X = \frac{\rho_a N_0}{\varphi_{\mathrm{R}_{a,j}\,\max}(1-\kappa\rho_a)}. \tag{B.3}
$$

Similar to (A.8), we have

$$
\begin{aligned}
F_X(x) &= \Pr\left(\frac{\rho_a N_0}{\varphi_{\mathrm{R}_{a,j}\,\max}(1-\kappa\rho_a)} < x\right)\\
&= 1 - \Pr\left(\frac{\varphi_{\mathrm{R}_{a,j}\,\max}(1-\kappa\rho_a)}{\rho_a N_0} < \frac{1}{x}\right)\\
&= 1 - F_{\varphi_{\mathrm{R}_{a,j}\,\max}(1-\kappa\rho_a)/(\rho_a N_0)}\left(\frac{1}{x}\right)\\
&= 1 - \left(1 + \sum_{k=1}^{K} C_K^k (-1)^k \exp\left(-k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}/x\right)\right)\\
&= \sum_{k=1}^{K} C_K^k (-1)^{k+1} \exp\left(-k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}/x\right).
\end{aligned}
\tag{B.4}
$$

By substituting (B.4) and $f_{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}(y) = \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \exp\left(-\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} y\right)$ into (B.2), we can easily obtain $\mathrm{OP}_{j,a}$ as in (B.5) at the top of next page.

Finally, by combining $\mathrm{OP}_{j,a} = 1$ when $\kappa \geq 1/\rho_a$, (B.5) and (26), the proof of Corollary 1 is concluded.

## Appendix C: Proof of Lemma 2

- *Case* $1: \kappa \geq 1/\rho_u$.

Similar to (A.1) ,we easily obtain $\mathrm{OP}_{j,a} = 1$.

- *Case* $2: \kappa < 1/\rho_u$.

Firstly, $\mathrm{OP}_{j,a}$ of the $j$th hop can be rewritten by

$$
\begin{aligned}
\mathrm{OP}_{j,a} &= \Pr\left(\Delta_{3,a,j} < \frac{\rho_a N_0}{1-\kappa\rho_a}\right)\\
&= \int_0^{+\infty} F_Y\left(\frac{\rho_a N_0}{y(1-\kappa\rho_a)}\right) f_{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}(y)\, dy,
\end{aligned}
\tag{C.1}
$$

where

$$
Y = \min\left(Z_{\mathrm{BR}_{a,j}}, \frac{\rho_a N_0}{\varphi_{\mathrm{R}_{a,j} sum}(1-\kappa\rho_a)}\right). \tag{C.2}
$$

Similar to (A.3), we have

$$
F_Y(x) = 1 - \left(1 - F_{Z_{\mathrm{BR}_{a,j}}}(x)\right) F_{\frac{\varphi_{\mathrm{R}_{a,j} sum}(1-\kappa\rho_a)}{\rho_a N_0}}\left(\frac{1}{x}\right). \tag{C.3}
$$

Moreover, the CDF of the summation of the exponential RVs can be obtained by

$$
\begin{aligned}
&F_{\frac{\varphi_{\mathrm{R}_{a,j} sum}(1-\kappa\rho_a)}{\rho_a N_0}}(y)\\
&= 1 - \sum_{k=0}^{K-1} \frac{\left(\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k} y\right)^k}{k!} \exp\left(-\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k} y\right).
\end{aligned}
\tag{C.4}
$$

Combining (A.4), (C.3) and (C.4), yields

$$
\begin{aligned}
F_Y(x) &= 1 - \exp\left(-\Omega_{\mathrm{BR}_{a,j}} x\right)\\
&+ \sum_{k=0}^{K-1} \frac{\left(\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}\right)^k}{x^k k!} \exp\left(-\Omega_{\mathrm{BR}_{a,j}} x - \frac{\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}}{x}\right).
\end{aligned}
\tag{C.5}
$$

Substituting (C.5) and $f_{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}(y)$ into (C.1), we obtain

$$
\mathrm{OP}_{j,a} = 1 - \left(I_1 - I_3\right), \tag{C.6}
$$

where $I_3$ can be expressed as in (C.7).

Similar to (A.11), after some algebraic manipulations, we obtain (C.8). Finally, substituting (C.8) into (C.6), we finish the proof.

## Appendix D: Proof of Corollary 2

At high $P$ region, we can obtain (D.1) from (18) as

$$
P_{\mathrm{R}_{a,j}}^{\max} \overset{P\to+\infty}{\approx} \begin{cases} Z_{\mathrm{BR}_{a,j}}; & \text{if } \kappa \geq 1/\rho_a \\ \frac{\rho_a N_0}{\varphi_{\mathrm{R}_{a,j} sum}(1-\kappa\rho_a)}; & \text{if } \kappa < 1/\rho_a \end{cases} \tag{D.1}
$$

- *Case* $1: \kappa \geq 1/\rho_u$.

Similarly, we have $\mathrm{OP}_{j,a} = 1$.

- *Case* $2: \kappa < 1/\rho_u$.

In this case, we obtain the following result:

$$
\begin{aligned}
\mathrm{OP}_{j,a} &\overset{P\to+\infty}{\approx} \Pr\left(Y < \frac{\rho_a}{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}(1-\kappa\rho_a)}\right)\\
&\overset{P\to+\infty}{\approx} \int_0^{+\infty} F_Y\left(\frac{\rho_a N_0}{y(1-\kappa\rho_a)}\right) f_{\gamma_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}}(y)\, dy,
\end{aligned}
\tag{D.2}
$$

$$\begin{aligned}\mathrm{OP}_{j,a} &\overset{P\to+\infty}{\approx} \int_0^{+\infty} \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \sum_{k=1}^{K} C_K^k (-1)^{k+1} \exp\left(-\frac{k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)y}{\rho_a N_0}\right) \exp\left(-\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} y\right) dy \\ &\overset{P\to+\infty}{\approx} \sum_{k=1}^{K} C_K^k (-1)^{k+1} \frac{\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\rho_a N_0}{\lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\rho_a N_0 + k\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)}. \end{aligned} \tag{B.5}$$

$$\begin{aligned} I_3 = &\sum_{k=0}^{K-1} \frac{\left[\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)\right]^k}{(\rho_a N_0)^k k!} \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \\ &\times \int_0^{+\infty} y^k \exp\left(-\frac{\Omega_{\mathrm{BR}_{a,j}}\rho_a N_0}{y(1-\kappa\rho_a)}\right) \exp\left(-\left(\frac{\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)}{\rho_a N_0} + \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\right) y\right) dy. \end{aligned} \tag{C.7}$$

$$\begin{aligned} I_3 = &2 \sum_{k=0}^{K-1} \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \rho_a N_0 \frac{\left[\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)\right]^k}{k!} \times \sqrt{\left(\frac{\Omega_{\mathrm{BR}_{a,j}}}{\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)^2 + \rho_a N_0 \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}(1-\kappa\rho_a)}\right)^{k+1}} \\ &\times K_{-k-1}\left(2\sqrt{\Omega_{\mathrm{BR}_{a,j}}\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k} + \frac{\Omega_{\mathrm{BR}_{a,j}}\rho_a N_0 \lambda_{R_{a,j}R_{a,j+1}}}{(1-\kappa\rho_a)}}\right). \end{aligned} \tag{C.8}$$

where

$$Y = \frac{\rho_a N_0}{\varphi_{\mathrm{R}_{u,j}sum}(1-\kappa\rho_a)}. \tag{D.3}$$

Moreover, using (C.4), we have

$$F_Y(x) = \sum_{k=0}^{K-1} \frac{\left(\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}\right)^k}{x^k k!} \exp\left(-\frac{\Omega_{R_{a,j},\mathrm{E}_k}}{x}\right), \tag{D.4}$$

Combining (D.2) and (D.4), after some manipulations, we can obtain $\mathrm{OP}_{j,a}$ as

$$\begin{aligned} \mathrm{OP}_{j,a} &\overset{P\to+\infty}{\approx} \sum_{k=0}^{K-1} \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}} \rho_a N_0 \left[\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a)\right]^k \\ &\times \left(\frac{1}{\Omega_{\mathrm{R}_{a,j}\mathrm{E}_k}(1-\kappa\rho_a) + \lambda_{\mathrm{R}_{a,j}\mathrm{R}_{a,j+1}}\rho_a N_0}\right)^{k+1}. \end{aligned} \tag{D.5}$$

Finally, by substituting $\mathrm{OP}_{j,a} = 1$ when $\kappa \geq 1/\rho_a$ and (D.5) when $\kappa < 1/\rho_u$ into (38), the proof in Corollary 2 is concluded.

## References

[1] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *J. Netw. Comput. Appl.*, vol. 60, pp. 192-219, Jan. 2016.

[2] F. Akhtar and M. H. Rehmani, "Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: A review," *Renew. Sustain. Energy Rev.*, vol. 45, pp. 769-784, May 2015.

[3] T. D. Hieu, L. T. Dung, B.S. Kim, "Stability-aware geographic routing in energy harvesting wireless sensor networks," *Sensors*, vol. 16, no. 5, pp. 1-15, 2016.

[4] S. Ghafoor, M. H. Rehmani, S. Cho, and S.-H. Park, "An efficient trajectory design for mobile sink in a wireless sensor network," *Comput. Electr. Eng.*, vol. 40, no. 7, pp. 2089-2100, 2014.

[5] L. R. Varshney, "Transporting Information and Energy Simultaneously," *in Proc. of IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 1612-1616.

[6] Q. Shi, L. Liu, W. Xu and R. Zhang, "Joint Transmit Beamforming and Receive Power Splitting for MISO SWIPT Systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3269-3280, Jun. 2014.

[7] M. Usman and I. Koo, "Access Strategy for Hybrid Underlay-Overlay Cognitive Radios With Energy Harvesting," *IEEE Sensors Journal*, vol. 14, no. 9, pp. 3164-3173, Sept. 2014.

[8] H. H. Chen, Y. Li, Y. Jiang, Y. Ma, B. Vucetic, "Distributed Power Splitting for SWIPT in Relay Interference Channels Using Game Theory," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 410-420, Jan. 2015.

[9] U. Baroudi, "Robot-Assisted Maintenance of Wireless Sensor Networks Using Wireless Energy Transfer," *IEEE Sensors Journal*, vol. 17, no. 14, pp. 4661-4671, Jul. 2017.

[10] R. Zhang and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989-2001, May 2013.

[11] X. Zhou, R. Zhang and C. K. Ho, "Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754-4767, Nov. 2013.

[12] 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, Jul. 2013.

[13] J. N. Laneman, D. N. C. Tse and G.W.Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062-3080, Dec. 2004.

[14] S. Guo, F. Wang, Y. Yang and B. Xiao, "Energy-Efficient Cooperative Transmission for Simultaneous Wireless Information and Power Transfer in Clustered Wireless Sensor Networks," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4405-4417, Nov. 2015.

[15] N. Jain and V. A. Bohara, "Energy Harvesting and Spectrum Sharing Protocol for Wireless Sensor Networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 697-700, Dec. 2015.

[16] T. Liu, X. Wang and L. Zheng, "A Cooperative SWIPT Scheme for Wirelessly Powered Sensor Networks," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2740-2752, Jun. 2017.

[17] M. Mao, N. Cao, Y. Chen and Y. Zhou, "Multi-hop Relaying Using Energy Harvesting," *IEEE Wireless Commun. Lett.*, vol. 4, pp. 565-568, Oct. 2015.

[18] I. W. Lai, C. H. Lee, K. C. Chen and E. Biglieri, "Open-Loop End-to-End Transmission for Multihop Opportunistic Networks With Energy-Harvesting Devices," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2860-2872, Jul. 2016.

[19] K. Chin, L. Wang and S. Soh, "Joint Routing and Links Scheduling in Two-Tier Multi-Hop RF-Energy Harvesting Networks," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1864-1867, Sept. 2016.

[20] E. Chen, M. Xia, DB da Costa and S. Aissa, "Multi-Hop Cooperative Relaying with Energy Harvesting from Co-Channel Interferences," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1199-1202, May 2017.

[21] 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.

[22] C. Xu, M. Zheng, W. Liang, H. Yu and Y. C. Liang, "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.

[23] A. D. Wyner, "The wire-tap channel," *The Bell Syst Techn J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[24] P. K. Gopala, L. Lai and H. E. Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[25] I. Krikidis, J. S. Thompson and S. McLaughlin, "Relay Selection for Secure Cooperative Networks with Jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

[26] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan and T. Q. Duong, "Relay Selection for Security Enhancement in Cognitive Relay Networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46-49, Feb. 2015.

[27] J. Mo, M. Tao and Y. Liu, "Relay Placement for Physical Layer Security: A Secure Connection Perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878-881, Jun. 2012.

[28] G. Geraci, S. Singh, J. Andrews, J. Yuan and I. Collings, "Secrecy Rates in Broadcast Channels With Confidential Messages and External Eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931-2943, May 2014.

[29] Y. Zhang, Y. Shen, H. Wang, J. Yong and X. Jiang, "On Secure Wireless Communications for IoT Under Eavesdropper Collusion," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1281-1293, Jul. 2016.

[30] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan and H. V. Poor, "Security Enhancement of Cooperative Single Carrier Systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90-103, Jan. 2015.

[31] M. Zhang and Y. Liu, "Energy Harvesting for Physical-Layer Security in OFDMA Networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 154-162, Jan. 2016.

[32] W. Yang, W. Mou, X. Xu, W. Yang and Y. Cai, "Energy Efficiency Analysis and Enhancement for Secure Transmission in SWIPT Systems Exploiting Full Duplex Techniques," *IET Commun.*, vol. 10, no. 14, pp. 1712-1720, Sept. 2016.

[33] A. Singh, M. R. Bhatnagar and R. K. Mallik, "Secrecy Outage of a Simultaneous Wireless Information and Power Transfer Cognitive Radio System," *IEEE Wireless Commun. Lett.*, vol. 5, no. 3, pp. 288-291, Mar. 2016.

[34] L. Jiang, H. Tian, C. Qin, S. Gjessing and Y. Zhang, "Secure Beamforming in Wireless-Powered Cooperative Cognitive Radio Networks," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 522-525, Mar. 2016.

[35] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe and M. S. Alouini, "On Secure Underlay MIMO Cognitive Radio Networks With Energy Harvesting and Transmit Antenna Selection," *IEEE Trans. Green Commun. and Netw.*, vol. 1, no. 2, pp. 192-203, Jun. 2017.

[36] W. Liu, X. Zhou, S. Durrani and P. Popovski, "Secure Communication With a Wireless-Powered Friendly Jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401-415, Jan. 2016.

[37] T. M. Hoang, T. Q. Duong, N. S. Vo and C. Kundu, "Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174-177, Apr. 2017.

[38] M. O. Hasna and M.-S. Alouini, "Outage Probability of Multihop Transmission over Nakagami Fading Channels," *IEEE Commun. Lett.*, vol. 7, no. 5, pp. 216-218, May 2003.

[39] V. A. Aalo, K. P. Peppas, G. P. Efthymoglou, M. M. Alwakeel and S. S. Alwakeel, "Serial Amplify-and-Forward Relay Transmission Systems in Nakagami-m Fading Channels With a Poisson Interference Field," *IEEE Trans. Veh. Techn.*, vol. 63, no. 5, pp. 2183-2196, Jun. 2014.

[40] J. Boyer, D. D. Falconer and H. Yanikomeroglu, "Multihop Diversity in Wireless Relaying Channels," *IEEE Trans. Commun.*, vol. 52, no. 10, pp. 1820-1830, Oct. 2004.

[41] H. Chen, L. Liu, J. D. Matyjas and M. J. Medley, "Cooperative Routing for Underlay Cognitive Radio Networks Using Mutual-Information Accumulation," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 7110-7122, Dec. 2015.

[42] M. R. Bhatnagar, "Performance Analysis of a Path Selection Scheme in Multi-Hop Decode-and-Forward Protocol," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 1980-1983, Dec. 2012.

[43] M. R. Bhatnagar, R. K. Mallik and O. Tirkkonen, "Performance Evaluation of Best-Path Selection in a Multihop Decode-and-Forward Cooperative System," *IEEE Trans. Veh. Techn.*, vol. 65, no. 4, pp. 2722-2728, Apr. 2016.

[44] T. D. Hieu, T. T. Duy, S-G Choi, "Performance Enhancement for Harvest-to-Transmit Cognitive Multi-hop Networks with Best Path Selection Method under Presence of Eavesdropper," in *Proc. IEEE 2018 20th ICACT*, pp. 323-328, 2018.

[45] E. Bjornson, M. Matthaiou and M. Debbah, "A New Look at Dual-hop Relaying: Performance Limits with Hardware Impairments," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4512-4525, Nov. 2013.

[46] 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.

[47] T. T. Duy, T. Q. Duong, D. B. da Costa, V. N. Q. 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.

[48] A. A. Boulogeorgos, D. S. Karas and G. K. Karagiannidis, "How much does I/Q Imbalance affect secrecy capacity?," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1305-1308, Jul. 2016.

[49] 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.

[50] N. N. Tan, T. T. Duy, L. G. Thien, T. T. Phuong and M. Voznak, "Energy Harvesting-based Spectrum Access with Incremental Cooperation, Relay Selection and Hardware Noises," *RadioEngineering*, vol. 26, no. 1, pp. 240-250, Apr. 2017.

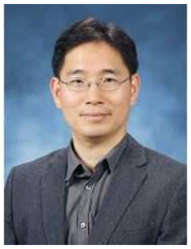
[51] V. P. Tuan and H. Y. Kong, "Impact of Residual Transmit RF Impairments on Energy Harvesting Relay Selection Systems," *Int. J. Electr.*, vol. 104, no. 6, pp. 928-941, Jun. 2017.

[52] X. Ding, T. Song, Y. Zou and X. Chen, "Security-Reliability Tradeoff for Friendly Jammer Assisted User-Pair Selection in the Face of Multiple Eavesdroppers," *IEEE Access*, vol. 4, pp. 8386-8393, Sept. 2016.

[53] I. S. Gradshten, I. M. Ryzhik, Table of integrals, series, and products, 7th ed. New York: Academic Press, 2007.

**Tran Dinh Hieu** was born in Gia Lai, Viet Nam, in 1989. He received the B.E. degree in Electronics and Telecommunication Engineering from Ho Chi Minh City University of Technology, Vietnam, in 2012. From 2015 to 2017, he studied the Master degree in Electronics and Computer Engineering from Hongik University, Korea. He is currently pursuing the Ph.D degree with Chungbuk National University, South Korea. His major research interests include: Physical layer security, cognitive radio, and cooperative communications.

**Tran Trung Duy** was born in Nha Trang city, Vietnam, in 1984. He received the B.E. degree in Electronics and Telecommunications Engineering from the French-Vietnamese training program for excellent engineers (PFIEV), HoChiMinh City University of Technology, Vietnam in 2007. In 2013, he received the Ph.D degree in electrical engineering from University of Ulsan, South Korea. In 2013, he joined the Department of Telecommunications, Posts and Telecommunications Institute of Technology (PTIT), as a lecturer. In 2016, he received the prestigious Exemplary Reviewer Certificates of IEEE Communications Letters and IEEE Transactions on Communications. He has been a member of Technical Program Committee for conferences such as SigTelCom, ComManTel, ATC, NICS, ISCE, ICACCI. From 2017, he served as an associate editor for REV Journal on Electronics and Communications (REV-JEC). His major research interests are cooperative communication, cooperative routing, cognitive radio, physical-layer security, energy harvesting, hardware impairments and NOMA.



**Byung-Seo Kim** (M'02) received his B.S. degree in Electrical Engineering from In-Ha University, In-Chon, Korea in 1998 and his M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Florida in 2001 and 2004, respectively. His Ph.D. study was supervised by Dr. Yuguang Fang. Between 1997 and 1999, he worked for Motorola Korea Ltd., PaJu, Korea as a Computer Integrated Manufacturing (CIM) Engineer in Advanced Technology Research and Development (ATR&D). From January 2005 to August 2007, he worked for Motorola Inc., Schaumburg Illinois, as a Senior Software Engineer in Networks and Enterprises. His research focuses in Motorola Inc. were designing protocol and network architecture of wireless broadband mission critical communications. He is currently an Associate Professor at the Department of Computer and Information Communication Engineering in Hongik University, Korea. He was Chairman of the department from 2012 to 2014. He served as the General Chair for General Chair of 3rd IWWCN 2017, and the TPC member for the IEEE VTC 2014-Spring and the EAI FUTURE2016, and ICGHIC 2016∼2019 conferences. He served as Guest Editors of special issues of International Journal of Distributed Sensor Networks (SAGE), IEEE Access, and Journal of the Institute of Electrics and Information Engineers. He was also served as the Member of Sejong-city Construction Review Committee and Ansan-city Design Advisory Board. His work has appeared in around 161 publications and 22 patents. He is IEEE Senior Member and Associative Editor of IEEE Access. His research interests include the design and development of efficient wireless/wired networks including link-adaptable/cross-layer-based protocols, multi-protocol structures, wireless CCNs/NDNs, Mobile Edge Computing, physical layer design for broadband PLC, and resource allocation algorithms for wireless networks.