IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 13, 2022, accepted February 25, 2022, date of publication February 28, 2022, date of current version March 8, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3155498

Impact of Self-Energy Recycling and Cooperative Jamming on SWIPT-Based FD Relay Networks With Secrecy Constraints

ISABELLA WANDERLEY GOMES DA SILVA[1], **(Student Member, IEEE),**
JOSÉ DAVID VEGA SÁNCHEZ[2], **(Student Member, IEEE),**
EDGAR EDUARDO BENITEZ OLIVO[1], **(Member, IEEE),**
AND DIANA PAMELA MOYA OSORIO[3], **(Member, IEEE)**
[1]São Paulo State University (UNESP), Campus of São João da Boa Vista, São João da Boa Vista 13876-750, Brazil
[2]Departamento de Electrónica, Telecomunicaciones y Redes de Información, Escuela Politécnica Nacional (EPN), Quito 170525, Ecuador
[3]Centre for Wireless Communications (CWC), University of Oulu, 90014 Oulu, Finland

Corresponding author: Diana Pamela Moya Osorio (diana.moyaosorio@oulu.fi)

This work was supported in part by the Academy of Finland, 6G Flagship, under Grant 318927; in part by the FAITH Project under Grant 334280; and in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 421850/2018-3.

ABSTRACT This paper investigates the secrecy performance of a power splitting-based simultaneous wireless information and power transfer cooperative relay network in the presence of an eavesdropper. The relay is considered to operate in full-duplex (FD) mode to perform both energy harvesting and information decoding simultaneously. To accomplish that, the relay is assumed to employ two rechargeable batteries, which switch between power supplying mode and charging mode at each transmission block. We also assume that the self-interference inherent of the FD mode is not completely suppressed. Therefore, it is assumed that, after some stages of passive and active self-interference cancellation, there is still a residual self-interference (RSI). A portion of this RSI (remaining after passive cancellation) is recycled for energy harvesting. In order to improve the system secrecy performance, it is considered that the relay can split its transmit power to send the information signal and to emit a jamming signal to degrade the eavesdropper's channel. The secrecy performance is evaluated in terms of the secrecy outage probability and the optimal secrecy throughput. Tight-approximate and asymptotic expressions are obtained for the secrecy outage probability, and the particle swarm optimization method is employed for addressing the secrecy throughput optimization problem. From numerical results, we show that the secrecy performance can be increased depending on the self-energy recycling channel condition. Finally, our derived expressions are validated via Monte Carlo simulations.

INDEX TERMS Cooperative jamming, full-duplex, physical layer security, relaying, simultaneous wireless information and power transfer.

I. INTRODUCTION

As the large-scale deployment of the fifth-generation (5G) wireless networks go forward, explosive growth in the number of connected devices across multiple global sectors is expected. Indeed, smart Internet of Things (IoT) devices equipped with sensors and actuators will be spread in critical infrastructure with the task of monitoring the most crucial and vulnerable parameters. Therefore, providing 5G and beyond networks with security and privacy is a significant concern and a challenging task, especially when considered the constrained resources in different use cases of machine-type communications (MTCs) [1].

In this sense, traditional cryptography-based techniques, carried out at upper layers, might not be capable of compelling with several MTC use cases' requirements. A new approach, referred to as physical layer security (PLS), has emerged as a promising candidate to enhance wireless networks' security [2], [3]. PLS techniques can potentially offer secure transmissions by efficiently exploiting the wireless

The associate editor coordinating the review of this manuscript and approving it for publication was Olutayo O. Oyerinde.

medium's properties, i.e., fading and interference, to provide a further level of protection over existing information security schemes. Pioneering works such as [4] and [5] proved that secure communications are possible without secret keys if the eavesdropping channel is degraded with respect to the legitimate channel. Particularly in [5], the secrecy capacity for the Gaussian wiretap channel was defined as the difference between legitimate and eavesdropping channel capacities.

On the other hand, the gains offered by cooperative relaying techniques have proved effective in providing secure and reliable communications [6]–[10]. For instance, in [6], a best-relay selection strategy was introduced considering the amplify-and-forward (AF) and decode-and-forward (DF) protocols. Only the single best relay that achieves the maximal secrecy capacity was chosen to forward the source's signal in each case. It was shown that for both protocols, optimal relay selection performs the same diversity order as the multiple relays combining approach. The work in [7] evaluates a network with DF relays in the presence of a passive eavesdropper capable of intercept information from both the source and the relays. To enhance the system secrecy, the authors proposed a max-ratio relay selection where every relay is equipped with a data buffer, and the best link is considered to be the one with the highest gain ratio between the available source-to-relay and relay-to-destination links. The authors in [8] proposed the cooperative jamming (CJ) technique whereby an external node emits an artificial noise to confuse multiple eavesdroppers in the system. By analyzing the secrecy outage probability (SOP), it was shown that a CJ approach could enhance energy efficiency and the system's security performance. In [9], the authors proposed a relay selection scheme whereby, according to both instantaneous and average secrecy capacity, two relays are selected, one to retransmit the information to the legitimate user and other to act as a jammer node, generating intentional interference to the relaying transmission in order to confuse the eavesdropper. By assessing the SOP, it was noted that CJ techniques are efficient solutions to provide security in scenarios with strong eavesdropper links. In [10] the secrecy performance of an AF relaying network with an untrusted relay node, considering the partial secrecy regime, was examined to guarantee a positive secrecy rate by using a destination-based jamming strategy.

All the previous works considered half-duplex (HD) relaying schemes, which are intrinsically inefficient in terms of spectrum resource usage. Since the communication occurs in orthogonal time slots, HD relaying requires at least twice the channel resources needed by direct transmission between source and destination. For this reason, full-duplex (FD) communications have gained increasing attention since FD nodes can support simultaneous transmission and reception of signals by using the same time and frequency resources. However, this spectral-efficiency gain comes at the cost of the self-interference (SI) caused by the transmit antenna on the receive antenna at the same node, which can severely impair the communication performance [11]. Several research groups have addressed this issue by proposing SI cancellation techniques and new transceiver designs, which have been shown to mitigate the SI significantly [12]. Nevertheless, SI cannot be completely eliminated because of RF impairments [13], so that the performance of FD networks is still limited by residual SI (RSI) [14]. For instance, in [15], the authors explore a communication network where a source intends to communicate to a FD destination in the presence of an eavesdropper. Therein, based on the performance analysis for the power allocation at the receiver, it was shown that the destination usually does not use all of its available power due to the residual self-interference. Furthermore, different works have analyzed the secrecy performance of FD relaying networks [16]–[19]. For instance, in [16], the SOP of a multiple FD-DF relay network with imperfect channel state information (CSI) was analyzed. Therein, relay selection was used, showing to be superior to the HD-based scheme. Moreover, it was also shown that when the average signal-to-noise ratio (SNR) of the eavesdropper increases, the RSI effect on the SOP can be considered negligible. In [17], a survey of PLS schemes for FD cooperative systems was provided. Furthermore, a source-based jamming technique was proposed where the source transmits a composite signal consisting of the confidential and jamming signals to improve the secrecy in a scenario with untrusted relays. The authors in [18] proposed an FD jamming relay scheme, which was analyzed in terms of SOP, where the relay simultaneously receives data from the source and sends jamming signals to the eavesdroppers, and then, in a different transmission block, the relay switches to HD mode to retransmit the information to the destination. In [19], the secrecy rates, and optimal power allocation were investigated for a two-hop FD-DF relaying scheme considering static and ergodic fading channels. Moreover, in [20], an FD destination, was considered to enable destination-based jamming in a cooperative network with multiple AF untrusted relays.

On the other hand, due to the low-cost and energy-constrained devices used in many massive MTC applications, it is of paramount importance to provide these networks with energy sustainability. In this context, wireless energy transfer (WET) emerges as a promising solution for overcoming the energy limitations of some MTC use cases [21]–[24]. The exchange of energy via wireless links can be classified as near-field WET and far-field WET, where the former employs inductive or capacitive coupling to accomplish the power transfer while the latter considers directive antennas to guarantee a transfer of power up to miliwatts [25]. Particularly, in far-field WET scenarios, the simultaneous wireless information and power transfer (SWIPT) techniques can provide remarkable gains not only in terms of energy consumption but also in terms of spectral efficiency, interference control, and transmission delay [22]. In [23], two different approaches for SWIPT were proposed, namely time-switching (TS) and power-splitting (PS). In TS-based SWIPT, the receiver harvests energy from a signal sent by the source and receives the source's transmitted information signal in a time-division manner. In PS-based SWIPT, the receiver handles the source's transmitted signal by splitting it into two components: one for energy harvesting (EH) and one for information decoding (ID). In [24], the outage probability of a FD cooperative network with an energy-constrained relay was evaluated. Furthermore, a PS-based SWIPT technique where the relay exploits the SI for EH is considered. The authors compare the performance attained for the FD relay with a HD device in order to verify the impact of the self-energy recycling in FD mode. In this context, several works have tackled SWIPT-based networks under secrecy constraints [26]–[34]. For instance, in [26], the secrecy performance of a mixed single-input multiple-output (SIMO) RF and free-space optical (FSO) communication system over generalized fading channels was studied by considering a fixed-gain relaying scheme, with an EH receiver as a possible eavesdropper. In [27], the authors investigated the PLS performance for cognitive radio systems with SWIPT. In such work, it was proposed a destination-assisted scheme in which the primary destination transmits a jamming signal to confuse the eavesdropper while it is also used to power the secondary user. The SOP and secrecy throughput were evaluated in [28] by considering a TS-based system, where a source intends to communicate with a wireless-powered FD destination node in the presence of a passive eavesdropper. PLS techniques for EH-based multiple-antenna HD-AF relay networks were studied in [29]. Moreover, the authors exploited an artificial noise signal, traditionally used to improve the secrecy rate, to assist the powering of an energy-constrained relay. In [31], the PLS of an AF relaying network where the destination is capable of decoding information and harvesting energy was investigated. In [32], the authors evaluate a TS-based FD relaying network in the presence of an eavesdropper. An external jammer node is considered to improve the system's secrecy performance. Furthermore, a comparison between the FD and HD operation modes at the jammer is also provided. It was shown that the FD jammer improves the secrecy performance when compared to the HD jammer. However, the degrees of improvement are highly dependent on parameters of the system. Besides, in [34] was considered a three-node relaying network setup with an untrusted AF relay, in which a TS-based SWIPT technique was employed to supply energy to the relay whereas a destination-based jamming technique was used to hinder the relay from eavesdropping. In [33], a similar network scheme was evaluated for two-way relay communications.

A. SUMMARY OF CONTRIBUTIONS

Notwithstanding the significant efforts carried out so far, several issues remain unexplored in the context of SWIPT-based FD relay networks with secrecy constraints. For instance, in contrast to [24] and [35], we contribute to the study of SWIPT-based relay networks by investigating a network with secrecy constraints. In addition, differently from [28], [34] and [32], we consider a PS-based FD relay node. In the proposed scheme, the relay is also assumed to leverage the RSI for self-energy recycling. That is, part of the energy used for information relaying can be harvested and reused in addition to the energy harvested from the source's transmitted signal [36]. The main contributions of this paper are summarized as follows:

- Similar to [35], we evaluate a PS-based FD relaying network where the relay node deploys two rechargeable batteries, so that one battery can be used for transmission while the other charges, which entails in a more pratical scenario.
- Unlike [37] and [38], where a source-based jamming technique is used to improve secrecy performance, we propose a cooperative relay-based jamming technique to enhance the secrecy performance in which the FD-DF relay with energy constraints can superpose a jamming signal to the confidential signal so that only the intended destination can decode it while the eavesdropper's channel is degraded.
- A tight approximation for the connection outage probability and the secrecy outage probability are derived to assess the impact of key system parameters on the network performance. It is worthwhile to mention that, in contrast to previous works [14], [35], we consider the existence of correlation between the random variables (RVs) of the instantaneous received SINRs for the first and second hop in both expressions.
- An asymtotic expression for the SOP is also derived, thus the outage floor at high SNR is characterized. We also compared the proposed scenario to a baseline scheme based on HD relaying with energy constraints.
- An asymptotic expression for the average secrecy capacity (ASC) is derived in order to asses the high-SNR slope and the power offset of the system.
- Finally, a particle swarm optimization (PSO) algorithm is employed in order to determine the optimal PS and jamming power allocation ratios that maximize the secrecy throughput subjected to a maximum SOP constraint.

Notation: Throughout this paper, $f_X(\cdot)$ and $F_X(\cdot)$ denote the probability density function (PDF) and cumulative density function (CDF) of a random variable (RV) X; $E[\cdot]$ is the expectation operator; $\Pr(\cdot)$ stands for probability; $I_0(\cdot)$, $\Gamma(\cdot)$ and $\Gamma(\cdot,\cdot)$ stands for the zero-order modified Bessel function of the first kind [39, Eq. 8.447.1], the gamma function [39, Eq. 8.324] and upper incomplete gamma function [39, Eq. 8.350.5], respectively; ${}_1\tilde{F}_1(\cdot;\cdot;\cdot)$ is the regularized hypergeometric function [40]; ${}_1F_1(\cdot;\cdot;\cdot)$ is the confluent hypergeometric function [39, Eq. 9.210.1]; $\mathrm{K}_1(\cdot)$ and $Q_1(\cdot;\cdot)$ stands for the first-order modified Bessel function of the second kind [39, Eq. 8.446] and the first order Marcum Q function [41, Eq. 4.34], respectively;and $[x]^+ = \max(x, 0)$.

II. SYSTEM MODEL

In Fig. 1, we illustrate a cooperative network consisting of one source (S) that intends to communicate with a destination (D) with the help of a DF relay (R) in the

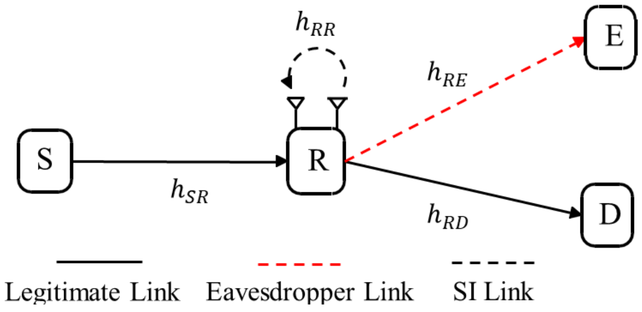

FIGURE 1. System model.

presence of an eavesdropper (E). The relay is assumed to be energy-constrained so that it harvests energy from the radio frequency (RF) signals transmitted by S according to a PS-SWIPT scheme. All terminals are equipped with a single antenna, except for R, which is equipped with one pair of transmitting and receiving antennas to operate in FD mode. Herein, we focus our analysis on a coverage extension scenario, where the direct link between S and D is severely attenuated, thus being negligible. We also assume that E is in the proximity of D, thus being capable of wiretapping information from R only.[1] Additionally, Wiretap codes are assumed for message transmission. All links are considered to undergo independent Rayleigh block fading, as well as additive white Gaussian noise (AWGN) with average power N_0. Accordingly, h_{SR}, h_{RD} and h_{RE} denote the channels coefficients for the links S-R, R-D and R-E, respectively, which are assumed to be independent circularly-symmetric Gaussian RVs, i.e., $h_i \sim \mathcal{CN}(0, \Omega_i)$, with $i \in \{\mathrm{SR}, \mathrm{RD}, \mathrm{RE}\}$, where $\Omega_i = E\{|h_i^2|\}$ is the average channel gain of the corresponding link.

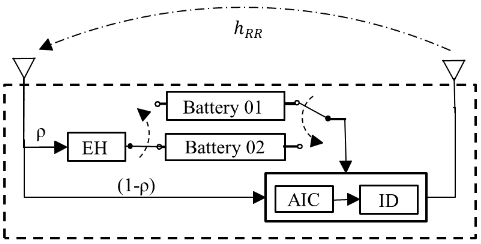

FIGURE 2. Block diagram for the operation of the FD relay node.

A. TRANSMISSION SCHEME

The transmission scheme can be described in two simultaneous processes. During the first process, S transmits a signal $s_{\mathrm{S}}(t)$ with power P_{S} to R, which splits the received signal for EH and ID. Similar to [35], the proposed harvest model for the relay deploys a battery group consisting of two rechargeable batteries, as depicted in Fig. 2. It is assumed that each battery contains enough redundant energy initially. The two batteries are activated for EH and power supply alternately in time switching manner, with the duration of each transmission block being denoted by T, divided equally into two-time slots. In each time slot, the power of the signal received at the relay is split for EH and ID according to the proportion $\rho : (1-\rho)$, where $\rho \in (0, 1)$ is the PS ratio. Furthermore, by considering the FD mode operation, the channel coefficients of RSI at the receive antenna after passive interference cancellation (self-energy recycling channel), and that obtained after active (analog and digital) interference cancellation (AIC) are denoted by $h^{\mathcal{E}}_{\mathrm{RR}}$ and $h^{\mathcal{I}}_{\mathrm{RR}}$, respectively. Thus, $h^{\mathcal{E}}_{\mathrm{RR}}$ can be modeled as a Rician fading feedback channel to account for a possible Line-of-Sight (LoS) component [11], [12], with shape factor K and scale parameter equal to the average channel gain, $\Omega^{\mathcal{E}}_{RR}$. In turn, since $h^{\mathcal{I}}_{\mathrm{RR}}$ is achieved after AIC, the LoS component is assumed to be strongly attenuated, so that the self-interference channel can be assumed to undergo Rayleigh fading, that is, $h^{\mathcal{I}}_{\mathrm{RR}} \sim \mathcal{CN}(0, \Omega^{\mathcal{I}}_{RR})$ [42].

During the second process, R transmits a superposed signal containing the information signal of the previous transmission block $s_{\mathrm{R}}(t)$ with power $(1-\theta)P_{\mathrm{R}}$ and an artificial jamming signal $s_j(t)$ with power θP_{R} (to hinder E from eavesdropping the information signal). Hence, the total transmission power at R is P_{R} and $\theta \in (0, 1)$ is the jamming power allocation ratio. Assuming that R can correctly decode the received signal, the corresponding transmit signal can be written as $s_{\mathrm{R}}(t) = s_{\mathrm{S}}(t-k)$, where k is the processing delay at the relay. For simplicity, we assume $k = 1$, which means that the relay message is delayed only by one block with respect to the source message. Under these considerations, the input signal at the EH receiver can be written as

$$y_{\mathrm{EH}}(t) = \sqrt{\rho}(\sqrt{P_{\mathrm{S}}}h_{\mathrm{SR}}s_{\mathrm{S}}(t) + \sqrt{P_{\mathrm{R}}}h^{\mathcal{E}}_{\mathrm{RR}}s_{\mathrm{S}}(t-1)). \quad (1)$$

In addition, it is considered that the transmitted signals at source and relay have mean power normalized to unity, that is $E\{|s_{\mathrm{S}}(t)|^2\} = E\{|s_{\mathrm{R}}(t)|^2\} = 1$. For notation simplicity, we consider $g_i \triangleq |h_i|^2$ for $i \in \{\mathrm{SR}, \mathrm{RR}, \mathrm{RD}\}$ denote the channel gains. This way, at the end of a time slot, the harvested energy at the relay can be expressed as[2]

$$E_H = \eta\rho(P_{\mathrm{S}}g_{\mathrm{SR}} + P_{\mathrm{R}}g^{\mathcal{E}}_{\mathrm{RR}})\frac{T}{2}, \quad (2)$$

where $\eta \in (0, 1)$ is the energy conversion efficiency factor. Simultaneously, the transmission is powered by a battery that is not switched to the EH mode in the current transmission block. Assuming that the harvested energy in (2) is the only energy available for transmission, P_{R} can be written as

$$P_{\mathrm{R}} = \frac{E_H}{T/2} = \eta\rho(P_{\mathrm{S}}g_{\mathrm{SR}} + P_{\mathrm{R}}g^{\mathcal{E}}_{\mathrm{RR}}) = \frac{\eta\rho P_{\mathrm{S}}g_{\mathrm{SR}}}{(1-\eta\rho g^{\mathcal{E}}_{\mathrm{RR}})}. \quad (3)$$

[1] As in [9] and [32], the described topology is validated by the assumption of an obstacle blocking the direct link between the source and destination as well as between the source and eavesdropper, while the relay is positioned in the surroundings of that obstacle such that the links between the relay and the other nodes are available.

[2] Similar to the works in [24], [35], we assume a linear EH model for mathematical tractability. It is worthwhile to mention that, as shown in [43], this assumption is accurate when the average power of the harvested energy at R is less than the saturation power level. In this case, the linear EH model is valid since a PS-based SWIPT is considered, so that a smaller amount of power arrives at the EH receiver.

In practice, due to the passive IC process, such as antenna isolation, $g_{\mathrm{RR}}^{\mathcal{E}}$ can be assumed less than 1 with high probability so that the denominator of (3) is positive [35]. Therefore, the received signal at the ID receiver, after AIC, is given by

$$y_{\mathrm{R}}(t) = \sqrt{(1-\rho)P_{\mathrm{S}}}h_{\mathrm{SR}}s_{\mathrm{S}}(t) + \sqrt{(1-\rho)P_{\mathrm{R}}}h_{\mathrm{RR}}^{\mathcal{I}}s_{\mathrm{S}}(t-1) + n_{\mathrm{R}}(t), \tag{4}$$

where $n_{\mathrm{R}}(t)$ is the AWGN component at R. Then, by assuming that D perfectly knows the jamming signal $s_j(t)$ [3] and the CSI of the link R-D [37], the received signals at the destination and the eavesdropper are given, respectively, by

$$y_{\mathrm{D}}(t) = \sqrt{(1-\theta)P_{\mathrm{R}}}h_{\mathrm{RD}}s_{\mathrm{S}}(t-1) + n_{\mathrm{D}}(t), \tag{5}$$

$$y_{\mathrm{E}}(t) = \sqrt{(1-\theta)P_{\mathrm{R}}}h_{\mathrm{RE}}s_{\mathrm{S}}(t-1) + \sqrt{\theta P_{\mathrm{R}}}h_{\mathrm{RE}}s_j(t) + n_{\mathrm{E}}(t), \tag{6}$$

where $n_{\mathrm{D}}(t)$ and $n_{\mathrm{E}}(t)$ are the AWGN components at D and E, respectively. Hence, by substituting (3) into (4), (5), and (6), and after some mathematical manipulations, the received instantaneous signal-to-interference-plus-noise (SINR) at R, D, and E can be expressed, respectively, as

$$\begin{aligned}\gamma_{\mathrm{R}} &= \frac{(1-\rho)P_{\mathrm{S}}g_{\mathrm{SR}}}{\frac{(1-\rho)\eta\rho P_{\mathrm{S}}g_{\mathrm{SR}}g_{\mathrm{RR}}^{\mathcal{I}}}{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}} + N_0}\\ &= \frac{\gamma_P(1-\rho)g_{\mathrm{SR}}\left(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}\right)}{\gamma_P\eta(1-\rho)\rho g_{\mathrm{RR}}^{\mathcal{I}}g_{\mathrm{SR}} - \eta\rho g_{\mathrm{RR}}^{\mathcal{E}} + 1},\end{aligned} \tag{7}$$

$$\gamma_{\mathrm{D}} = \frac{(1-\theta)\eta\rho P_{\mathrm{S}}g_{\mathrm{SR}}}{(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}})}\frac{g_{\mathrm{RD}}}{N_0} = \frac{(1-\theta)\left(\gamma_P\eta\rho g_{\mathrm{SR}}g_{\mathrm{RD}}\right)}{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}}, \tag{8}$$

$$\begin{aligned}\gamma_{\mathrm{RE}} &= \frac{(1-\theta)\eta\rho P_{\mathrm{S}}g_{\mathrm{SR}}}{(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}})}\frac{g_{\mathrm{RE}}}{\frac{\theta\eta\rho P_{\mathrm{S}}g_{\mathrm{SR}}}{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}}g_{\mathrm{RE}} + N_0}\\ &= \frac{(1-\theta)\left(\gamma_P\eta\rho g_{\mathrm{SR}}g_{\mathrm{RE}}\right)}{\gamma_P\eta\theta\rho g_{\mathrm{SR}}g_{\mathrm{RE}} + 1 - \eta\rho g_{\mathrm{RR}}^{\mathcal{E}}}.\end{aligned} \tag{9}$$

where $\gamma_P = P_{\mathrm{S}}/N_0$ is the total transmit system SNR. Then, by considering the DF protocol, the end-to-end SINR at the legitimate and eavesdropping links are, respectively, given by $\gamma_L = \min\{\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}\}$ and $\gamma_E = \min\{\gamma_{\mathrm{R}}, \gamma_{\mathrm{RE}}\}$.

B. NON-LINEAR ENERGY HARVESTING MODEL

For comparison purposes, the practical non-linear energy harvesting model proposed in [43] and illustrated in Fig. 3 is also included in our analysis. According to that model, it is considered that R begins energy harvesting when a sensitivity power value is attained, i.e., P_{min}. Also, R harvests energy according to a linear model until a saturation power level, i.e., P_{max}, for which P_R will be constant in this range. Under these considerations, the SINRs given in (7), (8) and (9) for the non-linear energy harvesting model can be rewritten as

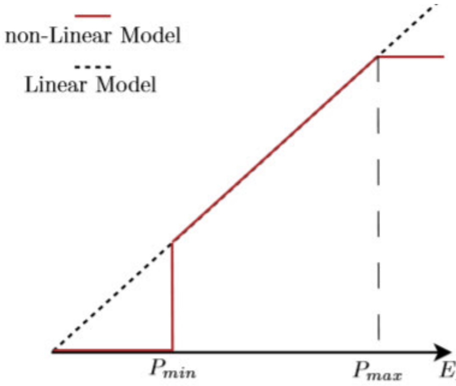

FIGURE 3. Comparison linear and non-linear energy harvesting models.

$$\gamma_{\mathrm{R}} = \begin{cases} (1-\rho)\gamma_P g_{\mathrm{SR}}, & P_R < P_{min}\\ \frac{\gamma_P(1-\rho)g_{\mathrm{SR}}\left(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}\right)}{\gamma_P\eta(1-\rho)\rho g_{\mathrm{RR}}^{\mathcal{I}}g_{\mathrm{SR}} - \eta\rho g_{\mathrm{RR}}^{\mathcal{E}} + 1}, & P_{min} \le P_R \le P_{max}\\ \frac{(1-\rho)\gamma_P g_{\mathrm{SR}}}{(1-\rho)\eta\rho P_{max}g_{\mathrm{RR}}^{\mathcal{I}} + 1}, & P_R > P_{max} \end{cases} \tag{10}$$

$$\gamma_{\mathrm{D}} = \begin{cases} 0, & P_R < P_{min}\\ \frac{(1-\theta)(\gamma_P\eta\rho g_{\mathrm{SR}}g_{\mathrm{RD}})}{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}}, & P_{min} \le P_R \le P_{max}\\ (1-\theta)\rho\eta P_{max}g_{\mathrm{RD}}, & P_R > P_{max} \end{cases} \tag{11}$$

$$\gamma_{\mathrm{RE}} = \begin{cases} 0, & P_R < P_{min}\\ \frac{(1-\theta)(\gamma_P\eta\rho g_{\mathrm{SR}}g_{\mathrm{RE}})}{\gamma_P\eta\theta\rho g_{\mathrm{SR}}g_{\mathrm{RE}} + 1 - \eta\rho g_{\mathrm{RR}}^{\mathcal{E}}}, & P_{min} \le P_R \le P_{max}\\ \frac{(1-\theta)\rho\eta P_{max}g_{\mathrm{RE}}}{\theta\rho\eta P_{max}g_{\mathrm{RE}} + 1}, & P_R > P_{max} \end{cases} \tag{12}$$

III. CONNECTION OUTAGE PROBABILITY

In this section, an analytical expression for the connection outage probability (COP) at the legitimate link is derived. For this purpose, we define the capacity of the legitimate link as follows:

Definition 1: The maximal achievable rate at the legitimate link by considering the FD-DF protocol is given by

$$C_{\mathrm{L}} = \log_2(1+\gamma_{\mathrm{L}}) = \log_2(1+\min\{\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}\}). \tag{13}$$

Therefore, for the proposed setup, the system is in outage if the channel capacity is less than a given target rate, $\mathcal{R}$. Thus, from (13), the outage probability can be expressed as

$$\begin{aligned}\mathrm{COP} &= \Pr(C_{\mathrm{L}} < \mathcal{R}) = \Pr(\min\{\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}\} < \tau),\\ &= 1 - \underbrace{\Pr(\gamma_{\mathrm{R}} > \tau, \gamma_{\mathrm{D}} > \tau)}_{\Theta}.\end{aligned} \tag{14}$$

where $\tau = 2^{\mathcal{R}} - 1$.

Remark 1: Notice from (7) *and* (8) *that* γ_{R} *and* γ_{D} *are correlated RVs, as both of them depend on the channel gains* g_{SR} *and* $g_{\mathrm{RR}}^{\mathcal{E}}$*. In our study, we consider this fact, which has been overlooked by previous works [14], [35].*

From Section II, we have that the channel gains g_i, with $i \in$ (SR, RD, RE), and $g_{\mathrm{RR}}^{\mathcal{I}}$ follow exponential distributions with means Ω_i and $\Omega_{\mathrm{RR}}^{\mathcal{I}}$, respectively, whereas $g_{\mathrm{RR}}^{\mathcal{E}}$ follows a

[3] This can be attained by considering that both R and D apply the same pseudo-random generator to generate the jamming signal while the eavesdropper does not. Besides, by further assuming that the CSI of the links can be obtained from pilot signals before transmission [44], D is able to gather complete knowledge to remove the jamming signal, $s_j(t)$.

non-central chi-squared distribution with PDF and CDF given by

$$f_{g_{\mathrm{RR}}^{\mathcal{E}}}(x)=\frac{(K+1)\exp\left(-K-\frac{(K+1)x}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)I_0\left(2\sqrt{\frac{K(K+1)x}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}, \tag{15}$$

$$F_{g_{\mathrm{RR}}^{\mathcal{E}}}(x)=1-Q_1\left(\sqrt{\frac{2}{K}},x\sqrt{\frac{2(K+1)}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right), \tag{16}$$

in which $|h_{\mathrm{RR}}^{\mathcal{E}}|$ is assumed to undergo Rician fading.

Proposition 1: The COP at the legitimate link for a dual-hop FD-DF relaying system with PS-SWIPT and self-energy recycling is given as in (17)*, shown at the bottom of the next page.*

Proof: The proof is provided in Appendix A. □

IV. SECRECY PERFORMANCE ANALYSIS

Definition 2: The secrecy capacity is defined as the difference between the channel capacities of the legitimate and wiretap channels, thus being expressed as [5]:

$$\begin{aligned}C_s&=[C_{\mathrm{L}}-C_{\mathrm{E}}]^+\\&=[\log_2(1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\})-\log_2(1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{RE}}\})]^+\\&=\left[\log_2\left(\frac{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}}{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{RE}}\}}\right)\right]^+.\end{aligned} \tag{18}$$

A. SECRECY OUTAGE PROBABILITY

Definition 3: For the proposed setup, the system is in secrecy outage if the secrecy capacity C_s is less than a target secrecy rate, i.e., $\mathcal{R}_s$. Thus, the SOP can be written from (18) as

$$\mathrm{SOP}=\Pr(C_s<\mathcal{R}_s)=\Pr\left(\frac{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}}{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{RE}}\}}<\tau_{\mathrm{s}}\right), \tag{19}$$

where $\tau_{\mathrm{s}}=2^{\mathcal{R}_s}$. In addition, since $\mathcal{R}_s\geq 0$, we have that $\Pr([x]^+<\mathcal{R}_s)=\Pr(x<\mathcal{R}_s)$, then the operator $[\cdot]^+$ has been removed. An approximate expression for the SOP of the proposed system, which is highly accurate at the medium-to-high SNR regime, can be obtained as stated in the following proposition.

Proposition 2: An approximation for the SOP of a dual-hop FD-DF relaying system with PS-SWIPT, self-energy recycling, and cooperative jamming is given by

$$\mathrm{SOP}\approx\sum_{n=0}^{N}(I_1+I_2), \tag{20}$$

where I_1 and I_2 are given by (21) and (22), respectively, shown at the bottom of the next page.

Proof: The proof is provided in Appendix B. □

Remark 2: To obtain the approximation in (20) *for the SOP, note that $\gamma_{\mathrm{RE}}\approx(1-\theta)/\theta$, thus indicating that the SINR at the eavesdropper is independent of the channel gain at the link R-E.*

Importantly, as previously stated in Remark 1, γ_{R} and γ_{D} are correlated RVs. In addition, for the SOP of the considered network setup, γ_{R} and γ_{RE} are also correlated random variables. These issues were taken into consideration throughout our analyses. Furthermore, as shall be seen from the numerical results, values of 200 for N and 50 for Φ suffice to render a very tight approximation.

B. ASYMPTOTIC SOP

In order to gain a better insight into the secrecy diversity order attained by the investigated system, its secrecy outage behavior at high SNR is determined in the following proposition.

Proposition 3: An asymptotic expression for the SOP of a dual-hop FD-DF relaying system with PS-SWIPT, self-energy recycling, and cooperative jamming is given by

$$\begin{aligned}\mathrm{SOP}^{\infty}=\sum_{n=0}^{N}\frac{e^{-K}K^n}{(n!)^2}&\left((K+1)^{n+1}e^{\frac{\theta}{\eta\theta\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}-\eta\rho\tau_{\mathrm{s}}\Omega_{\mathrm{RR}}^{I}}}\right.\\&\times\left(\Gamma(n+1)-\Gamma\left(n+1,\frac{\frac{K+1}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}+\frac{\theta}{(\theta-\tau_{\mathrm{s}})\Omega_{\mathrm{RR}}^{\mathcal{I}}}}{\eta\rho}\right)\right)\\&\left.\times\left(\frac{\theta\Omega_{\mathrm{RR}}^{E}}{\Omega_{\mathrm{RR}}^{I}(\theta-\tau_{\mathrm{s}})}+K+1\right)^{-n-1}\right).\end{aligned} \tag{23}$$

Proof: By considering the high SNR regime (i.e., as $\gamma_P\to\infty$) into (21) and (22), we have that $1/\gamma_P\to 0$. Then, by neglecting the high-order terms with respect to $1/\gamma_P$, and after some simplifications, the asymptotic SOP can be obtained as in (23). □

Remark 3: Note from (23) *that the asymptotic outage performance of the system is independent of γ_P. Consequently, the system's secrecy diversity order is zero, which is expected because of the deleterious effect of RSI inherent to FD relaying.*

V. AVERAGE SECRECY CAPACITY

Definition 4: The ASC is defined as the average of the secrecy rate over the instantaneous SNR of the legitimate and eavesdropper channels. According to [45], the ASC can be expressed as:

$$\mathrm{ASC}=\bar{C_{\mathrm{L}}}-\mathcal{L}(\bar{\gamma_{\mathrm{L}}},\bar{\gamma_{\mathrm{E}}}), \tag{24}$$

where $\bar{C_{\mathrm{L}}}$ is the average capacity of the legitimate link in the absence of the eavesdropper, given by

$$\bar{C_{\mathrm{L}}}=\frac{1}{\ln 2}\int_0^{\infty}\frac{1-F_{\gamma_{\mathrm{L}}(\gamma)}}{1+\gamma}d\gamma, \tag{25}$$

and $\mathcal{L}(\bar{\gamma_{\mathrm{L}}},\bar{\gamma_{\mathrm{E}}})$ is a form of ASC loss given by

$$\mathcal{L}(\bar{\gamma_{\mathrm{L}}},\bar{\gamma_{\mathrm{E}}})=\frac{1}{\ln 2}\int_0^{\infty}\frac{(1-F_{\gamma_{\mathrm{E}}(\gamma)})(1-F_{\gamma_{\mathrm{L}}(\gamma)})}{1+\gamma}d\gamma. \tag{26}$$

Thus, an asymptotic expression for the ASC of the proposed system is derived as in the following proposition.

Proposition 4: An asymptotic expression for the ASC of a dual-hop FD-DF relaying system with PS-SWIPT, self-energy recycling, and cooperative jamming is given by

$$\mathrm{ASC}^{\infty} = \frac{1}{\ln 2}\Bigg(\sum_{\gamma=1}^{n}\frac{e^{\gamma}}{1+\gamma}+\sum_{\gamma=1}^{m}\frac{e^{\gamma}}{1+\gamma}F_{\mathrm{L}}^{\infty}(\gamma)-\mathcal{L}(\bar{\gamma}_{\mathrm{L}},\bar{\gamma}_{\mathrm{E1}}) -\int_{0}^{\frac{1-\theta}{\theta}}\frac{(1-F_{\mathrm{L}}^{\infty}(\gamma))Q_{1}\left(\sqrt{\frac{2}{K}},\frac{\sqrt{2(K+1)}}{\eta\rho\sqrt{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)}{\gamma+1}d\gamma\Bigg) \tag{27}$$

where $F_{\mathrm{L}}^{\infty}(\gamma)$ and $\mathcal{L}(\bar{\gamma}_{\mathrm{L}},\bar{\gamma}_{\mathrm{E1}})$ are given as shown at the bottom of the page.

Proof: The proof is provided in appendix C. □

A. HIGH SNR SLOPE AND POWER OFFSET

To gain a better insight into the behaviour of the average secrecy capacity at high SNR, we evaluate the high SNR slope and the power offset of the system (given in bits/s/Hz) as follows [46]

$$S_{\infty} = \lim_{\gamma_P\to\infty}\frac{\mathrm{ASC}}{\log_2(\gamma_P)} \tag{30}$$

$$\mathcal{L}_{\infty} = \lim_{\gamma_P\to\infty}\left(\log_2(\gamma_P)-\frac{\mathrm{ASC}}{S_{\infty}}\right) \tag{31}$$

due to the intricacy of (27), we provide a numerical analysis of S_{∞} and $\mathcal{L}_{\infty}$ in Table 2 on the next section.

$$\mathrm{COP} = 1-\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\left(\frac{e^{-K}(-1)^{m}\left(\frac{K(K+1)}{\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)^{n+1}\Gamma\left(1-m,\frac{\tau}{\gamma_P\Omega_{\mathrm{SR}}-\gamma_P\rho\Omega_{\mathrm{SR}}}\right){}_1\tilde{F}_1\left(n+1;m+n+2;-\frac{K+1}{\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)\left(\frac{(1-\theta)\gamma_P\eta\rho\Omega_{\mathrm{SR}}\Omega_{\mathrm{RD}}}{\tau}\right)^{-m}}{K\Gamma(n+1)}\right.$$
$$\left.-\frac{\left(\frac{K(K+1)}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)^{n+1}e^{-\frac{1}{\eta\rho\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}}-K}\Gamma\left(1-m,\frac{\tau}{(\gamma_P-\gamma_P\rho)\Omega_{\mathrm{SR}}}\right)\left(\frac{(\rho-1)\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}-(\theta-1)\Omega_{\mathrm{RD}}}{\gamma_P\eta(\theta-1)(\rho-1)\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}\Omega_{\mathrm{SR}}\Omega_{\mathrm{RD}}}\right)^{m}{}_1F_1\left(n+1;m+n+2;\frac{(-K-1)\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}+\Omega_{\mathrm{RR}}^{\mathcal{E}}}{\eta\rho\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)}{(\eta\rho)^{n+1}K\Gamma(n+1)\Gamma(m+n+2)}\right). \tag{17}$$

$$I_1 \approx \frac{1}{(n!)^2}e^{-K}K^{n}\Bigg((K+1)^{n+1}\left(\frac{\theta\Omega_{\mathrm{RR}}^{\mathcal{E}}}{\Omega_{\mathrm{RR}}^{\mathcal{I}}(\theta-\tau_{\mathrm{s}})}+K+1\right)^{-n-1}\exp\left(\frac{\theta}{\eta\theta\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}-\eta\rho\tau_{\mathrm{s}}\Omega_{\mathrm{RR}}^{\mathcal{I}}}+\frac{\theta-\tau_{\mathrm{s}}}{\gamma_P\theta\Omega_{\mathrm{SR}}-\gamma_P\theta\rho\Omega_{\mathrm{SR}}}\right)$$
$$\times\left(\Gamma(n+1)-\Gamma\left(n+1,\frac{\frac{K+1}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}+\frac{\theta}{(\theta-\tau_{\mathrm{s}})\Omega_{\mathrm{RR}}^{\mathcal{I}}}}{\eta\rho}\right)\right)+\left(1-\exp\left(\frac{\theta-\tau_{\mathrm{s}}}{\gamma_P\theta\Omega_{\mathrm{SR}}-\gamma_P\theta\rho\Omega_{\mathrm{SR}}}\right)\right)\left(\Gamma(n+1)-\Gamma\left(n+1,\frac{K+1}{\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)\right)\Bigg). \tag{21}$$

$$I_2 \approx \frac{e^{-K}(\theta-\tau_{\mathrm{s}})K^{n}\Gamma\left(0,\frac{\tau_{\mathrm{s}}-\theta}{(\gamma_P\theta-\gamma_P\theta\rho)\Omega_{\mathrm{SR}}}\right)\left((K+1)\left(\Gamma(n+1)-\Gamma\left(n+1,\frac{K+1}{\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)\right)+\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}\left(\Gamma\left(n+2,\frac{K+1}{\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)-\Gamma(n+2)\right)\right)}{\gamma_P\eta(\theta-1)\theta(K+1)\rho(n!)^2\Omega_{\mathrm{SR}}\Omega_{\mathrm{RD}}}$$
$$+\sum_{\phi=0}^{\Phi}\frac{(-1)^{1-\phi}(\phi+1)\gamma_P^{-\phi-1}(\rho-1)^{-\phi}(\theta-\tau_{\mathrm{s}})K^{n}(K+1)^{n+1}{\Omega_{\mathrm{RR}}^{\mathcal{I}}}^{-\phi}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}^{-n-1}\Omega_{\mathrm{SR}}^{-\phi-1}\eta^{-\phi-n-2}\rho^{-\phi-n-2}}{(\theta-1)\theta\Gamma(n+1)\Omega_{\mathrm{RD}}\Gamma(n+\phi+3)}\left(\exp\left(\frac{\theta}{\eta\theta\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}-\eta\rho\tau_{\mathrm{s}}\Omega_{\mathrm{RR}}^{\mathcal{I}}}-K\right)\right.$$
$$\left.\times\Gamma\left(-\phi,-\frac{\theta-\tau_{\mathrm{s}}}{\gamma_P\theta\Omega_{\mathrm{SR}}-\gamma_P\theta\rho\Omega_{\mathrm{SR}}}\right){}_1F_1\left(n+1;n+\phi+3;-\frac{\frac{K+1}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}+\frac{\theta}{(\theta-\tau_{\mathrm{s}})\Omega_{\mathrm{RR}}^{\mathcal{I}}}}{\eta\rho}\right)\right) \tag{22}$$

$$F_{\mathrm{L}}^{\infty}(\gamma) = \sum_{x=1}^{z}\frac{(K+1)\exp\left(-\frac{(K+1)(1-e^{-x})}{\Omega_{\mathrm{RR}}^{\mathcal{E}}\eta\rho}-K\right)I_0\left(2\sqrt{\frac{K(K+1)(1-e^{-x})}{\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)\left(\frac{2e^{-\frac{1}{\eta\rho\gamma\Omega_{\mathrm{RR}}^{\mathcal{I}}}}\left(e^{\frac{1-e^{-x}}{\eta\rho\gamma\Omega_{\mathrm{RR}}^{\mathcal{I}}}}-e^{\frac{1}{\eta\rho\gamma\Omega_{\mathrm{RR}}^{\mathcal{I}}}}\right)\mathrm{K}_1\left(2\sqrt{\frac{\gamma\left(\frac{\eta\rho(1-e^{-x})}{\eta\rho}-1\right)}{\gamma_P\eta(\theta-1)\rho\Omega_{\mathrm{SR}}\Omega_{\mathrm{RD}}}}\right)}{\Omega_{\mathrm{SR}}\sqrt{\frac{\gamma_P\eta(\theta-1)\rho\Omega_{\mathrm{RD}}}{\gamma\Omega_{\mathrm{SR}}\left(\frac{\eta\rho(1-e^{-x})}{\eta\rho}-1\right)}}}+1\right)}{\Omega_{\mathrm{RR}}^{\mathcal{E}}\eta\rho} \tag{28}$$

$$\mathcal{L}(\bar{\gamma}_{\mathrm{L}},\bar{\gamma}_{\mathrm{E1}}) = \int_{0}^{\frac{1-\theta}{\theta}}\frac{(1-F_{\mathrm{L}}^{\infty}(\gamma))\left(1-\sum_{n=0}^{\infty}\frac{\left(K(K+1)\gamma\Omega_{\mathrm{RR}}^{\mathcal{I}}\right)^{n+1}\left((K+1)\gamma\Omega_{\mathrm{RR}}^{\mathcal{I}}-\Omega_{\mathrm{RR}}^{\mathcal{E}}\right)^{-(n+1)}e^{-\frac{1}{\eta\rho\gamma\Omega_{\mathrm{RR}}^{\mathcal{I}}}-K}\left(\Gamma(n+1)-\Gamma\left(n+1,\frac{\frac{K+1}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}-\frac{1}{\gamma\Omega_{\mathrm{RR}}^{\mathcal{I}}}}{\eta\rho}\right)\right)}{K(n!)^2}\right)}{\gamma+1} \tag{29}$$

VI. CONFIDENTIAL THROUGHPUT MAXIMIZATION

Herein, we consider the case where the codeword transmission rate, $\mathcal{R}$, and the confidential information rate, $\mathcal{R}_s$, can be adaptively chosen according to the instantaneous SNR estimated at the destination. Thus, the confidential throughput can be expressed as [47]:

$$\mathcal{T} = \mathcal{R}_s(1 - \text{COP}). \tag{32}$$

Therefore, we aim to find the optimal values for the PS ratio ρ, the jamming power allocation ratio θ, and the rate parameters that maximize the throughput subjected to maximum constraint secrecy, ϵ. Hence, the optimization problem can be formulated as

$$\max_{\mathcal{R}_s,\mathcal{R},\rho,\theta} \quad \mathcal{T}$$
$$\text{s.t. } \text{SOP}^{\infty} < \epsilon, \quad \mathcal{R} \geq \mathcal{R}_s, \; 0 < \rho < 1, 0 < \theta < 1. \tag{33}$$

The optimal parameters in (33) cannot be obtained analytically due to the intricacy of the expressions in (17) and (23). Alternatively, we propose using the Particle Swarm Optimization (PSO) method, which is shown in Algorithm 1. PSO is a learning technique based on the social behavior of bird flocking or fish schooling that is part of the evolutionary computing methods focused on the biological form of evolution [48]. Also, PSO is robust for multidimensionality and non-linearity optimization problems, easy to implement, has fewer parameters to adjust if compared to similar optimization techniques, and it can converge to the optimal solution in most cases [49].

Algorithm 1 PSO Algorithm

```
function PSO
    of ← Eq. (17)
    asympt ← Eq. (23)
    iterations ← #iterations
    p ← #population                          ▷ Population size
    c1 ← c − init                            ▷ Weighting coeff. for local best pos.
    c2 ← c − init                            ▷ Weighting coeff. for global best pos.
    w ← wvalue                               ▷ Inertia weight
    xmin ← [Rsmin $\mathcal{R}$min $\rho$min $\theta$min]            ▷ Min values
    xmax ← [Rsmax $\mathcal{R}$max $\rho$max $\theta$max]            ▷ Max values
    D ← length(xmin)                         ▷ Set Dimension size
    for i ← 1 to p do
        for j ← 1 to D do                    ▷ Initial Position
            x(i,j) ← (xmax(j)-xmin(j))∗rand()+xmin(j)
        end for
        if asympt(i) > $\epsilon$ or x(i,1) > x(i,2) then
            penalty ← penvalue
        end if
        of(i) ← of(i) + penalty
        if fbest < of(i) then
            fbest ← of(i)
            xbest ← x(i)
        end if
        xp ← x
        for j ← 1 to iterations do
            v ← w∗v+c1∗rand(p,D)∗(xp−x)+c2∗rand(p,D)
    ∗(xbest-x)
            x ← x + v
            for l ← 1 to D do
                if x(i,l)<xmin(l) then x(i,l) ← xmin(l)
                else if x(i,l)>xmax(l) then x(i,l) ← xmax(l)
                end if
                if fbest < of(i) then
                    fbest ← of(i)
                    xbest(l) ← x(i,l)
                end if
            end for
            w ← w∗0.70
        end for
    end for
    return fbest, xbest
end function
```

VII. NUMERICAL RESULTS AND DISCUSSIONS

In this section, the analytical expressions derived in Section IV are evaluated through some representative sample cases and validated via Monte Carlo simulations. For all analytical results, we have considered $N = 200$ and $\Phi = 50$. Unless specified otherwise, the rest of parameters are set as follows: i) path-loss exponent $\varphi = 4$; ii) target secrecy rate $\mathcal{R}_s = 1$ bps/Hz; iii) EH conversion efficiency factor $\eta = 1$; iv) transmit SNR $\gamma_{\text{P}} = 45$ dB; v) average channel gains at the S-R, R-D, and R-E links $\Omega_i = 20$ dB, $i \in \{\text{SR}, \text{RD}, \text{RE}\}$, and vi) average channel gains at the RSI link after passive and active interference cancellation, $\Omega_{\text{RR}}^{\mathcal{E}} = 0$ dB and $\Omega_{\text{RR}}^{\mathcal{I}} = -30$ dB, respectively. Moreover, for the optimization parameters in Algorithm 1, we have considered the following values: i) 20 for the number of iterations, ii) 800 for the population size, iii) 1 for the weighting coefficient for local and global best positions, and iv) 2 for the inertia weight. It is worth mentioning that the previously established values enhance our optimization problem's convergence speed. In table 1, we present a performance comparison between the PSO algorithm against built-in routines, namely, **NMaximize, NMinimize**, and **FindMaximum**,[4] which are available in widely-used mathematical software packages such as Wolfram Mathematica. Notice that, as the number of iterations increases, the numerical routines become more computationally demanding. Also, for the formulated optimization problem, the considered built-in routines fail to converge to a solution, mainly because the optimization methods used by these routines may not improve in every iteration, and the convergence is evaluated solely after a large number of iterations [50]. However, the PSO algorithm is capable of reaching a maximum solution with few iterations.

Fig. 4 illustrates the SOP versus transmit SNR γ_P, for different K-factor values at the RSI link, with PS ratio $\rho = 0.4$ and 0.8. We corroborate our analytical expressions via Monte Carlo simulations. It can be observed that our

[4] Among the methods implemented by the built-in routines of Wolfram Mathematica, we can cite the Nelder Mead; differential evolution; simulated annealing or the random search method for the **NMaximize** and **NMinimize** functions. Meanwhile, the **FindMaximum** function includes simpler methods such as the conjugate gradient, the Levenberg Marquardt and the interior-point method [50].

TABLE 1. Numerical optimization comparison.

Method	Iterations	Convergence
PSO	15	Yes
NMaximize	300	No
NMinimize	300	No
FindMaximum	2500	No

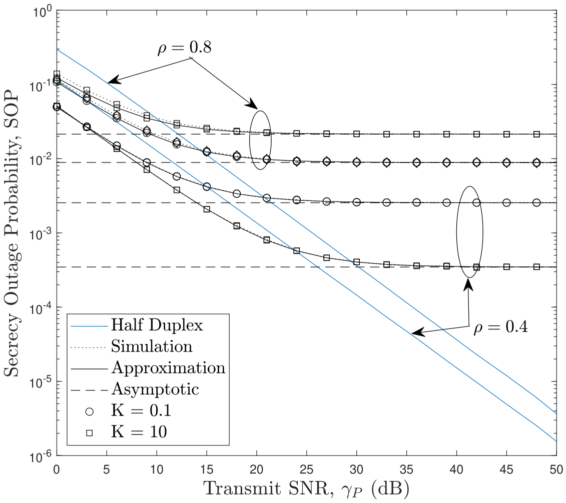

FIGURE 4. SOP vs transmit SNR for FD and HD relaying modes with different *K*-factor values at the RSI link and PS ratio $\rho = 0.4, 0.8$.

approximation is very tight, and perfectly matches the simulation results from medium to high SNR. In this figure, we also compare two relaying modes for the relay operation, namely, FD and HD modes. The HD mode analysis is provided only in terms of simulation. Note that, for low-to-medium values of the transmit SNR γ_P, the FD mode performance overcomes that of the HD. However, at high SNR, the HD mode reaches a better secrecy performance, independently of the amount of power employed for the EH process (determined by the PS ratio ρ). This behavior is expected since the system performance exhibits a floor caused by the RSI at the high SNR regime when the FD mode is employed. These results corroborate our findings in Remark 3 concerning the asymptotic analysis. Note also that employing more power for the ID process (lower value of ρ) results in an improved performance since the impact of the RSI at the relay is diminished. This fact is because the transmit power at the relay decreases as less amount of energy is harvested. Also, notice that a stronger LoS component (higher value of K) between the relay's antennas is beneficial for the system performance with a lower value of ρ. In contrast, when more power is allocated to the EH process (higher value of ρ), the system performance presents an opposite behavior since more transmit power is available at the relay from the EH process, as indicated by the relationship between ρ and the Rician-distributed channel gain $g_{\text{RR}}^{\mathcal{E}}$ in (3).

In Fig. 5 we have considered a two-dimensional network topology with S, D and E located at (0,0), (1,0) and (1,0.5),

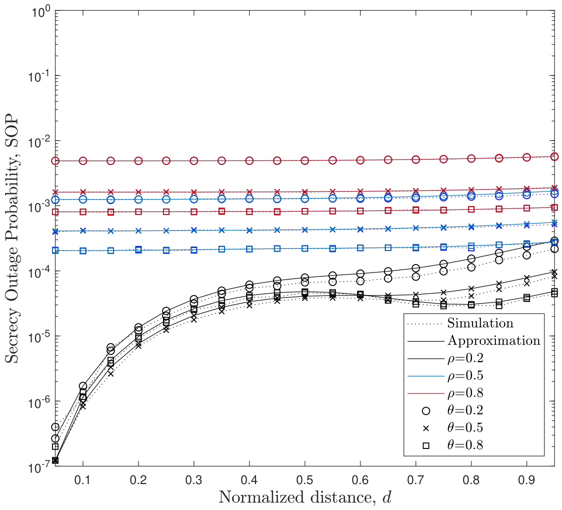

FIGURE 5. SOP vs normalized distance, *d*, for different values of ρ and θ.

respectively. Moreover, the average channel gains of all wireless links are assumed to be determined by the path loss, i.e., $\Omega_i = d_i^{-\varphi}, i \in$ (SR, RD, RE), where d_i is the distance between two terminals. The SOP is illustrated as a function of the normalized distance between S and R, $d = d_{\text{SR}}/d_{\text{SD}}$, considering different combinations of $\rho = 0.2, 0.5, 0.8$ and $\theta = 0.2, 0.5, 0.8$, with $K = 5$. Recall that, as pointed out in Remark 2, to obtain the approximation in (20), the SINR at the eavesdropper is independent of the channel gain at the link R-E and observe that except for the scenario with $\rho = 0.2$ in which the approximation derived in (20) slightly mismatches the Monte Carlo simulation results, the expression is very tight to the simulation curves. Notice that for $\rho = 0.2$, the best relay position is closer to S as more energy can be harvested on average to retransmit the information signal. We can also observe that in the vicinity of S ($\Omega_{\text{SR}} > \Omega_{\text{RD}}$), the amount of power allocated to the jamming signal does not significantly impact the secrecy performance. This behavior represents the best choice in terms of secrecy performance among all the considered jamming ratios, implying that it is better to allocate less energy to the EH process. On the other hand, as more power is allocated for EH (higher value of ρ), the normalized distance does not affect the secrecy performance, since the relay is allowed to harvest enough energy to recharge the batteries, independently of its relative position. Regarding the jamming signal, it can be observed that it is beneficial in terms of secrecy performance to consider a higher jamming power allocation ratio to deteriorate the eavesdropping channel without impact on the legitimate channel as D can perfectly cancel the jamming signal.

Fig. 6 illustrates the SOP versus the power splitting ratio for different combinations of the parameters at the RSI link after passive interference cancellation, i.e., K and $\Omega_{\text{RR}}^{\mathcal{E}}$. The total average channel gain at the RSI link is equal to $\Omega_{\text{RR}} = \Omega_{\text{RR}}^{\mathcal{E}} + \Omega_{\text{RR}}^{\mathcal{I}} = -30$ dB. Also, we consider a jamming power allocation ratio $\theta = 0.5$. As can be seen in (3), the energy

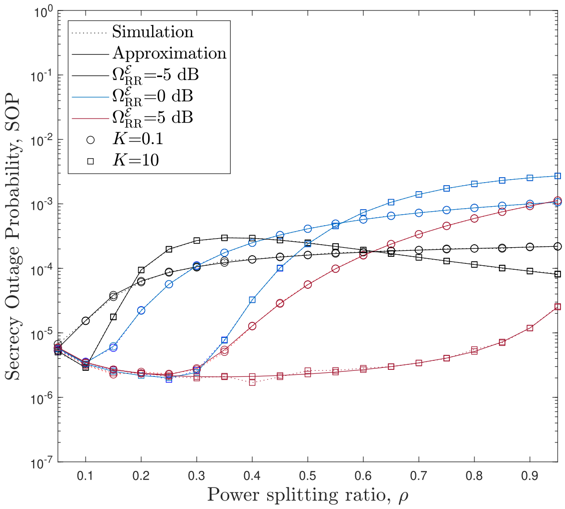

FIGURE 6. SOP vs power splitting ratio ρ for $K = 0.1, 10$ and $\Omega_{RR}^{\mathcal{E}} = -5, 0, 5$ dB, with $\theta = 0.5$.

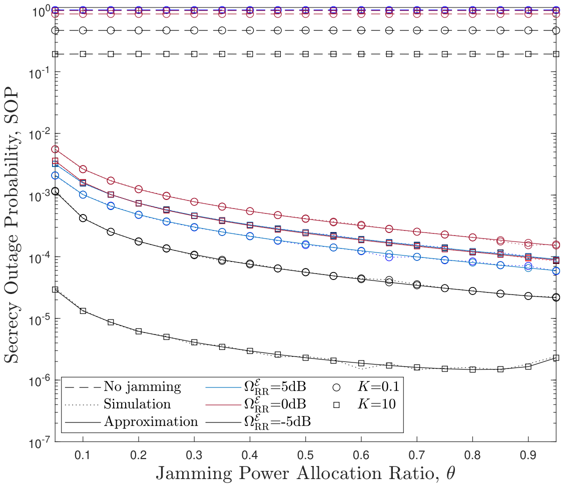

FIGURE 7. SOP vs jamming power allocation ratio θ for $K = 0.1, 10$ and $\Omega_{RR}^{\mathcal{E}} = -5, 0, 5$ dB, with $\rho = 0.5$.

available for transmission at R is related to ρ, K and $\Omega_{RR}^{\mathcal{E}}$. Therefore, even though the best performance for all curves tends to be attained when ρ is smaller, a slight variation of the other parameters may influence the performance. Note that the best performance is achieved when there is a higher RSI attenuation due to the antenna isolation and a stronger LoS component. As stated in [11], the AIC is based on the estimation of the self-interference wireless channel. With a stronger LoS component, the wireless channel's estimation is only related to the LoS component. The attenuation of that component gives most of the suppression achieved with the AIC. However, for the given value of Ω_{RR}, a weaker LoS component implies more indirect paths between the transmitter and receiver antennas, which indicates a worse channel condition after the passive IC and less efficient mitigation of interference by the AIC process. On the other hand, note that for higher values of ρ, the curves tends to have a decrease in performance, with the exception of the scenario with $\Omega_{RR}^{\mathcal{E}} = 5$ dB and $K = 10$, which presents an increase in performance for $\rho > 0.4$. This behaviour is expected since, in this case, the AIC achieves a higher average suppression, thus the estimation of the SI channel is improved.

Fig. 7 shows the SOP versus the jamming power allocation ratio for different combinations of the parameters at the RSI link after passive interference cancellation, i.e., K and $\Omega_{RR}^{\mathcal{E}}$. For this figure we also consider the total average channel gain at the RSI link equal to $\Omega_{RR} = \Omega_{RR}^{\mathcal{E}} + \Omega_{RR}^{\mathcal{I}} = -30$ dB, and the power splitting ratio is set to $\rho = 0.5$. Note that an improvement in the secrecy performance is attained as more power is allocated to the jamming signal transmission. Hence, as expected, there is a significant enhancement on the secrecy performance of the system if R transmits a jamming signal in comparison to when this technique is not employed. We can also observe a significant performance improvement when a higher SI attenuation is attained with passive interference cancellation, and a stronger direct path is available. However, for higher values of average channel gain at the self-energy recycling, the LoS component does not considerably impact the system performance. Therefore, we can conclude that the self-energy recycling channel's characteristics play a significant role in the secrecy performance. In this sense, it is crucial to determine how the EH process's power can affect the quality of transmission in terms of secrecy and improve the communication secrecy regardless of the amount of power allocated to the jamming signal used to hinder the eavesdropper.

Fig. 8 illustrates the SOP versus the average channel gain of the self-energy recycling link, $\Omega_{RR}^{\mathcal{E}}$, for distinct combinations of $K = 0.1, 5, 10$ and $\Omega_{RR}^{\mathcal{I}}$ with $\rho = 0.5$ and $\theta = 0.5$. Note that a higher suppression of SI can notably increase the secrecy performance, as expected. Also, it is observed that, as the self-energy recycling average channel gain decreases, the system performance exhibits a floor because the impact of the mitigation achieved with the antenna separation technique reduces [12]. Similarly, with a better performance of the passive suppression, the active interference cancellation's effectiveness reduces [11]. On the other hand, as $\Omega_{RR}^{\mathcal{E}}$ increases, the system reaches a critical point, where the transmit power of R in (3) is maximum and, therefore, the secrecy performance is highly affected. As previously stated in Fig. 6, after that point, as the self-energy recycling causes a lower attenuation, P_R decreases, and the average suppression achieved with AIC is higher since, from that point, the estimation of the SI channel is improved. Moreover, note that the power level of the LoS component can severely impact the secrecy performance. A weaker LoS component degrades the secrecy performance for higher values of $\Omega_{RR}^{\mathcal{E}}$ (>8 dB) and does not exhibit the same critical point as a stronger LoS component.

Fig. 9 illustrates the SOP as a function of the transmit SNR, γ_P, for different values of saturation power level,P_{max}, and sensitivity power level, P_{min} via Monte Carlo simulations. Here, we compare the proposed linear EH model against

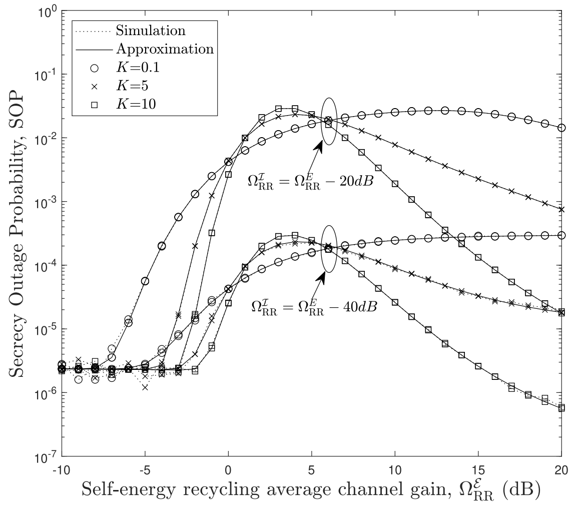

FIGURE 8. SOP vs self-energy recycling average channel gain, $\Omega^{\mathcal{E}}_{\mathrm{RR}}$, for different values of $K = 0.1, 5, 10$ and $\Omega^{\mathcal{I}}_{\mathrm{RR}}$, with $\rho = 0.5$ and $\theta = 0.5$.

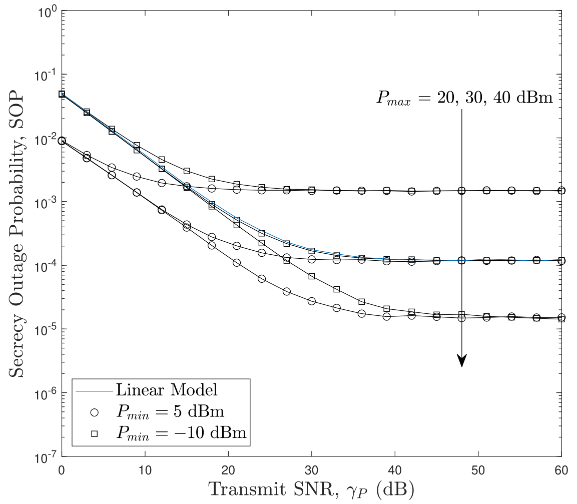

FIGURE 9. SOP vs transmit SNR for different values of P_{min} and P_{max} with $K = 5$, $\theta = 0.5$ and $\rho = 0.4$.

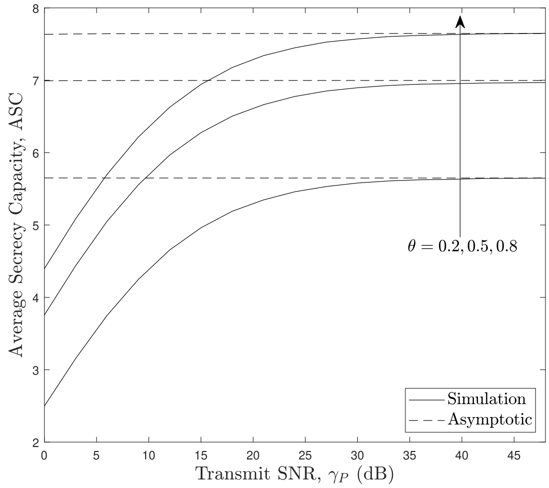

FIGURE 10. ASC vs Transmit SNR, γ_P, for different values of $\theta = 0.2, 0.5, 0.8$, with $\rho = 0.4$ and $K = 5$.

TABLE 2. Numerical high-snr slope and power offset.

Transmit SNR, γ_P (dB)	ASC$^{\infty}$	S_{∞} (bits/s/Hz)	$\mathcal{L}_{\infty}$ (bits/s/Hz)
40	6.968	0.524	-1×10^{-15}
60	6.968	0.350	0
80	6.968	0.262	-3×10^{-15}
100	6.968	0.210	0
300	6.968	0.006	1×10^{-14}

the non-linear counterpart. The system parameters are set to: $K = 5$, $\theta = 0.5$, and $\rho = 0.4$ From all curves, note that for $P_{max} = 30$ dBm and $P_{min} = -10$ dBm, the non-linear EH model overlaps those results obtained from the linear EH model. On the other hand, knowing that: i) the sensibility level of EH circuits is ≈ -27 dBm [51], and ii) the saturation level for EH circuits can support tens of milliWatts [52]. It can be observed that, under theses practical conditions, the proposed energy harvesting model can follow a linear model without incurring system performance penalties. Furthermore, stringent constrains on the saturation level lead to better performance for larger values of P_R, but higher values on the sensibility power level result in a faster convergence to the performance floor, as expected.

In Fig. 10 and Table 2, we evaluate the average secrecy capacity in terms of the system's transmit SNR. For the summations in (27) and (28), the values of $n = 180$, $m = 12$ and $z = 12$ provide an adequate fit. Furthermore, we also considered $\rho = 0.4$ and $K = 5$. From Fig. 10 and as previously stated for Fig. 7, it can be observed that increasing the amount of power allocated to the jamming signal highly improves the secrecy performance, as expected. Moreover, note that, similar to Fig. 4, the system performance exhibits a floor at the high SNR regime caused by the RSI. Thus, the high-SNR slope for this system equals 0.

To provide a more descriptive analysis in terms of S_{∞} and $\mathcal{L}_{\infty}$, for Table. 2 we have considered $\gamma_P = 40, 60, 80$, 100 and 300 dB and $\theta = 0.5$. Note that, as observed in (UM, Fig. 8), the floor observed at high-SNR indicates that the $S_{\infty} \to 0$. On the other hand, for the power offset analysis, it can be easily seen that given the definition in (31) and the attained values for S_{∞}, $\mathcal{L}_{\infty}$ is zero.

In the following figures, the effect of the power splitting ratio ρ, jamming power allocation ratio θ, target rate $\mathcal{R}$, and target secrecy rate $\mathcal{R}_s$ on the confidential throughput is illustrated. More specifically, Fig. 11 illustrates the effect of the power splitting ratio ρ and jamming power allocation ratio θ on the system throughput without considering the SOP constraint of the optimization problem in (33). We assume that $\mathcal{R}_s = \mathcal{R} = 1$ bps/Hz. As previously observed, the system has an increase in secrecy performance when less power is used for the EH process. On the other hand, the amount of

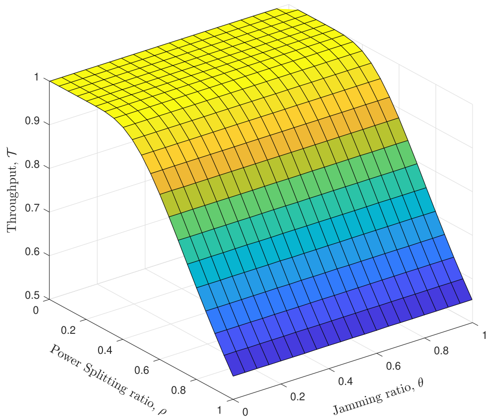

FIGURE 11. Throughput vs ρ, θ with $\mathcal{R}_s = \mathcal{R} = 1$ bps/Hz.

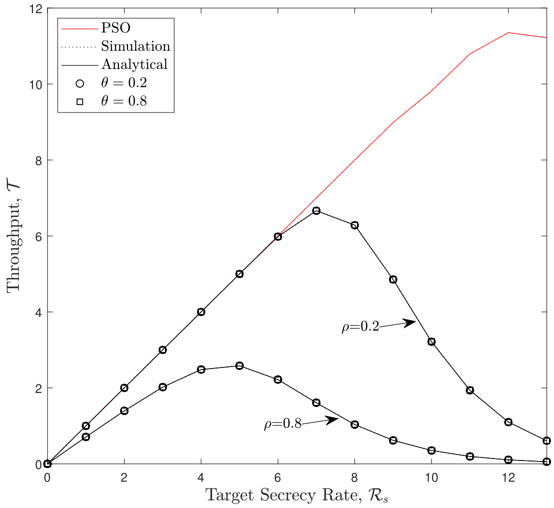

FIGURE 12. Throughput vs target secrecy rate, $\mathcal{R}_s$ with $K = 5$ and $\epsilon = 0.1$.

power allocated to the jamming signal does not impact the throughput given in (32).

In Fig. 12, the confidential throughput versus the secrecy rate $\mathcal{R}_s$ is analyzed. We consider that $\mathcal{R}_s = \mathcal{R}$, $K = 5$ and $\epsilon = 0.1$. Note that the optimization of the parameters allows the system to achieve higher rates, thus increasing the throughput. Moreover, even considering the SOP constraint in the analysis, similarly as in Fig. 11, θ does not impact the performance with smaller values of $\mathcal{R}_s$. However, the optimization shows that when the secrecy rate is greater than 8, the optimal throughput is achievable only if a significant amount of jamming is used to guarantee the security ($\theta \sim 0.7$). On the other hand, ρ notably impacts the maximum throughput achieved. As $\mathcal{R}_s$ increases, the optimal power splitting ratio obtained with the PSO algorithm decreases. The best throughput attained ($\mathcal{T} \sim 11.35$) has a target secrecy rate of $\mathcal{R}_s = 12$ and $\rho \sim 0.0055$. Based on [51], it still represents a practical scenario since the EH receiver sensitively is close to -27 dBm.

Fig 13 shows the confidential throughput $\mathcal{T}$ versus the SOP constraint ϵ with $K = 5$. The attained optimal results are compared with scenarios with fixed parameters, and regardless of the secrecy constraint, those results still achieve better performance. Unlike previous figures, we consider that $\mathcal{R}_s \geq \mathcal{R}$. Note that, for $\mathcal{R}_s = 2\mathcal{R}$, a significant increase in performance is obtained. Also, note that considering more flexible parameters, as the average channel gain at the RSI link after AIC on R, it is possible to increase the performance. However, it is necessary to allocate more power to the EH process ($\rho \sim 0.2$) to achieve the maximum throughput. Moreover, the secrecy constraint considerably impacts performance. With a less restricted secrecy constraint ϵ, the system can attain higher optimal throughput values. On the other hand, to ensure higher security (e.g., $\epsilon = 0.001$), it is necessary to allocate more power to the jamming signal ($\theta \sim 0.8$) to obtain the maximal throughput.

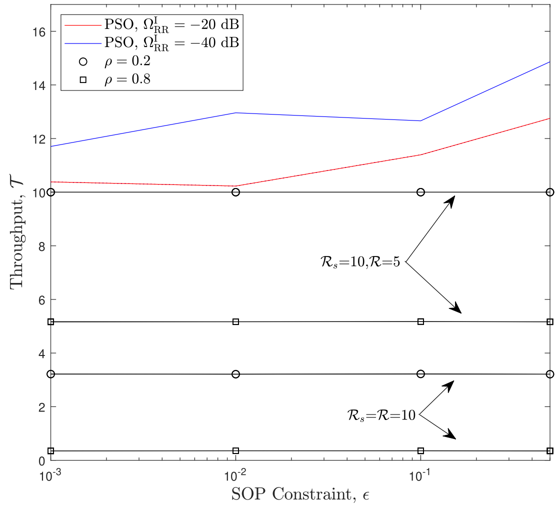

FIGURE 13. Throughput vs secrecy constraint, ϵ with $K = 5$.

VIII. CONCLUSION

This paper investigated the performance of a dual-hop FD-DF relaying network, in which the relay has energy constraints in terms of the secrecy outage probability and the maximal confidential throughput. A PS-based SWIPT technique was used to provide the relay with energy. In order to render the communication between source and destination secure, it was considered that the relay could use a fraction of its transmit power to send a jamming signal, which is intended to degrade the eavesdropper's channel. The destination was assumed to have full knowledge of the jamming signal so that it can entirely cancel it. A closed-form approximation expression for the secrecy outage probability was derived. Such expression proved to be very tight to the Monte Carlo simulation at medium-to-high SNR. The results showed that the self-energy recycling average channel gain highly impacts the secrecy performance. Depending on channel conditions, the amount of power allocated to the EH process can be optimized. It is possible to improve the secrecy performance regardless of how much power is allocated to the jamming signal during the transmission. Moreover, the LoS component acts as a critical parameter that affects the secrecy performance. A stronger LoS component significantly improves the system's security as long as less power is allocated to the EH process. However, as more energy is used to charge the batteries at the relay, a higher K-factor does not impact the performance. We also used heuristic optimization to maximize the confidential throughput by employing a PSO algorithm, showing that the maximum confidential throughput is achieved with lower ρ values. Also, numerical results showed that the power splitting ratio significantly impacted the system performance than the jamming power allocation ratio. However, by increasing the secrecy rate allowed for transmission and considering lower secrecy constraints, the optimization analysis showed that the amount of power allocated to the jamming signal becomes an important parameter, and it should be higher to ensure that the optimal throughput is achieved.

APPENDIX A
PROOF OF PROPOSITION 1

By replacing (7) and (8) into (14), Θ can be rewritten as

$$\begin{aligned}\Theta &= \Pr\Bigg(\frac{\gamma_P(1-\rho)g_{\mathrm{SR}}\left(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}\right)}{\gamma_P\eta(1-\rho)\rho g_{\mathrm{RR}}^{\mathcal{I}}g_{\mathrm{SR}}-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}+1} > \tau,\\ &\quad \frac{(1-\theta)\left(\gamma_P\eta\rho g_{\mathrm{SR}}g_{\mathrm{RD}}\right)}{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}} > \tau\Bigg),\\ &= \Pr\Bigg(g_{\mathrm{RD}} > \frac{\tau(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}})}{(1-\theta)\gamma_P\eta\rho g_{\mathrm{SR}}}, g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho},\\ &\quad g_{\mathrm{SR}}\gamma_P > \frac{\tau}{1-\rho}\Bigg| g_{\mathrm{RR}}^{\mathcal{I}} < \alpha\Bigg)\left(g_{\mathrm{RR}}^{\mathcal{I}} < \alpha\right). \qquad (34)\end{aligned}$$

where $\alpha = \frac{(\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}-1)(\gamma_P(\rho-1)g_{\mathrm{SR}}+\tau)}{\gamma_P\eta(1-\rho)\rho\tau g_{\mathrm{SR}}}$. Regarding the RVs of the system previously described in Definition II, Θ can be obtained as

$$\begin{aligned}\Theta &= \int_0^{\frac{1}{\eta\rho}}\int_0^{\frac{\tau}{\gamma_P-\gamma_P\rho}}\int_{\frac{\tau(1-\eta\rho z)}{(1-\theta)\gamma_P\eta\rho y}}^{\infty} F_{g_{\mathrm{RR}}^{\mathcal{I}}}(\alpha)f_{g_{\mathrm{RD}}}(x)f_{g_{\mathrm{SR}}}(y)\\ &\quad\times f_{g_{\mathrm{RR}}^{\mathcal{E}}}(z)dxdydz,\\ &= \int_0^{\frac{1}{\eta\rho}}\int_0^{\frac{\tau}{\gamma_P-\gamma_P\rho}} -\frac{e^{\left(-\frac{(K+1)z}{\Omega_{RR}^{\mathcal{E}}}-\frac{y}{\Omega_{\mathrm{SR}}}-K+\frac{\tau(\eta\rho z-1)}{(1-\theta)\gamma_P\eta\rho y\Omega_{RD}}\right)}(K+1)}{\Omega_{\mathrm{RR}}^{\mathcal{E}}\Omega_{\mathrm{SR}}}\\ &\quad\times I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)\left(e^{\left(\frac{(\eta\rho z-1)(\gamma_P(\rho-1)y+\tau)}{\gamma_P\eta(\rho-1)\rho\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}y}\right)}-1\right)dydz.\end{aligned} \qquad (35)$$

To facilitate the analysis in terms of y, (35) is split into two integrals. Furthermore, by using the expansion of the exponential function [39, Eq. 1.211.1], (35) can be expressed as

$$\begin{aligned}\Theta_1 &= \sum_{m=0}^{\infty}\int_0^{\frac{1}{\eta\rho}}\int_0^{\frac{\tau}{\gamma_P-\gamma_P\rho}}\frac{e^{-\frac{(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}-\frac{z}{\Omega_{\mathrm{SR}}}-K}\left(\frac{\tau(\eta\rho z-1)}{(1-\theta)\gamma_P\eta\rho z\Omega_{\mathrm{RD}}}\right)^m}{m!\Omega_{\mathrm{RR}}^{\mathcal{E}}\Omega_{\mathrm{SR}}}\\ &\quad\times(K+1)I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)dydz,\\ &= \sum_{m=0}^{\infty}\int_0^{\frac{1}{\eta\rho}}\frac{e^{-\frac{(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}-K}\Gamma\left(1-m,\frac{\tau}{\gamma_P\Omega_{\mathrm{SR}}-\gamma_P\rho\Omega_{\mathrm{SR}}}\right)(K+1)}{m!\Omega_{\mathrm{RR}}^{\mathcal{E}}\left(\frac{(1-\theta)\gamma_P\eta\rho\Omega_{\mathrm{SR}}\Omega_{\mathrm{RD}}}{\tau}\right)^m}\\ &\quad\times(\eta\rho z-1)^m I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)dz.\end{aligned} \qquad (36)$$

$$\begin{aligned}\Theta_2 &= \sum_{m=0}^{\infty}\int_0^{\frac{1}{\eta\rho}}\int_0^{\frac{\tau}{\gamma_P-\gamma_P\rho}} -\frac{\left(\frac{(\eta\rho z-1)\left(\rho\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}-\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}+(1-\theta)\Omega_{\mathrm{RD}}\right)}{(1-\theta)\gamma_P\eta(\rho-1)\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}y\Omega_{\mathrm{RD}}}\right)^m}{e^K(K+1)^{-1}m!\Omega_{\mathrm{RR}}^{\mathcal{E}}\Omega_{\mathrm{SR}}}\\ &\quad\times e^{\left(\frac{\eta\rho z-1}{\eta\rho\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}}-\frac{(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}-\frac{y}{\Omega_{\mathrm{SR}}}\right)}I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)dydz,\\ &= \sum_{m=0}^{\infty}\int_0^{\frac{1}{\eta\rho}} -\frac{\left(\frac{(\eta\rho z-1)\left(\rho\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}-\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}+(1-\theta)\Omega_{\mathrm{RD}}\right)}{(1-\theta)\gamma_P\eta(\rho-1)\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}y\Omega_{\mathrm{RD}}}\right)^m}{e^{-\left(\frac{\eta\rho z-1}{\eta\rho\tau\Omega_{\mathrm{RR}}^{\mathcal{I}}}\right)}e^{\left(\frac{(K+1)z+K\Omega_{\mathrm{RR}}^{\mathcal{E}}}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)}m!\Omega_{\mathrm{RR}}^{\mathcal{E}}}\\ &\quad\times(K+1)\Gamma\left(1-m,\frac{\tau}{(\gamma_P-\gamma_P\rho)\Omega_{\mathrm{SR}}}\right)\\ &\quad\times I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)dz.\end{aligned} \qquad (37)$$

Finally, by considering the series expansion of the Bessel Function [39, Eq. 8.447.1] in (36) and (37) and by adding $\Theta = \Theta_1 + \Theta_2$, (17) can be achieved.

APPENDIX B
Proof OF PROPOSITION 2

For the proposed system, the SOP can be formulated as (19)

$$\begin{aligned}\mathrm{SOP} &= \Pr\left(\frac{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}}{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{RE}}\}} < \tau_{\mathrm{s}}\right)\\ &= \Pr\left(\frac{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}-\tau_{\mathrm{s}}}{\tau_{\mathrm{s}}} < \min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{RE}}\}\right)\\ &= \Pr\Bigg(\frac{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}}{\tau_{\mathrm{s}}} < \gamma_{\mathrm{R}}+1,\\ &\quad \frac{1+\min\{\gamma_{\mathrm{R}},\gamma_{\mathrm{D}}\}}{\tau_{\mathrm{s}}} < \gamma_{\mathrm{RE}}+1\Bigg).\end{aligned} \qquad (38)$$

Next, the SOP can be further split into two probability terms regarding the valid cases of γ_{R} and γ_{D}. Therefore, (38) can be rewritten as

$$\begin{aligned}\mathrm{SOP} &= \Pr\left(1+\gamma_{\mathrm{R}} < \tau_{\mathrm{s}}\gamma_{\mathrm{R}}+\tau_{\mathrm{s}}, 1+\gamma_{\mathrm{R}} < \tau_{\mathrm{s}}\gamma_{\mathrm{RE}}+\tau_{\mathrm{s}}|\gamma_{\mathrm{R}} < \gamma_{\mathrm{D}}\right)\\ &\quad\times\Pr(\gamma_{\mathrm{R}} < \gamma_{\mathrm{D}})+\Pr\left(1+\gamma_{\mathrm{D}} < \tau_{\mathrm{s}}\gamma_{\mathrm{R}}+\tau_{\mathrm{s}},\right.\\ &\quad\left.1+\gamma_{\mathrm{D}} < \tau_{\mathrm{s}}\gamma_{\mathrm{RE}}+\tau_{\mathrm{s}}|\gamma_{\mathrm{R}} > \gamma_{\mathrm{D}}\right)\Pr(\gamma_{\mathrm{R}} > \gamma_{\mathrm{D}})\\ &= \underbrace{\Pr\left(\gamma_{\mathrm{R}} > 0, \gamma_{\mathrm{R}} < \tau_{\mathrm{s}}\gamma_{\mathrm{RE}}+\tau_{\mathrm{s}}-1, \gamma_{\mathrm{D}} > 0\right)}_{I_1}\\ &\quad+\underbrace{\Pr\left(\gamma_{\mathrm{R}} > -1+\tau_{\mathrm{s}}+\tau_{\mathrm{s}}\gamma_{\mathrm{RE}}, \gamma_{\mathrm{D}} < \tau_{\mathrm{s}}\gamma_{\mathrm{RE}}+\tau_{\mathrm{s}}-1\right)}_{I_2}.\end{aligned} \qquad (39)$$

A closed form approximation for the terms I_1 and I_2, which is accurate from medium-to-high SNR regime can be obtained by approximating the SINR γ_{RE} given in (9) when $\gamma_P \to \infty$ to $\gamma_{\mathrm{RE}} \approx (1-\theta)/\theta$. Furthermore, I_1 and I_2 can be reorganized and further derived as showing next. Firstly, by replacing (7) and (8) as well as the approximate form of (9) into (39), we get

$$\begin{aligned} I_1 \approx \Pr\Bigg(&\frac{(1-\theta)\left(\gamma_P\eta\rho g_{\mathrm{SR}} g_{\mathrm{RD}}\right)}{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}} > 0,\\ &0 < \frac{\gamma_P(1-\rho)g_{\mathrm{SR}}\left(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}\right)}{\gamma_P\eta(1-\rho)\rho g_{\mathrm{RR}}^{\mathcal{I}} g_{\mathrm{SR}} - \eta\rho g_{\mathrm{RR}}^{\mathcal{E}}+1}\\ &< \frac{(1-\theta)\tau_{\mathrm{s}}}{\theta}+\tau_{\mathrm{s}}-1\Bigg) \end{aligned} \tag{40}$$

$$\begin{aligned} I_2 \approx \Pr\Bigg(&\frac{(1-\theta)\tau_{\mathrm{s}}}{\theta}+\tau_{\mathrm{s}}-1 > \frac{(1-\theta)\left(\gamma_P\eta\rho g_{\mathrm{SR}} g_{\mathrm{RD}}\right)}{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}} > 0,\\ &\frac{\gamma_P(1-\rho)g_{\mathrm{SR}}\left(1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}\right)}{\gamma_P\eta(1-\rho)\rho g_{\mathrm{RR}}^{\mathcal{I}} g_{\mathrm{SR}} - \eta\rho g_{\mathrm{RR}}^{\mathcal{E}}+1} > \frac{(1-\theta)\tau_{\mathrm{s}}}{\theta}+\tau_{\mathrm{s}}-1\Bigg). \end{aligned} \tag{41}$$

Then, by solving I_1 in terms of the RVs of the system, it can be splitted into two probability terms regarding the valid regions of $g_{\mathrm{RR}}^{\mathcal{I}}$ and re-expressed as

$$\begin{aligned} I_1 \approx{}& \Pr\left(g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho}, g_{\mathrm{SR}} > \beta, g_{\mathrm{RD}} > 0 \,\middle|\, g_{\mathrm{RR}}^{\mathcal{I}} > \sigma\right)\Pr\left(g_{\mathrm{RR}}^{\mathcal{I}} > \sigma\right)\\ &+\Pr\left(g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho}, g_{\mathrm{SR}} \le \beta, g_{\mathrm{RD}} > 0 \,\middle|\, g_{\mathrm{RR}}^{\mathcal{I}} > 0\right)\\ &\times\Pr\left(g_{\mathrm{RR}}^{\mathcal{I}} > 0\right)\\ \approx{}& \underbrace{\Pr\left(g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho}, g_{\mathrm{SR}} > \beta, g_{\mathrm{RD}} > 0, g_{\mathrm{RR}}^{\mathcal{I}} > \sigma\right)}_{I_{1,a}}\\ &+\underbrace{\Pr\left(g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho}, g_{\mathrm{SR}} \le \beta, g_{\mathrm{RD}} > 0, g_{\mathrm{RR}}^{\mathcal{I}} > 0\right)}_{I_{1,b}}, \end{aligned} \tag{42}$$

where $\beta = \frac{\theta-\tau_{\mathrm{s}}}{\gamma_P\theta\rho-\gamma_P\theta}$, and $\sigma = \frac{\left(\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}-1\right)\left(\gamma_P\theta(\rho-1)g_{\mathrm{SR}}-\theta+\tau_{\mathrm{s}}\right)}{\gamma_P\eta(\rho-1)\rho g_{\mathrm{SR}}(\theta-\tau_{\mathrm{s}})}$. Similarly, I_2 can be rearranged as

$$\begin{aligned} I_2 \approx{}& \Pr\Bigg(g_{\mathrm{RD}} < \frac{(\theta-\tau_{\mathrm{s}})\left(\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}-1\right)}{\gamma_P\eta(1-\theta)\theta\rho g_{\mathrm{SR}}}, g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho},\\ &g_{\mathrm{SR}} > \beta g_{\mathrm{RR}}^{\mathcal{I}} \le \sigma\Bigg)\Pr\left(g_{\mathrm{RR}}^{\mathcal{I}} \le \sigma\right)\\ \approx{}& \Pr\Bigg(g_{\mathrm{RD}} < \frac{(\theta-\tau_{\mathrm{s}})\left(\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}-1\right)}{\gamma_P\eta(1-\theta)\theta\rho g_{\mathrm{SR}}}, g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho},\\ &g_{\mathrm{SR}} > \beta, g_{\mathrm{RR}}^{\mathcal{I}} \le \sigma\Bigg). \end{aligned} \tag{43}$$

Thus, considering the PDFs and CDF of the RVs of the system previously described in Definition II, the probability $I_{1,a}$ can be obtained as

$$\begin{aligned} I_{1,a} ={}& \int_0^{\frac{1}{\eta\rho}}\int_0^{\beta}\int_0^{\infty}\left(1-F_{g_{\mathrm{RR}}^{\mathcal{I}}}(\sigma)\right)f_{g_{\mathrm{RD}}}(x)f_{g_{\mathrm{SR}}}(y)f_{g_{\mathrm{RR}}^{\mathcal{E}}}(z)dxdydz\\ ={}& \int_0^{\frac{1}{\eta\rho}}\int_0^{\beta}\frac{e^{\left(-\frac{(\eta\rho z-1)\left(\gamma_P\theta(\rho-1)y-\theta+\tau_{\mathrm{s}}\right)}{\gamma_P\eta(\rho-1)\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}y(\theta-\tau_{\mathrm{s}})}-\frac{(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}-\frac{y}{\Omega_{\mathrm{SR}}}-K\right)}(K+1)}{\Omega_{\mathrm{RR}}^{\mathcal{E}}\Omega_{\mathrm{SR}}}\\ &\times I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)dydz, \end{aligned} \tag{44}$$

Due to the difficult tractability of (44), a good approximation, accurate from medium-to-high SNR regime can be obtained by applying $\lim_{\gamma_P\to\infty}\sigma$. Then, $I_{1,a}$ can be approximated by

$$\begin{aligned} I_{1,a} \approx{}& \int_0^{\frac{1}{\eta\rho}}\int_0^{\beta}\frac{e^{\left(\frac{\theta-\eta\theta\rho z}{\eta\theta\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}-\eta\rho\tau_{\mathrm{s}}\Omega_{\mathrm{RR}}^{\mathcal{I}}}-\frac{(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}-\frac{y}{\Omega_{\mathrm{SR}}}+K\right)}(K+1)}{\Omega_{\mathrm{RR}}^{\mathcal{E}}\Omega_{\mathrm{SR}}}\\ &\times I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathrm{E}}}}\right)dydz\\ \approx{}& \int_0^{\frac{1}{\eta\rho}}\frac{e^{\left(z\left(-\frac{\theta}{\Omega_{\mathrm{RR}}^{\mathcal{I}}(\theta-\tau_{\mathrm{s}})}-\frac{K+1}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)+\frac{\theta}{\eta\theta\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}-\eta\rho\tau_{\mathrm{s}}\Omega_{\mathrm{RR}}^{\mathcal{I}}}+\frac{\tau_{\mathrm{s}}}{\gamma_P\theta(\rho-1)\Omega_{\mathrm{SR}}}\right)}}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}\\ &\times e^{\frac{1}{\gamma_P\Omega_{\mathrm{SR}}-\gamma_P\rho\Omega_{\mathrm{SR}}}-K}(K+1)I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)dz. \end{aligned} \tag{45}$$

Next, by considering the series expansion of the Bessel function in (45), as given in [39, Eq. 8.447.1], $I_{1,a}$ can be written as

$$\begin{aligned} I_{1,a} \approx{}& \sum_{n=0}^{\infty}\frac{e^{-K}K^n}{(n!)^2}\Bigg((K+1)^{n+1}\left(\frac{\theta\Omega_{\mathrm{RR}}^{\mathcal{E}}}{\Omega_{\mathrm{RR}}^{\mathcal{I}}(\theta-\tau_{\mathrm{s}})}+K+1\right)^{-n-1}\\ &\times e^{\left(\frac{\theta}{\eta\theta\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}-\eta\rho\tau_{\mathrm{s}}\Omega_{\mathrm{RR}}^{\mathcal{I}}}+\frac{\theta-\tau_{\mathrm{s}}}{\gamma_P\theta\Omega_{\mathrm{SR}}-\gamma_P\theta\rho\Omega_{\mathrm{SR}}}\right)}\Bigg(\Gamma(n+1)\\ &-\Gamma\left(n+1, \frac{\frac{K+1}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}+\frac{\theta}{(\theta-\tau_{\mathrm{s}})\Omega_{\mathrm{RR}}^{\mathcal{I}}}}{\eta\rho}\right)\Bigg)\Bigg). \end{aligned} \tag{46}$$

Similarly, $I_{1,b}$ can be obtained as

$$\begin{aligned} I_{1,b} ={}& \int_0^{\frac{1}{\eta\rho}}\int_0^{\infty}\int_0^{\infty}F_{g_{\mathrm{SR}}}(\beta)f_{g_{\mathrm{RD}}}(x)f_{g_{\mathrm{RR}}^{\mathcal{I}}}(y)f_{g_{\mathrm{RR}}^{\mathcal{E}}}(z)dxdydz\\ \approx{}& \sum_{n=0}^{\infty}\frac{e^{-K}K^n}{(n!)^2}\left(\Gamma(n+1)-\Gamma\left(n+1, \frac{K+1}{\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{E}}}\right)\right)\\ &\times\left(1-e^{\frac{\theta-\tau_{\mathrm{s}}}{\gamma_P\theta\Omega_{\mathrm{SR}}-\gamma_P\theta\rho\Omega_{\mathrm{SR}}}}\right). \end{aligned} \tag{47}$$

Therefore, by adding the terms $I_1 \approx I_{1,a} + I_{1,b}$ and making some simplifications, (21) can be achieved. In addition, by following the same reasoning, the probability I_2 can be expressed as

$$
\begin{aligned}
I_2 &= \int_0^{\frac{1}{\eta\rho}} \int_\beta^\infty \int_0^{\frac{(\theta-\tau_s)\left(\eta\rho g_{RR}^{\mathcal{E}}-1\right)}{\gamma_P\eta(1-\theta)\theta\rho g_{SR}}} F_{g_{RR}^{\mathcal{I}}}(\sigma) f_{g_{RD}}(x) f_{g_{SR}}(y) \\
&\quad \times f_{g_{RR}^{\mathcal{E}}}(z) dx dy dz \\
&= \int_0^{\frac{1}{\eta\rho}} \int_\beta^\infty \frac{-e^{-\frac{(K+1)z}{\Omega_{RR}^{\mathcal{E}}}-\frac{y}{\Omega_{SR}}-K}(K+1)}{\Omega_{RR}^{\mathcal{E}}\Omega_{SR}} I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{RR}^{\mathcal{E}}}}\right) \\
&\quad \times \left(-1+e^{\frac{(\theta-\tau_s)(\eta\rho z-1)}{\gamma_P\eta(1-\theta)\theta\rho y}}\right)\left(1-e^{-\sigma}\right) dy dz. \qquad (48)
\end{aligned}
$$

Using the Maclaurin expression for the exponencial function [39, Eq. 0.318.2], we have that $e^\lambda \simeq 1+\lambda$ for small λ. Applying this into the term $e^{\frac{(\theta-\tau_s)(\eta\rho z-1)}{\gamma_P\eta(1-\theta)\theta\rho y}}$ a closed-form approximation for the integral (48) can be obtained. Additionally, (48) is split in two integrals in order to analyze it in terms of y variable, so we have

$$
\begin{aligned}
I_{2,a} &\approx \int_0^{\frac{1}{\eta\rho}} \int_\beta^\infty -\frac{(K+1)e^{-\frac{(K+1)z}{\Omega_{RR}^{\mathcal{E}}}-\frac{y}{\Omega_{SR}}-K}(\theta-\tau_s)(\eta\rho z-1)}{\left(\Omega_{RR}^{\mathcal{E}}\Omega_{SR}\right)(\gamma_P\eta(\theta-1)\theta\rho y\Omega_{RD})} \\
&\quad \times I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{RR}^{\mathcal{E}}}}\right) dy dz \\
&\approx \int_0^{\frac{1}{\eta\rho}} -\frac{(K+1)(\theta-\tau_s)(\eta\rho z-1)\, e^{-\frac{(K+1)z}{\Omega_{RR}^{E}}-K}}{\gamma_P\eta(\theta-1)\theta\rho\Omega_{RR}^{\mathcal{E}}\Omega_{SR}\Omega_{RD}} \\
&\quad \times \Gamma\left(0, \frac{\tau_s-\theta}{(\gamma_P\theta-\gamma_P\theta\rho)\Omega_{SR}}\right) I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{RR}^{\mathcal{E}}}}\right) dz. \qquad (49)
\end{aligned}
$$

$$
\begin{aligned}
I_{2,b} &\approx \int_0^{\frac{1}{\eta\rho}} \int_\beta^\infty -\frac{(K+1)e^{-\frac{(K+1)z}{\Omega_{RR}^{\mathcal{E}}}-\frac{y}{\Omega_{SR}}-K}(\theta-\tau_s)(\eta\rho z-1)}{\left(\Omega_{RR}^{\mathcal{E}}\Omega_{SR}\right)(\gamma_P\eta(\theta-1)\theta\rho y\Omega_{RD})} \\
&\quad \times e^{-\sigma} I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{RR}^{\mathcal{E}}}}\right) dy dz. \qquad (50)
\end{aligned}
$$

Using the series representation of the exponential function [39, Eq. 1.211.1], (50) can be rewritten as

$$
\begin{aligned}
I_{2,b} &\approx \sum_{\phi=0}^{\infty} \int_0^{\frac{1}{\eta\rho}} \int_\beta^\infty -\frac{(K+1)e^{-\frac{(K+1)z}{\Omega_{RR}^{\mathcal{E}}}-\frac{y}{\Omega_{SR}}-K}(\theta-\tau_s)e^{-\frac{\theta(\eta\rho z-1)}{\eta\rho\Omega_{RR}^{\mathcal{I}}(\theta-\tau_s)}}}{\left(\Omega_{RR}^{\mathcal{E}}\Omega_{SR}\right)(\gamma_P\eta(\theta-1)\theta\rho y\Omega_{RD})} \\
&\quad \times (\eta\rho z-1)\frac{\left(\frac{\eta\rho z-1}{\gamma_P\eta(\rho-1)\rho\Omega_{RR}^{\mathcal{I}}y}\right)^\phi}{\phi!} I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{RR}^{\mathcal{E}}}}\right) dy dz \\
&\approx \sum_{\phi=0}^{\infty} \int_0^{\frac{1}{\eta\rho}} \frac{(K+1)(\eta\rho z-1)\, e^{\left(\frac{\theta-\eta\theta\rho z}{\eta\theta\rho\Omega_{RR}^{\mathcal{I}}-\eta\rho\tau_s\Omega_{RR}^{\mathcal{I}}}-\frac{(K+1)z}{\Omega_{RR}^{\mathcal{E}}}-K\right)}}{\gamma_P\eta(\theta-1)\theta\rho\phi!\Omega_{RR}^{\mathcal{E}}\Omega_{RD}\Omega_{SR}} \\
&\quad \times \left(\frac{1-\eta\rho z}{\gamma_P\eta\rho\Omega_{RR}^{\mathcal{I}}\Omega_{SR}-\gamma_P\eta\rho^2\Omega_{RR}^{\mathcal{I}}\Omega_{SR}}\right)^\phi I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega_{RR}^{\mathcal{E}}}}\right) \\
&\quad \times (\theta-\tau_s)\Gamma\left(-\phi, -\frac{\theta-\tau_s}{\gamma_P\theta\Omega_{SR}-\gamma_P\theta\rho\Omega_{SR}}\right) dz. \qquad (51)
\end{aligned}
$$

Finally, by again considering the series expansion of the Bessel function in (49) and (51), and by adding $I_2 \approx I_{2,a} + I_{2,b}$, (22) can be obtained.

APPENDIX C
PROOF OF PROPOSITION 3

Given the definition of the end-to-end SINR at the legitimate receiver presented in Section II. We can express the CDF of γ_L as

$$
\begin{aligned}
F_L(\gamma) &= \Pr(\min(\gamma_R, \gamma_D) < \gamma), \\
&= \Pr(\gamma_R < \gamma | \gamma_D > 0)\Pr(\gamma_D > 0) \\
&\quad + \Pr(\gamma_R > \gamma | \gamma_D < \gamma)\Pr(\gamma_D < \gamma), \\
&= \Pr(\gamma_R < \gamma, \gamma_D > 0) + \Pr(\gamma_R > \gamma, \gamma_D < \gamma), \qquad (52)
\end{aligned}
$$

By considering the high SNR regime on the received SINR expressions given in (7), F_L can be rewritten as

$$
\begin{aligned}
F_L^\infty(\gamma) &= \Pr\left(g_{RR}^{\mathcal{I}} > \frac{1-\eta\rho g_{RR}^{\mathcal{E}}}{\eta\rho\gamma}, g_{RR}^{\mathcal{E}} < \frac{1}{\eta\rho}, g_{SR} > 0, g_{RD} > 0\right) \\
&\quad + \Pr\left(g_{RR}^{\mathcal{I}} < \frac{1-\eta\rho g_{RR}^{\mathcal{E}}}{\eta\rho\gamma}, g_{RR}^{\mathcal{E}} < \frac{1}{\eta\rho}, g_{SR} > 0,\right. \\
&\quad \left. g_{RD} < \frac{\gamma-\gamma\eta\rho g_{RR}^{\mathcal{E}}}{(1-\theta)(\gamma_P\eta\rho g_{SR})}\right), \qquad (53)
\end{aligned}
$$

In terms of the RVs of the system, $F_L^\infty(\gamma)$ can be splitted into two parts, $F_{L1}^\infty(\gamma)$ and $F_{L2}^\infty(\gamma)$, as

$$
F_{L1}^\infty(\gamma) = \int_0^{\frac{1}{\eta\rho}} \frac{I_0\left(2\sqrt{\frac{K(K+1)g_{RR}^{\mathcal{E}}}{\Omega_{RR}^{\mathcal{E}}}}\right)e^{-\frac{1-\eta\rho g_{RR}^{\mathcal{E}}}{\gamma\eta\rho\Omega_{RR}^{\mathcal{I}}}-\frac{(K+1)g_{RR}^{\mathcal{E}}}{\Omega_{RR}^{\mathcal{E}}}}}{e^K(K+1)^{-1}\Omega_{RR}^{\mathcal{E}}} dg_{RR}^{\mathcal{E}} \qquad (54)
$$

$$
\begin{aligned}
F_{L2}^\infty(\gamma) &= \int_0^{\frac{1}{\eta\rho}} \int_0^\infty (K+1) I_0\left(2\sqrt{\frac{K(K+1)g_{RR}^{\mathcal{E}}}{\Omega_{RR}^{\mathcal{E}}}}\right) e^{-\frac{(K+1)g_{RR}^{\mathcal{E}}}{\Omega_{RR}^{\mathcal{E}}}} \\
&\quad \times \frac{\left(1-e^{-\frac{1-\eta\rho g_{RR}^{\mathcal{E}}}{\gamma\eta\rho\Omega_{RR}^{\mathcal{I}}}}\right)\left(1-e^{-\frac{\gamma-\gamma\eta\rho g_{RR}^{\mathcal{E}}}{(1-\theta)(\gamma_P\eta\rho g_{SR})\Omega_{RD}}}\right)}{e^{\frac{g_{SR}}{\Omega_{SR}}+K}\Omega_{RR}^{\mathcal{E}}\Omega_{SR}} \\
&\quad \times dg_{SR} dg_{RR}^{\mathcal{E}}, \qquad (55)
\end{aligned}
$$

After some mathematical manipulations, $F_{L2}^\infty(\gamma)$ can be rewritten as [39, Eq. 3.961.1]

$$
\begin{aligned}
&F_{L2}^\infty(\gamma) \\
&= \int_0^{\frac{1}{\eta\rho}} (K+1) I_0\left(2\sqrt{\frac{K(K+1)g_{RR}^{\mathcal{E}}}{\Omega_{RR}^{\mathcal{E}}}}\right)\left(1-e^{-\frac{-1+\eta\rho g_{RR}^{\mathcal{E}}}{\gamma\eta\rho\Omega_{RR}^{\mathcal{I}}}}\right) \\
&\quad \times \left(\frac{2\mathrm{K}_1\left(2\sqrt{\frac{\gamma\left(\eta\rho g_{RR}^{\mathcal{E}}-1\right)}{\gamma_P\eta(\theta-1)\rho\Omega_{SR}\Omega_{RD}}}\right)}{\Omega_{SR}\sqrt{\frac{\gamma_P\eta(\theta-1)\rho\Omega_{RD}}{\gamma\Omega_{SR}\left(1+\eta\rho g_{RR}^{\mathcal{E}}\right)}}}+1\right)\frac{e^{-K-\frac{(K+1)g_{RR}^{\mathcal{E}}}{\Omega_{RR}^{\mathcal{E}}}}}{\Omega_{RR}^{\mathcal{E}}} dg_{RR}^{\mathcal{E}}. \qquad (56)
\end{aligned}
$$

By considering $g_{\mathrm{RR}}^{\mathcal{E}} = \frac{1-\exp(-x)}{\eta\rho}$ and applying the correct modifications on (54) and (56), we can obtain (28) resorting to the Gauss-Laguerre quadrature method [53, 25.4.45]. In the same way, we can obtain $\bar{C_{\mathrm{L}}}$ by resorting to the Gauss-Laguerre quadrature method again as

$$\begin{aligned}\bar{C_{\mathrm{L}}} &= \frac{1}{\ln 2}\int_0^\infty \frac{1-F_{\gamma_{\mathrm{L}}(\gamma)}}{1+\gamma}d\gamma,\\ &= \frac{1}{\ln 2}\left(\sum_{\gamma=1}^{n}\frac{e^{\gamma}}{1+\gamma}+\sum_{\gamma=1}^{m}\frac{e^{\gamma}}{1+\gamma}F_{\mathrm{L}}^{\infty}(\gamma)\right).\end{aligned} \tag{57}$$

Following a similar approach to derive (28), the CDF at the high SNR regime of γ_{E} can be expressed as

$$F_{\mathrm{E}}^{\infty}(\gamma) = \begin{cases}\Pr\left(g_{\mathrm{RR}}^{\mathcal{I}} > \frac{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}}{\eta\rho\gamma}, g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho}\right), & \gamma < \frac{1-\theta}{\theta}\\ \Pr\left(g_{\mathrm{RR}}^{\mathcal{I}} > 0, g_{\mathrm{RR}}^{\mathcal{E}} < \frac{1}{\eta\rho}\right), & \gamma > \frac{1-\theta}{\theta}\end{cases} \tag{58}$$

$$= \begin{cases}\int_0^{\frac{1}{\eta\rho}}\frac{(K+1)I_0\left(2\sqrt{\frac{K(K+1)g_{\mathrm{RR}}^{\mathcal{E}}}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}\right)}{\exp\left(\frac{1-\eta\rho g_{\mathrm{RR}}^{\mathcal{E}}}{\gamma\eta\rho\Omega_{\mathrm{RR}}^{\mathcal{I}}}+\frac{(K+1)g_{\mathrm{RR}}^{\mathcal{E}}}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}+K\right)\Omega_{\mathrm{RR}}^{\mathcal{E}}}dg_{\mathrm{RR}}^{\mathcal{E}}, & \gamma < \frac{1-\theta}{\theta}\\ 1-Q_1\left(\frac{\sqrt{2}}{\sqrt{K}}, \frac{\sqrt{2}\sqrt{\frac{K+1}{\Omega_{\mathrm{RR}}^{\mathcal{E}}}}}{\eta\rho}\right), & \gamma > \frac{1-\theta}{\theta}\end{cases} \tag{59}$$

Therefore, applying the series expansion of the Bessel Function [39, Eq. 8.447.1] on the first case of $F_{\mathrm{E}}^{\infty}(\gamma)$ and given the definition of $\mathcal{L}(\bar{\gamma_{\mathrm{L}}}, \bar{\gamma_{\mathrm{E}}})$, (29) can be obtained.

REFERENCES

[1] D. P. M. Osorio, E. E. B. Olivo, H. Alves, and M. Latva-Aho, "Safeguarding MTC at the physical layer: Potentials and challenges," *IEEE Access*, vol. 8, pp. 101437–101447, 2020.

[2] D. P. Moya Osorio, J. D. Vega Sanchez, and H. Alves, *Physical Layer Security for 5G and Beyond in 5G REF: The Essential 5G Reference Online*. Hoboken, NJ, USA: Wiley, 2019.

[3] J. Sánchez, L. Urquiza-Aguiar, M. Paredes, and D. Osorio, "Survey on physical layer security for 5G wireless networks," *Ann. Telecommun.*, vol. 76, pp. 155–174, Sep. 2020.

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

[5] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[6] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[7] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[8] 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.

[9] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[10] D. P. Moya Osorio, H. Alves, and E. E. Benitez Olivo, "On the secrecy performance and power allocation in relaying networks with untrusted relay in the partial secrecy regime," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2268–2281, 2020.

[11] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[12] C. D. Nwankwo, L. Zhang, A. Quddus, M. A. Imran, and R. Tafazolli, "A survey of self-interference management techniques for single frequency full duplex systems," *IEEE Access*, vol. 6, pp. 30242–30268, 2018.

[13] D. Korpi, T. Riihonen, V. Syrjälä, L. Anttila, M. Valkama, and R. Wichman, "Full-duplex transceiver system calculations: Analysis of ADC and linearity challenges," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3821–3836, Jul. 2014.

[14] E. E. Benitez Olivo, D. P. Moya Osorio, H. Alves, J. C. S. Santos Filho, and M. Latva-Aho, "Cognitive full-duplex decode-and-forward relaying networks with usable direct link and transmit-power constraints," *IEEE Access*, vol. 6, pp. 24983–24995, 2018.

[15] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[16] Q. Ding, M. Liu, and Y. Deng, "Secrecy outage probability analysis for full-duplex relaying networks based on relay selection schemes," *IEEE Access*, vol. 7, pp. 105987–105995, 2019.

[17] B. Van Nguyen, H. Jung, and K. Kim, "Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 131–137, Nov. 2018.

[18] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.

[19] L. Elsaid, L. Jimenez-Rodriguez, N. H. Tran, S. Shetty, and S. Sastry, "Secrecy rates and optimal power allocation for full-duplex decode-and-forward relay wire-tap channels," *IEEE Access*, vol. 5, pp. 10469–10477, 2017.

[20] D. P. Moya Osorio, E. E. Benitez Olivo, and H. Alves, "Secrecy performance for multiple untrusted relay networks using destination-based jamming with direct link," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2018, pp. 1–5.

[21] N. Zhao, S. Zhang, F. R. Yu, Y. Chen, A. Nallanathan, and V. C. M. Leung, "Exploiting interference for energy harvesting: A survey, research issues, and challenges," *IEEE Access*, vol. 5, pp. 10403–10421, 2017.

[22] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 264–302, 1st Quart., 2018.

[23] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1612–1616.

[24] I. W. G. da Silva, D. P. M. Osorio, E. E. B. Olivo, O. L. A. Lopez, H. Alves, and M. Latva-Aho, "On the performance of power splitting-based SWIPT in self-energy recycling full-duplex relaying networks," in *Proc. 54th Asilomar Conf. Signals, Syst., Comput.*, Nov. 2020, pp. 1–5.

[25] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 104–110, Nov. 2014.

[26] M. J. Saber, A. Keshavarz, J. Mazloum, A. M. Sazdar, and M. J. Piran, "Physical-layer security analysis of mixed SIMO SWIPT RF and FSO fixed-gain relaying systems," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2851–2858, Sep. 2019.

[27] R. Su, Y. Wang, and R. Sun, "Destination-assisted jamming for physical-layer security in SWIPT cognitive radio systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[28] W. Mou, Y. Cai, W. Yang, W. Yang, X. Xu, and J. Hu, "Exploiting full duplex techniques for secure communication in SWIPT system," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–6.

[29] 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.

[30] M. Liu and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1353–1356, Jun. 2017.

[31] H. Niu, B. Zhang, D. Guo, and Y. Huang, "Joint robust design for secure AF relay networks with SWIPT," *IEEE Access*, vol. 5, pp. 9369–9377, 2017.

[32] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 621–634, Mar. 2019.

[33] J. Zhang, X. Tao, H. Wu, and X. Zhang, "Secure transmission in SWIPT-powered two-way untrusted relay networks," *IEEE Access*, vol. 6, pp. 10508–10519, 2018.

[34] E. N. Egashira, E. E. Benitez Olivo, D. P. Moya Osorio, and H. Alves, "Secrecy performance of untrustworthy AF relay networks using cooperative jamming and SWIPT," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–6.

[35] H. Liu, K. J. Kim, K. S. Kwak, and H. V. Poor, "Power splitting-based SWIPT with decode-and-forward full-duplex relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7561–7577, Nov. 2016.

[36] Y. Zeng, H. Chen, and R. Zhang, "Bidirectional wireless information and power transfer with a helping relay," *IEEE Wireless Commun. Lett.*, vol. 20, no. 5, pp. 862–865, May 2016.

[37] S. Atapattu, N. Ross, Y. Jing, and M. Premaratne, "Source-based jamming for physical-layer security on untrusted full-duplex relay," *IEEE Commun. Lett.*, vol. 23, no. 5, pp. 842–846, May 2019.

[38] T. Koike-Akino and C. Duan, "Secrecy rate analysis of jamming superposition in presence of many eavesdropping users," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2011, pp. 1–6.

[39] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam, The Netherlands: Elsevier, 2007.

[40] E. W. Weisstein. *Regularized Hypergeometric Function*. Accessed: Apr. 20, 2021. [Online]. Available: https://mathworld.wolfram.com/RegularizedHypergeometricFunction.html

[41] M. K. Simon and M.-S. Alouini, *Digital Communication Over Fading Channels*, vol. 95. Hoboken, NJ, USA: Wiley, 2005.

[42] T. Kwon, S. Lim, S. Choi, and D. Hong, "Optimal duplex mode for DF relay in terms of the outage probability," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3628–3634, Sep. 2010.

[43] X. Xie, J. Chen, and Y. Fu, "Outage performance and QoS optimization in full-duplex system with non-linear energy harvesting model," *IEEE Access*, vol. 6, pp. 44281–44290, 2018.

[44] J. Chen, H. Chen, H. Zhang, and F. Zhao, "Spectral-energy efficiency tradeoff in relay-aided massive MIMO cellular networks with pilot contamination," *IEEE Access*, vol. 4, pp. 5234–5242, 2016.

[45] J. D. Vega Sanchez, D. P. M. Osorio, F. J. Lopez-Martinez, M. C. Paredes, and L. F. Urquiza-Aguiar, "Information-theoretic security of MIMO networks under $\kappa-\mu$ shadowed fading channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6302–6318, Jul. 2021.

[46] S. Jin, R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

[47] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[48] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proc. Int. Conf. Neural Netw.*, Nov./Dec. 1998, pp. 1942–1948.

[49] Y. Valle, G. K. Venayagamoorthy, S. Mohagheghi, J. C. Hernandez, and R. G. Harley, "Particle swarm optimization: Basic concepts, variants and applications in power systems," *IEEE Trans. Evol. Comput.*, vol. 12, no. 2, pp. 171–195, Apr. 2008.

[50] Wolfram Research. (2008). *Wolfram Mathematica Tutorial Collection: Constrained Optimization*. [Online]. Available: https://library.wolfram.com/infocenter/Books/8506/ConstrainedOptimization.pdf

[51] M. Stoopman, S. Keyrouz, H. J. Visser, K. Philips, and W. A. Serdijn, "Co-design of a CMOS rectifier and small loop antenna for highly sensitive RF energy harvesters," *IEEE J. Solid-State Circuits*, vol. 49, no. 3, pp. 622–634, Mar. 2014.

[52] P. N. Alevizos and A. Bletsas, "Sensitive and nonlinear far-field RF energy harvesting in wireless communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3670–3685, Jun. 2018.

[53] M. Abramowitz, *Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover, 1974.

ISABELLA WANDERLEY GOMES DA SILVA (Student Member, IEEE) was born in São Paulo, Brazil. She received the B.Sc. degree in electrical engineering from the Federal University of São Carlos, São Carlos, São Paulo, in 2021. She is currently pursuing the M.Sc. degree in electrical engineering with São Paulo State University (UNESP). In 2020, she was a Visiting Researcher at the Centre for Wireless Communications (CWC), University of Oulu, Finland, funded by the São Paulo Research Foundation (FAPESP). Her research interests include wireless communications in general, 5G and beyond networks, and PHY security.

JOSÉ DAVID VEGA SÁNCHEZ (Student Member, IEEE) received the B.Sc. degree in electronics engineering from the Escuela Politécnica del Ejército (ESPE), Sangolquí, Ecuador, in 2013, the M.Sc. degree in electrical engineering from the University of Campinas (UNICAMP), São Paulo, Brazil, in 2015, and the Ph.D. degree in electrical engineering from Escuela Politécnica Nacional (EPN), Quito, Ecuador, in 2022. He is a member of the Grupo de investigación en Redes Inalámbricas (GIRI), which was awarded among the best research groups from EPN, in 2019 and 2021. His research interests include modeling, analysis, and simulation of wireless fading channels.

EDGAR EDUARDO BENITEZ OLIVO (Member, IEEE) received the B.Sc. degree in electronics and telecommunications engineering from Armed Forces University-ESPE, Ecuador, in 2008, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Campinas, Brazil, in 2011 and 2015, respectively. In 2014, he was a Visiting Researcher with the Centre for Wireless Communications, University of Oulu, Finland. Since 2016, he has been with São Paulo State University (UNESP), Campus of São João da Boa Vista, Brazil, as an Assistant Professor. His research interests include wireless communications, with a current focus on enabling technologies towards 5G and beyond wireless networks. He has been involved as a TPC member in several conferences. He has served as a reviewer for many IEEE and non-IEEE journals.

DIANA PAMELA MOYA OSORIO (Member, IEEE) received the B.Sc. degree in electronics and telecommunications engineering from Armed Forces University (ESPE), Sangolquí, Ecuador, in 2008, and the M.Sc. and D.Sc. degrees in electrical engineering with emphasis on telecommunications and telematics from the University of Campinas (UNICAMP), Campinas, Brazil, in 2011 and 2015, respectively. Since 2015, she has been an Assistant Professor with the Department of Electrical Engineering, Federal University of São Carlos (UFSCar), São Carlos, Brazil. In 2020, she joined the 6GFlagship Program at the Centre for Wireless Communications (CWC), University of Oulu, Finland, as a Senior Research Fellow, and she is currently an Adjunct Professor in physical layer techniques for security. Her research interests include wireless communications in general, 5G and 6G networks, and physical layer security. She has also been a Postdoctoral Researcher at the Academy of Finland, since 2020. She has served as a TPC and a reviewer for several journals and conferences.