Impact of Wireless Energy Transfer Strategies on the Secrecy Performance of Untrustworthy Relay Networks

Edson Nobuyuki Egashira, Diana Pamela Moya Osorio, *Member, IEEE,*
and Edgar Eduardo Benitez Olivo, *Member, IEEE*

***Abstract*—This work investigates the secrecy outage performance of a dual-hop relaying network with an untrustworthy energy-constrained relay. A destination-based jamming technique is adopted in order to prevent the relay from decoding confidential messages from the source. Additionally, three time switching-based wireless energy transfer (WET) strategies are investigated for supplying power to relay, namely, i) from the source, ii) from the destination, and iii) from both source and destination. For these three strategies, we derive simple closed-form asymptotic expressions for the secrecy outage probability at high signal-to-noise ratio. Moreover, Monte Carlo simulations are carried out to verify the theoretical results through different illustrative cases. The effect of key system parameters on the secrecy performance is investigated, including the time allocation factor between the energy harvesting and information transmission phases, the power allocation factor between source and destination for the information transmission phase, and the relay's relative position between source and destination.**

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

I. Introduction

In the context of the challenges in security of confidential information transmitted over fifth-generation (5G) wireless networks, an approach called physical layer security (PLS) has emerged as a promising solution [1], [2]. PLS exploits the physical properties of wireless channels, such as the fading and interference phenomena, in order to achieve secure transmissions. In this sense, cooperative scenarios with untrustworthy relays have recently raised attention [3]–[5]. For instance, in [3], a cooperative scenario with multiple untrustworthy AF relays was considered, for which a positive secrecy rate was proven to be achieved, regardless of the transmit power and channel conditions, as long as there exists a considerable number of untrustworthy relays assisting the communication between the source and destination. In [4], the secrecy performance of an AF relaying network with an untrustworthy relay node was examined considering the partial secrecy regime, where a destination-based jamming (DBJ) technique is employed, in which the destination node is responsible for sending a jamming signal to the untrustworthy relay during the information transmission coming from the source. In [5], to improve the secrecy performance of a dual-hop untrustworthy relay system with direct link and multiple antennas at the destination, a FD-DBJ scheme with optimal antenna selection was proposed, for which an asymptotic expression for the secrecy outage probability was derived.

On the other hand, in order to comply with 5G-and-beyond (5GB) wireless network requirements, such as the support of a massive number of connected devices, it is necessary to adopt energy-efficient architectures [6]. In this sense, several works have reported the benefits of using simultaneous wireless information and power transfer (SWIPT) [7]–[12]. In [7], three wireless energy transfer (WET) schemes for a trustworthy relay system was analyzed, in which optimal transfer parameters were provided to maximize the information throughput. Therein, by considering that the relay is a energy-constrained device, WET schemes considered the energy supply to the relay using RF signals from the source (S-WET), from the destination (D-WET), and from both source and destination (SD-WET). In [8], the secrecy outage probability of a PS-based SWIPT strategy, considering a multiple untrustworthy AF relay network, was analyzed. In that work, a jamming-based scheme was proposed, whereby a cooperative jammer and a destination both inject jamming signals in order to protect the source's confidential information. In [9], an optimization algorithm is proposed to maximize the achievable secrecy rate of a three-node untrustworthy relay network by using a PS-based SD-WET strategy. In [10], a tradeoff between energy consumption and secrecy was investigated for a multiple untrustworthy relay network using a source-based jamming (SBJ) technique. In [11], the secrecy performance of a dual-hop untrustworthy AF relaying network with multiple destinations, which employs TS- and PS-based SWIPT policies with SD-WET, was analyzed. In [12], the authors investigate the secrecy performance of a TS-based SWIPT strategy for a three-node untrustworthy relay network using S-WET and DBJ. In this work, in addition to that strategy, we analyze the secrecy performance for two other WET strategies: D-WET and SD-WET. Also, we provide a comparison among these three strategies through sample scenarios.

This work was supported in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior—Brazil (CAPES)—Finance Code 001, in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 421850/2018-3, and in part by the Academy of Finland 6Genesis Flagship under Grant 318927.

Edson Nobuyuki Egashira and Edgar Eduardo Benitez Olivo are with São Paulo State University (UNESP), Campus of São João da Boa Vista, São João da Boa Vista 13876-750, Brazil (e-mail: edson.egashira@unesp.br; edgar.olivo@unesp.br).

Diana Pamela Moya Osorio is with the Centre for Wireless Communications, University of Oulu, Oulu 90014, Finland (e-mail:: diana.moyaosorio@oulu.fi)

II. System Model

Consider a dual-hop relaying system consisting of one source (S), one destination (D), and one untrustworthy AF relay (R) which operates in half duplex mode. All terminals are provided with a single antenna, and a time division multiple access scheme is considered to share the wireless medium among them. It is assumed that S reaches D only through the relaying link S→R→D due to a strong attenuation or blockage of the direct link S→D. All channels are considered to experience independent Rayleigh block fading and additive white Gaussian noise with average power N_0. Thus, $h_i \sim \mathcal{CN}(0, \Omega_i)$, $i \in \{\mathrm{SR}, \mathrm{RD}\}$, denote the channel coefficients of the S→R and R→D links, respectively, where $\mathcal{CN}(a, b)$ stands for complex circularly-symmetric Gaussian distribution with mean a and variance b, and $\Omega_i = E\{|h_i|^2\}$ is the average channel gain of the ith link, with $E\{\cdot\}$ denoting statistical expectation. This way, the channel gains $g_i \triangleq |h_i|^2$ follows an exponential distribution with mean Ω_i, where $i \in \{\mathrm{SR}, \mathrm{RD}\}$. The transmission process of a block of information is based on a TS-SWIPT approach, which is carried out in a total time interval T, consisting of EH and IT phases. In the first phase, R harvests the energy coming from another node—S, D, or both of them, depending on whether S-WET, D-WET, or SD-WET is being considered, respectively—during a time interval of αT, where $\alpha \in (0, 1)$ is the time allocation factor between the EH and IT phases. In the second phase, S transmits information to D with the help of R by using two equal time subintervals of $(1-\alpha)T/2$. In the first time subinterval, S sends an information signal to R, whereas D sends a jamming signal in order to preserve the information secrecy by hindering R. In the second time subinterval, by using the energy harvested during the first phase, R sends an amplified version of the received composite signal to D, which is capable to cancel the jamming signal at the reception, thereby being able to recover the information signal coming from S. Additionally, the transmit signal-to-noise ratios (SNRs) at S, R, and D are denoted, respectively, 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 corresponding transmit powers. Moreover, during the EH and IT phases, it is assumed that the transmit system power is constrained to P; accordingly, the transmit system SNR is defined as $\gamma_P = P/N_0$. Therefore, during the first subinterval for IT, the transmit powers at S and D for the transmission of the information and jamming signals are $P_{\mathrm{S}} = \delta P$ and $P_{\mathrm{D}} = (1-\delta)P$, respectively, where $\delta \in (0, 1)$ is a power allocation factor. On the other hand, the transmit power at R depends on the energy harvested according to the S-WET, D-WET, or SD-WET strategies. According to each strategy, the transmit power at R during the EH phase is given by

$$S-WET: P_{\mathrm{R}} = \theta P g_{\mathrm{SR}} \tag{1}$$

$$D-WET: P_{\mathrm{R}} = \theta P g_{\mathrm{RD}} \tag{2}$$

$$SD-WET: P_{\mathrm{R}} = \theta P[\mu g_{\mathrm{SR}} + (1-\mu) g_{\mathrm{RD}}], \tag{3}$$

where $\mu \in (0, 1)$ is the power allocation factor between S and D, and θ is given as

$$\theta = \frac{2\alpha\eta}{1-\alpha}, \tag{4}$$

where $\eta \in (0, 1)$ is the EH conversion efficiency factor.

III. Signal Model

In the first subinterval for IT, the received signal at R is given as

$$y_{\mathrm{R}}(t) = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t) + \sqrt{P_{\mathrm{D}}} h_{\mathrm{RD}} s_{\mathrm{J}}(t) + n_{\mathrm{R}}(t), \tag{5}$$

where $s_{\mathrm{I}}(t)$, $s_{\mathrm{J}}(t)$ and $n_{\mathrm{R}}(t)$ are the information signal coming from S, the jamming signal coming from D, and the noise component at R, respectively.

In the second subinterval for IT, by considering the relay operation under the AF protocol, the received signal at D coming from R is expressed as

$$y_{\mathrm{D}}(t) = \sqrt{P_{\mathrm{R}}} h_{\mathrm{RD}} \mathcal{G} y_{\mathrm{R}}(t) + n_{\mathrm{D}}(t), \tag{6}$$

where $n_{\mathrm{D}}(t)$ is the noise component at D, and $\mathcal{G}$ is the amplification factor relative to AF relaying protocol. This latter can be obtained by considering normalized unit-power signals, as well as considering that $\mathrm{E}\{|\mathcal{G} y_{\mathrm{R}}(t)|^2\}=1$. In doing so, we have that

$$\mathcal{G} = \sqrt{\frac{1}{P_{\mathrm{S}} g_{\mathrm{SR}} + P_{\mathrm{D}} g_{\mathrm{RD}} + N_0}}, \tag{7}$$

Thus, by substituting (5) into (6) and considering that D is able to effectively cancel the jamming signal, as this is perfectly known by itself, the signal received at D results in

$$y_{\mathrm{D}}(t_2) = \sqrt{P_{\mathrm{R}}} \mathcal{G} h_{\mathrm{RD}} \left[\sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t_1) + n_{\mathrm{R}}(t_1)\right] + n_{\mathrm{D}}(t_2). \tag{8}$$

From (8), the end-to-end received SNR at the legitimate link can be expressed as

$$\Gamma_\ell = \frac{P_{\mathrm{S}} P_{\mathrm{R}} g_{\mathrm{SR}} g_{\mathrm{RD}} \mathcal{G}^2}{P_{\mathrm{R}} g_{\mathrm{RD}} \mathcal{G}^2 N_0 + N_0} = \frac{\gamma_{\mathrm{S}} \gamma_{\mathrm{R}} g_{\mathrm{SR}} g_{\mathrm{RD}}}{\gamma_{\mathrm{R}} g_{\mathrm{RD}} + \gamma_{\mathrm{S}} g_{\mathrm{SR}} + \gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1}, \tag{9}$$

where we have replaced $\mathcal{G}$ by (7) and made some mathematical manipulations. On the other hand, the received SNR at the untrustworthy relay during the first IT subinterval can be determined from (5) as

$$\Gamma_e = \frac{P_{\mathrm{S}} g_{\mathrm{SR}}}{P_{\mathrm{D}} g_{\mathrm{RD}} + N_0} = \frac{\gamma_{\mathrm{S}} g_{\mathrm{SR}}}{\gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1}. \tag{10}$$

IV. Secrecy Outage Probability

In this section, we derive closed-form analytical expressions for the secrecy outage probability of the considered TS-based SWIPT strategies. For this purpose, we first revisit the definition of secrecy capacity (C_s) as the maximum transmission rate feasible for a secure communication, which is expressed as the non-negative difference between the capacities of the legitimate and eavesdropping channels, that is[1]

$$C_s = [C_\ell - C_e]^+ = \frac{1}{2} \log_2 \left(\frac{1+\Gamma_\ell}{1+\Gamma_e} \right), \tag{11}$$

where $[x]^+ \triangleq \max\{0, x\}$. Consequently, the secrecy outage probability is defined as the probability that the secrecy capacity in (11) falls below a target secrecy rate $\mathcal{R}$. Thus,

[1]The scalar factor $\frac{1}{2}$ in (11) is due to the HD relaying mode.

from (9) and (10), the secrecy outage probability is determined as

$$P_{\text{sout}} = \Pr\left(\frac{1}{2}\log_2\left(\frac{1+\Gamma_\ell}{1+\Gamma_e}\right) < \mathcal{R}\right) = \Pr\left(\frac{1+\frac{\gamma_{\text{S}}\gamma_{\text{R}}g_{\text{SR}}g_{\text{RD}}}{\gamma_{\text{R}}g_{\text{RD}}+\gamma_{\text{S}}g_{\text{SR}}+\gamma_{\text{D}}g_{\text{RD}}+1}}{1+\frac{\gamma_{\text{S}}g_{\text{SR}}}{\gamma_{\text{D}}g_{\text{RD}}+1}} < 2^{2\mathcal{R}} \triangleq \tau\right). \tag{12}$$

Remark 1. Note from (1), (2), and (3) that the transmit SNR γ_{R} in (12) is a random variable depending on the channel gain of either the S→R link, the R→D link, or both of them, as S-WET, D-WET, or SD-WET is considered, respectively. Thus, an exact analysis of the secrecy outage probability proved intricate. Aiming at achieving useful insights on the system performance, we perform an asymptotic analysis for the considered strategies, from which we provide simple closed-form expressions of the secrecy outage probability in the following propositions.

Proposition 1. *A closed-form asymptotic analytical expression for the secrecy outage probability of a dual-hop relaying network with an energy-constrained, untrustworthy AF relay, which is powered by RF signals coming from S using TS-based SWIPT and subject to DBJ, is given by*

$$P_{\text{sout}} \simeq \sqrt{\frac{(1-\delta)(\tau-1)}{\delta\theta\gamma_P}}\left(\frac{1}{\Omega_{\text{SR}}}\right) + \sqrt{\frac{\delta\tau}{(1-\delta)\theta\gamma_P}}\left(\frac{1}{\Omega_{\text{RD}}}\right). \tag{13}$$

Proof. See Appendix A. □

Proposition 2. *A closed-form asymptotic analytical expression for the secrecy outage probability of a dual-hop relaying network with an energy-constrained, untrustworthy AF relay, which is powered by RF signals coming from D using TS-based SWIPT and subject to DBJ, is given by*

$$P_{\text{sout}} \simeq \frac{\tau}{\delta\gamma_P\Omega_{\text{RD}}} + \left(\frac{\delta\tau\Omega_{\text{SR}}}{(1-\delta)\gamma_P\theta}\right)^{\frac{1}{3}}\frac{\Gamma(\frac{4}{3})}{\Omega_{\text{RD}}}. \tag{14}$$

Proof. See Appendix B. □

Proposition 3. *A closed-form asymptotic analytical expression for the secrecy outage probability of a dual-hop relaying network with an energy-constrained, untrustworthy AF relay, which is powered by RF signals coming simultaneously from both S and D using TS-based SWIPT and subject to DBJ, is given by*

$$P_{\text{sout}} \simeq \frac{\tau}{\delta\gamma_P\Omega_{\text{SR}}} + \frac{\tau\theta\mu+\sqrt{\tau^2\theta^2\mu^2+4\delta(1-\delta)\tau\theta\gamma_P\mu}}{2(1-\delta)\theta\gamma_P\mu\Omega_{\text{RD}}} \tag{15}$$

Proof. See Appendix C. □

V. Numerical Results and Discussions

In this section, we evaluate our new analytical expressions for the secrecy outage probability of a relaying system with an AF untrustworthy relay powered by different WET strategies over illustrative scenarios. We also present Monte Carlo simulations to corroborate our analysis. For this purpose, we consider a linear network topology, in which the distance between S and D is normalized to unity, and R is midway between those nodes, so that $d_{\text{SD}} = 1$, $d_{\text{SR}} = 0.5$, and $d_{\text{RD}} = 0.5$, where d_i, $i \in \{\text{SD}, \text{SR}, \text{RD}\}$, is the distance between two given nodes. In addition, we assume that $\Omega_i = d_i^{-\beta}$, where β is the path-loss exponent, that is, the average channel gain of the ith link is given by the path loss. In our illustrative scenarios, we set $\beta = 4$, the target secrecy rate to $\mathcal{R} = 1$ bps/Hz, and the EH conversion efficiency factor to $\eta = 0.5$.

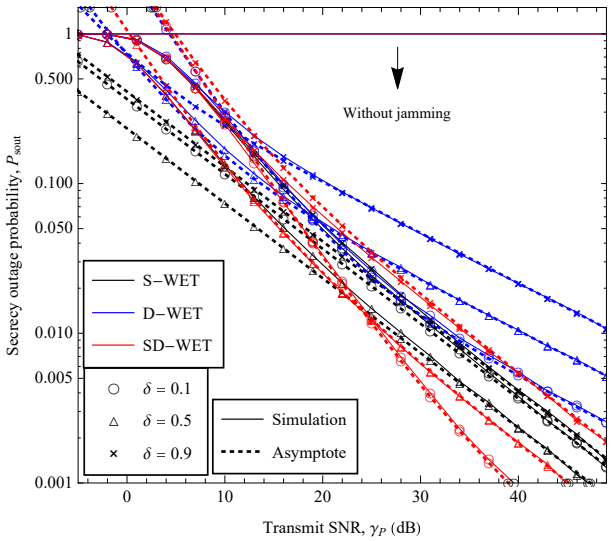

Fig. 1. Secrecy outage probability vs. transmit system SNR, for $\delta = 0.1, 0.5, 0.9$, with $\alpha = 0.5$ and $\mu = 0.5$.

Fig. 1 shows the secrecy outage probability as a function of transmit system SNR γ_P, considering the S-WET, D-WET and SD-WET strategies, for distinct values of the power allocation factor δ between S and D. In this case, we set the power allocation factor between the source and destination for the EH phase to $\mu = 0.5$. Note how our analytical expressions given by (13) to (15) are tight to the simulation results at medium-to-high SNR. By noticing D-WET and SD-WET strategies, at the high-SNR regime, the system secrecy performance improves as δ decreases, so that the jamming signal transmitted during the first subinterval of the IT phase becomes stronger. Moreover, we can observe that, at a high SNR regime and $\delta \leq 0.5$, the SD-WET strategy outperforms both S-WET- and D-WET-based counterparts. For all strategies, it is shown that legitimate nodes cannot communicate in secrecy without employing the DBJ technique.

Fig. 2 shows the secrecy outage probability versus the power allocation factor δ between S and D, considering S-WET, D-WET, and SD-WET strategies. In addition, we consider different values of the time allocation factor α, and we set the transmit system SNR to $\gamma_P = 30$ dB. For the SD-WET strategy, we set the power allocation factor between S and D for the EH phase to $\mu = 0.5$. Overall, we can notice that the system secrecy performance improves as α increases (i.e., as more time is allocated to the EH phase), irrespective of the power allocation factor δ between S and D. For S-WET, the secrecy performance for interval between $0.2 < \delta < 0.8$ remains roughly the same for a given value of α, which indicates that the power allocation factor between S and D for

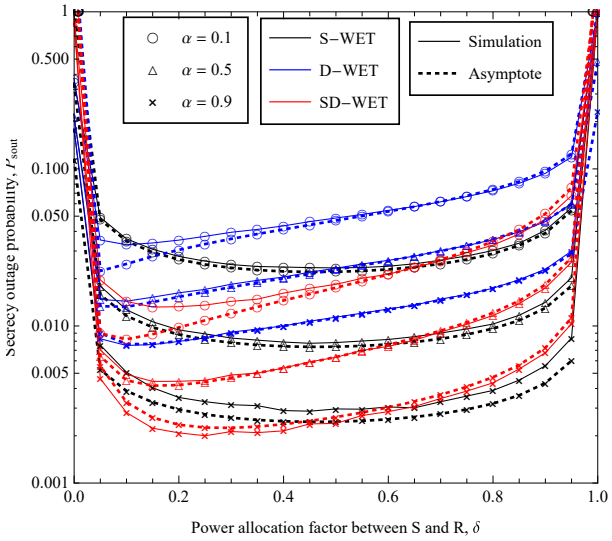

Fig. 2. Secrecy outage probability vs. power allocation factor δ in the IT phase, for $\alpha = 0.1, 0.5, 0.9$, with $\mu = 0.5$ and $\gamma_P = 30$ dB.

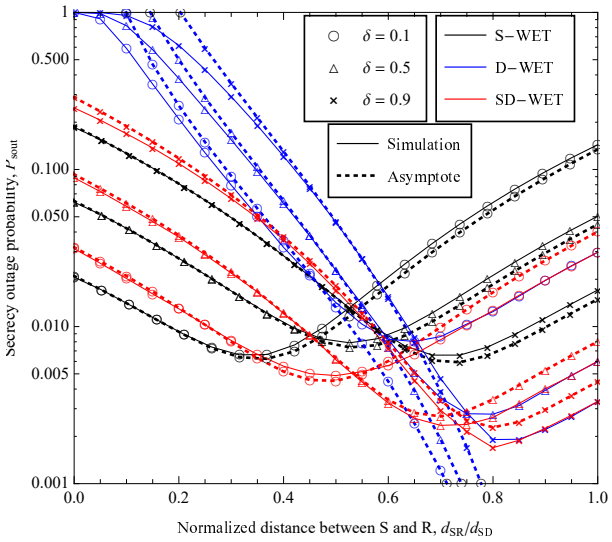

Fig. 3. Secrecy outage probability vs. normalized distance between S and R, $d_{\rm SR}/d_{\rm SD}$, for $\delta = 0.1, 0.5, 0.9$, with $\alpha = 0.5$, $\mu = 0.5$, and $\gamma_P = 30$ dB.

the transmission of information and jamming signals barely impacts the secrecy performance in this strategy. As to the D-WET strategy, we note that the secrecy performance worsens as δ increases—i.e., as more power is allocated to the source for the information signal transmission and, consequently, less power is allocated to the destination for the jamming signal transmission during the first subinterval of the IT phase—, irrespective of the value of α. In turn, we can notice from SD-WET strategy, for $0.1 < \delta < 0.7$, the secrecy performance clearly outperforms both the S-WET and D-WET cases, whereas for $\delta > 0.7$ this gain diminishes with respect to its counterparts, with the secrecy performance becoming similar to that of the S-WET strategy.

Fig. 3 illustrates the secrecy outage probability for S-WET, D-WET and SD-WET strategies as a function of the normalized distance between S and R $d_{\rm SR}/d_{\rm SD}$, for different values of power allocation factor between S and D δ and $\mu = 0.5$. We can observe that the system secrecy performance of SD-WET strategy is similar to that of the S-WET strategy for the relay's positions closer to the source, and similar to that of the D-WET strategy for the relay's positions closer to the destination. This can be explained from (3) by the fact that, depending on the relay's position, the gain channel of the first-hop or second-hop becomes stronger on average, so that the transmit power at R approximates the case of the S-WET or D-WET strategy, respectively. By comparing all strategies, we notice that the best WET strategy in terms of secrecy performance depends on the relay's position, as follows: S-WET for relay's positions closer to the source; SD-WET for relay's positions at half the distance between source and destination; and either D-WET or SD-WET for relay's positions closer to the destination.

VI. Conclusion

In this work, we investigated the secrecy outage performance of a relaying network with an energy-constrained, untrustworthy AF, in which a DBJ technique is used for providing information secrecy. We considered three different TS-based SWIPT strategies referred herein to as S-WET, D-WET and SD-WET, which enable the relay to be power supplied from the source, destination, or both of them, respectively. For all these strategies, we derived useful closed-form analytical expressions based on an asymptotic analysis, which were validated by Monte Carlo simulations. By applying these expressions to different illustrative scenarios, we assessed the impact of key system parameters on the secrecy performance, including the time allocation factor for the EH and IT phases, the power allocation factor between the source and destination for the transmission of information and jamming signals in the IT phase, and the relay's relative position between source and destination. Overall, it was observed that, for all strategies, the secrecy performance improves as the time allocation factor for EH increases. Also, the SD-WET strategy showed to outperform both S-WET and D-WET counterparts at medium to high SNR, with the secrecy performance improving as the jamming signal becomes stronger. As to the impact of the relay's relative position, the best secrecy performance was attained by the S-WET strategy when the relay approaches the source; by the SD-WET strategy when the relay is midway between the source and destination; and by either the D-WET or SD-WET strategy when the relay is close to the destination.

Appendix A
Proof of Proposition 1

From (12), by performing some manipulations, we have replaced $\gamma_{\rm R}$ by (1) and have considered a high SNR regime. Now, we analyze the corresponding integration regions. To do so, we propose an approximation based on two rectangular regions, which are attained by considering the horizontal and vertical asymptotes in the limits $g_{\rm SR}\to\infty$ and $g_{\rm RD}\to\infty$, respectively. Thus, the rectangular regions can be expressed as

$$\text{A1} = g_{\rm RD} < \frac{\tau\delta\theta + \sqrt{\tau^2\delta^2\theta^2 + 4\tau\delta^3(1-\delta)\theta\gamma_P}}{2\delta(1-\delta)\theta\gamma_P} \qquad (16)$$

$$\text{A2} = g_{\rm SR} < \frac{\theta(\tau-1)}{2\delta\theta\gamma_P}$$

$$+\frac{\sqrt{\theta^2(\tau-1)^2+4\delta(1-\delta)\theta\gamma_P(\tau-1)}}{2\delta\theta\gamma_P}. \tag{17}$$

Thus, by assuming that each region is independent and neglecting the terms proportional to $1/\gamma_P$, the Maclaurin series expansion of the exponential function is employed, so that $e^{-x} \simeq 1-x$ for $x \to 0$ [13, eq. (0.318.2)]. Then, a closed-form asymptotic expression for the secrecy outage probability of the system, considering the S-WET strategy, is obtained as in (13).

Appendix B
Proof of Proposition 2

By considering a high-SNR regime, we first approximate the numerator in the argument of $\Pr(\cdot)$ in (12); and then, after performing some manipulations we have used the upper bound for the harmonic mean, given by $\min\{A,B\} \geq AB/(A+B+1)$, then replaced $P_{\rm R}$ in $\gamma_{\rm R}$ as in (2), and considered a high SNR regime, thus neglecting the terms proportional to $1/\gamma_P$ and isolated the term $\min\{\cdot,\cdot\}$. Next, we determine the integration regions for the secrecy outage events in the argument of $\Pr(\cdot)$. Thus, an approximation to the secrecy outage probability of the system is given by

$$\begin{aligned}
&P_{\rm sout}\\
&= F_{g_{\rm SR}}(g_{\rm SR1}) + \int_{g_{\rm SR1}}^{g_{\rm SR2}} F_{g_{\rm RD}}\left(\frac{1}{2}\left(\frac{(1-\delta)^4\tau^2}{(1-\delta)^2\theta^2(\delta x\gamma_P-\tau)^2}\right.\right.\\
&+\left.\left.\frac{4\delta^2(1-\delta)^2\theta\tau x^2\gamma_P+\delta^2\theta^2\tau^2x^2-2\delta(1-\delta)^2\theta\tau^2x}{(1-\delta)^2\theta^2(\delta x\gamma_P-\tau)^2}\right)^{\frac{1}{2}}\right.\\
&+\left.\frac{-(1-\delta)^2\tau-\delta\theta\tau x}{2(1-\delta)\theta(\tau-\delta x\gamma_P)}\right) f_{g_{\rm SR}}(x)dx + \int_{g_{\rm SR2}}^{\infty} F_{g_{\rm RD}}\left(\left(\frac{\delta}{(1-\delta)}\right.\right.\\
&\times\left.\frac{\tau x}{2\theta\gamma_P}+\left(\frac{\delta^2\tau^2x^2}{4(1-\delta)^2\theta^2\gamma_P^2}-\frac{\tau^3}{27\theta^3\gamma_P^3}\right)^{\frac{1}{2}}\right)^{\frac{1}{3}}+\frac{\tau}{3\theta\gamma_P}\\
&\times\left.\left(\frac{\delta\tau x}{2(1-\delta)\theta\gamma_P}+\left(\frac{\delta^2\tau^2x^2}{4(1-\delta)^2\theta^2\gamma_P^2}-\frac{\tau^3}{27\theta^3\gamma_P^3}\right)^{\frac{1}{2}}\right)^{-\frac{1}{3}}\right)\\
&\times f_{g_{\rm SR}}(x)dx,
\end{aligned} \tag{18}$$

where $F_{g_{\rm SR}}(\cdot)$ and $f_{g_{\rm SR}}(\cdot)$ denote the cumulative distribution function and probability density function of $g_{\rm SR}$, respectively, and

$$\begin{aligned}
g_{\rm SR1} &= \frac{\tau}{\gamma_P\delta},\\
g_{\rm SR2} &= \frac{\theta\tau^2+5(1-\delta)^2\tau\gamma_P}{2\delta(1-\delta)^2\gamma_P^2}+\frac{1}{2}\left(\frac{\theta^3\tau^4+8(1-\delta)^6\tau\gamma_P^3}{\delta^2(1-\delta)^4\theta\gamma_P^4}\right.\\
&\quad\left.+\frac{17(1-\delta)^4\theta\tau^2\gamma_P^2+10(1-\delta)^2\theta^2\tau^3\gamma_P}{\delta^2(1-\delta)^4\theta\gamma_P^4}\right)^{\frac{1}{2}}.
\end{aligned}$$

By considering that the terms proportional to $1/\gamma_P$ and $1/\gamma_P^2$ in (18) go to zero in the high-SNR regime and applying the Maclaurin series expansion of the exponential function [13, eq. (0.318.2)] to the integrands in (18), after some algebraic manipulations, we attain a closed-form asymptotic expression for the secrecy outage probability of the system, considering the D-WET strategy, given as in (14).

Appendix C
Proof of Proposition 3

From (12), by replacing $\gamma_{\rm R}$ by (3), and after some algebraic manipulations, the secrecy outage probability can be approximated into two rectangular areas, C1 and C2, referred as horizontal and vertical asymptotes, $g_{\rm SR} \to \infty$ and $g_{\rm RD} \to \infty$, respectively. Thus, the regions are given as

$$\mathrm{C1} = g_{\rm RD} < \frac{\tau\theta\mu+\sqrt{\tau^2\theta^2\mu^2+4\tau\delta(1-\delta)\theta\gamma_P\mu}}{2(1-\delta)\theta\gamma_P\mu} \tag{19}$$

$$\mathrm{C2} = g_{\rm SR} < \frac{\tau}{\delta\gamma_P}. \tag{20}$$

By replacing (19) and (20) into $P_{\rm sout} \simeq \Pr(\mathrm{C1})+\Pr(\mathrm{C2})-\Pr(\mathrm{C1})\Pr(\mathrm{C2})$ and assuming a high-SNR regime scenario, whereby higher order terms proportional to $1/\gamma_P$ are neglected, terms are simplified using Maclaurin series expansion of the exponential function [13, eq. (0.318.2)], thus obtaining an useful closed-form asymptotic expression for the secrecy outage probability of the system considering the SD-WET strategy, given as in (15).

References

[1] 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.

[2] D. P. Osorio, J. D. Sanchez, and H. Alves, "Physical-layer security for 5G and beyond," in *Wiley 5G Ref.* American Cancer Society, 2019, pp. 1–19.

[3] G. Luo, J. Li, Z. Liu, X. Tao, and F. Yang, "Physical layer security with untrusted relays in wireless cooperative networks," in *Proc. IEEE WCNC*, San Francisco, USA, Mar. 2017, pp. 1–6.

[4] D. P. M. Osorio, H. Alves, and E. E. B. Olivo, "On the secrecy performance and power allocation in relaying networks with untrusted relay in the partial secrecy regime," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2268–2281, Dec. 2019.

[5] R. Zhao, X. Tan, D.-H. Chen, Y.-C. 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, Aug. 2018.

[6] A. Abrol and R. K. Jha, "Power optimization in 5G networks: A step towards green communication," *IEEE Access*, vol. 4, pp. 1355–1374, Apr. 2016.

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

[8] 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, Nov. 2017.

[9] 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, Mar. 2018.

[10] A. Mabrouk, A. El Shafie, K. Tourki, and N. Al-Dhahir, "An-aided relay-selection scheme for securing untrusted RF-EH relay systems," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 4, pp. 481–493, Aug. 2017.

[11] H. Shi, Y. Cai, D. Chen, J. Hu, W. Yang, and W. Yang, "Physical layer security in an untrusted energy harvesting relay network," *IEEE Access*, vol. 7, pp. 24 819–24 828, Feb. 2019.

[12] 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 PIMRC*, Istanbul, Turkey, Sep. 2019, pp. 1–6.

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