Research Article

Analysis of SWIPT-Enabled Relay Networks with Full-Duplex Destination-Aided Jamming

Jinglan Ou ¹, Hangchuan Shi ¹, Liubin Wang¹, Rui Ma ¹ and Haowei Wu ^{1,2,3}

¹College of Microelectronics and Communication Engineering, Chongqing University, Chongqing 400044, China

²Center of Communication and Tracking Telemetry Command, Chongqing University, Chongqing 400044, China

³Chongqing Key Laboratory of Space Information Network and Intelligent Information Fusion, Chongqing University, Chongqing 400044, China

Correspondence should be addressed to Haowei Wu; wuhaowei@cqu.edu.cn

Received 16 April 2021; Revised 30 May 2021; Accepted 17 June 2021; Published 8 July 2021

Academic Editor: Savio Sciancalepore

Copyright © 2021 Jinglan Ou et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Simultaneous wireless information and power transfer (SWIPT) is a major breakthrough in the field of low-power wireless information transmissions. In this paper, the secrecy performance of the SWIPT-enabled relay network with full-duplex destination-aided jamming is assessed, where both the power-splitting (PS) and time-switching (TS) schemes at the relay are considered with the linear and nonlinear energy harvesting models. The relay harvests energy from the confidential signal and artificial noise sent by the source and destination, respectively, and forwards the amplified signal to the destination, in the presence of an eavesdropper. The analytical closed-form expressions of the connection outage probability (COP), secrecy outage probability (SOP), and transmission outage probability (TOP) for PS- and TS-based schemes are derived, and the closed-form expression of the lower bound of ergodic secrecy capacity (ESC) is calculated. The asymptotic-form expressions of the COP, SOP, TOP, and ESC are further analyzed to capture the valuable information in the high SNR regime. Numerical results verify the correctness of analytical results, reveal the effects of the PS/TS ratio, and transmit the signal-to-noise ratio on secrecy performance.

1. Introduction

Wireless communication networks greatly facilitate our daily lives with the explosive growth of smart phones, wireless laptops, and tablet computers. Stable and continuous energy supply is a fundamental requirement for wireless devices, which are usually charged by wired power, batteries, or other natural resources such as wind and solar from the surrounding environment. As an emerging technique, wireless power transmission (WPT) technique harvesting energy from electromagnetic radiation of the radio frequency (RF) signal is a promising solution to provide sustainable energy for wireless devices [1–3]. Recently, RF power harvesting has been widely studied and applied in wireless systems which are hard to acquire regular electrical supply, especially under conditions of frequent movement and wide coverage of wireless terminals [4–6].

As a combination of wireless communication and WPT, simultaneous wireless information and power transfer (SWIPT) was proposed in [7]. With the advantages of high spectral efficiency and low energy consumption, SWIPT has drawn extensive attention on account of its potential ability to support wireless sensors and medical implants without frequent battery charging [8–10]. However, signals in SWIPT systems are particularly vulnerable to malicious attacks due to the strong signal power as well as the open nature of the wireless channel, which results in concerns about the security issue. Therefore, a lot of studies have been performed to prevent the leakage of private information, and physical layer security (PLS) has been proved to be one of the most effective solutions to improve the security of SWIPT systems [11]. The pivotal character of PLS is to utilize the intrinsic secrecy properties of wireless channels, which can help to realize the secure communication in SWIPT [12–15].

Cooperative jamming is regarded as a sensible approach to prevent information leakage for SWIPT. Generally, to degrade the eavesdropper, one helper node is deployed in the network to transmit a jamming signal such as the artificial noise (AN). The helper is also termed as a cooperative interference source which might be any node involved in the network, e.g., the source, relay, and destination.

As the self-cooperative jamming, the source can radiate the energy signal and the information signal superposed with the AN. In [13], the PLS issues in a multiuser SWIPT system were studied, where one multi-antenna source sends energy and information with the AN signal simultaneously to the information receiver and energy receivers. This deliberate interference is added into the source signal in order to degrade the information eavesdropping at the energy receivers. To obtain the maximum secrecy rate by optimizing the power allocation and AN-aided transmission, a SWIPT system, composing of an eavesdropper, a source, and several users, was investigated in [16], where the source acts as a cooperative jammer as well.

Legitimate communication partners, such as the relay, can also act as a jammer in the SWIPT network. In [17], a relay adopting the power-splitting (PS) scheme in the wiretap system was introduced to forward information and interfere the illegal eavesdropper, and an iterative algorithm was proposed to handle the problem of maximizing the secrecy rate in the worst case. A two-level strategy was proposed in [18] to achieve the minimization relay power, within the limit of secrecy rate and energy harvesting (EH) requirements through jointly optimizing the relay beamforming matrix, AN covariance and PS ratio.

The destination node can also assist the network in sending interference as well as receiving the intelligence signal. Two-hop cooperative communication with the destination transmitting the jamming signal was considered, and both adaptive time conversion and power cutting schemes were presented in [19], where the maximum secrecy capacity and its relationship with the time conversion ratio and power cutting rate are studied. A SWIPT-enabled system by full-duplex (FD) jamming at the intended receiver is proposed to enhance secrecy performance and the secrecy throughput of the system is analyzed in [20]. The FD destination node with the ability of emitting artificial noise is exploited to achieve better secrecy transmission in the three-node eavesdropping scenario of SWIPT, where the destination employed time-switching (TS) protocol to harvest energy, and the closed-form expressions of the connection outage probability (COP), the secrecy outage probability (SOP), the transmission outage probability (TOP), and the secrecy energy efficiency are derived [21]. In our previous study [22], an FD destination-assisted jamming scheme was adopted in a SWIPT-enabled trusted relay network, and the optimization problem was designed to achieve the optimal secrecy capacity, where only the PS scheme with the linear EH (LEH) model was considered.

Motivated by above observations, in this paper, the secrecy performance of a SWIPT-enabled four-node wiretap network with an amplify-and-forward (AF) relay and a

destination with jamming is investigated. The source, destination, and eavesdropper are considered to be under the uninterruptible power supplies. The relay replenishes energy from the RF signals including the information signal from the source and the AN signal from the destination, after which the relay amplifies the signal and then sends the correct information signal to the destination.

Our work is different from the following related papers: firstly, the source acted as a jammer in [13, 16], and the relay was the jammer in [17, 18]. Unlike these papers, the destination sent the jamming signal with FD to protect the classified information in our network, which is the fundamental difference between our and their works. Secondly, only the LEH model was utilized in [19, 21, 22], while both the linear and nonlinear EH models are considered in this treatise. Thirdly, the destination node was self-interference in our network, instead of disturbing the relay, which is unlike the network in [19]. In contrast to [20, 21], the author investigated the three-node system, while the network in this paper consists of four nodes. Fourthly, both the PS- and TS-based schemes are employed, while only the PS scheme was applied in [19, 22] and the TS in [22]. In addition, the COP, SOP, TOP, and ESC are analyzed in our research to provide a comprehensive and thorough guidance for practical application, while only SC was focused in [19, 22]. The contributions of our work are summarized as follows:

- (i) A SWIPT-enabled relay network is studied, where an FD destination receives the information, while transmitting the AN jamming at the same time. The secrecy performance of the network is analyzed for both the PS- and TS-based schemes under both the nonlinear and linear EH models at the relay.
- (ii) For both the PS and TS schemes, the closed-form expressions of the COP, SOP, TOP, and lower bound of the ergodic secrecy capacity (ESC) are presented under the linear and nonlinear EH models, and the asymptotic-form expressions of these metrics are given in the region of high signal-to-noise ratios (SNRs).
- (iii) The correctness of analytical expressions is verified by simulations, and the impacts of different system parameters on the COP, SOP, TOP, and lower bound of ESC are revealed. The simulation results imply that the optimal secrecy performance of the system can be achieved by optimizing the four metrics.

The rest of this paper is structured as follows. Section 2 describes the system model for the secure communication via the relay under both the linear and nonlinear EH models. In Section 3, the analytical expressions of the COP, SOP, TOP, and ESC for the PS- and TS-based relaying are derived. Numerical results are presented in Section 4, where effects of different system parameters on the secrecy performance of the SWIPT system with FD destination-assisted jamming are offered. Finally, conclusions are presented in Section 5.

2. System Model

2.1. Network Description. As shown in Figure 1, the SWIPT-enabled relay network is composed of four nodes, i.e., one source $\mathcal{S}$, one AF relay $\mathcal{R}$, one destination $\mathcal{D}$, and one eavesdropper $\mathcal{E}$. The relay depends on the wireless power supplies from the source and destination, while the source, destination, and eavesdropper are supplied by the stable power source. The FD destination with two antennas can transmit the AN signal and receive information signal from the relay at the same time, and other nodes equipped with only one antenna operate in the half-duplex mode. In addition, the source $\mathcal{S}$ only has a direct link with the relay $\mathcal{R}$, while the direct links of $\mathcal{S} - \mathcal{D}$ and $\mathcal{S} - \mathcal{E}$ are blocked by the physical obstacles, which is a common assumption in [23, 24].

2.1.1. Channel Description. The quasi-static frequency nonselective channel is considered in this model, which indicates that all the channel coefficients remain constant within a transmission block, but vary independently from one packet to another [25, 26]. Without loss of generality, it is assumed that the instantaneous channel state information of both the main channel and eavesdropping channel are available [27]. The channel power gain between the nodes i and j is defined as $|h_{ij}|^2$, which is the exponential distribution with mean $\lambda_{ij} = d_{ij}^{-\alpha}$, where i and $j \in \{\mathcal{S}, \mathcal{R}, \mathcal{D}, \mathcal{E}\}$, $i \neq j$, d_{ij} is the distance between nodes i and j , and α is the path-loss exponent. The channel coefficients for $\mathcal{S} - \mathcal{R}$, $\mathcal{R} - \mathcal{E}$, $\mathcal{R} - \mathcal{D}$, and $\mathcal{D} - \mathcal{E}$ links are represented as $h_{\mathcal{S}\mathcal{R}}$, $h_{\mathcal{R}\mathcal{E}}$, $h_{\mathcal{R}\mathcal{D}}$, and $h_{\mathcal{D}\mathcal{E}}$, respectively. The residual self-interference (RSI) channel coefficient at the destination is denoted as $h_{\mathcal{D}\mathcal{D}}$, which is regarded as the independent complex Gaussian random variable [20]. According to [28], after cancellation, the destination-aided jamming signal is regarded as the RSI, which is hypothesised to be independent of other signals and yields to Gaussian distribution with zero mean and σ_i^2 -variance. The variance is formulated as $\sigma_i^2 = kP_r^\nu$, where the two constants, i.e., $k > 0$ and $\nu \in [0, 1]$, depend on the interference cancellation scheme at the relay [29].

2.1.2. Secure Transmission. The communication process of the system includes energy harvesting, signal processing, and information transmitting, which are shown in Figure 1. Firstly, the source transmits confidential information signal toward the relay, and the destination sends the AN signal to the relay simultaneously, and then, the relay collects energy from the received signal, after which the relay amplifies the received signal. Finally, the relay with the full energy forwards the confidential information to the destination under the protection of the jamming signal.

In the following content, the PS- and TS-based schemes are introduced in the SWIPT system, where both the linear and nonlinear EH architectures are also taken into consideration at the relay. For the sake of simplicity, the energy

FIGURE 1: SWIPT-enabled relay network.

costs for data processing are ignored in all nodes, which means that most of the energy is used for data delivery [30].

2.2. Relay Protocol

2.2.1. Power-Splitting-Based Relaying. The PS-based scheme for the secure communication in the SWIPT system with FD jamming is illustrated in Figure 2, where the source-to-destination communication occurs in a slot of duration T . The slot is divided into two phases equally. The source transmits the information signal through power $P_{\mathcal{S}}$ toward the relay, and the destination sends the jamming signal through power $P_{\mathcal{D}}$ to the relay, where $P_{\mathcal{S}} = \xi P_{\text{total}}$ and $P_{\mathcal{D}} = (1 - \xi)P_{\text{total}}$ are the power from the source and destination separately, $\xi \in (0, 1)$ is the power allocation coefficient, and P_{total} is the total system power. The received energy from the RF signal is divided into two parts in the first phase, which depends on the PS ratio ρ , as ρ for the energy harvesting and $(1 - \rho)$ for the signal processing. In the second phase, the relay transmits the information to the destination.

For the energy harvesting at the relay based on the PS-based protocol, the linear EH and nonlinear EH (NLEH) models at $\mathcal{R}$ are discussed as following. Normally, the most existing research studies are based on the LEH model for it is tractable [21, 31]. The linear energy collection at the relay is

$$E_H^L = \frac{\eta \rho T (P_{\mathcal{S}} |h_{\mathcal{S}\mathcal{R}}|^2 + P_{\mathcal{D}} |h_{\mathcal{R}\mathcal{D}}|^2)}{2}, \quad (1)$$

where $\eta (0 < \eta < 1)$ represents the energy conversion efficiency.

The forwarding power at the relay for transmitting signals is written as

$$P_{\mathcal{R}}^L = \eta \rho E_r, \quad (2)$$

where $E_r = P_{\mathcal{S}} |h_{\mathcal{S}\mathcal{R}}|^2 + P_{\mathcal{D}} |h_{\mathcal{R}\mathcal{D}}|^2$.

The energy conversion efficiency actually relies on the input power, which means that the energy collected is nonlinear with the input power [32]. The NLEH model is also considered in this paper since it matches practical EH circuits better than the linear one [20]. To ensure the accuracy, practicability, and ease of processing for the analysis, the simplified NLEH model is exploited and represented as

FIGURE 2: PS scheme for secure communication in the SWIPT system.

$$P_{\mathcal{R}}^{\text{NL}} = \frac{p_1 \mathbb{E}\{P_{\mathcal{R}}^L\}}{\mathbb{E}\{P_{\mathcal{R}}^L\} + p_2}, \quad (3)$$

where $p_1 = c_1 - c_2/c_3$, $p_2 = c_3$, and $\mathbb{E}\{\cdot\}$ is the expectation operator and c_1 , c_2 , and c_3 are constants related to the detailed circuit specifications such as the resistance and capacitance [20]. The specific values of c_1 , c_2 , and c_3 are 0.3929, 0.01675, and 0.04401, respectively [33].

The nonlinear energy harvesting at the relay can be expressed as

$$E_H^{\text{NL}} = \frac{p_1 \rho E_r}{\rho E_r + p_2} \frac{T}{2}. \quad (4)$$

Hence, the power to forward signals at $\mathcal{R}$ is given by

$$P_{\mathcal{R}}^{\text{NL}} = \frac{p_1 \rho E_r}{\rho E_r + p_2}. \quad (5)$$

After energy harvesting, the information processing is discussed next. The received signal at the relay in the first phase is expressed as

$$y_{\mathcal{R}} = \sqrt{(1-\rho)P_{\mathcal{S}}} h_{\mathcal{S}\mathcal{R}} x_{\mathcal{S}} + \sqrt{(1-\rho)P_{\mathcal{D}}} h_{\mathcal{R}\mathcal{D}} x_{\text{AN}} + n_{\mathcal{R}}, \quad (6)$$

where $n_{\mathcal{R}}$ stands for the additive white Gaussian noise (AWGN) at the relay with zero mean and variance σ^2 .

Next, the AF relay transmits the amplified version of the received signal which is given by

$$x_{\mathcal{R}}^l = \frac{\sqrt{P_{\mathcal{R}}^L} y_{\mathcal{R}}}{\sqrt{(1-\rho)(P_{\mathcal{S}} |h_{\mathcal{S}\mathcal{R}}|^2 + P_{\mathcal{D}} |h_{\mathcal{R}\mathcal{D}}|^2) + \sigma^2}}, \quad (7)$$

where $l \in \{L, \text{NL}\}$ represents the LEH and NLEH, respectively.

The received signals at $\mathcal{D}$ and $\mathcal{E}$ with destination-aided jamming can be, respectively, expressed as

$$y_{\mathcal{D}}^l = h_{\mathcal{R}\mathcal{D}} x_{\mathcal{R}}^l + \sqrt{P_{\mathcal{D}}} h_{\mathcal{D}\mathcal{D}} x_{\text{AN}} + n_{\mathcal{D}}, \quad (8)$$

$$y_{\mathcal{E}}^l = h_{\mathcal{R}\mathcal{E}} x_{\mathcal{R}}^l + \sqrt{P_{\mathcal{D}}} h_{\mathcal{D}\mathcal{E}} x_{\text{AN}} + n_{\mathcal{E}}, \quad (9)$$

where $n_{\mathcal{D}}$ and $n_{\mathcal{E}}$ denote the AWGNs at the destination and eavesdropper with zero mean and variance σ^2 , respectively.

It is supposed that the destination can eliminate the AN signal by obtaining the exact information of the channel gain of the $\mathcal{R} - \mathcal{D}$ link, while the eavesdropper is interfered by the AN on the account of lacking channel information [25]. Plugging (7) into (8), the received instantaneous end-to-end SNR at $\mathcal{D}$ is given by

$$\Gamma_{\mathcal{D}}^l = \frac{(1-\rho)\gamma_{\mathcal{S}}\gamma_{\mathcal{R}}^l |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2}{\gamma_{\mathcal{R}}^l |h_{\mathcal{R}\mathcal{D}}|^2 + (k\gamma_{\mathcal{D}}^l + 1)((1-\rho)\gamma_{\Theta} + 1)}, \quad (10)$$

where $\gamma_{\mathcal{S}} = P_{\mathcal{S}}/\sigma^2$, $\gamma_{\mathcal{R}}^l = P_{\mathcal{R}}^l/\sigma^2$, $\gamma_{\mathcal{D}} = P_{\mathcal{D}}/\sigma^2$, $\gamma_{\Theta} = E_r/\sigma^2$, and $k\gamma_{\mathcal{D}}^l$ is the residual self-interference.

Similarly, the received SNR at $\mathcal{E}$ is obtained by the following equation:

$$\Gamma_{\mathcal{E}}^l = \frac{(1-\rho)\gamma_{\mathcal{S}}\gamma_{\mathcal{R}}^l |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2}{(1-\rho)\gamma_{\mathcal{R}}^l \gamma_{\mathcal{D}} |h_{\mathcal{R}\mathcal{D}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2 + \gamma_{\mathcal{R}}^l |h_{\mathcal{R}\mathcal{E}}|^2 + (\gamma_{\mathcal{D}} |h_{\mathcal{D}\mathcal{E}}|^2 + 1)((1-\rho)\gamma_{\Theta} + 1)}. \quad (11)$$

2.2.2. Time-Switching-Based Relaying. From the perspective of receiver's complexity, the TS is simpler than the PS as energy harvesting and information processing are separate in commercial circuits [34]. In the TS-based solution, the energy acquisition and information processing of the RF signal at the relay are performed separately during different time periods, depending on $\alpha \in (0, 1)$. The TS-based scheme of the SWIPT system with destination-aided FD jamming is shown in Figure 3, and the time period T is split into three phases. In the first phase, the relay takes αT to harvest energy from the received RF signals. During the second phase, the relay amplifies the signal from the source within $(1-\alpha)T/2$ period, and the relay sends the information signal to the destination at the remaining time $(1-\alpha)T/2$ in the third phase. Both the LEH and NLEH models for the TS scheme are discussed in the following part.

For the aforementioned TS policy, the harvested energy during the period of αT in the first phase is given by $E_H^L = \eta \alpha T E_r$. Thus, the power at $\mathcal{R}$ sending the amplified signal to the destination is written as $P_{\mathcal{R}}^L = 2\eta \alpha E_r / (1-\alpha)$. Similar to the nonlinear derivation of the PS-based scheme in section 2.2.1, the expression of NLEH for the TS-based scheme is $E_H^{\text{NL}} = \alpha T p_1 E_r / (E_r + p_2)$, and the relay's transmit power forwarding the information to destination is given as

$$P_{\mathcal{R}}^{\text{NL}} = \frac{2\alpha p_1 E_r}{(1-\alpha)(E_r + p_2)}. \quad (12)$$

In the second phase, the relay performs information processing after energy collections, where the signal received by the relay becomes

$$y_{\mathcal{R}} = \sqrt{P_{\mathcal{S}}} h_{\mathcal{S}\mathcal{R}} x_{\mathcal{S}} + \sqrt{P_{\mathcal{D}}} h_{\mathcal{R}\mathcal{D}} x_{\text{AN}} + n_{\mathcal{R}}. \quad (13)$$

FIGURE 3: TS scheme for secure communication in the SWIPT system.

Then, the signal sent by the relay in the third phase is

$$x_{\mathcal{R}}^I = \frac{\sqrt{P_{\mathcal{R}}^I} y_{\mathcal{R}}}{\sqrt{(P_{\mathcal{S}} |h_{\mathcal{S}\mathcal{R}}|^2 + P_{\mathcal{D}} |h_{\mathcal{R}\mathcal{D}}|^2) + \sigma_{\mathcal{R}}^2}}. \quad (14)$$

The received signals at $\mathcal{D}$ and $\mathcal{E}$ are the same as (8) and (9), respectively, which are not repeated here. Embedding (13) and (14) into (8), the received instantaneous end-to-end SNR at $\mathcal{D}$ is

$$\Gamma_{\mathcal{D}}^I = \frac{\gamma_{\mathcal{S}} \gamma_{\mathcal{R}}^I |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2}{\gamma_{\mathcal{R}}^I |h_{\mathcal{R}\mathcal{D}}|^2 + (k\gamma_{\mathcal{D}}^v + 1)(\gamma_{\Theta} + 1)}. \quad (15)$$

Likewise, the received SNR at $\mathcal{E}$ is represented by

$$\Gamma_{\mathcal{E}}^I = \frac{\gamma_{\mathcal{S}} \gamma_{\mathcal{R}}^I |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2}{\gamma_{\mathcal{R}}^I \gamma_{\mathcal{D}} |h_{\mathcal{R}\mathcal{D}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2 + \gamma_{\mathcal{R}}^I |h_{\mathcal{R}\mathcal{E}}|^2 + (\gamma_{\mathcal{D}} |h_{\mathcal{D}\mathcal{E}}|^2 + 1)(\gamma_{\Theta} + 1)}. \quad (16)$$

3. Performance Analysis

In this section, we proceed to derive the closed-form expressions of the COP, SOP, TOP, and lower bound of ESC for both PS and TS schemes to comprehensively and directly analyze the secrecy performance of the system.

3.1. Power-Splitting Protocol

3.1.1. COP. The destination fails to recover the source message from the relay when the channel capacity of the $\mathcal{R} - \mathcal{D}$ link is lower than the minimum transmission rate R_t (bps/Hz), which means a connection interruption has occurred. The channel capacity is defined as $C_M = 1/2 \log_2(1 + \Gamma_{\mathcal{D}})$ in Shannon's coding theorem. The factor 1/2 denotes the effective time of information transmission between the source and destination.

Mathematically, the COP is defined as [21]

$$P_{CO}^I = \Pr\{\Gamma_{\mathcal{D}}^I < \gamma_{th}^I\}, \quad (17)$$

where $\gamma_{th}^I = 2^{2R_t} - 1$ is the minimum transmission threshold.

Proposition 1. The closed-form expression of the COP for the SWIPT system with FD destination-aided jamming under the PS scheme is given by

$$P_{CO}^I = 1 - \frac{1}{m_y} e^{-(\gamma_{th}^I/m_x)} \left(2 \left(\frac{\mu}{\nu} \right)^{(1/2)} K_1(2\sqrt{\mu\nu}) \right), \quad (18)$$

where $m_y = \lambda_{\mathcal{R}\mathcal{D}}$, $m_x = (1 - \rho)\gamma_{\mathcal{S}}\lambda_{\mathcal{S}\mathcal{R}}$, $\mu = \gamma_{th}^I a_1/m_x b_1$, $\nu = 1/m_y$, $a_1 = (k\gamma_{\mathcal{D}}^v + 1)((1 - \rho)\gamma_{\Theta} + 1)$, and $b_1 = \gamma_{\mathcal{R}}^I$. Here, $K_1(\cdot)$ is the modified Bessel functions of the second kind (Eq. 8.407.2 in [35]).

Proof. See Appendix A.

To further capture the useful information for the secrecy performance, the asymptotic analysis of COPs is conducted in terms of LEH and NLEH models.

In the high SNR regime, i.e., $P_{\text{total}} \rightarrow \infty$, the analytical expression of COP in the SWIPT-enabled relay system adopting the LEH model is given by

$$P_{CO}^{I, \gamma_{\text{total}} \rightarrow \infty} = 1 - \frac{1}{\bar{m}_y} \left(2 \left(\frac{\bar{u}}{\bar{v}} \right)^{(1/2)} K_1(2\sqrt{\bar{u}\bar{v}}) \right), \quad (19)$$

where $\bar{m}_x = \lambda_{\mathcal{S}\mathcal{R}}$, $\bar{m}_y = \lambda_{\mathcal{R}\mathcal{D}}$, $k_1 = \xi \bar{d}$, $k_2 = \lambda_d d(1 - \xi)\lambda$, $\bar{u} = \gamma_{th}^I k_2/\bar{m}_x k_1$, $\bar{v} = 1/\bar{m}_y$, $\bar{d} = \eta \rho \lambda$, and $\lambda = \lambda_{\mathcal{S}\mathcal{R}} = \lambda_{\mathcal{R}\mathcal{D}} = \lambda_{\mathcal{R}\mathcal{E}} = \lambda_{\mathcal{D}\mathcal{E}}$ as the channel fading between nodes is independent and identical by default.

The asymptotic formula of COP adopting the PS scheme under the NLEH model is $P_{CO}^{NL, \gamma_{\text{total}} \rightarrow \infty} = 1$. Please refer to Appendix A for the derivation of asymptotic expressions of COP concerning the PS policy.

It can be found from the above analytical expressions that the COP eventually remains unchanged under the LEH model as the transmit SNR goes to infinity, while the COP is not reduced, but rises to reaching one instead under the NLEH model. $\square$

3.1.2. SOP. The SOP is an indispensable indicator to measure the confidential performance, concerning the relationship between the channel capacity of the $\mathcal{R} - \mathcal{E}$ link and the eavesdropping rate $R_e = R_t - R_s$, where R_s is the secrecy rate and $R_s \leq R_t$ [36]. The SOP reflects in the security outage when the standard channel capacity of the $\mathcal{R} - \mathcal{E}$ link is higher than R_e . The SOP is defined as

$$P_{SO}^I = \Pr\{\Gamma_{\mathcal{E}}^I \geq \gamma_{th}^e\}, \quad (20)$$

where $\gamma_{th}^e = 2^{2R_e} - 1$ is the secrecy rate threshold.

Proposition 2. The closed-form expression of SOP in the SWIPT system with FD destination-aided jamming under the PS scheme can be obtained as

$$P_{SO}^I = \frac{1}{m_z} \frac{m_x^2}{m_z m_x + b_2 m_y \gamma_{th}^e} e^{-(\gamma_{th}^e/m_x)} \sum_{k=1}^N w_k \frac{m_z^2 x_k}{\gamma_{th}^e m_w + m_x m_z x_k} e^{(-\gamma_{th}^e a_2/m_x m_z x_k)}, \quad (21)$$

where $m_z = \gamma_{\mathcal{R}}^l \lambda_{\mathcal{R}\mathcal{E}}$, $m_w = a_2 \gamma_{\mathcal{D}} \lambda_{\mathcal{D}\mathcal{E}}$, $a_2 = (1 - \rho) \gamma_{\mathcal{D}} + 1$, and $b_2 = (1 - \rho) \gamma_{\mathcal{D}}$. Here, x_k is the k th root of Laguerre polynomial $L_n(x)$, $w_k = x_k / (N + 1)^2 [L_{N+1}(x_k)]^2$ is the weight, and N is the nonnegative integer determining the accuracy and correctness of the calculation result.

Proof. See Appendix B.

$$P_{\text{SO}}^{L, \gamma_{\text{total}} \rightarrow \infty} = \frac{\tilde{m}_x k_3}{\tilde{m}_z (\gamma_{\text{th}}^e \tilde{m}_y + \tilde{m}_x k_3)} \cdot \left(\frac{\gamma_{\text{th}}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z \tilde{d} k_3} e^{(\gamma_{\text{th}}^e \lambda \tilde{m}_w / \tilde{m}_x \tilde{m}_z \tilde{d} k_3)} \text{Ei} \left(-\frac{\gamma_{\text{th}}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z \tilde{d} k_3} \right) + \tilde{m}_z \right), \quad (22)$$

where $\tilde{m}_z = \lambda_{\mathcal{R}\mathcal{E}}$, $\tilde{m}_w = \lambda_{\mathcal{D}\mathcal{E}}$, and $k_3 = \xi/1 - \xi$. Here, $\text{Ei}(x)$ is the exponential integral, defined as $\text{Ei}(x) = \int_{-\infty}^x e^t/t dt$ (Eq. 8.211.1 in [35]).

Under the NLEH model, the expression of SOP in the high SNRs is $P_{\text{SO}}^{\text{NL}, \gamma_{\text{total}} \rightarrow \infty} = 0$. Refer to Appendix B for the derivation process of asymptotic expressions of SOP accepting the PS policy.

Through the above work, the confidentiality interruption of the system can be analyzed accurately. Apparently, by rising the transmit SNR, SOP can achieve zero under the NLEH model, whereas the SOP in the LEH one stays nonnegative constant.

Equation (21) is sophisticated and hard to understand, so the asymptotic-form expressions of SOP under both LEH and NLEH models are discussed as well. The theoretical expression of the SOP under the high SNRs in the LEH model is

The TOP as a new outage metric is introduced in [21] to measure both the security and reliability of information transmission, which is defined as

$$P_{\text{TO}}^l = 1 - \Pr\{\Gamma_{\mathcal{D}}^l \geq \gamma_{\text{th}}^l, \Gamma_{\mathcal{E}}^l < \gamma_{\text{th}}^e\}. \quad (23)$$

From the previous analysis, it is known that $\Gamma_{\mathcal{D}}^l$ and $\Gamma_{\mathcal{E}}^l$ are not independent of each other. By following the same derivation steps as COP and using the property of the cumulative distribution function (CDF), the analytical expression of TOP is

$$P_{\text{TO}}^l = 1 - \frac{1}{m_y} e^{-(\gamma_{\text{th}}^e/m_x)} \left(2 \left(\frac{\mu}{\nu} \right)^{(1/2)} K_1(2\sqrt{\mu\nu}) \right) + \frac{m_x^2}{m_z(m_x + b_2 m_y \gamma_{\text{th}}^e)} e^{-(\gamma_{\text{th}}^e/m_x)} \sum_{k=1}^N w_k \frac{m_z^2 x_k}{\gamma_{\text{th}}^e m_w + m_x m_z x_k} e^{(-\gamma_{\text{th}}^e a_2 / m_x m_z x_k)}. \quad (24)$$

Equations (25) and (26) indicate the asymptotic-form expressions of the TOP of the SWIPT system with FD

destination-aided jamming under the LEH and NLEH, respectively:

$$P_{\text{TO}}^{L, \gamma_{\text{total}} \rightarrow \infty} = 1 - \frac{1}{\tilde{m}_y} \left(2 \left(\frac{\tilde{u}}{\tilde{v}} \right)^{1/2} K_1(2\sqrt{\tilde{u}\tilde{v}}) \right) + \frac{\tilde{m}_x k_3}{\tilde{m}_z (\gamma_{\text{th}}^e \tilde{m}_y + \tilde{m}_x k_3)} \cdot \left(\frac{\gamma_{\text{th}}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z \tilde{d} k_3} e^{(\gamma_{\text{th}}^e \lambda \tilde{m}_w / \tilde{m}_x \tilde{m}_z \tilde{d} k_3)} \text{Ei} \left(-\frac{\gamma_{\text{th}}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z \tilde{d} k_3} \right) + \tilde{m}_z \right), \quad (25)$$

$$P_{\text{TO}}^{\text{NL}, \gamma_{\text{total}} \rightarrow \infty} = 1. \quad (26)$$

The proof for the asymptotic TOP is the same as that of the asymptotic SOP, thus, the authors skip the proof for brevity. As stated above, the COP, SOP, and TOP can describe the statistical properties of the accessible secrecy performance, and the TOP plays a decisive role when considering both security and reliability. $\square$

3.1.3. ESC. The ESC is another important index for measuring and analyzing the secrecy performance, which describes the average of the attainable secrecy rate for all possible channel conditions and stands for the maximum transmission rate when an eavesdropper cannot decode the

confidential information that is being transmitted. The ESC can be stated as

$$\bar{R}_{\text{sec}}^l = \mathbb{E}\{R_{\text{sec}}^l\}, \quad (27)$$

where $R_{\text{sec}}^l = 1/2 [\log_2(1 + \Gamma_{\mathcal{D}}^l) - \log_2(1 + \Gamma_{\mathcal{E}}^l)]$ is the instantaneous secrecy rate and $1/2$ is the valid time for the transmission of messages.

According to Kalamkar and Banerjee [25], the expression in (27) has no closed-form and is intractable; inspired by it, the lower-bounded form of ESC is given by

$$\bar{R}_{\text{sec}}^l \geq \frac{1}{2 \ln 2} [\mathbb{E}\{\ln(1 + \Gamma_{\mathcal{D}}^l)\} - \mathbb{E}\{\ln(1 + \Gamma_{\mathcal{E}}^l)\}]. \quad (28)$$

Proposition 3. *The closed expression of the lower bound of ESC in the SWIPT network with PS-based relaying and FD jamming can be written as*

$$\bar{R}_{\text{sec}^l} \geq \frac{1}{2\ln 2} (K_1 - K_2), \quad (29)$$

where

$$K_1 = - \sum_{k=1}^N w_k e^{(1/m_x)(1+(a_1/b_1 m_y x_k))} \text{Ei}\left(-\frac{1}{m_x} \left(1 + \frac{a_1}{b_1 m_y x_k}\right)\right)$$

$$K_2 = \ln \left(1 + m_x \sum_{k=1}^N w_k \frac{m_z x_k}{m_j m_z z_k - m_q} \ln \left(\frac{m_j m_z x_k}{m_q}\right)\right), \quad (30)$$

where $m_j = b_2 m_y + 1$ and $m_q = m_w + a_2$.

Proof. See Appendix C.

The lower bound expression of ESC is too complicated to obtain intuitive information. Consequently, the asymptotic ESC when the transmit SNR goes to infinity is necessary. For the LEH model, the asymptotic form of ESC is

$$\bar{R}_{\text{sec}^L, \gamma_{\text{total}} \rightarrow \infty} \geq \frac{1}{2\ln 2} (H_1 - H_2), \quad (31)$$

where

$$H_1 = - \sum_{k=1}^N w_k \left(e^{(1/\tilde{m}_x \tilde{m}_y k_4 x_k)} \text{Ei}\left(-\frac{1}{\tilde{m}_x \tilde{m}_y k_4 x_k}\right) \right)$$

$$H_2 = \ln \left(1 + \left(\sum_{k=1}^N w_k \frac{\tilde{m}_z x_k}{\tilde{d} \tilde{m}_z \tilde{m}_z x_k - \tilde{m}_w \lambda} \ln \left(1 + \frac{\tilde{d} \tilde{m}_z \tilde{m}_z x_k - \tilde{m}_w \lambda}{\tilde{m}_w \lambda}\right) \right) \right), \quad (32)$$

where $k_4 = k_1/k_2$.

For the NLEH model, the asymptotic expression of ESC in the four-node SWIPT-enabled network is $\bar{R}_{\text{sec}^{\text{NL}}, \gamma_{\text{total}} \rightarrow \infty} = 0$. Refer to Appendix C for the derivation of asymptotic expressions of ESC under the PS policy.

From the asymptotic ESC under the LEH and NLEH models, the ESC in the NLEH mode is worsened to zero when the transmit SNR is extremely large. Therefore, it is irrational to increase the transmit SNR blindly to obtain high ESC. Although the closed expression of the lower bound of ESC presented in Proposition 3 is intricate, the closed-form one is able to achieve rapid calculation in popular mathematical software such as MATLAB, thereby providing an efficient method to acquire the ESC of the system and intuitive analysis of the effects about system parameters whereas avoiding the time-consuming Monte Carlo simulations. $\square$

3.2. Time-Switching Protocol

3.2.1. COP. For the TS policy, the channel capacity is $C_M = 1 - \alpha/2 \log_2(1 + \Gamma_{\mathcal{D}})$, and the factor $(1 - \alpha)/2$ stands for the effective time of the information transmission.

Proposition 4. *The closed-form expression for the COP of the SWIPT system with cooperative jamming under the TS scheme can be obtained as*

$$P_{\text{CO}}^l = 1 - \frac{1}{m_y} e^{-(\gamma_{\text{th}}^t/m_x)} \left(2 \left(\frac{\mu}{\gamma} \right)^{(1/2)} K_1(2\sqrt{\mu\gamma}) \right), \quad (33)$$

where $m_y = \lambda_{\mathcal{R}\mathcal{D}}$, $\gamma_{\text{th}}^t = 2^{(2R_t/(1-\alpha))} - 1$, $m_x = \gamma_{\mathcal{S}} \lambda_{\mathcal{S}\mathcal{R}}$, $\mu = \gamma_{\text{th}}^t a_1/m_x b_1$, $\nu = 1/m_y$, $a_1 = (k\gamma_{\mathcal{D}}^v + 1)(\gamma_{\Theta} + 1)$, and $b_1 = \gamma_{\mathcal{R}}^l$.

Proof. The proof obeys the same steps which are used to deduce the expression of COP under the PS strategy in Appendix A. Thus, we skip the proof for the TS policy for brevity.

Likewise, in the asymptotic case, the expression of COP under the LEH model is

$$P_{\text{CO}}^{L, \gamma_{\text{total}} \rightarrow \infty} = 1 - \frac{1}{\tilde{m}_y} \left(2 \left(\frac{\tilde{u}}{\tilde{\nu}} \right)^{(1/2)} K_1(2\sqrt{\tilde{u}\tilde{\nu}}) \right), \quad (34)$$

where $\tilde{m}_y = \lambda_{\mathcal{R}\mathcal{D}}$, $\tilde{u} = \gamma_{\text{th}}^t = k_2/\tilde{m}_x k_1$, $\tilde{\nu} = 1/\tilde{m}_y$, $\tilde{m}_x = \lambda_{\mathcal{S}\mathcal{R}}$, $k_1 = \xi \tilde{d}$, $k_2 = \lambda_{dd}(1 - \xi)\lambda$, and $\tilde{d} = 2\eta\alpha\lambda/(1 - \alpha)$.

The asymptotic-form expression of COP under the NLEH mode in the SWIPT system with FD jamming is $P_{\text{CO}}^{\text{NL}, \gamma_{\text{total}} \rightarrow \infty} = 1$. Refer to Appendix D for the derivation of asymptotic expressions of COP under the TS policy.

It can be clearly found from (33) that the system adopting the TS strategy is more prone to cause a break between the source and destination than that adopting the PS strategy due to the higher threshold in the case of the same minimum transmission rate, which inspires us to choose the two schemes (TS and PS) according to the actual information transfer rate. In the actual parameter setting, increasing α is capable of raising the threshold γ_{th}^t , which means meeting the requirements of secure communication between source and destination nodes is

more difficult; hence, interruptions are more likely to happen. $\square$

3.2.2. SOP

$$P_{SO}^I = \frac{m_x^2}{m_z(m_x + b_2 m_y \gamma_{th}^e)} e^{-(\gamma_{th}^e/m_x)} \sum_{k=1}^N w_k \frac{m_z^2 x_k}{\gamma_{th}^e m_w + m_x m_z x_k} e^{(-\gamma_{th}^e a_2/m_x m_z x_k)}, \quad (35)$$

where $\gamma_{th}^e = 2^{(2R_c/1-\alpha)} - 1$, $b_2 = \gamma_{\mathcal{D}}$, $a_2 = \gamma_{\Theta} + 1$, $m_z = \gamma_{\mathcal{R}}^I \lambda_{\mathcal{R}\mathcal{E}}$, and $m_w = a_2 \gamma_{\mathcal{D}} \lambda_{\mathcal{D}\mathcal{E}}$.

Proof. Similar to the derivation of SOP under the PS strategy.

Proposition 5. The SOP for the SWIPT system with TS-based relaying and FD destination-aided jamming is obtained as

In the high SNR regime with $P_{\text{total}} \rightarrow \infty$, the expression for SOP employing the TS scheme under the LEH model is

$$P_{SO}^{L, \gamma_{\text{total}} \rightarrow \infty} = \frac{1}{\tilde{m}_z} \frac{\tilde{m}_x k_3}{\gamma_{th}^e \tilde{m}_y + \tilde{m}_x k_3} \cdot \left(\frac{\gamma_{th}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z d k_3} e^{(\gamma_{th}^e \lambda \tilde{m}_w / \tilde{m}_x \tilde{m}_z d k_3)} \text{Ei} \left(-\frac{\gamma_{th}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z d k_3} \right) + \tilde{m}_z \right), \quad (36)$$

where $\tilde{m}_z = \lambda_{\mathcal{R}\mathcal{E}}$, $\tilde{m}_w = \lambda_{\mathcal{D}\mathcal{E}}$, and $k_3 = \xi/(1-\xi)$.

Under the NLEH model, the asymptotic expression of SOP adopting the TS policy is written as $P_{SO}^{NL, \gamma_{\text{total}} \rightarrow \infty} = 0$. Refer to Appendix D for the derivation of asymptotic expressions of SOP under the TS scheme.

For the TS policy, the SOP under the NLEH model drops to zero as the transmit SNR goes to infinity, while SOP under

the LEH converges to a deterministic value in the high SNR regime, which reminds us that increasing the transmit SNR appropriately can reduce the SOP in the practical nonlinear circuit design.

The expression for the TOP in the SWIPT with FD destination-aided jamming system utilizing the TS scheme is given by

$$P_{TO}^I = 1 - \frac{1}{m_y} e^{-(\gamma_{th}^e/m_x)} \left(2 \left(\frac{\mu}{\nu} \right)^{1/2} K_1(2\sqrt{\mu\nu}) \right) + \frac{m_x^2}{m_z(m_x + b_2 m_y \gamma_{th}^e)} e^{-(\gamma_{th}^e/m_x)} \sum_{k=1}^N w_k \frac{m_z^2 x_k}{\gamma_{th}^e m_w + m_x m_z x_k} e^{(-\gamma_{th}^e a_2/m_x m_z x_k)}. \quad (37)$$

The asymptotic form expressions for the TOP of the SWIPT-enabled network with the TS protocol under the LEH and NLEH models are

$$P_{TO}^{L, \gamma_{\text{total}} \rightarrow \infty} = 1 - \frac{1}{\tilde{m}_y} \left(2 \left(\frac{\tilde{u}}{\tilde{v}} \right)^{(1/2)} K_1(2\sqrt{\tilde{u}\tilde{v}}) \right) + \frac{\tilde{m}_x k_3}{\tilde{m}_z (\gamma_{th}^e \tilde{m}_y + \tilde{m}_x k_3)} \cdot \left(\frac{\gamma_{th}^e \lambda \tilde{m}_w}{\tilde{m}_x d k_3} e^{(\gamma_{th}^e \lambda \tilde{m}_w / \tilde{m}_x \tilde{m}_z d k_3)} \text{Ei} \left(-\frac{\gamma_{th}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z d k_3} \right) + \tilde{m}_z \right),$$

$$P_{TO}^{NL, \gamma_{\text{total}} \rightarrow \infty} = 1, \quad (38)$$

respectively.

The above analysis of the TS policy alerts us to quantify both the reliability and security at both the legitimate and eavesdropper separately, that is, allocating appropriate time spending on gathering energy to ensure a reliable communication and enough transmit SNR to guarantee that self-jamming signals can protect confidential information from wiretapping. $\square$

3.2.3. ESC. In the TS policy, the instantaneous secrecy rate $R_{\text{sec}} = (1-\alpha)/2 [\log_2(1 + \Gamma_{\mathcal{D}}^I) - \log_2(1 + \Gamma_{\mathcal{E}}^I)]$, which shows that the effective time is related to the TS ratio α .

Proposition 6. The analytical expression of ESC for the SWIPT system with FD destination-aided jamming under the TS scheme is given by

$$\bar{R}_{\text{sec}} \geq \frac{1-\alpha}{2\ln 2} (K_1 - K_2), \quad (39) \quad \text{where}$$

$$K_1 = -\frac{1}{m_y} \sum_{k=1}^N w_k e^{(1/m_x)(1+(a_1/b_1 m_y x_k))} \text{Ei}\left(-\frac{1}{m_x} \left(1 + \frac{a_1}{b_1 m_y x_k}\right)\right)$$

$$K_2 = \ln\left(1 + m_x \sum_{k=1}^N w_k \frac{m_z x_k}{m_j m_z x_k - m_q} \ln\left(\frac{m_j m_z x_k}{m_q}\right)\right), \quad (40)$$

where $m_j = b_2 m_y + 1$ and $m_q = m_w + a_2$.

As the proof is similar to the derivation for the lower bound of ESC under the PS strategy, it is omitted for the sake of brevity.

Now, the case of the transmit SNR going to infinity is considered, and the lower bound of ESC under the TS policy is approximated as

$$\bar{R}_{\text{sec}}^{L, \gamma_{\text{total}} \rightarrow \infty} \geq \frac{1-\alpha}{2\ln 2} (H_1 - H_2), \quad (41)$$

where

$$H_1 = -\sum_{k=1}^N w_k \left(e^{(1/\tilde{m}_x \tilde{m}_y k_4 x_k)} \text{Ei}\left(-\frac{1}{\tilde{m}_x \tilde{m}_y k_4 x_k}\right) \right),$$

$$H_2 = \ln\left(1 + \left(\sum_{k=1}^N w_k \frac{\tilde{m}_z \tilde{x}_j}{\tilde{m}_z \tilde{d} \tilde{m}_z x_j - \tilde{m}_w \lambda} \ln\left(1 + \frac{\tilde{m}_z \tilde{d} \tilde{m}_z x_k - \tilde{m}_w \lambda}{\tilde{m}_w \lambda}\right)\right)\right), \quad (42)$$

where $k_4 = k_1/k_2$.

For the NLEH model, the analytical expression for ESC in the high SNR regime under the TS policy is $\bar{R}_{\text{sec}}^{\text{NLEH}, \gamma_{\text{total}} \rightarrow \infty} = 0$. The proof is similar to the derivation for asymptotic expression ESC under the PS strategy, which is omitted here.

It can be clearly found from analytical expressions that the TS ratio α not only affects ESC by influencing the instantaneous SNR at the destination but also directly determines ESC as an effective time factor. Therefore, comparing with the PS strategy, the fluctuation in ESC under the TS scheme with α is more obvious. Hence, the TS ratio α must be carefully designed based on the actual environment to achieve the optimal ESC.

4. Discussion and Results

In this section, the correctness of the analytical expressions is demonstrated by Monte Carlo simulations and the impacts with respect to the PS/TS ratio and transmit SNR on the secrecy performance of the SWIPT-enabled system with FD destination-aided jamming are represented. As depicted in the following figures, theoretical results are in exact agreement with the numerical simulations, which shows that the closed expressions are correct. Unless otherwise specified, we set the default parameters according to [25, 37] as follows: $\eta = 0.7$, $\xi = 0.5$, $d_{ij} = 5\text{m}$, $\mathcal{L} = 2.7$, $\rho = 0.4$, $\alpha = 0.4$, $\sigma^2 = -90\text{ dBm}$, $R_t = 3\text{ bps/Hz}$, and $R_s = 2.5\text{ bps/Hz}$. In the legend of the following figures, “Sim.” and “Ana.” stand for

the Monte Carlo simulations and results of analytical expressions, respectively.

4.1. Transmit SNR. Figure 4 plots the COP versus the transmit SNR under the LEH and NLEH models adopting both the PS- and TS-based schemes. For the NLEH model, the initial value of the COP decreases to the minimum at the beginning as the transmit SNR grows and then gives enlarged returns with further increase in the transmit SNR. For the LEH one, the original COP keeps decreasing with the SNR ascending until it converges to an exact value. The reason for the different variations of COP under the two EH models is that the information signal has a greater positive effect on the destination at first and benefits the reliability, while with the further rising of transmit SNR, the negative effect of the interference signal becomes more pronounced, which is reflected in the fact that the curve either reverses change or keeps equilibrium, after reaching the extreme value. One can also note that the COP under the TS scheme is larger than that under the PS.

Figure 5 examines that the SOP under different EH models varies quite significantly. The SOP in the LEH model increases rapidly with the ascending of the transmit SNR, attaining its maximum and keeping constant. By contrast, in the NLEH model, SOP gradually decreases to zero after reaching the maximum value. It is also discovered that the analytical results of SOPs can tally well with the asymptotic

FIGURE 4: COP versus the transmit SNR.

FIGURE 6: TOP versus the transmit SNR.

FIGURE 5: SOP versus the transmit SNR.

results as $\gamma_{total} \rightarrow \infty$ when the transmit SNR is high enough. Due to the addition of the self-interference signal, the overall SOP is relatively small.

Figure 6 shows the TOP versus the transmit SNR under the LEH and NLEH models adopting both the PS- and TS-based schemes. The TOP is determined jointly by both the COP and SOP, and the trend of the TOP curve is similar to that of the COP in Figure 4, which inspires us to weigh the

SOP and COP according to the actual situation to get desirable safety. One interesting observation is that the result of the TS-based scheme achieves lower than that of the PS-based scheme under the same condition.

The relationship between the ESC and transmit SNR is shown in Figure 7. The ESC curve shows a positive growth before reaching the extreme value. After accomplishing the peak value, the ESC in the LEH model hardly changes, while the ESC of the NLEH one drops to zero gradually. This is because the negative influence of the interference signal on the ESC, and the positive influence of the source signal cancel out each other into a saturation region eventually under the LEH model. However, when the SNR is high, the effect of useful signals is slight, while the effect of noisy signals is dominant, resulting in a decrease in the ESC under the NLEH model.

From the above analysis, for different models, the higher transmit SNR does not signify better performance. Apparently, increasing the transmit SNR blindly may cause a waste of resources as well as performance degradation.

4.2. Power-Splitting Ratio (ρ)/Time-Switching Ratio (α). Figure 8 shows the impacts of the PS ratio ρ and TS ratio α on the COP. It can be clearly found from Figure 8(a) that the COPs under the LEH model are more sensitive to the PS ratio or TS ratio. Figure 8(b) shows that, (1) for the TS, the COP first goes down and then climbs up as α becomes large. This is because increasing α enhances transmission power at the relay, while cutting down the effective communication time. (2) For the PS, increasing ρ can better suppress the occurrence of connection interruption, especially, under the linear model. The reason is that a greater PS ratio ρ means the relay can obtain more energy and the effective

FIGURE 7: ESC versus the transmit SNR.

FIGURE 8: COP versus ρ/α . (a) Transmit SNR = 60 dB. (b) Transmit SNR = 110 dB.

communication time is unimpeded by ρ , which makes the end-to-end SNR at the destination higher.

Figure 9 is provided to observe the impacts of the PS ratio ρ and TS ratio α on the SOP. In Figure 9(a), it can be obviously found that, (1) for the PS, the SOP has positive correlation with ρ . This is because increasing the PS ratio ρ means more power for energy harvesting and less power for information processing which continuously reduces the ability of the relay to receive signals, thereby making the SOP rapidly increase. (2) For the TS, once α crosses a fixed value,

the SOP begins to degrade as α rises. The reason is that increasing α degrades the strength of the received signal at the relay and makes the eavesdropping channel of the relay worsen, which results in the SOP reducing. In Figure 9(b), the variation of SOP with α is nonlinear as the TS ratio α influences the whole communication processes.

Figure 10 plots the regularities of the TOP in the PS ratio ρ and TS ratio α . The curves of TOP are similar to that of the COP under the corresponding transmit SNR. This is because the TOP is the resultant of the COP and SOP.

FIGURE 9: SOP versus ρ/α . (a) Transmit SNR = 60 dB. (b) Transmit SNR = 110 dB.

FIGURE 10: TOP versus ρ/α . (a) Transmit SNR = 60 dB. (b) Transmit SNR = 110 dB.

Figure 11 illustrates the achievable ESC for both the PS and TS schemes versus the ρ and α , respectively. The ESC is limited by a secrecy capacity ceiling when ρ or α goes beyond

a specific threshold. It should be noted that properly increasing α or ρ can effectively improve the ESC of the SWIPT system with FD destination-aided jamming. However, for

FIGURE 11: ESC versus ρ/α . (a) Transmit SNR = 60 dB. (b) Transmit SNR = 110 dB.

the TS scheme, a high time conversion rate leads to short effective time of information transmission, and the ESC drops sharply.

5. Conclusion

We have investigated the secrecy performance of the relay system with FD destination-aided jamming, where both the LEH and NLEH models have been considered in the energy-constrained relay. The closed-form expressions for the COP, SOP, TOP, and lower bound of ESC have been derived selecting both the PS and TS protocols. Monte Carlo simulations confirmed the correctness of the derived expression, and analytical results reveal the influence of network parameters on the secrecy performance, which provides some insights in the actual design. For instance, increasing the transmission SNR does not necessarily improve the security and reliability of the system and may even worsen them. Enhancing the intensity of the AN signal at the destination can benefit the security of the system, but can erode the reliability. The energy harvesting model adopted by the relay has a great influence on the secrecy performance of the system. For the future work, we would introduce the intelligent reflecting surface into our network to design a security scheme and achieve the optimal power transfer efficiency and secrecy capacity. In addition, it would be interesting to analyze the secrecy performance in the context of multi-users scenarios with the intelligent reflecting surface.

Appendix

A

The proof for the analytical expressions of COP under the PS-based scheme in general and asymptotic cases is in the following.

We let $X = (1 - \rho)\gamma_{\mathcal{S}}|h_{\mathcal{S}\mathcal{R}}|^2$ and $Y = |h_{\mathcal{R}\mathcal{D}}|^2$. According to the properties of CDF and the probability density function (PDF), X and Y follow the exponential distribution, where $E\{X\} = m_x$ and $E\{Y\} = m_y$. Hence, the COP in (17) is rewritten as

$$\begin{aligned} P_{CO} &= \Pr\left\{\frac{b_1 XY}{b_1 Y + a_1} < \gamma_{th}^t\right\} \\ &= 1 - \frac{1}{m_y} \int_0^\infty e^{-(\gamma_{th}^t (b_1 + a_1/y)/m_x b_1)} e^{-y/m_y} dy \\ &= 1 - \frac{1}{m_y} e^{-(\gamma_{th}^t/m_x)} \int_0^\infty e^{-(\gamma_{th}^t a_1/m_x b_1 y)} e^{-(y/m_y)} dy. \end{aligned} \quad (\text{A.1})$$

In this way, the issue of obtaining the closed-form of COP is turned to a mathematical problem of two-dimensional probability calculation. Letting $\mu = \gamma_{th}^t a_1/m_x b_1$ and $\nu = 1/m_y$ and utilizing Eq. 3.324.1 in [35], the analytical expression of COP is represented as

$$P_{CO} = 1 - \frac{1}{m_y} e^{-(\gamma_{th}^t/m_x)} \left(2\left(\frac{\mu}{\nu}\right)^{(1/2)} K_1(2\sqrt{\mu\nu})\right). \quad (\text{A.2})$$

To get the asymptotic expression of COP, the instantaneous SNR at the destination with $P_{\text{total}} \rightarrow \infty$ is written as

$$\Gamma_{\mathcal{D}}^{I, \gamma_{\text{total}} \rightarrow \infty} = \frac{(1 - \rho)\xi\gamma_{\text{total}}\gamma_{\mathcal{R}}^I |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2}{\gamma_{\mathcal{R}}^I |h_{\mathcal{R}\mathcal{D}}|^2 + k(1 - \xi)\gamma_{\text{total}}(1 - \rho)\gamma_{\mathcal{D}}^I}, \quad (\text{A.3})$$

where $\gamma_{\text{total}} = P_{\text{total}}/\sigma^2$.

Based on equations (2) and (5), one can get

$$\gamma_{\mathcal{R}}^{\gamma_{\text{total}}} \rightarrow \infty = \begin{cases} \eta\rho\lambda\gamma_{\text{total}}, & \text{LEH,} \\ p_1, & \text{NLEH.} \end{cases} \quad (\text{A.4})$$

Substituting (A.4) into (A.3), then $\Gamma_{\mathcal{D}}^{\gamma_{\text{total}} \rightarrow \infty}$ is further written as

$$\Gamma_{\mathcal{D}}^{L, \gamma_{\text{total}} \rightarrow \infty} = \frac{\xi \bar{d} |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2}{\lambda_{dd} (1 - \xi) \lambda}, \quad (\text{A.5})$$

$$\Gamma_{\mathcal{D}}^{\text{NL}, \gamma_{\text{total}} \rightarrow \infty} = \frac{(1 - \rho) \xi \bar{d} |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2}{\lambda_{dd} (1 - \xi) \gamma_{\text{total}} (1 - \rho) \lambda} = 0. \quad (\text{A.6})$$

According to (9), $P_{\text{CO}}^{L, \gamma_{\text{total}} \rightarrow \infty}$ is described as

$$\begin{aligned} P_{\text{CO}}^{L, \gamma_{\text{total}} \rightarrow \infty} &= \Pr \left\{ \frac{\xi \bar{d} |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2}{\lambda_{dd} (1 - \xi) \lambda} < \gamma_{\text{th}}^t \right\} \\ &= \Pr \left\{ \frac{k_1 \tilde{X} \tilde{Y}}{k_2} < \gamma_{\text{th}}^t \right\} \\ &= 1 - \frac{1}{\tilde{m}_y} \int_0^\infty e^{-(\gamma_{\text{th}}^t k_2 / \tilde{m}_x k_1 y)} e^{-(y / \tilde{m}_y)} dy \quad (\text{A.7}) \\ &= 1 - \frac{1}{\tilde{m}_y} \int_0^\infty e^{-(\tilde{u} / y)} e^{-\tilde{v} y} dy \\ &= 1 - \frac{1}{\tilde{m}_y} \left(2 \left(\frac{\tilde{u}}{\tilde{v}} \right)^{(1/2)} K_1 (2 \sqrt{\tilde{u} \tilde{v}}) \right), \end{aligned}$$

where $\tilde{X}$ and $\tilde{Y}$ follow the exponential distributions, $\mathbb{E}\{\tilde{X}\} = \tilde{m}_x$, and $\mathbb{E}\{\tilde{Y}\} = \tilde{m}_y$. The tilde $\sim$ is attached on the variables in the asymptotic analysis to distinguish from those in the precise analysis.

B

The proof for the analytical expressions of SOP under the PS-based scheme in general case and asymptotic case is in the following.

Similar to the way of deriving the closed-form expression of COP, the following exponential distributions $Z = \gamma_{\mathcal{R}}^t |h_{\mathcal{R}\mathcal{E}}|^2$ and $W = a_2 \gamma_{\mathcal{D}} |h_{\mathcal{D}\mathcal{E}}|^2$ are introduced, where the means of Z and W are $\gamma_{\mathcal{R}}^t \lambda_{\mathcal{R}\mathcal{E}}$ and $a_2 \gamma_{\mathcal{D}} \lambda_{\mathcal{D}\mathcal{E}}$, respectively. Thus, the SOP in (20) is rewritten as

$$P_{\text{SO}} = 1 - \Pr \left\{ \frac{XZ}{b_2 YZ + Z + W + a_2} < \gamma_{\text{th}}^e \right\}. \quad (\text{B.1})$$

After further mathematical manipulations, P_{SO} is expressed as

$$\begin{aligned} P_{\text{SO}} &= 1 - \Pr \left\{ X < \gamma_{\text{th}}^e \left(b_2 Y + 1 + \frac{(W + a_2)}{Z} \right) \right\} \\ &= \frac{1}{m_z} \frac{m_x^2}{m_x + b_2 m_y \gamma_{\text{th}}^e} e^{-(\gamma_{\text{th}}^e / m_x)} \int_0^\infty \frac{z}{m_x z + m_w \gamma_{\text{th}}^e} e^{-(z / m_z)} e^{-(a_2 \gamma_{\text{th}}^e / m_x z)} dz. \end{aligned} \quad (\text{B.2})$$

To compute the complicated integrals in (B.2), the Gauss-Laguerre quadrature is utilized, which is an extension of the Gaussian quadrature method for approximating the value of integrals and defined as

$$\int_0^{+\infty} e^{-x} f(x) dx \approx \sum_{i=1}^N \omega_i f(x_i), \quad (\text{B.3})$$

where x_i is the i -th root of Laguerre polynomial $L_n(x)$ as $L_n(x) = e^x d^n/dx^n (x^n e^{-x})$; the weight ω_i is given by Abramowitz and Stegun [38] as $\omega_i = x_i / (n+1)^2 [L_{n+1}(x_i)]^2$, and N determines the precision and accuracy of the calculation result [39]. Based on equation (B.3), the closed-form expression of P_{SO} is approximated as

$$P_{\text{SO}} \approx \frac{1}{m_z} \frac{m_x^2}{m_x + b_2 m_y \gamma_{\text{th}}^e} e^{-(\gamma_{\text{th}}^e / m_x)} \sum_{k=1}^N w_k \frac{m_z^2 x_k}{\gamma_{\text{th}}^e m_w + m_x m_z x_k} e^{(-\gamma_{\text{th}}^e a_2 / m_x m_z x_k)}. \quad (\text{B.4})$$

To certify asymptotic-form expressions of the SOP, the end-to-end SNR at the eavesdropper when the transmit SNR goes to infinity is obtained as

$$\Gamma_{\mathcal{E}}^{L, \gamma_{\text{total}} \rightarrow \infty} = \frac{\xi \bar{d} |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2}{\bar{d} (1 - \xi) |h_{\mathcal{R}\mathcal{D}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2 + \lambda (1 - \xi) |h_{\mathcal{D}\mathcal{E}}|^2}, \quad (\text{B.5})$$

where $\Gamma_{\mathcal{E}}^{\text{NL}, \gamma_{\text{total}} \rightarrow \infty} = 0$; then, $P_{\text{SO}}^{L, \gamma_{\text{total}} \rightarrow \infty}$ is given by

$$\begin{aligned} P_{\text{SO}}^{L, \gamma_{\text{total}} \rightarrow \infty} &= \Pr \left\{ \frac{1}{2} \log_2 (1 + \Gamma_{\mathcal{E}}^{L, \gamma_{\text{total}} \rightarrow \infty}) \geq R_e \right\} \\ &= 1 - \Pr \left\{ \frac{\xi \bar{d} \tilde{X} \tilde{Z}}{\bar{d} (1 - \xi) \tilde{Y} \tilde{Z} + \lambda (1 - \xi) \tilde{W}} < \gamma_{\text{th}}^e \right\} \\ &= 1 - \Pr \left\{ \underbrace{\frac{k_3 \bar{d} \tilde{X} \tilde{Z}}{\bar{d} \tilde{Y} \tilde{Z} + \lambda \tilde{W}}}_{I_1} < \gamma_{\text{th}}^e \right\}, \end{aligned} \quad (\text{B.6})$$

where exponential distributions are $\tilde{Z} = |h_{\mathcal{R}\mathcal{E}}|^2$, $\tilde{W} = |h_{\mathcal{D}\mathcal{E}}|^2$, $\mathbb{E}(\tilde{Z}) = \tilde{m}_z = \lambda_{\mathcal{R}\mathcal{E}}$, and $\mathbb{E}(\tilde{W}) = \tilde{m}_w = \lambda_{\mathcal{R}\mathcal{E}}$.

By the probability theory and Eq. 3.353.5 in [35], we can get

$$I_1 = 1 - \left(\frac{\tilde{m}_x k_3}{\gamma_{\text{th}}^e \tilde{m}_y + \tilde{m}_x k_3} \right) \left(\frac{\gamma_{\text{th}}^e \lambda \tilde{m}_w}{\tilde{m}_z \tilde{m}_x dk_3} e^{(\gamma_{\text{th}}^e \lambda \tilde{m}_w / \tilde{m}_x \tilde{m}_z dk_3)} \text{Ei} \left(-\frac{\gamma_{\text{th}}^e \lambda \tilde{m}_w}{\tilde{m}_x \tilde{m}_z dk_3} \right) + 1 \right). \quad (\text{B.7})$$

C

The proof for the analytical expressions of ESC under the PS-based scheme in the general case and asymptotic case is in the following.

Calculation of the ESC is divided into two parts, i.e., $\mathcal{E}\{\ln(1 + \Gamma_{\mathcal{D}}^l)\}$ and $\mathcal{E}\{\ln(1 + \Gamma_{\mathcal{E}}^l)\}$. Based on equation (B.3), the former part is calculated as

$$\begin{aligned} \mathbb{E}\{\ln(1 + \Gamma_{\mathcal{D}}^l)\} &= \mathbb{E}\left\{ \ln \left(1 + \frac{b_1 XY}{b_1 Y + a_1} \right) \right\} \\ &= \frac{1}{m_x m_y} \int_0^\infty \int_0^\infty \ln \left(1 + \frac{b_1 xy}{b_1 y + a_1} \right) e^{-(x/m_y)} e^{-(y/m_x)} dx dy \\ &= -\frac{1}{m_y} \int_0^\infty e^{(1/m_y)(1 + (a_1/b_1)y)} \text{Ei} \left(-\frac{1}{m_x} \left(1 + \frac{a_1}{b_1 y} \right) \right) e^{-(y/m_y)} dy \\ &= -\sum_{k=1}^N w_k e^{(1/m_x)(1 + (a_1/b_1 m_y x_k))} \text{Ei} \left(-\frac{1}{m_x} \left(1 + \frac{a_1}{b_1 m_y x_k} \right) \right). \end{aligned} \quad (\text{C.1})$$

According to Jensen's inequality, $\mathbb{E}\{\ln(1 + \Gamma_{\mathcal{E}}^l)\} \leq \ln(1 + \mathcal{E}(\Gamma_{\mathcal{E}}^l))$ is obtained since $\ln(1 + x)$ is a concave function with

respect to x . Substituting X , Y , Z , and W into $\mathcal{E}\{\ln(1 + \Gamma_{\mathcal{E}}^l)\}$, it is formulated as

$$\begin{aligned}\mathbb{E}\{\ln(1 + \Gamma_\epsilon^l)\} &= \mathbb{E}\left\{\ln\left(1 + \frac{XZ}{b_2YZ + Z + W + a_2}\right)\right\} \leq \ln\left(1 + \underbrace{\mathbb{E}\left(\frac{XZ}{b_2YZ + Z + W + a_2}\right)}_{I_2}\right), \\ I_2 &= \mathbb{E}\left\{\frac{XZ}{b_2YZ + Z + W + a_2}\right\}, \\ &= m_x \underbrace{\mathbb{E}\left\{\frac{Z}{b_2YZ + Z + W + a_2}\right\}}_{I_3}.\end{aligned}\tag{C.2}$$

Letting $J = b_2Y + 1$ and $Q = W + a_2$, I_3 is represented as

$$\begin{aligned}I_3 &= \mathbb{E}\left(\frac{Z}{ZJ + Q}\right) \\ &= \underbrace{\frac{1}{m_z m_j m_q} \int_0^\infty \int_0^\infty \int_0^\infty \frac{z}{zj + q} e^{-(z/m_z)} e^{-(j/m_j)} e^{-(q/m_q)} dz dj dq}_{I_4}.\end{aligned}\tag{C.3}$$

Based on Eq. 3.352.4 in [35] and Gauss-Laguerre quadrature, I_4 is derived by

$$\begin{aligned}I_4 &= \frac{1}{m_z m_j m_q} \int_0^\infty e^{-(z/m_z)} \int_0^\infty \left(-e^{(1/m_j)(q/z)} \text{Ei}\left(-\frac{q}{m_j z}\right)\right) e^{-(q/m_q)} dq dz \\ &= \frac{1}{m_z} \int_0^\infty e^{-(z/m_z)} \left(\frac{z}{m_j z - m_q} \ln\left(\frac{m_j z}{m_q}\right)\right) dz \\ &= \sum_{k=1}^N w_k \frac{m_z x_k}{m_j m_z x_k - m_q} \ln\left(\frac{m_j m_z x_k}{m_q}\right).\end{aligned}\tag{C.4}$$

The asymptotic form expression of ESC is composed of H_1 and H_2 , and the term H_1 is obtained by

$$\begin{aligned}H_1 &= \mathbb{E}\{\ln(1 + \Gamma_{\mathcal{D}}^{L, \gamma_{\text{total}} \rightarrow \infty})\} \\ &= \frac{1}{\tilde{m}_x \tilde{m}_y} \int_0^\infty \int_0^\infty \ln(1 + k_4 xy) e^{-(x/\tilde{m}_x)} e^{-(y/\tilde{m}_y)} dx dy \\ &= - \sum_{k=1}^N w_k \left(\frac{1}{e^{\tilde{m}_x \tilde{m}_y k_4 x_k} \text{Ei}\left(-\frac{1}{\tilde{m}_x \tilde{m}_y k_4 x_k}\right)} \right),\end{aligned}\tag{C.5}$$

where the integration by parts method and Gauss-Laguerre quadrature are applied to compute the double integral in the second step.

Furthermore, the term H_2 is acquired by

$$H_2 = \ln\left(1 + \underbrace{\mathbb{E}\{\Gamma_{\mathcal{E}}^{L, \gamma_{\text{total}} \rightarrow \infty}\}}_{I_5}\right),\tag{C.6}$$

where I_5 is computed by Eq. 5.231.1 in [35] and Gauss-Laguerre quadrature and can be given by

$$\begin{aligned}I_5 &= \mathbb{E}\left\{\frac{\xi \bar{d} |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2}{\bar{d}(1 - \xi) |h_{\mathcal{R}\mathcal{D}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2 + \lambda(1 - \xi) |h_{\mathcal{D}\mathcal{E}}|^2}\right\} \\ &= \sum_{k=1}^N w_k \frac{\tilde{m}_z x_k}{\tilde{m}_z \bar{d} \tilde{m}_z x_k - \tilde{m}_w \lambda} \ln\left(1 + \frac{\tilde{m}_z \bar{d} \tilde{m}_z x_k - \tilde{m}_w \lambda}{\tilde{m}_w \lambda}\right).\end{aligned}\tag{C.7}$$

D

The proof for the asymptotic-form expressions under the TS-based scheme is in the following.

For the TS-based protocol, as γ_{total} tends to infinity, the end-to-end SNR at the destination is

$$\Gamma_{\mathcal{D}}^{L, \gamma_{\text{total}} \rightarrow \infty} = \frac{\xi \gamma_{\text{total}} \gamma_{\mathcal{R}}^L |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2}{\gamma_{\mathcal{R}}^L |h_{\mathcal{R}\mathcal{D}}|^2 + k(1 - \xi) \gamma_{\text{total}} \gamma_{\Theta}}, \quad (\text{D.1})$$

and the transmission power at the relay in the asymptotic case is

$$\gamma_{\mathcal{R}}^{L, \gamma_{\text{total}} \rightarrow \infty} = \begin{cases} \frac{2\eta\alpha\lambda}{1 - \alpha} \gamma_{\text{total}}, & \text{LEH,} \\ \frac{2\alpha p_1}{1 - \alpha}, & \text{NLEH.} \end{cases} \quad (\text{D.2})$$

Accordingly, D.1 is rewritten as $\Gamma_{\mathcal{D}}^{L, \gamma_{\text{total}} \rightarrow \infty} = \xi \bar{d} |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{D}}|^2 / \lambda_d (1 - \xi) \lambda$ and $\Gamma_{\mathcal{D}}^{\text{NL}, \gamma_{\text{total}} \rightarrow \infty} = 0$. The remaining deducing steps are similar to the asymptotical derivation of COP under the PS scheme in Appendix A, which are omitted here.

To obtain the asymptotic expression of SOP under the TS-based scheme, the instantaneous SNRs at eavesdropper are reformulated as $\Gamma_{\mathcal{E}}^{L, \gamma_{\text{total}} \rightarrow \infty} = \xi \bar{d} |h_{\mathcal{S}\mathcal{R}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2 / \bar{d} (1 - \xi) |h_{\mathcal{R}\mathcal{D}}|^2 |h_{\mathcal{R}\mathcal{E}}|^2 + \lambda (1 - \xi) |h_{\mathcal{D}\mathcal{E}}|^2$ and $\Gamma_{\mathcal{E}}^{\text{NL}, \gamma_{\text{total}} \rightarrow \infty} = 0$. For more detailed derivations, refer to the formula-deduced process of SOP in the asymptotic case under the PS strategy in Appendix B.

Data Availability

No data were used to support the findings of the study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Advanced Research Project of Civil Aerospace Technologies in 13th Five-Year Plan (D010201) and Special Foundation for Chongqing Science and Technology Talent (cstc2019yszx-jcyjX0006 and cstc2020yszx-jscxX0004).

References

- [1] S. A. A. Kazmi and S. Coleri, "Optimization of full-duplex relaying system with non-linear energy harvester," *IEEE Access*, vol. 8, pp. 201566–201576, 2020.
- [2] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, C. Symeon, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): recent advances and future challenges," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 264–302, 2018.
- [3] D. N. Hanh, H. V. Khuong, and D. D. Thiem, "Secrecy analysis of overlay mechanism in radio frequency energy harvesting networks with jamming under Nakagami-m fading," *Wireless Personal Communications*, 2021.
- [4] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 1989–2001, 2013.
- [5] H. H. Jang, K. W. Choi, and D. I. Kim, "Novel frequency-splitting SWIPT for overcoming amplifier nonlinearity," *IEEE Wireless Communication Letters*, vol. 6, no. 9, pp. 826–829, 2020.
- [6] P. Tedeschi, S. Sciancalepore, and R. D. Pietro, "Security in energy harvesting networks: a survey of current solutions and research challenges," *IEEE Communication Surveys and Tutorials*, vol. 22, no. 4, pp. 2658–2693, 2020.
- [7] L. R. Varshney, "Transporting information and energy simultaneously," in *Proceedings of the 2008 IEEE International Symposium On Information Theory (ISIT)*, pp. 1612–1616, Toronto, Ontario, Canada, July 2008.
- [8] S. Bi, Y. Zeng, and R. Zhang, "Wireless powered communication networks: an overview," *IEEE Wireless Communication*, vol. 2, no. 23, pp. 10–18, 2016.
- [9] S. Bi, C. Ho, and R. Zhang, "Wireless powered communication: opportunities and challenges," *IEEE Communications Magazine*, vol. 4, no. 53, pp. 117–125, 2015.
- [10] X. Lu, P. Wang, D. Niyato et al., "Wireless networks with RF energy harvesting: a contemporary survey," *IEEE Communication Surveys and Tutorials*, vol. 2, no. 17, pp. 757–789, 2015.
- [11] X. Chen, D. W. K. Ng, and H. H. Chen, "Secrecy wireless information and power transfer: challenges and opportunities," *IEEE Communications Magazine*, vol. 2, no. 23, pp. 51–61, 2016.
- [12] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Transactions on Vehicular Technology*, vol. 1, no. 65, pp. 180–190, 2016.
- [13] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Transactions on Signal Processing*, vol. 7, no. 62, pp. 1850–1863, 2014.
- [14] Q. Shi, W. Xu, J. Wu et al., "Secure beamforming for MIMO broadcasting with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 5, no. 14, pp. 2841–2853, 2015.
- [15] Y. Wu and Y. Huo, "A survey of cooperative jamming-based secure transmission for energy-limited systems," *Wireless Communication and Mobile Computing*, vol. 2021, Article ID 6638405, 11 pages, 2021.
- [16] X. Qiu, T. Jiang, and W. Zou, "Physical layer security in simultaneous wireless information and power transfer networks," in *Proceedings of the 2017 17th International Symposium On Communications and Information Technologies (ISCIT)*, pp. 1–4, Cairns, Australia, September 2017.
- [17] H. Niu, B. Zhang, K. K. Wong, and F. Zhou, "Robust AN-aided secure beamforming and power splitting in wireless-powered AF relay networks," *IEEE Systems Journal*, vol. 3, no. 13, pp. 2543–2546, 2019.
- [18] H. Niu, B. Zhang, D. Guo et al., "Joint robust design for secure AF relay networks with SWIPT," *IEEE Access*, vol. 5, pp. 9369–9377, 2017.
- [19] K. Lee, J. Hong, H. Choi et al., "Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 2793–2803, 2018.
- [20] R. Ma, H. Wu, J. Ou et al., "Power splitting-based SWIPT systems with full-duplex jamming," *IEEE Transactions on Vehicular Technology*, vol. 9, no. 69, pp. 9822–9836, 2020.

- [21] W. Yang, W. Mou, X. Xu et al., "Energy efficiency analysis and enhancement for secure transmission in SWIPT systems exploiting full duplex techniques," *IET Communications*, vol. 14, no. 10, pp. 1712–1720, 2016.
- [22] H. Wu, L. Wang, R. Ma et al., "Full-duplex destination-aided jamming scheme for SWIPT-enabled relay networks," in *Proceedings of the 2020 IEEE Global Communications Conference*, pp. 1–6, Taipei, Taiwan, December-2020.
- [23] T. M. Hoang, X. N. Tran, B. C. Nguyen et al., "On the performance of MIMO full-duplex relaying system with SWIPT under outdated CSI," *IEEE Transactions on Vehicular Technology*, vol. 12, no. 69, Article ID 15580, 2020.
- [24] L. Wang, Y. Cai, Y. Zou et al., "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259–6274, 2016.
- [25] S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Transactions on Vehicular Technology*, vol. 3, no. 66, pp. 2199–2213, 2017.
- [26] K. Song, M. Nie, J. Jiang et al., "On the secrecy for relay-aided SWIPT Internet of Things system with cooperative eavesdroppers," *IEEE Access*, vol. 9, Article ID 28204, 2021.
- [27] R. Zhao, X. Tan, D. Chen et al., "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," *IEEE Transactions on Vehicular Technology*, vol. 12, no. 67, Article ID 11511, 2018.
- [28] S. Atapattu, N. Ross, Y. Jing et al., "Source-based jamming for physical-layer security on untrusted full-duplex relay," *IEEE Communications Letters*, vol. 5, no. 23, pp. 842–846, 2019.
- [29] S. Atapattu, P. Dharmawansa, M. D Renzo et al., "Multi-user relay selection for full-duplex radio," *IEEE Transactions on Communications*, vol. 2, no. 67, pp. 955–972, 2019.
- [30] A. A. Nasir, X. Zhou, S. Durrani et al., "Wireless-powered relays in cooperative communications: time-switching relaying protocols and throughput analysis," *IEEE Transactions on Communications*, vol. 5, no. 63, pp. 1607–1622, 2015.
- [31] X. Tang, W. Yang, Y. Cai et al., "Security of full-duplex jamming SWIPT system with multiple non-colluding eavesdroppers," in *Proceedings of the 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 66–69, Macau, China, July 2017.
- [32] E. Boshkovska, D. W. K. Ng, N. Zlatanov et al., "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2082–2085, 2015.
- [33] Y. Chen, N. Zhao, and M. Alouini, "Wireless energy harvesting using signals from multiple fading channels," *IEEE Transactions on Communications*, vol. 11, no. 65, pp. 5027–5039, 2017.
- [34] Y. Gu and S. Aissa, "RF-based energy harvesting in decode-and-forward relaying systems: ergodic and outage capacities," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6425–6434, 2015.
- [35] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic, New York, NY, USA, 8th edition, 2015.
- [36] R. Ma, S. Yang, M. Du et al., "Improving physical layer security jointly using full-duplex jamming receiver and multi-antenna jammer in wireless networks," *IET Communications*, vol. 10, no. 13, pp. 1530–1536, 2019.
- [37] M. Tatar Mamaghani, A. Kuhestani, and K. Wong, "Secure two-way transmission via wireless-powered untrusted relay and external jammer," *IEEE Transactions on Vehicular Technology*, vol. 9, no. 67, pp. 8451–8465, 2018.
- [38] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, Dover Publications, New York, NY, USA, 2th edition, 1965.
- [39] D. Conte, L. G. Ixaru, B. Paternoster et al., "Exponentially-fitted Gauss-Laguerre quadrature rule for integrals over an unbounded interval," *Journal of Computational and Applied Mathematics*, vol. 1, no. 255, pp. 725–736, 2014.