Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2368201, 15 pages
https://doi.org/10.1155/2021/2368201

Research Article

Simultaneous Jamming-and-Transmitting Scheme for Spectrum-Sharing Relaying Networks with Nonlinear Energy Scavenging

Triet Pham-Minh,[1] **Khuong Ho-Van**,[2,3] **and Khanh Nghi-Vinh**[1]

[1]*Tra Vinh University, Vietnam*
[2]*Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam*
[3]*Vietnam 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 20 June 2021; Revised 22 September 2021; Accepted 6 October 2021; Published 19 October 2021

Academic Editor: Changqing Luo

This paper recommends a simultaneous jamming-and-transmitting scheme for spectrum-sharing relaying networks with nonlinear energy scavenging. More specifically, spectrum-sharing relaying networks include a secondary source which expects to communicate with a secondary destination but impossible due to communication blockage between them, a secondary relay which helps the source overcome this blockage, a primary receiver, and a wiretapper which steals secret messages from both source and relay. To motivate assistance, the relay scavenges radio frequency energy from the source with practical nonlinear energy scavenger (NL-ES) instead of linear energy scavenger (L-ES) as in previous publications. Additionally, both source and relay perform simultaneous jamming-and-transmitting to secure their communication. The intercept and outage probabilities of the recommended scheme are evaluated through exact closed-form formulas, which are corroborated by Monte-Carlo simulations. Illustrative results show that the proposed scheme offers the reliability-security trade-off yet suffers error floor at large maximum transmit/interference power. Moreover, its performance can be optimally set with appropriate system parameters. Notably, the proposed scheme can guarantee absolute security with proper parameter setting. Furthermore, the NL-ES is practical but performs significantly worse than the L-ES.

1. Introduction

1.1. Background. Energy in radio frequency (RF) signals can be scavenged to power wireless users for improving energy efficiency, solving energy shortage, and offering green communication in advanced communication networks [1–4]. Two typical paradigms, expressly power-splitting (PS) and time-switching (TS), efficiently implement RF energy scavenging (ES) where the former performs ES and data restoring at the same time while the latter carries out these operations independently in distinct times [5]. As a result, the former demands lower circuitry implementation than the latter. Energy scavenger can be classified as linear (L) [6] or nonlinear (NL) [7]. Practically, circuit components of the energy scavenger include diodes and inductors. These NL components explicitly mean the NL-ES paradigm is more practical than the L-ES one. Therefore, this paper focuses on a class of NL energy scavengers, namely, piecewise linearity in [7], to assess performance of RF ES systems.

Spectrum sharing (the literature names the spectrum-sharing operation mode differently as the underlay one; moreover, cognitive radios can operate in other two modes (interweave and overlay) which are beyond our scope) is the typical operation mode of cognitive radios aiming at improving significantly spectrum utilization efficiency [8]. This mode restricts transmit power of cognitive radios by the tolerable interference power at the primary users and their maximum transmit power [9, 10]. These power constraints limit their transmit power, shortening their coverage range and causing discontinuity in direct transmission between cognitive radios. Also, unfavorable propagation conditions (e.g., severe fading and heavy channel loss) are other causes to discontinuity in direct transmission. Consequently, a secondary relay, which can amplify-and-forward

(AF) or decode-and-forward (DF) secondary source signals to a secondary destination, should be utilized to ensure continuity in direct transmission. Nevertheless, the relay, which participates in relaying source signals as a volunteer, may be staggering to spend its personal energy for this operation. To raise the motivation for the relay, the energy scavenged from the source by recent advanced energy scavenging technologies should power its operation [11–13]. As such, the relay not only extends the coverage range of the secondary source but also keeps direct transmission continuous without sacrificing its personal energy. Nonetheless, the energy harvested by the relay is typically limited, and thus, the question is if the relay can assist direct transmission reliably as well as secure its transmission to the secondary destination against the overhearing of wiretappers. Another concern is that wiretappers also overhear communication through the source-relay hop and hence how to secure this hop. The current paper is aimed at solving these concerns. Before presenting the related works, it should be recalled that the jamming method, which produces intentionally jamming signals to interrupt solely the wiretappers, is popular and efficient in securing information transmission [14].

1.2. Related Works. Direct communication with the NL-ES in both cognitive and noncognitive radio networks has been extensively considered in [15–28]. In addition, a variety of publications investigated relaying networks with the NL-ES but for noncognitive users (e.g., [14, 29–36]) or non-spectrum-sharing users (e.g., overlay users [7, 37–40]). Nonetheless, few works studied performance analysis for spectrum-sharing relaying networks with nonlinear energy scavenging (SSRNwNLES). Specifically, Ref. [41] considered the basic system model for SSRNwNLES where a secondary DF relay aids direct secondary source-destination transmission. Secondary communication interferes signal reception of a primary receiver. Nevertheless, Ref. [41] assumed an eavesdropper wiretaps legitimate information over solely the second hop (from the relay to the destination). Moreover, Ref. [41] only simulated the secrecy outage probability under the maximum transmit power constraint (MTPC) and the interference power restriction (IPR) without proposing any technique to protect legitimate information over both (source-relay and relay-destination) hops. In [42], the authors reconsidered the system model in [41] for maximizing the throughput but without the eavesdropper. The authors in [43] considered SSRNwNLES with several secondary relays and primary users. Although [43] presented the bit error rate analysis, the spectrum-sharing mode imposes implicit constraints on the operations of the cognitive radios without explicitly investigating the IPR and the MTPC, simplifying significantly the analysis. Moreover, Ref. [43] did not study the security aspect of the considered system model. In [44], the authors studied SSRNwNLES with several secondary relays and destinations. However, only relays are constrained by both maximum transmit and interference powers while the source is imposed by the interference power restriction. Furthermore, Refs. [42, 44] were not interested in performance analysis and security issue.

1.3. Contributions. The above literature survey indicates that concurrent considerations of performance analysis and security issue in SSRNwNLES have been still an open topic so far. This paper is the first attempt to research that topic with the following contributions:

(i) Propose a simultaneous jamming-and-transmitting scheme to secure message transmission over both source-relay and relay-destination hops in the system model in [41] by asking both the relay and the source to broadcast simultaneously legitimate and jamming signals. Apparently, the proposed scheme solved the security issue left by previous works [41–44]

(ii) Recommend the relay to scavenge energy in source signals with the nonlinear energy scavenger to increase its motivation in relaying source messages

(iii) Propose precise formulas of intercept probability (IP) and outage probability (OP) for evaluating rapidly both security and reliability of the recommended scheme without invoking exhaustive Monte-Carlo simulations. The derivation of the OP and the IP accounts for both the MTPC and the IPR. These analyses were obviously ignored in [41–44]

(iv) Optimize crucial system parameters using the recommended IP/OP expressions

(v) Prove the absolute security achievable with proper system parameter setting

(vi) Illustrate multifarious results of the reliability and security performances to make helpful conclusions; for instance, the unchanged IP/OP as either the MTPC or the IPR is forsaken, considerable security/reliability improvement as setting properly system parameters, the reliability-security trade-off, and the inferiority of the NL-ES to the L-ES

1.4. Organization. The next section describes the recommended simultaneous jamming-and-transmitting scheme for SSRNwNLES. Then, Section 3 details the derivation of the accurate closed-form IP/OP expressions. Next, Section 4 illustrates analytical/simulated results on the recommended scheme. Eventually, Section 5 ends the paper with insightful comments.

2. Simultaneous Jamming-and-Transmitting Scheme

Figure 1 sketches the system model under consideration where the secondary destination D expects to get signals from the secondary source S. The eavesdropper E tries to extract the source message. Because of bad propagation conditions such as dire fading and severe channel loss, direct $S \longrightarrow D$ transmission may be discontinuous. Therefore, the DF relay R between S and D should be utilized to relay S's signal to D for keeping the $S \longrightarrow D$ transmission continuous.

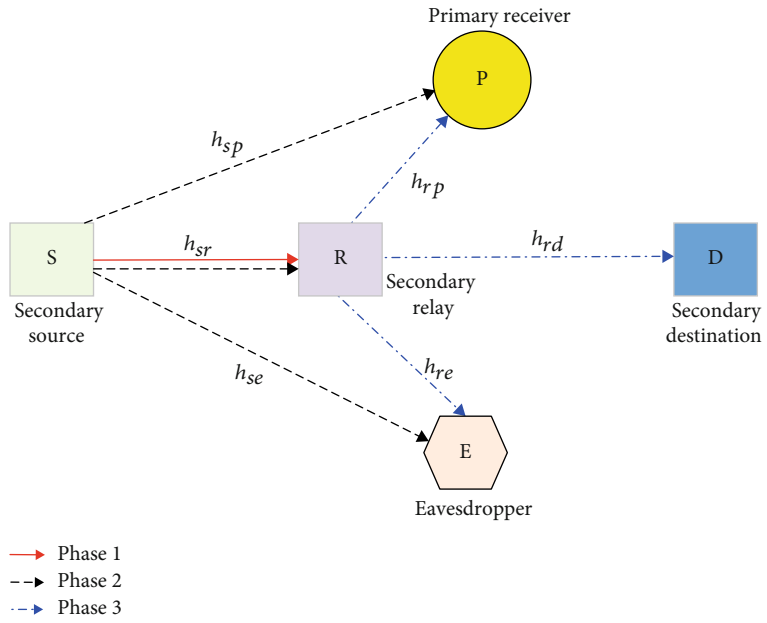

Figure 1: System model.

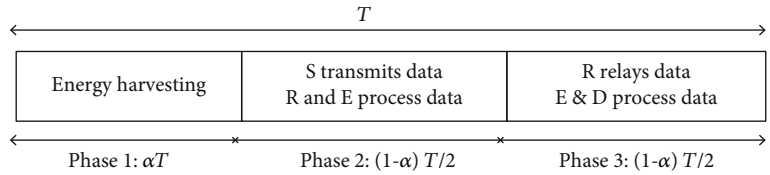

Figure 2: Phase times.

To reward for R's assistance, R only relays the source message with the energy scavenged in the source signals. Accordingly, secret messages reach D in three phases with a total duration of T as shown in Figure 2. Also, due to the spectrum-sharing operation mode, cognitive radios (S and R) interfere (in the spectrum-sharing operation mode, primary users interfere cognitive radios; nonetheless, such an interference is forsaken under scenarios that it follows the Gaussian distribution or the distance between the primary user and the cognitive radio is adequately large; forsaking such an interference is admitted extensively in the literature of the spectrum-sharing networks (please refer to [45–47])) the primary receiver P.

Figure 1 notates channel gain h_{bc}, $b \in \{S, R\}$, $c \in \{E, R, D, P\}$. This paper considers all independent flat block Rayleigh fading channels, and hence, h_{bc} is represented by a zero-mean θ_{bc}-variance complex Gaussian random variable, namely, $h_{bc} \sim \mathcal{CN}(0, \theta_{bc})$, and is unchanged during T but changes independently in the next T. Additionally, state information of all channels is assumed to be perfectly (channel state information (CSI) may be imperfectly estimated [48–50]; we reserve the case of imperfect CSI in our future works; instead, we focus on proposing a solution to secure SSRNwNLES in both transmission phases and analyze its intercept/outage performance in this paper) acquired, for example, through pilot estimation [51]. Furthermore, the path loss can be considered in θ_{bc} as $\theta_{bc} = d_{bc}^{-\delta}$ where d_{bc} and δ notate the $b \longrightarrow c$ distance and the path-loss exponent, correspondingly. The following notates the channel power gain as $g_{bc} = |h_{bc}|^2$ whose pdf (probability density function) and cdf (cumulative distribution function) are addressed, respectively, as

$$f_{g_{bc}}(x) = \frac{1}{\theta_{bc}} e^{-(x/\theta_{bc})} \Phi(x),$$
$$F_{g_{bc}}(x) = \left(1 - e^{-(x/\theta_{bc})}\right) \Phi(x), \tag{1}$$

where $\Phi(x)$ is the unit step function.

We notate P_s as the secondary source's transmit power. Then, the spectrum-sharing operation mode regulates P_s such that S interferes P with the amount of the interference power $P_s g_{sp}$ below the tolerable interference threshold I_t of P, i.e., $P_s g_{sp} \leq I_t$. Also, P_s is restricted by the maximum transmit power $\check{P}_s$ according to hardware specification, i.e.,

$P_s \le \check{P}_s$. Consequently, combining these power constraints regulates P_s as

$$P_s = \min\left(\frac{I_t}{g_{sp}}, \check{P}_s\right). \tag{2}$$

In (2), the equality is set for maximizing the cognitive radios' transmission range [52].

In Phase 1 with a duration of αT, the nonlinear energy harvester at R generates the following power [7].

$$\check{P}_r = \begin{cases} LP_s g_{sr} & , P_s g_{sr} \le \rho, \\ L\rho & , P_s g_{sr} > \rho, \end{cases} \tag{3}$$

where $L = 2\psi\alpha/(1-\alpha)$ with $\psi \in (0,1)$ being the energy converting efficiency and $\alpha \in (0,1)$ being a time fraction; ρ is the power saturation threshold.

Different from the conventional direct communication scheme where S sends only its data to D in Phase 2, our scheme allows S to use a fraction of its power $(1-\beta)P_s$ to send its message x_s and the remaining power βP_s to broadcast jamming signal x_a in order to protect its data against the eavesdropper. Here, $\beta \in (0,1)$ stands for the power distribution coefficient for the legitimate message and the jamming signal at S. As such, the signal transmitted by S can be expressed as $u_s = \sqrt{(1-\beta)P_s}x_s + \sqrt{\beta P_s}x_a$ and the received signals at R and E are uniquely expressed to be

$$y_m = h_{sm}\left(\sqrt{(1-\beta)P_s}x_s + \sqrt{\beta P_s}x_a\right) + \varepsilon_m, \tag{4}$$

where the additive noise at the receiver $m \in \{r, e\}$ is denoted as $\varepsilon_m \sim \mathcal{CN}(0, \varepsilon_m)$.

The a priori characteristic of the jamming signal is assumably known at R; for example, x_a can be a pseudorandom signal whose seed is shared with R [14]. As such, the jamming signal merely interrupts the eavesdropper and can be definitely abolished from the received signal of R. After annihilating the jamming signal, R further processes the following signal for decoding x_s:

$$\tilde{y}_r = h_{sr}\sqrt{(1-\beta)P_s}x_s + \varepsilon_r. \tag{5}$$

R obtains the signal-to-noise ratio (SNR) from (5) for recovering x_s to be

$$\Gamma_{sr} = \frac{g_{sr}P_s(1-\beta)}{\varepsilon_r}. \tag{6}$$

Generating x_a is merely shared between S and R but E is blind with it. Accordingly, the signal-to-noise plus interference ratio (SNIR) which E can obtain for recovering x_s in Phase 2 is deduced from (4) to be

$$\Gamma_{se} = \frac{g_{se}P_s(1-\beta)}{g_{se}P_s\beta + \varepsilon_e}. \tag{7}$$

In Phase 3 with a duration of $(1-\alpha)T/2$, R broadcasts the restored signal $\hat{x}_s$ as well as the jamming signal $\hat{x}_a$ to secure $\hat{x}_s$ against the eavesdropper. Consequently, the signals received at E and D have the same form as

$$y_w = h_{rw}\left(\sqrt{(1-\lambda)P_r}\hat{x}_s + \sqrt{\lambda P_r}\hat{x}_a\right) + \varepsilon_w, \tag{8}$$

where the receive antenna of $w \in \{d, e\}$ causes the additive noise $\varepsilon_w \sim \mathcal{CN}(0, \varepsilon_w)$; $\lambda \in (0,1)$ stands for the power distribution factor for the restored signal and the jamming signal at R; P_r is the transmit power of R. For the spectrum-sharing operation mode, P_r is constrained as

$$P_r = \min\left(\check{P}_r, \frac{I_t}{g_{rp}}\right). \tag{9}$$

Thanks to the property of the jamming signal $\hat{x}_a$ and processing it similarly to Phase 2, the SNR at D and the SNIR at E in Phase 3 are correspondingly given by

$$\Gamma_{rd} = \frac{g_{rd}P_r(1-\lambda)}{\varepsilon_d}, \tag{10}$$

$$\Gamma_{re} = \frac{g_{re}P_r(1-\lambda)}{g_{re}P_r\lambda + \varepsilon_e}. \tag{11}$$

It is seen from the denominators of (7) and (11) that E suffers the amount of jamming power in both last phases. This amount mitigates the probability of recovering precisely x_s at E, eventually improving the message security.

The DF operation of R results in the aggregated SNIR at D for recovering x_s as

$$\Gamma_d = \min(\Gamma_{sr}, \Gamma_{rd}). \tag{12}$$

In order for E to improve its intercept capability, it needs to combine its received signals in Phase 2 and Phase 3. We assume E prefers affordable complexity. Then, it can employ the signal selection combining method (other combining

methods which E can employ are maximum ratio combining and equal gain combining [53]; nonetheless, although these methods offer better performance, they require higher implementation complexity), which produces the entire SNIR to be

$$\Gamma_e = \max(\Gamma_{se}, \Gamma_{re}). \tag{13}$$

The channel capacity which $w \in \{d, e\}$ acquires to recover x_s is represented to be

$$\mathscr{R}_w = \frac{1-\alpha}{2}\log_2(1+\Gamma_w). \tag{14}$$

3. Security and Reliability Analyses

Communication reliability and message security can be measured through the OP at D and the IP at E, respectively. These probability expressions of the proposed simultaneous jamming-and-transmitting scheme for SSRNwNLES are derived to quickly evaluate both reliability and security without exhaustive simulations.

3.1. Intercept Probability. The intercept event occurs when the channel capacity of E surpasses the target spectral efficiency $\tilde{\mathscr{R}}_e$. Consequently, the IP is expressed to be

$$\Psi = \Pr\left\{\mathscr{R}_e \geq \tilde{\mathscr{R}}_e\right\} = \Pr\left\{\Gamma_e \geq \widetilde{\Gamma}_e\right\}, \tag{15}$$

where $\widetilde{\Gamma}_e = 2^{2\tilde{\mathscr{R}}_e/(1-\alpha)} - 1$.
Inserting (13) into (15) yields

$$\begin{aligned}\Psi &= \Pr\left\{\max(\Gamma_{se}, \Gamma_{re}) \geq \widetilde{\Gamma}_e\right\} \\ &= 1 - \Pr\left\{\max(\Gamma_{se}, \Gamma_{re}) < \widetilde{\Gamma}_e\right\} \\ &= 1 - \mathscr{E}_{P_s}\left\{\underbrace{\Pr\left\{\Gamma_{se} < \widetilde{\Gamma}_e \middle| P_s\right\}}_{\Psi_1}\underbrace{\Pr\left\{\Gamma_{re} < \widetilde{\Gamma}_e \middle| P_s\right\}}_{\Psi_2}\right\},\end{aligned} \tag{16}$$

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

Plugging (7) into Ψ_1 in (16) results in

$$\begin{aligned}\Psi_1 &= \Pr\left\{\frac{g_{se}P_s(1-\beta)}{g_{se}P_s\beta + \varepsilon_e} < \widetilde{\Gamma}_e \middle| P_s\right\} \\ &= \Pr\left\{g_{se}P_s\left(1-\beta-\widetilde{\Gamma}_e\beta\right) < \widetilde{\Gamma}_e\varepsilon_e \middle| P_s\right\} \\ &= \begin{cases}\bar{\Psi}_1, & \widetilde{\Gamma}_e < \dfrac{(1-\beta)}{\beta}, \\ 1, & \widetilde{\Gamma}_e \geq \dfrac{(1-\beta)}{\beta},\end{cases}\end{aligned} \tag{17}$$

where

$$\bar{\Psi}_1 = \Pr\left\{g_{se} < \frac{\widetilde{\Gamma}_e\varepsilon_e}{P_s\left(1-\beta-\widetilde{\Gamma}_e\beta\right)} \middle| P_s\right\} = 1 - e^{-(N/P_s)}, \tag{18}$$

with $N = \widetilde{\Gamma}_e\varepsilon_e/(1-\beta-\widetilde{\Gamma}_e\beta)\theta_{se}$.

Since $\widetilde{\Gamma}_e = 2^{2\tilde{\mathscr{R}}_e/(1-\alpha)} - 1$, (17) shows that the eavesdropping of E in Phase 2 can be completely eliminated by splitting appropriately times for energy harvesting and signal transmission (i.e., selecting α), allocating properly S's power to the jamming signal (i.e., selecting β), and setting reasonably the target spectral efficiency $\tilde{\mathscr{R}}_e$ such that the inequality $\widetilde{\Gamma}_e \geq (1-\beta)/\beta$ holds.

Inserting (11) into Ψ_2 in (16) yields

$$\begin{aligned}\Psi_2 &= \Pr\left\{\frac{g_{re}P_r(1-\lambda)}{g_{re}P_r\lambda + \varepsilon_e} < \widetilde{\Gamma}_e \middle| P_s\right\} \\ &= \Pr\left\{g_{re}P_r\left(1-\lambda-\lambda\widetilde{\Gamma}_e\right) < \widetilde{\Gamma}_e\varepsilon_e \middle| P_s\right\} \\ &= \begin{cases}\bar{\Psi}_2, & \widetilde{\Gamma}_e < \dfrac{(1-\lambda)}{\lambda}, \\ 1, & \widetilde{\Gamma}_e \geq \dfrac{(1-\lambda)}{\lambda},\end{cases}\end{aligned} \tag{19}$$

where

$$\begin{aligned}\bar{\Psi}_2 &= \Pr\left\{g_{re} < \frac{\widetilde{\Gamma}_e\varepsilon_e}{P_r\left(1-\lambda-\lambda\widetilde{\Gamma}_e\right)} \middle| P_s\right\} \\ &= \mathscr{E}_{P_r}\left\{\Pr\left\{g_{re} < \frac{\widetilde{\Gamma}_e\varepsilon_e}{P_r\left(1-\lambda-\lambda\widetilde{\Gamma}_e\right)} \middle| P_r, P_s\right\}\right\} \\ &= \mathscr{E}_{P_r}\left\{1 - e^{-\left(\widetilde{\Gamma}_e\varepsilon_e/\left(P_r\left(1-\lambda-\lambda\widetilde{\Gamma}_e\right)\theta_{re}\right)\right)} \middle| P_s\right\}.\end{aligned} \tag{20}$$

Because $\widetilde{\Gamma}_e = 2^{2\tilde{\mathscr{R}}_e/(1-\alpha)} - 1$, (19) indicates that the eavesdropping of E in Phase 3 can be completely eliminated by splitting appropriately times for energy harvesting and signal transmission (i.e., selecting α), allocating properly R's power

to the jamming signal (i.e., selecting λ), and setting reasonably the target spectral efficiency $\tilde{\mathscr{R}}_e$ such that the inequality $\widetilde{\Gamma}_e \geq (1-\lambda)/\lambda$ holds.

Given P_r in (9), (20) is further simplified as

$$\begin{aligned}\bar{\Psi}_2 &= \mathscr{E}_{g_{sr},g_{rp}}\left\{1-e^{-\left(\widetilde{\Gamma}_e\varepsilon_e/\left(\min\left(\check{P}_r,I_t/g_{rp}\right)\left(1-\lambda-\lambda\widetilde{\Gamma}_e\right)\theta_{re}\right)\right)}\middle| P_s\right\}\\ &= \mathscr{E}_{g_{sr}}\left\{1-\int_0^{I_t/\check{P}_r} e^{-\left(\widetilde{\Gamma}_e\varepsilon_e/\left(\check{P}_r\left(1-\lambda-\lambda\widetilde{\Gamma}_e\right)\theta_{re}\right)\right)}\frac{e^{-x/\theta_{rp}}}{\theta_{rp}}dx\right.\\ &\quad\left.-\int_{I_t/\check{P}_r}^{\infty} e^{-\left(\widetilde{\Gamma}_e\varepsilon_e/\left(I_t\left(1-\lambda-\lambda\widetilde{\Gamma}_e\right)\theta_{re}/x\right)\right)}\frac{e^{-x/\theta_{rp}}}{\theta_{rp}}dx\middle| P_s\right\}\\ &= \mathscr{E}_{g_{sr}}\left\{\underbrace{1-e^{-\left(Q/\check{P}_r\right)}+He^{-\left(Q/\check{P}_rH\right)}}_{A}\middle| P_s\right\},\end{aligned} \tag{21}$$

where $Q=\widetilde{\Gamma}_e\varepsilon_e/(1-\lambda-\lambda\widetilde{\Gamma}_e)\theta_{re}$ and $H=\theta_{rp}Q/(I_t+\theta_{rp}Q)$.

Based on (3), two cases of $\check{P}_r$ are considered when deriving (21) as follows.

Case 1. ($\check{P}_r = L\rho$).

This case holds when $g_{sr} > \rho/P_s$. By averaging $\mathscr{A}$ in (21) over this region, one obtains $\bar{\Psi}_2$ for this case as

$$\bar{\Psi}_{21}=\int_{\rho/P_s}^{\infty}\left(1-e^{-(Q/A\rho)}+He^{-(Q/AH\rho)}\right)\frac{e^{-x/\theta_{sr}}}{\theta_{sr}}dx=Me^{-(\rho/\theta_{sr}P_s)}, \tag{22}$$

where $M=1-e^{-(Q/A\rho)}+He^{-(Q/AH\rho)}$.

Case 2. ($\check{P}_r = LP_sg_{sr}$).

This case holds when $g_{sr} \leq \rho/P_s$. By averaging $\mathscr{A}$ in (21) over $g_{sr} \leq \rho/P_s$, one obtains $\bar{\Psi}_2$ for this case as

$$\begin{aligned}\bar{\Psi}_{22}&=\int_0^{\rho/P_s}\left(1-e^{-(Q/LP_sx)}+He^{-(Q/LHP_sx)}\right)\frac{e^{-x/\theta_{sr}}}{\theta_{sr}}\mathrm{d}x\\ &=1-e^{-(\rho/P_s\theta_{sr})}+\frac{1}{\theta_{sr}}\int_0^{\rho/P_s}e^{-(x/\theta_{sr})}\left(He^{-(Q/LHP_sx)}-e^{-(Q/LP_sx)}\right)dx.\end{aligned} \tag{23}$$

Using the series expansion for $e^{-x/\theta_{sr}}$, one rewrites (23) as

$$\begin{aligned}\bar{\Psi}_{22}&=1-e^{-(\rho/P_s\theta_{sr})}+\frac{1}{\theta_{sr}}\int_0^{\rho/P_s}\left[\sum_{k=0}^{\infty}\frac{1}{k!}\left(-\frac{x}{\theta_{sr}}\right)^k\right]\\ &\quad\cdot\left(He^{-(Q/LHP_sx)}-e^{-(Q/LP_sx)}\right)dx.\end{aligned} \tag{24}$$

Performing the variable change $t = 1/x$, one reduces (24) to

$$\begin{aligned}\bar{\Psi}_{22}&=1-e^{-(\rho/P_s\theta_{sr})}+\frac{1}{\theta_{sr}}\sum_{k=0}^{\infty}\frac{(-\theta_{sr})^{-k}}{k!}\int_{\frac{P_s}{\rho}}^{\infty}t^{-k-2}\\ &\quad\cdot\left(He^{-(Qt/LHP_s)}-e^{-(Qt/LP_s)}\right)dt\\ &=1-e^{-(\rho/P_s\theta_{sr})}+\sum_{k=0}^{\infty}\frac{J}{\mathrm{P}_s^{k+1}},\end{aligned} \tag{25}$$

where $J=(((Q/[\theta_{sr}L])^{k+1})/(k!(k+1)!))[\sum_{m=1}^{k+1}(-L\rho/Q)^m(m-1)!\{e^{-(Q/L\rho)}+(-1)^{m+1}H^{m-k}e^{-(Q/LH\rho)}\}-\mathrm{Ei}(-Q/L\rho)+H^{-k}\mathrm{Ei}(-Q/LH\rho)]$ with $\mathrm{Ei}(\cdot)$ being the exponential integral.

The total probability law simplifies (21) as

$$\bar{\Psi}_2=\bar{\Psi}_{21}+\bar{\Psi}_{22}=1+(M-1)e^{-(\rho/P_s\theta_{sr})}+\sum_{k=0}^{\infty}\frac{J}{P_s^{k+1}}. \tag{26}$$

Inserting (18) into (17) and (26) into (19), one obtains Ψ_1 and Ψ_2 as

$$\Psi_1=\begin{cases}1-e^{-(N/P_s)}, & \widetilde{\Gamma}_e<\dfrac{(1-\beta)}{\beta},\\ 1, & \widetilde{\Gamma}_e\geq\dfrac{(1-\beta)}{\beta},\end{cases} \tag{27}$$

$$\Psi_2=\begin{cases}1+(M-1)e^{-(\rho/\theta_{sr}P_s)}+\displaystyle\sum_{k=0}^{\infty}\frac{J}{P_s^{k+1}}, & \widetilde{\Gamma}_e<\dfrac{(1-\lambda)}{\lambda},\\ 1, & \widetilde{\Gamma}_e\geq\dfrac{(1-\lambda)}{\lambda}.\end{cases} \tag{28}$$

Plugging (27) and (28) into (16), one obtains

$$\Psi=\begin{cases}\check{\Psi}_1, & \widetilde{\Gamma}_e\geq\max\left(\dfrac{[1-\beta]}{\beta},\dfrac{[1-\lambda]}{\lambda}\right),\\ \check{\Psi}_2, & \dfrac{(1-\beta)}{\beta}\leq\widetilde{\Gamma}_e<\dfrac{(1-\lambda)}{\lambda},\\ \check{\Psi}_3, & \dfrac{(1-\lambda)}{\lambda}\leq\widetilde{\Gamma}_e<\dfrac{(1-\beta)}{\beta},\\ \check{\Psi}_4, & \widetilde{\Gamma}_e<\min\left(\dfrac{[1-\beta]}{\beta},\dfrac{[1-\lambda]}{\lambda}\right).\end{cases} \tag{29}$$

Since $\widetilde{\Gamma}_e=2^{2\tilde{\mathscr{R}}_e/(1-\alpha)}-1$, it is indicated from (29) that the security of the proposed simultaneous jamming-and-

transmitting scheme experiences four different levels dependent on adjusting the system parameters ($\tilde{\mathscr{R}}_e$, α, β, λ).

The following sequentially computes $\breve{\Psi}_1$, $\breve{\Psi}_2$, $\breve{\Psi}_3$, and $\breve{\Psi}_4$ to numerically evaluate (29). First, we start with $\breve{\Psi}_1$. It is straightforward to infer that

$$\breve{\Psi}_1 = 0. \tag{30}$$

Because $\widetilde{\Gamma}_e = 2^{2\tilde{\mathscr{R}}_e/(1-\alpha)} - 1$, (30) indicates that the eavesdropping of E can be completely eliminated in the proposed simultaneous jamming-and-transmitting scheme where both legitimate messages (of S and R) are protected in Phase 2 and Phase 3 by splitting appropriately times for energy harvesting and signal transmission (i.e., selecting α), distributing reasonably S's power to the jamming signal (i.e., selecting β), allocating properly R's power to the jamming signal (i.e., selecting λ), and setting the target spectral efficiency $\tilde{\mathscr{R}}_e$ such that the inequality, $\widetilde{\Gamma}_e \geq \max\left([1-\beta]/\beta, [1-\lambda]/\lambda\right)$, holds.

Second, $\breve{\Psi}_2$ is written explicitly as

$$\breve{\Psi}_2 = 1 - \mathscr{E}_{P_s}\left\{1 + (M-1)e^{-(\rho/\theta_{sr}P_s)} + \sum_{k=0}^{\infty}\frac{J}{P_s^{k+1}}\right\}. \tag{31}$$

Given P_s in (2), one solves (31) in closed form as

$$\begin{aligned}
\breve{\Psi}_2 &= -\int_0^{I_t/\breve{P}_s}\left((M-1)e^{-\left(\rho/\theta_{sr}\breve{P}_s\right)} + \sum_{k=0}^{\infty}\frac{J}{\breve{P}_s^{k+1}}\right)\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx \\
&\quad - \int_{I_t/\breve{P}_s}^{\infty}\left((M-1)e^{-(\rho x/\theta_{sr}I_t)} + \sum_{k=0}^{\infty}\left(\frac{x}{I_t}\right)^{k+1}J\right)\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx \\
&= -\left((M-1)e^{-\left(\rho/\theta_{sr}\breve{P}_s\right)} + \sum_{k=0}^{\infty}\frac{J}{\breve{P}_s^{k+1}}\right)\left(1 - e^{-\left(I_t/\theta_{sp}\breve{P}_s\right)}\right) \\
&\quad - \frac{M-1}{\theta_{sp}}\left(\frac{\rho}{\theta_{sr}I_t} + \frac{1}{\theta_{sp}}\right)^{-1}e^{-\left((\rho/\theta_{sr}I_t)+1/\theta_{sp}\right)I_t/\breve{P}_s} \\
&\quad - e^{-\left(I_t/\breve{P}_s\theta_{sp}\right)}\sum_{k=0}^{\infty}\sum_{n=0}^{k+1}\frac{(k+1)!\theta_{sp}^{k+1}J}{n!I_t^{k+1-n}\left(\theta_{sp}\breve{P}_s\right)^n}.
\end{aligned} \tag{32}$$

Third, $\breve{\Psi}_3$ has an explicit form as

$$\breve{\Psi}_3 = 1 - \mathscr{E}_{P_s}\left\{1 - e^{-N/P_s}\right\}. \tag{33}$$

With P_s in (2), the expectation in (33) is evaluated as

$$\begin{aligned}
\breve{\Psi}_3 &= \int_0^{I_t/\breve{P}_s} e^{-N/\breve{P}_s}\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx + \int_{I_t/\breve{P}_s}^{\infty} e^{-N/(I_t/x)}\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx \\
&= e^{-N/\breve{P}_s}\left(1 - e^{-I_t/\theta_{sp}\breve{P}_s}\right) + \left(\frac{\theta_{sp}N}{I_t} + 1\right)^{-1}e^{-\left((N/I_t)+\left(1/\theta_{sp}\right)\right)I_t/\breve{P}_s}.
\end{aligned} \tag{34}$$

Finally, $\breve{\Psi}_4$ is given by

$$\begin{aligned}
\breve{\Psi}_4 &= 1 - \mathscr{E}_{P_s}\left\{\left(1 - e^{-N/P_s}\right)\left(1 + (M-1)e^{-\rho/\theta_{sr}P_s} + \sum_{k=0}^{\infty}\frac{J}{P_s^{k+1}}\right)\middle| P_s\right\} \\
&= \breve{\Psi}_2 + \breve{\Psi}_3 + \mathscr{E}_{P_s}\left\{(M-1)e^{-((\rho/\theta_{sr})+N)1/P_s} + \sum_{k=0}^{\infty}J\frac{e^{-N/P_s}}{P_s^{k+1}}\middle| P_s\right\}.
\end{aligned} \tag{35}$$

With P_s in (2), the expectation in (35) is evaluated as

$$\begin{aligned}
\breve{\Psi}_4 &= \breve{\Psi}_2 + \breve{\Psi}_3 + \int_0^{I_t/\breve{P}_s}\Bigg((M-1)e^{-((\rho/\theta_{sr})+N)1/\breve{P}_s} \\
&\quad + \sum_{k=0}^{\infty}J\frac{e^{-N/\breve{P}_s}}{\breve{P}_s^{k+1}}\Bigg)\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx + \int_{I_t/\breve{P}_s}^{\infty} \\
&\quad \cdot\left((M-1)e^{-((\rho/\theta_{sr})+N)\frac{x}{I_t}} + \sum_{k=0}^{\infty}J\left(\frac{x}{I_t}\right)^{k+1}e^{-Nx/I_t}\right)\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx \\
&= \breve{\Psi}_2 + \breve{\Psi}_3 + \Bigg((M-1)e^{-((\rho/\theta_{sr})+N)1/\breve{P}_s} \\
&\quad + e^{-N/\breve{P}_s}\sum_{k=0}^{\infty}\frac{J}{\breve{P}_s^{k+1}}\Bigg)\left(1 - e^{-I_t/\theta_{sp}\breve{P}_s}\right) + (M-1) \\
&\quad \cdot\left(\frac{\theta_{sp}}{I_t}\left[N + \frac{\rho}{\theta_{sr}}\right] + 1\right)^{-1}e^{-\left(N+(\rho/\theta_{sr})+\left(I_t/\theta_{sp}\right)\right)1/\breve{P}_s} \\
&\quad + \frac{e^{-\left(N+I_t/\theta_{sp}\right)/\breve{P}_s}}{1+\theta_{sp}N/I_t}\sum_{k=0}^{\infty}\sum_{i=0}^{k+1}\left(N + \frac{I_t}{\theta_{sp}}\right)^{i-k-1}\frac{(k+1)!J}{i!\breve{P}_s^i}.
\end{aligned} \tag{36}$$

3.2. Outage Probability. The outage event happens as the channel capacity of D subceeds the target spectral efficiency $\tilde{\mathscr{R}}_d$. Accordingly, the OP is addressed to be

$$Y = \Pr\left\{\mathscr{R}_d \leq \tilde{\mathscr{R}}_d\right\} = \Pr\left\{\Gamma_d \leq \widetilde{\Gamma}_d\right\}, \tag{37}$$

where $\widetilde{\Gamma}_d = 2^{2\tilde{\mathscr{R}}_d/(1-\alpha)} - 1$.

Employing Γ_d in (12) reduces (37) to

$$\begin{aligned}
Y &= \Pr\left\{\min\left(\Gamma_{sr}, \Gamma_{rd}\right) \leq \widetilde{\Gamma}_d\right\} \\
&= 1 - \Pr\left\{\min\left(\Gamma_{sr}, \Gamma_{rd}\right) > \widetilde{\Gamma}_d\right\} \\
&= 1 - \mathscr{E}_{P_s}\left\{\underbrace{\mathscr{E}_{g_{sr}}\left\{\tilde{Y}\middle| g_{sr} > \frac{\widetilde{\Gamma}_d\varepsilon_r}{P_s(1-\beta)}\right\}}_{\tilde{Y}}\middle| P_s\right\},
\end{aligned} \tag{38}$$

where $\tilde{Y} = \Pr\left\{g_{rd} > \widetilde{\Gamma}_d\varepsilon_d/P_r(1-\lambda)\right\}$.

Given P_r in (9), $\tilde{Y}$ is rewritten as

$$\begin{aligned}\tilde{Y} &= \mathscr{E}_{g_{rp}}\left\{\Pr\left\{g_{rd} > \frac{\widetilde{\Gamma}_d\varepsilon_d}{(1-\lambda)\min\left(\check{P}_r, I_t/g_{rp}\right)}\right\}\right\}\\ &= \mathscr{E}_{g_{rp}}\left\{e^{-\widetilde{\Gamma}_d\varepsilon_d/\left((1-\lambda)\theta_{rd}\min\left(\check{P}_r, I_t/g_{rp}\right)\right)}\right\}\\ &= \int_0^{I_t/\check{P}_r} e^{-\widetilde{\Gamma}_d\varepsilon_d/\left((1-\lambda)\theta_{rd}\check{P}_r\right)}\frac{e^{-x/\theta_{rd}}}{\theta_{rp}}dx\\ &\quad + \int_{I_t/\check{P}_r}^{\infty} e^{-\widetilde{\Gamma}_d\varepsilon_d x/((1-\lambda)\theta_{rd}I_t)}\frac{e^{-x/\theta_{rp}}}{\theta_{rp}}dx\\ &= e^{-W/\check{P}_r} - Ge^{-W/\check{P}_rG},\end{aligned} \tag{39}$$

where $W = \widetilde{\Gamma}_d\varepsilon_d/((1-\lambda)\theta_{rd})$ and $G = \theta_{rp}W/(\theta_{rp}W + I_t)$.

Based on (3), two cases of $\check{P}_r$ are considered when deriving $\bar{Y}$ in (38) as follows.

Case 1. ($\check{P}_r = LP_sg_{sr}$).

This case holds when $g_{sr} \le \rho/P_s$. Incorporating this condition with $g_{sr} > \varepsilon_r\widetilde{\Gamma}_d/(P_s(1-\beta))$ in (38) results in existence region of g_{sr} to be $D/P_s < g_{sr} \le \rho/P_s$ where $D = \varepsilon_r\widetilde{\Gamma}_d/(1-\beta)$. By averaging $\tilde{Y}$ in (39) over this region, one obtains $\bar{Y}$ for this case as $\bar{Y}_1 = \int_{D/P_s}^{\rho/P_s}(e^{-W/LP_sx} - Ge^{-W/LGP_sx})(e^{-x/\theta_{sr}}/\theta_{sr})dx$. Applying the series expansion for $e^{-x/\theta_{sr}}$ and then performing the variable change $t = 1/x$, one solves the integral in $\bar{Y}_1$ as

$$\begin{aligned}\bar{Y}_1 &= \frac{1}{\theta_{sr}}\int_{D/P_s}^{\rho/P_s}\left(\sum_{k=0}^{\infty}\frac{1}{k!}\left[-\frac{x}{\theta_{sr}}\right]^k\right)\left(e^{-W/LP_sx} - Ge^{-W/LGP_sx}\right)dx\\ &= \sum_{k=0}^{\infty}\frac{(-\theta_{sr})^{-k-1}}{k!}\int_{P_s/D}^{P_s/\rho}\left(e^{-Wt/LP_s} - Ge^{-Wt/LGP_s}\right)\frac{1}{t^{k+2}}dt\\ &= \sum_{k=0}^{\infty}\frac{(-\theta_{sr})^{-k-1}}{k!}\left\{\int_{P_s/D}^{\infty}\left(e^{-Wt/LP_s} - Ge^{-Wt/LGP_s}\right)\frac{1}{t^{k+2}}dt\right.\\ &\quad \left. - \int_{P_s/\rho}^{\infty}\left(e^{-Wt/LP_s} - Ge^{-Wt/LGP_s}\right)\frac{1}{t^{k+2}}dt\right\} = \sum_{k=0}^{\infty}\frac{V}{P_s^{k+1}},\end{aligned} \tag{40}$$

where $V = (1/(k!(k+1)!))(W/\theta_{sr}L)^{k+1}\{\mathrm{Ei}(-W/L\rho) - \mathrm{Ei}(-W/LD) + G^{-k}[\mathrm{Ei}(-W/LDG) - \mathrm{Ei}(-W/LG\rho)] + \sum_{u=1}^{k+1}(u-1)!(-L/W)^u[D^ue^{-W/LD} - \rho^ue^{-W/L\rho} - G^{u-k}(D^ue^{-W/LDG} - \rho^ue^{-W/LG\rho})]\}$.

Case 2. ($\check{P}_r = L\rho$).

This case holds when $g_{sr} > \rho/P_s$. Incorporating this condition with $g_{sr} > \varepsilon_r\widetilde{\Gamma}_d/(P_s(1-\beta))$ in (38) results in existence region of $g_{sr} > B/P_s$ where $B = \max(\varepsilon_r\widetilde{\Gamma}_d/(1-\beta), \rho)$. By averaging $\tilde{Y}$ in (39) over this region, one obtains $\bar{Y}$ for this case as

$$\bar{Y}_2 = \int_{B/P_s}^{\infty}\left(e^{-W/L\rho} - Ge^{-W/LG\rho}\right)\frac{e^{-x/\theta_{sr}}}{\theta_{sr}}dx = Ue^{-B/\theta_{sr}P_s}, \tag{41}$$

where $U = e^{-W/L\rho} - Ge^{-W/LG\rho}$.

The total probability law simplifies $\bar{Y}$ in (38) as

$$\bar{Y} = \bar{Y}_1 + \bar{Y}_2 = Ue^{-B/\theta_{sr}P_s} + \sum_{k=0}^{\infty}\frac{V}{P_s^{k+1}}. \tag{42}$$

Plugging (42) into $\bar{Y}$ in (38) with a note that P_s is given in (2) results in

$$\begin{aligned}Y &= 1 - \mathscr{E}_{P_s}\left\{Ue^{-B/\theta_{sr}P_s} + \sum_{k=0}^{\infty}\frac{V}{P_s^{k+1}}\right\}\\ &= 1 - \int_0^{I_t/\check{P}_s}\left(Ue^{-B/\theta_{sr}\check{P}_s} + \sum_{k=0}^{\infty}\frac{V}{\check{P}_s^{k+1}}\right)\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx\\ &\quad - \int_{I_t/\check{P}_s}^{\infty}\left(Ue^{-Bx/\theta_{sr}I_t} + \sum_{k=0}^{\infty}V\left(\frac{x}{I_t}\right)^{k+1}\right)\frac{e^{-x/\theta_{sp}}}{\theta_{sp}}dx\\ &= 1 - \left(Ue^{-B/\theta_{sr}\check{P}_s} + \sum_{k=0}^{\infty}\frac{V}{\check{P}_s^{k+1}}\right)\left(1 - e^{-I_t/\theta_{sp}\check{P}_s}\right)\\ &\quad - U\left(\frac{\theta_{sp}B}{\theta_{sr}I_t} + 1\right)^{-1}e^{-\left((B/\theta_{sr}) + \left(I_t/\theta_{sp}\right)\right)1/\check{P}_s}\\ &\quad - \sum_{k=0}^{\infty}\sum_{i=0}^{k+1}\left(\frac{\theta_{sp}}{I_t}\right)^{k+1-i}e^{-I_t/\theta_{sp}\check{P}_s}\frac{(k+1)!V}{i!\check{P}_s^i}.\end{aligned} \tag{43}$$

3.3. Asymptotic Analysis. The asymptotic intercept and outage probabilities are analyzed under consideration of the following extreme cases: (1) Case 1: high maximum transmit power ($\check{P}_s \longrightarrow \infty$) and (2) Case 2: high maximum interference power ($I_t \longrightarrow \infty$). Case 2 corresponds to noncognitive networks (i.e., no interference power constraint) or no interference caused by secondary users on primary users (e.g., secondary users are distant from primary users or secondary-primary channels are blocked).

Case 1. ($\check{P}_s \longrightarrow \infty$).

The intercept probability in this scenario becomes

$$\Psi^{\check{P}_s\longrightarrow\infty} = \begin{cases} 0, & \widetilde{\Gamma}_e \ge \max\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right),\\ \check{\Psi}_2^{\check{P}_s\longrightarrow\infty}, & \frac{(1-\beta)}{\beta} \le \widetilde{\Gamma}_e < \frac{(1-\lambda)}{\lambda},\\ \check{\Psi}_3^{\check{P}_s\longrightarrow\infty}, & \frac{(1-\lambda)}{\lambda} \le \widetilde{\Gamma}_e < \frac{(1-\beta)}{\beta},\\ \check{\Psi}_4^{\check{P}_s\longrightarrow\infty}, & \widetilde{\Gamma}_e < \min\left(\frac{[1-\beta]}{\beta}, \frac{[1-\lambda]}{\lambda}\right),\end{cases} \tag{44}$$

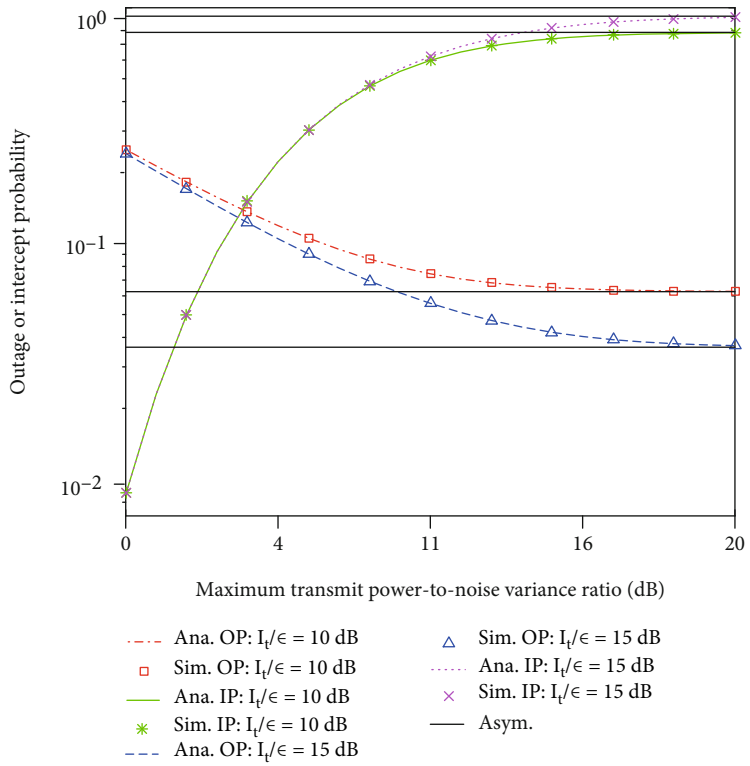

FIGURE 3: IP and OP versus $\Theta = \check{P}_s/\varepsilon$. "Ana." and "Sim." represent the simulation result and the analytical result in Section 3, respectively, while "Asym." represents the asymptotic result.

where $\check{\Psi}_2^{\check{P}_s\longrightarrow\infty}$, $\check{\Psi}_3^{\check{P}_s\longrightarrow\infty}$, and $\check{\Psi}_4^{\check{P}_s\longrightarrow\infty}$ are obtained from $\check{\Psi}_2$ in (32), $\check{\Psi}_3$ in (34), and $\check{\Psi}_4$ in (36), respectively, as $\check{\Psi}_2^{\check{P}_s\longrightarrow\infty} = \lim_{\check{P}_s\longrightarrow\infty}\check{\Psi}_2 = (1+(\theta_{sp}\rho/\theta_{sr}I_t))^{-1}(1-M) - \sum_{k=0}^{\infty}(\theta_{sp}/I_t)^{k+1}(k+1)!J$, $\check{\Psi}_3^{\check{P}_s\longrightarrow\infty} = \lim_{\check{P}_s\longrightarrow\infty}\check{\Psi}_3 = ((\theta_{sp}N/I_t)+1)^{-1}$, and $\check{\Psi}_4^{\check{P}_s\longrightarrow\infty} = \lim_{\check{P}_s\longrightarrow\infty}\check{\Psi}_4 = \check{\Psi}_2^{\check{P}_s\longrightarrow\infty} + (M-1)((\theta_{sp}/I_t)[(\rho/\theta_{sr})+N]+1)^{-1} + \check{\Psi}_3^{\check{P}_s\longrightarrow\infty} + (I_t/\theta_{sp})\sum_{k=0}^{\infty}(k+1)!(N+(I_t/\theta_{sp}))^{-k-2}J$.

Likewise, the outage probability in this scenario is obtained from (43) to be

$$Y^{\check{P}_s\longrightarrow\infty} = \lim_{\check{P}_s\longrightarrow\infty} Y = 1 - \left(\frac{\theta_{sp}B}{\theta_{sr}I_t}+1\right)^{-1} U - \sum_{k=0}^{\infty}(k+1)!\left(\frac{\theta_{sp}}{I_t}\right)^{k+1} V. \tag{45}$$

It is observed from (44) and (45) that when the maximum transmit power is large, both IP and OP converge, creating the error floors (or zero diversity orders). This result will be validated in Figure 3.

Case 2. ($I_t \longrightarrow \infty$).

The intercept probability in this case becomes

$$\Psi^{I_t\longrightarrow\infty} = \begin{cases} 0, & \widetilde{\Gamma}_e \geq \max\left(\dfrac{[1-\beta]}{\beta}, \dfrac{[1-\lambda]}{\lambda}\right), \\ \check{\Psi}_2^{I_t\longrightarrow\infty}, & \dfrac{(1-\beta)}{\beta} \leq \widetilde{\Gamma}_e < \dfrac{(1-\lambda)}{\lambda}, \\ \check{\Psi}_3^{I_t\longrightarrow\infty}, & \dfrac{(1-\lambda)}{\lambda} \leq \widetilde{\Gamma}_e < \dfrac{(1-\beta)}{\beta}, \\ \check{\Psi}_4^{I_t\longrightarrow\infty}, & \widetilde{\Gamma}_e < \min\left(\dfrac{[1-\beta]}{\beta}, \dfrac{[1-\lambda]}{\lambda}\right), \end{cases} \tag{46}$$

where $\check{\Psi}_2^{I_t\longrightarrow\infty}$, $\check{\Psi}_3^{I_t\longrightarrow\infty}$, and $\check{\Psi}_4^{I_t\longrightarrow\infty}$ are obtained from $\check{\Psi}_2$ in (32), $\check{\Psi}_3$ in (34), and $\check{\Psi}_4$ in (36), respectively, as $\check{\Psi}_2^{I_t\longrightarrow\infty} = \lim_{I_t\longrightarrow\infty}\check{\Psi}_2 = (1-M_1)e^{-\rho/\theta_{sr}\check{P}_s} - \sum_{k=0}^{\infty}J_1/\check{P}_s^{k+1}$, $\check{\Psi}_3^{I_t\longrightarrow\infty} = \lim_{I_t\longrightarrow\infty}\check{\Psi}_3 = e^{-N/\check{P}_s}$, and $\check{\Psi}_4^{I_t\longrightarrow\infty} = \lim_{I_t\longrightarrow\infty}\check{\Psi}_4 = \check{\Psi}_2^{I_t\longrightarrow\infty} + \check{\Psi}_3^{I_t\longrightarrow\infty} + (M_1-1)e^{-(N+(\rho/\theta_{sr}))1/\check{P}_s} + e^{-N/\check{P}_s}\sum_{k=0}^{\infty}J_1/\check{P}_s^{k+1}$ where $J_1 = \lim_{I_t\longrightarrow\infty}J = (1/(k!(k+1)!))(Q/L\theta_{sr})^{k+1}[e^{-Q/L\rho}\sum_{u=1}^{k+1}(u-1)!(-L\rho/Q)^u - \mathrm{Ei}(-Q/L\rho)]$ and $M_1 = \lim_{I_t\longrightarrow\infty}M = 1-e^{-Q/L\rho}$.

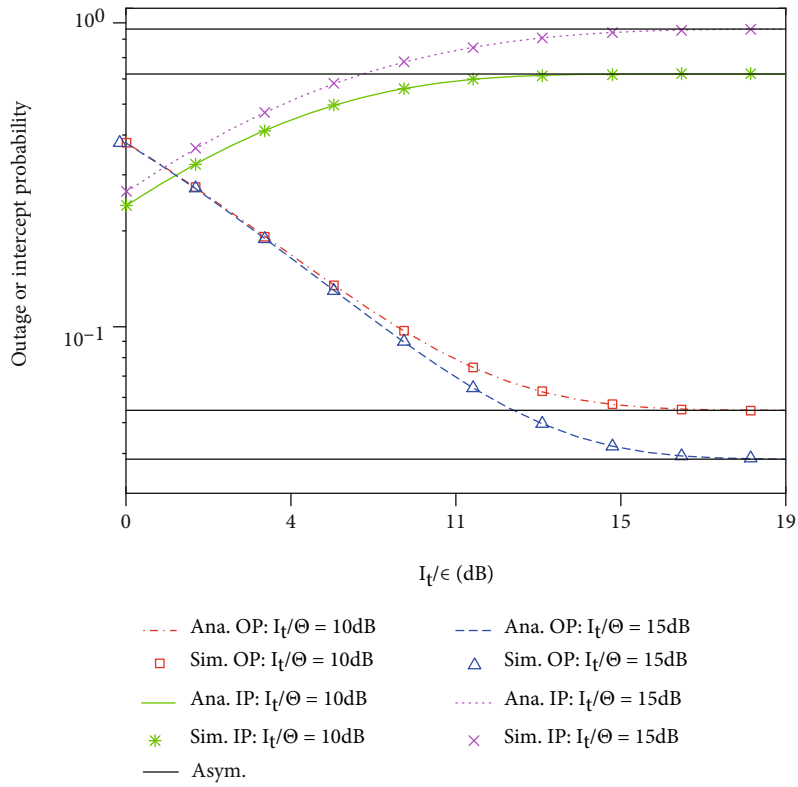

Figure 4: IP and OP versus I_t/ε.

Likewise, the outage probability in this scenario is obtained from (38) to be

$$Y^{I_t\longrightarrow\infty} = \lim_{I_t\longrightarrow\infty} Y = 1 - U_1 e^{-B/\theta_{sr}\check{P}_s} - \sum_{k=0}^{\infty} \frac{V_1}{\check{P}_s^{k+1}}, \quad (47)$$

where $U_1 = \lim_{I_t\longrightarrow\infty} U = e^{-W/L\rho}$ and $V_1 = \lim_{I_t\longrightarrow\infty} V = (1/(k!(k+1)!))(W/\theta_{sr}L)^{k+1}\{\mathrm{E}i(-W/L\rho) - \mathrm{E}i(-W/LD) + \sum_{u=1}^{k+1}(u-1)!(-L/W)^u[e^{-W/LD}D^u - e^{-W/L\rho}\rho^u]\}$.

It is seen from (46) and (47) that when the maximum interference power is large, both IP and OP also converge, creating the error floors (or zero diversity orders). This result will be validated in Figure 4.

4. Demonstrative Results

The current section demonstrates simulated/theoretical results to assess both security and reliability of the proposed jamming-and-transmitting scheme for spectrum-sharing relaying networks with nonlinear energy scavenging via essential parameters. Monte-Carlo simulations (the Monte-Carlo simulation is widely accepted, e.g., [54]; therefore, an explanation of its operation should not be included in this paper) produce simulated results while the derived expressions in Section 3 are calculated to achieve theoretical ones. For illustration intention, users are arbitrarily positioned in the 2-dimensional plane as E at (0.6,–0.5), P at (0.9,0.8), D at (1.0,0.0), R at (0.5,0.0), and S at (0.0,0.0). Unless otherwise stated, the following parameters are considered: the target spectral efficiency $\tilde{\mathcal{R}}_e = \tilde{\mathcal{R}}_d = 0.3$ bps/Hz, the path-loss exponent $\delta = 3$, the energy converting efficiency $\psi = 0.9$, and equal noise variances $\varepsilon_d = \varepsilon_r = \varepsilon_e = \varepsilon$.

Figure 3 plots the IP and the OP versus $\Theta = \check{P}_s/\varepsilon$ for $\alpha = 0.35$, $\rho/\varepsilon = 10$ dB, $\beta = 0.48$, and $\lambda = 0.63$. The results demonstrate the coincidence between the simulation and the analysis, validating the accurateness of the analytical results. Moreover, the reliability of the system is enhanced and the security is decreased with increasing $\check{P}_s$, which comes from the reality that increasing $\check{P}_s$ facilitates R in recovering successfully the source data and scavenging more energy in the source signals, hence mitigating the outage probability in Phase 3. Likewise, E is also beneficial in both Phase 2 and Phase 3 when $\check{P}_s$ increases, so the intercept probability also grows with $\check{P}_s$. However, both IP and OP converge at high $\check{P}_s$. Such a convergence is owing to the power distribution of the spectrum-sharing operation mode for S and R in (2) and (9) where transmit powers are uncorrelated with $\check{P}_s$ for large $\check{P}_s$ (i.e., as $\check{P}_s$ is adequately large, the MTPC is not necessary), causing the constant IP/OP. Such a constant IP/OP is named as the asymptotic IP/OP, which was analyzed in Subsection 3.3. Furthermore, the OP goes down and the IP goes up with increasing I_t. This observation is comprehended similarly to the case of increasing $\check{P}_s$ owing to the power distribution of the spectrum-sharing operation mode for S and R. Due to the opposite trends of the IP and

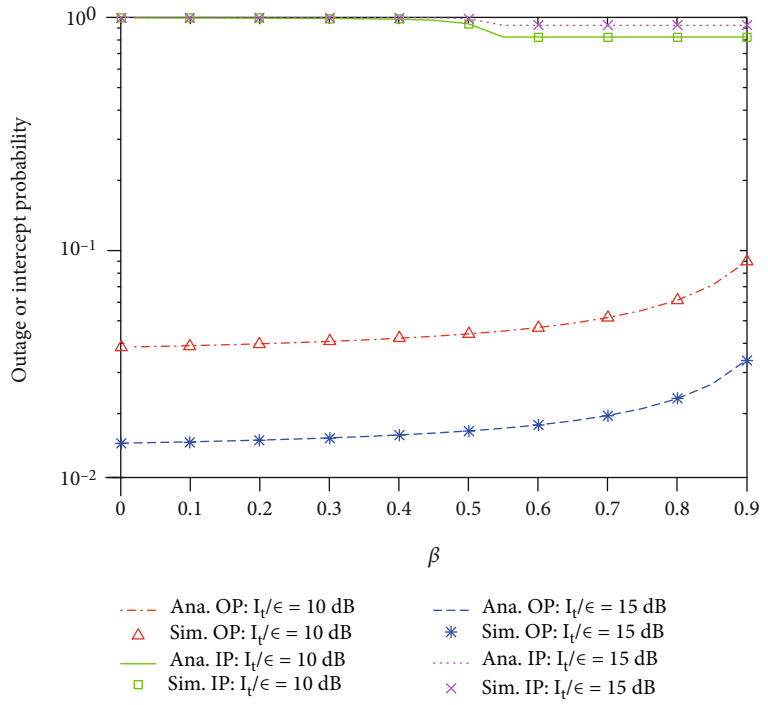

FIGURE 5: IP and OP versus β.

the OP, the security-reliability trade-off is observed. By the exhaustive search, any security-reliability trade-off level can be found straightforwardly; for example, Figure 3 reveals that the best security-reliability trade-off wherein the OP and the IP are equal occurs at $\Theta = 3.84$ dB for $I_t/\varepsilon = 10$ dB.

Figure 4 plots the IP/OP versus I_t/ε for the same specifications as Figure 3. The results reveal the coincidence between the simulation and the analysis, asserting the correctness of the analytical results. Moreover, the reliability/security is improved/degraded with increasing I_t and $\breve{P}_s$, which shows the security-reliability trade-off. By the exhaustive search, any security-reliability trade-off level can be found easily; for instance, Figure 4 unveils that the best security-reliability trade-off wherein the IP and the OP are equal happens at $I_t/\varepsilon = 1.46$ dB for $\Theta = 10$ dB. Nonetheless, the reliability and the security converge at large I_t, which validates the asymptotic analysis in Subsection 3.3. The results in Figure 4 are comprehended similarly to those in Figure 3.

Figure 5 exposes the IP/OP versus the power distribution coefficient β at S, which presents the percentage of power that S uses to transmit the jamming signal, for $\breve{P}_s/\varepsilon = 20$ dB, $\rho/\varepsilon = 15$ dB, $\alpha = 0.35$, and $\lambda = 0.48$. The results unveil the coincidence between the analysis and the simulation, affirming the correctness of the analytical results. It is noted that β is the superposition coefficient which is inversely proportional to S's signal but proportional to the jamming signal in Phase 2. Consequently, the increase in β creates less energy for S to transmit information signal and less chance for R to decode successfully the message, which leads to the growth of the OP and the slight decline of the IP. However, the IP remains constant for $\widetilde{\Gamma}_e \geq (1-\beta)/\beta$ (or $\beta \geq 1/(1+\widetilde{\Gamma}_e)$) as seen from (27). This is because E suffers a complete outage in Phase 2, and hence, the IP only depends on Phase 3. Moreover, the reliability trades off with the security owing to the opposite trends of the IP and the OP, which was also observed similarly to Figure 3. Additionally, the security/reliability is degraded/enhanced with the increase in I_t, which is similar to results in previous figures.

Figure 6 demonstrates the IP/OP versus the power distribution coefficient λ at R, which presents the percentage of power that R uses to transmit the jamming signal, for $\breve{P}_s/\varepsilon = 20$ dB, $\rho/\varepsilon = 15$ dB, $\alpha = 0.35$, and $\beta = 0.63$. The results reveal the coincidence between the analysis and the simulation, asserting the correctness of the analytical results. Moreover, it is seen that the reliability is deteriorated while the security is better with increasing λ. This can be comprehended by the power allocation of the spectrum-sharing operation mode at R for the legitimate signal and the jamming signal, similar to Figure 5. Notably, the IP reduces to zero and the absolute security is achievable when λ is greater than a certain value; for example, $\lambda > 0.5$ as in the case of Figure 6. This can be interpreted as follows. Since $\beta = 0.63$ and $\alpha = 0.35$, the inequality $\beta \geq 1/(1+\widetilde{\Gamma}_e)$ holds where $\widetilde{\Gamma}_e = 2^{2\widetilde{\mathcal{R}}_e/(1-\alpha)} - 1$. Therefore, when $\lambda \geq 1/(1+\widetilde{\Gamma}_e)$, E suffers a complete outage in both phases (2 and 3) as seen in (29), causing $\Psi = 0$. In addition, the security trades off with the reliability owing to the opposite trends of the IP and the OP, which was also observed similarly to Figure 3. Additionally, the security/reliability is deteriorated/enhanced with respect to the increase in I_t, as anticipated.

Figure 7 plots the IP/OP versus the time fraction α for $\breve{P}_s/\varepsilon = 20$ dB, $\rho/\varepsilon = 15$ dB, $\beta = 0.48$, and $\lambda = 0.63$. The results unveil the coincidence between the analysis and the simulation, affirming the correctness of the analytical results.

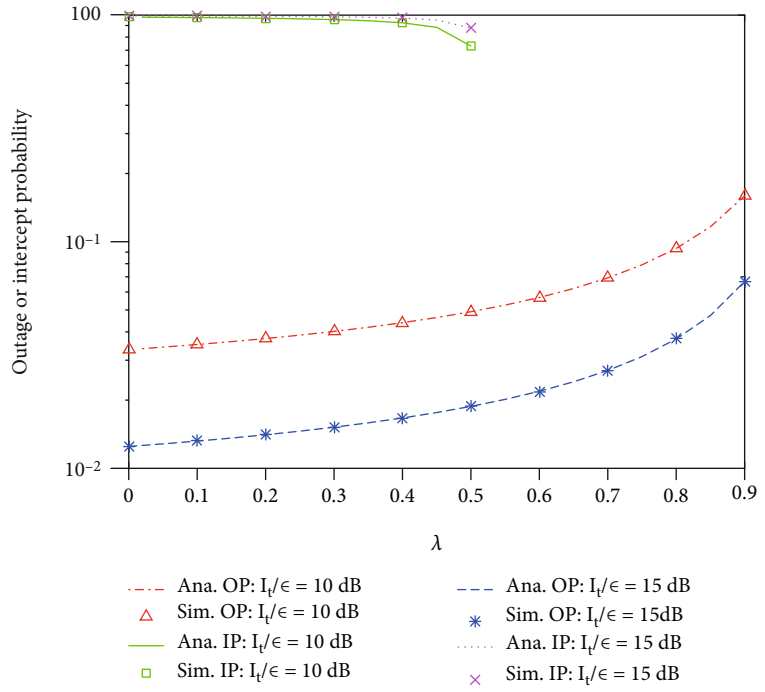

Figure 6: OP and IP versus λ.

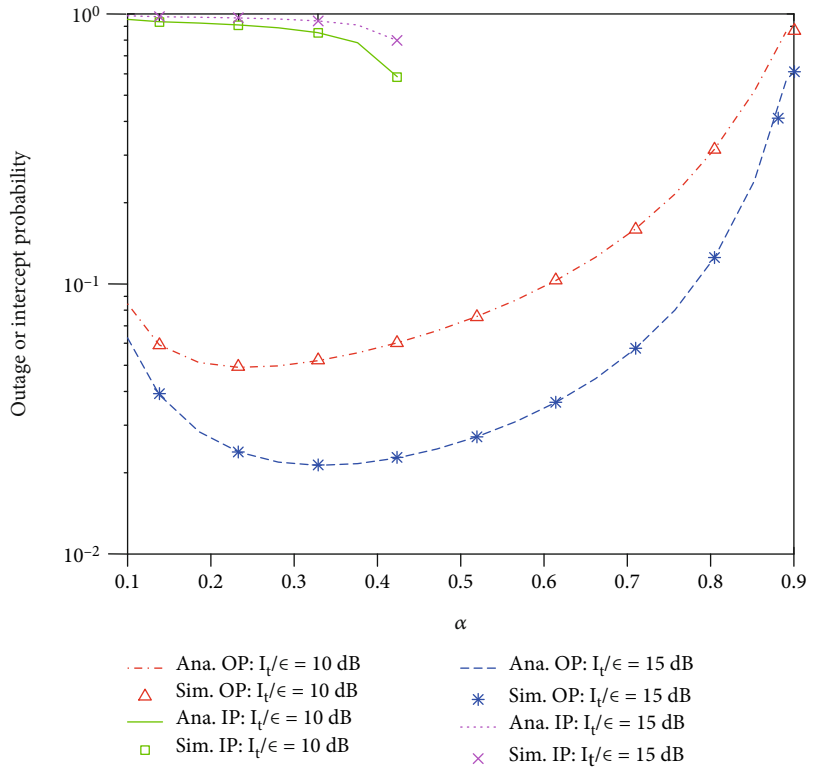

Figure 7: IP and OP versus α.

Further, α can be selected optimally for the best reliability; for instance, $\alpha_{opt} = 0.3$ is seen in Figure 7. α_{opt} is available owing to the following reality. The increase in α extends the duration of Phase 1 (energy harvesting stage), facilitating R in harvesting more energy and recovering successfully the source message with a higher possibility. Notwithstanding, the increase in α also deteriorates the channel capacities in Phase 2 and Phase 3 (information transmission stage)

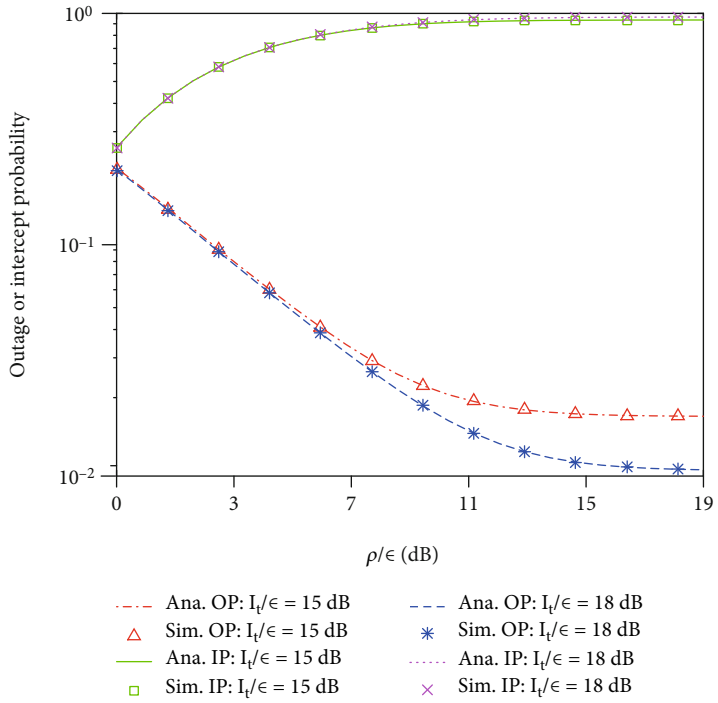

Figure 8: IP and OP versus ρ/ε.

because of the factor $(1-\alpha)/2$ before the logarithm in (14). Accordingly, α can be optimally adopted to balance the durations of energy scavenging and data transmission stages for the best reliability. Interestingly, the security is enhanced with increasing α. Some reasons lead to this observation as follows. Firstly, increasing α reduces the channel capacities at E, which can be explained as above. Secondly, although increasing α helps R collect more energy, E suffers the increase of the jamming power from R, eventually reducing the IP. Moreover, the IP reduces to zero for large α. This is because large α makes the inequality $\widetilde{\Gamma}_e \geq \max([1-\lambda]/\lambda, [1-\beta]/\beta)$ holds where $\widetilde{\Gamma}_e = 2^{2\tilde{\mathscr{R}}_e/(1-\alpha)} - 1$, and hence, the IP reduces to zero according to (29), which is similar to the results in Figure 6. In addition, the security/reliability is degraded/enhanced with the increase in I_t, as anticipated.

Figure 8 exposes the IP/OP versus ρ/ε for $\check{P}_s/\varepsilon = 20$ dB, $\beta = 0.63$, and $\lambda = 0.48$. The results reveal the coincidence between the analysis and the simulation, affirming the correctness of the analytical results. Further, the reliability-security trade-off of the proposed jamming-and-transmitting scheme is observed in this figure. Nonetheless, the reliability gain increases faster than the security loss with increasing the power saturation threshold of the NL energy scavenger ρ, exposing the advantage of both relaying and jamming in our scheme in ensuring high reliability with affordable security threat. Moreover, the starting points at which the IP and the OP start to be saturated are coincident at ρ/ε of approximately 15 dB. That the IP and the OP are saturated at large ρ is because large ρ reduces the NL energy harvester to the linear one. In addition, the security/reliability is degraded/enhanced with the increase in I_t, as anticipated.

5. Conclusion

This paper recommended the simultaneous jamming-and-transmitting scheme for spectrum sharing relaying networks with the nonlinear energy scavenger. Its security and reliability were analyzed and assessed with the intercept and outage probabilities under the IPR and the MTPC. The recommended analysis is validated by multifarious Monte-Carlo simulations. Illustrative results expose that the relay capable of scavenging RF energy enhances drastically the reliability even when the direct secondary source-destination link is unreliable because of bad propagation conditions. Moreover, jamming in both signal transmission phases achieve better security even with increasing transmission power. Additionally, the reliability of the proposed scheme can be optimized with selecting appropriately the time fraction. Notably, the networks can achieve the absolute security with adopting a suitable set of α, β, λ, and $\tilde{\mathscr{R}}_e$. Further, the proposed scheme offers the security-reliability compromise but suffers saturated performance at large maximum transmit/interference power. Furthermore, the reliability/security of the NL-ES is significantly worse/better than that of the L-ES.

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 Tra Vinh University under grant contract number 181/HD.HDKH&DT-DHTV. For the other supports, Khuong Ho-Van 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] N. Shinohara, "Trends in wireless power transfer: WPT technology for energy harvesting, mllimeter-wave/THz rectennas, MIMO-WPT, and advances in near-field WPT applications," *IEEE Microwave Magazine*, vol. 22, no. 1, pp. 46–59, 2021.

[2] F. Benkhelifa, H. ElSawy, J. A. Mccann, and M. S. Alouini, "Recycling cellular energy for self-sustainable IoT networks: a spatiotemporal study," *IEEE Transactions on Wireless Communications*, vol. 19, no. 4, pp. 2699–2712, 2020.

[3] Z. Liang and J. Yuan, "Modelling and prediction of mobile service channel power density for RF energy harvesting," *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 741–744, 2020.

[4] K. Ali and D. J. Rogers, "An orientation-independent multi-input energy harvesting wireless sensor node," *IEEE Transactions on Industrial Electronics*, vol. 68, no. 2, pp. 1665–1674, 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 Internet of Things 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, Article ID 8867148, 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] Z. Ali, G. A. S. Sidhu, M. Waqas, L. Xing, and F. Gao, "A joint optimization framework for energy harvesting based cooperative CR networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 452–462, 2019.

[9] N. I. Miridakis, T. A. Tsiftsis, G. C. Alexandropoulos, and M. Debbah, "Simultaneous spectrum sensing and data reception for cognitive spatial multiplexing distributed systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3313–3327, 2017.

[10] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M. S. Alouini, "On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 2, pp. 192–203, 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. 24819–24828, 2019.

[12] N. I. Miridakis, T. A. Tsiftsis, and G. C. Alexandropoulos, "MIMO underlay cognitive radio: optimized power allocation, effective number of transmit antennas and harvest-transmit tradeoff," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 4, pp. 1101–1114, 2018.

[13] D. Mishra and G. C. Alexandropoulos, "Transmit precoding and receive power splitting for harvested power maximization in MIMO SWIPT systems," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 3, pp. 774–786, 2018.

[14] F. Wang and X. Zhang, "Secure resource allocation for polarization-based non-linear energy harvesting over 5G cooperative CRNs," *IEEE Wireless Communications Letters*, 2020.

[15] 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.

[16] G. Ma, J. Xu, Y.-F. Liu, and M. R. Vedady 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.

[17] 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 Internet of Things Journal*, vol. 8, no. 3, pp. 1702–1715, 2021.

[18] T. X. Vu, S. Chatzinotas, S. Gautam, E. Lagunas, and B. Ottersten, "Joint optimization for PS-based SWIPT multi-user systems with non-linear energy harvesting," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Seoul, Korea, May 2020.

[19] 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.

[20] 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.

[21] 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, Beijing, China, Aug. 2018.

[22] 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.

[23] 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, Kansas City, MO, USA, May 2018.

[24] 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.

[25] Y. Che, Y. Lai, S. Luo, K. Wu, and L. Duan, "UAV-aided information and energy transmissions for cognitive and sustainable 5G networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1668–1683, 2021.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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, Chengdu, China, Dec. 2018.

[31] 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.

[32] 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.

[33] 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, Abu Dhabi, United Arab Emirates, Dec. 2018.

[34] 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.

[35] 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, Nanning, China, Oct. 2020.

[36] Y. Zhang, X.-Q. Jiang, H. Hai, J. Hau, and K. Z. 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, Xi'an, China, Dec. 2019.

[37] 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.

[38] 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.

[39] 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.

[40] A. Prathima, D. S. Gurjar, S. Y. A. Prathima, D. S. Gurjar, and S. Yadav, "Two-way cooperative cognitive radio networks with nonlinear RF-energy harvester," in *2020 IEEE Latin-American Conference on Communications (LATINCOM)*, pp. 1–6, Santo Domingo, Dominican Republic, Nov. 2020.

[41] 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, Kanpur, India, July 2019.

[42] H. Li and X. Zhao, "Throughput maximization with energy harvesting in UAV-assisted cognitive mobile relay networks," *IEEE Transactions Cognitive Communications and Networking*, vol. 7, no. 1, pp. 197–209, 2021.

[43] A. Shome, A. K. Dutta, and S. Chakrabarti, "BER performance analysis of energy harvesting underlay cooperative cognitive radio network with randomly located primary users and secondary relays," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 5, pp. 4740–4752, 2021.

[44] T.-V. Nguyen, T.-N. Tran, K. Shim, T. Huynh-The, and B. An, "A deep-neural-network-based relay selection scheme in wireless-powered cognitive IoT networks," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7423–7436, 2021.

[45] X. Zhang, J. Xing, Z. Yan, Y. Gao, and W. Wang, "Outage performance study of cognitive relay networks with imperfect channel knowledge," *IEEE Communications Letters*, vol. 17, no. 1, pp. 27–30, 2013.

[46] M. Seyfi, S. Muhaidat, and J. Liang, "Relay selection in cognitive radio networks with interference constraints," *IET Communications*, vol. 7, no. 10, article 922930, 2013.

[47] M. Nguyen, N. P. Nguyen, D. B. da Costa, H. K. Nguyen, and R. T. de Sousa, "Secure cooperative half-duplex cognitive radio networks with K-th best relay selection," *IEEE Access*, vol. 5, pp. 6678–6687, 2017.

[48] H. Sun, F. Zhou, R. Q. Hu, and L. Hanzo, "Robust beamforming design in a NOMA cognitive radio network relying on SWIPT," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 142–155, 2019.

[49] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 918–931, 2018.

[50] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2450–2464, 2017.

[51] 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.

[52] R. Zhao, Y. Yuan, L. Fan, and Y. C. He, "Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-m fading channels," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2017.

[53] B. Vucetic and J. Yuan, *Space-Time Coding*, John Wiley & Sons, 2003.

[54] N. T. Thomopoulos, *Essentials of Monte Carlo Simulation: Statistical Methods for Building Simulation Models*, Springer, New York Heidelberg Dordrecht London, 2013.