IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 4, 2018, accepted October 15, 2018, date of publication October 26, 2018, date of current version November 30, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2878275

Secrecy Analysis of SWIPT-Enabled Cooperative Networks With DF HPTSR Protocol

FESTUS KEHINDE OJO AND MOHD FADZLI MOHD SALLEH, (Member, IEEE)
School of Electrical and Electronic Engineering, Universiti Sains Malaysia, Nibong Tebal 14300, Malaysia

Corresponding author: Mohd Fadzli Mohd Salleh (fadzlisalleh@usm.my)

This work was supported by the Research University Individual (RUI) Grant under grant number 8014051.

ABSTRACT The simultaneous wireless information and power transfer (SWIPT) technology is recently used to sustain the lifetime of energy-constrained relay nodes in wireless cooperative networks. An example to achieve this technology is the hybridized power-time splitting-based relaying (HPTSR) protocol. However, the information security aspect of wireless cooperative networks is important and needs adequate attention. In this paper, we perform the secrecy analysis of a SWIPT-enabled cooperative network with source–relay link-based decode-and-forward HPTSR protocol, which can enhance the operational lifetime of the relay nodes and the secrecy performance of the entire cooperative network. Specifically, we examine the secrecy performance of the considered network by deriving the analytical expressions for the near-optimal power splitting factor, secrecy outage probability, and secure energy efficiency of the system. All analytical results are confirmed by numerical simulations. Our results show that the SWIPT-enabled cooperative network outperforms the conventional relaying scheme-based network presented in literature at relatively high signal-to-noise ratios.

INDEX TERMS Cooperative networks, energy harvesting, hybridized power-time splitting based relaying protocol, secure transmission, SWIPT.

I. INTRODUCTION

Wireless communication networks are prone to eavesdropping due to their broadcasting feature [1]. This condition results in the degradation in secrecy information capacity. The secrecy information capacity is the maximum rate of secret information that can be forwarded from the source to the destination in the presence of one or more eavesdroppers that attempt to overhear the information transmitted between the source and the destination. Cooperative relaying techniques are used to improve the throughput [2], [3] and the physical layer security (PLS) of wireless networks against eavesdroppers by taking the advantage of physical characteristics of wireless channels, such as multipath fading and noise [4]–[8].

Wireless energy harvesting (EH) via radio frequency (RF) signals is recently gaining considerable attention in the academe and industries as a solution to prolong the lifetime of energy-constrained wireless communication nodes because RF signals can convey energy and information simultaneously [9]–[13]. Specifically, the evolution of the wireless energy transmission leads to power sharing in wireless communication and the idea of a new network called EH cooperative networks [14], [15]. For the EH cooperative networks, the cooperative relays can harvest energy from the received RF signals and process information concurrently; this technology is termed the simultaneous wireless information and power transfer (SWIPT) [16], [17]. Unlike the conventional relaying schemes (CRSs) (i.e., without SWIPT at the relays), the harvested energy can be stored in the rechargeable batteries that power the relays and can then be utilized during information transmission between the relays and the destination.

The EH cooperative relay nodes can be used to utilize the physical layer characteristics of wireless channels for supporting a secured transmission from a source to a destination with the existence of one or more eavesdroppers. The EH-enabled relay maintains a constant operation and connection between the source and the destination without the use of external energy sources. In SWIPT communication systems, various resources are used, such as antenna, frequency, time, and power. Practically, the resource allocation in SWIPT plays an important role in performance enhancement. The performance of this resource allocation depends on the channel state information (CSI) at the transmitter. If this resource allocation is properly managed, then

SWIPT-enabled relay systems can achieve higher system capacity than CRS-based systems, thereby improving the PLS of the wireless network [8].

Two different protocols, namely, power splitting relaying (PSR) and time switching relaying (TSR), have been proposed to achieve SWIPT; these protocols are widely adopted in the literature with amplify-and-forward (AF) and decode-and-forward (DF) cooperative schemes [8], [9], [18]–[21]. In the PSR protocol, the receiver splits the received RF signal into two parts by using the power splitting (PS) factor; one is for EH, and the other is for information processing. In the TSR protocol, the receiver switches between EH and information processing on the basis of the time switching (TS) factor. The throughput performance of the two protocols has been investigated in literature. However, the throughput performance of the PSR or TSR protocol is affected by the channel statistics of the CSI [9], which rapidly changes the strength of the received signals. To mitigate this problem, Ojo and Salleh [22] proposed the hybridized power-time splitting-based relaying (HPTSR) protocol based on channel-enabled PS and TS factors. In the HPTSR protocol, the intermediate relay node only harvests energy and then cooperates in transmitting the information from the source to the destination on the basis of the statistics of the CSI acquired. Consequently, maximum capacity of information occurs at the destination.

In [8], the secrecy capacity of a cooperative compressed sensing AF (CCS-AF) wireless communication network in the presence of eavesdroppers based on the PSR protocol was investigated. In this work, the utilized network contains multiple source nodes, multiple relay nodes in the presence of multiple eavesdroppers, and one destination node. The source nodes transmit their information to the relay nodes at the same time, and the relays harvest energy from the received RF signals on the basis of the PSR protocol. The effects of the system parameters, such as energy conversion efficiency, relay location, relay number, and the PS factor, on the secrecy capacity of the system were investigated. The simulation results showed that the proposed CCS-AF relaying scheme achieves better secrecy capacity than the traditional relaying scheme under certain requirements.

In [19], the secrecy capacity of a half-duplex EH-based multi-antenna AF relaying network in the presence of an eavesdropper was studied. After the source transmits in this model, the intended destination sends an artificial noise signal to transfer energy to the relay and to improve the system security. This artificial noise is simply canceled at the intended destination since it has the knowledge of the information unlike the eavesdropper. Salem *et al.* [19] derived the analytical expressions for the ergodic secrecy capacity for TSR-based, PSR-based, and ideal relaying receivers. The simulation results showed that the secrecy capacity performance of the PSR-based receiver is better than that of the TSR-based receiver in the considered network.

In [20], the secrecy outage probability of a cooperative secure network using TSR protocol was examined. The authors defined the secrecy outage probability as the probability that the achievable secrecy rate is less than a given secrecy code rate. Unlike Salem *et al.* [19] that used one intermediate relay node, those in [20] used a relay and a jammer as two intermediate nodes to enhance the desired channel gain and simultaneously interfere with the eavesdropping channel.

In [21], the secrecy rate performance of a wireless cooperative relaying network based on DF and AF PSR protocol was investigated [21]. The network model consists of a source node, a relay node, a destination node, and a power beacon that supplies energy to the relay and the source simultaneously. The source transmits a signal to the destination with the assistance of the relay. The simulation results revealed that the system utilizing PSR protocol is more beneficial than the traditional system in terms of energy efficiency without much deterioration in its secrecy performance.

In [23], a cooperative network comprising a source, multiple DF relays, and a destination in the presence of an active eavesdropper was considered. Unlike the previous works, the eavesdropper was assumed to be part of the communication network. In this work, the closed-form expressions for the secrecy outage probability were derived. The work proposed a proactive relay selection strategy to improve the secrecy outage probability of the considered system by minimizing the eavesdropping capacity. Unfortunately, the relay selection by the proactive eavesdropper is damaging to the system because the system secrecy deteriorates as the number of relay increases. The work in [23] did not apply EH technique at any of the communication nodes.

In [24], a jamming cooperation network model of an AF relaying under PLS in which a source node forwards a secrecy signal to a destination node via an AF relay node was presented. An eavesdropper node attempts to overhear the secrecy signal that is sent from the source to the destination. The authors derived the asymptotic expression for the secrecy outage probability of the achievable secrecy rate of the considered network and proposed two separate-jamming cooperation transmission protocols, namely, source–jammer and destination–jammer. However, the authors did not apply EH technique at any of the communication nodes.

In [25], a cooperative jamming (CJ)-based scheme for secrecy improvement was examined. In particular, an exact transmit model for secrecy rate maximization problem that is subject to the secrecy outage probability constraint was formulated and consequently solved on the basis of asymptotic analysis. The simulation results revealed that the CJ-based design outperforms the design without CJ in terms of secrecy rate and secure energy efficiency. Notably, Hu *et al.* [25] ignored the impact of EH in their considered network.

In [26], outage performance of SWIPT scheme in the threshold AF and DF cooperative relaying techniques was investigated. In this work, the closed-form analytical expressions for outage probability of both relaying techniques were derived without considering the secrecy level of the considered system. In [27], the secrecy outage performance of a two-hop cooperative network comprising a source node, a relay node, and a destination in the presence of an eavesdropper was investigated. In this work, the system secrecy outage performance was improved by the introduction of the proposed source–relay ($S-R$) link-based threshold DF relaying strategy, in which the relay was activated on the basis of the instantaneous signal-to-noise ratio (SNR) of the received signal across $S-R$ link. The numerical results showed that the proposed strategy outperforms the traditional DF scheme. However, the authors ignored SWIPT at the relay node. As a result, the relay node exhibits limited time of operation due to energy constraint.

The SWIPT technique can allocate energy in an efficient way due to the capability of energy and information transfer exhibited by the RF signals. To the best of our knowledge, the impact of the SWIPT technique on the secrecy performance has not been well investigated for the cooperative networks because some of the existing works (i.e., [23]–[25], [27]) focus on the CRS without SWIPT at the relay but with either the relay node equipped with a non-rechargeable battery or a non-battery relay node. Therefore, the security level of such networks is threatened by the presence of the eavesdropper(s) due to energy constraint at the relay. Motivated by the work in [27], we analyze a secure SWIPT-enabled cooperative network with $S-R$ link-based DF HPTSR protocol to enhance the secrecy outage performance and secure energy efficiency of the considered cooperative network.

Unlike in [27], the relay node harvests energy from the received RF signals and then stores the energy in a rechargeable battery for future transmission (i.e., relay–destination transmission), thereby prolonging the operational lifetime of the relay node. Unlike in [8] and [19] that considered the PS and TS parameters separately and in [22] that used the HPTSR protocol combining the PS and TS parameters, we determine the analytical expressions for the optimal PS factor in terms of the TS factor, secrecy outage probability, and secure energy efficiency of the considered SWIPT-enabled cooperative network. Our numerical results reveal that the SWIPT-enabled cooperative network outperforms the CRS-based cooperative network presented in [27] in terms of secrecy outage probability and secure energy efficiency.

The main contributions of this study are summarized as follows:

- We analyze a secure SWIPT-enabled cooperative network with $S-R$ link-based DF HPTSR protocol, which can enhance the operational lifetime of a relay node and the secrecy performance.
- We examine the secrecy performance of the considered SWIPT-enabled cooperative network with $S-R$ link-based DF HPTSR protocol by deriving the analytical expressions for the optimal PS factor in terms of the TS factor, secrecy outage probability, and secure energy efficiency. As a result, an interesting double-objective model in the field of EH for a secure transmission is obtainted. This model can offer a trade-off between secrecy outage and energy consumed unlike those in the previous works that either focus on secrecy outage probability or secrecy capacity alone.
- Our numerical results show that the SWIPT-enabled cooperative network with $S-R$ link-based DF HPTSR protocol outperforms the CRS-based cooperative network reported in [27] in terms of secrecy performance at relatively high SNRs.

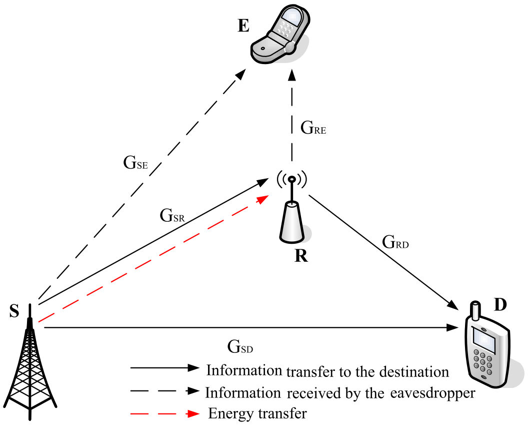
E
GSE
GRE
GSR
R
GRD
S
D
GSD
Information transfer to the destination
Information received by the eavesdropper
Energy transfer

FIGURE 1. Secure SWIPT-enabled cooperative network.

The rest of the paper is organized as follows. Section II describes the system model. Section III presents the analysis of the secrecy performance of the SWIPT-enabled cooperative network with $S-R$ link-based DF HPTSR protocol. Section IV provides the numerical results. Finally, Section V elaborates the conclusions.

II. SYSTEM MODEL

In this paper, we consider a secure SWIPT-enabled cooperative network as shown in Fig. 1. This network comprises a source S, an EH-enabled relay R, a destination D, and an eavesdropper E, which makes effort to overhear the personal message sent by the source S and the re-transmitted message by the relay R. The harvested energy by the relay R can be saved in a rechargeable battery to be used for information transmission on $R-D$ link. We assumed that all links in the considered network experience independent and identically distributed (iid) Rayleigh fading. Also, it is assumed that each communication node is supplied with a single antenna and operates in the half-duplex transmission mode.

Moreover, we consider the $S-R$ link based DF HPTSR communication protocol for allocating the system resource. The transmission process takes two time slots. In the first time slot, S sends the information to R and D but E attempts to overhear it. Then, R harvests energy from the RF signal sent by S and simultaneously decodes the information sent via the $S-R$ link. In the second time slot, if R decodes the information bits successfully, R will help forwarding the decoded information bits to D. In this case, two versions of the transmitted signal are avialable at both D and E. If R fails to decode the received information, it will not

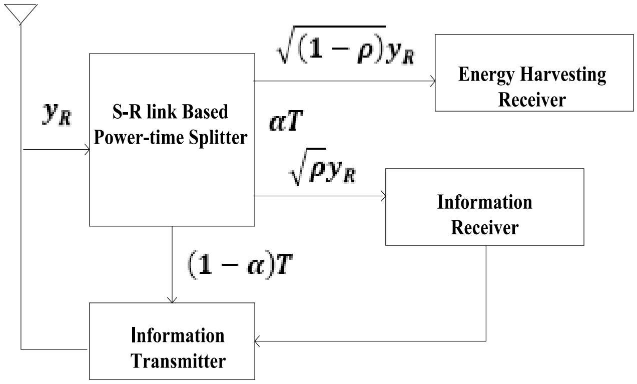

FIGURE 2. The architecture of the relay receiver for the $S-R$ link based DF HPTSR protocol.

assist in forwarding any information to D. In this model, it is assumed that the main commucation channels are always better than the eavesdropping channels [27]. To reduce the complexity of our analysis, we adopt the selection combining (SC) technique [28] at both D and E. Specifically, each of the information receivers will select one of the received signals from either S or R respectively.

The architecture of the relay receiver for the $S-R$ link based DF HPTSR protocol is as shown in Fig. 2. The received signal at R is represented by y_R, and the fraction of time used for energy harvesting and information reception on the $S-R$ link in the first time slot is αT; where α with $0 < \alpha < 1$ represents the time switching factor. The transmission block time is represented by T. Also, ρ with $0 < \rho < 1$, represents the power splitting factor for the DF HPTSR protocol. The $S-R$ link based power-time splitter divides the power of the received signal at R into $\rho : (1-\rho)$ proportion. The portion of the received signal power sent to the information receiver is ρP_S and the remaining received signal power at the EH receiver is $(1-\rho) P_S$, where P_S is the transmitted power from the source. In the second time slot, R uses the remaining block time $(1-\alpha) T$ and the energy harvested during the first time slot for information transmission over the $R-D$ link [22].

Furthermore, the EH-enabled relay R is activated base on the instantaneous SNR of the received signal across $S-R$ link. It means that the operation of R is solely based on a pre-set threshold SNR (γ_o). If the received SNR is greater than γ_o, the probability of an error at R is invariably small. Then, R will re-transmit the decoded signal to D. If the received SNR is smaller than γ_o, then R will remain inactive. In this paper, d_{ij} represents the distance between nodes i and j, where $i, j \in \{S, R, D, E\}$. Also, $\varepsilon\{.\}$ and $|.|$ represent the expectation and absolute value operations, respectively.

III. SECRECY PERFORMANCE ANALYSIS OF THE SWIPT-ENABLED COOPERATIVE NETWORK

In this section, we present the analysis of the secrecy performance of the SWIPT-enabled cooperative network with $S-R$ link based DF HPTSR protocol by characterizing it into two phases, namely, secrecy outage probability and secure energy efficiency.

A. SECRECY OUTAGE PROBABILITY PERFORMANCE ANALYSIS

In order to analyze the secrecy outage probability P_{SOP} performance of the SWIPT-enabled cooperative network with $S-R$ link based DF HPTSR protocol, we first characterize the optimal channel capacity or the equivalent SNR of the considered communication protocol. In the first phase of the signal transmission, the received signals at D and E are expressed as

$$y_D^1 = \sqrt{\frac{P_S}{d_{SD}^{\beta}}} G_{SD} x_t + n_D, \tag{1a}$$

$$y_E^1 = \sqrt{\frac{P_S}{d_{SE}^{\beta}}} G_{SE} x_t + n_E, \tag{1b}$$

respectively, where P_S is the transmitted power from S, x_t is the normalized transmitted signal from S, i.e. $\varepsilon\left\{|x_t|^2\right\} = 1$, β is the path loss exponent. The small-scale fading coefficients for $S-D$ and $S-E$ links are G_{SD} and G_{SE} respectively. The parameters n_D and n_E represent the zero mean additive white Gaussian noise (AWGN) at D and E, respectively.

Since R is EH-enabled with DF HPTSR protocol, the received signal y_{R-EH} at the input of the EH receiver in the first phase of transmission is given by

$$y_{R-EH} = \sqrt{\frac{(1-\rho) P_S}{d_{SR}^{\beta}}} G_{SR} x_t + n_{SR}, \tag{2}$$

where G_{SR} is the small-scale fading coefficient for $S-R$ link and n_{SR} is the zero mean AWGN at R. Therefore, the amount of harvested energy E_R during the harvesting time, αT can be obtained as

$$E_R = \eta \alpha T (1-\rho) \frac{P_S |G_{SR}|^2}{d_{SR}^{\beta}}, \tag{3}$$

where η with $0 < \eta < 1$ is the energy conversion efficiency, which depends on the rectification process [9].

After power splitting and down conversion of the RF signal to baseband signal, the received signal y_{R-I} at the input of the R information receiver can be expressed as

$$y_{R-I} = \sqrt{\frac{\rho P_S}{d_{SR}^{\beta}}} G_{SR} x_t + n_R, \tag{4}$$

where $n_R = \sqrt{\rho} n_{SR} + n_{RC}$, and n_{RC} is the sampled AWGN as a result of RF band to baseband signal conversion [9], [29]. For simplicity, we assume that all the AWGNs in this analysis have equal variances, σ_o^2. Consequently, the channel capacity of the $S-R$ link, C_{SR} can be expressed as

$$C_{SR} = \frac{(1-\alpha)}{2} \log_2\left(1 + \frac{\rho P_S |G_{SR}|^2}{d_{SR}^{\beta} \sigma_o^2}\right), \tag{5}$$

Now, the SNR of the received signal at E, R, and D can be given as

$$\gamma_{SE} = \frac{P_S\,|G_{SE}|^2}{d_{SE}^{\beta}\sigma_o^2}, \tag{6a}$$

$$\gamma_{SR} = \frac{\rho P_S\,|G_{SR}|^2}{d_{SR}^{\beta}\sigma_o^2}, \tag{6b}$$

$$\gamma_{SD} = \frac{P_S\,|G_{SD}|^2}{d_{SD}^{\beta}\sigma_o^2}, \tag{6c}$$

respectively.

In the second phase of the transmission, if R successfully decodes the transmitted signal x_t, it will forward the re-encoded signal $\overline{x_t}$ to D. The received signals at E and D are given by

$$y_E^2 = \sqrt{\frac{P_R}{d_{RE}^{\beta}}}\,G_{RE}\overline{x_t} + n_E, \tag{7a}$$

$$y_D^2 = \sqrt{\frac{P_R}{d_{RD}^{\beta}}}\,G_{RD}\overline{x_t} + n_D, \tag{7b}$$

respectively, where P_R is the transmission power of R which depends on the harvested energy in (3), G_{RE} and G_{RD} represent the small-scale fading coefficients for $R-E$ and $R-D$ links, respectively. Thus, P_R is given by

$$P_R = \frac{E_R}{(1-\alpha)\,T}, \tag{8}$$

Substituting (3) into (8), then P_R can be re-written as

$$P_R = \left(\frac{\eta\alpha\,(1-\rho)}{1-\alpha}\right)\frac{P_S\,|G_{SR}|^2}{d_{SR}^{\beta}}, \tag{9}$$

Similarly, the channel capacity of the $R-D$ link, C_{RD} can be written as

$$\begin{aligned} C_{RD} &= \frac{(1-\alpha)}{2}\log_2\left(1+\frac{P_R\,|G_{RD}|^2}{d_{RD}^{\beta}\sigma_o^2}\right), \\ &= \frac{(1-\alpha)}{2}\log_2\left(1+\left(\frac{\eta\alpha\,(1-\rho)}{1-\alpha}\right)\frac{P_S\,|G_{SR}|^2\,|G_{RD}|^2}{d_{SR}^{\beta}d_{RD}^{\beta}\sigma_o^2}\right), \end{aligned} \tag{10}$$

Next, we express the SNR of the received signals at E and D as

$$\gamma_{RE} = \frac{P_R\,|G_{RE}|^2}{d_{RE}^{\beta}\sigma_o^2} = \left(\frac{\eta\alpha\,(1-\rho)}{1-\alpha}\right)\frac{P_S\,\left|G_{RE_1}\right|^2}{d_{SR}^{\beta}d_{RE}^{\beta}\sigma_o^2}, \tag{11a}$$

$$\gamma_{RD} = \frac{P_R\,|G_{RD}|^2}{d_{RD}^{\beta}\sigma_o^2} = \left(\frac{\eta\alpha\,(1-\rho)}{1-\alpha}\right)\frac{P_S\,\left|G_{RD_1}\right|^2}{d_{SR}^{\beta}d_{RD}^{\beta}\sigma_o^2}, \tag{11b}$$

respectively, where $\left|G_{RE_1}\right|^2 = |G_{SR}|^2\,|G_{RE}|^2$ and $\left|G_{RD_1}\right|^2 = |G_{SR}|^2\,|G_{RD}|^2$.

For the near-optimal transmission on the $S-R-D$ link, we examine the $S-R$ link based DF HPTSR power allocation that maximizes the channel capacity or the equivalent SNR of the $S-R-D$ link. Thus, the end-to-end SNR of $S-R-D$ link γ_{SRD}, under the considered protocol can be expressed as

$$\gamma_{SRD} = \max_{\alpha,\,\rho}\left(\min\left(\gamma_{SR},\ \gamma_{RD}\right)\right), \tag{12}$$

The solution to this design must yield an approximate or equal SNR for both $S-R$ and $R-D$ links [30], [31]. Thus, the near-optimal solution is written as

$$\gamma_{SR} \approx \gamma_{RD}, \tag{13}$$

Substituting (6b) and (11b) into (13), we can obtain either the near-optimal value of α or ρ by fixing the other. Therefore, by fixing α, the near-optimal ρ^* can be expressed as

$$\begin{aligned} \rho^* &= \frac{\eta\alpha\,|G_{RD}|^2}{d_{RD}^{\beta}\,(1-\alpha)+\eta\alpha\,|G_{RD}|^2}, \\ &= \frac{1}{\left[\frac{d_{RD}^{\beta}(1-\alpha)}{\eta\alpha|G_{RD}|^2}\right]+1}, \end{aligned} \tag{14}$$

It follows that $\left[\frac{d_{RD}^{\beta}(1-\alpha)}{\eta\alpha|G_{RD}|^2}\right] > 0$. Therefore, it can be verified that the analytical expression for ρ^* in (14) satisfies $0 < \rho^* < 1$. Furthermore, we can see that ρ^* depends on the time switching factor α and the distance d_{RD}.

Since all the channels experience Rayleigh fading, the probability density function (PDF) of $|\chi|^2$ can be modeled as

$$f_{|\chi|^2}(\theta) = \frac{1}{\chi}\exp\left(\frac{-\theta}{\chi}\right), \tag{15}$$

where $\chi \in \{G_{SE},\ G_{SD},\ G_{SR},\ G_{RE},\ G_{RD}\}$, which is defined as $\varepsilon\left\{|\chi|^2\right\}$.

Likewise, γ_{SE}, γ_{SR}, γ_{SD}, γ_{RE}, and γ_{RD} are exponentially distributed with parameters δ_{SE}, δ_{SR}, δ_{SD}, δ_{RE}, and δ_{RD}, respectively, where

$$\delta_{SE} = \frac{d_{SE}^{\beta}\sigma_o^2}{P_S}, \tag{16a}$$

$$\delta_{SR} = \frac{d_{SR}^{\beta}\sigma_o^2}{P_S}, \tag{16b}$$

$$\delta_{SD} = \frac{d_{SD}^{\beta}\sigma_o^2}{P_S}, \tag{16c}$$

$$\delta_{RE} = \frac{d_{SR}^{\beta}d_{RE}^{\beta}\sigma_o^2}{\left(\frac{\eta\alpha(1-\rho)}{1-\alpha}\right)P_S}, \tag{16d}$$

$$\delta_{RD} = \frac{d_{SR}^{\beta}d_{RD}^{\beta}\sigma_o^2}{\left(\frac{\eta\alpha(1-\rho)}{1-\alpha}\right)P_S}, \tag{16e}$$

Also, the cumulative distribution function (CDF) of γ_{SRD}, can be written as

$$F_{\gamma_{SRD}}(x) = 1-\exp\left(-\delta_{SRD}x\right), \tag{17}$$

where $\delta_{SRD} = \delta_{SR} + \delta_{RD}$. By adopting the SC technique, the received SNR at E and D can be expressed as

$$\gamma_{E_{SC}} = \begin{cases} \gamma_{SE}, & \text{if } \gamma_{SR} \leq \gamma_o \\ \max\left(\gamma_{SE}, \gamma_{RE}\right), & \text{else}, \end{cases} \tag{18}$$

$$\gamma_{D_{SC}} = \begin{cases} \gamma_{SD}, & \text{if } \gamma_{SR} \leq \gamma_o \\ \max\left(\gamma_{SD}, \gamma_{SRD}\right), & \text{else}, \end{cases} \tag{19}$$

respectively.

To determine the secrecy level of the considered communication network, the instantaneous secrecy capacity of the network C_{HPTSR} is defined as the maximum difference between the mutual information of the main communication channel and the eavesdropper channel [8], [27], [32], which could be written as

$$C_{HPTSR} = \begin{cases} \left(C_M - C_E\right), & \text{if } \gamma_{D_{SC}} > \gamma_{E_{SC}} \\ 0, & \text{else}, \end{cases} \tag{20a}$$

where C_M is the instantaneous capacity of the main communication channel and C_E is the instantaneous capacity of the eavesdropper channel.

If $\gamma_{SR} \leq \gamma_o$, then we have

$$C_{HPTSR} = \begin{cases} \left[\log_2\left(1+\gamma_{SD}\right) - \log_2\left(1+\gamma_{SE}\right)\right], & \text{if } \gamma_{SE} \leq \gamma_{SD} \\ 0, & \text{else} \end{cases} \tag{20b}$$

If $\gamma_{SR} \geq \gamma_o$, then C_{HPTSR} can be expressed as

$$C_{HPTSR} = \begin{cases} \dfrac{(1-\alpha)}{2}\left[\Delta_1 - \Delta_2\right], & \text{if } \gamma_{E_{SC}} \leq \gamma_{D_{SC}} \\ 0, & \text{else}, \end{cases} \tag{20c}$$

where

$$\begin{aligned} \Delta_1 &= \log_2\left(1 + \max\left(\gamma_{SD}, \gamma_{SRD}\right)\right), \\ \Delta_2 &= \log_2\left(1 + \max\left(\gamma_{SE}, \gamma_{RE}\right)\right), \\ \gamma_{D_{SC}} &= \max\left(\gamma_{SD}, \gamma_{SRD}\right), \quad \text{and} \\ \gamma_{E_{SC}} &= \max\left(\gamma_{SE}, \gamma_{RE}\right). \end{aligned}$$

Thus, the secrecy outage probability P_{SOP}, using $S-R$ link based DF HPTSR protocol for the considered network with the threshold capacity C_o can be written as

$$\begin{aligned} P_{SOP}\left(C_o\right) = {} & P_r\left(\gamma_{SR} \leq \gamma_o\right) P_r\left(C_{HPTSR} \leq C_o | \gamma_{SR} \leq \gamma_o\right) \\ & + P_r\left(\gamma_{SR} > \gamma_o\right) P_r\left(C_{HPTSR} \leq C_o | \gamma_{SR} > \gamma_o\right) \end{aligned} \tag{21}$$

where $P_r(\nabla)$ denotes the probability that the event ∇ occurs.

Next, we derive the analytical expression of P_{SOP} for the considered network as follows. Considering the $S-R$ link based DF HPTSR protocol, the probability that γ_{SR} is below the pre-set threshold γ_o can be expressed as

$$\begin{aligned} P_r\left(\gamma_{SR} \leq \gamma_o\right) &= \int_0^{\gamma_o} \delta_{SR} \exp\left(-\delta_{SR} x\right) dx \\ &= 1 - \exp\left(-\delta_{SR}\gamma_o\right), \end{aligned} \tag{22}$$

Consequently, the probability that γ_{SR} is greater than the pre-set threshold γ_o can be given as

$$\begin{aligned} P_r\left(\gamma_{SR} \geq \gamma_o\right) &= 1 - \int_0^{\gamma_o} \delta_{SR} \exp\left(-\delta_{SR} x\right) dx \\ &= \exp\left(-\delta_{SR}\gamma_o\right), \end{aligned} \tag{23}$$

Also, the conditional probability that the instantaneous secrecy capacity of the considered network C_{HPTSR} is below C_o when $\gamma_{SR} \leq \gamma_o$ can be given as

$$\begin{aligned} & P_r\left(C_{HPTSR} \leq C_o | \gamma_{SR} \leq \gamma_o\right) \\ &\quad = P_r\left(C_{HPTSR} \leq C_o\right) \\ &\quad = P_r\left(\left\{\log_2\left(1+\gamma_{SD}\right) - \log_2\left(1+\gamma_{SE}\right)\right\} \leq C_o\right) \\ &\quad = P_r\left(\log_2\left(\frac{1+\gamma_{SD}}{1+\gamma_{SE}}\right) \leq C_o\right) \\ &\quad = P_r\left(\left(\frac{1+\gamma_{SD}}{1+\gamma_{SE}}\right) \leq 2^{C_o}\right) \\ &\quad = P_r\left(\gamma_{SD} \leq \gamma_{SE}2^{C_o} + 2^{C_o} - 1\right) \\ &\quad = \Delta_3 \int_0^{\gamma_{SE}2^{C_o}+2^{C_o}-1} \delta_{SD} \exp\left(-\delta_{SD}\gamma_{SD}\right) d\gamma_{SD} \\ &\quad = 1 - \left(\frac{\delta_{SE}\exp\left(-\delta_{SD}\left(2^{C_o}-1\right)\right)}{\delta_{SE} + \delta_{SD}2^{C_o}}\right), \end{aligned} \tag{24}$$

where $\Delta_3 = \int_0^{\infty} \delta_{SE} \exp\left(-\delta_{SE}\gamma_{SE}\right) d\gamma_{SE}$.

When $\gamma_{SR} > \gamma_o$, we can obtain the probability that the instantaneous secrecy capacity C_{HPTSR} falls below C_o as

$$\begin{aligned} & P_r\left(C_{HPTSR} \leq C_o | \gamma_{SR} \geq \gamma_o\right) \\ &\quad = P_r\left(\frac{(1-\alpha)}{2}\left[\log_2\left(1+\gamma_{D_{SC}}\right) - \log_2\left(1+\gamma_{E_{SC}}\right)\right]\right) \\ &\quad = P_r\left(\left(\frac{1+\gamma_{D_{SC}}}{1+\gamma_{E_{SC}}}\right) \leq 2^{\left(\frac{2C_o}{1-\alpha}\right)}\right) \\ &\quad = P_r\left(\gamma_{D_{SC}} \leq \gamma_{E_{SC}}\delta_o + \delta_o - 1\right) \\ &\quad = \int_0^{\infty} f_{\gamma_{E_{SC}}}\left(\gamma_{E_{SC}}\right) \int_0^{\gamma_{E_{SC}}\delta_o+\delta_o-1} f_{\gamma_{D_{SC}}}\left(\gamma_{D_{SC}}\right) d\gamma_{D_{SC}} d\gamma_{E_{SC}} \\ &\quad = \int_0^{\infty} f_{\gamma_{E_{SC}}}\left(\gamma_{E_{SC}}\right) F_{\gamma_{D_{SC}}}\left(\gamma_{E_{SC}}\delta_o + \delta_o - 1\right) d\gamma_{E_{SC}}, \end{aligned} \tag{25}$$

Where $\delta_o = 2^{\left(\frac{2C_o}{1-\alpha}\right)}$, $f_{\gamma_{E_{SC}}}(x)$ and $f_{\gamma_{D_{SC}}}(x)$ are the PDF of $\gamma_{E_{SC}}$ and $\gamma_{D_{SC}}$, respectively, and $F_{\gamma_{D_{SC}}}(x)$ is the CDF of $\gamma_{D_{SC}}$.

Given $\gamma_{D_{SC}} = \max\left(\gamma_{SD}, \gamma_{SRD}\right)$ and $\gamma_{E_{SC}} = \max(\gamma_{SE}, \gamma_{RE})$, we can write $f_{\gamma_{E_{SC}}}(x)$ and $F_{\gamma_{D_{SC}}}(x)$ as

$$\begin{aligned} f_{\gamma_{E_{SC}}}(x) = {} & \delta_{SE}\exp\left(-\delta_{SE}x\right)\left\{1 - \exp\left(-\delta_{RE}x\right)\right\} \\ & + \delta_{RE}\exp\left(-\delta_{RE}x\right)\left\{1 - \exp\left(-\delta_{SE}x\right)\right\}, \end{aligned} \tag{26}$$

$$F_{\gamma_{D_{SC}}}(x) = \left(1 - \exp\left(-\delta_{SD}x\right)\right)\left(1 - \exp\left(-\delta_{SRD}x\right)\right), \tag{27}$$

By putting (26) and (27) into (25), $P_r\left(C_{HPTSR} \le C_o | \gamma_{SR} \ge \gamma_o\right)$ can be expressed as

$$\begin{aligned} &P_r\left(C_{HPTSR} \le C_o | \gamma_{SR} \ge \gamma_o\right) \\ &= \int_0^\infty \delta_{SE} \exp\left(-\delta_{SE}\gamma_{E_{SC}}\right)\left[1-\exp\left(-\delta_{RE}\gamma_{E_{SC}}\right)\right] \\ &\quad \times \left[1-\exp\left(-\delta_{SD}\left(\gamma_{E_{SC}}\delta_o+\delta_o-1\right)\right)\right] \\ &\quad \times \left[1-\exp\left(-\delta_{SRD}\left(\gamma_{E_{SC}}\delta_o+\delta_o-1\right)\right)\right] d\gamma_{E_{SC}} \\ &\quad + \int_0^\infty \delta_{RE} \exp\left(-\delta_{RE}\gamma_{E_{SC}}\right)\left[1-\exp\left(-\delta_{SE}\gamma_{E_{SC}}\right)\right] \\ &\quad \times \left[1-\exp\left(-\delta_{SD}\left(\gamma_{E_{SC}}\delta_o+\delta_o-1\right)\right)\right] \\ &\quad \times \left[1-\exp\left(-\delta_{SRD}\left(\gamma_{E_{SC}}\delta_o+\delta_o-1\right)\right)\right] d\gamma_{E_{SC}}, \end{aligned} \tag{28}$$

Finally, we use (15) given in [27] to obtain $P_r(C_{HPTSR} \le C_o|\gamma_{SR} \ge \gamma_o)$ as

$$\begin{aligned} &P_r\left(C_{HPTSR} \le C_o | \gamma_{SR} \ge \gamma_o\right) \\ &= 1 - \left[\frac{\delta_{SE}}{\delta_{SE}+\delta_{SD}\delta_o} + \frac{\delta_{RE}}{\delta_{RE}+\delta_{SD}\delta_o}\right]\exp\left(\delta_{SD}\left(1-\delta_o\right)\right) \\ &\quad + \left[\frac{\delta_{SE}+\delta_{RE}}{\delta_{SE}+\delta_{RE}+\delta_{SD}\delta_o}\right]\exp\left(\delta_{SD}\left(1-\delta_o\right)\right) \\ &\quad - \left[\frac{\delta_{SE}}{\delta_{SE}+\delta_{SRD}\delta_o} + \frac{\delta_{RE}}{\delta_{RE}+\delta_{SRD}\delta_o}\right]\exp\left(\delta_{SRD}\left(1-\delta_o\right)\right) \\ &\quad + \left[\frac{\delta_{SE}+\delta_{RE}}{\delta_{SE}+\delta_{RE}+\delta_{SRD}\delta_o}\right]\exp\left(\delta_{SRD}\left(1-\delta_o\right)\right) \\ &\quad - \left[\frac{\delta_{SE}+\delta_{RE}}{\delta_{SE}+\delta_{RE}+\left(\delta_{SD}+\delta_{SRD}\right)\delta_o}\right]\exp((\delta_{SD}+\delta_{SRD})(1-\delta_o)) \\ &\quad + \left[\frac{\delta_{SE}}{\delta_{SE}+\left(\delta_{SD}+\delta_{SRD}\right)\delta_o} + \frac{\delta_{RE}}{\delta_{RE}+\left(\delta_{SD}+\delta_{SRD}\right)\delta_o}\right] \\ &\quad \times \exp\left(\left(\delta_{SD}+\delta_{SRD}\right)\left(1-\delta_o\right)\right), \end{aligned} \tag{29}$$

By substituting (22), (23), (24) and (29) into (21), the analytical expression of P_{SOP} for the considered network can be obtained as

$$P_{SOP} = a_1 + \left\{a_2 + a_3 - a_4 + a_5 - a_6 + a_7 a_8\right\} a_9, \tag{30}$$

where

$$a_1 = \left[1-\exp\left(-\delta_{SR}\gamma_o\right)\right]\left[1-\left(\frac{\delta_{SE}\exp\left(-\delta_{SD}\left(2^{C_o}-1\right)\right)}{\delta_{SE}+\delta_{SD}2^{C_o}}\right)\right]$$

$$a_2 = 1 - \left[\frac{\delta_{SE}}{\delta_{SE}+\delta_{SD}\delta_o} + \frac{\delta_{RE}}{\delta_{RE}+\delta_{SD}\delta_o}\right]\exp\left(\delta_{SD}\left(1-\delta_o\right)\right),$$

$$a_3 = \left[\frac{\delta_{SE}+\delta_{RE}}{\delta_{SE}+\delta_{RE}+\delta_{SD}\delta_o}\right]\exp\left(\delta_{SD}\left(1-\delta_o\right)\right),$$

$$a_4 = \left[\frac{\delta_{SE}}{\delta_{SE}+\delta_{SRD}\delta_o} + \frac{\delta_{RE}}{\delta_{RE}+\delta_{SRD}\delta_o}\right]\exp\left(\delta_{SRD}\left(1-\delta_o\right)\right),$$

$$a_5 = \left[\frac{\delta_{SE}+\delta_{RE}}{\delta_{SE}+\delta_{RE}+\delta_{SRD}\delta_o}\right]\exp\left(\delta_{SRD}\left(1-\delta_o\right)\right),$$

$$a_6 = \left[\frac{\delta_{SE}+\delta_{RE}}{\delta_{SE}+\delta_{RE}+\left(\delta_{SD}+\delta_{SRD}\right)\delta_o}\right]\exp((\delta_{SD}+\delta_{SRD})\left(1-\delta_o\right))$$

$$a_7 = \left[\frac{\delta_{SE}}{\delta_{SE}+\left(\delta_{SD}+\delta_{SRD}\right)\delta_o} + \frac{\delta_{RE}}{\delta_{RE}+\left(\delta_{SD}+\delta_{SRD}\right)\delta_o}\right]$$

$$a_8 = \exp\left(\left(\delta_{SD}+\delta_{SRD}\right)\left(1-\delta_o\right)\right), \quad \text{and}$$

$$a_9 = \exp\left(-\delta_{SR}\gamma_o\right).$$

B. SECURE ENERGY EFFICIENCY PERFORMANCE ANALYSIS

In order to gain insight into the secure energy efficiency performance of the considered network, we focus on the cooperative transmission by assuming that the direct link between S and D is in deep fading. Now, we define secure energy efficiency as the ratio of the system channel capacity to the total energy consumed in one transmission block time [33], [34]. In the HPTSR protocol, network nodes are activated based on the assigned time slot as shown in Fig. 2. The source node S is activated during the first time slot of energy transfer and information delivery to the relay. The relay node R and the eavesdropper node E are in operation for the entire transmission block while the destination D operates when receiving the information forwarded by R. We assume that each node has a constant circuit power consumption for signal processing, which is different from the power used for transmitting signal. Therefore, the total energy consumption with the DF HPTSR protocol in the considered cooperative network is written as

$$E_T^C = \left(\alpha P_x + P_y + (1-\alpha) P_z + P_e + \alpha P_S\right) T, \tag{31}$$

where P_x, P_y, P_z, and P_e represent the consumed circuit power at S, R, D, and E, respectively.

Then, the instantaneous system channel capacity C_S^{SRD} of the considered cooperative network can be expressed as

$$C_S^{SRD} = \begin{cases} \dfrac{(1-\alpha)}{2}\left[\Delta_3 - \Delta_4\right], & if\ \gamma_{E_{SC}} \le \gamma_{SRD} \\ 0, & else, \end{cases} \tag{32}$$

where $\Delta_3 = \log_2\left(1+\gamma_{SRD}\right)$, $\Delta_4 = \log_2\left(1+\gamma_{E_{SC}}\right)$, $\gamma_{SRD} = \max\left(\gamma_{SR}, \gamma_{RD}\right)$, and $\gamma_{E_{SC}} = \max\left(\gamma_{SE}, \gamma_{RE}\right)$.

Finally, the secure energy efficiency ϕ_{EE} of the system is given as

$$\phi_{EE} = \frac{C_S^{SRD}}{E_T^C}, \tag{33}$$

IV. NUMERICAL RESULTS

This section presents the numerical results of the secrecy performance analysis for the SWIPT-enabled cooperative network. In the simulations, we set the transmit power at the source $P_S = 10$ dB, the threshold capacity $C_o = 3$ dB, the minimum acceptable SNR $\gamma_o = 0.5$ dB, the noise variance $\sigma_o^2 = -20$ dB, the path loss exponent $\beta = 2.7$ as presented in [9], and the energy harvesting efficiency $\eta = 0.9$. The simplified model of the SWIPT-enabled cooperative network is shown in Fig. 3.

The distance between S and D is normalized to a unit value and the coordinates of each node on the $X - Y$ plane are

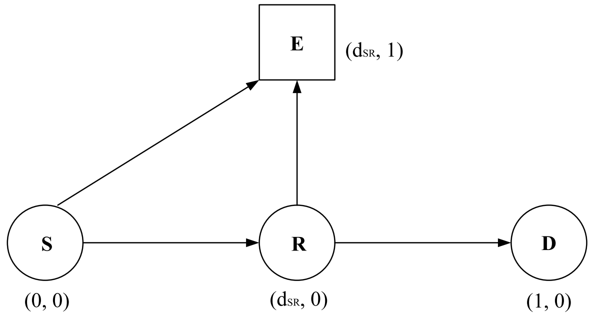

FIGURE 3. Simplified model of the SWIPT-enabled cooperative network.

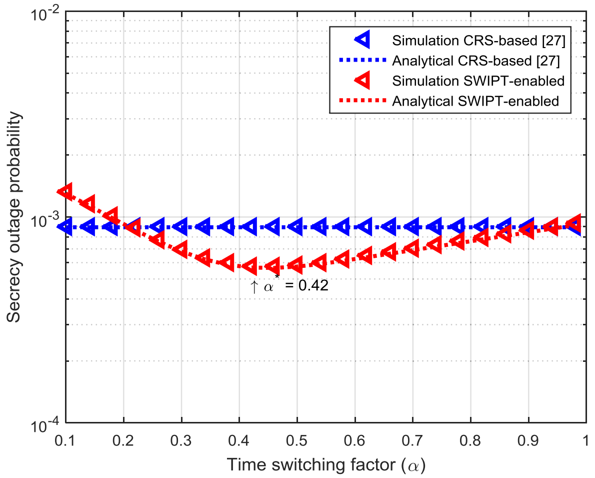

FIGURE 4. Secrecy outage probability against time switching factor (α).

indicated so as to demonstrate the effect of the relay's position on the system secrecy performance. Simulation results for secrecy outage probability depend on the expression given in (21) which is evaluated by averaging the expression over 10^6 random realizations of the Rayleigh fading channels.

In order to show the effectiveness of our analysis, we present the secrecy outage probability performance against time switching factor (α) as shown in Fig. 4 by setting $d_{SR} = 0.3$. For the purpose of comparison, we plot the performance of the CRS-based network as investigated in [27] under the same simulation conditions by setting $P_R = 10$ dB.

As observed in Fig. 4, simulation results show that for smaller values of α, the CRS-based network outperforms the SWIPT-enabled cooperative network with $S - R$ link based DF HPTSR protocol in terms of the secrecy outage probability. The reason is that at smaller values of α, the time expended on EH is not adequate for the relay R to harvest the required energy for transmission and finally resulting in high probability of error at R. However, it is clearly seen that the secrecy outage probability performance of the CRS-based cooperative network remains constant since it does not depend on the time switching factor α. By contrast, the secrecy outage probability performance of the SWIPT-enabled cooperative network with $S - R$ link based DF HPTSR protocol improves as α increases from 0.1 to 0.42; but later, the secrecy outage probability performance deteriorates as α increases beyond 0.42. By inspection, the near-optimal time switching value, α^* is 0.42.

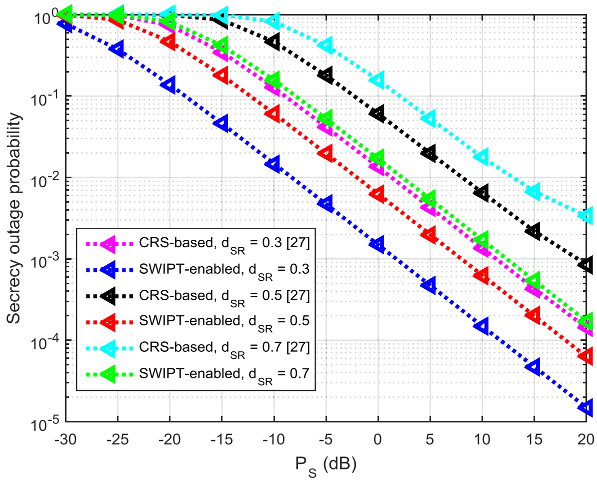

FIGURE 5. Secrecy outage probability against transmitted power at the source P_S for different values of d_{SR}.

The practical interpretation of this result is that any value of α smaller than α^* means lesser time would be expended for EH and more time for information transfer and thus the secrecy outage probability performance actually reduces. Conversely, when the value of α is greater than α^*, it means that more time is wasted on EH but lesser time for information transfer. Therefore, the secrecy outage probability of the system increases. At the near-optimal time switching factor α^*, it is evident from Fig. 4 that the SWIPT-enabled cooperative network significantly outperforms the CRS-based cooperative network in terms of secrecy outage probability. Furthermore, the results obtained using the analytical expressions developed in this paper match the simulation results, which establishes the correctness of our analysis.

The plot of secrecy outage probability performance against transmitted power at the source P_S with different values of d_{SR} is presented in Fig. 5. As previously illustrated, we set the near-optimal time switching factor $\alpha^* = 0.42$.

It is observed that the secrecy outage probability of both the CRS-based and the SWIPT-enabled cooperative networks is improved when P_S increases and d_{SR} decreases. A larger d_{SR} represents a higher path loss on the $S-R$ link which is an advantage for eavesdropping on the $S-E$ link and a threat to the network security. At all values of P_S, the SWIPT-enabled cooperative network outperforms the CRS-based cooperative network. Specifically, at larger P_S the SWIPT-enabled cooperative network shows a significant improvement over the CRS-based cooperative network. The reason is that the SWIPT-enabled cooperative relay can save more of the harvested energy for usage during a future transmission as P_S increases, thereby extending the relay's lifetime and the entire cooperative network security.

The plot of secrecy outage probability performance of the proposed SWIPT-enabled cooperative networks against (G_{SR}/G_{RD}) for different values of G_{RE} is shown in Fig. 6,

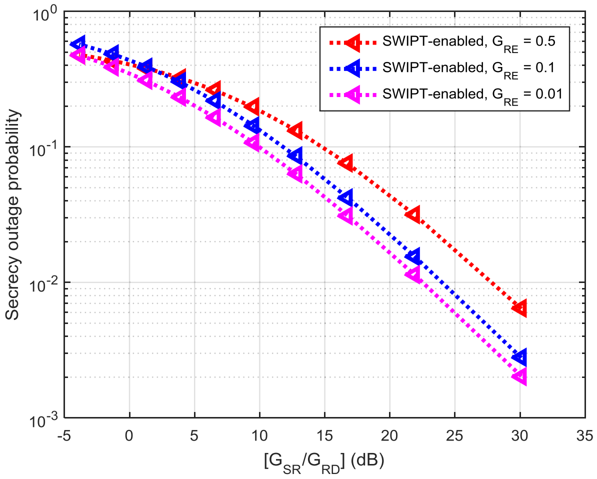

FIGURE 6. Secrecy outage probability against (G_{SR}/G_{RD}) for different values of G_{RE}.

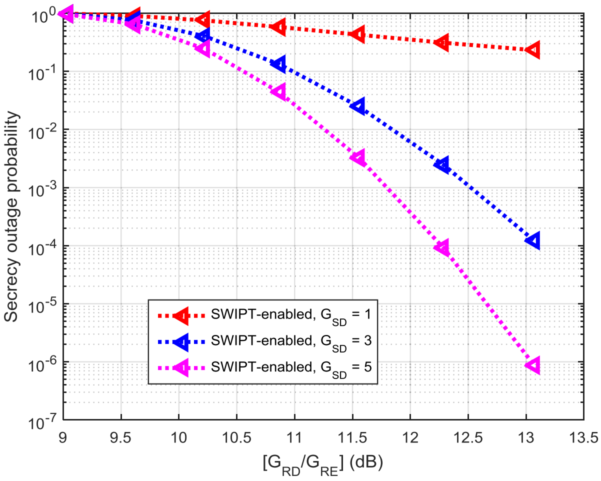

FIGURE 7. Secrecy outage probability against (G_{RD}/G_{RE}) for different values of G_{SD}.

where G_{SR} and G_{RD} are the $\varepsilon\left\{|G_{SR}|^2\right\}$ and $\varepsilon\left\{|G_{RD}|^2\right\}$, respectively. It is clearly seen that the secrecy outage probability can be enhanced when $\left(G_{SR}/G_{RD}\right)$ increases. The reason is that a larger value of $\left(G_{SR}/G_{RD}\right)$ indicates a better $S-R$ link which provides high security against eavesdropping. Moreover, it is observed from Fig. 6 that the secrecy outage probability of the considered network can also be enhanced by reducing G_{RE}, because a larger G_{RE} means a better $R-E$ link which is beneficial for eavesdropping and consequently reducing the security level of the considered network.

In Fig. 7, we present the secrecy outage probability performance of the SWIPT-enabled cooperative network against $\left(G_{RD}/G_{RE}\right)$ for different values of G_{SD}. As observed in Fig. 7, the secrecy outage probability of the SWIPT-enabled network decreases as $\left(G_{RD}/G_{RE}\right)$ increases. The reason is that a larger value of $\left(G_{RD}/G_{RE}\right)$ indicates a better $R-D$ link which provides high security against eavesdropping during second phase of transmission. Also, it is observed from Fig. 7 that the secrecy outage probability can also be enhanced by increasing G_{SD}, because a larger G_{SD} means a better $S-D$ link which is also beneficial to the considered network by exploiting the diversity gain via the adopted SC technique.

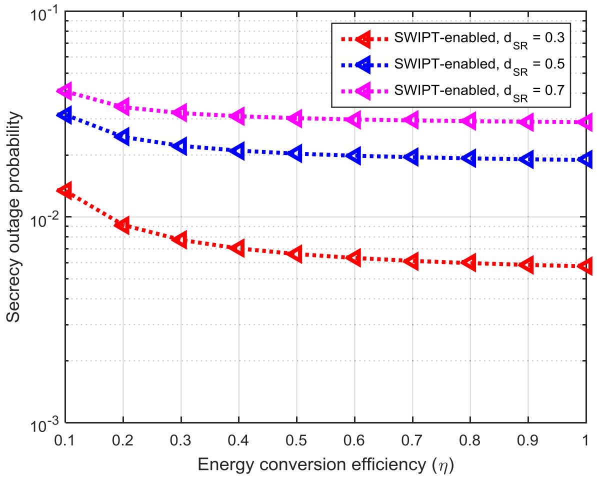

FIGURE 8. Secrecy outage probability against energy conversion efficiency η for different values of d_{SR}.

Fig. 8 shows the effect of the energy conversion efficiency η on the secrecy outage probability performance of the SWIPT-enabled cooperative network for different values of source-relay distance d_{SR}. It can be observed that as η of the relay receiver increases, the secrecy outage probability performance of the SWIPT-enabled cooperative network improves. The smaller the value of d_{SR}, the better the system secrecy outage probability. At smaller d_{SR}, the $S-R$ link path loss is lesser and R is able to harvest enough energy and decode the received information with a smaller probability of error.

Then, R will assist the information transmission between S and D, ultimately resulting in the diversity gain at D. Moreover, the secrecy outage probability decreases slowly with η particularly when η is greater than 0.4. The practical interpretation of this result is that EH devices with high η is inessential because it incurs a high economic cost.

Fig. 9 illustrates the plot of secure energy efficiency ϕ_{EE} against P_S by setting $P_x = P_y = P_z = 10^{-3}$ W, $P_e = 10^{-4}$ W and $T = 1$, for both cooperative networks. It can be observed from Fig. 9 that the two networks behave similarly. The ϕ_{EE} first increases and later decreases as P_S increases for both the SWIPT-enabled and the CRS-based cooperative networks. This is due to the fact that more energy is being consumed at higher P_S, thereby resulting in the decrease in ϕ_{EE}, since ϕ_{EE} is modeled as the ratio of the system capacity to the total energy consumed. At low P_S region, the SWIPT-enabled cooperative network is more energy efficient than the CRS-based cooperative network. However, at high P_S of 20 dB the performance gain is significantly reduced. This can offer a tradeoff between the secrecy outage performance and the transmitted power cost.

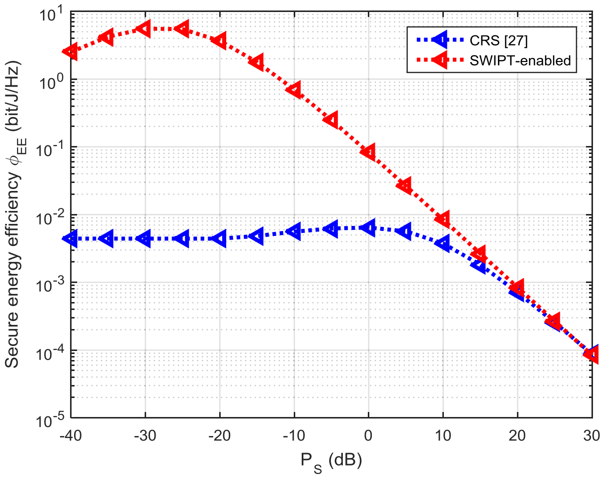

FIGURE 9. Secure energy efficiency against P_S.

V. CONCLUSION

This paper analyzes a secure SWIPT-enabled cooperative network with $S-R$ link based DF HPTSR protocol that can improve the operational lifetime of a relay node and the secrecy performance of the cooperative network. In particular, we investigated the secrecy performance of the considered network by deriving the analytical expressions for the near-optimal power splitting factor in order to maximize the system channel capacity, the secrecy outage probability and the secure energy efficiency. Our numerical results revealed that the SWIPT-enabled cooperative network achieves better secrecy outage probability performance and more energy efficient than the CRS-based cooperative network.

REFERENCES

[1] P. Yan, Y. Zou, and J. Zhu, "Energy-aware multiuser scheduling for physical-layer security in energy-harvesting underlay cognitive radio systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2084–2096, Mar. 2018.

[2] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2035–2048, Mar. 2018.

[3] F. K. Ojo, D. O. Akande, and M. F. M. Salleh, "An overview of RF energy harvesting and information transmission in cooperative communication networks," *Telecommun. Syst.*, pp. 1–14, Jul. 2018, doi: 10.1007/s11235-018-0483-8.

[4] H. Khodakarami and F. Lahouti, "Link adaptation for physical layer security over wireless fading channels," *IET Commun.*, vol. 6, no. 3, pp. 353–362, 2012.

[5] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[6] T. A. Le, H. X. Nguyen, Q.-T. Vien, and M. Karamanoglu, "Secure information transmission in the presence of energy-harvesting eavesdroppers in multi-cell networks," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–5.

[7] 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.

[8] S. Chang, J. Li, X. Fu, and L. Zhang, "Energy harvesting for physical layer security in cooperative networks based on compressed sensing," *Entropy*, vol. 19, no. 9, p. 462, 2017.

[9] 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.

[10] 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.

[11] C. Yuen, M. Elkashlan, Y. Qian, T. Q. Duong, L. Shu, and F. Schmidt, "Energy harvesting communications: Part 2 [guest editorial]," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 54–55, Jun. 2015.

[12] T. P. Do, Y. Jeong, and Y. H. Kim, "Rate optimization of two-way relaying with wireless information and power transfer," *Information*, vol. 8, no. 4, p. 141, 2017.

[13] A. Rajaram, D. N. K. Jayakody, K. Srinivasan, B. Chen, and V. Sharma, "Opportunistic-harvesting: RF wireless power transfer scheme for multiple access relays system," *IEEE Access*, vol. 5, pp. 16084–16099, 2017.

[14] Z. Ding, I. Krikidis, B. Sharif, and H. V. Poor, "Impact of channel state information on wireless energy harvesting cooperative networks with spatially random relays," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 4072–4076.

[15] D.-T. Do, "Optimal throughput under time power switching based relaying protocol in energy harvesting cooperative networks," *Wireless Pers. Commun.*, vol. 87, no. 2, pp. 551–564, 2016.

[16] 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.

[17] P. Ramezani and A. Jamalipour, "Throughput maximization in dual-hop wireless powered communication networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9304–9312, Oct. 2017.

[18] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Throughput and ergodic capacity of wireless energy harvesting based DF relaying network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 4066–4071.

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

[20] 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.

[21] P. Jindal and R. Sinha, "Energy efficiency and secure communication with power splitting energy harvesting technique for single relay network," in *Proc. Int. Conf. Comput. Appl.*, Sep. 2017, pp. 215–219.

[22] F. K. Ojo and M. F. M. Salleh, "Throughput analysis of a hybridized power-time splitting based relaying protocol for wireless information and power transfer in cooperative networks," *IEEE Access*, vol. 6, pp. 24137–24147, 2018.

[23] S. Ghose, C. Kundu, and O. A. Dobre, "Secrecy outage of proactive relay selection by eavesdropper," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[24] P. N. Son, V. P. Tuan, P. Sol, and L. T. Anh, "Improving the secrecy of cooperative transmissions using unshared jamming," in *Proc. 4th NAFOSTED Conf. Inf. Comput. Sci.*, Nov. 2017, pp. 31–36.

[25] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R.-F. Liao, "Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108–2117, Mar. 2018.

[26] G. Pan and C. Tang, "Outage performance on threshold AF and DF relaying schemes in simultaneous wireless information and power transfer systems," *AEU-Int. J. Electron. Commun.*, vol. 71, pp. 175–180, Sep. 2017.

[27] J. Yao, J. Ye, D. Wang, H. Lei, and G. Pan, "Secure source-relay link based threshold DF relaying scheme," *AEU-Int. J. Electron. Commun.*, vol. 85, pp. 144–149, Feb. 2018.

[28] H. Chen, Y. Li, J. L. Rebelatto, B. F. Uchôa-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, no. 7, pp. 1700–1711, Apr. 2015.

[29] S. Mahama, D. K. P. Asiedu, and K.-J. Lee, "Simultaneous wireless information and power transfer for cooperative relay networks with battery," *IEEE Access*, vol. 5, pp. 13171–13178, 2017.

[30] Z. Qi, Z. Jingmei, S. Chunju, W. Ying, Z. Ping, and H. Rong, "Power allocation for regenerative relay channel with Rayleigh fading," in *Proc. IEEE 59th Veh. Technol. Conf. (VTC-Spring)*, vol. 2, May 2004, pp. 1167–1171.

[31] Y. W. Hong, W. J. Huang, F. H. Chiu, and C. C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 47–57, May 2007.

[32] E. J. Candés, J. K. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Commun. Pure Appl. Math.*, vol. 59, no. 8, pp. 1207–1223, 2006.

[33] Q. Zhang, C. Yang, H. Haas, and J. S. Thompson, "Energy efficient downlink cooperative transmission with BS and antenna switching off," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 5183–5195, Sep. 2014.

[34] S. Hu and Z. Ding, "Secure communication in cooperative network with wireless information and power transfer," *IET Signal Process.*, vol. 9, no. 9, pp. 663–669, 2015.

FESTUS KEHINDE OJO was born in Ilesa, Nigeria. He received the B.Tech. degree in electronic and electrical engineering from the Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria, in 2008, the M.Eng. degree in electrical and electronic engineering (communication engineering option) from the Federal University of Technology, Akure, Nigeria, in 2012. He is currently pursuing the Ph.D. degree at the School of Electrical and Electronic Engineering, Universiti Sains Malaysia. He is currently a Lecturer II with the Department of Electronic and Electrical Engineering, LAUTECH. His main research interests include signal processing and wireless energy harvesting in cooperative networks. He is a Corporate Member of the Nigerian Society of Engineers and a registered Engineer with the Council for the Regulation of Engineering, Nigeria.

MOHD FADZLI MOHD SALLEH (M'03) was born in Bagan Serai, Malaysia. He received the B.S. degree in electrical engineering from the Polytechnic University, Brooklyn, NY, USA, in 1995, the M.S. degree in communication engineering from the University of Manchester Institute of Science and Technology, Manchester, U.K., in 2002, and the Ph.D. degree from the University of Strathclyde, Glasgow, U.K., in 2006.

He was a Software Engineer with the Department of Research and Development, Motorola, Penang, Malaysia, until 2001. He is currently an Associate Professor with the School of Electrical and Electronic Engineering, Universiti Sains Malaysia. He has supervised eight Ph.D. degree students to graduation. His main research interests include source coding and signal processing for application in telecommunications and wireless communication networks.