Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9976837, 12 pages
https://doi.org/10.1155/2021/9976837

Research Article

Impact of Artificial Noise on Security Capability of Energy Harvesting Overlay Networks

Khuong Ho-Van [1,2] **and Thiem Do-Dac** [1,2,3]

[1]*Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam*
[2]*Vietnam National University Ho Chi Minh City, Linh Trung Ward, Thu Duc District, Ho Chi Minh City, Vietnam*
[3]*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 Thiem Do-Dac; thiemdd@tdmu.edu.vn

Received 23 March 2021; Revised 28 April 2021; Accepted 24 May 2021; Published 21 June 2021

Academic Editor: Zhaolong Ning

Artificial noise, energy harvesting, and overlay communications can assure design metrics of modern wireless networks such as data security, energy efficiency, and spectrum utilization efficiency. This paper studies impact of artificial noise on security capability of energy harvesting overlay networks in which the cognitive transmitter capable of self-powering its operation by harvesting radio frequency energy and self-securing its communications against eavesdroppers by generating artificial noise amplifies and forwards the signal of the primary transmitter as well as transmits its individual signal concurrently. To quantify this impact, the current paper firstly suggests accurate expressions of crucial security performance indicators. Then, computer simulations are supplied to corroborate these expressions. Finally, numerous results are demonstrated to expose insights into this impact from which optimum specifications are determined. Notably, primary/cognitive communications can be secured at distinct degrees by flexibly controlling multiple specifications of the suggested system model.

1. Introduction

Fifth generation (5G) networks provide a huge number of emerging wireless services and thus pressure considerably telecommunication infrastructure [1]. Indeed, one of the 5G network's pivotal services is Internet of Things (IoT), which is applied extensively from civilian (e.g., healthcare, transportation, electricity, and public safety) to military (e.g., smart bases and tactical reconnaissance) [2]. Nevertheless, when deploying IoT, a large number of simultaneously connected devices consume tremendous amount of energy, and thus it is necessary to enhance energy efficiency to not only linger the life-time of devices but also mitigate energy demand. Moreover, IoT needs a large spectrum to allot instantaneous operation of a huge number of users, and hence in the spectrum shortage-and-scarcity situation as today [3], solutions of upgrading spectral efficiency should be proposed. Similarly to IoT, 5G mobile wireless communications, which also serve the growing number of mobile devices and requires increasingly high data rate, need effective spectrum-and-energy utilization solutions to satisfy its requirements [4]. Such a pressure can be released with modern technology solutions of high (energy, spectrum utilization, spectral) efficiencies as follows.

Cognitive users (CUs), which usually operate in underlay, overlay, and interweave mechanisms, can utilize the licensed frequency band (LFB) of primary users (PUs) without harming signal reception of PUs, hence drastically enhancing spectral efficiency and reducing spectrum scarcity problem [5]. In the underlay mechanism, CUs have access permission to the LFB solely if CUs limit interference power induced at PUs under a tolerable degree. CUs working in the overlay mechanism access simultaneously the LFB with PUs; yet, performance indicators of PUs are remained or enhanced with complicated signal processing techniques. On the contrary, the interweave mechanism only leaves unused bandwidth of PUs for CUs' access. While most literature has intensively studied the underlay and interweave mechanisms, a handful of works have concentrated on the overlay mechanism. Since the overlay mechanism can

compromise performances between cognitive and primary communications better than other mechanisms, it greatly attracts this paper.

Viable solutions to improve energy efficiency of wireless networks can be listed as network planning, hardware solutions, radio frequency (RF) energy harvesting, etc. Among these solutions, harvesting energy from RF signals neither demands complex energy harvesting equipments nor depends time-variant energy resources. Such advantages of this energy harvesting solution induce it to become a bright candidate deployed in small-size users in 5G mobile communications or IoT to provision energy, linger the life-time, and enhance energy efficiency [6–8]. Currently, this solution can be carried out through SWIPT (simultaneous wireless information and power transfer) [9–11] or relaying communications [12–14].

Energy harvesting overlay networks (EHONs) can exploit concurrently advantages of both applicable (energy harvesting and cognitive radio) technologies to satisfy various design metrics of advanced networks including high-energy and spectral efficiencies [15, 16]. Nonetheless, both cognitive and primary users in these networks are allowed to transmit on the LFB concomitantly that may facilitate eavesdroppers in emulating legal users to overhear privacy messages, seriously alerting security problems. To supplement and enhance security performance for conventional encryption and cryptographic solutions, physical layer security (PHY security) has lately been emerged as a promising candidate [17–19]. PHY security can be deployed with numerous techniques, including relaying and jamming. Among these techniques, jamming (or generating artificial noise) has been widely exploited thanks to its efficient, simple, and flexible implementation [20]. Accordingly, this paper generates artificial noise in EHONs to secure communications for both primary and cognitive users.

1.1. Existing Publications. This paper studies the impact of artificial noise in EHONs where a primary transmitter cannot connect directly a primary receiver in some scenarios (e.g., heavy shadowing), and hence a cognitive transmitter supports primary communications in exchange for its access to the LFB. The cognitive transmitter operating in the amplify-and-forward (AF) mechanism scavenges RF energy in the primary transmitter's signals and sends not only its privacy signal but also the primary transmitter's signal and artificial noise. Message transmission of the cognitive transmitter is overheard by an eavesdropper.

Whilst most publications have investigated the PHY security for energy harvesting (interweave/underlay) networks, a handful works have paid attention to the overlay mechanism [5, 21–28]. More specifically, [21] investigated the almost similar system model to ours but EHONs are secured by asking a devoted jammer to jam the eavesdropper. In [22, 23], the primary receiver was exploited to corrupt the eavesdropper rather than the devoted jammer as in [21]. Additionally, [21] disagrees [22, 23] in the energy harvesting (EH) technique, the EH-capable device, and the assistance mechanism. The former utilized the cognitive transmitter as a decode-and-forward (DF) relay and exploited the EH-capable jammer which scavenges energy based on the time switching protocol [29]. Meanwhile, the latter employed the cognitive transmitter as the AF relay and as an energy scavenger that bases on the power splitting protocol [30]. To better secure primary communications, [24] suggested to jam the eavesdropper by the primary receiver as well as the dedicated jammer. Nonetheless, the analysis on the secrecy outage probability (SOP) of both primary and cognitive communications was not reported in [21–24]. In [25], EHONs are secured with the multiuser scheduling and the transmit antenna selection. Moreover, [25] analyzed the SOP/ergodic rate of primary/cognitive communications. Recently, a bulk of dedicated jammers were recommended to secure EHONs, and the SOP of cognitive and primary communications was suggested in closed form [5]. Nevertheless, distinguishing from [21–24], the cognitive user relays the primary signal and sends its privacy signal independently in [5, 25]. This demands at least three phases (phase 1: energy scavenging and PU's communications, phase 2: CU's communications to PU, and phase 3: CU's communications to CU) to complete message communications of both PU and CU, reducing drastically spectral efficiency and analysis complexity. As such, the closed-form analysis on the ergodic rate of cognitive communications and the SOP of cognitive and primary communications in [5, 25] are tractable.

Lately, [26–28] suggested that a two-phase ([26, 28] are conference versions where [26] considered Rayleigh fading while [28] generalized [26] with Nakagami-m fading. Because of conference versions, [26, 28] briefly outlined few results without any proof) transmission scheme incorporated with artificial noise generation in EHONs to enhance spectral efficiency and security capability. Moreover, [26–28] analyzed the SOP of cognitive and primary communications in EHONs. Nonetheless, similarly to [5, 25], the authors in [26–28] considered the DF cognitive users, which may cease primary communications if CUs fail to restore primary message.

1.2. Contributions. The current paper contributes the following:

(i) Suggest a new operation principle of the cognitive transmitter which permits it to scavenge energy from the primary transmitter, amplify and forward primary signal, and create a signal combination of primary signal, cognitive signal, and artificial noise. This principle is flexible in trading-off the security capability of primary communications with that of cognitive communications and optimizing system design by appropriately adopting (time switching, power splitting, power allocation) coefficients. It is reminded that compared to the DF cognitive transmitter in [5] and [26–28], the AF cognitive transmitter in this paper is simpler and prevents error propagation. Moreover, the AF cognitive transmitter in this paper always maintains primary communications while the DF cognitive transmitter in [5, 26–28] assures primary communications only when it decodes correctly primary message

(ii) Suggest a novel signal model to represent signals/-quantities corresponding to the considered operation principle of the cognitive transmitter, from which the performance metrics are formulated

(iii) Propose accurate pivotal security performance indicator expressions for quickly assessing the impact of artificial noise on the security performance of both cognitive and primary communications. The indicators are the SOP, secrecy throughput, intercept probability, and positive secrecy capacity probability. Furthermore, these expressions are applicable to both nonlinear and linear energy harvesting models

(iv) Show the presence of optimal pivotal specifications for the optimal security capability and the optimal security trade-off between cognitive and primary communications

(v) Supply various insightful results on the security capability of cognitive/primary communications in key specifications

1.3. Outline. The next part describes the system model. Derivations of accurate pivotal security performance indicator expressions are presented in part 3. Illustrative results are provided in part 4 and eventually, and part 5 ends the paper.

2. System Description

2.1. System Model. Figure 1 demonstrates an EHON where the primary transmitter-receiver pair, $T-R$, cannot communicate to each other directly owing to channel impairments (e.g., deep fading). Consequently, the cognitive transmitter S, which is in the coverage range of T, can aid T by relaying T's message to R. It is assumed that S is able to scavenge the RF energy in signals of T and spends the scavenged energy for its operation. Moreover, S operates in the overlay mechanism where it relays T's message to R and transmits its privacy data to the cognitive receiver D. Communications of S is overheard by an eavesdropper E. In order to mitigate the overhearing capability of E, S sends artificial noise together with messages of T and S.

Figure 1 denotes h_{sp}, h_{sd}, h_{se}, and h_{ps} as ($S \to R$, $S \to D$, $S \to E$, $T \to S$) channel coefficients, respectively. This paper models these channel coefficients as $h_{sp} \sim \mathcal{CN}(0, \mu_{sp})$, $h_{sd} \sim \mathcal{CN}(0, \mu_{sd})$, $h_{se} \sim \mathcal{CN}(0, \mu_{se})$, and $h_{\mathrm{ps}} \sim \mathcal{CN}(0, \mu_{\mathrm{ps}})$, correspondingly. Such a channel coefficient model indicates Rayleigh fading channels. Integrating path loss into channel characteristics models μ_{ab} with $a \in \{p, s\}$ and $b \in \{s, p, d, e\}$ as $\mu_{ab} = d_{ab}^{-\rho}$ in which ρ is the path-loss exponent and d_{ab} is the $a-b$ distance. Then, $f_{g_{ab}}(x) = e^{-x/\mu_{ab}}/\mu_{ab}$ and $F_{g_{ab}}(x) = 1 - e^{-x/\mu_{ab}}$ are correspondingly the probability density function (PDF) and the cumulative distribution function (CDF) of the channel gain $g_{ab} = |h_{ab}|^2$.

The total transmission time τ for both T and S to finish data transmission to corresponding receivers comprises two phases as seen in Figure 1. In phase 1 of $\alpha\tau$ with $\alpha \in (0, 1)$ being the time switching factor, T with the transmission power of P_p sends its symbol x_p for S to harvest energy relied on the power splitting protocol and amplify T's signal. Such a protocol divides S's received signal into two parts: one part $\sqrt{\lambda}y_s$ (y_s is S's received signal, and $\lambda \in (0, 1)$ is the power splitting factor) for harvesting energy and another part $\sqrt{1-\lambda}y_s$ for amplifying T's signal (signal processing at S consumes assumedly negligible energy. Such an assumption is acceptable in previous works (e.g., [5–16, 21–25, 29, 30]). In phase 2 of $(1-\alpha)\tau$, S broadcasts a superposition of three signals: amplified primary signal, cognitive signal, and artificial noise.

2.2. Signal Model. In phase 1, S receives the signal

$$y_s = h_{ps}\sqrt{P_p}x_p + n_s, \tag{1}$$

where the received antenna of S creates the additive white Gaussian noise (AWGN) $n_s \sim \mathcal{CN}(0, \sigma_s^2)$.

Based on Figure 1, the harvested energy of S is

$$E_s = \eta\Xi\left\{\left|\sqrt{\lambda}y_s\right|^2\right\}\alpha\tau = \eta\lambda\left(P_p g_{ps} + \sigma_s^2\right)\alpha\tau \approx \alpha\eta\lambda P_p g_{ps}\tau, \tag{2}$$

where $\eta \in (0, 1)$ is the energy conversion efficiency, and $\Xi\{\cdot\}$ is the expectation operator. The approximation in (2) holds because the signal power dominates the noise power.

In phase 2, S has transmission power as

$$P_s = \frac{E_s}{(1-\alpha)\tau} \approx AP_p g_{ps}, \tag{3}$$

where $A = \alpha\eta\lambda/(1-\alpha)$.

One of the inputs of the signal generator in Figure 1 is $\tilde{y}_s = \sqrt{1-\lambda}y_s + \tilde{n}_s$ where $\tilde{n}_s \sim \mathcal{CN}(0, \tilde{\sigma}_s^2)$ is the AWGN owing to the passband-to-baseband signal conversion. Superseding (1) into $\tilde{y}_s$ yeilds

$$\tilde{y}_s = \sqrt{(1-\lambda)P_p}h_{ps}x_p + \sqrt{1-\lambda}n_s + \tilde{n}_s. \tag{4}$$

The signal generator amplifies $\tilde{y}_s$ before combining with cognitive signal and artificial noise. More specifically, the signal generator creates the signal $\bar{x}_s = \beta\tilde{y}_s + \sqrt{\theta(1-\kappa)P_s}x_s + \sqrt{(1-\theta)P_s}x_a$ where β is the amplification factor, θ is the power allocation factor for desired signals and artificial noise, κ is the power allocation factor for cognitive and primary signals, x_s is S's the unit power symbol, and x_a is the unit power artificial noise. The amplification factor β is determined so that the total power of S is P_s. Consequently, the power to amplify the primary signal is $\theta\kappa P_s$ from which β is given by

$$\beta = \sqrt{\frac{\theta\kappa P_s}{\Xi\{|\tilde{y}_s|^2\}}} = \sqrt{\frac{\theta\kappa P_s}{(1-\lambda)P_p g_{ps} + (1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2}}. \tag{5}$$

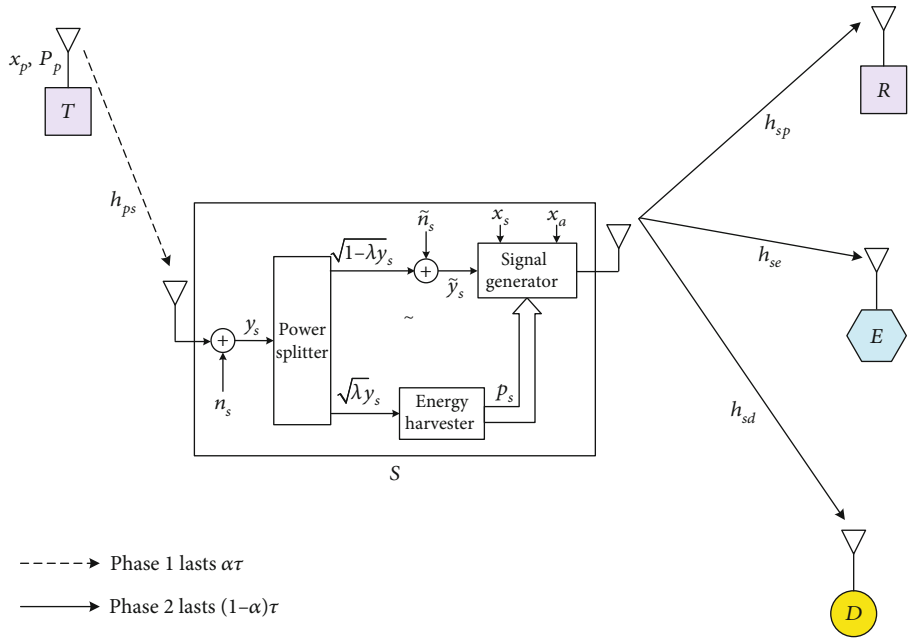

Figure 1: System model.

In phase 2, the received signals at R, D, E are correspondingly represented as

$$y_p = h_{sp}\bar{x}_s + n_p, y_d = h_{sd}\bar{x}_s + n_d, y_e = h_{se}\bar{x}_s + n_e, \quad (6)$$

where the received antennas of R, D, E induce the noises $n_p \sim \mathcal{CN}(0, \sigma_p^2)$, $n_d \sim \mathcal{CN}(0, \sigma_d^2)$, and $n_e \sim \mathcal{CN}(0, \sigma_e^2)$, respectively.

S purposely generates the artificial noise x_a to solely deteriorate the wire tapping of E but not to mitigate the performance of the legitimate receivers (D, R). Such artificial noise generation can be implemented by enabling S to share. For instance, the artificial noise generator at S has the seed that is shared with D and R securely through a collaboration contract solely among S, D, and R prior to any start of message transmission. Open literature widely accepted this artificial noise generating mechanism (e.g., [5, 20, 22, 23]).x_a with D and R. Consequently, the legitimate receivers (D, R) are able to reproduce accurately the artificial noise and perfectly annihilate it, eventually yielding the artificial noise-free signals at R and D as

$$\tilde{y}_p = h_{sp}\tilde{x}_s + n_p, \tilde{y}_d = h_{sd}\tilde{x}_s + n_d, \quad (7)$$

where $\tilde{x}_s = \beta\tilde{y}_s + \sqrt{\theta(1-\kappa)P_s}x_s$.

Inserting $\tilde{y}_s$ in (4) into $\tilde{x}_s$ and then substituting $\tilde{x}_s$ into (7), one rewrites (7) as

$$\begin{aligned}\tilde{y}_p = {} & \sqrt{(1-\lambda)P_p}h_{sp}\beta h_{ps}x_p + h_{sp}\sqrt{\theta(1-\kappa)P_s}x_s \\ & + h_{sp}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + n_p,\end{aligned} \quad (8)$$

$$\begin{aligned}\tilde{y}_d = {} & \sqrt{(1-\lambda)P_p}h_{sd}\beta h_{ps}x_p + h_{sd}\sqrt{\theta(1-\kappa)P_s}x_s \\ & + h_{sd}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + n_d,\end{aligned} \quad (9)$$

from which signal-to-interference plus noise ratios (SINRs) for recovering x_p at R and x_s at D are, respectively, given by

$$\begin{aligned}\gamma_p &= \frac{\Xi\left\{\left|\sqrt{(1-\lambda)P_p}h_{sp}\beta h_{ps}x_p\right|^2\right\}}{\Xi\left\{\left|h_{sp}\sqrt{\theta(1-\kappa)P_s}x_s + h_{sp}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + n_p\right|^2\right\}} \\ &= \frac{(1-\lambda)P_p g_{sp}g_{ps}\beta^2}{g_{sp}\theta(1-\kappa)P_s + g_{sp}\beta^2\left([1-\lambda]\sigma_s^2 + \tilde{\sigma}_s^2\right) + \sigma_p^2},\end{aligned} \quad (10)$$

$$\begin{aligned}\gamma_d &= \frac{\Xi\left\{\left|h_{sd}\sqrt{\theta(1-\kappa)P_s}x_s\right|^2\right\}}{\Xi\left\{\left|\sqrt{(1-\lambda)P_p}h_{sd}\beta h_{ps}x_p + h_{sd}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + n_d\right|^2\right\}} \\ &= \frac{\theta(1-\kappa)P_s g_{sd}}{(1-\lambda)P_p g_{ps}g_{sd}\beta^2 + g_{sd}\beta^2\left([1-\lambda]\sigma_s^2 + \tilde{\sigma}_s^2\right) + \sigma_d^2}.\end{aligned} \quad (11)$$

Substituting P_s in (3) and β in (5) into (10) and (11) and after some manipulations, one simplifies (10) and (11) as

$$\gamma_p = \frac{Gg_{sp}}{Hg_{sp} + J}, \quad (12)$$

$$\gamma_d = \frac{\bar{G}g_{sd}}{\bar{H}g_{sd} + \bar{J}}, \quad (13)$$

where $B = \sigma_s^2 + \tilde{\sigma}_s^2/(1-\lambda)$, $\bar{J} = \sigma_d^2$,

$$G = \theta\kappa A P_p^2 g_{ps}^2, \tag{14}$$

$$H = \theta A\left[B + (1-\kappa)P_p g_{ps}\right]P_p g_{ps}, \tag{15}$$

$$J = \left(P_p g_{ps} + B\right)\sigma_p^2, \tag{16}$$

$$\bar{G} = \theta(1-\kappa)AP_p g_{ps}, \tag{17}$$

$$\bar{H} = \theta\kappa AP_p g_{ps}. \tag{18}$$

Inserting (4) into $\bar{x}_s$ and then plugging $\bar{x}_s$ into y_e in (6), one rewrites (6) for E as

$$\begin{aligned} y_e = {} & h_{se}\beta\sqrt{(1-\lambda)P_p}h_{ps}x_p + h_{se}\sqrt{\theta(1-\kappa)P_s}x_s \\ & + h_{se}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + h_{se}\sqrt{(1-\theta)P_s}x_a + n_e. \end{aligned} \tag{19}$$

The understanding of the artificial noise x_a is known at R, D, and S for protecting x_s and x_p; yet, E does not know x_a. Consequently, the SINRs at E for recovering x_s and x_p are derived from (19), respectively, as

$$\begin{aligned} \gamma_e^s &= \frac{\Xi\left\{\left|h_{se}\sqrt{\theta(1-\kappa)P_s}x_s\right|^2\right\}}{\Xi\left\{\left|h_{se}\beta\sqrt{(1-\lambda)P_p}h_{ps}x_p + h_{se}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + h_{se}\sqrt{(1-\theta)P_s}x_a + n_e\right|^2\right\}} \\ &= \frac{g_{se}\theta(1-\kappa)P_s}{(1-\lambda)P_p\beta^2 g_{se}g_{ps} + g_{se}\beta^2\left[(1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2\right] + g_{se}(1-\theta)P_s + \sigma_e^2}, \end{aligned} \tag{20}$$

$$\begin{aligned} \gamma_e^p &= \frac{\Xi\left\{\left|h_{se}\beta\sqrt{(1-\lambda)P_p}h_{ps}x_p\right|^2\right\}}{\Xi\left\{\left|h_{se}\sqrt{\theta(1-\kappa)P_s}x_s + h_{se}\beta\left(\sqrt{1-\lambda}n_s + \tilde{n}_s\right) + h_{se}\sqrt{(1-\theta)P_s}x_a + n_e\right|^2\right\}} \\ &= \frac{(1-\lambda)P_p\beta^2 g_{se}g_{ps}}{g_{se}\theta(1-\kappa)P_s + g_{se}\beta^2\left[(1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2\right] + g_{se}(1-\theta)P_s + \sigma_e^2}. \end{aligned} \tag{21}$$

Equations (20) and (21) expose that S intentionally produces the amount of the artificial noise power, $g_{se}(1-\theta)P_s$, to interfere the eavesdropper. As such, boosting this amount would secure message transmission for x_s and x_p.

Substituting P_s in (3) and β in (5) into (20) and (21) and after some manipulations, one simplifies (20) and (21) as

$$\gamma_e^s = \frac{\bar{G}g_{se}}{\bar{U}g_{se} + \bar{J}}, \tag{22}$$

$$\gamma_e^p = \frac{Gg_{se}}{Ug_{se} + J}, \tag{23}$$

where

$$U = A\left[B + (1-\theta\kappa)P_p g_{ps}\right]P_p g_{ps}, \tag{24}$$

$$\bar{U} = (1-\theta+\theta\kappa)AP_p g_{ps}, \tag{25}$$

and $\sigma_s^2 = \sigma_e^2 = \sigma_d^2 = \sigma_p^2 = \tilde{\sigma}_s^2 = N_0$ is assumed without loss of generality.

The channel capacities of D and R in phase 2 are, respectively, given by

$$C_d = (1-\alpha)\log(1+\gamma_d), \tag{26}$$

$$C_p = (1-\alpha)\log\left(1+\gamma_p\right), \tag{27}$$

where phase 2 of $(1-\alpha)\tau$ induces the prelogarithm factor $(1-\alpha)$.

Similarly, the channel capacities at E for decoding x_p and x_s in phase 2 are deduced, respectively, as

$$C_{Ep} = (1-\alpha)\log(1+\gamma_e^p), \tag{28}$$

$$C_{Es} = (1-\alpha)\log(1+\gamma_e^s). \tag{29}$$

The capacity difference between R and E for restoring x_p is defined as the secrecy capacity for x_p:

$$\tilde{C}_p = \left[C_p - C_{Ep}\right]^+ = (1-\alpha)\left[\log\frac{1+\gamma_p}{1+\gamma_e^p}\right]^+, \tag{30}$$

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

Similarly, the capacity difference between D and E for restoring x_s is the secrecy capacity for x_s:

$$\tilde{C}_s = (1-\alpha)\left[\log\frac{1+\gamma_d}{1+\gamma_e^s}\right]^+. \tag{31}$$

3. Security Analysis

The vital performance indicator to rate the security performance of wireless transmission is the SOP that is the probability of the secrecy capacity below the required security degree C_0. In this section, accurate SOP expressions are firstly proposed to quickly assess the security performance for x_p and x_s without time-consuming simulations. Then, other vital security capability indicators including the positive secrecy capacity possibility (PSCP), the intercept possibility (IP), and the secrecy throughput (ST) are derived from the SOP formulas.

3.1. SOP for the Primary Message x_p. The SOP for the primary message x_p is defined as

$$\mathcal{O}_p(C_0) = \Pr\left\{\tilde{C}_p < C_0\right\}. \tag{32}$$

Plugging $\tilde{C}_p$ in (30) into (32) results in

$$\mathcal{O}_p(C_0) = \Xi_{g_{ps}}\left\{\Psi\left(g_{ps}\right)\right\}, \tag{33}$$

where $X = 1 + Gg_{sp}/(Hg_{sp} + J)$, $Y = 1 + Gg_{se}/(Ug_{se} + J)$, $D = 2^{C_0/(1-\alpha)}$, and

$$\Psi\left(g_{ps}\right) = \Pr\left\{X < DY | g_{ps}\right\}. \tag{34}$$

To numerically assess (33), one needs the exact closed-form expression of $\Psi(g_{ps})$ in (34), which is presented as follows.

The accurate expression of $\Psi(g_{ps})$ is

$$\Psi\left(g_{ps}\right) = \begin{cases} 1 - Re^{\frac{J}{\mu_{sp}H} + \frac{J}{\mu_{se}U}}\Lambda, & K < V \\ 1 - Re^{\frac{J}{\mu_{sp}H} + \frac{J}{\mu_{se}U}}\varphi, & 1 \le V < K \\ 1, & V < 1 \end{cases}, \tag{35}$$

where

$$L = \frac{G}{H} + 1, \tag{36}$$

$$K = \frac{G}{U} + 1, \tag{37}$$

$$V = \frac{L}{D}, \tag{38}$$

$$M = \frac{1}{K-1} - \frac{1}{K-V}, \tag{39}$$

$$N = \frac{1}{V-1} + \frac{1}{K-V}, \tag{40}$$

$$Q = \frac{JG}{\mu_{sp}H^2D}, \tag{41}$$

$$R = \frac{JG}{\mu_{se}U^2}, \tag{42}$$

$$\begin{aligned} \Lambda = e^{\frac{Q}{K-V}} \Bigg\{ & \frac{1}{R} e^{-\frac{R}{K-1}} - \frac{Q}{(K-V)^2} e^{\frac{R}{V-K}} Ei(-RM) \\ & + \sum_{g=2}^{\infty} \frac{Q^g(-R)^{g-1}}{(K-V)^{2g} g!(g-1)!} \\ & \cdot \left[e^{-\frac{R}{K-1}} \sum_{c=1}^{g-1} \frac{(c-1)!}{(-RM)^c} - e^{\frac{R}{V-K}} Ei(-RM) \right] \Bigg\}, \end{aligned} \tag{43}$$

$$\begin{aligned} \varphi = & \frac{e^{R/(V-K)}}{(V-K)^2} \sum_{g=0}^{\infty} \frac{R^g(-Q)^{g+1}}{(V-K)^{2g} g!(g+1)!} \\ & \cdot \left[e^{-\frac{Q}{V-1}} \sum_{c=1}^{g+1} \frac{(c-1)!}{(-QN)^c} - e^{\frac{Q}{K-V}} Ei(-QN) \right], \end{aligned} \tag{44}$$

with $Ei(x)$being the exponential-integral function [31].

$\Psi(g_{ps})$ in (35) can be shown with the help of Appendix C in [27] and some proper variable changes.

Because $\Psi(g_{ps})$ is a function of random variables (G, H, J, U) which are also functions of the random variable g_{ps} according to (14), (15), (16), and (24), $\mathcal{O}_p(C_0)$ in (33) is computed through the single-variable integral as

$$\mathcal{O}_p(C_0) = \int_0^{\infty} \Psi(x) f_{g_{ps}}(x) dx = \int_0^{\infty} \Psi(x) \frac{e^{-x/\mu_{ps}}}{\mu_{ps}} dx. \tag{45}$$

In order to compute (45), one must determine $\Psi(x)$ in (35) for the specific value of x. Towards this end, one considers two expressions, $K - V$ and $V - 1$, which are functions of $x = g_{ps}$. By using K in (37) and V in (38), one can, respectively, express $K - V$ and $V - 1$ as

$$K - V = (D - 1 + \theta\kappa - D\kappa)(x - x_1)(x - x_2), \tag{46}$$

$$V - 1 = (D\kappa - D + 1)x - B(D-1)/P_p, \tag{47}$$

where $x_1 = -B/P_p$ and $x_2 = -B(D-1)/P_p(D - 1 + \theta\kappa - D\kappa)$.

It is straightforward to infer cases in Table 1 where $\bar{x} = B(D-1)/P_p(D\kappa - D + 1)$. Based on Table 1, three cases are considered to compute (45) as follows.

Case 1. $D < (1 - \theta\kappa)/(1 - \kappa)$.

This case results in

$$\begin{cases} x > x_2, & K < V \\ \bar{x} < x < x_2, & 1 < V < K \\ x < \bar{x}, & V < 1 \end{cases}, \tag{48}$$

and hence

$$\begin{aligned} \mathcal{O}_p(C_0) = & \int_0^{\bar{x}} \frac{e^{-x/\mu_{ps}}}{\mu_{ps}} dx + \int_{\bar{x}}^{x_2} \left(1 - Re^{\frac{J}{\mu_{sp}H} + \frac{J}{\mu_{se}U}}\varphi\right) \frac{e^{-x/\mu_{ps}}}{\mu_{ps}} dx \\ & + \int_{x_2}^{\infty} \left(1 - Re^{\frac{J}{\mu_{sp}H} + \frac{J}{\mu_{se}U}}\Lambda\right) \frac{e^{-x/\mu_{ps}}}{\mu_{ps}} dx = 1 - \frac{A_1}{\mu_{ps}}, \end{aligned} \tag{49}$$

where $A_1 = \int_{\bar{x}}^{x_2} R\varphi e^{(J/\mu_{sp}H) + (J/\mu_{se}U) - x/\mu_{ps}} dx + \int_{x_2}^{\infty} R\Lambda e^{(J/\mu_{sp}H) + (J/\mu_{se}U) - x/\mu_{ps}} dx$.

Case 2. $(1 - \theta\kappa)/(1 - \kappa) < D < 1/(1 - \kappa)$.

This case results in

$$\begin{cases} \bar{x} < x, & 1 < V < K \\ x < \bar{x}, & V < 1 \end{cases}, \tag{50}$$

Table 1: Inequalities: $K > V$ and $V > 1$.

$D > \frac{1-\theta\kappa}{1-\kappa}$	$D < \frac{1-\theta\kappa}{1-\kappa}$		$D < \frac{1}{1-\kappa}$		$D > \frac{1}{1-\kappa}$
$V < K$	$V > K$	$V < K$	$V > 1$	$V < 1$	$V < 1$
	$x > x_2$	$x < x_2$	$x > \bar{x}$	$x < \bar{x}$	

and thus

$$\mathcal{O}_p(C_0) = \int_0^{\bar{x}} \frac{e^{-x/\mu_{ps}}}{\mu_{ps}} dx + \int_{\bar{x}}^{\infty} \left(1 - Re^{\frac{J}{\mu_{sp}H} + \frac{J}{\mu_{se}U}} \varphi\right) \frac{e^{-x/\mu_{ps}}}{\mu_{ps}} dx = 1 - \frac{A_2}{\mu_{ps}}, \tag{51}$$

where $A_2 = \int_{\bar{x}}^{\infty} R\varphi e^{(J/\mu_{sp}H)+(J/\mu_{se}U)-x/\mu_{ps}} dx$.

Case 3. $1/(1-\kappa) < D$.

This case results in $V < 1$, and thus

$$\mathcal{O}_p(C_0) = 1. \tag{52}$$

In summary, the SOP for the primary message x_p is expressed as

$$\mathcal{O}_p(C_0) = \begin{cases} 1 - \frac{A_1}{\mu_{ps}}, & D < \frac{1-\theta\kappa}{1-\kappa} \\ 1 - \frac{A_2}{\mu_{ps}}, & \frac{1-\theta\kappa}{1-\kappa} < D < \frac{1}{1-\kappa} \\ 1, & \frac{1}{1-\kappa} < D \end{cases}. \tag{53}$$

3.2. SOP for the Cognitive Message x_s. The SOP for the cognitive message x_s is expressed as

$$\mathcal{O}_s(C_0) = \Pr\left\{\tilde{C}_s < C_0\right\}. \tag{54}$$

Inserting $\tilde{C}_s$ in (31) into (54) yields

$$\mathcal{O}_s(C_0) = \Xi_{g_{ps}}\left\{Y\left(g_{ps}\right)\right\}, \tag{55}$$

where

$$Y\left(g_{ps}\right) = \Pr\left\{\frac{1 + \bar{G}g_{sd}/\left(\bar{H}g_{sd} + \bar{J}\right)}{1 + \bar{G}g_{se}/\left(\bar{U}g_{se} + \bar{J}\right)} < D \middle| g_{ps}\right\}. \tag{56}$$

Both Y in (56) and Ψ in (34) share a similar form. Accordingly, by substituting variables appropriately into Ψ in (35), one achieves the accurate expression of Y. More specifically, Y is computed by using Ψ in (35) with $G \to \bar{G}$, $H \to \bar{H}$, $J \to \bar{J}$, $U \to \bar{U}$, and $\mu_{sp} \to \mu_{sd}$. Consequently, the derivation of Y is ignored here for compactness.

Since $Y(g_{ps})$ is a function of random variables $(\bar{G}, \bar{H}, \bar{U})$ which are also functions of the random variable g_{ps} according to (17), (18), and (25), $\mathcal{O}_s(C_0)$ in (55) is computed as

$$\mathcal{O}_s(C_0) = \int_0^{\infty} Y(x) f_{g_{ps}}(x) dx. \tag{57}$$

In order to compute (57), it should be noted that $\bar{K} = (\bar{G}/\bar{U}) + 1 = 1/(1 - \theta + \theta\kappa)$ and $\bar{V} = (\bar{L}/D) = (\bar{G}/\bar{H} + 1)/D = (1/D\kappa)$ are constants. Therefore, (57) is explicitly rewritten as

$$\mathcal{O}_s(C_0) = \begin{cases} 1 - \frac{1}{\mu_{ps}} \int_0^{\infty} \bar{R} e^{\frac{\bar{J}}{\mu_{sd}\bar{H}} + \frac{\bar{J}}{\mu_{se}\bar{U}} - \frac{x}{\mu_{ps}}} \bar{\Lambda} dx, & \bar{K} < \bar{V} \\ 1 - \frac{1}{\mu_{ps}} \int_0^{\infty} \bar{R} e^{\frac{\bar{J}}{\mu_{sd}\bar{H}} + \frac{\bar{J}}{\mu_{se}\bar{U}} - \frac{x}{\mu_{ps}}} \bar{\varphi} dx, & 1 \le \bar{V} < \bar{K} \\ 1, & \bar{V} < 1 \end{cases}$$

$$= \begin{cases} 1 - \frac{1}{\mu_{ps}} \int_0^{\infty} \bar{R} e^{\frac{\bar{J}}{\mu_{sd}\bar{H}} + \frac{\bar{J}}{\mu_{se}\bar{U}} - \frac{x}{\mu_{ps}}} \bar{\Lambda} dx, & D < \frac{1-\theta+\theta\kappa}{\kappa} \\ 1 - \frac{1}{\mu_{ps}} \int_0^{\infty} \bar{R} e^{\frac{\bar{J}}{\mu_{sd}\bar{H}} + \frac{\bar{J}}{\mu_{se}\bar{U}} - \frac{x}{\mu_{ps}}} \bar{\varphi} dx, & \frac{1-\theta+\theta\kappa}{\kappa} \le D < \frac{1}{\kappa}, \\ 1, & D > \frac{1}{\kappa} \end{cases} \tag{58}$$

where $x = g_{ps}$ and $\bar{R}$, $\bar{\Lambda}$, $\bar{\varphi}$ are correspondingly achieved from R, Λ, ad φ with $G \to \bar{G}$, $H \to \bar{H}$, $J \to \bar{J}$, $U \to \bar{U}$, and $\mu_{sp} \to \mu_{sd}$.

3.3. Comments

3.3.1. Absolute Unsecurity. Since $D = 2^{C_0/(1-\alpha)}$, (53) and (58) show that the SOP for the primary/cognitive message takes different values dependent on the correlation among C_0, α, θ, and κ. Especially, the primary (or cognitive) communications are absolutely unsecured when $\kappa < 1 - 2^{-C_0/(1-\alpha)}$ or $\kappa > 2^{-C_0/(1-\alpha)}$.

3.3.2. Vital Security Performance Measures. The accurate expressions of $\mathcal{O}_p$ and $\mathcal{O}_s$ can be numerically computed by multiple softwares such as Mathematica and Matlab. Accordingly, such expressions are useful in quickly rating the influence of artificial noise on the secrecy performance of both cognitive and primary transmission in EHONs without exhaustive simulations. Upon our knowledge, these formulas are novel. Furthermore, they facilitate in deriving the formulas for other vital security performance measures. More specifically, the IP is the possibility of the negative secrecy capacity. Accordingly, the IP of primary/cognitive communications is obtained as

$$IP_v = \Pr\left\{\tilde{C}_v < 0\right\} = \mathcal{O}_v(0), \tag{59}$$

where $v = s, p$.

The PSCP is the possibility of the positive secrecy capacity. Consequently, the PSCP of primary/cognitive communications is represented as

$$PSCP_v = \Pr\left\{\tilde{C}_v > 0\right\} = 1 - \mathcal{O}_v(0). \tag{60}$$

Eventually, the ST is the multiplication of the secrecy communication possibility at a certain secrecy capacity with that secrecy capacity. Consequently, the ST of primary/cognitive communications is achieved as

$$ST_v = [1 - \mathcal{O}_v(C_0)]C_0. \tag{61}$$

3.3.3. Nonlinear Energy Harvesting. This paper mainly focuses on the linear energy harvesting (LEH) model in (2). Nonetheless, our analytical results are still extended to the nonlinear energy harvesting (NLEH) models (e.g., [32, 33]). Indeed, for the NLEH models, P_s in (3) is a nonlinear function of g_{ps}. Therefore, the forms of γ_p in (12), γ_d in (13), γ_e^s in (22), and γ_e^p in (23) are unchanged for the NLEH models. Nonetheless, some quantities in (12), (13), (22), and (23), which are functions of P_s, are different for the LEH and NLEH models. More specifically, for the NLEH models, γ_p in (12), γ_d in (13), γ_e^s in (22), and γ_e^p in (23) are correspondingly expressed as

$$\tilde{\gamma}_p = \frac{\tilde{G}g_{sp}}{\tilde{H}g_{sp} + \sigma_p^2}, \tag{62}$$

$$\tilde{\gamma}_d = \frac{\tilde{\tilde{G}}g_{sd}}{\tilde{\tilde{H}}g_{sd} + \sigma_d^2}, \tag{63}$$

$$\tilde{\gamma}_e^s = \frac{\tilde{\tilde{G}}g_{se}}{\tilde{\tilde{U}}g_{se} + \sigma_e^2}, \tag{64}$$

$$\tilde{\gamma}_e^p = \frac{\tilde{G}g_{se}}{\tilde{U}g_{se} + \sigma_e^2}, \tag{65}$$

where $\tilde{G} = (1-\lambda)P_p g_{ps}\beta^2$, $\tilde{H} = \theta(1-\kappa)P_s + \beta^2([1-\lambda]\sigma_s^2 + \tilde{\sigma}_s^2)$, $\tilde{\tilde{G}} = \theta(1-\kappa)P_s$, $\tilde{\tilde{H}} = (1-\lambda)P_p g_{ps}\beta^2 + \beta^2([1-\lambda]\sigma_s^2 + \tilde{\sigma}_s^2)$, $\tilde{\tilde{U}} = (1-\lambda)P_p\beta^2 g_{ps} + \beta^2[(1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2] + (1-\theta)P_s$, and $\tilde{U} = \theta(1-\kappa)P_s + \beta^2[(1-\lambda)\sigma_s^2 + \tilde{\sigma}_s^2] + (1-\theta)P_s$.

Since β is a function of g_{ps}, the quantities ($\tilde{G}$, $\tilde{H}$, $\tilde{\tilde{G}}$, $\tilde{\tilde{H}}$, $\tilde{\tilde{U}}$, $\tilde{U}$) are just functions of g_{ps}. Therefore, for the NLEH models, the SOP for the primary message, $\mathcal{O}_p(C_0)$, and the SOP for the cognitive message, $\mathcal{O}_s(C_0)$, can be, respectively, computed by using (45) and (57) with appropriate variable changes.

4. Illustrative Results

The SOPs of both primary and cognitive communications in EHONs are assessed through pivotal specifications. For demonstration purposes, some specifications are randomly specified as the primary receiver R at $(0.4,-0.2)$, the primary transmitter T at $(-0.2,0.2)$, the eavesdropper E at $(0.5,-0.1)$, the cognitive receiver D at $(0.5,0.0)$, the cognitive transmitter S at $(d, 0.0)$, the energy conversion efficiency $\eta = 0.9$, and the path-loss exponent $\rho = 3$. In the following figures, the simulated result is denoted as "Sim," while the theoretical results in (53) and (58) are denoted as "The.". Furthermore, these figures are generated with a set of specifications (the primary transmission power-to-noise variance ratio $P_p/N_0 = 10$ dB, $d = 0.0$, the power splitting factor $\lambda = 0.6$, the power allocation factor for primary and cognitive signals $\kappa = 0.6$, the power allocation factor for desired signals and artificial noise $\theta = 0.7$, and the target security degree $C_0 = 0.1$ bits/s/Hz) unless stated otherwise. These figures expose that the theoretical and simulated results are in a perfect match, validating the exactness of (53) and (58).

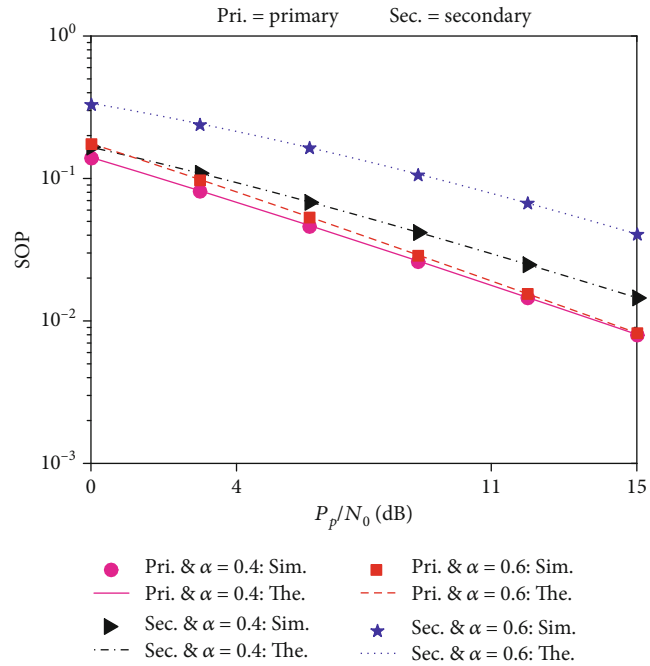

Figure 2: SOPs w.r.t P_p/N_0.

Figure 2 demonstrates the SOPs with respect to (w.r.t) P_p/N_0. This figure exposes that the security performance is proportional to P_p/N_0, which is interpreted as follows. Increasing P_p/N_0 facilitates S to scavenge more energy from T and thus increasing the SINRs in phase 2 and reducing the SOPs. Furthermore, the security performance of primary communications outperforms that of cognitive communications. This is because among the amount of the power θP_s reserved for transmitting legitimate data, and S allocates 60% ($\kappa = 0.6$) of this amount to amplify and forward the primary signal and 40% ($1 - \kappa = 0.4$) of that to send the cognitive data. Moreover, increasing the time switching factor α degrades the security performance of both cognitive and primary communications (i.e., $\mathcal{O}_p$ (or $\mathcal{O}_s$) at $\alpha = 0.6$ that is larger than $\mathcal{O}_p$ (or $\mathcal{O}_s$) at $\alpha = 0.4$). The reason is that although increasing α helps S scavenge more energy from T in phase 1 (i.e., the SINRs at receivers in phase 2 also increase), the

secrecy capacities in phase 2 reduce since they are weighted by $1-\alpha$. Therefore, $\mathcal{O}_p$ and $\mathcal{O}_s$ may increase with α.

Figure 3 shows the SOPs w.r.t θ, which expose that the security performance of both cognitive and primary transmission is maximized at optimal values of θ, which balance the transmission powers for the legal (primary and cognitive) messages and the artificial noise. Additionally, the best security performance of both primary and cognitive communications increases with increasing α. The reason is that increasing α permits S to scavenge more energy from T and thus, increasing transmission power for both privacy message and the artificial noise. Therefore, the amount of the artificial noise at E increases, eventually improving the security performance. Moreover, the best security performance of primary communications is higher than that of cognitive communications. This can be comprehended from the fact that $\kappa = 0.6$ allots more power for S to transmit T's message than S's message.

Figure 4 demonstrates the SOPs w.r.t κ. The results illustrate that increasing κ enhances the security performance of primary communications (i.e., $\mathcal{O}_p$ decreases) while degrades that of cognitive communications (i.e., $\mathcal{O}_s$ increases). This is apparent because κ interprets the percentage of S's transmission power allocated for T's signal while $1-\kappa$ interprets the percentage of S's transmission power allocated for S's signal. Consequently, increasing κ mitigates $\mathcal{O}_p$ but boosts $\mathcal{O}_s$. Thanks to the contradictory security performance propensity of $\mathcal{O}_p$ and $\mathcal{O}_s$ w.r.t κ, there exists a value of κ where $\mathcal{O}_p$ and $\mathcal{O}_s$ are similar (e.g., $\kappa \simeq 0.524$ for $\alpha = 0.4$ as seen in Figure 4). Additionally, increasing α degrades the security capability at $\mathcal{O}_p = \mathcal{O}_s$, which is comprehended similarly as Figure 2. Moreover, primary (or cognitive) communications 1s always in outage for some range of κ, for instance, $\mathcal{O}_p = 1$ for $\kappa \leq 0.23$ and $\mathcal{O}_s = 1$ for $\kappa \geq 0.84$ when $\alpha = 0.4$ as seen in Figure 4. This is comprehended as follows. Small κ means that the percentage of S's transmission power allocated for T's signal is small, and hence R receives less power for decoding T's message, leading to the outage event. Also, large κ means that the percentage of S's transmission power allocated for S's signal is small, and thus D receives less power for decoding S's message, leading to the outage event.

Figure 5 plots the SOPs w.r.t C_0. This figure exposes that increasing C_0 deteriorates the security performance of both primary and cognitive communications until a complete outage as expected. Moreover, primary communications are more secured than cognitive communications, which is comprehended similarly as Figure 2 due to $\kappa = 0.6$. Furthermore, increasing α does not always enhance the security capability of both primary and cognitive communications. For instance, when C_0 is smaller than 0.078 (or 0.086) bits/s/Hz, increasing α improves message security for the cognitive (or primary) communications; nevertheless, when C_0 is greater than 0.078 (or 0.086) bits/s/Hz, this performance tendency is reversed. This is because the value of α must be selected to poise the harvested energy in phase 1 with the secrecy capacities in phase 2.

Figure 6 plots the SOPs w.r.t α, which expose that the security capability of both cognitive and primary communications is maximized with the optimum selection of α. The optimum value of α, which minimizes SOPs, was recognized and explained as in the previous figures. Additionally, the security capability compromise between cognitive and primary communications is achieved by adopting κ appropriately to allot S's transmission power for messages of S and T. This remark was also pointed out from Figure 4. Furthermore, the security performance of both primary and cognitive communications is in a complete outage for a large value of α (e.g., $\alpha \geq 0.75$ causes $\mathcal{O}_p = 1$ when $\kappa = 0.5$). This is

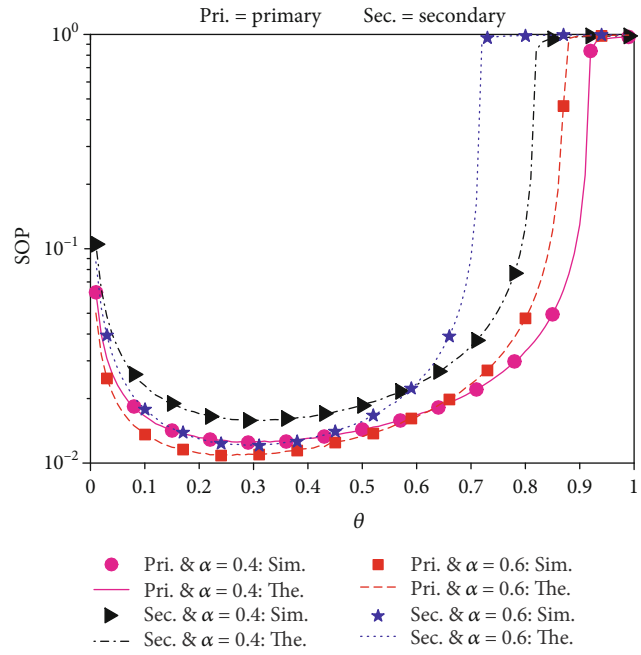

Figure 3: SOPs w.r.t θ.

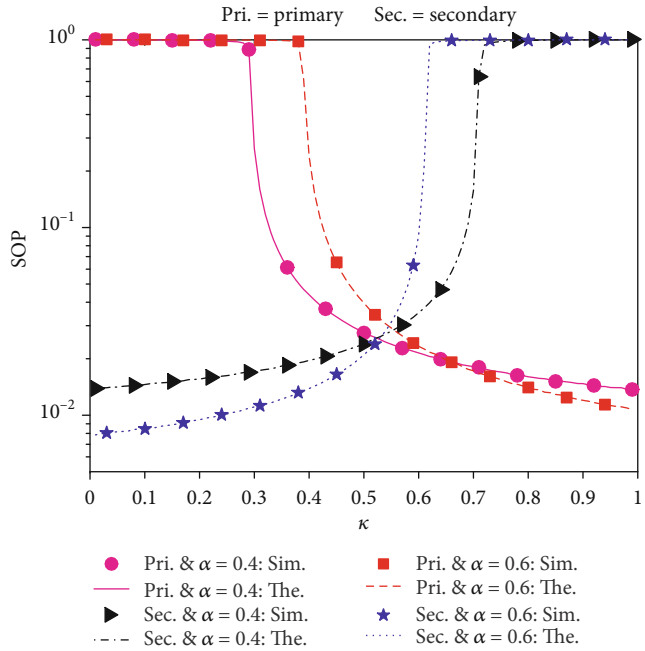

Figure 4: SOPs w.r.t κ.

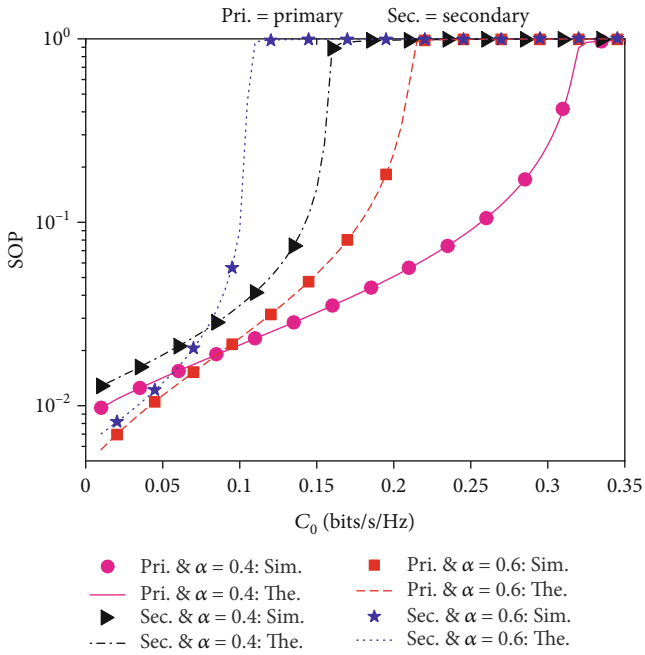

Figure 5: SOPs w.r.t C_0.

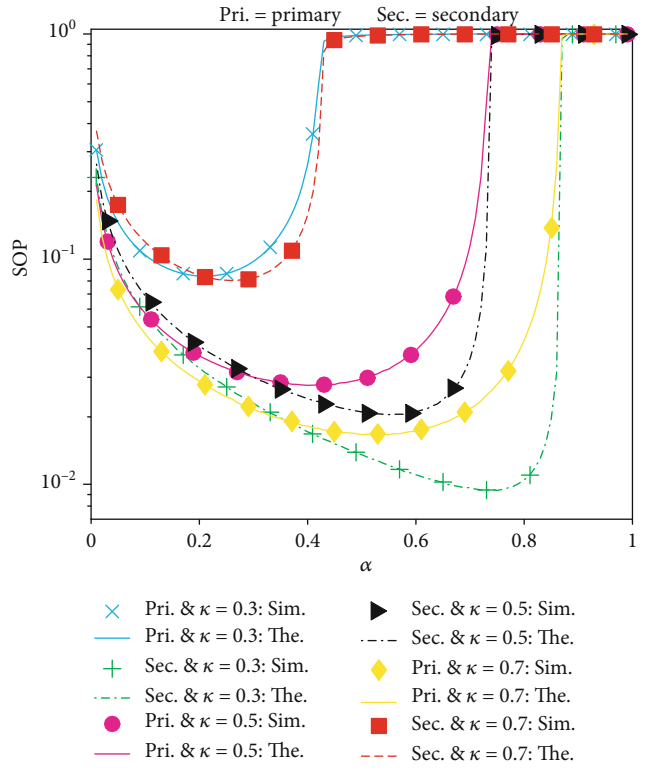

Figure 6: SOPs w.r.t α.

attributed to the fact that the large value of α significantly reduces the secrecy capacities in phase 2, causing the secrecy outage.

Figure 7 demonstrates the SOPs w.r.t λ. The results demonstrate that increasing λ improves the security capability of cognitive communications. The reason is that increasing λ

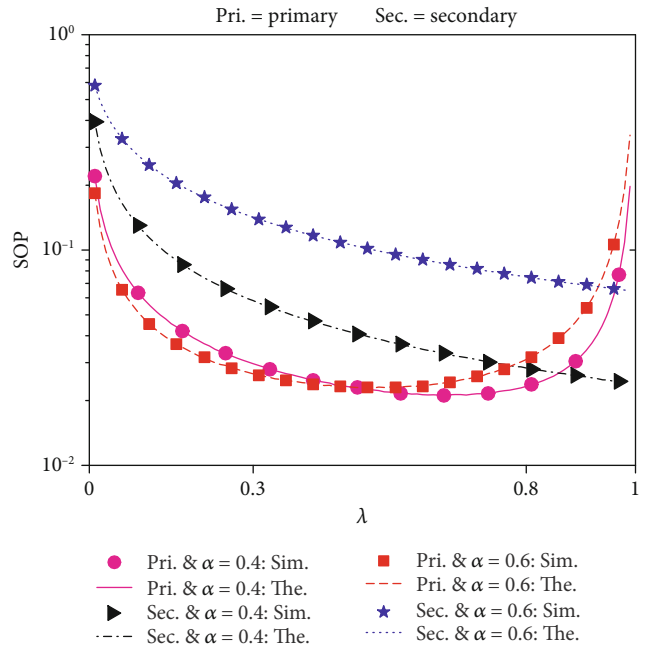

Figure 7: SOPs w.r.t λ.

boosts the harvested energy but reduces the power of T's signal in the received signal at S before amplifying T's signal; thus, the power for transmitting S's data is higher in Phase 2, intimately mitigating $\mathcal{O}_s$. Nevertheless, λ is adopted reasonably to optimize the security performance of primary communications. The optimal λ for minimum $\mathcal{O}_p$ is to balance between the harvested energy and the power of T's signal in the received signal at S. Additionally, the best security performance of primary communications is higher than that of cognitive communications due to $\kappa = 0.6$, which is a similar remark observed from the previous figures. Moreover, α significantly affects the security capability of cognitive communications while slightly impacts that of primary communications.

Locations of users in energy harvesting overlay networks affect the harvested energy in phase 1 as well as the secrecy capacities in phase 2, eventually impacting the SOPs. Figure 8 plots the SOPs w.r.t the variation of S's location. The results demonstrate that when S is close to (E, D, R) yet distant from T (i.e., d increases), the security capability of primary communications is degraded, which is comprehended as follows. As d rises, the power of T's signal in the received signal at S decreases, leading to a reduction in the power of T's signal at corresponding receivers (R, D, E) after relayed by S and an increase in $\mathcal{O}_p$. Nevertheless, this performance tendency is reversed for cognitive communications. This is because x_s is not affected by d while received at corresponding receivers (R, D, E) with higher power due to lower path loss between S and corresponding receivers (R, D, E), leading to the decrease in $\mathcal{O}_s$. The opposite secrecy capability tendencies of cognitive and primary communications with d represent the performance compromise between them, which can be flexibly established by choosing the appropriate location of S. Furthermore, increasing α degrades the security

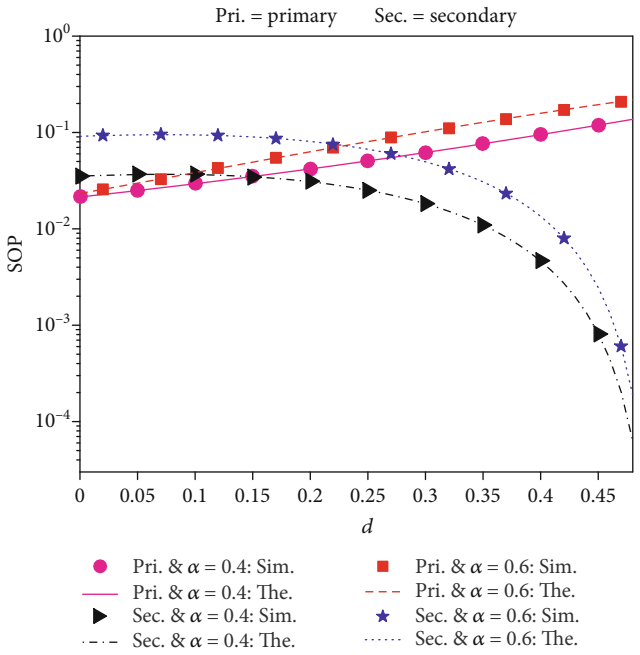

Figure 8: SOPs w.r.t d.

performance of both primary and cognitive communications. This is apprehended similarly as the previous figures.

5. Conclusions

This paper investigated EHONs where the cognitive transmitter operating in the amplify-and-forward mechanism relays the signal of the primary transmitter as well as transmits its privacy signal. The cognitive transmitter self-powers its operation by harvesting RF energy and self-secures both primary and cognitive communications against eavesdroppers by generating the artificial noise. The security performance of both cognitive and primary communications was measured through numerous important indicators (SOP, IP, PSCP, ST), which were numerically evaluated by the recommended accurate formulas. Multiple results are supplied to validate these formulas as well as shed insights into the influence of the artificial noise on the security performance of EHONs with respect to pivotal specifications. Additionally, optimum specifications were found through exhaustive searches relied on the recommended formulas, which well serves as a design instruction. Moreover, the security capability compromise between cognitive and primary communications can be adjusted by selecting specifications reasonably.

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 author(s) declare(s) that they have no conflicts of interest.

Acknowledgments

This research is funded by the Vietnam National University HoChiMinh City (VNU-HCM) under grant number B2021-20-01. We 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] J. Wang, Y. Liu, S. Niu, and H. Song, "Extensive throughput enhancement for 5G enabled UAV swarm networking," *IEEE Journal on Miniaturization for Air and Space Systems*, 2021.

[2] H. Tran-Dang and D. S. Kim, "FRATO: fog resource based adaptive task offloading for delay-minimizing IoT service provisioning," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 10, pp. 2491–2508, 2021.

[3] FCC, *Spectrum policy task force report*, ET Docket 02 - 135, 2002.

[4] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.

[5] K. Ho-Van and T. Do-Dac, "Overlay networks with jamming and energy harvesting: security analysis," *Arabian Journal for Science and Engineering*, 2021.

[6] W. Bai, Z. Ma, Y. Han et al., "Joint optimization of computation offloading, data compression, energy harvesting, and application scenarios in fog computing," *IEEE Access*, vol. 9, pp. 45462–45473, 2021.

[7] Y. Wang, K. Yang, W. Wan, Y. Zhang, and Q. Liu, "Energy efficient data and energy integrated management strategy for IoT devices based on RF energy harvesting," *IEEE Internet of Things Journal*, 2021.

[8] X. Tang, G. Xie, and Y. Cui, "Self-sustainable long range backscattering communication using RF energy harvesting," *IEEE Internet of Things Journal*, 2021.

[9] T. T. Chan and T. M. Lok, "Utilizing interference by network coding for simultaneous wireless information and power transfer," *IEEE Wireless Communications Letters*, 2021.

[10] W. Lee, K. Lee, H. H. Choi, and V. C. Leung, "Deep learning for SWIPT: optimization of transmit-harvest-respond in wireless-powered interference channel," *IEEE Transactions on Wireless Communications*, p. 1, 2021.

[11] A. Khalili, S. Zargari, Q. Wu, D. W. Ng, and R. Zhang, "Multi-objective resource allocation for IRS-aided SWIPT," *IEEE Wireless Communications Letters*, p. 1, 2021.

[12] K. Ma, Z. Li, P. Liu et al., "Reliability-constrained throughput optimization of industrial wireless sensor networks with energy harvesting relay," *IEEE Internet of Things Journal*, 2021.

[13] R. Z. Batool, A. Hassan, R. Ahmad, and W. Ahmed, "Improvement of QoS through relay selection for hybrid SWIPT protocol," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–5, USA, 2021.

[14] B. C. Nguyen, T. M. Hoang, and T. Kim, "Impacts of nonlinear energy harvesting and residual self-interference on the performance of full-duplex decode-and-forward relay system," *IEEE Access*, vol. 9, pp. 42333–42344, 2021.

[15] Y. A. Le QN, N. P. Nguyen, O. A. Dobre, and R. Zhao, "Full-duplex non-orthogonal multiple access cooperative overlay spectrum-sharing networks with SWIPT," *IEEE Transactions*

on Green Communications and Networking, vol. 5, no. 1, pp. 322–334, 2021.

[16] S. Solanki, P. K. Upadhyay, D. B. Da 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.

[17] H. Lei, Z. Dai, K. H. Park, W. Lei, G. Pan, and M. S. Alouini, "Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6384–6395, 2018.

[18] X. Shang, H. Yin, Y. Wang, M. Li, and Y. Wang, "Secure multiuser Scheduling for Hybrid Relay-assisted wireless powered cooperative communication networks with full-duplex destination-based jamming," *IEEE Access*, vol. 9, pp. 49774–49787, 2021.

[19] H. Lei, H. Zhang, I. S. Ansari et al., "On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-m fading Channels," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 614–627, 2017.

[20] H. Yu and J. Joung, "Design of the power and dimension of artificial noise for secure communication systems," *IEEE Transactions on Communications*, p. 1, 2021.

[21] D. Wang, F. Zhou, and V. C. Leung, "Primary privacy preserving with joint wireless power and information transfer for cgnitive radio networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 683–693, 2020.

[22] R. Su, Y. Wang, and R. Sun, "Secure cooperative transmission in cognitive AF relay systems with destination-aided jamming and energy harvesting," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–5, Istanbul, Turkey, 2019.

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

[24] M. Xu, T. Jing, X. Fan, Y. Wen, and Y. Huo, "Secure transmission solutions in energy harvesting enabled cooperative cognitive radio networks," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Barcelona, Spain, 2018.

[25] M. Li, H. Yin, Y. Huang, Y. Wang, and R. Yu, "Physical layer security in overlay cognitive radio networks with energy harvesting," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11274–11279, 2018.

[26] H. Dang-Ngoc, B. Ho-Quoc, and K. Ho-Van, "Key secrecy performance metrics of overlay networks with energy scavenging and artificial noise," in *2020 4th International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, pp. 77–81, Vietnam, 2020.

[27] H. Dang-Ngoc, K. Ho-Van, and T. Do-Dac, "Secrecy analysis of overlay mechanism in radio frequency energy harvesting networks with jamming under Nakagami-m fading," *Wireless Personal Communications*, 2021.

[28] N. Pham-Thi-Dan, B. Ho-Quoc, K. Ho-Van et al., "Secrecy throughput analysis of energy scavenging overlay networks with artificial noise," in *2020 International Conference on Advanced Technologies for Communications (ATC)*, pp. 90–94, Vietnam, 2020.

[29] 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.

[30] W. Zhao, R. She, and H. Bao, "Security energy efficiency maximization for two-way relay assisted cognitive radio NOMA network With self-interference harvesting," *IEEE Access*, vol. 7, pp. 74401–74411, 2019.

[31] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic, San Diego, CA, 6th edition, 2000.

[32] L. Shi, W. Cheng, Y. Ye, H. Zhang, and R. Q. Hu, "Heterogeneous power-splitting based two-way DF relaying with nonlinear energy harvesting," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, United Arab Emirates, 2018.

[33] Y. Ye, L. Shi, X. Chu, and G. Lu, "On the outage performance of ambient backscatter communicationsy," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7265–7278, 2020.