Security Analysis of Relay Selection in Energy Scavenging-based Cognitive Networks

Ngoc Pham-Thi-Dan[1,2,3], Nguyen Bui-Trung[1,2], Huynh Nguyen[1,2], Quan Lam-Minh[1,2], Khuong Ho-Van[1,2], Son Pham-Ngoc[4], Son Vo-Que[1,2], Thiem Do-Dac[1,2,5]
[1]*Ho Chi Minh City University of Technology*
[2]*Vietnam National University Ho Chi Minh City*
[3]*Posts and Telecommunications Institute of Technology - HoChiMinh Campus*
[4]*Ho Chi Minh City University of Technology and Education*
[5]*Thu Dau Mot University*
ngocptd@ptithcm.edu.vn, 1612270@hcmut.edu.vn, 1611379@hcmut.edu.vn, 1612808@hcmut.edu.vn, hvkhuong@hcmut.edu.vn, ngocsond00vta1@gmail.com, sonvq@hcmut.edu.vn, thiemdd@tdmu.edu.vn

***Abstract*—We introduce a relay selection strategy to secure energy scavenging-based cognitive networks in this paper. The introduced strategy selects a relay which satisfies two conditions: i) decode correctly data of secondary source and ii) obtain the highest secrecy capacity to the secondary destination. To assess promptly the efficacy of the introduced strategy, the secrecy outage probability (SOP) is firstly derived in exact closed form. The recommended SOP expression is then verified by Monte-Carlo simulations. Finally, useful comments on security performance of the recommended relay selection strategy are withdrawn from various results relying on the recommended SOP expression.**

***Index Terms*—Security; energy scavenging; relay selection; underlay.**

I. Introduction

Energy scavenging-based cognitive networks (ESbCNs) are originated from a combination of two emerging (energy scavenging and cognitive radio) technologies which meet stringent requirements of modern wireless communications networks, namely green communications, high spectral efficiency, high energy efficiency [1]. Nonetheless, the nature of cognitive radio networks, which allows cognitive radios to access licensed spectrum of primary users, imposes serious security issues where malicious users can imitate the operation mechanism of cognitive radios to wire-tap legitimate data [2]. Additionally, although scavenging energy in radio frequency signals can solve energy shortage problem and improve energy efficiency, scavenged energy is typically limited, restricting radio coverage of wireless users [3]. The radio coverage can be extended with relay selection where one relay among several available relays is selected to relay source signals to the destination even though source-destination channel is blocked [4]. All above issues are solved in this paper by proposing a relay selection strategy to secure ESbCNs. This strategy selects a relay which satisfies two conditions: i) decode exactly data of the secondary source and ii) achieve the highest secrecy capacity to the secondary destination. All relays can harvest energy from both primary and secondary sources to create their motivation for helping the secondary source in relaying its signal to the secondary destination.

A. Literature review

Most relevant works studied securing direct/relaying communications in ESbCNs [5]–[15]. Upon our knowledge only three publications in [16]–[18] investigated the relay selection in ESbCNs. More specifically, [16] researched the secrecy performance of the traditional reactive relay selection strategy in ESbCNs. However, [16] solely provided the simulated SOP results under consideration of (interference and peak transmit) power constraints. The strategy mentioned in [16] chooses one relay that achieves the largest relay-destination signal-to-noise ratio (SNR). In addition, [16] investigated the time switching-based energy harvesting paradigm (TSEHP), which permits the relay to harvest energy from solely the source signal. To secure further ESbCNs, [17] recommended a path selection strategy in which the best path is chosen. Additionally, fixed beacons supply wireless energy for the relays through TSEHP in [17]. Moreover, [17] merely performed the analysis on connection outage probability. Lately, [18] recommended a relay selection strategy to adopt a relay that restores correctly source data and minimizes the SNR at the eavesdropper. In [18], the secondary transmit power is restricted by the maximum (interference and peak transmit) powers and the power splitting-based energy scavenging paradigm (PSESP) is investigated for energy scavenging. Furthermore, [18] carried out solely the intercept outage probability analysis. Moreover, [16]–[18] ignored the interference from the primary source (namely, primary interference). Generally, the primary interference should be investigated in cognitive radio networks since both (secondary and primary) users send information simultaneously on the same link. Additionally, the primary interference is advantageous for relays to scavenge energy. Also, [16]–[18] did not study the primary outage restriction and the SOP (a critical

security performance metric in the aspect of information theory) analysis.

B. Contributions

This paper has the following contributions:

- Recommend the relay selection strategy for securing the secondary source-destination communication in scenarios that their direct communication is unavailable. The recommended strategy optimizes the secrecy capacity of the selected relay-destination channel and the relays harvest the energy from both (secondary and primary) signals with the PSESP. Furthermore, the relays must recover exactly the secondary source data before forwarding it to the secondary destination.
- Recommend exact closed-form SOP formula under consideration of both primary outage restraint and peak transmit power restraint, and the primary interference to promptly evaluate the SOP of the recommended relay selection strategy in ESbCNs.
- Employ the recommended expression to set optimal key specifications.
- Provide various results to shed insights on the secrecy performance; for instance, the smallest SOP achievable with proper adoption of the time-switch factor and the primary transmit power; the secrecy capability saturation at high peak transmit power.

C. Organization

The next section depicts the investigated system overview. Then, section III derives the SOP in details. Next, section IV supplies simulated/theoretical results and eventually, section V terminates our work.

II. System Overview

A. System description

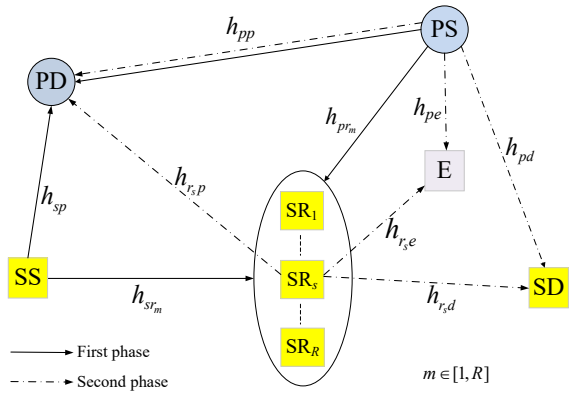

Fig. 1. System model.

Consider an ESbCN with the proposed relay selection strategy in Fig. 1. The secondary source (SS) completes its transmission to the secondary destination (SD) with the aid of the adopted secondary relay (SR_s) in two phases. The first phase lasts θT while the second phase lasts $(1-\theta)T$ where θ with $\theta \in (0,1)$ and T signify the time-switch factor and the total duration for transmission from SS to SD via SR_s, correspondingly.

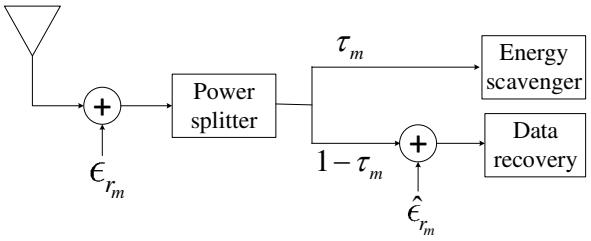

Fig. 2. Power splitting paradigm at SR_m.

The first phase is for both SS and the primary source (PS) to send simultaneously their secret data to SD and the primary destination (PD), correspondingly, creating both (secondary and primary) interferences. The secondary interference (i.e., in the secondary to primary direction) has been well studied in the literature yet the primary interference (i.e., in the primary to secondary direction) is usually neglected (e.g., [8]–[13], [15]–[19]). Accordingly, that our paper accounts for these interferences is apparently more general than existing works yet with more complicated performance analysis. The eavesdropper (E) overhears the SS's information. Owing to contaminated propagation environment, SD and E cannot receive the SS's signals reliably. Consequently, the secondary relays SR_m, $m \in [1, R]$, between SS and SD should be employed to relay the SS's signal to SD. To save power and bandwidth, the current paper adopts a relay SR_s in a subgroup of relays that restore exactly the SS's data. Furthermore, to motivate the assistance of the relays, only the energy scavenged from the RF signals is consumed by the relays for relaying purpose. The PSESP (e.g., [20] and [21]) is employed for energy scavenging as seen in Fig. 2. To be more specific, SR_m harvests energy in the signals of both PS and SS. As such, our paper converts even the primary interference to an useful energy source. The signal power received at SR_m is split into two fractions: one for recovering the SS's data and another for scavenging the energy.

The second phase is for the selected relay SR_s to recover the SS's data and relay the decoded data to SD at the same time that PS sends its data to PD, which again causes secondary and primary interferences. At the end of the secondary phase, SD makes an effort to restore the SS's data from the transmit signal of SR_s while E overhears it.

B. Channel model

Let $h_{\mathrm{xy}} \in \{h_{pp}, h_{pe}, h_{pd}, h_{pr_m}, h_{sp}, h_{sr_m}, h_{r_m p}, h_{r_m e}, h_{r_m d}\}$ represent $\{\mathrm{PS} \to \mathrm{PD}, \mathrm{PS} \to \mathrm{E}, \mathrm{PS} \to \mathrm{SD}, \mathrm{PS} \to \mathrm{SR}_m, \mathrm{SS} \to \mathrm{PD}, \mathrm{SS} \to \mathrm{SR}_m, \mathrm{SR}_m \to \mathrm{PD}, \mathrm{SR}_m \to \mathrm{E}, \mathrm{SR}_m \to \mathrm{SD}\}$ channel coefficient. Then, the channel gain is denoted as $g_{\mathrm{xy}} = |h_{\mathrm{xy}}|^2$. Assume Rayleigh fading and hence, the channel coeffi-

cient h_{xy} is represented by a complex Gaussian random variable with zero-mean and κ_{xy}-variance, namely, $h_{\mathrm{xy}} \sim \mathcal{CN}(0, \kappa_{\mathrm{xy}})$. Accounting for path-loss, κ_{xy} is represented as $\kappa_{\mathrm{xy}} = d_{\mathrm{xy}}^{-\psi}$ where d_{xy} denotes the $\mathrm{x}-\mathrm{y}$ distance and ψ stands for the path-loss exponent.

C. Signal model

SR_m and PD receive signals in the first phase, respectively, to be

$$y_{r_m} = h_{sr_m}\sqrt{P_s}x_s + h_{pr_m}\sqrt{P_p}x_p + \epsilon_{r_m}, \quad (1)$$

$$y_{p1} = h_{sp}\sqrt{P_s}x_s + h_{pp}\sqrt{P_p}x_p + \epsilon_{p1}, \quad (2)$$

where x_s and x_p are correspondingly the transmit symbols of SS and PS; $\epsilon_{r_m} \sim \mathcal{CN}(0, \xi_{r_m})$ and $\epsilon_{p1} \sim \mathcal{CN}(0, \xi_p)$ are the noises at SR_m and PD, respectively; the transmit powers of SS and PS are P_s and P_p, correspondingly.

The relay SR_m splits its received signal y_{r_m} into two parts: one part of $\sqrt{\tau_m}y_{r_m}$ is for energy harvesting and another part of $\sqrt{1-\tau_m}y_{r_m}$ is for data recovery. Here τ_m with $\tau_m \in (0,1)$ denotes the power-split factor. Relied on $\sqrt{\tau_m}y_{r_m}$, SR_m accumulates the scavenged energy in the first phase as $E_{r_m} = \zeta_m\tau_m\left(P_s\kappa_{sr_m} + P_p\kappa_{pr_m} + \xi_{r_m}\right)\theta T$ where ζ_m with $\zeta_m \in (0,1)$ stands for the energy harvesting efficiency. Then, SR_m spends the harvested energy E_{r_m} to send signal in the second phase with the peak transmit power as $\bar{P}_{r_m} = \theta\zeta_m\tau_m\left(P_s\kappa_{sr_m} + P_p\kappa_{pr_m} + \xi_{r_m}\right)/(1-\theta)$. Moreover, after down-converting signals from passband to baseband which also creates the noise $\hat{\epsilon}_{r_m} \sim \mathcal{CN}\left(0, \hat{\xi}_{r_m}\right)$, recovering x_s uses the signal $\hat{y}_{r_m} = \sqrt{1-\tau_m}y_{r_m} + \hat{\epsilon}_{r_m}$. Plugging (1) in $\hat{y}_{r_m}$ results in $\hat{y}_{r_m} = \sqrt{(1-\tau_m)P_s}h_{sr_m}x_s + \sqrt{(1-\tau_m)P_p}h_{pr_m}x_m + \sqrt{1-\tau_m}\epsilon_{r_m} + \hat{\epsilon}_{r_m}$, which produces the SNIR (Signal-to-Noise plus Interference Ratio) for restoring x_s as $\Gamma_{sr_m} = P_s g_{sr_m}/\left(P_p g_{pr_m} + \check{\xi}_{r_m}\right)$ where $\check{\xi}_{r_m} = \xi_{r_m} + \hat{\xi}_{r_m}/(1-\tau_m)$.

Generally, SD, E, and PD receive signals from the arbitrary relay SR_m in the second phase, respectively, as

$$y_{r_m d} = h_{r_m d}\sqrt{P_{r_m}}x_{r_m} + h_{pd}\sqrt{P_p}x_p + \epsilon_d, \quad (3)$$

$$y_{r_m e} = h_{r_m e}\sqrt{P_{r_m}}x_{r_m} + h_{pe}\sqrt{P_p}x_p + \epsilon_e, \quad (4)$$

$$y_{r_m p} = h_{r_m p}\sqrt{P_{r_m}}x_{r_m} + h_{pp}\sqrt{P_p}x_p + \epsilon_{p2}, \quad (5)$$

where $\epsilon_d \sim \mathcal{CN}(0, \xi_d)$, $\epsilon_e \sim \mathcal{CN}(0, \xi_e)$, and $\epsilon_{p2} \sim \mathcal{CN}(0, \xi_p)$ are the noises at SD, E, and PD, respectively; P_{r_m} is the transmit power of SR_m.

Assuming that SR_m is scheduled for transmission in the second phase. Then, the SNIRs at SD and E are correspondingly inferred from (3) and (4) as $\Gamma_{r_m d} = P_{r_m} g_{r_m d}/\left(P_p g_{pd} + \xi_d\right)$ and $\Gamma_{r_m e} = P_{r_m} g_{r_m e}/\left(P_p g_{pe} + \xi_e\right)$ from which channel capacities achievable at SD and E through the help of SR_m are respectively represented as $C_{r_m d} = (1-\theta)\log_2\left(1+\Gamma_{r_m d}\right)$ and $C_{r_m e} = (1-\theta)\log_2\left(1+\Gamma_{r_m e}\right)$ where the pre-log coefficient of $(1-\theta)$ is thanks to the time of the second phase of $(1-\theta)T$.

The subtraction of $C_{r_m e}$ from $C_{r_m d}$ is defined as the secrecy capacity. Consequently, with the help of SR_m, the secrecy capacity is given by

$$\mathcal{C}_{r_m} = (1-\theta)\left[\log_2\frac{1+\Gamma_{r_m d}}{1+\Gamma_{r_m e}}\right]^+, \quad (6)$$

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

D. Power distribution

The SNIR at PD in the first phase is inferred from (2) as $\Gamma_{p1} = P_p g_{pp}/\left(P_s g_{sp} + \xi_p\right)$ from which the achievable channel capacity of PD in this phase is $C_{p1} = \theta\log_2\left(1+\Gamma_{p1}\right)$. Likewise, the SNIR at PD in the second phase under the activation of SR_m is computed from (5) as $\Gamma_{p2m} = P_p g_{pp}/\left(P_{r_m} g_{r_m p} + \xi_p\right)$ from which the available channel capacity of PD in the second phase under the activation of SR_m is $C_{p2m} = (1-\theta)\log_2\left(1+\Gamma_{p2m}\right)$.

The quality of service (QoS) of primary users (PUs) is the highest priority in cognitive radio networks. As such, the secondary transmitters (SS and SR_m) must ensure the QoS of PUs while they are operating. This paper represents the QoS of PUs as the outage probability of PD. Consequently, the transmit powers of PUs must be adjusted for the outage probability of PD below a predetermined value ϱ. More specifically, P_{r_m} and P_s must be constrained by

$$\Pr\left\{C_{p2m} \le R_p\right\} \le \varrho, \quad \Pr\left\{C_{p1} \le R_p\right\} \le \varrho, \quad (7)$$

which are named as the primary outage constraints. Here, R_p is the predetermined spectral efficiency of PD.

The transmit powers of SR_m and SS are further restrained by $\bar{P}_{r_m}$ and $\bar{P}_s$, which are their maximum transmit powers established by energy harvester and hardware design, correspondingly. Accordingly, P_{r_m} and P_s are subject to

$$P_{r_m} \le \bar{P}_{r_m}, \quad P_s \le \bar{P}_s, \quad (8)$$

which are called the maximum transmit power constraints.

The solutions of the equation systems by setting the equalities in (7) and (8) yield the transmit powers of P_s and P_{r_m} as

$$P_s = \min\left(\frac{P_p\kappa_{pp}}{\Gamma_{p1}\kappa_{sp}}\left[\frac{1}{1-\varrho}e^{-\frac{\Gamma_{p1}\xi_p}{P_p\kappa_{pp}}} - 1\right]^+, \bar{P}_s\right) \quad (9)$$

$$P_{r_m} = \min\left(\frac{P_p\kappa_{pp}}{\Gamma_{p2}\kappa_{r_m p}}\left[\frac{1}{1-\varrho}e^{-\frac{\Gamma_{p2}\xi_p}{P_p\kappa_{pp}}} - 1\right]^+, \bar{P}_{r_m}\right) \quad (10)$$

where $\Gamma_{p1} = 2^{R_p/\theta} - 1$ and $\Gamma_{p2} = 2^{R_p/(1-\theta)} - 1$.

The proofs of (9) and (10) are the same as [23, eq. (18)] and [23, eq. (20)].

E. Relay selection

It is well-known that SR_m obtains the channel capacity in the first phase as $C_{sr_m} = \theta \log_2(1+\Gamma_{sr_m})$ bits/s/Hz where the presence of the pre-log factor θ is owing to the time of the first phase of θT. Moreover, SR_m recovers correctly the SS's data if C_{sr_m} is above the predetermined value, denoted as R_s, namely, $C_{sr_m} \geq R_s$ or $\Gamma_{sr_m} \geq \Gamma_s$ where $\Gamma_s = 2^{R_s/\theta} - 1$.

Denote $\mathcal{R}$ as the set of relays, which recovered exactly the SS's data:

$$\mathcal{R} = \left\{ \mathrm{SR}_m : \Gamma_{sr_m} \geq \Gamma_s \right\}. \tag{11}$$

The proposed relay selection: The relay SR_s in $\mathcal{R}$ is selected to forward the SS's data in the second phase if its secrecy capacity is the largest among all the relays in $\mathcal{R}$. As such, the secrecy capacity of the proposed relay selection strategy in ESbCNs is addressed to be

$$\mathcal{C}_{\mathrm{sec}} = \max_{\mathrm{SR}_m \in \mathcal{R}} (1-\theta) \left[\log_2 \left(\frac{1+\Gamma_{r_m d}}{1+\Gamma_{r_m e}} \right) \right]^+. \tag{12}$$

III. Security analysis

According to information theory, the SOP is the most important performance indicator for assessing the security of wireless communication. It refers to the probability which the system cannot reach the preset security level $\bar{C}_t$ (i.e., $\mathcal{C}_{sec} < \bar{C}_t$). Accordingly, the smaller SOP signifies the more secured wireless communication. The current section derives the SOP in details for the recommended relay selection strategy in ESbCNs. The recommended explicit formula of the SOP facilitates security capability evaluation swiftly.

The recommended relay selection strategy in ESbCNs bears the SOP to be

$$\Upsilon = \Pr\left\{ \mathcal{C}_{\mathrm{sec}} < \bar{C}_t \right\} = \mathcal{L}_1 + \sum_{m=1}^{R} \sum_{n=1}^{C_R^m} \mathcal{L}_2 \mathcal{L}_3 \tag{13}$$

where $C_R^m = \frac{R!}{m!(R-m)!}$ is the binomial coefficient; $|\cdot|$ stands for the cardinality of the set; $\mathcal{M} = \{\mathcal{F}, \mathcal{K}_n^m\}$; $\mathcal{U} = \{\mathcal{Y}[i_1], ..., \mathcal{Y}[i_j]\}$; $\mathcal{Y} = \mathcal{M} \backslash g$; $\mathcal{F} = \{\mathcal{K}_n^m[l_1], ..., \mathcal{K}_n^m[l_i]\}$; $\mathcal{K}_n^m$ represents the n^{th} combination among C_R^m compositions, each including m different constituents received from the set of R distinct constituents; $\mathcal{V} = \{\mathcal{U}, \mathcal{Y}\}$; $\mathrm{Ei}(\cdot)$ is the exponential integral;

$$\mathcal{L}_1 = \prod_{k=1}^{R} \mathcal{G}_k \tag{14}$$

$$\mathcal{L}_2 = 1 + (-1)^{|\mathcal{K}_n^m|} \mathcal{L}_{2\mathcal{K}_n^m} + \sum_{i=1}^{|\mathcal{K}_n^m|-1} (-1)^i \sum_{l_1=1}^{|\mathcal{K}_n^m|-i+1} \sum_{l_2=l_1+1}^{|\mathcal{K}_n^m|-i+2} \cdots \sum_{l_i=l_{i-1}+1}^{|\mathcal{K}_n^m|} \mathcal{L}_{2\mathcal{F}} \tag{15}$$

$$\mathcal{L}_3 = \prod_{u \in \mathcal{K}_n^m} (1-\mathcal{G}_u) \prod_{v \notin \mathcal{K}_n^m} \mathcal{G}_v \tag{16}$$

with

$$C_t = \bar{C}_t / (1-\theta) \tag{17}$$

$$U_m = P_p / (\kappa_{r_m d} P_{r_m}) \tag{18}$$

$$I_m = \xi_d / (\kappa_{r_m d} P_{r_m}) \tag{19}$$

$$A_m = P_p / (\kappa_{r_m e} P_{r_m}) \tag{20}$$

$$G_m = \xi_e / (\kappa_{r_m e} P_{r_m}) \tag{21}$$

$$H_k = \kappa_{sr_k} P_s / (\kappa_{pr_k} P_p) \tag{22}$$

$$J_k = \check{\xi}_{r_k} / (\kappa_{sr_k} P_s) \tag{23}$$

$$K_g = \left[\frac{1}{\kappa_{pd}} + \left(2^{C_t} - 1\right) \sum_{v \in \mathcal{M}} U_v \right] \frac{I_g + 2^{-C_t} G_g}{U_g} \tag{24}$$

$$L_g = \left[\frac{1}{\kappa_{pd}} + \left(2^{C_t} - 1\right) \sum_{v \in \mathcal{M}} U_v \right] 2^{-C_t} \frac{A_g}{U_g} \tag{25}$$

$$V_u = 2^{C_t} \left(\frac{A_u}{U_u} - \frac{A_g}{U_g} \right)^{-1} \times \left(\frac{I_u + 2^{-C_t} G_u}{U_u} - \frac{I_g + 2^{-C_t} G_g}{U_g} \right) \tag{26}$$

$$N_g = \left[\prod_{u \in \mathcal{M}, u \neq g} 2^{-C_t} \left(\frac{A_u}{U_u} - \frac{A_g}{U_g} \right) \right]^{-1} e^{K_g} \tag{27}$$

$$M_u = \prod_{g \in \mathcal{B}, g \neq u} \frac{1}{V_g - V_u} \tag{28}$$

$$\mathcal{G}_k = 1 - H_k \frac{e^{-J_k \Gamma_s}}{\Gamma_s + H_k} \tag{29}$$

$$\mathcal{L}_{2\mathcal{M}} = e^{-\left(2^{C_t}-1\right) \sum\limits_{u \in \mathcal{M}} I_u} 2^{-C_t |\mathcal{M}|} \left(\prod_{u \in \mathcal{M}} \frac{1}{U_u} \right) \mathcal{E} \tag{30}$$

$$\mathcal{E} = -\frac{\prod\limits_{g \in \mathcal{M}} A_g}{\kappa_{pe} \kappa_{pd}} \sum_{g \in \mathcal{M}} N_g \left\{ \Delta_\emptyset + (-1)^{|\mathcal{Y}|} \Delta_{\mathcal{Y}} + \sum_{y=1}^{|\mathcal{Y}|-1} (-1)^y \sum_{n_1=1}^{|\mathcal{Y}|-y+1} \sum_{n_2=n_1+1}^{|\mathcal{Y}|-y+2} \cdots \sum_{n_y=n_{y-1}+1}^{|\mathcal{Y}|} \Delta_{\mathcal{U}} \right\} \tag{31}$$

$$\Delta_\emptyset = \Phi\left(\frac{1}{\kappa_{pe}} - L_g, L_g, K_g \right) + \frac{G_g}{A_g} \Omega\left(\frac{1}{\kappa_{pe}} - L_g, L_g, K_g \right) \tag{32}$$

$$\Delta_{\mathcal{V}} = \left[\prod_{u \in \mathcal{V}} \left(V_u - \frac{G_u}{A_u} \right) \right] \sum_{u \in \mathcal{V}} M_u \left\{ \Omega\left(\frac{1}{\kappa_{pe}} - L_g, L_g, K_g \right) + \left(\frac{G_g}{A_g} - V_u \right) \Psi\left(\frac{1}{\kappa_{pe}} - L_g, V_u, L_g, K_g \right) \right\} \tag{33}$$

$$\Theta(j,k) = -e^{jk} \mathrm{Ei}(-jk). \tag{34}$$

$$\Omega(j,k,l) = \frac{\mathrm{Ei}(-l)}{j} + \frac{e^{-l}}{j} \Theta\left(j+k, \frac{l}{k} \right) \tag{35}$$

$$\Phi(u,v,l) = \frac{\mathrm{Ei}(-l)}{u^2} + \frac{e^{-l}}{u(u+v)} + \frac{e^{-l}}{u} \left(\frac{1}{u} - \frac{l}{v} \right) \Theta\left(u+v, \frac{l}{v} \right) \tag{36}$$

$$\Psi\left(j,k,l,c\right)=\int_{0}^{\infty}\frac{e^{-jx}}{x+k}\mathrm{Ei}(-lx-c)\,dx. \tag{37}$$

The function $\Psi\left(j,k,l,c\right)$ can be formed in a precise explicit representation as [22, eq. (19)] by letting the parameter a of [22, eq. (19)] be 0. As such, the exact explicit representation of $\Psi\left(j,k,l,c\right)$ should not be summarized here for compactness.

The proof of (13) is ignored in this paper due to space limitation.

The recommended SOP expression in (13) is useful for evaluating promptly the secrecy performance as seen in the next section. Upon our understanding, this expression is novel.

IV. Results and Discussion

The current section exemplifies simulated/theoretical results to estimate the security capability of the recommended relay selection strategy in ESbCNs through crucial specifications where (13) is computed to generate theoretical results and Monte-Carlo simulation creates simulated ones. Without loss of generality, power-split factors, noise variances, and the efficiencies of energy harvesters are assumed to be equal, namely, $\xi_p=\xi_d=\xi_e=\xi_{r_m}=\hat{\xi}_{r_m}=N_0$, $\zeta_m=\zeta$, $\tau_m=\tau$ for $m\in[1,R]$. Moreover, crucial specifications under investigation are listed as PD at (0.7, 0.6), PS at (0.2, 0.8), SD at (1.0, 0.0), SR_1 at $(0.3402, 0.0421)$, SR_2 at $(0.2063, 0.1785)$, SR_3 at $(0.3132, 0.1696)$, SR_4 at $(0.3954, -0.1489)$, SR_5 at $(0.2534, 0.0243)$, SS at (0.0, 0.0), E at (1.0, 0.4), $\zeta=0.9$, $\psi=4$.

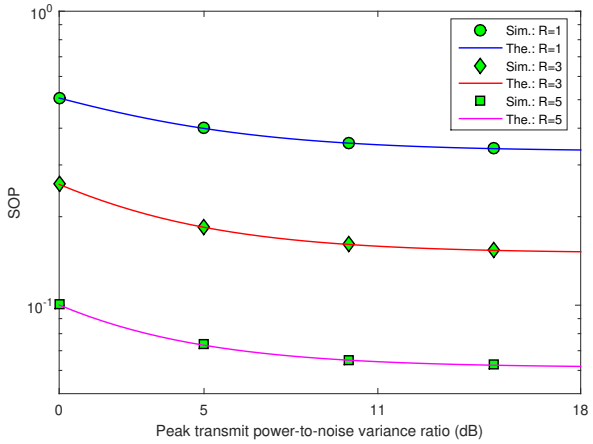

Fig. 3. SOP with respect to (w.r.t) $\bar{P}_s/N_0$.

Fig. 3 shows the security performance w.r.t peak transmit power-to-noise variance ratio $\bar{P}_s/N_0$ for $\theta=0.6$, $P_p/N_0=15$ dB, $\tau=0.8$, $\varrho=0.1$, $R_s=0.2$ bits/s/Hz, $R_p=0.3$ bits/s/Hz, $\bar{C}_t=0.1$ bits/s/Hz. The figure affirms the exactness of (13) thanks to the match between the simulation and theory. Additionally, the security is improved with the increase[1] in R. This obviously shows the efficacy of the recommended relay selection strategy in guaranteeing the high security for ESbCNs. Furthermore, the security is enhanced with increasing $\bar{P}_s/N_0$, which comes from the reality that increasing $\bar{P}_s/N_0$ facilitates SR_m in restoring exactly the SS's data with larger probability and in harvesting more RF energy from source signals, eventually improving the security in the second phase. Nonetheless, the security is saturated at high $\bar{P}_s/N_0$. Such saturation originates from the power distribution for SS and SR_m in (9) and (10) where the transmit powers of SS and SR_m are uncorrelated with $\bar{P}_s/N_0$ at high $\bar{P}_s/N_0$ (namely, the maximum transmit power restraint is neglected at high $\bar{P}_s/N_0$), inducing the saturated security.

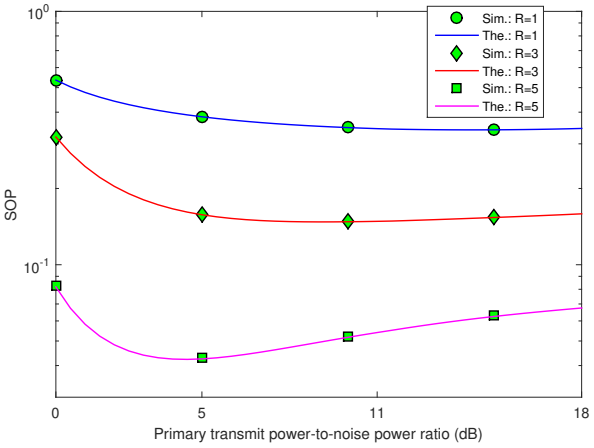

Fig. 4. SOP w.r.t P_p/N_0.

Fig. 4 depicts the security performance w.r.t P_p/N_0 for $R_p=0.3$ bits/s/Hz, $\tau=0.8$, $\varrho=0.1$, $\bar{P}_s/N_0=15$ dB, $\theta=0.6$, $\bar{C}_t=0.1$ bits/s/Hz, $R_s=0.2$ bits/s/Hz. This figure corroborates (13) because the theory matches the simulation. Furthermore, the security is enhanced with the increase in R, validating the effectiveness of the recommended relay selection strategy in ensuring the high security for ESbCNs. Moreover, the security performance is optimized at a middling value of P_p for a certain R. The roots for this result are as follows. For small values of P_p, the primary interference is also small yet the SUs have to send with small power to ensure the quality of service of PD to be constant at $\varrho=0.1$. Consequently, the security is bad. Likewise, large values of P_p induce the high primary interference yet the SUs have to send with large power to ensure the good signal reception at PD with $\varrho=0.1$. Increasing primary interference maybe surpass increasing transmit power of secondary users and hence, the security is bad for large values of P_p. Consequently, a moderate value of P_p offers the best security performance.

[1] $R=1$ simplifies the recommended relay selection to non-relay selection in [11]–[15]. As such, the efficacy of the recommended relay selection strategy is exposed when $R>1$ and is implicitly compared with the non-relay selection strategy ($R=1$).

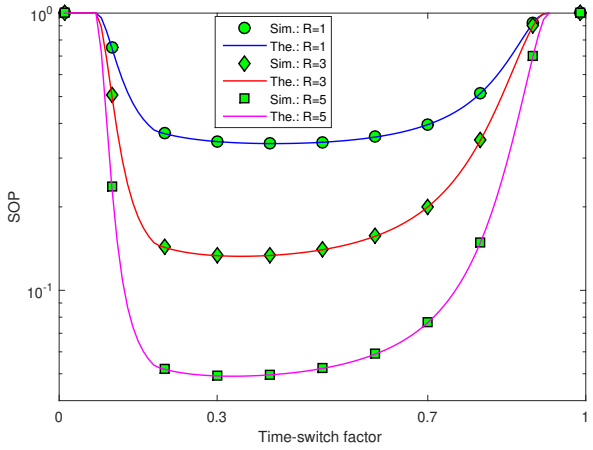

Fig. 5. SOP w.r.t α.

Fig. 5 displays the security performance w.r.t θ for $\bar{C}_t = 0.1$ bits/s/Hz, $\varrho = 0.1$, $\bar{P}_s/N_0 = 8$ dB, $\tau = 0.8$, $P_p/N_0 = 12$ dB, $R_s = 0.2$ bits/s/Hz, $R_p = 0.3$ bits/s/Hz. The figure verifies the preciseness of (13) since the theory matches the simulation. Additionally, the secrecy performance is better with the increase in R as anticipated. Moreover, the proper selection of the time-switch factor, namely θ_{opt}, achieves the best security. The reasons for the existence of θ_{opt} are as follows. Increasing θ prolongs the time of the first phase and thus, SR_m harvests more energy and recovers the SS's message more exactly. Yet, increasing θ also deteriorates the secrecy capacity in the second phase and consequently, the security performance is degraded. Therefore, the compromise between the times of two phases is optimized with θ_{opt} for the best security capability.

V. Conclusions

The current paper firstly recommended the relay selection strategy for energy scavenging cognitive networks and then analyzed its SOP considering the primary outage restriction, the primary interference, Rayleigh fading, and the maximum transmit power restraint. The recommended analysis is affirmed by computer simulations and facilitates in assessing quickly the security performance in important specifications. Various results demonstrate the considerable security performance improvement with the increasing number of relays and the performance saturation at high peak transmit power. In addition, the SOP of the recommended relay selection strategy in ESbCNs can be optimized with the proper selection of the time-switch factor and the primary transmit power.

References

[1] K. Ho-Van *et al.*, "Impact of Channel Estimation-and-Artificial Noise Cancellation Imperfection on Artificial Noise-Aided Energy Harvesting Overlay Networks," Telecom. Sys. To appear.

[2] K. Ho-Van *et al.*, "Impact of Artificial Noise on Security Capability of Energy Harvesting Overlay Networks," Wire. Commun. and Mobi. Comp. To appear.

[3] D. N. Hanh *at al.*, "Secrecy Analysis of Overlay Mechanism in Radio Frequency Energy Harvesting Networks with Jamming under Nakagami-m fading," Wire. Per. Commun., vol. 110, no. 2, pp. 829-846, Jan. 2020.

[4] A. Bletsas *et al.*, "A Simple Cooperative Diversity Method based on Network Path Selection," IEEE JSAC, vol. 24, no. 3, pp. 659-672, Mar. 2006.

[5] N. Pham-Thi-Dan *et al.*, "Effect of Nakagami-m Fading on Secrecy Outage of Energy Scavenging Underlay Cognitive Networks," in Proc. IEEE ATC, Vietnam, 2019, pp. 287-291.

[6] D. Wang *et al.*, "Secure Energy Efficiency for NOMA Based Cognitive Radio Networks With Nonlinear Energy Harvesting," IEEE Access, vol. 6, pp. 62707-62716, Oct. 2018.

[7] F. Wang *et al.*, "Secure Resource Allocation for Cooperative Cognitive Radio Networks with Dedicated Energy Sources," in Proc. IEEE ICC, USA, 2018, pp. 1-6.

[8] H. Lei *et al.*, "On Secure Underlay MIMO Cognitive Radio Networks With Energy Harvesting and Transmit Antenna Selection," IEEE Trans. Green Commun. and Netw., vol. 1, no. 2, pp. 192-203, Jun. 2017.

[9] A. Singh *et al.*, "Secrecy Outage Performance of SWIPT Cognitive Radio Network With Imperfect CSI," IEEE Access, vol. 8, pp. 3911-3919, Dec. 2020.

[10] R. Tan *et al.*, "Secrecy Performance of Cognitive Radio Sensor Networks with an Energy-Harvesting based Eavesdropper and Imperfect CSI," in Proc. AsianHOST, China, 2018, pp. 80-85.

[11] N. Pham-Thi-Dan *et al.*, "Security Analysis for Cognitive Radio Network with Energy Scavenging Capable Relay over Nakagami-m Fading Channels," in Proc. IEEE ISEE, Vietnam, 2019, pp. 68-72.

[12] M. Bouabdellah *et al.*, "Cooperative Energy Harvesting Cognitive Radio Networks With Spectrum Sharing and Security Constraints," IEEE Access, vol. 7, pp. 173329-173343, Nov. 2019.

[13] T. Nguyen *et al.*, "Cognitive Multihop Wireless Powered Relaying Networks Over Nakagami-m Fading Channels," IEEE Access, vol. 7, pp. 154600-154616, Oct. 2019.

[14] W. Zhao *et al.*, "Security Energy Efficiency Maximization for Two-Way Relay Assisted Cognitive Radio NOMA Network With Self-Interference Harvesting," IEEE Access, vol. 7, pp. 74401-74411, Jun. 2019.

[15] N. Pham-Thi-Dan *et al.*, "On Security Capability of Cooperative Communications in Energy Scavenging Cognitive Radio Networks," in Proc. IEEE ATC, Vietnam, 2019, pp. 89-93.

[16] P. Maji *et al.*, "Secrecy Outage of a Cognitive Radio Network with Selection of Energy Harvesting Relay and Imperfect CSI," Wire. Per. Commun., vol. 100, no. 2, pp. 571-586, May 2018.

[17] T. D. Hieu *et al.*, "Performance Enhancement for Harvest-to-Transmit Cognitive Multi-hop Networks with Best Path Selection Method under Presence of Eavesdropper," in Proc. IEEE ICACT, Korea, 2018, pp. 323-328.

[18] K. Ho-Van *et al.*, "Security Enhancement for Energy Harvesting Cognitive Networks with Relay Selection," Wire. Commun. and Mobi. Comp., vol. 2020, Article ID 8867148, pp. 1-13.

[19] N. Pham-Thi-Dan *et al.*, "Energy Harvesting Cooperative Cognitive Networks: Relay Selection for Information Security," in Proc. IEEE ISEE, Vietnam, 2019, pp. 93-96.

[20] P. Nguyen-Huu *et al.*, "Bidirectional Relaying with Energy Harvesting Capable Relay: Outage Analysis for Nakagami-m Fading," Telecom. Sys., vol. 69, no. 3, pp. 335347, Nov. 2018.

[21] K. Ho-Van *et al.*, "Overlay Networks with Jamming and Energy Harvesting: Security Analysis," Arabian J. for Sci. and Eng. To appear.

[22] K. Ho-Van *et al.*, "Reliability-Security Trade-off Analysis of Cognitive Radio Networks with Jamming and Licensed Interference," Wire. Commun. and Mobi. Comp., vol. 2018, Article ID 5457176, pp. 1-15.

[23] K. Ho-Van, "Outage Analysis of Opportunistic Relay Selection in Underlay Cooperative Cognitive Networks under General Operation Conditions," IEEE Trans. Veh. Tech., vol. 65, no. 10, pp. 81458154, Oct. 2016.