

Research Article

Relay Selection-and-Jamming Scheme with Nonlinear Energy Harvesting

Triet Pham-Minh ¹, **Khuong Ho-Van** ^{2,3}, **Hoa Nguyen-Minh** ¹
and **Khanh Nghi-Vinh** ¹

¹Tra Vinh University, Vietnam

²Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam

³Vietnam National University Ho Chi Minh City, Linh Trung Ward, Thu Duc District, Ho Chi Minh City, Vietnam

Correspondence should be addressed to Khuong Ho-Van; hvkhuong@hcmut.edu.vn

Received 19 August 2021; Revised 15 September 2021; Accepted 25 September 2021; Published 11 October 2021

Academic Editor: Muhammad Asghar Khan

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

When direct source-destination communications are in outage, relay selection is a preferable solution to improve reliability for this communications. However, such a relay selection makes the eavesdropper better overhear source data through both source-relay and relay-destination communication hops, losing data security. To improve both reliability and security, this paper proposes a relay selection-and-jamming (RaJ) scheme to select one intermediate node as a conventional relay and another node as a jammer. To enhance energy efficiency, all intermediate nodes harvest radio frequency energy in source signals for their operations with nonlinear energy harvesting (NL-EH). The security and reliability of the RaJ scheme are assessed through suggested rigorous/asymptotic expressions and are significantly better than two benchmark schemes without neither jamming nor both relay selection and jamming. Additionally, they can be optimized with reasonable selection of specifications. Moreover, the NL property of the energy harvesters dramatically affects the reliability but negligibly degrades the security for the RaJ scheme. Furthermore, the linear EH (L-EH) is more reliable but less secure than the NL-EH.

1. Introduction

1.1. Background. Radio frequency energy harvesting (RF EH), which exploits available RF signals to power communication devices, can solve problems of energy efficiency, energy shortage, and green communications in modern wireless systems [1–4]. RF EH is efficiently implemented through power-splitting (PS) and time-switching (TS) protocols in which the former carries out EH and data decoding in the same duration while the latter performs them separately in different durations (i.e., the latter requires lower circuitry implementation than the former) [5]. For performance analysis, EH has been modelled as linear (L) [6] or NL [7]. The linear EH (L-EH) model represents the linear increase of the scavenged energy with the input RF power. Nonetheless, nonlinear (NL) behaviors of EH circuit elements (e.g., diodes and inductors)

induce the NL-EH model more realistic and precise than the L-EH one. As such, this paper is interested in the NL-EH model for practical-and-exact performance analysis.

When direct source-destination communications are in outage due to severe propagation conditions (strong path-loss, heavy shadowing, and deep fading), relay selection in which only one intermediate node among all available nodes between the source-destination pair is selected to satisfy a preset criterion is regarded as a technique that is efficient in improving communication reliability and reducing complexity as well as economical in bandwidth and power [8]. Nonetheless, such a relay selection offers the eavesdropper more chances to overhear source message through both source-relay and relay-destination communication hops instead of merely one hop in direct source-destination communications, threatening data security. To conceal

legitimate data, the jamming technique where jamming signals (or artificial noises) are purposively generated to impair solely the eavesdropper has been popularly exploited [9].

This paper assumes two intermediate nodes, which are self-powered by scavenging RF energy in source signals with the practical NL-EH, are willing to ameliorate both reliability and security for data transmission between the source-destination pair. The question is which node plays a role as a traditional relay to enhance communication reliability and as a jammer to protect secret data over both hops. Our solution, relay selection-and-jamming (RaJ) scheme, solves this question.

1.2. Previous Works. Our proposed RaJ scheme differs [7, 10–22] which investigated problems of security and/or reliability for the NL-EH (References which studied the L-EH with/without relaying (e.g., [5, 6, 9]) or the NL-EH without relaying (e.g., [23–35]) must not be surveyed because this paper considers simultaneously the NL-EH, relaying, and jamming.) with relaying. More specifically, [7, 10] analyzed the reliability of the pure relaying (namely, the nonrelay selection nonjamming (nRnJ)) scheme in terms of outage probability (OP). In the nRnJ scheme in [7, 10], the relay performs the amplify-and-forward (AF) operation on source signals with energy harvested by the TS protocol. Reconsidering the nRnJ scheme and the AF relay in [7, 10], the authors in [11, 12] analyzed and simulated the reliability in terms of bit error rate and throughput, respectively. Additionally, both [11, 12] utilized the PS protocol for scavenging energy in source signals. Secrecy performance quantified by secrecy outage probability was simulated in [13], and the OP was analyzed in [14–20] for the same nRnJ scheme as [7]. Notwithstanding, all the works in [13–20] investigated the decode-and-forward (DF) relay, which is also a research object of this paper. As compared to the AF relay, the DF relay is advantageous in preventing noise enhancement, probably improving the overall system performance. In [21], the throughput was simulated for the nonrelay selection-and-jamming (nRaJ) scheme where one relay capable of EH is appointed as a conventional relay and another user is dedicated as an energy supplier as well as a jammer. Instead of dedicating an intermediate node as a jammer in [21], the authors in [22] availed the destination as a jammer. Further, [22] considered the AF relay and the energy harvesting based on the PS protocol. However, the performance analysis on the ergodic secrecy capacity and the total harvested energy was not included in [22].

1.3. Contributions. Beside proposing the RaJ scheme with the NL-EH, this paper suggests the rigorous/asymptotic formulas of the OP and the intercept probability (IP) to quickly assess both reliability and security. These expressions are then simplified to obtain the OP/IP of the nRnJ and RnJ (relay selection nonjamming) schemes for performance comparison and highlighting the efficacy of simultaneous relay selection and jamming. Moreover, the OP/IP of the RaJ scheme with the L-EH is derived. Monte-Carlo simulations validate these analyses and shed insights into the reliability/security of the considered schemes and the feature of the NL-EH in comparison to the L-EH.

bility/security of the considered schemes and the feature of the NL-EH in comparison to the L-EH.

1.4. Structure. The remainder of this paper is structured as follows. Part 2 describes the investigated system. Next, part 3 provides detailed derivations of reliability and security of the proposed RaJ scheme. Then, two (nRnJ and RnJ) benchmark schemes are discussed in part 4. Subsequently, some useful remarks are withdrawn in part 5, especially the remark on the L-EH. Finally, part 6 presents simulated/theoretical results, and part 7 closes the paper.

2. System Description

Figure 1 sketches the considered RaJ scheme where the source S fails to convey secret messages directly to the destination D owing to bad propagation conditions (e.g., severe fading and strong shadowing). Therefore, two intermediate nodes, R_0 and R_1 , are exploited with different roles as a traditional relay R to heal $S \rightarrow D$ communications and as a jammer J to protect secret data against the eavesdropper E . To improve energy efficiency, R_0 and R_1 scavenge RF energy in source signals through the TS protocol and utilize scavenged energy for relaying and jamming operations. Accordingly, secret data reaches D in three stages with an entire duration of T .

In stage I with (Stage I is just for energy harvesting. Consequently, S transmits an arbitrary signal, which carries RF energy, not necessarily the secret information or a deterministic signal.) a duration of αT , the nonlinear energy harvester of R_i , $i = \{0, 1\}$, generates the power [7]:

$$P_{r_i} = \begin{cases} A_i P_s g_{sr_i} & , P_s g_{sr_i} \leq \zeta_{th}, \\ A_i \zeta_{th} & , P_s g_{sr_i} > \zeta_{th}, \end{cases} \quad (1)$$

where $A_i = 2\vartheta_i\alpha/(1-\alpha)$; ϑ_i is energy converting efficiency; α is a time fraction; P_s is the transmission power of S ; ζ_{th} is the saturation threshold; $g_{sr_i} = |h_{sr_i}|^2$ is the $S \rightarrow R_i$ channel gain. Flat block Rayleigh fading channels are considered, and hence, h_{sr_i} is modelled ($h_{xy} \sim \mathcal{CN}(0, \lambda_{xy})$) notates a zero-mean λ_{xy} -variance complex Gaussian random variable. Therefore, $g_{xy} = |h_{xy}|^2$ obeys exponential distribution with mean λ_{xy} , shortly denoted as $g_{xy} \sim \mathcal{E}(\lambda_{xy})$, resulting in its cumulative distribution function (CDF) and the probability density function (PDF) as $F_{g_{xy}}(w) = 1 - e^{-w/\lambda_{xy}}$ and $f_{g_{xy}}(w) = e^{-w/\lambda_{xy}}/\lambda_{xy}$, respectively, where $w \geq 0$.) as $h_{sr_i} \sim \mathcal{CN}(0, \lambda_{sr_i})$ and is unchanged during T but changes independently in the next T . To guarantee S 's messages to be restored correctly at the intermediate nodes with the highest possibility, ultimately limiting error propagation as much as possible, R_i and R_j with $j = 1 - i$ are selected as the conventional relay and the jammer, respectively, if $g_{sr_i} > g_{sr_j}$ (i.e., the $S - R_i$ channel is better than the $S \rightarrow R_j$ channel).

Inserting (10) into (12), one obtains

$$\begin{aligned} I^{\text{Raj}} &= \mathbb{P}\{\max(\Omega_{se}, \Omega_{r_i e}) \geq \bar{\Omega}\} \\ &= 1 - \mathbb{P}\{\max(\Omega_{se}, \Omega_{r_i e}) < \bar{\Omega}\} \stackrel{(a)}{=} 1 \\ &\quad - \underbrace{\sum_{i=0}^1 \mathbb{P}\{\Omega_{se} < \bar{\Omega}, \Omega_{r_i e} < \bar{\Omega}, g_{sr_i} > g_{sr_j}\}}_{\bar{I}}, \end{aligned} \quad (13)$$

where $\stackrel{(a)}{=}$ follows the total probability law and the event $\{g_{sr_i} > g_{sr_j}\}$ means R_i as a conventional relay while R_j as a jammer.

Let $X = g_{sr_i}$, $Y = g_{sr_j}$, and $Z = P_{r_i} g_{r_i e} + \sigma^2$. Then, plugging (5) and (8) into \bar{I} in (13) results in

$$\bar{I} = \mathbb{E}_{X,Y} \left\{ \underbrace{\mathbb{P}\{P_s g_{se} < \bar{\Omega} Z, P_{r_i} g_{r_i e} < \bar{\Omega} Z\}}_{\bar{I}} \middle| X > Y \right\}, \quad (14)$$

where $\mathbb{E}\{\cdot\}$ is the expectation operator.

\bar{I} in (14) is expressed in closed-form as

$$\begin{aligned} \bar{I} &= \mathbb{E}_Z \left\{ F_{g_{se}} \left(\frac{\bar{\Omega} Z}{P_s} \right) F_{g_{r_i e}} \left(\frac{\bar{\Omega} Z}{P_{r_i}} \right) \right\} \\ &= \int_0^\infty \left(1 - e^{-\bar{\Omega} (P_{r_i} x + \sigma^2) / P_s \lambda_{se}} \right) \left(1 - e^{-\bar{\Omega} (P_{r_i} x + \sigma^2) / P_{r_i} \lambda_{r_i e}} \right) \frac{e^{-x/\lambda_{r_j e}}}{\lambda_{r_j e}} dx \\ &= 1 - \frac{e^{-\bar{\Omega} \sigma^2 / P_s \lambda_{se}}}{\bar{\Omega} P_{r_i} \lambda_{r_i e} / P_s \lambda_{se} + 1} - \frac{e^{-\bar{\Omega} \sigma^2 / P_{r_i} \lambda_{r_i e}}}{\bar{\Omega} P_{r_i} \lambda_{r_i e} / P_{r_i} \lambda_{r_i e} + 1} \\ &\quad + \frac{e^{-\bar{\Omega} \sigma^2 / P_s \lambda_{se} - \bar{\Omega} \sigma^2 / P_{r_i} \lambda_{r_i e}}}{\bar{\Omega} P_{r_i} \lambda_{r_i e} / P_s \lambda_{se} + \bar{\Omega} P_{r_i} \lambda_{r_i e} / P_{r_i} \lambda_{r_i e} + 1}. \end{aligned} \quad (15)$$

Based on (1), four combinations of (P_{r_i}, P_{r_j}) are considered when deriving (14) as follows.

Combination 1: $(P_{r_i}, P_{r_j}) = (A_i P_s g_{sr_i}, A_j P_s g_{sr_j})$

This combination holds when $X \leq \zeta_{\text{th}} / P_s$ and $Y \leq \zeta_{\text{th}} / P_s$. Incorporating these conditions with $X > Y$ in (14) results in existence region of (X, Y) as $Y \leq X$ and $X \leq \zeta_{\text{th}} / P_s$. By averaging \bar{I} in (15) over this region, one obtains \bar{I} for this combination as

$$\bar{I}_1 = \frac{1}{\lambda_{sr_i}} \int_0^{\zeta_{\text{th}} / P_s} I_1 e^{-x/\lambda_{sr_i}} dx, \quad (16)$$

where

$$I_1 = \frac{1}{\lambda_{sr_j}} \int_0^X \tilde{I} e^{-y/\lambda_{sr_j}} dy. \quad (17)$$

Invoking \tilde{I} in (15) with $(P_{r_i}, P_{r_j}) = (A_i P_s X, A_j P_s Y)$ and after some simplifications, the integral in (17) is solved as

$$\begin{aligned} I_1 &= 1 - e^{-X/\lambda_{sr_j}} - \frac{\lambda_{se} e^{-\bar{\Omega} \sigma^2 / P_s \lambda_{se}}}{\bar{\Omega} A_j \lambda_{r_j e} \lambda_{sr_j}} \\ &\quad \cdot \left[\Theta \left(X, \frac{1}{\lambda_{sr_j}}, \frac{\lambda_{se}}{\bar{\Omega} A_j \lambda_{r_j e}} \right) + \frac{A_i \lambda_{r_i e} X}{\lambda_{se}} e^{-\bar{\Omega} \sigma^2 / P_s \lambda_{se} - \frac{\bar{\Omega} \sigma^2}{A_i P_s \lambda_{r_i e} X}} \Theta \right. \\ &\quad \cdot \left(X, \frac{1}{\lambda_{sr_j}}, \frac{A_i \lambda_{r_i e} X}{\bar{\Omega} A_j \lambda_{r_j e}} \right) - \frac{e^{-\bar{\Omega} \sigma^2 / A_i P_s \lambda_{r_i e} X}}{1 + \lambda_{se} / A_i \lambda_{r_i e} X} \Theta \\ &\quad \left. \cdot \left(X, \frac{1}{\lambda_{sr_j}}, \frac{1}{\bar{\Omega} A_j \lambda_{r_j e} / \lambda_{se} + \bar{\Omega} A_j \lambda_{r_j e} / A_i \lambda_{r_i e} X} \right) \right], \end{aligned} \quad (18)$$

where $\Theta(a, b, c) = \int_0^a e^{-bx} / (x + c) dx = e^{bc} [Ei(-ab - bc) - Ei(-bc)]$ with $Ei\{\cdot\}$ is the exponential integral [46].

Combination 2: $(P_{r_i}, P_{r_j}) = (A_i P_s g_{sr_i}, A_j \zeta_{\text{th}})$

This combination holds when $X \leq \zeta_{\text{th}} / P_s$ and $Y > \zeta_{\text{th}} / P_s$. Incorporating these conditions with $X > Y$ in (14) results in empty region of (X, Y) . Therefore, one obtains \bar{I} for this combination as

$$\bar{I}_2 = 0. \quad (19)$$

Combination 3: $(P_{r_i}, P_{r_j}) = (A_i \zeta_{\text{th}}, A_j P_s g_{sr_j})$

This combination holds when $X > \zeta_{\text{th}} / P_s$ and $Y \leq \zeta_{\text{th}} / P_s$. Incorporating these conditions with $X > Y$ in (14) results in existence region of (X, Y) as $X > \zeta_{\text{th}} / P_s$ and $Y \leq \zeta_{\text{th}} / P_s$. By averaging \bar{I} in (15) over this region, one obtains \bar{I} for this combination as

$$\bar{I}_3 = \underbrace{\int_{\zeta_{\text{th}} / P_s}^\infty f_X(x) dx}_{\bar{I}_{31}} \underbrace{\int_0^{\zeta_{\text{th}} / P_s} \tilde{I} f_Y(y) dy}_{\bar{I}_{32}}, \quad (20)$$

where $\bar{I}_{31} = e^{-\zeta_{\text{th}} / P_s \lambda_{sr_i}}$ and \bar{I}_{32} is expressed in closed-form as follows after invoking \tilde{I} in (15), substituting (P_{r_i}, P_{r_j}) with $(A_i \zeta_{\text{th}}, A_j P_s Y)$ and executing simplifications:

$$\begin{aligned} \bar{I}_{32} &= 1 - e^{-\zeta_{\text{th}} / P_s \lambda_{sr_j}} - \frac{\lambda_{se} e^{-\bar{\Omega} \sigma^2 / P_s \lambda_{se}}}{\bar{\Omega} A_j \lambda_{sr_j} \lambda_{r_j e}} \left[\Theta \left(\frac{\zeta_{\text{th}}}{P_s}, \frac{1}{\lambda_{sr_j}}, \frac{\lambda_{se}}{\bar{\Omega} A_j \lambda_{r_j e}} \right) \right. \\ &\quad + \frac{A_i \lambda_{r_i e} \zeta_{\text{th}}}{\lambda_{se} P_s} e^{-\bar{\Omega} \sigma^2 / P_s \lambda_{se} - \bar{\Omega} \sigma^2 / A_i \lambda_{r_i e} \zeta_{\text{th}}} \Theta \\ &\quad \cdot \left(\frac{\zeta_{\text{th}}}{P_s}, \frac{1}{\lambda_{sr_j}}, \frac{A_i \lambda_{r_i e} \zeta_{\text{th}}}{\bar{\Omega} A_j \lambda_{r_j e} P_s} \right) - \frac{e^{-\bar{\Omega} \sigma^2 / A_i \lambda_{r_i e} \zeta_{\text{th}}}}{1 + \lambda_{se} P_s / A_i \lambda_{r_i e} \zeta_{\text{th}}} \Theta \\ &\quad \left. \cdot \left(\frac{\zeta_{\text{th}}}{P_s}, \frac{1}{\lambda_{sr_j}}, \frac{1}{\bar{\Omega} A_j \lambda_{r_j e} / \lambda_{se} + \bar{\Omega} A_j \lambda_{r_j e} P_s / A_i \lambda_{r_i e} \zeta_{\text{th}}} \right) \right]. \end{aligned} \quad (21)$$

Combination 4: $(P_{r_i}, P_{r_j}) = (A_i \zeta_{\text{th}}, A_j \zeta_{\text{th}})$

This combination holds when $X > \zeta_{\text{th}} / P_s$ and $Y > \zeta_{\text{th}} / P_s$. Incorporating these conditions with $X > Y$ in (14) results

in existence region of (X, Y) as $X > Y$ and $Y > \zeta_{\text{th}}/P_s$. By averaging \tilde{I} in (15) over this region, one obtains \bar{I} for this combination as

$$\bar{I}_4 = \int_{\zeta_{\text{th}}/P_s}^{\infty} \left[\int_y^{\infty} \tilde{I}_4 f_X(x) dx \right] f_Y(y) dy = \frac{e^{-\left(\lambda_{sr_i} + \lambda_{sr_j}\right) \zeta_{\text{th}} / \lambda_{sr_i} \lambda_{sr_j} P_s}}{1 + \lambda_{sr_j} / \lambda_{sr_i}} \tilde{I}_4, \quad (22)$$

where \tilde{I}_4 is \tilde{I} in (15) with $(P_{r_i}, P_{r_j}) = (A_i \zeta_{\text{th}}, A_j \zeta_{\text{th}})$, which is a constant.

Now it is ready to simplify (13) using the total probability law as

$$I^{\text{RaJ}} = 1 - \sum_{i=0}^1 \sum_{k=1}^4 \bar{I}_k = 1 - \sum_{i=0}^1 (\bar{I}_1 + \bar{I}_{31} \bar{I}_{32} + \bar{I}_4). \quad (23)$$

The asymptotic IP, $I_{\text{asym}}^{\text{RaJ}}$, is obtained when P_s approaches infinity. In the asymptotic region, only the combination 4 happens and hence,

$$I_{\text{asym}}^{\text{RaJ}} = 1 - \lim_{P_s \rightarrow \infty} \bar{I}_4 = 1, \quad (24)$$

which indicates a complete insecurity.

3.2. Outage Probability. The OP is addressed as the probability which E restores x_s unsuccessfully. Consequently, the OP is the probability that \mathbb{R} is greater than \mathbb{C}_d , namely,

$$O^{\text{RaJ}} = \mathbb{P}\{\mathbb{C}_d \leq \mathbb{R}\} = \mathbb{P}\{\Omega_d \leq \bar{\Omega}\}. \quad (25)$$

Given Ω_d in (9), one rewrites (25) as

$$\begin{aligned} O^{\text{RaJ}} &= \mathbb{P}\{\min(\Omega_{sr_i}, \Omega_{r_d}) < \bar{\Omega}\} \\ &= 1 - \mathbb{P}\{\min(\Omega_{sr_i}, \Omega_{r_d}) > \bar{\Omega}\} \\ &= 1 - \underbrace{\sum_{i=0}^1 \mathbb{P}\{\Omega_{sr_i} > \bar{\Omega}, \Omega_{r_d} > \bar{\Omega}, X > Y\}}_{\bar{O}}. \end{aligned} \quad (26)$$

Plugging (4) and (7) into \bar{O} in (26) results in

$$\begin{aligned} \bar{O} &= \mathbb{E}_{X,Y} \left\{ \mathbb{P} \left\{ g_{r_d} > \frac{\bar{\Omega} \sigma^2}{P_{r_i}} \right\} \middle| X > Y, X > \frac{\bar{\Omega} \sigma^2}{P_s} \right\} \\ &= \mathbb{E}_{X,Y} \left\{ e^{-\bar{\Omega} \sigma^2 / P_{r_i} \lambda_{r_d}} \middle| X > Y, X > \frac{\bar{\Omega} \sigma^2}{P_s} \right\}. \end{aligned} \quad (27)$$

Based on (1), two cases of P_{r_i} are considered when deriving (27) as follows.

Case 1. $P_{r_i} = A_i P_s X$

This case holds when $X \leq \zeta_{\text{th}}/P_s$. Incorporating this condition with $X > Y$ and $X > \bar{\Omega} \sigma^2 / P_s$ in (27) results in existence region of (X, Y) . More specifically, if $\bar{\Omega} \sigma^2 > \zeta_{\text{th}}$, then the

existence region is empty and hence, \bar{O} in (27) becomes $\bar{O}_1 = 0$. Otherwise, the existence region is $Y < X$ and $\bar{\Omega} \sigma^2 / P_s < X \leq \zeta_{\text{th}}/P_s$. By averaging $e^{-\bar{\Omega} \sigma^2 / A_i P_s \lambda_{r_d} X}$ in (27) over this region, one obtains \bar{O} for this case as

$$\begin{aligned} \bar{O}_1 &= \int_{\bar{\Omega} \sigma^2 / P_s}^{\zeta_{\text{th}}/P_s} e^{-\bar{\Omega} \sigma^2 / A_i P_s \lambda_{r_d} X} \left[\int_0^X f_Y(y) dy \right] f_X(x) dx \\ &= \frac{1}{\lambda_{sr_i}} \left[\Psi \left(\frac{\bar{\Omega} \sigma^2}{P_s}, \frac{\zeta_{\text{th}}}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega} \sigma^2}{A_i P_s \lambda_{r_d}} \right) \right. \\ &\quad \left. - \Psi \left(\frac{\bar{\Omega} \sigma^2}{P_s}, \frac{\zeta_{\text{th}}}{P_s}, \frac{1}{\lambda_{sr_i}} + \frac{1}{\lambda_{sr_j}}, \frac{\bar{\Omega} \sigma^2}{A_i P_s \lambda_{r_d}} \right) \right], \end{aligned} \quad (28)$$

where $\Psi(u, v, k, l)$ is given in (A.1) in Appendix A.

Case 2. $P_{r_i} = A_i \zeta_{\text{th}}$

This case holds when $X > \zeta_{\text{th}}/P_s$. Incorporating this condition with $X > Y$ and $X > \bar{\Omega} \sigma^2 / P_s$ in (27) results in existence region of (X, Y) as $Y < X$ and $X > B$ where $B = \max(\bar{\Omega} \sigma^2, \zeta_{\text{th}})/P_s$. By averaging $e^{-\bar{\Omega} \sigma^2 / A_i \lambda_{r_d} \zeta_{\text{th}}}$ in (27) over this region, one obtains \bar{O} for this case as

$$\begin{aligned} \bar{O}_2 &= e^{-\bar{\Omega} \sigma^2 / A_i \lambda_{r_d} \zeta_{\text{th}}} \int_B^{\infty} \left[\int_0^X f_Y(y) dy \right] f_X(x) dx \\ &= e^{-\bar{\Omega} \sigma^2 / A_i \lambda_{r_d} \zeta_{\text{th}} - B / \lambda_{sr_i}} \left(1 - \frac{\lambda_{sr_j} e^{-B / \lambda_{sr_j}}}{\lambda_{sr_i} + \lambda_{sr_j}} \right). \end{aligned} \quad (29)$$

Now it is ready to simplify (26) using the total probability law as

$$O^{\text{RaJ}} = 1 - \sum_{i=0}^1 (\bar{O}_1 + \bar{O}_2). \quad (30)$$

The asymptotic OP, $O_{\text{asym}}^{\text{RaJ}}$, is obtained when P_s approaches infinity. In the asymptotic region, only the case 2 happens and hence,

$$O_{\text{asym}}^{\text{RaJ}} = 1 - \sum_{i=0}^1 \lim_{P_s \rightarrow \infty} \bar{O}_2 = 1 - \sum_{i=0}^1 \frac{\lambda_{sr_i} e^{-\bar{\Omega} \sigma^2 / A_i \lambda_{r_d} \zeta_{\text{th}}}}{\lambda_{sr_i} + \lambda_{sr_j}}, \quad (31)$$

which indicates joint impact of three involved channels (λ_{sr_i} , λ_{sr_j} , and λ_{r_d}) on communication reliability.

3.3. Comment. Both I^{RaJ} and O^{RaJ} in (23) and (30) are expressed in novel-and-exact forms, facilitating in evaluating swiftly both security and reliability of the proposed RaJ scheme with the NL-EH without exhaustive simulations. In addition, they are leveraged to derive performance measures for benchmark schemes as well as linear energy harvesters.

4. Benchmark Schemes (RnJ and nRnJ)

4.1. The RnJ Scheme. To evaluate the efficacy of the jamming operation in our scheme, we compare it with the only relay selection scheme (e.g., [6, 47]) which lets R_j be idle in our scheme, namely, the RnJ scheme. The OP of the RnJ scheme is the same as that of ours (i.e., $O^{\text{RnJ}} = O^{\text{RaJ}}$) but the IP of the former is different from that of the latter. Following the derivation of O^{RaJ} in (30) with the note that $P_{r_j} = 0$, one obtains the IP of the RnJ scheme as

$$I^{\text{RnJ}} = 1 - \left(1 - e^{-\bar{\Omega}\sigma^2/P_s\lambda_{se}}\right) \sum_{i=0}^1 \cdot \left[\frac{\lambda_{sr_i}}{\lambda_{sr_i} + \lambda_{sr_j}} - \frac{1}{\lambda_{sr_i}} \Phi\left(\frac{\zeta_{th}}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i} e}\right) + \frac{1}{\lambda_{sr_i}} \Phi\left(\frac{\zeta_{th}}{P_s}, \frac{1}{\lambda_{sr_i}} + \frac{1}{\lambda_{sr_j}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i} e}\right) - e^{-\zeta_{th}/P_s\lambda_{sr_i} - \bar{\Omega}\sigma^2/A_i\lambda_{r_i}e\zeta_{th}} \left(1 - \frac{\lambda_{sr_j} e^{-\zeta_{th}/P_s\lambda_{sr_j}}}{\lambda_{sr_i} + \lambda_{sr_j}}\right) \right], \quad (32)$$

where $\Phi(v, k, l)$ is given in (B.1) in Appendix B.

The asymptotic OP of the RnJ scheme is

$$I_{\text{asym}}^{\text{RnJ}} = \lim_{P_s \rightarrow \infty} I^{\text{RnJ}} = 1, \quad (33)$$

which indicates a complete insecurity.

4.2. The nRnJ Scheme. To evaluate the efficacy of simultaneous relay selection and jamming in our scheme, we compare it with the nRnJ scheme (e.g., [7]) which lets R_i always relay the source data and R_j be idle in our scheme (i.e., pure relaying). Then, the IP of the nRnJ scheme is

$$I^{\text{nRnJ}} = 1 - \mathbb{P}\{\Omega_{se} < \bar{\Omega}, \Omega_{r_i e} < \bar{\Omega}\} = 1 - \mathbb{P}\{P_s g_{se} < \bar{\Omega}\sigma^2, P_{r_i} g_{r_i e} < \bar{\Omega}\sigma^2\}. \quad (34)$$

By considering two cases of P_{r_i} as for deriving O^{RaJ} in (30), one obtains the IP of the nRnJ scheme as

$$I^{\text{nRnJ}} = 1 - \left(1 - e^{-\bar{\Omega}\sigma^2/P_s\lambda_{se}}\right) \cdot \left[1 - e^{-\zeta_{th}/P_s\lambda_{sr_i} - \bar{\Omega}\sigma^2/A_i\lambda_{r_i}e\zeta_{th}} - \frac{1}{\lambda_{sr_i}} \Phi\left(\frac{\zeta_{th}}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i} e}\right)\right], \quad (35)$$

from which the asymptotic IP of the nRnJ scheme is given by

$$I_{\text{asym}}^{\text{nRnJ}} = \lim_{P_s \rightarrow \infty} I^{\text{nRnJ}} = 1, \quad (36)$$

which indicates a complete insecurity.

The OP of the nRnJ scheme is expressed to be

$$O^{\text{nRnJ}} = 1 - \mathbb{P}\{\Omega_{sr_i} > \bar{\Omega}, \Omega_{r_i d} > \bar{\Omega}\} = 1 - \mathbb{P}\{P_s g_{sr_i} > \bar{\Omega}\sigma^2, P_{r_i} g_{r_i d} > \bar{\Omega}\sigma^2\}. \quad (37)$$

By considering two cases of P_{r_i} as for deriving O^{RaJ} in (30), one obtains the OP of the nRnJ scheme as

$$O^{\text{nRnJ}} = \begin{cases} 1 - e^{-\bar{\Omega}\sigma^2/A_i\zeta_{th}\lambda_{r_i d} - B/\lambda_{sr_i}} - \frac{1}{\lambda_{sr_i}} \Psi\left(\frac{\bar{\Omega}\sigma^2}{P_s}, \frac{\zeta_{th}}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i} d}\right), & \bar{\Omega}\sigma^2 < \zeta_{th}, \\ 1 - e^{-\bar{\Omega}\sigma^2/A_i\zeta_{th}\lambda_{r_i d} - B/\lambda_{sr_i}}, & \bar{\Omega}\sigma^2 > \zeta_{th}, \end{cases} \quad (38)$$

from which the asymptotic OP of the nRnJ scheme is given by

$$O_{\text{asym}}^{\text{nRnJ}} = \lim_{P_s \rightarrow \infty} O^{\text{nRnJ}} = 1 - e^{-\bar{\Omega}\sigma^2/A_i\zeta_{th}\lambda_{r_i d}}, \quad (39)$$

which indicates the dependence of communication reliability on only the $R_i \rightarrow D$ channel.

5. Remarks

Remark 1. Three (RaJ, RnJ, and nRnJ) schemes are completely insecure as $P_s \rightarrow \infty$ (please refer to (24), (33), and (36)). This is reasonable since E receives strong signals from S as $P_s \rightarrow \infty$, making E decode successfully source data.

Remark 2. For the L-EH (i.e., ζ_{th} in (1) is infinite), the IP and the OP of the RaJ scheme are, respectively, addressed as

$$I_{\text{Lin}}^{\text{RaJ}} = \lim_{\zeta_{th} \rightarrow \infty} I^{\text{RaJ}} = 1 - \frac{1}{\lambda_{sr_i}} \sum_{i=0}^1 \int_0^{\infty} I_1 e^{-x/\lambda_{sr_i}} dx, \quad (40)$$

$$O_{\text{Lin}}^{\text{RaJ}} = \lim_{\zeta_{th} \rightarrow \infty} O^{\text{RaJ}} = 1 - \frac{1}{\lambda_{sr_i}} \sum_{i=0}^1 \left[\Lambda\left(\frac{\bar{\Omega}\sigma^2}{P_s}, \frac{1}{\lambda_{sr_i}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i} d}\right) - \Lambda\left(\frac{\bar{\Omega}\sigma^2}{P_s}, \frac{1}{\lambda_{sr_i}} + \frac{1}{\lambda_{sr_j}}, \frac{\bar{\Omega}\sigma^2}{A_i P_s \lambda_{r_i} d}\right) \right], \quad (41)$$

where $\Lambda(\cdot, \cdot, \cdot)$ is expressed in (A.4) in Appendix B.

6. Demonstrative Results

This part illustrates theoretical/simulated results to evaluate both reliability and security of the considered schemes via pivotal parameters. Monte-Carlo simulations produce simulated results while the derived expressions in parts 3–5 are calculated to achieve theoretical ones. Path-loss is accounted by modelling fading power of $x \rightarrow y$ channel as $\lambda_{xy} = d_{xy}^{-3}$ where d_{xy} is the $x \rightarrow y$ distance. For illustration purpose, users are located on a 2-dimension plane

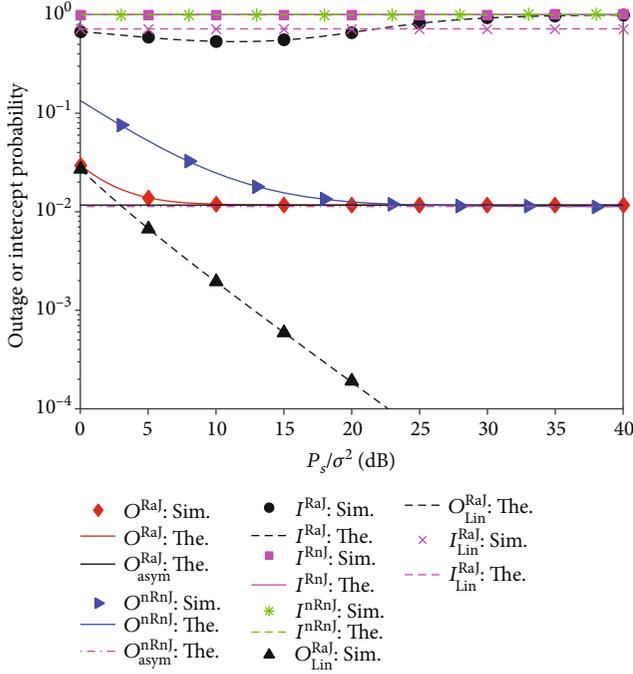


FIGURE 2: IP or OP versus P_s/σ^2 . “The.” and “Sim.” represent the theoretical and the simulated results, correspondingly.

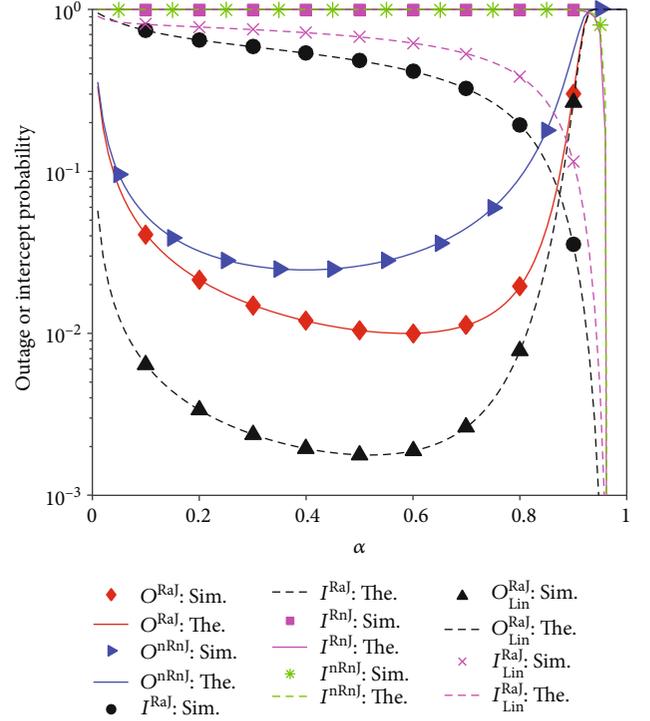


FIGURE 3: IP or OP versus α .

where S at $(0.0,0.0)$, D at $(1.0,0.0)$, E at $(0.5,0.3)$, R_0 at $(0.4877,0.0503)$, and R_1 at $(0.4763,-0.0490)$; $\vartheta_i = 0.9$, $i \in \{0, 1\}$; $\mathbb{R} = 0.3$ bits/s/Hz. Since both RaJ and RnJ schemes achieve the same OP (i.e., $O^{\text{RnJ}} = O^{\text{RaJ}}$), the following results only expose O^{RaJ} .

Results in Figures 2–4 show coincidences between theory and simulation and between asymptote and theory at large P_s , validating both rigorous and asymptotic analyses. Moreover, these figures demonstrate that without jamming, two (RnJ and nRnJ) benchmark schemes suffer a complete insecurity ($I^{\text{RnJ}} = I^{\text{nRnJ}} = 1$) since secret data is not protected in both stages (II and III) as in the proposed RaJ scheme which is drastically secured (i.e., $I^{\text{RaJ}} < 1$). Furthermore, with relay selection, both (RaJ and RnJ) schemes achieve significantly better reliability than the nRnJ scheme (i.e., $O^{\text{RaJ}} = O^{\text{RnJ}} < O^{\text{nRnJ}}$). Therefore, the proposed RaJ scheme, which exploits simultaneous jamming and relay selection, considerably outperforms the (RnJ and nRnJ) benchmark schemes in terms of security as well as reliability.

Figure 2 unveils the OP/IP via P_s/σ^2 for $\zeta_{\text{th}}/\sigma^2 = 10$ dB and $\alpha = 0.4$. It is observed that O^{RaJ} decreases with increasing P_s , which makes sense because of increasing the harvested energy. Nevertheless, I^{RaJ} is minimum (i.e., the security reaches the peak) at a certain value of P_s . This implies that increasing P_s does not always improve security because E also benefits from receiving strong signals from S and R_j , eventually wire-tapping more source data. Interestingly, the minimum I^{RaJ} happens at the asymptotic OP $O_{\text{asym}}^{\text{RaJ}}$, and hence, P_s can be optimized to obtain the best reliability and security performances. Compared to the NL-EH, the L-EH apparently

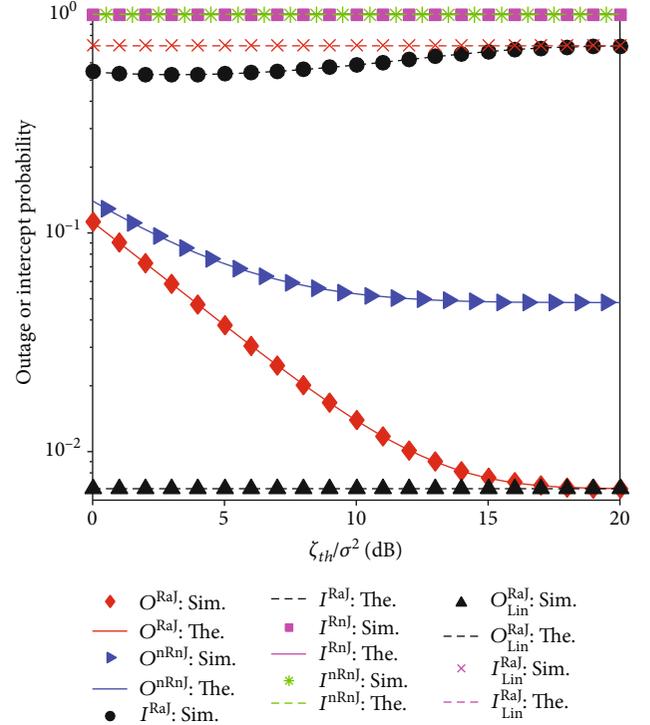


FIGURE 4: IP or OP versus $\zeta_{\text{th}}/\sigma^2$.

offers considerably better reliability ($O_{\text{Lin}}^{\text{RaJ}} < O^{\text{RaJ}}$). However, the security of the former (I^{RaJ}) fluctuates around that of the latter ($I_{\text{Lin}}^{\text{RaJ}}$) with increasing P_s .

Figure 3 plots the IP/OP versus α for $P_s/\sigma^2 = \zeta_{th}/\sigma^2 = 10$ dB. It is noted that α is proportional to the EH time but inversely proportional to the signal processing time (stages II and III). Accordingly, α should be optimally adopted to balance these times for optimum reliability. Figure 3 shows that the RaJ and nRnJ schemes reach the lowest OP at $\alpha = 0.6$ and $\alpha = 0.4$, respectively. Interestingly, the security of the proposed RaJ scheme is considerably enhanced (i.e., I^{RaJ} significantly decreases) with increasing α . Some reasons lead to this observation as follows. Firstly, increasing α reduces the channel capacity at E because of the factor $(1 - \alpha)/2$ before the logarithm in (11), causing the decrease of I^{RaJ} . Secondly, although increasing α helps R_i and R_j collect more energy, E suffers the increase of the jamming power from R_j , eventually reducing I^{RaJ} . Compared to the NL-EH, the L-EH is drastically more reliable ($O_{Lin}^{RaJ} < O^{RaJ}$) but less secure ($I_{Lin}^{RaJ} > I^{RaJ}$).

Figure 4 exposes the IP/OP versus ζ_{th}/σ^2 for $P_s/\sigma^2 = 5$ dB and $\alpha = 0.4$. The reliability-and-security trade-off of the proposed RaJ scheme is observed in this figure. Nonetheless, the reliability gain increases faster than the security loss with increasing the saturation threshold of the NL energy scavenger ζ_{th} , exposing the advantage of both relay selection and jamming in our scheme in ensuring high reliability with affordable security threat. Such a trade-off with increasing ζ_{th} is reasonable since the NL-EH operates in the linear mode with higher harvested energy more frequently in the range of large ζ_{th} . Indeed, the performances of the NL-EH, I^{RaJ} and O^{RaJ} , reach those of the L-EH, I_{Lin}^{RaJ} and O_{Lin}^{RaJ} , at large ζ_{th} .

7. Conclusions

The current paper recommended the relay selection-and-jamming scheme for radio frequency energy harvesting networks with the nonlinear energy harvester. Its security and reliability were also analyzed via the intercept and outage probabilities. Thanks to selecting the relay with the highest probability of decoding the source data and jamming the eavesdropper in both signal transmission stages, the proposed RaJ scheme achieved better reliability and security than the (RnJ and nRnJ) benchmark schemes without neither jamming nor both relay selection and jamming. Additionally, the best performance of the recommended scheme is achievable with choosing properly the source power and the time fraction, respectively. Moreover, the nonlinearity property of the energy harvesters significantly affects the reliability yet slightly degrades the security for the proposed scheme. Furthermore, the nonlinear energy harvester is less reliable yet more secure than the linear energy harvester.

Appendix

A. Derivation of $\Psi(u, v, k, l)$ in (28)

$\Psi(u, v, k, l)$ in (28) is

$$\Psi(u, v, k, l) = \int_u^v e^{-kx-l/x} dx = \Lambda(u, k, l) - \Lambda(v, k, l), \quad (\text{A.1})$$

where

$$\Lambda(c, k, l) = \int_c^\infty e^{-kx-l/x} dx. \quad (\text{A.2})$$

Invoking the series expansion for $e^{-l/x}$, one rewrites (A.2) as

$$\begin{aligned} \Lambda(c, k, l) &= \int_c^\infty e^{-kx} \left(\sum_{m=0}^{\infty} \frac{1}{m!} \left[-\frac{l}{x} \right]^m \right) dx \\ &= \sum_{m=0}^{\infty} \frac{(-l)^m}{m!} \int_c^\infty \frac{e^{-kx}}{x^m} dx \stackrel{y=kx}{=} \sum_{m=0}^{\infty} \frac{(-kl)^m}{m!k} \int_{kc}^\infty \frac{e^{-y}}{y^m} dy. \end{aligned} \quad (\text{A.3})$$

Using [46] (Equation (3.381.6)), the last integral in (A.3) is numerically evaluated as $(kc)^{-m/2} e^{-kc/2} W_{-m/2, (1-m)/2}(kc)$ where $W_{k,l}(z)$ is the Whittaker's function. Plugging this result into (A.3), one obtains

$$\Lambda(c, k, l) = \sum_{m=0}^{\infty} \frac{(-l)^m}{m!} k^{m/2-1} c^{-m/2} e^{-kc/2} W_{-m/2, (1-m)/2}(kc). \quad (\text{A.4})$$

By plugging (A.4) into (A.1), one represents $\Psi(u, v, k, l)$ in (28) in a precise closed form.

B. Derivation of $\Phi(v, k, l)$ in (32)

$\Phi(v, k, l)$ in (32) is

$$\Phi(v, k, l) = \int_0^v e^{-kz-l/z} dz = \int_0^\infty e^{-kz-l/z} dz - \underbrace{\int_v^\infty e^{-kz-l/z} dz}_{\Lambda(v, k, l)}, \quad (\text{B.1})$$

where $\Lambda(\cdot, \cdot, \cdot)$ is expressed in (A.4).

Availing [46] (Equation (3.471.9)), $\int_0^\infty e^{-kz-l/z} dz$ in (B.1) is solved as $2\sqrt{l/k} K_1(2\sqrt{kl})$ where $K_1(z)$ is the modified Bessel function of the second kind. Plugging this result into (B.1), one obtains

$$\Phi(v, k, l) = 2\sqrt{\frac{l}{k}} K_1(2\sqrt{kl}) - \Lambda(v, k, l). \quad (\text{B.2})$$

Data Availability

The authors declare that all data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study/work/research was fully funded by the Tra Vinh University under grant contract number 181/HD.HDKH&DT-DHTV. The other supports Khuong Ho-Van who would like to thank Ho Chi Minh City University of Technology (HCMUT), VNU-HCM for the support of time and facilities for this study.

References

- [1] T. N. Tran, T. P. Vo, P. Fazio, and M. Voznak, "SWIPT model adopting a PS framework to aid IoT networks inspired by the emerging cooperative NOMA technique," *IEEE Access*, vol. 9, pp. 61489–61512, 2021.
- [2] D. Xu and H. Zhu, "Sum-rate maximization of wireless powered primary users for cooperative CRNs: NOMA or TDMA at cognitive users?," *IEEE Transactions on Communications*, vol. 69, no. 7, pp. 4862–4876, 2021.
- [3] D. Dash, "Geometric algorithm for finding time-sensitive data gathering path in energy harvesting sensor networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.
- [4] Y. Xu, H. Xie, C. Liang, and F. R. Yu, "Robust secure energy efficiency optimization in SWIPT-aided heterogeneous networks with a non-linear energy harvesting model," *IEEE IoT Journal*, vol. 8, no. 19, pp. 14908–14919, 2021.
- [5] L. Ge, G. Chen, Y. Zhang, J. Tang, J. Wang, and J. A. Chambers, "Performance analysis for multihop cognitive radio networks with energy harvesting by using stochastic geometry," *IEEE IoT Journal*, vol. 7, no. 2, pp. 1154–1163, 2020.
- [6] K. Ho-van and T. Do-Dac, "Security enhancement for energy harvesting cognitive networks with relay selection," *Wireless Communications and Mobile Computing*, vol. 2020, 13 pages, 2020.
- [7] S. Solanki, P. K. Upadhyay, D. B. D. Costa, H. Ding, and J. M. Moualeu, "Performance analysis of piece-wise linear model of energy harvesting-based multiuser overlay spectrum sharing networks," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1820–1836, 2020.
- [8] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Journal on selected areas in communications*, vol. 24, no. 3, pp. 659–672, 2006.
- [9] D. Wang, F. Zhou, and V. C. M. Leung, "Primary privacy preserving with joint wireless power and information transfer for cognitive radio networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 683–693, 2020.
- [10] S. A. A. Kazmi and S. Coleri, "Optimization of full-duplex relaying system with non-linear energy harvester," *IEEE Access*, vol. 8, pp. 201566–201576, 2020.
- [11] M. Babaei, U. Aygolu, M. Basaran, and L. Durak-Ata, "BER performance of full-duplex cognitive radio network with non-linear energy harvesting," *IEEE Transactions on Green Communications and Networking*, vol. 4, no. 2, pp. 448–460, 2020.
- [12] A. Anwar, S. T. Shah, S. F. Hasan, and D. R. Shin, "SWIPT-based three-step multiplicative amplify-and-forward two-way relay networks with non-linear energy conversion model," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 152–157, China, 2018.
- [13] P. Maji, S. D. Roy, and S. Kundu, "Physical layer security with non-linear energy harvesting relay," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, India, 2019.
- [14] K. Agrawal, M. F. Flanagan, and S. Prakriya, "NOMA with battery-assisted energy harvesting full-duplex relay," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13952–13957, 2020.
- [15] A. Hakimi, M. Mohammadi, Z. Mobini, and Z. Ding, "Full-duplex non-orthogonal multiple access cooperative spectrum-sharing networks with non-linear energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 10925–10936, 2020.
- [16] P. Raut, P. K. Sharma, T. A. Tsiftsis, and Y. Zou, "Power-time splitting-based non-linear energy harvesting in FD short-packet communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9146–9151, 2020.
- [17] Y. Liu, Y. Ye, H. Ding, F. Gao, and H. Yang, "Outage performance analysis for SWIPT-based incremental cooperative NOMA networks with non-linear harvester," *IEEE Communications Letters*, vol. 24, no. 2, pp. 287–291, 2020.
- [18] L. Shi, W. Cheng, Y. Ye, H. Zhang, and R. Q. Hu, "Heterogeneous power-splitting based two-way DF relaying with non-linear energy harvesting," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, United Arab Emirates, 2018.
- [19] X. Xie, J. Chen, and Y. Fu, "Outage performance and QoS optimization in full-duplex system with non-linear energy harvesting model," *IEEE Access*, vol. 6, pp. 44281–44290, 2018.
- [20] Y. Liu, F. Gao, X. Deng, T. Wu, and X. Zhang, "Performance analysis for incremental DF relaying networks with non-linear energy harvesting," in *2020 IEEE 20th International Conference on Communication Technology (ICCT)*, pp. 354–360, China, 2020.
- [21] F. Wang and X. Zhang, "Secure resource allocation for polarization-based non-linear energy harvesting over 5G cooperative CRNs," *IEEE Wireless Communications Letters*, p. 1, 2020.
- [22] Y. Zhang, X. Q. Jiang, H. Hai, J. Hau, and K. Peng, "Generalized non-linear energy harvesting protocol for enhancing security of AF multi-antenna relaying systems," in *2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE)*, pp. 195–201, China, 2019.
- [23] D. Wang and S. Men, "Secure energy efficiency for NOMA based cognitive radio networks with nonlinear energy harvesting," *IEEE Access*, vol. 6, pp. 62707–62716, 2018.
- [24] L. Ni, X. da, H. Hu, M. Zhang, and K. Cumanan, "Outage constrained robust secrecy energy efficiency maximization for EH cognitive radio networks," *IEEE Wireless Communications Letters*, vol. 9, no. 3, pp. 363–366, 2020.
- [25] N. Shanin, L. Cottatellucci, and R. Schober, "Markov decision process based design of SWIPT systems: non-linear EH circuits, memory, and impedance mismatch," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 1259–1274, 2021.
- [26] S. Bayat, A. Khalili, and Z. Han, "Resource allocation for MC MISO-NOMA SWIPT-enabled HetNets with non-linear energy harvesting," *IEEE Access*, vol. 8, pp. 192270–192281, 2020.
- [27] D. Wang, F. Rezaei, and C. Tellambura, "Performance analysis and resource allocations for a WPCN with a new nonlinear energy harvester model," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1403–1424, 2020.

- [28] G. Ma, J. Xu, Y. F. Liu, and M. R. V. Moghadam, "Time-division energy beamforming for multiuser wireless power transfer with non-linear energy harvesting," *IEEE Wireless Communications Letters*, vol. 10, no. 1, pp. 53–57, 2021.
- [29] Z. Zhu, N. Wang, W. Hao, Z. Wang, and I. Lee, "Robust beamforming designs in secure MIMO SWIPT IoT networks with a non-linear channel model," *IEEE IoT Journal*, vol. 69, no. 2, pp. 1867–1878, 2020.
- [30] T. X. Vu, S. Chatzinotas, S. Gautam, E. Lagunas, and B. Ottersten, "Joint optimization for PS-based SWIPT multiuser systems with non-linear energy harvesting," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Seoul, Korea (South), 2020.
- [31] X. Liu, Y. Gao, M. Guo, and N. Sha, "Secrecy throughput optimization for the WPCNs with non-linear EH model," *IEEE Access*, vol. 7, pp. 59477–59490, 2019.
- [32] Y. Lu, K. Xiong, P. Fan, Z. Ding, Z. Zhong, and K. B. Letaief, "Global energy efficiency in secure MISO SWIPT systems with non-linear power-splitting EH model," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 216–232, 2019.
- [33] S. Gao, K. Xiong, R. Jiang, L. Zhou, and H. Tang, "Outage performance of wireless-powered SWIPT networks with non-linear EH model in Nakagami-m fading," in *2018 14th IEEE International Conference on Signal Processing (ICSP)*, pp. 668–671, China, 2018.
- [34] F. Zhou, Z. Chu, Y. Wu, N. Al-Dhahir, and P. Xiao, "Enhancing PHY security of MISO NOMA SWIPT systems with a practical non-linear EH model," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, USA, 2018.
- [35] E. Boshkovska, D. W. K. Ng, L. Dai, and R. Schober, "Power-efficient and secure WPCNs with hardware impairments and non-linear EH circuit," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2642–2657, 2018.
- [36] P. Chakraborty and S. Prakriya, "Secrecy performance of an idle receiver assisted underlay secondary network," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9555–9560, 2017.
- [37] R. Su, Y. Wang, and R. Sun, "Secure cooperative transmission in cognitive AF relay systems with destination-aided jamming and energy harvesting," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–5, Turkey, 2019.
- [38] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1319–1329, 2017.
- [39] X. Hu, X. Zhang, H. Huang, and Y. Li, "Secure transmission via jamming in cognitive radio networks with position spatially distributed eavesdroppers," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6, Spain, 2016.
- [40] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO cooperative cognitive radio networks," in *2015 IEEE International Conference on Communications (ICC)*, pp. 7609–7614, UK, 2015.
- [41] Zhihui Shu, Yi Qian, and Song Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.
- [42] Y. Wu, X. Chen, and X. Chen, "Secure beamforming for cognitive radio networks with artificial noise," in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–5, China, 2015.
- [43] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and artificial noise design for cognitive MIMOME wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6753–6758, 2016.
- [44] V. D. Nguyen, T. Q. Duong, O. A. Dobre, and O. S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2609–2623, 2016.
- [45] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*, John Wiley & Sons, Inc., Hoboken, New Jersey, Second edition, 2005.
- [46] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press, San Diego, CA, USA, 6th edition, 2000.
- [47] J. Ye, Z. Liu, H. Zhao, G. Pan, Q. Ni, and M. S. Alouini, "Relay selections for cooperative underlay CR systems with energy harvesting," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 358–369, 2019.