Secure Wireless Communications with Relay Selection and Wireless Powered Transfer

Nam-Phong Nguyen[*], Yuzhen Huang[†], Trung Q. Duong[*], Zoran Hadzi-Velkov[§], and Berk Canberk[‡]
[*]Queen's University Belfast, UK (e-mail: {pnguyen04,trung.q.duong}@qub.ac.uk)
[†]PLA University of Science and Technology, China (e-mail: yzh_huang@sina.com)
[‡]Ss. Cyril and Methodius University, Macedonia (e-mail: zoranhv@feit.ukim.edu.mk)
[‡]Istanbul Technical University, Turkey (e-mail: canberk@itu.edu.tr)

***Abstract*—In this paper, we investigate the secrecy performance of an energy harvesting relay network, where a legitimate source communicates with a legitimate destination via the assistance of multiple trusted relays. In the considered system, the source and relays deploy the time-switching based radio frequency energy harvesting technique to harvest energy from a multi-antenna beacon. Different antenna selection and relay selection schemes are applied to enhance the security of the system. Specifically, two relay selection schemes based on the partial and full knowledge of channel state information are proposed. The exact closed-form expressions of the systems secrecy outage probability in these schemes are derived. A Monte-Carlo based simulation validates our analysis results.**

I. Introduction

Relay networks have been well-known for enhancing the coverage of wireless systems. In addition, various relay selection protocols and relaying schemes, such as amplify-and-forward (AF) and decode-and-forward (DF), were introduced to relay networks and proved to bring significant improvements [1]. However, in some cases (i.e wireless sensor networks (WSNs)), the source and relay nodes are energy-constrained, which limits the network performance. Prolonging the life time of these networks has many difficulties since replacing or recharging nodes' batteries is either inconvenient (e.g widely distributed) or undesirable (e.g inside human body) [2]. To overcome such a challenge, radio frequency (RF) energy harvesting (EH) has been proposed to relay network and has attracted a great deal of attention recently [3]–[5]. To enable EH, a wireless node is equipped with rectifying circuits that can transform RF signal from source nodes into DC current. This DC current is then used for the signal processing and transmission of the wireless node. In [6] and [7], the authors investigated a EH system that the destination simultaneously receives information signal and harvests RF energy from the source. Inspired by these works, in [8]–[10], the authors studied the performance of wireless communication systems that are applied EH technique. These studies have laid a solid foundation for understanding the role of EH in the relay networks.

Although the EH relay networks have significant advantages, transmitting energy and information simultaneously makes the data transmissions vulnerable to security attacks. The upper layer cryptographic techniques are typically deployed to secure the confidential messages against wiretapping in the conventional wireless communications. However, these high layer security schemes are more expensive and uncertain. To support the existing cryptographic protocols, physical layer security (PLS), which exploits the characteristics of wireless channels to improve the security of wireless transmission [11], has been proposed as a promising solution [12]–[19]. Recently, there have been studies on PLS for EH networks. In [20], the authors considered the simultaneously wireless information and power transferring network with eavesdroppers and two types of receivers: desired receivers and idle receivers, in which the latter are treated as potential eavesdroppers. In [21], the authors proposed a cooperative jamming scheme, where a multi-antenna jammer harvests energy from the source and uses this energy to transmit jamming signals. In [19], the security performance of EH single-relay networks has been considered. Nevertheless, the secrecy performance of EH multiple-relay networks has not been well investigated.

In this paper, we investigate the security performance of an EH relay network, in which the source and relays are powered by RF energy from a multi-antenna beacon. The time-switching (TS) based EH technique is applied at the source and relays thanks to its high throughput [7]. In addition, DF protocol is used at the relays with the assumption that the source and relays use different code books to improve the secrecy performance [22]. The eavesdropper in the considered system performs a passive eavesdropping scenario and listens to both the source and relays. Two relay selection schemes, namely partial relay selection (PRS) and optimal relay selection (ORS), are proposed. In these two scenarios, the beacon applies antenna selection technique to maximize the EH channel of either the source (MEHS) or the relays (MEHR).

II. System and Channel Models

We consider a network consisting of a beacon B, a source S, K DF relays R_k, $k = \{1, ..., K\}$, a destination D and an eavesdropper E as shown in Fig. 1. The beacon B is equipped with N antennas while S, R_k, E, and D are equipped with single antenna. We assume that all the channels are Rayleigh distributed. Therefore, the channel power gains are exponential distributed with parameter λ_{XY}, where $X \in \{\mathsf{B}, \mathsf{S}, \mathsf{R}\}$ and $Y \in \{\mathsf{S}, \mathsf{R}, \mathsf{E}, \mathsf{D}\}$. The additive white Gaussian noise (AWGN) at R and D have zero mean and variance N_0.

A. Energy Harvesting Scheme

In the considered system, S and R_k harvest energy from B, and then use this energy to transmit signal. We assume that B

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

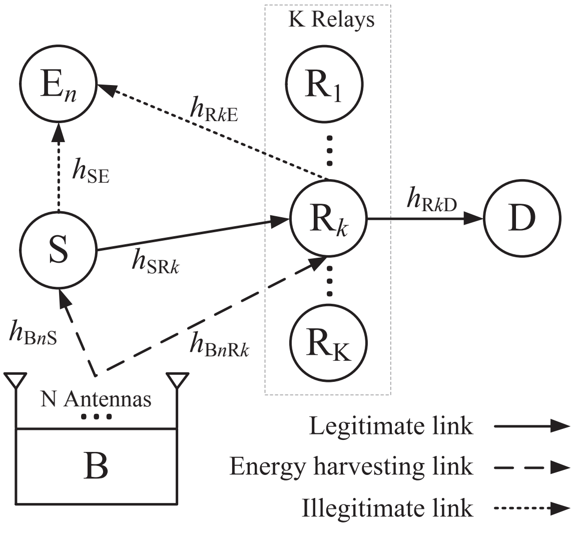

Fig. 1: System model.

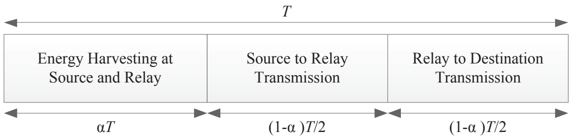
T
Energy Harvesting at Source and Relay
Source to Relay Transmission
Relay to Destination Transmission
αT
(1-α)T/2
(1-α)T/2

Fig. 2: Time switching based protocol.

can only be temporarily deployed to power S and R_k because of its duty of transmitting information to other nodes. The TS based technique is applied at S and R as described in Fig. 2. Therefore, the energy harvested at S and R_k respectively are [7]

$$E_{\mathsf{S}} = \eta \mathcal{P}_{\mathsf{B}} \alpha T |h_{\mathsf{B}_n\mathsf{S}}|^2, \tag{1}$$

$$E_{\mathsf{R}} = \eta \mathcal{P}_{\mathsf{B}} \alpha T |h_{\mathsf{B}_n\mathsf{R}_k}|^2, \tag{2}$$

where $0 < \eta < 1$ is the efficiency coefficient of the energy conversion process, $\mathcal{P}_{\mathsf{B}}$ is the transmit power of B, T is the transmission block time in which a block of information is sent from S to D, $|h_{\mathsf{B}_n\mathsf{S}}|^2$ and $|h_{\mathsf{B}_n\mathsf{R}_k}|^2$ are channel power gain of the links from the n^{th} antenna at $\mathsf{B} \to \mathsf{S}$ and R_k, respectively, $0 \leq \alpha \leq 1$, which depends on the schedule of B, is the fraction of the block time in which S and R_k harvest energy from B. Optimizing α is out of the scope of this paper. Under the assumption that the processing energy at S and R_k is negligible, the transmit power of S and R_k are respectively given by [7]

$$\mathcal{P}_{\mathsf{S}} = \frac{2\eta \mathcal{P}_{\mathsf{B}} |h_{\mathsf{B}_n\mathsf{S}}|^2 \alpha}{(1-\alpha)}, \tag{3}$$

$$\mathcal{P}_{\mathsf{R}} = \frac{2\eta \mathcal{P}_{\mathsf{B}} |h_{\mathsf{B}_n\mathsf{R}_k}|^2 \alpha}{(1-\alpha)}. \tag{4}$$

In order to reduce the complexity of signal processing, the beacon in the considered network applies antenna selection technique to facilitate S and R in harvesting energy.

1) Maximize the Source's Energy Harvesting Link (MEHS): The chosen antenna can be selected to strengthen the $\mathsf{B} \to \mathsf{S}$ link as follows:

$$s = \arg \max_{n=1,\dots,N} (|h_{\mathsf{B}_n\mathsf{S}}|^2), \tag{5}$$

2) Maximize the Relay's Energy Harvesting Link (MEHR): For maximizing the $\mathsf{B} \to \mathsf{R}_{k^*}$ link, the chosen antenna can be selected as

$$r = \arg \max_{n=1,\dots,N} (|h_{\mathsf{B}_n\mathsf{R}_{k^*}}|^2), \tag{6}$$

where the subscript k^* indicates the selected relay after the relay selection process.

B. Security Scenarios

In the considered network, E can listen to both $\mathsf{S} \to \mathsf{R}_k$ and $\mathsf{R}_k \to \mathsf{D}$ links. We assume that there is no direct link from $\mathsf{B} \to \mathsf{E}$. Therefore, E is not disturbed by the EH phase of S and R_k. Attempting to enhance security performance, S and R_k use different code books. Therefore, the secrecy capacity of the considered system is written as [22]

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

where C_{1s} and C_{2s} are the secrecy capacity of the first hop and the second hop, respectively. The secrecy capacity of the first hop and the second hop are respectively expressed as follows:

$$C_{1s} = \frac{1-\alpha}{2} \log_2 \frac{1+\gamma_{1\mathsf{M}}}{1+\gamma_{1\mathsf{E}}} = \epsilon \log_2 \frac{1+\gamma_{1\mathsf{M}}}{1+\gamma_{1\mathsf{E}}}, \tag{8}$$

$$C_{2s} = \frac{1-\alpha}{2} \log_2 \frac{1+\gamma_{2\mathsf{M}}}{1+\gamma_{2\mathsf{E}}} = \epsilon \log_2 \frac{1+\gamma_{2\mathsf{M}}}{1+\gamma_{2\mathsf{E}}}, \tag{9}$$

where the fraction $\frac{1-\alpha}{2}$ indicates that the transmission duration for the first hop and the second hop are $\frac{(1-\alpha)T}{2}$ of the total block time T, $\gamma_{1\mathsf{M}}$ is the signal to noise ratio (SNR) at R_{k^*}, $\gamma_{2\mathsf{M}}$ is the SNR at D, $\gamma_{1\mathsf{E}}$ and $\gamma_{2\mathsf{E}}$ are the SNRs of the first and the second hop at E, respectively, $\epsilon = \frac{1-\alpha}{2}$. $\gamma_{1\mathsf{M}}$ is given by

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

where $\gamma_{\mathsf{M}} = \frac{\mathcal{P}_{\mathsf{B}}}{N_0}$, $\xi = \frac{2\eta\alpha}{(1-\alpha)}$, and $|h_{\mathsf{SR}_{k^*}}|^2$ are the channel power gains of $\mathsf{S} \to \mathsf{R}_{k^*}$ links. Similarly, $\gamma_{2\mathsf{M}}$, $\gamma_{1\mathsf{E}}$, and $\gamma_{2\mathsf{E}}$ are respectively shown as

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

$$\gamma_{1\mathsf{E}} = \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_{n^*}\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2, \tag{12}$$

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

where $|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2$, $|h_{\mathsf{SE}}|^2$, and $|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2$ are the channel power gains of $\mathsf{R}_{k^*} \to \mathsf{D}$, $\mathsf{S} \to \mathsf{E}$, and $\mathsf{R}_{k^*} \to \mathsf{E}$ links, respectively, $\gamma_{\mathsf{E}} = \frac{\mathcal{P}_{\mathsf{B}}}{N_{\mathsf{E}}}$ and N_{E} is the variance of AWGN at E.

1) Partial Relay Selection (PRS): In some networks such as WSNs, relay selection can not utilized based on the channel state of all links in the network due to energy constraints. Therefore, the PRS scheme chooses the helping relay based on the channel state information (CSI) of the $\mathsf{S} \to \mathsf{R}$ links. The aiding relay R_{k^*} is selected as

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

The SNR at R_{k^*} is expressed as

$$\gamma_{1\mathsf{M}} = \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_{n^*}\mathsf{S}}|^2 \max_{k=1,\dots,K} (|h_{\mathsf{SR}_k}|^2), \tag{15}$$

where $n^* \in \{s, r\}$. From (15), (5), and (6), the secrecy capacity of the PRS scheme with two different antenna selection strategies at B are written as

$$\begin{aligned} C_{\mathsf{PRS}}^{\mathsf{MEHS}} &= \epsilon \log_2 \min \left(\frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SR}_{k^*}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2}, \right. \\ & \left. \frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_s\mathsf{R}_{k^*}}|^2 |h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_s\mathsf{R}_{k^*}}|^2 |h_{\mathsf{R}_{k^*}\mathsf{E}}|^2} \right), \end{aligned} \tag{16}$$

$$\begin{aligned} C_{\mathsf{PRS}}^{\mathsf{MEHR}} &= \epsilon \log_2 \min \left(\frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_r\mathsf{S}}|^2 |h_{\mathsf{SR}_{k^*}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_r\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2}, \right. \\ & \left. \frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_r\mathsf{R}_{k^*}}|^2 |h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_r\mathsf{R}_{k^*}}|^2 |h_{\mathsf{R}_{k^*}\mathsf{E}}|^2} \right). \end{aligned} \tag{17}$$

2) Optimal Relay Selection (ORS): In the ORS scheme, S has full knowledge of CSI to choose the aiding relay for maximizing the secrecy capacity of the system. The aiding relay R_{k^*} is chosen as

$$\begin{aligned} k^* = \arg \max_{k=1,\dots,K} & \left[\min \left(\frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_{n^*}\mathsf{S}}|^2 |h_{\mathsf{SR}_k}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_{n^*}\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2}, \right. \right. \\ & \left. \left. \frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_{n^*}\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{D}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_{n^*}\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{E}}|^2} \right) \right]. \end{aligned} \tag{18}$$

From (18) and (5), the secrecy capacity of the ORS scheme with MEHS is written as

$$\begin{aligned} C_{\mathsf{ORS}}^{\mathsf{MEHS}} = \epsilon \log_2 \max_{k=1,\dots,K} & \left[\min \left(\frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SR}_k}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2}, \right. \right. \\ & \left. \left. \frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_s\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{D}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_s\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{E}}|^2} \right) \right]. \end{aligned} \tag{19}$$

From (18) and (6), the secrecy capacity of the ORS scheme with MEHR is given as

$$\begin{aligned} C_{\mathsf{ORS}}^{\mathsf{MEHR}} = \epsilon \log_2 \max_{k=1,\dots,K} & \left[\min \left(\frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_r\mathsf{S}}|^2 |h_{\mathsf{SR}_k}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_r\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2}, \right. \right. \\ & \left. \left. \frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_r\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{D}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_r\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{E}}|^2} \right) \right]. \end{aligned} \tag{20}$$

III. Secrecy Outage Probability

In this section, the exact close-form expressions of the considered system's SOP are derived.

A. Partial Relay Selection

1) Maximizing Energy Harvesting Channel for The Source: From (16), we have

$$\begin{aligned} & \mathbb{P} \left\{ C_{\mathsf{PRS}}^{\mathsf{MEHS}} < R_{th} \right\} \\ &= \mathbb{P} \left\{ \min \left(\frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SR}_{k^*}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2}, \right. \right. \\ & \left. \left. \frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_s\mathsf{R}_{k^*}}|^2 |h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_s\mathsf{R}_{k^*}}|^2 |h_{\mathsf{R}_{k^*}\mathsf{E}}|^2} \right) < 2^{\frac{R_{th}}{\epsilon}} \right\} \\ &= \mathbb{P} \left\{ \gamma_{\mathsf{PRS}}^{\mathsf{MEHS}} < \beta \right\} \\ &= F_{\gamma_{\mathsf{PRS}}^{\mathsf{MEHS}}} (\beta), \end{aligned} \tag{21}$$

where $\beta = 2^{\frac{R_{th}}{\epsilon}}$.

From (21) we have the following lemma.

Lemma 1: The CDF of $\gamma_{\mathsf{PRS}}^{\mathsf{MEHS}}$ is formulated as follows:

$$\begin{aligned} & F_{\gamma_{\mathsf{PRS}}^{\mathsf{MEHS}}} (\beta) \\ &= 1 - \sum_{k=1}^{K} \sum_{n=1}^{N} \binom{K}{k} \binom{N}{n} (-1)^{k+n} \\ & \times \frac{4 \gamma_{\mathsf{M}} (\beta - 1) \lambda_{\mathsf{SE}} \lambda_{\mathsf{RE}} \sqrt{n \lambda_{\mathsf{BS}} \lambda_{\mathsf{BR}} \; k \lambda_{\mathsf{SR}} \lambda_{\mathsf{RD}}}}{\xi (k \gamma_{\mathsf{E}} \lambda_{\mathsf{SR}} \beta + \gamma_{\mathsf{M}} \lambda_{\mathsf{SE}}) (\gamma_{\mathsf{E}} \lambda_{\mathsf{RD}} \beta + \gamma_{\mathsf{M}} \lambda_{\mathsf{RE}})} \\ & \times \mathbf{K}_1 \left(2 \sqrt{\frac{\lambda_{\mathsf{RD}} \lambda_{\mathsf{BR}} (\beta - 1)}{\gamma_{\mathsf{M}} \xi}} \right) \mathbf{K}_1 \left(2 \sqrt{\frac{k \lambda_{\mathsf{SR}} \; n \lambda_{\mathsf{BS}} (\beta - 1)}{\gamma_{\mathsf{M}} \xi}} \right), \end{aligned} \tag{22}$$

where $\mathbf{K}_1(\cdot)$ is the modified Bessel function of the second kind.

Proof: The proof is given in Appendix A. ■

2) Maximizing Energy Harvesting Channel for The Selected Relay: From (17), the CDF of $\gamma_{\mathsf{PRS}}^{\mathsf{MEHR}}$ can be derived as

$$\begin{aligned} & F_{\gamma_{\mathsf{PRS}}^{\mathsf{MEHR}}} (\beta) \\ &= 1 - \sum_{k=1}^{K} \sum_{n=1}^{N} \binom{K}{k} \binom{N}{n} (-1)^{k+n} \\ & \times \frac{4 \gamma_{\mathsf{M}} (\beta - 1) \lambda_{\mathsf{SE}} \lambda_{\mathsf{RE}} \sqrt{\lambda_{\mathsf{BS}} \; n \lambda_{\mathsf{BR}} \; k \lambda_{\mathsf{SR}} \lambda_{\mathsf{RD}}}}{\xi (k \gamma_{\mathsf{E}} \lambda_{\mathsf{SR}} \beta + \gamma_{\mathsf{M}} \lambda_{\mathsf{SE}}) (\gamma_{\mathsf{E}} \lambda_{\mathsf{RD}} \beta + \gamma_{\mathsf{M}} \lambda_{\mathsf{RE}})} \\ & \times \mathbf{K}_1 \left(2 \sqrt{\frac{n \lambda_{\mathsf{RD}} \lambda_{\mathsf{BR}} (\beta - 1)}{\gamma_{\mathsf{M}} \xi}} \right) \mathbf{K}_1 \left(2 \sqrt{\frac{k \lambda_{\mathsf{SR}} \lambda_{\mathsf{BS}} (\beta - 1)}{\gamma_{\mathsf{M}} \xi}} \right). \end{aligned} \tag{23}$$

B. Optimal Relay Selection

1) Maximizing Energy Harvesting Channel for The Source: From (19), we have

$$\begin{aligned} & \mathbb{P} \left\{ C_{\mathsf{ORS}}^{\mathsf{MEHS}} < R_{th} \right\} \\ &= \mathbb{P} \left\{ \max_{k=1,\dots,K} \left[\min \left(\frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SR}_k}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_s\mathsf{S}}|^2 |h_{\mathsf{SE}}|^2}, \right. \right. \right. \\ & \left. \left. \left. \frac{1 + \gamma_{\mathsf{M}} \xi |h_{\mathsf{B}_{n^*}\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{D}}|^2}{1 + \gamma_{\mathsf{E}} \xi |h_{\mathsf{B}_{n^*}\mathsf{R}_k}|^2 |h_{\mathsf{R}_k\mathsf{E}}|^2} \right) \right] < 2^{\frac{R_{th}}{\epsilon}} \right\} \\ &= \mathbb{P} \left\{ \gamma_{\mathsf{ORS}}^{\mathsf{MEHS}} < \beta \right\} \\ &= F_{\gamma_{\mathsf{ORS}}^{\mathsf{MEHS}}} (\beta). \end{aligned} \tag{24}$$

From (24) we have the following lemma.

Lemma 2: The CDF of $\gamma_{\mathsf{ORS}}^{\mathsf{MEHS}}$ is derived as follows:

$$\begin{aligned}
&F_{\gamma_{\mathsf{ORS}}^{\mathsf{MEHS}}}(\beta)\\
&= 1-\sum_{k=1}^{K}\sum_{n=1}^{N}\binom{K}{k}\binom{N}{n}(-1)^{k+n}\left(2\sqrt{\frac{\gamma_{\mathsf{M}}(\beta-1)}{\xi}}\right)^{k+1}\\
&\times\left[\frac{\lambda_{\mathsf{RE}}\sqrt{\lambda_{\mathsf{BR}}\lambda_{\mathsf{RD}}}}{\gamma_{\mathsf{M}}\lambda_{\mathsf{RE}}+\gamma_{\mathsf{E}}\lambda_{\mathsf{RD}}\beta}\mathbf{K}_1\left(2\sqrt{\frac{\lambda_{\mathsf{RD}}\lambda_{\mathsf{BR}}(\beta-1)}{\gamma_{\mathsf{M}}\xi}}\right)\right]^{k}\\
&\times\frac{\lambda_{\mathsf{SE}}\sqrt{n\lambda_{\mathsf{BS}}\ k\lambda_{\mathsf{SR}}}}{k\gamma_{\mathsf{E}}\lambda_{\mathsf{SR}}\beta+\gamma_{\mathsf{M}}\lambda_{\mathsf{SE}}}\mathbf{K}_1\left(2\sqrt{\frac{k\lambda_{\mathsf{SR}}\ n\lambda_{\mathsf{BS}}(\beta-1)}{\gamma_{\mathsf{M}}\xi}}\right). \qquad (25)
\end{aligned}$$

Proof: The proof is given in Appendix B. ■

2) Maximizing Energy Harvesting Channel for The Selected Relay: From (20), similar to $\gamma_{\mathsf{ORS}}^{\mathsf{MEHS}}$, we have the lemma.

Lemma 3: The CDF of $\gamma_{\mathsf{ORS}}^{\mathsf{MEHR}}$ can be derived as

$$\begin{aligned}
&F_{\gamma_{\mathsf{ORS}}^{\mathsf{MEHR}}}(\beta)\\
&= 1-\sum_{k=1}^{K}\binom{K}{k}(-1)^{k+1}\frac{\gamma_{\mathsf{M}}\lambda_{\mathsf{SE}}}{k\gamma_{\mathsf{E}}\lambda_{\mathsf{SR}}\beta+\gamma_{\mathsf{M}}\lambda_{\mathsf{SE}}}\\
&\times\left[\sum_{n=1}^{N}\binom{N}{n}(-1)^{n+1}\frac{4(\beta-1)\lambda_{\mathsf{RE}}\sqrt{n\lambda_{\mathsf{BS}}\lambda_{\mathsf{BR}}\lambda_{\mathsf{SR}}\lambda_{\mathsf{RD}}}}{\xi(\gamma_{\mathsf{M}}\lambda_{\mathsf{RE}}+\beta\gamma_{\mathsf{E}}\lambda_{\mathsf{RD}})}\right.\\
&\left.\times\mathbf{K}_1\left(2\sqrt{\frac{n\lambda_{\mathsf{RD}}\lambda_{\mathsf{BR}}(\beta-1)}{\gamma_{\mathsf{M}}\xi}}\right)\mathbf{K}_1\left(2\sqrt{\frac{\lambda_{\mathsf{SR}}\lambda_{\mathsf{BS}}(\beta-1)}{\gamma_{\mathsf{M}}\xi}}\right)\right]^{k}. \qquad (26)
\end{aligned}$$

Proof: The proof is given in Appendix C. ■

IV. Numerical Results

In this section, the simulation results based on Monte Carlo method are provided to verify the accuracy of the above performance analysis. In the two-dimensional topology, the co-ordinates of B, S, R, D, and E are $(0,0)$, $(1,1)$, $(2,0)$, $(3,0)$, and $(1,-4)$, respectively. The distance between the nodes is calculated as $d_{AB}=\sqrt{(x_A-x_B)^2+(y_A-y_B)^2}$, where A and B have the co-ordinates (x_A,y_A) and (x_B,y_B), respectively. To take path-loss into account, we assume $\lambda_X = d_X^{pl}$, where pl is the path-loss exponent and $\lambda_X = \{\lambda_{\mathsf{BS}},\lambda_{\mathsf{BR}},\lambda_{\mathsf{SR}},\lambda_{\mathsf{SE}},\lambda_{\mathsf{RE}},\lambda_{\mathsf{RE}},\lambda_{\mathsf{RD}}\}$. In this simulation, $pl=3$, $R_{th}=0.2$ bits/s/Hz, $\eta=0.7$, and $\alpha=0.5$.

Fig. 3 shows the SOP of the considered system in all the schemes. In general, the ORS scheme has better secrecy performance than the PRS scheme in both antenna selection strategies at the beacon. In this figure, the values of K and N are varied to examine the effect of the number of relays and the number of antennas at B on the secrecy performance of the considered system. As increasing K and N, the performance of the ORS scheme significantly improves while the SOP in the MEHR+PRS schemes slightly decreases. Meanwhile, the SOP in the MEHS+PRS scheme only reduces in the low SNR regime.

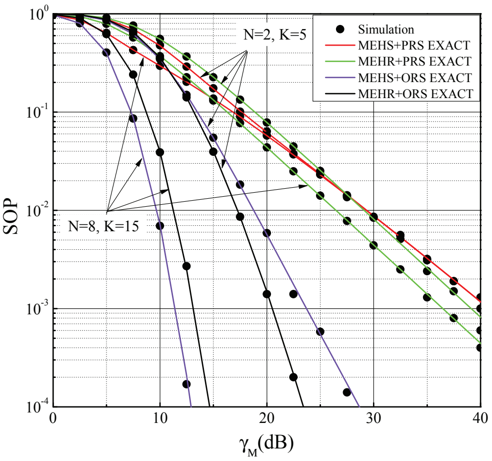

Fig. 3: SOP of the considered system vs γ_{M} in all schemes.

V. Conclusions

In this paper, the secrecy performance of the energy harvesting system with multiple relays and multiple antennas beacon has been investigated. In particular, the time-switching based energy harvesting technique was applied at S and R to harvest wireless energy from the beacon. In addition, the effect of four schemes, namely MEHS+PRS, MEHR+PRS, MEHS+ORS and MEHR+PRS, on the security of the considered system were examined. The exact closed-form expressions of the system's SOP in these schemes are derived. Finally, the numerical results were provided to validate our correctness.

Acknowledgement

This work was supported by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, by the Newton Institutional Link under Grant ID 172719890, and by the Newton Research Collaboration Program under Grant ID NRCP1516/1/131.

Appendix A
Proof of Lemma 1

From (21), we have

$$\gamma_{\mathsf{1PRS}}^{\mathsf{MEHS}} = \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{B}_s\mathsf{S}}|^2|h_{\mathsf{SR}_{k^*}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{B}_s\mathsf{S}}|^2|h_{\mathsf{SE}}|^2}, \qquad (A.1)$$

$$\gamma_{\mathsf{2PRS}}^{\mathsf{MEHS}} = \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{B}_s\mathsf{R}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{B}_s\mathsf{R}_{k^*}}|^2|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2}. \qquad (A.2)$$

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

$$\begin{aligned}
&\mathbb{P}\left\{\gamma_{\mathsf{1PRS}}^{\mathsf{MEHS}}<x\right\}\\
&= \int_0^\infty\int_0^\infty F_{|h_{\mathsf{SR}_{k^*}}|^2}\left(\frac{x[1+\gamma_{\mathsf{E}}\xi zt]-1}{\gamma_{\mathsf{M}}\xi z}\right)\\
&\times f_{|h_{\mathsf{B}_s\mathsf{S}}|^2}(z)\, f_{|h_{\mathsf{SE}}|^2}(t)\, dz\, dt\\
&= 1-\sum_{k=1}^{K}\sum_{n=1}^{N}\binom{K}{k}\binom{N}{n}(-1)^{k+n}\frac{n\gamma_{\mathsf{M}}\lambda_{\mathsf{BS}}\lambda_{\mathsf{SE}}}{\gamma_{\mathsf{M}}\lambda_{\mathsf{SE}}+xk\gamma_{\mathsf{E}}\lambda_{\mathsf{SR}}}\\
&\times 2\sqrt{\frac{k\lambda_{\mathsf{SR}}(x-1)}{n\gamma_{\mathsf{M}}\xi\lambda_{\mathsf{BS}}}}\mathbf{K}_1\left(2\sqrt{\frac{n\ k\lambda_{\mathsf{SR}}\lambda_{\mathsf{BS}}\ (x-1)}{\gamma_{\mathsf{M}}\xi}}\right). \qquad (A.3)
\end{aligned}$$

After performing some mathematical manipulations, (A.3) can be achieved with the help of [23, Eq. (3.324.1)].

The CDF of $\gamma_{\mathsf{2PRS}}^{\mathsf{MEHS}}$ is given as

$$\begin{aligned}
&\mathbb{P}\left\{\gamma_{\mathsf{2PRS}}^{\mathsf{MEHS}} < x\right\} = \int_0^\infty\int_0^\infty F_{|h_{\mathsf{R}_{k^*}\mathsf{D}}|^2}\left(\frac{x[1+\gamma_{\mathsf{E}}\xi yz]-1}{\gamma_{\mathsf{M}}\xi y}\right) \\
&\times f_{|h_{\mathsf{B}_s\mathsf{R}_{k^*}}|^2}\left(y\right) f_{|h_{\mathsf{R}_{k^*}\mathsf{E}}|^2}\left(z\right) dy\ dz \\
&= 1 - \frac{\gamma_{\mathsf{M}}\lambda_{\mathsf{BR}}\lambda_{\mathsf{RE}}}{\gamma_{\mathsf{M}}\lambda_{\mathsf{RE}} + x\lambda_{\mathsf{RD}}\gamma_{\mathsf{E}}} 2\sqrt{\frac{\lambda_{\mathsf{RD}}(x-1)}{\gamma_{\mathsf{M}}\xi\lambda_{\mathsf{BR}}}} \\
&\times \mathbf{K}_1\left(2\sqrt{\frac{\lambda_{\mathsf{RD}}\lambda_{\mathsf{BR}}\ (x-1)}{\gamma_{\mathsf{M}}\xi}}\right). \qquad \text{(A.4)}
\end{aligned}$$

(A.4) is obtained with the help of [23, Eq. (3.324.1)].

From (A.3) and (A.4) we have (22).

Appendix B
Proof of Lemma 2

From (24), we have $\gamma_{\mathsf{1ORS}}^{\mathsf{MEHS}} = \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{B}_s\mathsf{S}}|^2|h_{\mathsf{SR}_k}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{B}_s\mathsf{S}}|^2|h_{\mathsf{SE}}|^2}$ and $\gamma_{\mathsf{2ORS}}^{\mathsf{MEHS}} = \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{B}_s\mathsf{R}_k}|^2|h_{\mathsf{R}_k\mathsf{D}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{B}_s\mathsf{R}_k}|^2|h_{\mathsf{R}_k\mathsf{E}}|^2}$.

We denote that $Y_o = |h_{\mathsf{B}_s\mathsf{S}}|^2$, and $Z_o = |h_{\mathsf{SE}}|^2$. The CDF of $\gamma_{\mathsf{ORS}}^{\mathsf{MEHS}}$ can be derived as follows:

$$\begin{aligned}
&F_{\gamma_{\mathsf{ORS}}^{\mathsf{MEHS}}}\left(x\right) = \\
&\int_0^\infty\int_0^\infty \left[1-(1-F_{\gamma_{\mathsf{1ORS}}^{\mathsf{MEHS}}|Y_o,Z_o}\left(x\right))(1-F_{\gamma_{\mathsf{2ORS}}^{\mathsf{MEHS}}}\left(x\right))\right]^K \\
&\times f_{Y_o}\left(y\right) f_{Z_o}\left(z\right) dy\ dz. \qquad \text{(B.1)}
\end{aligned}$$

After performing some mathematical manipulations, we achieve (25) with the help of [23, Eq. (3.324.1)].

Appendix C
Proof of Lemma 3

From (20), we have

$$\begin{aligned}
\gamma_{\mathsf{1ORS}}^{\mathsf{MEHR}} &= \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{B}_r\mathsf{S}}|^2|h_{\mathsf{SR}_k}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{B}_r\mathsf{S}}|^2|h_{\mathsf{SE}}|^2}, \\
\gamma_{\mathsf{2ORS}}^{\mathsf{MEHR}} &= \frac{1+\gamma_{\mathsf{M}}\xi|h_{\mathsf{B}_r\mathsf{R}_k}|^2|h_{\mathsf{R}_k\mathsf{D}}|^2}{1+\gamma_{\mathsf{E}}\xi|h_{\mathsf{B}_r\mathsf{R}_k}|^2|h_{\mathsf{R}_k\mathsf{E}}|^2}. \qquad \text{(C.1)}
\end{aligned}$$

We denote that $Z_o = |h_{\mathsf{SE}}|^2$. The CDF of $\gamma_{\mathsf{ORS}}^{\mathsf{MEHR}}$ can be derived as follows:

$$\begin{aligned}
&F_{\gamma_{\mathsf{ORS}}^{\mathsf{MEHS}}}\left(x\right) = \int_0^\infty\int_0^\infty \left[1-(1-F_{\gamma_{\mathsf{1ORS}}^{\mathsf{MEHR}}|Z_o}\left(x\right))(1-F_{\gamma_{\mathsf{2ORS}}^{\mathsf{MEHR}}}\left(x\right))\right]^K \\
&\times f_{Z_o}\left(z\right) dy\ dz. \qquad \text{(C.2)}
\end{aligned}$$

After performing some mathematical manipulations, we obtain (26) with the help of [23, Eq. (3.324.1)].

References

[1] A. Bletsas, H. Shin, and M. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, Sep. 2007.

[2] 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.

[3] Z. Hadzi-Velkov, I. Nikoloska, G. K. Karagiannidis, and T. Q. Duong, "Wireless networks with energy harvesting and power transfer: Joint power and time allocation," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 50–54, Jan. 2016.

[4] Z. Hadzi-Velkov, N. Zlatanov, T. Q. Duong, and R. Schober, "Rate maximization of decode-and-forward relaying systems with RF energy harvesting," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2290–2293, Dec. 2015.

[5] Y. Liu, L. Wang, S. A. Raza Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[6] 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.

[7] 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.

[8] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4788–4799, Sep. 2013.

[9] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[10] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607–1622, May 2015.

[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[12] 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.

[13] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[14] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[15] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5051, Dec. 2015.

[16] L. Fan, N. Yang, T. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multi-user multi-relay networks," *IEEE Trans. Wireless Commun.*, vol. PP, no. 99, pp. 1–1, Feb. 2016.

[17] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.

[18] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[19] J. Zhang, X.-T. Doan, N.-P. Nguyen, and T. Mai, "Secrecy outage probability of energy harvesting relaying system with power beacon," in *Proc. IEEE SigTelCom*, Da Nang, Vietnam, Jan. 2017.

[20] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[21] 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.

[22] 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.

[23] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. San Diego, CA: Academic press, 2007.