Secrecy Performance of Untrustworthy AF Relay Networks using Cooperative Jamming and SWIPT

E. N. Egashira*, E. E. Benitez Olivo*, D. P. Moya Osorio†, and H. Alves‡
*São Paulo State University (UNESP), Campus of São João da Boa Vista, São João da Boa Vista-SP, Brazil
†Department of Electrical Engineering, Federal University of São Carlos, São Carlos-SP, Brazil
‡Centre for Wireless Communications, University of Oulu, Oulu, Finland
edson.egashira@unesp.br, edgar.olivo@unesp.br, dianamoya@ufscar.br, hirley.alves@oulu.fi

***Abstract*—In this paper, the secrecy outage performance of a three-node amplify-and-forward relay network with an untrustworthy relay is investigated. To enable a secure transmission, we consider a destination-based jamming technique to prevent the relay from successfully decoding the secret messages between the source and the destination. In addition, the relay is assumed to be an energy-constrained device, thus being first energized by the source in order to be able to retransmit the information to the destination. In doing so, a time switching-based simultaneous wireless information and power transfer scheme is used. A closed-form asymptotic expression for the secrecy outage probability is derived in order to obtain a tight approximation at medium-to-high signal-to-noise ratio. The accuracy of the performed analysis is corroborated by Monte Carlo simulations through different illustrative cases. Numerical results show the impact of key system parameters on the secrecy performance, such as the time allocation factor between the energy harvesting and information transmission phases, the power allocation factor between source and destination for cooperative jamming, and the relay position, so as to provide insights on the design criteria for energy efficient and secure networks.**

***Index Terms*—Cooperative jamming, physical layer security, secrecy outage probability, SWIPT, untrustworthy relay.**

I. Introduction

The fifth generation (5G) of wireless mobile communications will not be just an enhanced version of the 4G broadband service with much higher data rates, as part of the enhanced mobile broadband service (eMBB), but it will also provide support for massive machine-type communication (mMTC) and ultra-reliable and low-latency communication (URLLC) services. Thus, 5G networks will be of paramount importance to meet the requirements of paradigms such as the Internet of Things (IoT) [1].

In this context, one of the main concerns is related to the security of critical information to be transmitted through 5G networks. Traditional cryptography-based protocols requiring key distribution or certificate management might be difficult to implement for a large number of devices, as expected in mMTC networks [2]. Over the last few years, a new approach to strengthen the security in wireless networks, which is based on the fundamentals of information theory, has gained special attention [2], [3]. This approach, referred to as physical layer security (PLS), capitalize on the physical proprieties of wireless channels, such as channel state information (CSI), fading, and interference, to provide a further level of protection over existing information security schemes. Particularly, cooperative jamming (CJ) is an appealing PLS technique to tackle eavesdropper attacks [4], whereby an external node is in charge of sending an artificial interference (or jamming) signal to the eavesdropper during the information transmission (IT). As an alternative approach, the source or destination themselves can play the role of jammers. Such techniques are referred to as source-based jamming (SBJ) or destination-based jamming (DBJ), respectively.

Besides, PLS can be combined with relay-based cooperative communication techniques in order to boost the performance of wireless communication systems not only in terms of information secrecy, but also in terms of reliability and coverage extension [4], [5]. However, these benefits rely on the assumption that the relay is a trustworthy node willing to cooperate in the communication process between source and destination. Although one can expect that potential eavesdropping attacks come from external nodes, the relay may leak information for its own benefit, thus becoming a possible eavesdropper. In this sense, the study of cooperative relaying scenarios with untrustworthy relays has received special attention [6]–[8]. In [6], it was shown that cooperation is possible even if the relay is untrustworthy. In [7], an approximate analysis of the average achievable secrecy rate and an asymptotic analysis of the secrecy outage probability were performed for an untrusted relay system using DBJ. In [8], an approximate analytical expression for the secrecy outage probability of multiple untrusted relay system using DBJ was derived.

On the other hand, in addition to the stringent security requirements for 5G networks, the deployment of mMTC services require small, low-cost devices, thus bringing out the importance of providing these networks with energy sustainability. In this context, wireless power transfer (WPT) and energy harvesting (EH) techniques have the potential to significantly increase the network energy efficiency.

Recently, the simultaneous wireless information and power transfer (SWIPT) technique has attracted attention in the context of energy-constrained cooperative relaying networks, by considering either trustworthy or untrustworthy relays [9]–[11]. For example, in [9], the outage probability of three basic WPT schemes for a trusted relay system was

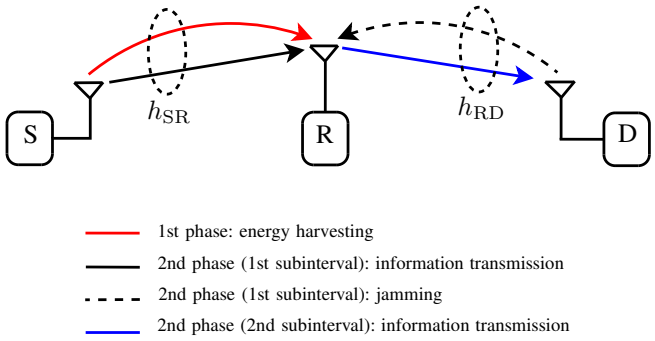

Fig. 1. System model.

analyzed, in which the relay is powered from the source (S-WPT), from the destination (D-WPT) or jointly from the source and destination (SD-WPT). In [10], a power-splitting-based S-WPT scheme for a multiple untrusted relay network was analyzed in terms of outage probability. In that work, the destination and a cooperative jammer are invoked to inject jamming signals in order to prevent any information leakage to the unstrusted relays. More recently, in [11], a time-switching SD-WPT scheme for a three-node untrusted relay network was proposed, in which a DBJ technique is employed to secure information transmissions. In that work, the achievable secrecy rate is maximized by optimizing the power splitting factors at the source and destination.

Although great efforts have been carried out so far to grasp insights on the trade-offs of using PLS and SWIPT techniques in cooperative relaying networks, a number of issues remain unexplored. In this work, we contribute to the study of untrustworthy relay networks using CJ and SWIPT techniques, aiming at improving the system performance in terms of secrecy, energy efficiency, and reliability. Different from previous related works, herein we consider a three-node relaying network setup with an untrustworthy amplify-and-forward (AF) relay, in which a time-switching-based S-WPT technique is employed to supply energy to the relay and a DBJ technique is used to hinder the relay so as to secure the end-to-end transmissions from the source to the destination. For the proposed setup, a closed-form approximate expression for the secrecy outage probability is derived in order to assess the effect of key system parameters on the network performance.

Notation: herein we use $f_A(\cdot)$ and $F_A(\cdot)$ to denote the probability density function (PDF) and cumulative distribution function (CDF) of a random variable A, respectively, $\mathrm{E}\{\cdot\}$ to denote expectation, $\Pr(\cdot)$ to denote probability, $\mathcal{CN}(a,b)$ to denote complex circularly-symmetric Gaussian distribution with mean a and variance b, and $[c]^+ \triangleq \max\{0,c\}$.

II. System Model

Fig. 1 illustrates a cooperative network with a source (S), a destination (D), and an AF relay (R) operating in half duplex (HD) mode. All nodes in the network are considered to be single antenna devices and operate in time division multiple access (TDMA). The direct link S→D is assumed to be severely attenuated, such that the communication between S and D is only feasible through the relaying link S→R→D.

In this system, the relay is considered to be powered by radio frequency (RF) signals coming from S, based on time switching (i.e., following a time-switching-based S-WPT scheme). This way, the transmission process of a block of information is assumed to be carried out in a total time interval T, which consists of two orthogonal phases, one for EH and one for IT. In the first phase, R harvests energy from S during a time interval αT, where $\alpha \in (0,1)$ is the time-switching factor. In the second phase, S communicates with D under the assistance of R, using two equal time subintervals of duration $(1-\alpha)T/2$. In the first time subinterval, S transmits an information signal to R, while D sends a jamming signal to hinder R from leaking secret information. In the second time subinterval, R retransmits to D an amplified version of the signal received from S, which is corrupted by jamming, using all the energy harvested during the first phase. At the reception, D is assumed to effectively cancel the jamming signal transmitted in the previous phase, since this signal is perfectly known by D.

Additionally, all channels are considered to undergo independent Rayleigh block fading, as well as additive white gaussian noise (AWGN) with average power N_0. Accordingly, the channel coefficients for the links S→R and R→D are modeled, respectively, as $h_i \sim \mathcal{CN}(0,\Omega_i)$, with $i \in \{\mathrm{SR},\mathrm{RD}\}$, where $\Omega_i = \mathrm{E}\{|h_i|^2\}$ is the average channel gain of the corresponding link. Thus, $g_{\mathrm{SR}} \triangleq |h_{\mathrm{SR}}|^2$ and $g_{\mathrm{RD}} \triangleq |h_{\mathrm{RD}}|^2$ are the channel gains following exponential distributions with means Ω_{SR} and Ω_{RD}, respectively. Moreover, the transmit signal-to-noise ratios (SNRs) at the source, relay, and destination are denoted by $\gamma_{\mathrm{S}} = P_{\mathrm{S}}/N_0$, $\gamma_{\mathrm{R}} = P_{\mathrm{R}}/N_0$, and $\gamma_{\mathrm{D}} = P_{\mathrm{D}}/N_0$, where P_{S}, P_{R}, and P_{D} are the transmit powers at S, R, and D, respectively. In addition, the transmit system power is assumed to be limited to P for the EH phase and for the IT phase, so that the transmit system SNR is given by $\gamma_P = P/N_0$. Thus, during the first IT subinterval, the transmit system power P is allocated to S and D by using a power allocation factor $\delta \in (0,1)$, such that $P_{\mathrm{S}} = \delta P$ and $P_{\mathrm{D}} = (1-\delta)P$. On the other hand, the energy harvested by R from the signal coming from S during the EH phase is given by

$$E_S = \eta \alpha T P g_{\mathrm{SR}}, \tag{1}$$

where $\eta \in (0,1)$ is the EH efficiency factor, so that the transmit power at R is given by

$$P_R = \frac{E_S}{(1-\alpha)T/2} \overset{(a)}{=} \frac{2\eta\alpha P g_{\mathrm{SR}}}{(1-\alpha)}$$

$$\overset{(b)}{=}\theta P g_{\mathrm{SR}}, \tag{2}$$

where in step (a) we have replaced E_S by (1), and in step (b) we define $\theta = (2\alpha\eta)/(1-\alpha)$.

III. Signal Model

Under the considerations exposed above, the signal model is presented in the following. Afterwards, the received SNRs at R and D are determined.

During the first ID subinterval, the received signal at R is given as

$$y_{\mathrm{R}}(t) = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t) + \sqrt{P_{\mathrm{D}}} h_{\mathrm{RD}} s_{\mathrm{J}}(t) + n_{\mathrm{R}}(t), \tag{3}$$

where $s_{\mathrm{I}}(t)$ is the information signal coming from S, $s_{\mathrm{J}}(t)$ is the jamming signal coming from D, and $n_{\mathrm{R}}(t)$ is the noise component at R. Then, during the second ID subinterval and considering the AF relaying protocol, the received signal at D coming from R is given as

$$y_{\mathrm{D}}(t) = \sqrt{P_{\mathrm{R}}} h_{\mathrm{RD}} \mathcal{G} y_{\mathrm{R}}(t) + n_{\mathrm{D}}(t), \tag{4}$$

where $n_{\mathrm{D}}(t)$ is the noise component at D, and $\mathcal{G}$ is the amplification factor relative to the AF relaying protocol, given as

$$\mathcal{G} = \sqrt{\frac{1}{P_{\mathrm{S}} g_{\mathrm{SR}} + P_{\mathrm{D}} g_{\mathrm{RD}} + N_0}}, \tag{5}$$

which can be obtained by considering normalized unit-power signals, i.e., $\mathrm{E}\{|s_{\mathrm{I}}(t)|^2\}=\mathrm{E}\{|s_{\mathrm{J}}(t)|^2\}=1$, and the fact that $\mathrm{E}\{|\mathcal{G} y_{\mathrm{R}}(t)|^2\}=1$ must be satisfied. Thus, by substituting (3) into (4) and considering that D effectively cancels the jamming signal (as this signal is perfectly known by itself, as previously stated), the received signal at D can be expressed as

$$\begin{aligned} y_{\mathrm{D}}(t_2) = \sqrt{P_{\mathrm{R}}} \mathcal{G} h_{\mathrm{RD}} \big[\sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t_1) \\ + \sqrt{P_{\mathrm{D}}} h_{\mathrm{RD}} s_{\mathrm{J}}(t_1) + n_{\mathrm{R}}(t_1) \big] + n_{\mathrm{D}}(t_2). \end{aligned} \tag{6}$$

Then, the end-to-end received SNR at the legitimate link can be obtained from (6) as

$$\begin{aligned} \Gamma_\ell &= \frac{P_{\mathrm{R}} g_{\mathrm{RD}} \mathcal{G}^2 P_{\mathrm{S}} g_{\mathrm{SR}}}{P_{\mathrm{R}} g_{\mathrm{RD}} \mathcal{G}^2 N_0 + N_0} \\ &\overset{(c)}{=} \frac{\gamma_{\mathrm{S}} \gamma_{\mathrm{R}} g_{\mathrm{SR}} g_{\mathrm{RD}}}{\gamma_{\mathrm{R}} g_{\mathrm{RD}} + \gamma_{\mathrm{S}} g_{\mathrm{SR}} + \gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1}, \end{aligned} \tag{7}$$

where in step (c) we have replaced $\mathcal{G}$ by (5) and performed some manipulations. Note from (2) that γ_{R} is a function of the channel gain at the S→R link, g_{SR}.

On the other hand, the received SNR at the eavesdropping link, which refers to the SNR received at the untrustworthy relay during the first IT subinterval, can be obtained from (3) as

$$\Gamma_e = \frac{P_{\mathrm{S}} g_{\mathrm{SR}}}{P_{\mathrm{D}} g_{\mathrm{RD}} + N_0} = \frac{\gamma_{\mathrm{S}} g_{\mathrm{SR}}}{\gamma_{\mathrm{D}} g_{\mathrm{RD}} + N_0}. \tag{8}$$

IV. Secrecy Outage Probability

In this section, we present analytical expressions for the secrecy outage probability of the untrustworthy relay system under study. To this end, we begin revisiting the definition of the secrecy capacity C_s as the maximum transmission rate achievable for a secure communication, given by the difference between the capacity of the legitimate channel, C_ℓ, and that of the eavesdropping channel, C_e (in this case, the S→R link itself). Thus, we have that

$$\begin{aligned} C_s &= [C_\ell - C_e]^+ \\ &= \frac{1}{2} \log_2 \left(\frac{1+\Gamma_\ell}{1+\Gamma_e} \right). \end{aligned} \tag{9}$$

Therefore, the secrecy outage probability is defined as the probability that the secrecy capacity in (9) is less than a target secrecy rate $\mathcal{R}$, thus being formulated from (7) and (8) as

$$\begin{aligned} P_{\mathrm{sout}} &= \Pr\left(\frac{1}{2} \log_2 \left(\frac{1+\Gamma_\ell}{1+\Gamma_e} \right) < \mathcal{R} \right), \\ &= \Pr\left(\frac{1+\Gamma_\ell}{1+\Gamma_e} < 2^{2\mathcal{R}} \right) \\ &= \Pr\left(\frac{1 + \frac{\gamma_{\mathrm{S}} \gamma_{\mathrm{R}} g_{\mathrm{SR}} g_{\mathrm{RD}}}{\gamma_{\mathrm{R}} g_{\mathrm{RD}} + \gamma_{\mathrm{S}} g_{\mathrm{SR}} + \gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1}}{1 + \frac{\gamma_{\mathrm{S}} g_{\mathrm{SR}}}{\gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1}} < 2^{2\mathcal{R}} \triangleq \tau \right). \end{aligned} \tag{10}$$

In light of (10), an exact analysis of the secrecy outage probability proves rather intricate, leading to a non-closed form solution. For mathematical tractability, in the following we obtain a closed-form expression built on an asymptotic analysis, which accurately determines the system performance at the medium-to-high SNR regime. Thus, by noticing from (10) that at high SNR the numerator of the ratio in $\Pr(\cdot)$ can be approximated by the end-to-end received SNR at the legitimate link, so that the term 1 is neglected, performing some manipulations, and using the well-known upper bound for the harmonic mean given by $\min\{X,Y\} \geq XY/(X+Y+1)$, the secrecy outage probability can be expressed from (10) as

$$\begin{aligned} P_{\mathrm{sout}} &= \Pr\left(\frac{\frac{\gamma_{\mathrm{R}}}{\gamma_{\mathrm{R}}+\gamma_{\mathrm{D}}}}{1+\frac{\gamma_{\mathrm{S}} g_{\mathrm{SR}}}{\gamma_{\mathrm{D}} g_{\mathrm{RD}}+1}} \min\{\gamma_{\mathrm{S}} g_{\mathrm{SR}}, (\gamma_{\mathrm{R}}+\gamma_{\mathrm{D}}) g_{\mathrm{RD}}\} < \tau \right) \\ &= \Pr\left(\frac{\gamma_{\mathrm{R}}}{\gamma_{\mathrm{R}}+\gamma_{\mathrm{D}}} \min\{\gamma_{\mathrm{S}} g_{\mathrm{SR}}, (\gamma_{\mathrm{R}}+\gamma_{\mathrm{D}}) g_{\mathrm{RD}}\} \right. \\ &\qquad \left. < \tau \left(1 + \frac{\gamma_{\mathrm{S}} g_{\mathrm{SR}}}{\gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1} \right) \right) \\ &\overset{(d)}{=} \Pr\left(\frac{\theta \gamma_P g_{\mathrm{SR}}}{\theta \gamma_P g_{\mathrm{SR}} + (1-\delta)\gamma_P} \right. \\ &\qquad \times \min\{\delta \gamma_P g_{\mathrm{SR}}, [\theta \gamma_P g_{\mathrm{SR}} + (1-\delta)\gamma_P] g_{\mathrm{RD}}\} \\ &\qquad \left. < \tau \left(\frac{(1-\delta)\gamma_P g_{\mathrm{RD}} + 1 + \delta \gamma_P g_{\mathrm{SR}}}{(1-\delta)\gamma_P g_{\mathrm{RD}} + 1} \right) \right) \\ &= \Pr\left(\frac{\theta \gamma_P g_{\mathrm{SR}}}{\theta g_{\mathrm{SR}} + 1 - \delta} \min\{\delta g_{\mathrm{SR}}, [\theta g_{\mathrm{SR}} + (1-\delta)] g_{\mathrm{RD}}\} \right. \end{aligned}$$

$$< \tau \left(\frac{(1-\delta) g_{\mathrm{RD}} + \frac{1}{\gamma_P} + \delta g_{\mathrm{SR}}}{(1-\delta) g_{\mathrm{RD}} + \frac{1}{\gamma_P}} \right) \Bigg)$$

$$\overset{(e)}{=} \Pr \Bigg(\min\{\delta g_{\mathrm{SR}}, [\theta g_{\mathrm{SR}} + (1-\delta)] g_{\mathrm{RD}}\} < \tau \left(\frac{(1-\delta) g_{\mathrm{RD}} + \delta g_{\mathrm{SR}}}{\gamma_P (1-\delta) g_{\mathrm{RD}}} \right) \left(\frac{\theta g_{\mathrm{SR}} + 1 - \delta}{\theta g_{\mathrm{SR}}} \right) \Bigg). \tag{11}$$

where in step (d) we have used that $\gamma_{\mathrm{R}} = P_{\mathrm{R}}/N_0 = \theta \gamma_P g_{\mathrm{SR}}$, with θ given as in (2), and in step (e) we have neglected the terms $1/\gamma_P$ of the previous step, as the high SNR regime is being considered. The expression in (11) is the first step towards Proposition 1, where we provide an analytical expression for the secrecy outage probability of the system under study.

Proposition 1. *A closed-form asymptotic analytical expression for the secrecy outage probability of a relaying system with an untrustworthy AF relay, using DBJ and time-switching-based SWIPT, is given by*

$$P_{\mathrm{sout}} = 1 - e^{\lambda} + \frac{\tau}{\delta \gamma_P \theta \Omega_{\mathrm{SR}} \Omega_{\mathrm{RD}}} \left[\left(e^{\lambda} - e^{\sqrt{2}\lambda} \right) \theta \Omega_{\mathrm{SR}} + (1-\delta) \left(\mathrm{Ei}(\sqrt{2}\lambda) - \mathrm{Ei}(\lambda) \right) \right] + \frac{e^{\sqrt{2}\lambda}}{\Omega_{\mathrm{SR}}} \sqrt{\frac{\delta \tau}{(1-\delta)\theta \gamma_P}}, \tag{12}$$

where

$$\lambda = -\frac{1}{\Omega_{\mathrm{SR}}} \sqrt{\frac{(1-\delta)\tau}{\delta \theta \gamma_P}}. \tag{13}$$

Proof. The proof is provided in the appendix. □

V. Numerical Results and Discussions

The analytical expression derived in the previous section is now evaluated for illustrative scenarios. Monte Carlo simulation-based results are also presented, which fully validate our analysis. For this purpose, let us consider a linear network topology in which the normalized distances between S and R, between R and D, and between S and D are set to $d_{\mathrm{SR}} = 0.5$, $d_{\mathrm{RD}} = 0.5$ and $d_{\mathrm{SD}} = 1$, respectively. We consider that the average channel gain of all links are determined by the path loss, that is, $\Omega_i = d_i^{-\beta}$, $i \in \{\mathrm{SR}, \mathrm{SD}\}$, where d_i is the distance between two nodes, and β is the path loss exponent which is set to 4. In addition, the target secrecy rate is set to $\mathcal{R} = 1$ bps, and the EH efficiency factor to $\eta = 0.5$[1].

Fig. 2 depicts the secrecy outage probability as a function of transmit system SNR γ_P, for different values of power allocation factor δ between the source and destination at the first subinterval of the IT phase (to transmit information and jamming signals, respectively). Note how the derived asymptotic expression provide a very good fit to the actual performance at medium to high SNR. Note also that the best system secrecy performance is attained for $\delta = 0.5$, that is,

[1]This value has typically adopted in several related works [12]–[14].

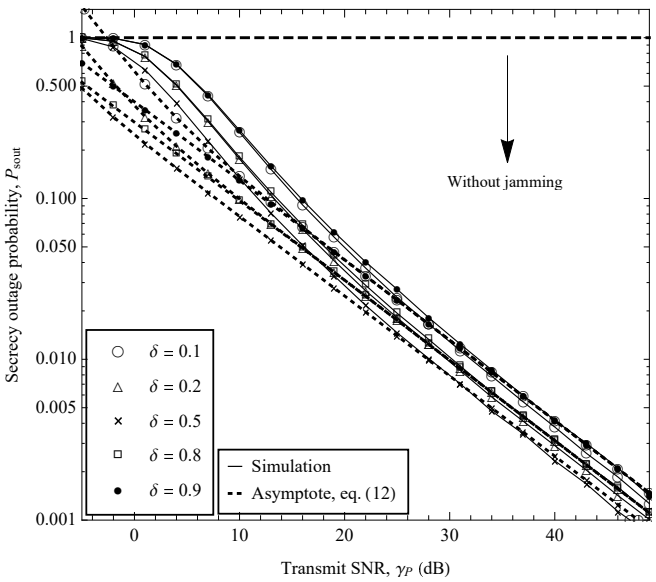

Fig. 2. Secrecy outage probability versus transmit SNR γ_P, for different values of $\delta = 0.1, 0.2, 0.5, 0.8, 0.9$, considering $\alpha = 0.5$. For comparison, the secrecy performance by allocating P to S, without using jamming, is also presented.

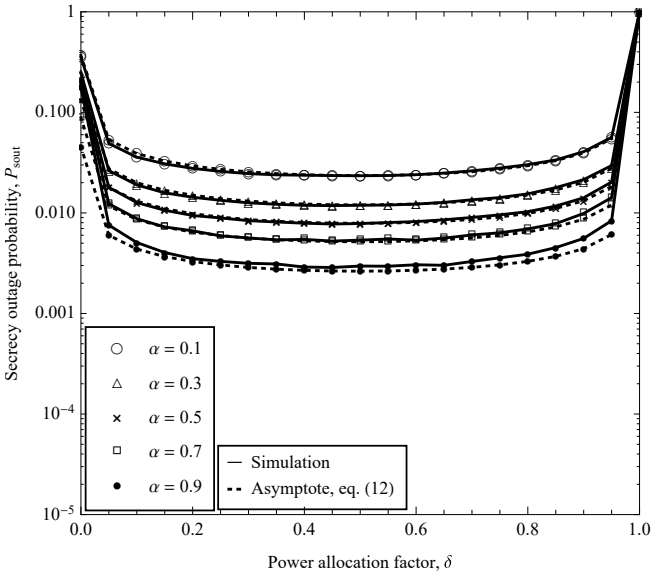

Fig. 3. Secrecy outage probability versus power allocation factor δ, for different values of $\alpha = 0.1, 0.3, 0.5, 0.7, 0.9$, considering $\gamma_P = 30$ dB.

for a balanced power allocation condition between S and D. Otherwise, for an unbalanced power allocation between S and D, the system secrecy performance worsens. However, we can notice a symmetrical behavior of the curves for the cases $\delta = (0.1, 0.9)$ and $\delta = (0.2, 0.8)$. This can be explained by the fact that, by virtue of (10), in those cases either the information reliability at the destination or the information secrecy at the untrustworthy relay is compromised. For comparison, in order to evince the benefits of cooperative jamming, the system secrecy performance by allocating P to S, without employing jamming, is also illustrated.

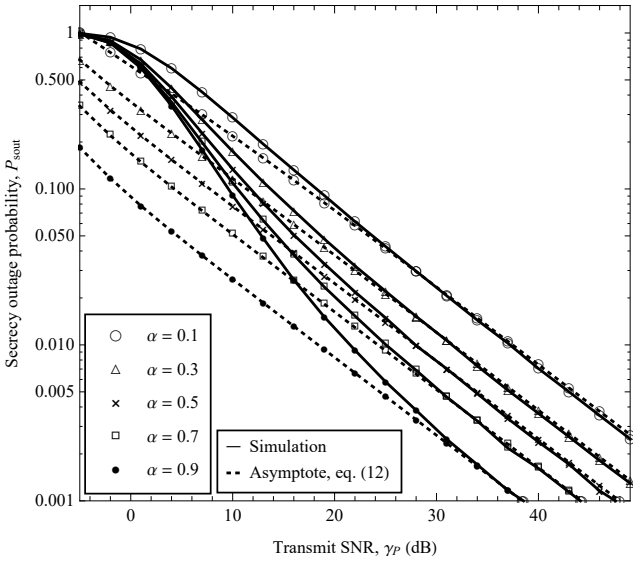

Fig. 4. Secrecy outage probability versus transmit SNR γ_P, for different values of time allocation factor $\alpha = 0.1, 0.3, 0.5, 0.7, 0.9$, considering $\delta = 0.5$.

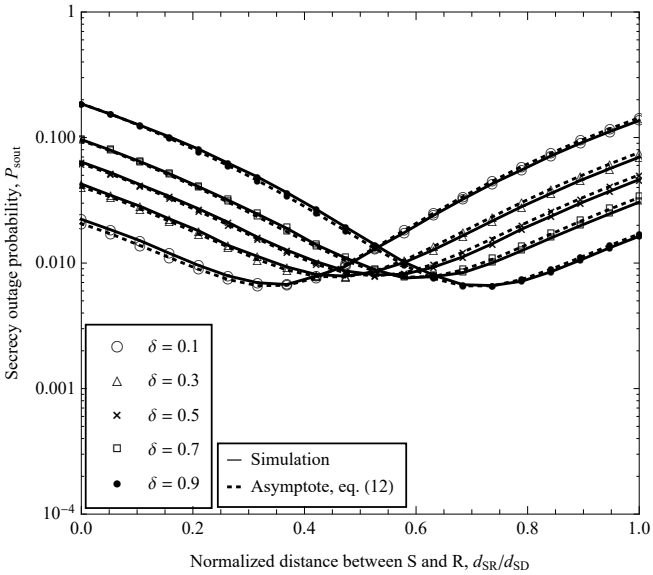

Fig. 5. Secrecy outage probability versus normalized distance between S and R, $d_{\rm SR}/d_{\rm SD}$, for different values of $\delta = 0.1, 0.3, 0.5, 0.7, 0.9$, considering $\gamma_P =$ 30 dB and $\alpha = 0.5$.

Fig. 3 illustrates the secrecy outage performance of the system as a function of the power allocation factor δ, for different values of time allocation factor α. Once again, note how the analytical result approximates very well the true system performance for all the sample cases. Note that the secrecy performance improves as the charging time increases, irrespective of the power allocation factor.

Fig. 4 shows the secrecy outage probability as a function of the transmit system SNR γ_P, for different values of time allocation factor α between the EH and IT phases. In this scenario, the higher the value of α, more time interval for EH at R and, consequently, the higher the transmit power at R is used for information transmission, thus improving the secrecy outage probability of the system. In addition, we can notice from the curves at high SNR that, by increasing α from 0.1 to 0.5, approximately 8 dB of transmit system power can be saved.

Fig. 5 illustrates the secrecy outage probability as a function of the normalized distance between R and S, $d_{\rm SR}/d_{\rm SD}$. We can observe that as the untrustworthy relay approaches the source, the better strategy is to allocate more power to the destination during the first interval of the IT phase, thus making the jamming signal stronger. In turn, for positions of the relay closer to the destination, allocating more power to the source yields the better performance, in order to strengthen the first hop of the legitimate link. In the latter case, although allocating more power to the source also strengthens the eavesdropper link, the average power of the jamming signal increases, thus improving the secrecy outage performance.

VI. Conclusion

In this work, we investigated the secrecy outage performance of a relaying system with an untrustworthy AF relay, wherein we have used DBJ and time-switching-based SWIPT techniques for information secrecy and energy efficiency purposes, respectively. We obtained a closed-form analytical expression based on an asymptotic analysis that was validated with Monte Carlo simulations. Our closed-form analytical expression can be used to guide in the design of secure and energy efficient wireless networks, with untrustworthy and energy-constrained relays by taking into account key system parameters such as time allocation factor between the EH and IT phases of a time switching-based SWIPT scheme, and the power allocation factor between the source and destination, employed during the first subinterval at the IT phase. From the results, it was observed that the DBJ technique play an essential role to achieve secure transmissions.

The proposed system model could be used as a benchmark for future works based on DBJ, in which other power supplying strategies for the relay can be assessed, such as destination-based WPT or a hybrid power supplying scheme that considers the channel conditions of the network.

Appendix

Herein we obtain a closed-form asymptotic expression for the secrecy outage probability of the proposed system. To this end, we begin by determining the integration regions for the outage events in the argument of $\Pr(\cdot)$ in (12). To tackle the term $\min\{\cdot,\cdot\}$ in this latter expression, we consider the following two conditions: (i) $\delta g_{\rm SR} < (\theta g_{\rm SR} + 1 - \delta) g_{\rm RD}$ and (ii) $\delta g_{\rm SR} > (\theta g_{\rm SR} + 1 - \delta) g_{\rm RD}$. For the first condition, it follows from (12) that the integration region is given by

$$\left[g_{\rm RD} > \frac{\delta g_{\rm SR}}{1 - \delta + \theta g_{\rm SR}} \bigcap 0 < g_{\rm SR} \leq \frac{1}{2} \left(\frac{\tau}{\delta \gamma_P} + \frac{1}{\delta \gamma_P} \sqrt{\frac{\tau}{\theta}} \right. \right.$$

$$\times\sqrt{\theta\tau+4\delta(1-\delta)\gamma_P}\Big)\bigcap\Big(\gamma_P>0\bigcup\gamma_P>\frac{\theta\tau}{\delta(1-\delta)}\Big)\Big]$$
$$\bigcup\Big\{\frac{\delta g_{\rm SR}}{1-\delta+\theta g_{\rm SR}}<g_{\rm RD}<\frac{\delta\tau g_{\rm SR}(\delta-1-\theta g_{\rm SR})}{(1-\delta)[(1-\delta)\tau+\theta g_{\rm SR}(\tau-\gamma_P\delta g_{\rm SR})]}$$
$$\bigcap\gamma_P\delta\Big[\tau+\gamma_P\delta\Big(\sqrt{\frac{\tau[4\gamma_P\delta(1-\delta)+\theta\tau]}{\gamma_P^2\delta^2\theta}}-2g_{\rm SR}\Big)\Big]<0$$
$$\bigcap\Big[0<\gamma_P\le\frac{\theta\tau}{\delta(1-\delta)}\bigcup\Big(\gamma_P>\frac{\theta\tau}{\delta(1-\delta)}\bigcap\frac{3(1-\delta)\tau}{\gamma_P\delta(1-\delta)-\theta\tau}$$
$$+\sqrt{\frac{(1-\delta)^2\tau[8\gamma_P\delta(1-\delta)+\theta\tau]}{\theta[\gamma_P\delta(1-\delta)-\theta\tau]^2}}>2g_{\rm SR}\Big)\Big]\Big\}. \quad (14)$$

Otherwise, for the second condition, the integration region is given by

$$\Big\{0<g_{\rm RD}<\frac{\delta g_{\rm SR}}{1-\delta+\theta g_{\rm SR}}\bigcap\Big[0<\gamma_P\le\frac{\theta\tau}{\delta(1-\delta)}$$
$$\bigcup\Big(\gamma_P>\frac{\theta\tau}{\delta(1-\delta)}\bigcap\frac{3(1-\delta)\tau}{\gamma_P\delta(1-\delta)-\theta\tau}+\frac{1-\delta}{\gamma_P\delta(1-\delta)-\theta\tau}$$
$$\times\sqrt{\frac{\tau[8\gamma_P\delta(1-\delta)+\theta\tau]}{\theta}}\ge 2g_{\rm SR}\Big)\Big]\Big\}\bigcup\Big\{\gamma_P\theta g_{\rm SR}\Big[\tau$$
$$+\gamma_P\theta g_{\rm SR}\Big(\sqrt{\frac{\tau[(1-\delta)\tau+4\gamma_P\delta\theta g_{\rm SR}^2]}{\gamma_P^2(1-\delta)\theta^2 g_{\rm SR}^2}}-2g_{\rm RD}\Big)\Big]>0$$
$$\bigcap g_{\rm SR}>\frac{1}{2}\Big(\frac{3(1-\delta)\tau}{\gamma_P\delta(1-\delta)-\theta\tau}+\frac{1-\delta}{\gamma_P\delta(1-\delta)-\theta\tau}$$
$$+\sqrt{\frac{\tau[8\gamma_P\delta(1-\delta)+\theta\tau]}{\theta}}\Big)\bigcap\gamma_P>\frac{\theta\tau}{\delta(1-\delta)}\Big\}. \quad (15)$$

This way, we can develop the secrecy outage probability from (14) and (15) in integral form as

$$P_{\rm sout}=\int_0^{g_{\rm SR1}}f_{g_{\rm SR}}(x)\left(1-F_{g_{\rm RD}}\left(\frac{\delta x}{1-\delta+\theta x}\right)\right)dx$$
$$+\int_{g_{\rm SR1}}^{g_{\rm SR2}}\left[F_{g_{\rm RD}}\left(-\frac{\delta\tau x\,(1-\delta+\theta x)}{(1-\delta)\,[\tau-\delta\tau+\theta x\,(\tau-\delta x\gamma_P)]}\right)\right.$$
$$\left.-F_{g_{\rm RD}}\left(\frac{\delta x}{1-\delta+\theta x}\right)\right]f_{g_{\rm SR}}(x)dx$$
$$+\int_0^{g_{\rm SR2}}f_{g_{\rm SR}}(x)F_{g_{\rm RD}}\left(\frac{\delta x}{1-\delta+\theta x}\right)dx$$
$$+\int_{g_{\rm SR2}}^{\infty}F_{g_{\rm RD}}\left(\frac{1}{2}\sqrt{\frac{(1-\delta)\tau^2+4\delta\theta\tau x^2\gamma_P}{(1-\delta)\theta^2x^2\gamma_P^2}}\right.$$
$$\left.+\frac{\tau}{2\theta x\gamma_P}\right)f_{g_{\rm SR}}(x)dx, \quad (16)$$

where

$$g_{\rm SR1}=\frac{1}{2}\sqrt{\frac{\theta\tau^2+4\delta(1-\delta)\tau\gamma_P}{\delta^2\theta\gamma_P^2}}+\frac{\tau}{2\delta\gamma_P}, \quad (17)$$

$$g_{\rm SR2}=\frac{1}{2}\sqrt{\frac{(1-\delta)^2\theta\tau^2+8\delta(1-\delta)^3\tau\gamma_P}{\theta\,[\theta\tau-\delta(1-\delta)\gamma_P]^{\,2}}}$$
$$+\frac{3(1-\delta)\tau}{2\,[\delta(1-\delta)\gamma_P-\theta\tau]}. \quad (18)$$

By noticing that the terms proportional to $1/\gamma_P$ and $1/\gamma_P^2$ in (16) go to zero in the high-SNR regime, using the Maclaurin series expansion of the exponential function in [15, eq. (0.318.2)], whereby $e^{-x}\simeq 1-x$ for $x\to 0$, and solving the resulting integrals, a closed-form asymptotic expression for the secrecy outage probability is attained as in (12).

ACKNOWLEDGMENT

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES) - Finance Code 001, the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq, Proc. 421850/2018-3 and Proc. 428649/2016-5), the São Paulo Research Foundation (FAPESP, Proc. 17/20990-6), the Academy of Finland 6Genesis Flagship (grant 318927), and the EE-IoT (grant 319008).

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[2] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, pp. 1–1, 2018.

[4] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[5] A. Mabrouk, K. Tourki, and N. Hamdi, "Relay selection for optimized cooperative jamming scheme," in *Proc. 23rd European Signal Process. Conf. (EUSIPCO)*, Aug. 2015, pp. 86–90.

[6] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[7] R. Zhao, X. Tan, D. Chen, Y. He, and Z. Ding, "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11 511–11 524, Dec. 2018.

[8] 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 *IEEE PIMRC*, Sep. 2018, pp. 1–5.

[9] C. Zhang and Y. Chen, "Wireless power transfer strategies for cooperative relay system to maximize information throughput," *IEEE Access*, vol. 5, pp. 2573–2582, 2017.

[10] A. E. Shafie, A. Mabrouk, K. Tourki, N. Al-Dhahir, and R. Hamila, "Securing untrusted RF-EH relay networks using cooperative jamming signals," *IEEE Access*, vol. 5, pp. 24 353–24 367, 2017.

[11] R. Yao, Y. Lu, T. A. Tsiftsis, N. Qi, T. Mekkawy, and F. Xu, "Secrecy rate-optimum energy splitting for an untrusted and energy harvesting relay network," *IEEE Access*, vol. 6, pp. 19 238–19 246, 2018.

[12] Z. Chen, L. X. Cai, Y. Cheng, and H. Shan, "Sustainable cooperative communication in wireless powered networks with energy harvesting relay," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 8175–8189, Dec. 2017.

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

[14] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *Proc. IEEE GLOBECOM*, Dec. 2014, pp. 3145–3150.

[15] I. Gradshteyn and I. Ryzhik, *Table of Integrals, series and products*. New York, NY: Elsevier, 2007.