Reliability-Security in Wireless-Powered Cooperative Network with Friendly Jammer

Van Duc PHAN[1], *Thanh Luan NGUYEN*[2], *Tran Tin PHU*[3], *Van Vinh NGUYEN*[4]

[1]Faculty of Automotive Engineering, School of Engineering and Technology, Van Lang University,
69/68 Dang Thuy Tram Street, 700000 Ho Chi Minh City, Vietnam
[2]Faculty of Electronics Technology, Industrial University of Ho Chi Minh City,
12 Nguyen Van Bao Street, 700000 Ho Chi Minh City, Vietnam
[3]Faculty of Information Technology, Ton Duc Thang University,
19 Nguyen Huu Tho Street, 700000 Ho Chi Minh City, Vietnam
[4]Department of Information Assurance, FPT University, Hoa Lac Hi-tech Park, 100000 Hanoi, Vietnam

duc.pv@vlu.edu.vn, nguyenthanhluan@iuh.edu.vn, phutrantin79@gmail.com, vinhnv27@fe.edu.vn

DOI: 10.15598/aeee.v20i4.4511

Article history: Received Mar 22, 2022; Revised Aug 11, 2022; Accepted Sep 20, 2022; Published Dec 31, 2022.

Abstract. *In this paper, we study the Outage Probability (OP) and the Intercept Probability (IP) of Wireless-Powered Cooperative Networks (WPCNs) in the presence of a malicious eavesdropper and a friendly jammer. We specifically present the system model and the power splitting Energy Harvesting (EH) architecture to increase system reliability and security. In addition, we obtain exact analytical equations for the OP and IP. Asymptotic analysis in the low Signal-to-Jam Ratio (SJR) regimes expressed in integral-form expressions are provided to observe the lower bound of the IP. Finally, all derivations are validated by simulation results using the Monte Carlo method.*

Keywords

Energy Harvesting, Intercept Probability, Outage Probability.

1. Introduction

Energy Harvesting (EH) is one of the core features for the development of self-sustaining wireless networks, and is envisioned to play a vital role in Industry 4.0. Solid-state batteries, which are commonly utilized as to power energy-constrained wireless devices, are formerly required on-site maintenance such as as recharging, replacing or reducing the network's self-sufficiency. The integration of EH-assisted nodes as alternative sources of wireless network power is regarded as one of the most promising techniques for developing the next generation of wireless networks while diminishing the requirement for external power sources [1], [2] and [3]. EH technologies convert various sources of ambient energy into electricity, which may then be used to power energy-constrained wireless devices such as sensors, remote monitoring devices, and wearable or implanted medical equipment [4], [5], [6], [7] and [8].

Cryptography-based security technologies have historically been used to ensure high security requirement [9]. Physical-Layer Security (PLS) has been proposed as a possible solution for mitigating physical layer security holes. A PLS technique is applied at the physical layer to safeguard communication between two terminals through the use of Quantum Key Distribution (QKD). The core principle behind PLS is that each node creates a random sequence that it keeps hidden from the other nodes. When high security constraints are in place, PLS techniques are preferred for ensuring a secure end-to-end communication [10] and [11]. The primary idea behind this form of data transfer is that each message gets divided into many sub-messages, and is then sent out to wireless nodes throughout the network for reassembling at the receivers [10] and [11]. There has been extensive research on using PLS in wireless networks with cooperative relaying, Ambient

Backscatter Communication (ABC), jamming and Multiple-Input-Multiple-Output (MIMO) [12], [13], [14], [15] and [16].

In this paper, we study the effects of a malevolent eavesdropper and friendly jammer on the Outage Probability (OP) and Intercept Probability (IP) for PLS. We presented a system model and an energy harvesting architecture to improve the reliability and security of power splitting systems. Furthermore, we develop accurate analytical formulations for both OP and IP. The lower bound of the IP, as determined via an asymptotic analysis (in low-SJR), is given in integral form. Finally, the Monte Carlo approach is utilized to validate all derivations.

2. System Model

We study the trade-off between reliability and security in networks that use a relay node, R, to communicate between a source node, S, and a destination node, D. Considering that the communication from S to D is overheard by a malicious eavesdropper, E, a friendly jammer J is deployed in an attempt to block transmission of information from S to E as shown in Fig. 1. In this paper, we explore the scenario where R is an EH node capable of harvesting energy to assist $S \to D$ transmission, which is equally divided into two time slots. In the first time slot, both S and J simultaneously broadcasts the information signal, x_S, and the jamming signal, x_J. At R, some of the received power is exploited for EH operation; the rest of that energy is used for information processing [3], [17], [18] and [19]. In order to capture the effect of small-scale fading on channel coeffiecent, we consider h_{XY} defined as: $h_{\mathrm{XY}} \triangleq \mathrm{PL}_{\mathrm{XY}}^{-1/2} g_{\mathrm{XY}}$, where $\mathrm{PL}_{\mathrm{XY}}$ specifies path loss and g_{XY} is a circularly symmetric complex Gaussian random variable whose mean and variance equal variance 0 and 1, respectively. Hence, the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) of node X's channel power gain to that of node Y are [15], [16] and [17] given by Eq. (1), respectively, for $x > 0$, where $\lambda_{\mathrm{XY}} \triangleq 1/\mathrm{PL}_{\mathrm{XY}}$:

$$\begin{aligned} f_{|h_{\mathrm{XY}}|^2}(x) &= \frac{1}{\lambda_{\mathrm{XY}}} e^{-\frac{x}{\lambda_{\mathrm{XY}}}}, \\ F_{|h_{\mathrm{XY}}|^2}(x) &= 1 - e^{-\frac{x}{\lambda_{\mathrm{XY}}}}. \end{aligned} \tag{1}$$

We use the 3rd Generation Partnership Project (3GPP) Urban Micro path loss at frequencies ranging from 2 to 6 GHz and distances ranging from 10 to 2000 m to simulate wireless signal propagation in urban contexts [20] and [21]. The 3GPP UMi path loss model is presented by [20], [21] and [22] $\mathrm{PL}_{\mathrm{XY}}(\mathrm{dB}) = 36.7\log_{10}(D) + 22.7 + 26\log_{10}(f_c)$, where f_c (GHz) denotes the carrier frequency and D is the distance.

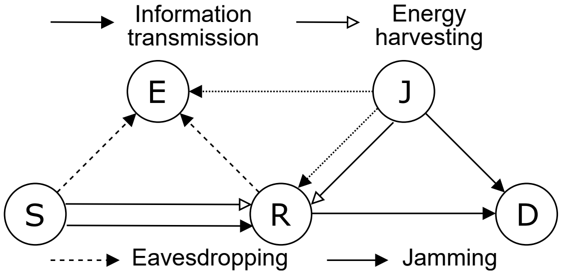

Fig. 1: System model.

2.1. Energy Harvesting

In the first time slot, both S and J broadcast their signals as illustrated in Fig. 1. By principles of power-splitting EH architecture in [8], the harvested energy at R is calculated as $\eta\beta\left[P_S\left|h_{\mathrm{SR}}\right|^2 + \theta P_J\left|h_{\mathrm{JR}}\right|^2\right] T/2$. As a result, the harvested power is $P_R = \frac{E_R}{T/2}$ [8] and can be further expressed as:

$$P_R = \eta\beta\left[P_S\left|h_{\mathrm{SR}}\right|^2 + \theta P_J\left|h_{\mathrm{JR}}\right|^2\right], \tag{2}$$

where $0 \le \beta \le 1$ is the fraction of received power being exploited for EH, θ denotes the power control coefficient for J, η is the EH efficiency, where $0 \le \eta \le 1$, [8], P_S denotes the transmission power of S and P_J is the power budget of J.

2.2. Transmission Scheme

In the first time slot, the source node broadcasts the unit-energy information signal x_S, where $\mathbb{E}[|x_S|^2] = 1$ W. The friendly jammer uses only a portion of its total power budget to broadcast x_J, where $\mathbb{E}[|x_J|^2] = 1$ W, thereby jamming E. Consequently, the received signals at R and E can be expressed as Eq. (3) and Eq. (4), respectively:

$$\begin{aligned} y_{\mathrm{SR}} = &\sqrt{(1-\beta)P_S}\, h_{\mathrm{SR}} x_S + \\ &+ \sqrt{\theta(1-\beta)P_J}\, h_{\mathrm{JR}} x_J + n_R, \end{aligned} \tag{3}$$

$$y_{\mathrm{SE}} = \sqrt{P_S}\, h_{\mathrm{SE}} x_S + \sqrt{\theta P_J}\, h_{\mathrm{JE}} x_J + n_E, \tag{4}$$

where $n_R \sim \mathcal{CN}(0, \sigma_R^2)$ and $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ are the Additive White Gaussian Noises (AWGNs) at R and E with variances σ_R^2 (W) and σ_E^2 (W), respectively.

If R correctly decodes x_S, it transmits an encoded version of that message, denoted as $\hat{x}_S$, in its next transmission slot. Accordingly, the received signals E and D in the second time slot can be expressed as EQ. (5) and Eq. (6), respectively:

$$y_{\mathrm{RD}} = \sqrt{P_R}\, h_{\mathrm{RD}} \hat{x}_S + \sqrt{(1-\theta)P_J}\, h_{\mathrm{JD}} x_J + n_D, \tag{5}$$

$$y_{\mathrm{RE}} = \sqrt{P_R}\, h_{\mathrm{RE}} \hat{x}_S + \sqrt{(1-\theta)P_J}\, h_{\mathrm{JE}} x_J + n_E, \tag{6}$$

where $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ and $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ are AWGNs at D and E, respectively, where $\mathbb{E}[|n_D|^2] = \sigma_D^2$ (W) and $\mathbb{E}[|n_E|^2] = \sigma_E^2$ (W).

Utilizing Eq. (3) and Eq. (5), the end-to-end (e2e) Signal-to-Noise Ratio (SNR) at D can be obtained as:

$$\gamma_D^{\mathrm{e2e}} = \min\left[\bar{\gamma}_{\mathrm{SR}}|h_{\mathrm{SR}}|^2, \eta\beta\left(\bar{\gamma}_{\mathrm{SD}}|h_{\mathrm{SR}}|^2 + \right.\right.$$
$$\left.\left. + \theta\bar{\gamma}_{\mathrm{JD}}|h_{\mathrm{JR}}|^2\right)|h_{\mathrm{RD}}|^2\right], \tag{7}$$

where $\bar{\gamma}_{\mathrm{SR}} \triangleq (1-\beta)\frac{P_S}{\sigma_R^2}$, $\bar{\gamma}_{\mathrm{SD}} \triangleq \frac{P_S}{\sigma_D^2}$, and $\bar{\gamma}_{\mathrm{JD}} \triangleq \frac{P_J}{\sigma_D^2}$.

Utilizing Eq. (4) and Eq. (6), the e2e SNR at E can be expressed as:

$$\gamma_E^{\mathrm{e2e}} = \max\left[\frac{\bar{\gamma}_{\mathrm{SE}}|h_{\mathrm{SE}}|^2}{\theta\bar{\gamma}_{\mathrm{JE}}|h_{\mathrm{JE}}|^2 + 1}, \frac{\eta\beta}{(1-\theta)\bar{\gamma}_{\mathrm{JE}}|h_{\mathrm{JE}}|^2 + 1}\cdot\right.$$
$$\left.\cdot\left(\bar{\gamma}_{\mathrm{SE}}|h_{\mathrm{SR}}|^2 + \theta\bar{\gamma}_{\mathrm{JE}}|h_{\mathrm{JR}}|^2\right)|h_{\mathrm{RE}}|^2\right], \tag{8}$$

where $\bar{\gamma}_{\mathrm{SE}} \triangleq \frac{P_S}{\sigma_E^2}$, and $\bar{\gamma}_{\mathrm{JE}} \triangleq \frac{P_J}{\sigma_E^2}$.

2.3. Outage Probability

The OP at D is defined as the probability that the e2e SNR is lower than a specified threshold γ_{th} [23]. As a result, we obtain that:

$$\mathrm{OP}(\gamma) = \Pr\left[\gamma_D^{\mathrm{e2e}} < \gamma_{\mathrm{th}}\right]. \tag{9}$$

Theorem 1. *The OP at D can be derived in an exact closed-form expression as:*

$$\mathrm{OP}(\gamma) = 1 - \frac{1}{1 - \dfrac{c\lambda_{\mathrm{SR}}}{\lambda_{\mathrm{JR}}}}\left(e^{-\frac{a}{\lambda_{\mathrm{SR}}} + \frac{ac}{\lambda_{\mathrm{JR}}}}\gamma_1\cdot\right.$$
$$\left.\cdot\left(\frac{d}{\lambda_{\mathrm{RD}}}; \frac{b}{\lambda_{\mathrm{JR}}\lambda_{\mathrm{RD}}}\right) - \gamma_1\left(\frac{d}{\lambda_{\mathrm{RD}}}; \frac{b}{c\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}}\right)\right) -$$
$$+ e^{-\frac{d}{\lambda_{\mathrm{RD}}} - \frac{a}{\lambda_{\mathrm{SR}}}} - \gamma_1\left(\frac{d}{\lambda_{\mathrm{RD}}}; \frac{b}{c\lambda_{\mathrm{RD}}\lambda_{\mathrm{SR}}}\right), \tag{10}$$

where $\gamma_v(x; y)$ denotes the v-th order lower generalized incomplete gamma function [24].

Proof. By substituting Eq. (7) into Eq. (9), and after some mathematical manipulations, we obtain:

$$\mathrm{OP}(\gamma) = 1 - \Pr\left[d > |h_{\mathrm{RD}}|^2, \frac{b}{c|h_{\mathrm{RD}}|^2} > \right.$$
$$\left. > |h_{\mathrm{SR}}|^2 > a, |h_{\mathrm{JR}}|^2 > \frac{b}{|h_{\mathrm{RD}}|^2} - c|h_{\mathrm{SR}}|^2\right] -$$
$$+ \Pr\left[|h_{\mathrm{SR}}|^2 > a, |h_{\mathrm{RD}}|^2 > d\right] -$$
$$+ \Pr\left[|h_{\mathrm{SR}}|^2 > \frac{b}{c|h_{\mathrm{RD}}|^2}, |h_{\mathrm{RD}}|^2 < d\right], \tag{11}$$

where $a \triangleq \frac{\gamma_{\mathrm{th}}}{\bar{\gamma}_{\mathrm{SR}}}$, $b \triangleq \frac{\gamma_{\mathrm{th}}}{\eta\beta\theta\bar{\gamma}_{\mathrm{JD}}}$, $c \triangleq \frac{\bar{\gamma}_{\mathrm{SD}}}{\theta\bar{\gamma}_{\mathrm{JD}}}$, and $d \triangleq \frac{\bar{\gamma}_{\mathrm{SR}}}{\eta\beta\bar{\gamma}_{\mathrm{SD}}}$.

Accordingly, the analytical-form expression of the above probability is given by:

$$\mathrm{OP}(\gamma) = 1 -$$
$$+ \int_0^d f_{|h_{\mathrm{RD}}|^2}(z)\mathrm{d}z \int_a^{\frac{b}{cz}} f_{|h_{\mathrm{SR}}|^2}(y)\mathrm{d}y \int_{\frac{b}{z} - cy}^{\infty} f_{|h_{\mathrm{JR}}|^2}(x)\mathrm{d}x -$$
$$+ \int_d^{\infty} f_{|h_{\mathrm{RD}}|^2}(z)\mathrm{d}z \int_a^{\infty} f_{|h_{\mathrm{SR}}|^2}(x)\mathrm{d}x -$$
$$+ \int_0^d f_{|h_{\mathrm{RD}}|^2}(z)\mathrm{d}z \int_{\frac{b}{cz}}^{\infty} f_{|h_{\mathrm{SR}}|^2}(x)\mathrm{d}x. \tag{12}$$

Plugging the PDF of $|h_{\mathrm{XY}}|^2$ into Eq. (12), using the identity $\int e^{ax}\mathrm{d}x = \frac{e^{ax}}{a}$, and some mathematical steps, we obtain:

$$\mathrm{OP}(\gamma) = 1 - \frac{\dfrac{1}{\lambda_{\mathrm{RD}}\lambda_{\mathrm{SR}}}}{\dfrac{1}{\lambda_{\mathrm{SR}}} - \dfrac{c}{\lambda_{\mathrm{JR}}}}\left(e^{-\frac{a}{\lambda_{\mathrm{SR}}} + \frac{ac}{\lambda_{\mathrm{JR}}}}\cdot\right.$$
$$\left.\cdot\int_0^d e^{\frac{z}{\lambda_{\mathrm{RD}}} - \frac{b}{\lambda_{\mathrm{JR}}}\frac{1}{z}}\mathrm{d}z - \int_0^d e^{\frac{z}{\lambda_{\mathrm{RD}}} - \frac{b}{c\lambda_{\mathrm{SR}}}\frac{1}{z}}\mathrm{d}z\right) - \tag{13}$$
$$- e^{-\frac{d}{\lambda_{\mathrm{RD}}} - \frac{a}{\lambda_{\mathrm{SR}}}} - \frac{1}{\lambda_{\mathrm{RD}}}\int_0^d e^{-\frac{b}{c\lambda_{\mathrm{SR}}}\frac{1}{z} - \frac{z}{\lambda_{\mathrm{RD}}}}\mathrm{d}z.$$

Using $\int_0^x t^{\alpha-1}e^{-at-bt^{-1}}\mathrm{d}t = a^{\alpha}\gamma_{\alpha}(ax; ab)$, we obtain Eq. (10). This completes the proof of Thm. 1. □

2.4. Intercept Probability

The Intercept Probability (IP) is defined by [25]:

$$\mathrm{IP}(\gamma_{\mathrm{th}}) = \Pr\left[\gamma_E^{\mathrm{e2e}} \geq \gamma_{\mathrm{th}}\right]. \tag{14}$$

Before deriving the analytical form of Eq. (14), we introduce the following Lem. 1 to aid further analysis.

Lemma 1. *Let us denote $\gamma_{\mathrm{SJR}} = |h_{\mathrm{SR}}|^2 + \frac{\theta P_J}{P_S}|h_{\mathrm{JR}}|^2$, its PDF is obtained as:*

$$f_{\gamma_{\mathrm{SJR}}}(\gamma) = \frac{1}{1 - \dfrac{\lambda_{\mathrm{SR}}P_S}{\theta\lambda_{\mathrm{JR}}P_J}}\frac{P_S}{\theta P_J\lambda_{\mathrm{JR}}}e^{-\frac{\gamma P_S}{\theta P_J\lambda_{\mathrm{JR}}}} +$$
$$+ \frac{1}{1 - \dfrac{\theta\lambda_{\mathrm{JR}}P_J}{\lambda_{\mathrm{SR}}P_S}}\frac{1}{\lambda_{\mathrm{SR}}}e^{-\frac{\gamma}{\lambda_{\mathrm{SR}}}}, \ \gamma > 0. \tag{15}$$

Proof. The PDF of γ_{SJR} can be obtained as follows:

$$
\begin{aligned}
f_{\gamma_{\mathrm{SJR}}}(\gamma) &= \mathcal{L}^{-1}\left\{\int_0^\infty e^{-sx} f_{\gamma_{\mathrm{SJR}}}(x)\mathrm{d}x; s,\gamma\right\} = \\
&= \mathcal{L}^{-1}\left\{\int_0^\infty e^{-\frac{s\theta P_J}{P_S}y} f_{|h_{\mathrm{JR}}|^2}(y)\mathrm{d}y \cdot \right. \\
&\quad \left. \cdot \int_0^\infty e^{-sx} f_{|h_{\mathrm{SR}}|^2}(x)\mathrm{d}x; s,\gamma\right\} = \\
&= \frac{\frac{P_S}{P_J}}{\theta\lambda_{\mathrm{JR}}\lambda_{\mathrm{SR}}}\mathcal{L}^{-1}\left\{\frac{1}{s+\frac{P_S}{\theta\lambda_{\mathrm{JR}}P_J}}\frac{1}{s+\frac{1}{\lambda_{\mathrm{SR}}}}; s,\gamma\right\} = \\
&= \frac{1}{\theta\lambda_{\mathrm{JR}}\lambda_{\mathrm{SR}}}\frac{P_S}{P_J}\frac{1}{\frac{1}{\lambda_{\mathrm{SR}}}-\frac{P_S}{\theta\lambda_{\mathrm{JR}}P_J}} \cdot \\
&\quad \cdot\mathcal{L}^{-1}\left\{\frac{1}{s+\frac{P_S}{\theta\lambda_{\mathrm{JR}}P_J}}-\frac{1}{s+\frac{1}{\lambda_{\mathrm{SR}}}}; s,\gamma\right\},
\end{aligned}
\tag{16}
$$

where $\mathcal{L}^{-1}\{F(s); s,\gamma\}$ is the inverse Laplace transform from s-domain to γ-domain. Utilizing the linear property of inverse Laplace transform and the identity $\mathcal{L}^{-1}\{\frac{1}{s+a}; s,t\} = e^{-at}$, we obtain Eq. (15). This completes the proof of Lem. 1. □

Theorem 2. *The IP at E can be derived as:*

$$
\begin{aligned}
\mathrm{IP}_E(\gamma_{\mathrm{th}}) &= \frac{1}{\lambda_{\mathrm{JE}}}\int_0^\infty \frac{f_{\gamma_{\mathrm{SJR}}}(t)}{\frac{1}{\lambda_{\mathrm{JE}}}+\frac{\gamma_{\mathrm{th}}(1-\theta)P_J}{\eta\beta\lambda_{\mathrm{RE}}P_S}\frac{1}{t}} \cdot \\
&\cdot e^{-\frac{\gamma_{\mathrm{th}}}{\eta\beta\bar{\gamma}_{\mathrm{SE}}\lambda_{\mathrm{RE}}}\frac{1}{t}}\mathrm{d}t + \frac{e^{-\frac{\gamma_{\mathrm{th}}}{\bar{\gamma}_{\mathrm{SE}}\lambda_{\mathrm{SE}}}}}{1+\frac{\gamma_{\mathrm{th}}\theta\lambda_{\mathrm{JE}}P_J}{\lambda_{\mathrm{SE}}P_S}} - \frac{e^{-\frac{\gamma_{\mathrm{th}}}{\bar{\gamma}_{\mathrm{SE}}\lambda_{\mathrm{SE}}}}}{\lambda_{\mathrm{JE}}} \cdot \\
&\cdot \int_0^\infty \frac{f_{\gamma_{\mathrm{SJR}}}(t)}{\frac{1}{\lambda_{\mathrm{JE}}}+\frac{\gamma_{\mathrm{th}}\theta P_J}{\lambda_{\mathrm{SE}}P_S}+\frac{\gamma_{\mathrm{th}}(1-\theta)P_J}{\eta\beta\lambda_{\mathrm{RE}}P_S}\frac{1}{t}} e^{-\frac{\gamma_{\mathrm{th}}}{\eta\beta\bar{\gamma}_{\mathrm{SE}}\lambda_{\mathrm{SE}}}\frac{1}{t}}\mathrm{d}t.
\end{aligned}
\tag{17}
$$

Proof. By substituting Eq. (8) into Eq. (14) and after some mathematical manipulations, we obtain:

$$
\begin{aligned}
\mathrm{IP}_E(\gamma_{\mathrm{th}}) &= 1-\int_0^\infty f_{\gamma_{\mathrm{SJR}}}(t)\mathrm{d}t\int_0^\infty f_{|h_{\mathrm{JE}}|^2}(z)\mathrm{d}z \cdot \\
&\cdot \int_0^{\frac{\gamma_{\mathrm{th}}(1-\theta)P_J}{\eta\beta P_S}\frac{z}{t}+\frac{\gamma_{\mathrm{th}}}{\eta\beta\bar{\gamma}_{\mathrm{SE}}}\frac{1}{t}} f_{|h_{\mathrm{RE}}|^2}(y)\mathrm{d}y \cdot \\
&\cdot \int_0^{\frac{\gamma_{\mathrm{th}}\theta P_J}{P_S}z+\frac{\gamma_{\mathrm{th}}}{\bar{\gamma}_{\mathrm{SE}}}} f_{|h_{\mathrm{SE}}|^2}(x)\mathrm{d}x.
\end{aligned}
\tag{18}
$$

Substituting the PDF of $|h_{\mathrm{XY}}|^2$ and γ_{SJR} in Lem. 1 into the above equation, using the identity $\int e^{ax}\mathrm{d}x = \frac{e^{ax}}{a}$ and after some steps, we obtain Eq. (17). This completes the proof of Thm. 2. □

It is noted that when the average Signal-to-Jam Ratio (SJR) is relatively low, $\frac{P_S}{P_J} \to 0$, the IP at E is lower-bounded by:

$$
\mathrm{IP}_E^{\mathrm{lwb}}(\gamma_{\mathrm{th}}) = \frac{1}{\lambda_{\mathrm{JE}}\lambda_{\mathrm{JR}}}\int_0^\infty \frac{e^{-\frac{y}{\lambda_{\mathrm{JR}}}-\frac{\gamma_{\mathrm{th}}}{\eta\beta\theta\lambda_{\mathrm{RE}}\bar{\gamma}_{\mathrm{JE}}}\frac{1}{y}}}{\frac{1}{\lambda_{\mathrm{JE}}}+\frac{\gamma_{\mathrm{th}}(1-\theta)}{\eta\beta\theta\lambda_{\mathrm{RE}}}\frac{1}{y}}\mathrm{d}y. \tag{19}
$$

2.5. No Friendly Jammer (NFJ)

When J is not presented to jam E, the e2e SNR at E becomes [27]:

$$
\gamma_E^{\mathtt{NFJ},\mathrm{e2e}} = P_S\max\left[|h_{\mathrm{SE}}|^2, \eta\beta|h_{\mathrm{SR}}|^2|h_{\mathrm{RE}}|^2\right]\sigma_E^{-2}. \tag{20}
$$

Note that the max$[\cdot,\cdot]$ operation is necessary because E also eavesdrops on information from S rather than just from R as in [27].

In addition, we can obtain the e2e SNR at D as follows:

$$
\gamma_D^{\mathtt{NFJ},\mathrm{e2e}} = P_S\min\left[\sigma_R^{-2}, \eta\beta\sigma_D^{-2}|h_{\mathrm{RD}}|^2\right]|h_{\mathrm{SR}}|^2. \tag{21}
$$

3. Results and Discussion

Monte Carlo simulations are provided in this section to assess the validity and reliability of the analysis in the previous sections. We observe a network area of 400 square meters, the noise power density is -174 dBm·Hz^{-1} with bandwidth being 10 MHz [26]. The carrier frequency is 3 GHz. We consider that D and E are in close proximity to R. J, on the other hand, is further away from R and E. By default, we consider $\eta = 1$ [8] and [12], $\gamma_{\mathrm{th}} = 0$ dB and $P_J = 1$ mW, respectively. Finally, define the average SJR as follows: SJR $\triangleq \frac{P_S}{P_J}$. The simulation results are conducted with the help of computer software, such as MATLAB. In the literature, the Monte Carlo (MC) method is used to obtain simulation results [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], and [26] by considering 10^6 independent realizations of h_{SR}, h_{JR}, h_{RD}, h_{JD}, h_{RE}, h_{SE}, and h_{JE}. The simulation result of OP is obtained by taking the average of the event γ_D^{e2e} in Eq. (7) is lower than γ_{th}, and that of IP is the average of the event γ_E^{e2e} in (8) is higher than γ_{th}.

In Fig. 2, we study the join impact of EH ratio, β, and the power control factor at J (i.e.,θ). The simulation results obtained by plugging Eq. (7) into

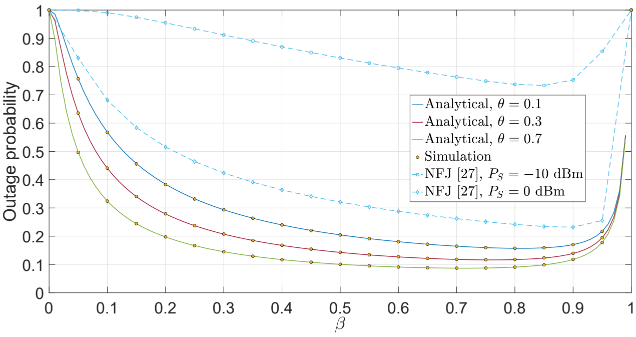

Fig. 2: OP versus β and θ, where SJR = 0 dB.

Eq. (9) match perfectly the analytical results defined in Eq. (10), which validates our analysis. In general, as θ increases, the amount of harvested power in Eq. (2) increases, which later increases the SNR at D as in Eq. (7). As a result, the e2e OP at D decreases, which improves the system transmission reliability. Plugging Eq. (21) into Eq. (9), we obtain the e2e OP, which shows that deploying J can result in higher outage at D.

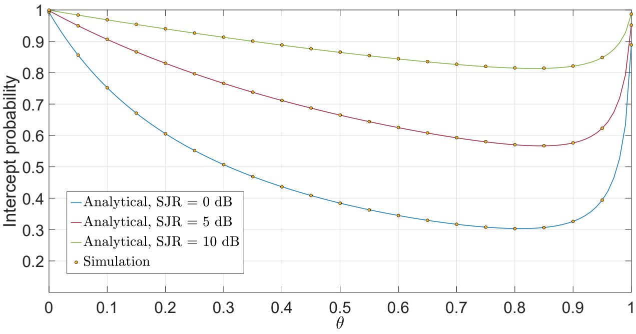

Fig. 3: IP versus θ and the average SJR (dB), where $\beta = 0.8$.

In Fig. 3, we study the IP at E versus the power control coefficient at J (i.e., θ) considering varying average SJR values. It is demonstrated that the simulation results obtained by substituting Eq. (8) into Eq. (14) accurately represent the analytical results in Eq. (17). With increasing θ, the IP decreases, improving system security until θ reaches an optimal value that yields the lowest value of IP. Beyond this optimal value, however, more power is harvested at R while E becomes less prone to jamming, leading to a decline in system IP. In addition, increasing the average SJR can also dramatically minimize the IP.

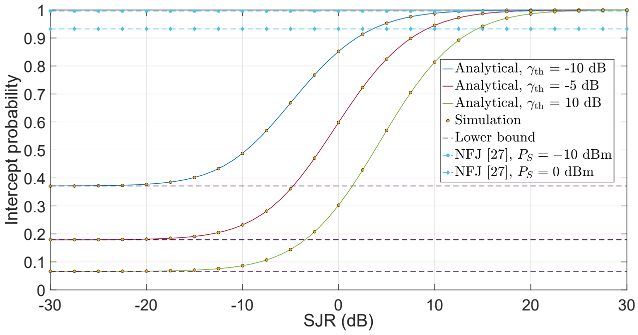

Fig. 4: IP versus the average SJR and γ_{th} (dB), where $\beta = \theta = 0.8$.

In Fig. 4, we study the IP at E versus the average SJR and the SNR threshold. The dashed curves are obtained from Eq. (19), which verifies its analysis. As γ_{th} increases, the IP decreases, which improves system secrecy. By plugging Eq. (20) into Eq. (14), we extract the e2e IP of NFJ, demonstrating that using a friendly jammer rather than NFJ in [27] considerably enhances system security. Although lowering P_S results in a lower IP without the Jammer, it dramatically increases the e2e OP, as is seen in Fig. 2.

4. Conclusion

In this research we investigated how the presence of a malicious eavesdropper and friendly jammer affects the outage and intercept probability in WPCNs. For this reason, we have developed a system model and power splitting protocol that will improve the reliability and security. Furthermore, we develop accurate analytical formulations for the outage probability and intercept probability. The asymptotic low Signal-to-Jam Ratio (SJR) in integral-form expressions revealed that the IP's lower bounds in the low SJR regime depend on the decoding threshold, the EH ratio, and the power control coefficient. Our findings suggest that by tuning the EH ratio and the power control coefficient, the OP and IP can be effectively sub-optimized.

Author Contributions

V.D.P. developed the system model. T.L.N. and T.T.P. performed the analytic calculations and performed the numerical simulations. All authors contributed to the final version of the manuscript. V.V.N. and V.D.P. supervised the project.

References

[1] WILLIAMS, A. J., M. F. TORQUATO, I. M. CAMERON, A. A. FAHMY and J. SIENZ. Survey of Energy Harvesting Technologies for Wireless Sensor Networks. *IEEE Access*. 2021, vol. 9, iss. 1, pp. 77493–77510. ISSN 2169-3536. DOI: 10.1109/ACCESS.2021.3083697.

[2] MA, D., G. LAN, M. HASSAN, W. HU and S. K. DAS. Sensing, Computing, and Commu-

nications for Energy Harvesting IoTs: A Survey. *IEEE Communications Surveys & Tutorials*. 2020, vol. 22, iss. 2, pp. 1222–1250. ISSN 1553-877X. DOI: 10.1109/COMST.2019.2962526.

[3] NASIR, A. A., X. ZHOU, S. DURRANI and R. A. KENNEDY. Relaying Protocols for Wireless Energy Harvesting and Information Processing. *IEEE Transactions on Wireless Communications*. 2013, vol. 12, iss. 7, pp. 3622–3636. ISSN 1558-2248. DOI: 10.1109/TWC.2013.062413.122042.

[4] NGUYEN, T. N., T. H. Q. MINH, P. T. TRAN, M. VOZNAK, T. T. DUY, T.-L. NGUYEN and P. T. TIN. Performance enhancement for energy harvesting based two-way relay protocols in wireless ad-hoc networks with partial and full relay selection methods. *Ad Hoc Networks*. 2019, vol. 84, iss. 1, pp. 178–187. ISSN 1570-8713. DOI: 10.1016/j.adhoc.2018.10.005.

[5] YANG, Z., W. XU and M. SHIKH-BAHAEI. Energy Efficient UAV Communication With Energy Harvesting. *IEEE Transactions on Vehicular Technology*. 2020, vol. 69, iss. 2, pp. 1913–1927. ISSN 1939-9359. DOI: 10.1109/TVT.2019.2961993.

[6] TOAN, H. V., T. M. HOANG, T. T. DUY and L. T. DUNG. Outage Probability and Ergodic Capacity of a Two-User NOMA Relaying System with an Energy Harvesting Full-Duplex Relay and Its Interference at the Near User. *Sensors*. 2020, vol. 20, iss. 22, pp. 1–21. ISSN 1424-8220. DOI: 10.3390/s20226472.

[7] NGUYEN, T. N., T. H. Q. MINH, P. T. TRAN and M. VOZNAK. Adaptive Energy Harvesting Relaying Protocol for Two-Way Half-Duplex System Network over Rician Fading Channels. *Wireless Communications and Mobile Computing*. 2018, vol. 2018, iss. 1, pp. 1–10. ISSN 1530-8677. DOI: 10.1155/2018/7693016.

[8] IN, C., H.-M. KIM and W. CHOI. Achievable Rate-Energy Region in Two-Way Decode-and-Forward Energy Harvesting Relay Systems. *IEEE Transactions on Communications*. 2019, vol. 67, iss. 6, pp. 3923–3935. ISSN 1558-0857. DOI: 10.1109/TCOMM.2019.2901783.

[9] BACKES, M. and B. PFITZMANN. Relating symbolic and cryptographic secrecy. *IEEE Transactions on Dependable and Secure Computing*. 2005, vol. 2, iss. 2, pp. 109–123. ISSN 1941-0018. DOI: 10.1109/TDSC.2005.25.

[10] SHANNON, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal*. 1949, vol. 28, iss. 2, pp. 656–715. ISSN 0005-8580. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[11] OMRI, A. and M. O. HASNA. Average Secrecy Outage Rate and Average Secrecy Outage Duration of Wireless Communication Systems With Diversity Over Nakagami-m Fading Channels. *IEEE Transactions on Wireless Communications*. 2018, vol. 17, iss. 6, pp. 3822–3833. ISSN 1558-2248. DOI: 10.1109/TWC.2018.2816648.

[12] TASHMAN, D. H., W. HAMOUDA and J. M. MOUALEU. On Securing Cognitive Radio Networks-Enabled SWIPT Over Cascaded κ-μ Fading Channels With Multiple Eavesdroppers. *IEEE Transactions on Vehicular Technology*. 2022, vol. 71, iss. 1, pp. 478–488. ISSN 1939-9359. DOI: 10.1109/TVT.2021.3127321.

[13] MURATKAR, T. S., A. BHURANE, P. K. SHARMA and A. KOTHARI. Physical Layer Security Analysis in Ambient Backscatter Communication With Node Mobility and Imperfect Channel Estimation. *IEEE Communications Letters*. 2022, vol. 26, iss. 1, pp. 27–30. ISSN 1558-2558. DOI: 10.1109/LCOMM.2021.3123893.

[14] TANG, J., G. CHEN and J. P. COON. Secrecy Performance Analysis of Wireless Communications in the Presence of UAV Jammer and Randomly Located UAV Eavesdroppers. *IEEE Transactions on Information Forensics and Security*. 2019, vol. 14, iss. 11, pp. 3026–3041. ISSN 1556-6021. DOI: 10.1109/TIFS.2019.2912074.

[15] SANCHEZ, J. D. V., D. P. M. OSORIO, F. J. LOPEZ-MARTINEZ, M. C. P. PAREDES and L. F. URQUIZA-AGUIAR. Information-Theoretic Security of MIMO Networks Under κ-μ Shadowed Fading Channels. *IEEE Transactions on Vehicular Technology*. 2021, vol. 70, iss. 7, pp. 6302–6318. ISSN 1939-9359. DOI: 10.1109/TVT.2021.3086026.

[16] THAKUR, A., A. KUMAR, N. GUPTA and P. CHATTERJEE. Secrecy Analysis of Reconfigurable Underlay Cognitive Radio Networks With SWIPT and Imperfect CSI. *IEEE Transactions on Network Science and Engineering*. 2022, vol. 9, iss. 1, pp. 89–97. ISSN 2327-4697. DOI: 10.1109/TNSE.2020.3040531.

[17] TIN, P. T., M. TRAN, T. N. NGUYEN and T.-L. NGUYEN. A new look at energy harvesting half-duplex DF power splitting protocol relay network over rician channel in case of maximizing capacity. *Indonesian Journal of Electrical Engineering and Computer Science*. 2019, vol. 13, iss. 1, pp. 249–257. ISSN 2502-4760. DOI: 10.11591/ijeecs.v13.i1.pp249-257.

[18] TIN, P. T., L. A. VU, T. N. NGUYEN and T.-L. NGUYEN. User selection protocol

in DF cooperative networks with hybrid TSR-PSR protocol based full-duplex energy harvesting over rayleigh fading channel: system performance analysis. *Indonesian Journal of Electrical Engineering and Computer Science*. 2019, vol. 13, iss. 2, pp. 534–542. ISSN 2502-4760. DOI: 10.11591/ijeecs.v13.i2.pp534-542.

[19] TIN, P. T., M. TRAN, T. N. NGUYEN and T.-L. NGUYEN. System performance analysis of hybrid time-power switching protocol of EH bidirectional relaying network in amplify-and-forward mode. *Indonesian Journal of Electrical Engineering and Computer Science*. 2019, vol. 14, iss. 1, pp. 118–126. ISSN 2502-4760. DOI: 10.11591/ijeecs.v14.i1.pp118-126.

[20] 3GPP. *3GPP-TR-36.814 V9.0.0. Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects.* Release 9. 2010.

[21] BJORNSON, E., O. OZDOGAN and E. G. LARSSON. Intelligent Reflecting Surface Versus Decode-and-Forward: How Large Surfaces are Needed to Beat Relaying? *IEEE Wireless Communications Letters*. 2020, vol. 9, iss. 2, pp. 244–248. ISSN 2162-2345. DOI: 10.1109/LWC.2019.2950624.

[22] RAPPAPORT, T. S., Y. XING, G. R. MACCARTNEY, A. F. MOLISCH, E. MELLIOS and J. ZHANG. Overview of Millimeter Wave Communications for Fifth-Generation (5G) Wireless Networks—With a Focus on Propagation Models. *IEEE Transactions on Antennas and Propagation*. 2017, vol. 65, iss. 12, pp. 6213–6230. ISSN 1558-2221. DOI: 10.1109/TAP.2017.2734243.

[23] PHU, T. T., D.-V. PHAN, D.-H. HA, T. N. NGUYEN, M. TRAN and M. VOZNAK. Non-linear energy harvesting based power splitting relaying in full-duplex AF and DF relaying networks: system performance analysis. *Proceedings of the Estonian Academy of Sciences*. 2020, vol. 69, iss. 4, pp. 368–381. ISSN 1736-7530. DOI: 10.3176/proc.2020.4.06.

[24] CHAUDHRY, M. A. and S. M. ZUBAIR. Generalized incomplete gamma functions with applications. *Journal of Computational and Applied Mathematics*. 1994, vol. 55, iss. 1, pp. 99–123. ISSN 1879-1778. DOI: 10.1016/0377-0427(94)90187-2.

[25] EL-MALEK, A. H. A., A. M. SALHAB, S. A. ZUMMO and M.-S. ALOUINI. Security-Reliability Trade-Off Analysis for Multiuser SIMO Mixed RF/FSO Relay Networks With Opportunistic User Scheduling. *IEEE Transactions on Wireless Communications*. 2016, vol. 15, iss. 9, pp. 5904–5918. ISSN 1558-2248. DOI: 10.1109/TWC.2016.2572681.

[26] DO, T. N., G. KADDOUM, T. L. NGUYEN, D. B. DA COSTA and Z. J. HAAS. Multi-RIS-Aided Wireless Systems: Statistical Characterization and Performance Analysis. *IEEE Transactions on Communications*. 2021, vol. 69, iss. 12, pp. 8641–8658. ISSN 1558-0857. DOI: 10.1109/TCOMM.2021.3117599.

[27] NGUYEN, A.-N., V. N. VO, C. SO-IN, D.-B. HA, S. SANGUANPONG and Z. A. BAIG. On Secure Wireless Sensor Networks With Cooperative Energy Harvesting Relaying. *IEEE Access*. 2019, vol. 7, iss. 1, pp. 139212–139225. ISSN 2169-3536. DOI: 10.1109/ACCESS.2019.2941915.

About Authors

Van Duc PHAN was born in 1975 in Long An province, Vietnam. He received his M.Sc. degree from Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam and Ph.D. degree from Da-Yeh University, Taiwan, in 2016. Currently, his research interests are in sliding mode control, non-linear systems, flywheel store energy systems, optimization algorithms, simultaneous wireless information and power transfer, visible light communication, physical layer security, and cognitive radio.

Thanh Luan NGUYEN (corresponding author) was born in Phu Yen, Vietnam, in 1994. He received the B.Sc. degree (Valedictorian) from the Ho Chi Minh City University of Technology and Education, Vietnam, in 2016. He is currently a Research Assistant with the Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH). He has authored and co-authored over 10 ISI-Indexed journals with over 200 citations. His research interests include Non-Orthogonal Multiple Access (NOMA), energy harvesting, stochastic geometry, generalized fading channels, and other emerging wireless technologies.

Tran Tin PHU was born in Khanh Hoa, Vietnam, in 1979. He received his Bachelor's degree (2002) and Master's degree (2008) from Ho Chi Minh City University of Science. He is currently a lecturer at the Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Vietnam. In 2019, he received his Ph.D. degree from the University of Ostrava, Czech Republic. His major research interests are wireless communication in the 5th generation mobile networks, energy harvesting, performance of cognitive radio, physical layer security and NOMA.

Van Vinh NGUYEN was born in Binh Dinh, Vietnam, in 1984. He received the B.E. degree in Computer Science from Nha Trang University, Vietnam, in 2008. In 2015, he received a Master's degree in Computer Science from University of Transport and Communications, Vietnam. He is currently a lecturer at the Department of Information Assurance (IA), FPT University, Ho Chi Minh City, Vietnam. His research interests are wireless communication in the 5th generation mobile networks, networking, cybersecurity, physical layer security and NOMA.