Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 2109837, 13 pages
https://doi.org/10.1155/2019/2109837

Research Article

Relaying Communications in Energy Scavenging Cognitive Networks: Secrecy Outage Probability Analysis

Khuong Ho-Van [1] **and Thiem Do-Dac** [1,2]

[1] *Ho Chi Minh City University of Technology, VNU-HCM, 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam*
[2] *Thu Dau Mot University, 6 Tran Van On Street, Phu Hoa Ward, Thu Dau Mot City, Binh Duong Province, Vietnam*

Correspondence should be addressed to Khuong Ho-Van; khuong.hovan@yahoo.ca

Received 1 March 2019; Revised 9 April 2019; Accepted 16 April 2019; Published 6 May 2019

Guest Editor: Zoran Stamenkovic

This paper exploits a self-powered secondary relay to not only maintain but also secure communications between a secondary source and a secondary destination in cognitive radio networks when source-destination channel is unavailable. The relay scavenges energy from radio frequency (RF) signals of the primary transmitter and the secondary source and consumes the scavenged energy for its relaying activity. Under the maximum transmit power constraint, Rayleigh fading, the primary outage constraint, and the interference from the primary transmitter, this paper suggests an accurate closed-form expression of the secrecy outage probability to promptly assess the security performance of relaying communications in energy scavenging cognitive networks. The validity of the proposed expression is verified by computer simulations. Numerous results demonstrate the security performance saturation in the range of large maximum transmit power or high required outage probability of primary users. Moreover, the security performance is a function of several system parameters among which the relay's position, the power splitting factor, and the time splitting factor can be optimized to achieve the minimum secrecy outage probability.

1. Introduction

Currently low spectrum utilization efficiency is a great motivation for the application of the cognitive radio technology which enables secondary/unlicensed users to access the allocated spectrum of primary/licensed users in order to better exploit the available spectrum [1]. Cognitive radios operate on three (overlay, underlay, and interweave) mechanisms amidst which the underlay one is more preferable owing to its low system design complexity [2]. According to the underlay mechanism, the transmit power of secondary users (SUs) must be adaptively limited to obey the maximum transmit power constraint imposed by hardware design and the primary outage constraint imposed by communication reliability of primary users (PUs) [3]. These power constraints set the upper-bound on the power of secondary transmitters, inflicting unreliable communication through the direct channel between a secondary source and a secondary destination. Another reason for unreliable communication through the direct channel is the blockage of this channel owing to heavy path-loss, severe fading, and strong shadowing. A secondary relay between the source and the destination should be exploited to reduce the path-loss for hop-to-hop communication, mitigate severe fading and strong shadowing, and relax the requirement of high transmit power for long distance communication. Therefore, the relay can bridge the source with the destination in order to maintain reliable connection between them [4]. Nevertheless, as a helper, the relay may be unenthusiastic to utilize its private energy for assistance activity. Currently modern technologies make feasible for self-powered terminals that can scavenge energy with high energy conversion efficiency from green energy sources (e.g., radio frequency signals [5, 6]). Consequently, the relay can utilize its scavenged energy to lengthen the transmission range of the source, better remaining the continuous connection between the source and the destination. However, the scavenged energy may be insufficient, and, hence, the problem is whether the relay can guarantee reliable and secure communication between the source and the destination under the threat

of eavesdroppers in the information-theoretic aspect. This aspect confirms that wireless communication is secured when the capacity difference between the desired channel and the wiretap channel is positive [7]. This paper finds the solution to such a problem.

1.1. Literature Review. This subsection merely surveys published works related to security performance analysis for relaying communications in energy scavenging cognitive networks. Therefore, published works which did not reflect a complete set of specifications such as power constraints for SUs, security performance analysis, relaying communications, and energy scavenging should not be surveyed (e.g., [8–13] merely dealt with the security performance analysis for direct communications (i.e., without relaying) in energy scavenging cognitive networks). Through this survey, contributions of the current paper will be summarized in the next subsection.

The authors in [14] exploited the secondary relay between the secondary source and the secondary destination to not only expand the transmission range of the source but also secure its communication. The system model in [14] considered the decode-and-forward relay, the power splitting based energy scavenging mechanism which allows the relay to scavenge energy from the signals of both the secondary source and the primary transmitter, the maximum transmit power constraint, the interference power constraint, and the interference from the primary transmitter to the relay. Nevertheless, [14] neglected the interference from the primary transmitter to the secondary destination and the eavesdropper. The authors in [15] studied the same problem as [14] but with three different points: (i) the amplify-and-forward relay is used; (ii) the time splitting based energy scavenging mechanism allows the relay to scavenge energy from only the signal of the secondary source; (iii) the interference from the primary transmitter is ignored. To improve the security performance, [16] extended [15] with allowing both the source and the relay to jam the eavesdropper. The authors in [17] continued to expand the work in [16] with relay selection for more secure information transmission. As an alternative approach to enhance the security performance, [18] proposed a path selection scheme where the path with the highest end-to-end channel capacity is selected. The system model in [18] ignored interference from PUs and allowed the relays to scavenge the energy from the signals of dedicated beacons based on the time splitting mechanism. Nevertheless, [18] merely analyzed the connection outage probabilities (the connection outage probability is the probability that the received signal-to-noise ratio is below a threshold) at the destination and the eavesdropper.

In summary, [14–18] considered relaying communications in energy scavenging cognitive networks. However, they neglected the secrecy outage analysis (i.e., only simulation results are provided in [14–18]), the primary outage constraint, and the interference from the primary transmitter to all secondary receivers. This paper will complement their shortcomings to complete the framework of the secrecy outage analysis for relaying communications in energy scavenging cognitive networks.

1.2. Contributions. This paper extends the system model in [14–18] with noticeable differences as follows:

(i) The decode-and-forward relay is activated merely when it can exactly restore the source information. This limits the error propagation (e.g., [14])

(ii) The relay exploits the interference from the primary transmitter for energy scavenging. This is helpful in turning unwanted signals to useful energy source and differs from [15–18] where the interference from the primary transmitter is not exploited for energy scavenging

(iii) Periods of two (energy scavenging and information processing) stages are unequal. This facilitates optimizing these periods for minimum secrecy outage probability (SOP). Also, this makes our work distinguished from [14–16] where these stages are of equal times

(iv) This paper proposes the accurate closed-form SOP analysis, which differs from [14–18] in which only simulation results are presented

The contributions of the paper are highlighted as follows:

(i) Exploit a secondary relay to guarantee secure communications between the secondary source and the secondary destination in case that their direct communication is in outage. The relay is capable of scavenging the energy from both signals of the secondary source and the primary transmitter. Also, it must be successful in restoring the source information before taking part in the relaying activity

(ii) Suggest accurate closed-form expressions for crucial security performance metrics such as the SOP, the probability of strictly positive secrecy capacity (PSPSC), the intercept probability (IP) under both maximum transmit power constraint and primary outage constraint, and interference from the primary transmitters to promptly evaluate the security performance of relaying communications in energy scavenging cognitive networks without time-consuming computer simulations

(iii) Employ the suggested expressions to optimize important system parameters

(iv) Provide numerous results to obtain helpful insights into security performance such as the security performance saturation in the range of large maximum transmit power or high required outage probability of PUs and the minimum secrecy outage probability achievable with appropriate selection of the relay's position, the time splitting factor, and the power splitting factor

1.3. Structure of Paper. The paper continues as follows. System model, signal model, secrecy capacity, and secondary power allocation are described in the next section. Section 3 details the derivation of important performance metrics such as the SOP, the PSPSC, and the IP. Section 4 presents

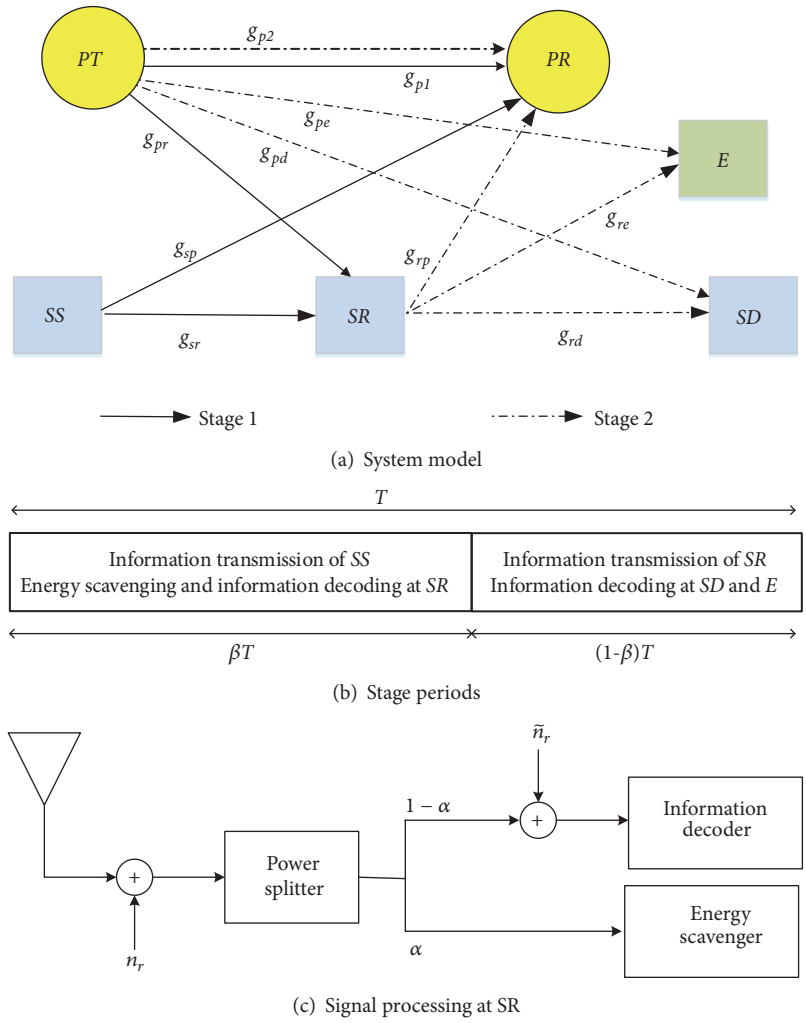

FIGURE 1: System model.

simulated/numerical results and Section 5 concludes the paper.

2. System Model, Signal Model, Secrecy Capacity, and Secondary Power Allocation

2.1. System Model. Figure 1(a) illustrates relaying communications in energy scavenging cognitive networks. Relaying communications experience two stages as shown in Figure 1(b).

In stage 1, both the secondary source *SS* and the primary transmitter *PT* simultaneously broadcast their own information to the secondary destination *SD* and the primary receiver *PR*, respectively, causing mutual interference signals between the secondary network and the primary network. The interference signals from the secondary network to the primary network are considered in most published works while those from the primary network to the secondary network are usually neglected (e.g., [19–21] and references therein). Therefore, by considering these mutual interference signals, our work is apparently more general than the existing ones but the secrecy outage probability analysis is more sophisticated. The eavesdropper *E* intends to wire-tap the secondary source's information. Owing to heavy path-loss, severe fading, and large shadowing, the secondary source's signals cannot reach *SD* and *E*. As such, it is supposed that the secondary relay *SR* is in the radio coverage of *SS* and eager to assist *SS* by forwarding *SS*'s information to *SD* according to the decode-and-forward principle. *SR* is a self-powered terminal for its relaying operation which is capable of scavenging the energy from the received signals according to the power splitting method (e.g., [22, 23]) as observed in Figure 1(c). More specifically, *SR* scavenges the energy from the RF signals of both *SS* and *PT*. This means that *SR* takes advantage of the interference signal (from *PT*) for useful purpose of energy scavenging. The power splitting method divides the received signal at *SR* into two parts: one part for recovering the source information (it is supposed that the information decoder consumes the negligible amount of the energy, which is commonly assumed in most existing publications (e.g., [8–14] and references therein)) and the other for scavenging the energy.

In stage 2, *SR* is idle if it fails to restore the source information. Otherwise, it forwards the restored source information to *SD* in parallel to the information transmission of *PT*. At the end of stage 2, *SD* tries to recover while *E* eavesdrops the source information from *SR*'s transmit signal.

2.2. Signal Model. In Figure 1(a), $g_{\mathtt{ab}} \in \{g_{p1}, g_{p2}, g_{pe}, g_{pd}, g_{pr}, g_{sp}, g_{sr}, g_{rp}, g_{re}, g_{rd}\}$ denotes the channel coefficient between a corresponding pair of the transmitter and the receiver. Although Figure 1(a) only shows one primary transmitter-receiver pair, the realistic scenario may have two pairs communicating in two stages. To reflect such a scenario, two different channel coefficients, g_{p1} and g_{p2}, are used to represent two different channels for two primary transmitter-receiver pairs in two stages. All frequency nonselective independent Rayleigh fading channels are supposed, producing the zero-mean $\kappa_{\mathtt{ab}}$-variance circular symmetric complex Gaussian distribution for $g_{\mathtt{ab}}$, i.e., $g_{\mathtt{ab}} \sim \mathcal{CN}(0, \kappa_{\mathtt{ab}})$. When the path-loss is accounted, $\kappa_{\mathtt{ab}}$ can be represented as $\kappa_{\mathtt{ab}} = l_{\mathtt{ab}}^{-\nu}$, with $l_{\mathtt{ab}}$ denoting the transmitter a-receiver b distance, and ν denoting the path-loss exponent. As such, it is implicit in the sequel that the probability density function (pdf) and the cumulative distribution function (cdf) of the channel gain $|g_{\mathtt{ab}}|^2$ are, respectively, given by

$$f_{|g_{\mathtt{ab}}|^2}(x) = \frac{e^{-x/\kappa_{\mathtt{ab}}}}{\kappa_{\mathtt{ab}}}, \tag{1}$$

$$F_{|g_{\mathtt{ab}}|^2}(x) = 1 - e^{-x/\kappa_{\mathtt{ab}}}, \tag{2}$$

where $x \geq 0$.

In Figure 1(b), β with $\beta \in (0, 1)$ and T correspondingly denote the time splitting factor and the total transmission time from *SS* to *SD* through *SR*. In Figure 1(c), α with $\alpha \in (0, 1)$ denotes the power splitting factor. With the notations in Figure 1 in mind, the signals are modelled as follows.

By denoting u_s and u_{p1} as the unity-power transmit symbols of *SS* and *PT* in stage 1, correspondingly, the received signals at *SR* and *PR* can be, respectively, represented as

$$v_r = g_{sr}\sqrt{P_s}u_s + g_{pr}\sqrt{P_{p1}}u_{p1} + n_r, \tag{3}$$

$$v_{p1} = g_{sp}\sqrt{P_s}u_s + g_{p1}\sqrt{P_{p1}}u_{p1} + n_{p1}, \tag{4}$$

where $n_r \sim \mathcal{CN}(0, \varrho_r^2)$ and $n_{p1} \sim \mathcal{CN}(0, \varrho_{p1}^2)$ are the additive white Gaussian noises (AWGN) produced by the receive antennas at *SR* and *PR*, respectively; P_s and P_{p1} are the transmit powers of *SS* and *PT* in stage 1, respectively.

Based on the operation principle in Figure 1(c), the relay *SR* partitions the received signal v_r into two parts: the first part of $\sqrt{\alpha}v_r$ input to the energy scavenger and the second part of $\sqrt{1-\alpha}v_r$ input to the information decoder. Given the energy conversion efficiency of the energy scavenger as μ with $\mu \in (0, 1)$, the average amount of the energy which *SR* can scavenge in stage 1 is given by

$$\begin{aligned} W_{rm} &= \mu \mathrm{E}\left\{\left|\sqrt{\alpha}v_r\right|^2\right\}\beta T \\ &= \mu\alpha\left(P_s\kappa_{sr} + P_{p1}\kappa_{pr} + \varrho_r^2\right)\beta T, \end{aligned} \tag{5}$$

where $\mathrm{E}\{\cdot\}$ denotes the statistical average.

The maximum transmit power which *SR* can use for information transmission in stage 2 is given by

$$P_{rm} = \frac{W_{rm}}{(1-\beta)T} = \frac{\beta\mu\alpha}{1-\beta}\left(P_s\kappa_{sr} + P_{p1}\kappa_{pr} + \varrho_r^2\right). \tag{6}$$

The signal input to the information decoder in Figure 1(c) can be expressed as

$$\tilde{v}_r = \sqrt{1-\alpha}v_r + \tilde{n}_r, \tag{7}$$

where $\tilde{n}_r \sim \mathcal{CN}(0, \tilde{\varrho}_r^2)$ is the noise produced by the passband-to-baseband signal converter.

Plugging (3) into (7) results in $\tilde{v}_r = \sqrt{(1-\alpha)P_s}g_{sr}u_s + \sqrt{(1-\alpha)P_{p1}}g_{pr}u_{p1} + \sqrt{1-\alpha}n_r + \tilde{n}_r$ from which the SINR (Signal-to-Interference plus Noise Ratio) at the input of the information decoder can be represented as

$$\begin{aligned} \varphi_{sr} &= \frac{(1-\alpha)P_s\left|g_{sr}\right|^2}{(1-\alpha)P_{p1}\left|g_{pr}\right|^2 + (1-\alpha)\varrho_r^2 + \tilde{\varrho}_r^2} \\ &= \frac{P_s\left|g_{sr}\right|^2}{P_{p1}\left|g_{pr}\right|^2 + \hat{\varrho}_r^2}, \end{aligned} \tag{8}$$

where

$$\hat{\varrho}_r^2 = \varrho_r^2 + \frac{\tilde{\varrho}_r^2}{1-\alpha}. \tag{9}$$

Then, the channel capacity which *SR* achieves in stage 1 is $C_{sr} = \beta\log_2(1+\varphi_{sr})$ bps/Hz where the prelog factor of β is because the period of stage 1 is βT. According to the communication theory, *SR* can restore the source information when its channel capacity is higher than the required spectral efficiency of SUs, C_1, i.e., $C_{sr} \geq C_1$. In order words, u_s is successfully recovered at *SR* if $\varphi_{sr} \geq \varphi_1$ where $\varphi_1 = 2^{C_1/\beta} - 1$.

In stage 2, *SR* transmits the recovered source symbol u_r with the transmit power P_r if it can successfully restore the source information (i.e., $\varphi_{sr} \geq \varphi_1$ and $u_r = u_s$). Otherwise, it keeps idle. The information transmission of *SR* is in parallel to that of *PT*. As such, *SD*, *E*, and *PR* correspondingly receive the following signals:

$$v_{rd} = \begin{cases} g_{rd}\sqrt{P_r}u_r + g_{pd}\sqrt{P_{p2}}u_{p2} + n_d, & \varphi_{sr} \geq \varphi_1 \\ g_{pd}\sqrt{P_{p2}}u_{p2} + n_d, & \varphi_{sr} < \varphi_1, \end{cases} \tag{10}$$

$$v_{re} = \begin{cases} g_{re}\sqrt{P_r}u_r + g_{pe}\sqrt{P_{p2}}u_{p2} + n_e, & \varphi_{sr} \geq \varphi_1 \\ g_{pe}\sqrt{P_{p2}}u_{p2} + n_e, & \varphi_{sr} < \varphi_1, \end{cases} \tag{11}$$

$$v_{rp} = \begin{cases} g_{rp}\sqrt{P_r}u_r + g_{p2}\sqrt{P_{p2}}u_{p2} + n_{p2}, & \varphi_{sr} \geq \varphi_1 \\ g_{p2}\sqrt{P_{p2}}u_{p2} + n_{p2}, & \varphi_{sr} < \varphi_1, \end{cases} \tag{12}$$

where $n_d \sim \mathcal{CN}(0, \varrho_d^2)$, $n_e \sim \mathcal{CN}(0, \varrho_e^2)$, and $n_{p2} \sim \mathcal{CN}(0, \varrho_{p2}^2)$ are the noises produced by the receive antennas at

SD, *E*, and *PR*, correspondingly; P_{p2} and u_{p2} are, respectively, the transmit power and the unity-power transmit symbol of *PT* in stage 2. That (P_{p1}, u_{p1}) differs from (P_{p2}, u_{p2}) reflects the realistic scenario where two different primary transmitter-receiver pairs may communicate in two stages.

2.3. Secrecy Capacity. The SINRs at *SD* and *E* can be achieved from (10) and (11) as

$$\varphi_{rd} = \begin{cases} \dfrac{P_r \left|g_{rd}\right|^2}{P_{p2}\left|g_{pd}\right|^2 + \varrho_d^2}, & \varphi_{sr} \geq \varphi_1 \\ 0, & \varphi_{sr} < \varphi_1, \end{cases} \tag{13}$$

$$\varphi_{re} = \begin{cases} \dfrac{P_r \left|g_{re}\right|^2}{P_{p2}\left|g_{pe}\right|^2 + \varrho_e^2}, & \varphi_{sr} \geq \varphi_1 \\ 0, & \varphi_{sr} < \varphi_1. \end{cases} \tag{14}$$

Then, *SD* and *E* obtain channel capacities correspondingly as [24]

$$C_{rd} = (1-\beta)\log_2(1+\varphi_{rd}), \tag{15}$$

$$C_{re} = (1-\beta)\log_2(1+\varphi_{re}), \tag{16}$$

where the prelog factor of $1-\beta$ is because the time of stage 2 is $(1-\beta)T$.

The secrecy capacity of relaying communications in energy scavenging cognitive networks, which is the difference between the channel capacities of the trusted channel (from *SR* to *SD*) and the wiretap channel (from *SR* to *E*), is expressed as [7]

$$\begin{aligned} \mathscr{C}_{sec} &= \left[C_{rd} - C_{re}\right]^+ \\ &= \begin{cases} (1-\beta)\left[\log_2 \dfrac{1+\varphi_{rd}}{1+\varphi_{re}}\right]^+, & \varphi_{sr} \geq \varphi_1 \\ 0, & \varphi_{sr} < \varphi_1, \end{cases} \end{aligned} \tag{17}$$

where $[x]^+$ denotes $\max(x, 0)$.

2.4. Secondary Power Allocation. The SINR at *PR* in stage 1 is computed from (4) as

$$\varphi_{p1} = \frac{P_{p1}\left|g_{p1}\right|^2}{P_s\left|g_{sp}\right|^2 + \varrho_{p1}^2}. \tag{18}$$

Then, the channel capacity that *PR* achieves in stage 1 is

$$C_{p1} = \beta \log_2\left(1+\varphi_{p1}\right). \tag{19}$$

Similarly, the SINR at *PR* in stage 2 is computed from (12) as

$$\varphi_{p2} = \begin{cases} \dfrac{P_{p2}\left|g_{p2}\right|^2}{P_r\left|g_{rp}\right|^2 + \varrho_{p2}^2}, & \varphi_{sr} \geq \varphi_1 \\ \dfrac{P_{p2}\left|g_{p2}\right|^2}{\varrho_{p2}^2}, & \varphi_{sr} < \varphi_1 \end{cases} \tag{20}$$

and the channel capacity that *PR* achieves in stage 2 is

$$C_{p2} = (1-\beta)\log_2\left(1+\varphi_{p2}\right). \tag{21}$$

Because the secondary transmitters (*SS* and *SR*) opportunistically access the spectrum of the primary users, their transmit powers must be limited such that the outage probability of the primary receiver is below a certain threshold λ. More specifically, P_s and P_r must be constrained by

$$\Pr\left\{C_{p1} \leq C_2\right\} \leq \lambda, \tag{22}$$

$$\Pr\left\{C_{p2} \leq C_2\right\} \leq \lambda, \tag{23}$$

where C_2 is the required spectral efficiency of *PR*.

Constraints in (22) and (23) are, namely, the primary outage constraints.

The transmit powers of *SS* and *SR* must be also limited by their maximum transmit powers, P_{sm} and P_{rm}, respectively, which are determined by the hardware implementation and the energy scavenger, correspondingly. Therefore, P_s and P_r are upper-bounded by

$$P_s \leq P_{sm}, \tag{24}$$

$$P_r \leq P_{rm}. \tag{25}$$

Constraints in (24) and (25) are, namely, the maximum transmit power constraints.

Transmit power constraints for P_s in (22) and (24) result in

$$P_s = \min\left(\frac{P_{p1}\kappa_{p1}}{\varphi_{21}\kappa_{sp}}\left[\frac{1}{1-\lambda}e^{-\varphi_{21}\varrho_{p1}^2/P_{p1}\kappa_{p1}} - 1\right]^+, P_{sm}\right), \tag{26}$$

where $\varphi_{21} = 2^{C_2/\beta} - 1$.

Similarly, transmit power constraints for P_r in (23) and (25) result in

$$P_r = \min\left(\frac{P_{p2}\kappa_{p2}}{\varphi_{22}\kappa_{rp}}\left[\frac{1}{1-\lambda}e^{-\varphi_{22}\varrho_{p2}^2/P_{p2}\kappa_{p2}} - 1\right]^+, P_{rm}\right), \tag{27}$$

where $\varphi_{22} = 2^{C_2/(1-\beta)} - 1$.

In (26) and (27), κ_{p1} and κ_{p2} represent the fading powers of the channels between the primary transmitter and the primary receiver in stage 1 and stage 2, respectively.

The derivation of (26) follows [25, eq. (18)] while the derivation of (27) follows [25, eq. (20)] with a note that (27) is obtained with φ_{p2} in the case that *SR* is active (i.e., $\varphi_{sr} \geq \varphi_1$). The case that *SR* is idle is of no interest because the source information cannot reach the secondary destination.

3. SOP Analysis

The SOP is a crucial performance metric in assessing information security of wireless communications in the information-theoretic aspect. It is defined as the probability that the secrecy capacity $\mathscr{C}_{sec}$ does not reach a required security degree $\overline{C}_3$. As such, the smaller the SOP is, the more

secure the wireless communication is. In this section, the SOP of relaying communications in energy scavenging cognitive networks is derived in closed form, which facilitates not only evaluating security performance without exhaustive simulations but also inferring other crucial security performance metrics such as the IP and the PSPSC.

The SOP of relaying communications in energy scavenging cognitive networks is given by

$$\Upsilon\left(\overline{C}_3\right) = \Pr\left\{\mathscr{C}_{\text{sec}} < \overline{C}_3\right\}, \tag{28}$$

where $\Pr\{\mathscr{V}\}$ is the probability of the event $\mathscr{V}$.

Since $\mathscr{C}_{\text{sec}}$ is nonnegative when $\varphi_{sr} \geq \varphi_1$ as seen in (17), one can decompose (28) into two cases as

$$\begin{aligned}\Upsilon\left(\overline{C}_3\right) = \Pr&\left\{(1-\beta)\left[\log_2\left(\frac{1+\varphi_{rd}}{1+\varphi_{re}}\right)\right]^+ < \overline{C}_3 \mid \varphi_{sr}\right.\\ &\left.\geq \varphi_1\right\}\Pr\left\{\varphi_{sr} \geq \varphi_1\right\} + \Pr\left\{0 < \overline{C}_3 \mid \varphi_{sr} < \varphi_1\right\}\\ &\cdot \Pr\left\{\varphi_{sr} < \varphi_1\right\}.\end{aligned} \tag{29}$$

Because the required security degree $\overline{C}_3$ is positive, (29) is rewritten as

$$\begin{aligned}&\Upsilon\left(\overline{C}_3\right)\\ &= \underbrace{\Pr\left\{\left[\log_2\left(\frac{1+\varphi_{rd}}{1+\varphi_{re}}\right)\right]^+ < \frac{\overline{C}_3}{1-\beta} \mid \varphi_{sr} \geq \varphi_1\right\}}_{\mathscr{I}_1}\underbrace{\Pr\left\{\varphi_{sr} \geq \varphi_1\right\}}_{1-\mathscr{I}_2}\\ &\quad + \underbrace{\Pr\left\{\varphi_{sr} < \varphi_1\right\}}_{\mathscr{I}_2}.\end{aligned} \tag{30}$$

Theorem 1. *The accurate closed-form representation of $\mathscr{I}_1$ is given by*

$$\begin{aligned}\mathscr{I}_1 = {}& CD\Psi(D,C) + C\Phi(D,C) + \frac{e^{(1-2^{C_3})B}AC}{2^{C_3}(C-G)}\\ &\cdot \Phi\left(2^{C_3}B + D, C\right)\\ &+ \frac{e^{(1-2^{C_3})B}AC}{2^{C_3}(C-G)}\left(D + \frac{1}{C-G}\right)\\ &\cdot \left[\Psi\left(2^{C_3}B + D, C\right) - \Psi\left(2^{C_3}B + D, G\right)\right],\end{aligned} \tag{31}$$

where

$$A = \frac{\kappa_{rd}P_r}{\kappa_{pd}P_{p2}}, \tag{32}$$

$$B = \frac{\varrho_d^2}{\kappa_{rd}P_r}, \tag{33}$$

$$C = \frac{\kappa_{re}P_r}{\kappa_{pe}P_{p2}}, \tag{34}$$

$$D = \frac{\varrho_e^2}{\kappa_{re}P_r}, \tag{35}$$

$$G = 1 + 2^{-C_3}(A-1), \tag{36}$$

$$\Psi(a,b) = -e^{ab}Ei(-ab), \tag{37}$$

$$\Phi(a,b) = \frac{1}{b} + ae^{ab}Ei(-ab), \tag{38}$$

$$C_3 = \frac{\overline{C}_3}{1-\beta}, \tag{39}$$

with $Ei(\cdot)$ being the exponential integral in [26].

Proof. Please refer to Appendix. □

Theorem 2. *The accurate closed-form representation of $\mathscr{I}_2$ is given by*

$$\mathscr{I}_2 = 1 - U\frac{e^{-V\varphi_1}}{\varphi_1 + U}, \tag{40}$$

where

$$U = \frac{\kappa_{sr}P_s}{\kappa_{pr}P_{p1}}, \tag{41}$$

$$V = \frac{\widetilde{\varrho}_r^2}{\kappa_{sr}P_s}. \tag{42}$$

Proof. By imitating the derivation of (A.5) in the Appendix, it is easy to see that $\mathscr{I}_2$ is the cdf of φ_{sr} evaluated at φ_1. Therefore, $\mathscr{I}_2$ can be represented as (40), completing the proof. □

Plugging (31) and (40) into (30), one obtains the accurate closed-form expression of the SOP for relaying communications in energy scavenging cognitive networks as $\Upsilon(\overline{C}_3) = \mathscr{I}_1(1-\mathscr{I}_2) + \mathscr{I}_2$. This expression is useful to quickly evaluate the security performance without exhaustive simulations. To the best of the authors' understanding, this expression is newly reported. Moreover, some crucial security performance metrics (e.g., the IP or the PSPSC) can be easily derived from this expression. More specifically, the IP refers to the probability that the secrecy capacity is negative [27], i.e.,

$$\Theta = \Pr\left\{\mathscr{C}_{sec} < 0\right\} = \Upsilon(0). \tag{43}$$

Table 1: Simulation parameters.

PARAMETER	VALUE
Path-loss exponent	$\nu = 4$
Energy conversion efficiency	$\mu = 0.9$
Coordinate of *SS*	*SS* at (0.0, 0.0)
Coordinate of *SD*	*SD* at (1.0, 0.0)
Coordinate of *PT*	*PT* at (0.2, 0.8)
Coordinate of *PR*	*PR* at (0.9, 0.7)
Coordinate of *E*	*E* at (1.0, 0.4)
Coordinate of *SR*	*SR* at (d, 0.0)

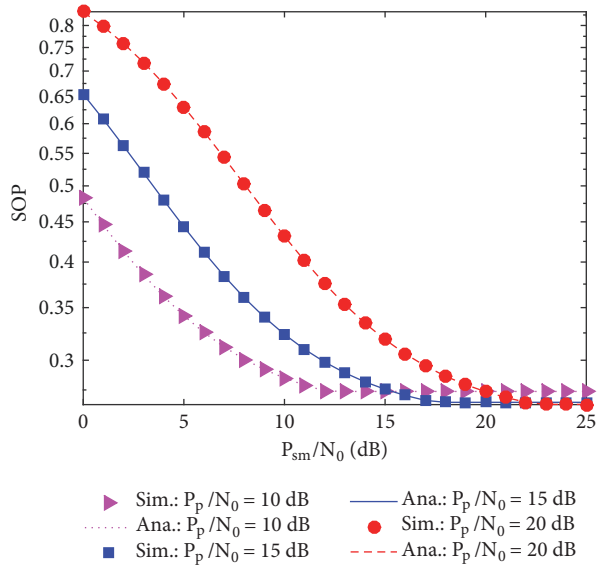

Figure 2: SOP versus P_{sm}/N_0. "Sim." and "Ana." represent "Simulation" and "Analysis," respectively.

Additionally, the PSPSC refers to the probability that the secrecy capacity is strictly positive, i.e.,

$$\Omega = \Pr\{\mathscr{C}_{sec} > 0\} = 1 - \Pr\{\mathscr{C}_{sec} < 0\} = 1 - \Upsilon(0). \quad (44)$$

4. Results and Discussions

Simulated/numerical results in this section are collected to assess the security performance of relaying communications in energy scavenging cognitive networks in terms of the SOP through typical parameters. Numerical results are produced by (30) while simulated ones are generated by Monte-Carlo simulation with 10^7 channel realizations. Without loss of generality, equal noise variances are supposed (i.e., $\varrho_{p1}^2 = \varrho_{p2}^2 = \varrho_d^2 = \varrho_e^2 = \varrho_r^2 = \widetilde{\varrho}_r^2 = N_0$) and only one primary transmitter-receiver pair is considered (i.e., $\kappa_{p1} = \kappa_{p2} = \kappa_{pp}$ and $P_{p1} = P_{p2} = P_p$). Simulation parameters under investigation are specified in Table 1.

Figure 2 shows the SOP versus the maximum transmit power-to-noise variance ratio P_{sm}/N_0 for $d = 0.5$, $\lambda = 0.1$, $C_1 = 0.2$ bps/Hz, $C_2 = 0.3$ bps/Hz, $\overline{C}_3 = 0.1$ bps/Hz, $\alpha = 0.8$, $\beta = 0.6$, and $P_p/N_0 = 10, 15, 20$ dB. This figure verifies the accuracy of (30) due to the exact agreement between the analysis and the simulation. Additionally, the SOP decreases with increasing P_{sm}/N_0. This is attributed to the fact that increasing P_{sm}/N_0 offers *SR* more opportunities to correctly recover the source information and to scavenge more energy from the RF signals of *SS*, eventually decreasing the outage probability in stage 2. Nevertheless, the SOP suffers the error floor in the range of high P_{sm}/N_0. This error floor originates from the power allocation mechanism for *SS* and *SR* (please recall (26) and (27)) where *SS* and *SR* transmit signals with powers independent of P_{sm}/N_0 in the range of large P_{sm}/N_0 (i.e., the maximum transmit power constraint is ignored when P_{sm}/N_0 is large), resulting in the constant SOP. Furthermore, the SOP increases with increasing P_p/N_0. This is because increasing the power of the primary transmitter inflicts more interference to secondary receivers which cannot be compensated by the increase in the energy of *SR* scavenged from the transmit signals of *PT*. However, when P_{sm}/N_0 is greater than a certain value, the SOP decreases with increasing P_p/N_0. For example, when P_{sm}/N_0 is greater than 15.5 dB, the SOP with $P_p/N_0 = 10$ dB is larger than the SOP with $P_p/N_0 = 15$ dB. This can be explained as follows. When P_{sm}/N_0 is greater than a certain value, the transmit power of *SS* is large according to (26). Therefore, the relay can scavenge more energy from the transmit signal of *SS* according to (6). This increases the transmit power of the relay according to (27), which can better compensate for more interference from the primary transmitter due to larger value of P_p/N_0, ultimately reducing the SOP.

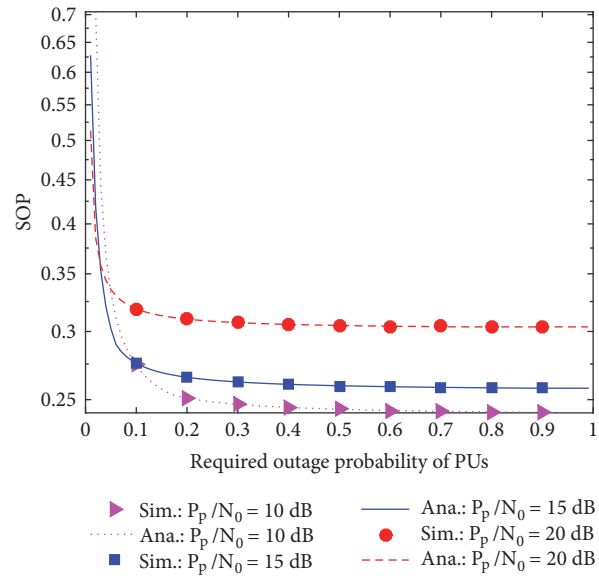

Figure 3: SOP versus λ.

Figure 3 demonstrates the SOP versus the required outage probability of PUs, λ, for $P_{sm}/N_0 = 15$ dB, $d = 0.5$, $\alpha = 0.8$, $\beta = 0.6$, $C_1 = 0.2$ bps/Hz, $C_2 = 0.3$ bps/Hz, $\overline{C}_3 = 0.1$ bps/Hz, and $P_p/N_0 = 10, 15, 20$ dB. This figure validates (30) due to the match between the simulation and the analysis. Moreover, increasing the required outage probability of PUs

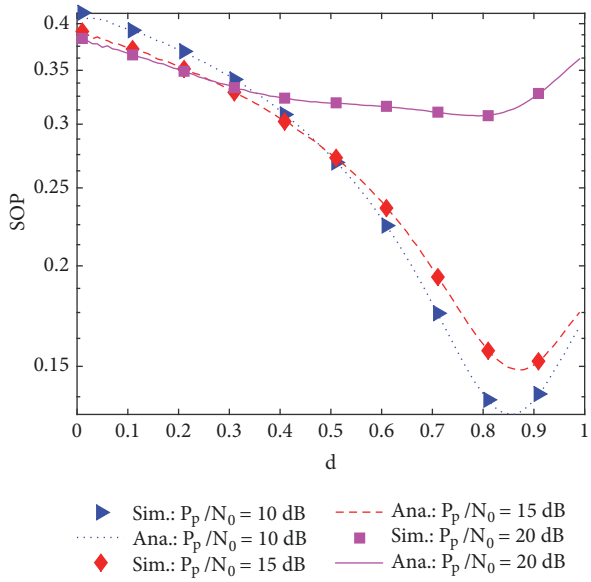

FIGURE 4: SOP versus the relay's position.

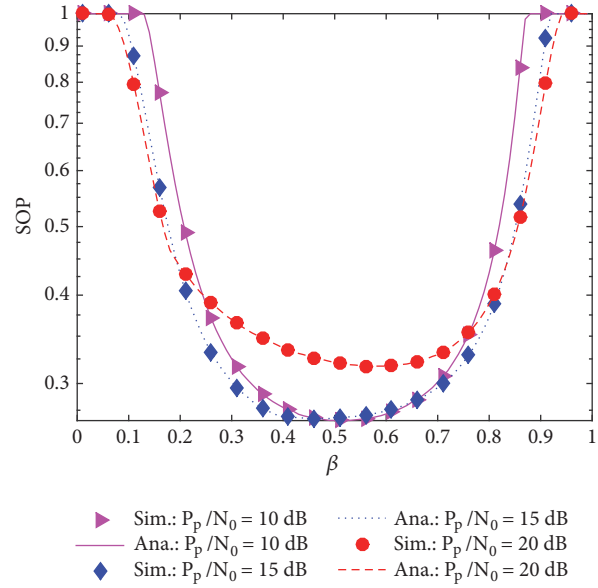

FIGURE 5: SOP versus the time splitting factor.

decreases the SOP. This is because such an increase allows PUs to tolerate more interference from SUs. Therefore, SUs can transmit signals with higher powers, eventually reducing the outage in stage 2. Nevertheless, the SOP is saturated in the range of large λ (e.g., $\lambda > 0.5$). Such a SOP saturation is because of the power allocation mechanism in (26) and (27) where the second term in P_s (or P_r) is independent of λ. Therefore, P_s (or P_r) is constant for large values of λ at which the first term dominates the second term in P_s (or P_r), causing the error floor in the SOP. Furthermore, the SOP saturation level increases with increasing P_p/N_0. This can be comprehended from increasing the interference on SUs when P_p/N_0 increases.

Figure 4 shows the SOP versus the relay's position (i.e., d) for $P_{sm}/N_0 = 15$ dB, $\beta = 0.6$, $\lambda = 0.1$, $\alpha = 0.8$, $C_1 = 0.2$ bps/Hz, $C_2 = 0.3$ bps/Hz, $\overline{C}_3 = 0.1$ bps/Hz, and $P_p/N_0 = 10, 15, 20$ dB. This figure confirms the validity of (30) due to the exact agreement between the simulation and the analysis. We are reminded that the secrecy outage event occurs as R cannot successfully recover the source information (i.e., SS is distant from SR) or SR cannot reliably send the decoded source information to SD (i.e., SD is distant from SR). As such, it is obvious that there is always an existence of the relay's optimum position, which optimally trades off the probability that SR can correctly restore the source information with the probability that SR can reliably send the decoded source information to SD to minimize the SOP. Figure 4 confirms this fact which achieves the minimum SOP as SR is $d_{opt} = 0.86, 0.87, 0.79$ distant from SS for $P_p/N_0 = 10, 15, 20$ dB, respectively. Moreover, the minimum SOP corresponding to the relay's optimum position increases with increasing the interference from PUs (i.e., increasing P_p/N_0) as expected. However, when d is smaller than a certain value, the SOP decreases with increasing P_p/N_0. For instance, when d is smaller than 0.48, the SOP with $P_p/N_0 =$ 10 dB is larger than the SOP with $P_p/N_0 = 15$ dB. This can be interpreted as follows. When d is smaller than a certain value (i.e., SR is nearer to SS), SR can correctly decode the source information with a higher probability and scavenge more energy from the transmit signal of SS. This increases the transmit power of the relay, which can better compensate for more interference from the primary transmitter due to larger value of P_p/N_0, ultimately reducing the SOP.

Figure 5 illustrates the SOP versus β for $d = 0.5$, $P_{sm}/N_0 = 15$ dB, $\lambda = 0.1$, $\alpha = 0.5$, $C_1 = 0.2$ bps/Hz, $C_2 = 0.3$ bps/Hz, $\overline{C}_3 = 0.1$ bps/Hz, and $P_p/N_0 = 10, 15, 20$ dB. This figure validates (30) because the simulation perfectly matches the analysis. In addition, there exist optimum values of β (e.g., $\beta_{opt} = 0.51, 0.46, 0.56$ for $P_p/N_0 = 10, 15, 20$ dB, correspondingly as shown in Figure 5) for the minimum SOPs. The existence of β_{opt} can be interpreted as follows. Increasing β prolongs the period of stage 1, and thus, SR can scavenge more energy and correctly restore the source information with a higher probability. Nevertheless, increasing β can also mitigate the secrecy capacity in stage 2, and thus, the SOP increases. Consequently, β should be selected to optimally compromise the periods of two stages for the minimum SOP. Furthermore, the minimum SOP corresponding to the optimum value of β increases with P_p/N_0 as expected. However, when β is outside a certain range, the SOP decreases with increasing P_p/N_0. For instance, when β is outside $[0.47, 0.66]$, the SOP with $P_p/N_0 = 10$ dB is larger than the SOP with $P_p/N_0 = 15$ dB. This can be interpreted as follows. The value of β affects the required SINRs of PR (i.e., $\varphi_{21} = 2^{C_2/\beta} - 1$ and $\varphi_{22} = 2^{C_2/(1-\beta)} - 1$ as seen in (26) and (27)). Therefore, the primary receiver has more chances to obtain the required SINRs when P_p/N_0 increases. Accordingly, it can be more tolerable with the interference from the secondary transmitters. Furthermore, the relay has more chances to scavenge more energy from the transmit

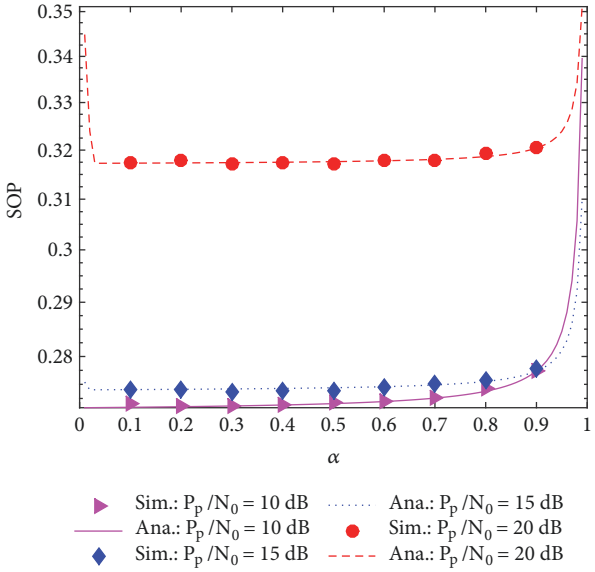

Figure 6: SOP versus the power splitting factor.

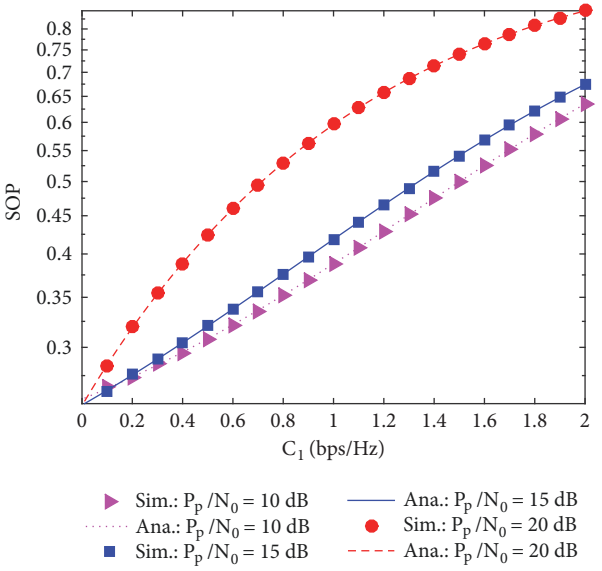

Figure 7: SOP versus the required spectral efficiency of SUs.

signal of PT when P_p/N_0 increases. As such, the relay transmits signals with higher power, which can better compensate for more interference from the primary transmitter due to larger value of P_p/N_0, eventually mitigating the SOP.

Figure 6 demonstrates the SOP versus α for $P_{sm}/N_0 = 15$ dB, $\lambda = 0.1$, $d = 0.5$, $\beta = 0.6$, $C_1 = 0.2$ bps/Hz, $C_2 = 0.3$ bps/Hz, $\overline{C}_3 = 0.1$ bps/Hz, and $P_p/N_0 = 10, 15, 20$ dB. This figure exposes an exact agreement between the simulation and the analysis, validating (30). Moreover, the SOP can be minimized by optimally selecting α. The existence of the optimal value of α for the minimum SOP can be explained as follows. Increasing α permits SR to scavenge more energy, and thus, SR can enhance its transmission reliability in stage 2, ultimately decreasing the SOP. Nevertheless, increasing α also decreases the energy for the information decoder, decreasing the probability that SR can correctly restore the source information in stage 1 and inflicting more secrecy outage in stage 2. Consequently, α should be optimally adopted to compromise transmission reliability of SS and SR in both stages. Furthermore, the minimum SOP corresponding to the optimum value of α increases with P_p/N_0 as expected.

Figure 7 illustrates the SOP versus the required spectral efficiency of SUs, C_1, for $P_{sm}/N_0 = 15$ dB, $\beta = 0.6$, $\lambda = 0.1$, $d = 0.5$, $\alpha = 0.8$, $C_2 = 0.3$ bps/Hz, $\overline{C}_3 = 0.1$ bps/Hz, and $P_p/N_0 = 10, 15, 20$ dB. This figure verifies a perfect match between the simulation and the analysis, confirming the precision of (30). In addition, the SOP increases with increasing C_1. This is apparent because the higher the required spectral efficiency of SUs, the lower the probability for the relay to correctly restore the source information, and, hence, the higher the probability for the system to be outage in stage 2. Moreover, the SOP is higher for larger values of P_p/N_0 as expected.

Figure 8 demonstrates the SOP versus the required spectral efficiency of PUs, C_2, for $P_{sm}/N_0 = 15$ dB, $\beta = 0.6$, $\lambda = 0.1$, $d = 0.5$, $\alpha = 0.8$, $C_1 = 0.2$ bps/Hz,

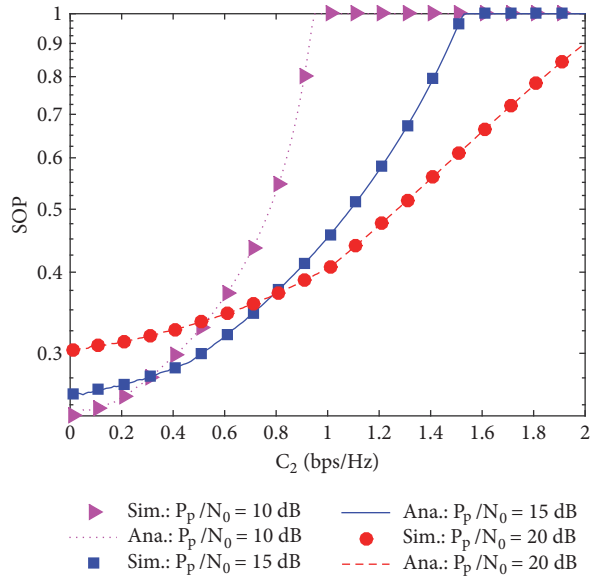

Figure 8: SOP versus the required spectral efficiency of PUs.

$\overline{C}_3 = 0.1$ bps/Hz, and $P_p/N_0 = 10, 15, 20$ dB. This figure confirms an exact agreement between the analysis and the simulation, validating (30). Additionally, the SOP increases with increasing C_2. This is because for the fixed value of λ (please see (22) and (23)) the higher the required spectral efficiency of PUs is, the lower the interference at PUs caused by SUs must be, and, hence, the lower the transmit power of SUs must be, leading to the higher SOP. Nevertheless, the system is always in outage at large values of C_2. This is because according to (26) and (27), the terms inside $[\cdot]^+$ are inversely proportional to φ_{21} and φ_{22} (or C_2). As such, increasing C_2 up to a certain value (e.g., 1.53 bps/Hz for $P_p/N_0 = 15$ dB) incurs $[\cdot]^+ = 0$ and, hence, P_s and P_r are always zero when C_2 exceeds a threshold, causing the system outage all the

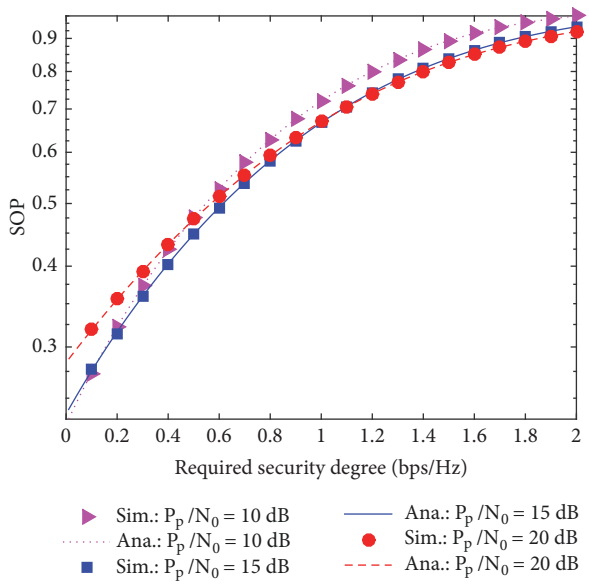

Figure 9: SOP versus the required security degree.

time. Furthermore, the SOP is affected by P_p/N_0 as expected. More noticeably, when C_2 is greater than a certain value, the SOP decreases with increasing P_p/N_0. For example, when C_2 is greater than 0.31 bps/Hz, the SOP with $P_p/N_0 = 10$ dB is larger than the SOP with $P_p/N_0 = 15$ dB. This can be interpreted as follows. The primary receiver has more chances to obtain the required spectral efficiency C_2 when P_p/N_0 increases. As such, it can be more tolerable with the interference from the secondary transmitters. Moreover, the relay has more chances to scavenge more energy from the transmit signal of PT when P_p/N_0 increases. Accordingly, the relay transmits signals with higher power, which can better compensate for more interference from the primary transmitter due to larger value of P_p/N_0, eventually reducing the SOP.

Figure 9 shows the SOP versus the required security degree $\overline{C}_3$ for $P_{sm}/N_0 = 15$ dB, $\beta = 0.6$, $\lambda = 0.1$, $d = 0.5$, $\alpha = 0.8$, $C_1 = 0.2$ bps/Hz, $C_2 = 0.1$ bps/Hz, and $P_p/N_0 = 10, 15, 20$ dB. This figure validates (30) because of the match between the analysis and the simulation. Additionally, the SOP increases with increasing $\overline{C}_3$. This is because, given system parameters, the higher the required security degree, the higher the SOP. Moreover, the SOP is influenced by P_p/N_0 as expected.

5. Conclusion

This paper evaluated the security performance of relaying communications in energy scavenging cognitive networks in terms of the SOP. For quick performance assessment, the accurate closed-form expression of the SOP was derived under consideration of Rayleigh fading, the primary outage constraint, the interference from PUs, and the maximum transmit power constraint. The validity of the proposed expression was verified by computer simulations. Various results exposed that the self-powered relay considerably enhances the security performance even when the source-destination channel is unavailable owing to deep fading, severe path-loss, and strong shadowing. Moreover, the security performance suffered the error floor in the range of large maximum transmit power or high required outage probability of PUs. Furthermore, the security performance of relaying communications in energy scavenging cognitive networks depends on several system parameters among which the time splitting factor, the relay's position, and the power splitting factor should be optimally selected to minimize the SOP.

Appendix

Proof of Theorem 1. Decompose $\mathcal{I}_1$ into two cases, $\log_2((1+\varphi_{rd})/(1+\varphi_{re})) > 0$ and $\log_2((1+\varphi_{rd})/(1+\varphi_{re})) < 0$; one can simplify it as

$$\begin{aligned}\mathcal{I}_1 = {} & \Pr\left\{\log_2\left(\frac{1+\varphi_{rd}}{1+\varphi_{re}}\right) < C_3 \mid \log_2\left(\frac{1+\varphi_{rd}}{1+\varphi_{re}}\right) \geq 0, \varphi_{sr} \geq \varphi_1\right\} \times \Pr\left\{\log_2\left(\frac{1+\varphi_{rd}}{1+\varphi_{re}}\right) \geq 0 \mid \varphi_{sr} \geq \varphi_1\right\} + \Pr\left\{0 < C_3 \mid \log_2\left(\frac{1+\varphi_{rd}}{1+\varphi_{re}}\right) < 0, \varphi_{sr} \geq \varphi_1\right\} \Pr\left\{\log_2\left(\frac{1+\varphi_{rd}}{1+\varphi_{re}}\right) < 0 \mid \varphi_{sr} \geq \varphi_1\right\}, \end{aligned} \tag{A.1}$$

where C_3 is defined in (39).

Because the required security degree is positive (i.e., $\overline{C}_3 > 0$), (A.1) is further shortened as

$$\begin{aligned}\mathcal{I}_1 &= \Pr\left\{\frac{1+\varphi_{rd}}{1+\varphi_{re}} < 2^{C_3} \mid \varphi_{sr} \geq \varphi_1\right\} \\ &= \Pr\left\{\varphi_{rd} < 2^{C_3}(1+\varphi_{re}) - 1 \mid \varphi_{sr} \geq \varphi_1\right\} \\ &= \int_0^{\infty}\int_0^{2^{C_3}(1+x)-1} f_{\varphi_{re},\varphi_{rd}}(x, y \mid \varphi_{sr} \geq \varphi_1)\, dy\, dx. \end{aligned} \tag{A.2}$$

Because φ_{rd} and φ_{re} are statistically independent, their joint pdf can be represented as a product of their marginal pdfs, i.e., $f_{\varphi_{re},\varphi_{rd}}(x, y \mid \varphi_{sr} \geq \varphi_1) = f_{\varphi_{re}}(x \mid \varphi_{sr} \geq \varphi_1) f_{\varphi_{rd}}(y \mid \varphi_{sr} \geq \varphi_1)$. Then, (A.2) is rewritten as

$$\begin{aligned}\mathcal{I}_1 &= \int_0^{\infty}\left[\int_0^{2^{C_3}(1+x)-1} f_{\varphi_{rd}}(y \mid \varphi_{sr} \geq \varphi_1)\, dy\right] \cdot f_{\varphi_{re}}(x \mid \varphi_{sr} \geq \varphi_1)\, dx \\ &= \int_0^{\infty} F_{\varphi_{rd}}\left(2^{C_3}[1+x] - 1 \mid \varphi_{sr} \geq \varphi_1\right) \cdot f_{\varphi_{re}}(x \mid \varphi_{sr} \geq \varphi_1)\, dx. \end{aligned} \tag{A.3}$$

To numerically evaluate (A.3), the cdf of φ_{rd}, $F_{\varphi_{rd}}(z \mid \varphi_{sr} \geq \varphi_1)$, and the pdf of φ_{re}, $f_{\varphi_{re}}(z \mid \varphi_{sr} \geq \varphi_1)$, must be derived first.

The cdf of φ_{rd} is computed from its definition as

$$\begin{aligned} F_{\varphi_{rd}}(z \mid \varphi_{sr} \geq \varphi_1) &= \Pr\{\varphi_{rd} \leq z \mid \varphi_{sr} \geq \varphi_1\} \\ &= \Pr\left\{\frac{P_r |g_{rd}|^2}{P_{p2} |g_{pd}|^2 + \varrho_d^2} \leq z\right\} \\ &= \Pr\left\{|g_{rd}|^2 \leq \frac{z}{P_r}\left(P_{p2} |g_{pd}|^2 + \varrho_d^2\right)\right\} \\ &= \int_0^\infty F_{|g_{rd}|^2}\left(\frac{z}{P_r}\left[P_{p2} |g_{pd}|^2 + \varrho_d^2\right]\right) f_{|g_{pd}|^2}(x)\, dx \\ &= \int_0^\infty \left(1 - e^{-(z/\kappa_{rd}P_r)(P_{p2}x + \varrho_d^2)}\right) \frac{1}{\kappa_{pd}} e^{-x/\kappa_{pd}} dx. \end{aligned} \tag{A.4}$$

The last integral in (A.4) is straightforwardly computed, resulting in

$$F_{\varphi_{rd}}(z \mid \varphi_{sr} \geq \varphi_1) = 1 - A\frac{e^{-Bz}}{z + A}, \tag{A.5}$$

where A and B are given by (32) and (33), respectively.

Similarly, the cdf of φ_{re} has the same form as that of φ_{rd}:

$$F_{\varphi_{re}}(z \mid \varphi_{sr} \geq \varphi_1) = 1 - C\frac{e^{-Dz}}{z + C}, \tag{A.6}$$

where C and D are given by (34) and (35), respectively.

Taking the derivative of $F_{\varphi_{re}}(z \mid \varphi_{sr} \geq \varphi_1)$ with respect to z arrives at

$$f_{\varphi_{re}}(z \mid \varphi_{sr} \geq \varphi_1) = CD\frac{e^{-Dz}}{z + C} + C\frac{e^{-Dz}}{(z + C)^2}. \tag{A.7}$$

Plugging (A.5) and (A.7) with reasonable variable substitutions into (A.3), one obtains

$$\begin{aligned} \mathcal{I}_1 &= \int_0^\infty \left[1 - A\frac{e^{-B(2^{C_3}x + 2^{C_3} - 1)}}{2^{C_3}x + 2^{C_3} - 1 + A}\right]\left[CD\frac{e^{-Dx}}{x + C} + C \cdot \frac{e^{-Dx}}{(x + C)^2}\right] dx = CD\int_0^\infty \frac{e^{-Dx}}{x + C}dx \\ &\quad + C\int_0^\infty \frac{e^{-Dx}}{(x + C)^2}dx \\ &\quad - 2^{-C_3}e^{-B(2^{C_3} - 1)}ACD\int_0^\infty \frac{e^{-2^{C_3}Bx}}{x + 1 + 2^{-C_3}(A - 1)}\frac{e^{-Dx}}{x + C}dx \\ &\quad - 2^{-C_3}e^{-B(2^{C_3} - 1)}AC\int_0^\infty \frac{e^{-2^{C_3}Bx}}{x + 1 + 2^{-C_3}(A - 1)}\frac{e^{-Dx}}{(x + C)^2}dx. \end{aligned} \tag{A.8}$$

By letting $G = 1 + 2^{-C_3}(A - 1)$ as in (36) and applying the partial fraction decomposition to $1/(x + G)(x + C)$ and $1/(x + G)(x + C)^2$, one can transform (A.8) to

$$\begin{aligned} \mathcal{I}_1 &= CD\int_0^\infty \frac{e^{-Dx}}{x + C}dx + C\int_0^\infty \frac{e^{-Dx}}{(x + C)^2}dx \\ &\quad - 2^{-C_3}e^{-B(2^{C_3} - 1)}ACD\int_0^\infty \frac{e^{-(2^{C_3}B + D)x}}{(x + G)(x + C)}dx \\ &\quad - 2^{-C_3}e^{-B(2^{C_3} - 1)}AC\int_0^\infty \frac{e^{-(2^{C_3}B + D)x}}{(x + G)(x + C)^2}dx \\ &= CD\int_0^\infty \frac{e^{-Dx}}{x + C}dx + C\int_0^\infty \frac{e^{-Dx}}{(x + C)^2}dx \\ &\quad - 2^{-C_3}e^{-B(2^{C_3} - 1)}\frac{ACD}{C - G}\left[\int_0^\infty \frac{e^{-(2^{C_3}B + D)x}}{x + G}dx - \int_0^\infty \frac{e^{-(2^{C_3}B + D)x}}{x + C}dx\right] - 2^{-C_3}e^{-B(2^{C_3} - 1)} \\ &\quad \cdot \frac{AC}{C - G}\left[\frac{1}{C - G}\int_0^\infty \frac{e^{-(2^{C_3}B + D)x}}{x + G}dx - \frac{1}{C - G}\int_0^\infty \frac{e^{-(2^{C_3}B + D)x}}{x + C}dx - \int_0^\infty \frac{e^{-(2^{C_3}B + D)x}}{(x + C)^2}dx\right]. \end{aligned} \tag{A.9}$$

It is obvious that the integrals in the last equality of (A.9) have the two following forms:

$$\Psi(a, b) = \int_0^\infty \frac{e^{-ax}}{x + b}dx, \tag{A.10}$$

$$\Phi(a, b) = \int_0^\infty \frac{e^{-ax}}{(x + b)^2}dx. \tag{A.11}$$

The accurate closed form of (A.10) is presented as (37) by changing the variable $y = x + b$ and applying the definition of the exponential integral in [26].

To obtain the accurate closed form of (A.11) as presented in (38), partial integration is firstly implemented in the integral in (A.11) as $\Phi(a, b) = 1/b - a\int_0^\infty e^{-ax}/(x + b)dx$ and, then, one applies (A.10) to transform (A.11) to (38).

By representing the integrals in the last equality of (A.9) in terms of $\Psi(a, b)$ and $\Phi(a, b)$, one can reduce (A.9) to (31). This completes the proof. □

Data Availability

We 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 research is funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number B2019-20-01.

References

[1] Y. Zhang, R. Lu, B. Cao, and Q. Zhang, "Cooperative jamming-based physical-layer security of cooperative cognitive radio networks: system model and enabling techniques," *IET Communications*, vol. 13, no. 5, pp. 539–544, 2019.

[2] K. Ho-Van and T. Do-Dac, "Impact of primary interference on secrecy performance of physical layer security in cognitive radio networks," *Wireless Personal Communications*, vol. 100, no. 3, pp. 1099–1127, 2018.

[3] H. Tran, T. X. Quach, H.-V. Tran, and E. Uhlemann, "Optimal energy harvesting time and power allocation policy in crn under security constraints from eavesdroppers," in *Proceedings of the 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2017*, pp. 1–8, Canada, October 2017.

[4] B. R. Manoj, R. K. Mallik, M. R. Bhatnagar, and S. Gautam, "Virtual full-duplex relaying in multi-hop DF cooperative networks using half-duplex relays with buffers," *IET Communications*, vol. 13, no. 5, pp. 489–495, 2019.

[5] L. Ni, X. Da, H. Hu, Y. Huang, R. Xu, and M. Zhang, "Outage constrained robust transmit design for secure cognitive radio with practical energy harvesting," *IEEE Access*, vol. 6, pp. 71444–71454, 2018.

[6] C. Li, J. Wang, and M. Li, "Spatiotemporal compression-transmission strategies for energy-harvesting wireless sensor networks," *IET Communications*, vol. 13, no. 5, pp. 630–636, 2019.

[7] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[8] 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.

[9] J. Qiao, H. Zhang, F. Zhao, and D. Yuan, "Secure transmission and self-energy recycling with partial eavesdropper CSI," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1531–1543, 2018.

[10] K. Khalil and M. S. Khan, "Futiling eavesdropping in harvested energy powered cognitive radio networks under secrecy constraints and multi slot spectrum sensing schedule," in *Proceedings of the 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–6, Sukkur, Pakistan, March 2018.

[11] R. Su, Y. Wang, and R. Sun, "Destination-assisted jamming for physical-layer security in SWIPT cognitive radio systems," in *Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Barcelona, Spain, April 2018.

[12] X. Chen, L. Guo, X. Li, C. Dong, J. Lin, and P. T. Mathiopoulos, "Secrecy rate optimization for cooperative cognitive radio networks aided by a wireless energy harvesting jammer," *IEEE Access*, vol. 6, pp. 34127–34134, 2018.

[13] F. Zhou, Z. Chu, H. Sun, and V. C. Leung, "Resource allocation for secure MISO-NOMA cognitive radios relying on SWIPT," in *Proceedings of the 2018 IEEE International Conference on Communications (ICC 2018)*, pp. 1–6, Kansas City, MO, USA, May 2018.

[14] S. Raghuwanshi, P. Maji, S. D. Roy, and S. Kundu, "Secrecy performance of a dual hop cognitive relay network with an energy harvesting relay," in *Proceedings of the 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1622–1627, Jaipur, India, September 2016.

[15] F. P. Benedict, P. Maji, S. D. Roy, and S. Kundu, "Secrecy analysis of a Cognitive Radio Network with an energy harvesting AF relay," in *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1358–1363, Chennai, India, March 2017.

[16] P. Maji, S. D. Roy, and S. Kundu, "Physical layer security in cognitive radio network with energy harvesting relay and jamming in the presence of direct link," *IET Communications*, vol. 12, no. 11, pp. 1389–1395, 2018.

[17] P. Maji, B. Prasad, S. D. Roy, and S. Kundu, "Secrecy outage of a cognitive radio network with selection of energy harvesting relay and imperfect CSI," *Wireless Personal Communications*, vol. 100, no. 2, pp. 571–586, 2018.

[18] T. D. Hieu, T. T. Duy, and S. G. Choi, "Performance enhancement for harvest-to-transmit cognitive multi-hop networks with best path selection method under presence of eavesdropper," in *Proceedings of the 2018 20th International Conference on Advanced Communications Technology (ICACT)*, pp. 323–328, Chuncheon-si Gangwon-do, South Korea, Feburary 2018.

[19] 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.

[20] M. Seyfi, S. Muhaidat, and J. Liang, "Relay selection in cognitive radio networks with interference constraints," *IET Communications*, vol. 7, no. 10, pp. 922–930, 2013.

[21] K. Ho-Van, "Influence of channel information imperfection on outage probability of cooperative cognitive networks with partial relay selection," *Wireless Personal Communications*, vol. 94, no. 4, pp. 3285–3302, 2017.

[22] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Transactions on Communications*, vol. 61, no. 11, pp. 4754–4761, 2013.

[23] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622–3636, 2013.

[24] E. Biglieri, J. Proakis, and S. Shamai, "Fading channels: information-theoretic and communications aspects," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 44, no. 6, pp. 2619–2692, 1998.

[25] K. Ho-Van, "Outage analysis of opportunistic relay selection in underlay cooperative cognitive networks under general operation conditions," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8145–8154, 2016.

[26] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press, San Diego, Calif, USA, 6 edition, 2000.

[27] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103–5113, 2013.