Journal of Computer Science and Cybernetics, V.36, N.3 (2020), 205–231
DOI 10.15625/1813-9663/36/3/14987

SECURITY CAPABILITY ANALYSIS OF COGNITIVE RADIO NETWORK WITH SECONDARY USER CAPABLE OF JAMMING AND SELF-POWERING

NGOC PHAM-THI-DAN[1,2,3], KHUONG HO-VAN[2,3,*], HANH DANG-NGOC[2,3], THIEM DO-DAC[2,3,4], PHONG NGUYEN-HUU[2,3], SON VO-QUE[2,3], SON PHAM-NGOC[5], LIEN HONG-PHAM[5]

[1]*Posts and Telecommunications Institute of Technology - HoChiMinh Campus, Vietnam*
[2]*Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City, Vietnam*
[3]*Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam*
[4]*Thu Dau Mot University, Binh Duong Province, Vietnam*
[5]*Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, Vietnam*

Abstract. This paper investigates a cognitive radio network where a secondary sender assists a primary transmitter in relaying primary information to a primary receiver and also transmits its own information to a secondary recipient. This sender is capable of jamming to protect secondary and/or primary information against an eavesdropper and self-powering by harvesting radio frequency energy of primary signals. Security capability of both secondary and primary networks are analyzed in terms of secrecy outage probability. Numerous results corroborate the proposed analysis which serves as a design guideline to quickly assess and optimize security performance. More importantly, security capability trade-off between secondary and primary networks can be totally controlled with appropriate selection of system parameters.

Keywords. Jamming; Self-powering; Cognitive radios; Security.

1. INTRODUCTION

Next generation mobile networks provide a wide range of emerging services and hence, require modern technologies with better spectrum utilization efficiency, energy efficiency, and information security [1]. Spectrum utilization efficiency can be improved with cognitive radio technology which allows secondary users (SUs) to transmit their information in licensed spectrum of primary users (PUs) without corrupting received signals of PUs. Three typical operation mechanisms of SUs are underlay, overlay, and interweave [2]. In the underlay and overlay mechanisms, SUs and PUs operate concurrently but the former limits SUs' transmit power for tolerable interference at PUs while the latter applies advanced signal processing methods to remain or enhance performance of PUs. Meanwhile, the interweave mechanism merely permits SUs to utilize unoccupied spectrum of PUs.

Many feasible solutions such as hardware solutions [3], harvesting energy from available sources (e.g., solar, radio frequency (RF) powers, thermal, wind, ...) [4], network planning [5] can improve energy efficiency. Among these solutions, RF energy harvesting neither demands

*Corresponding author.
E-mail addresses: ngocptd@ptithcm.edu.vn (N.P.T.Dan); hvkhuong@hcmut.edu.vn (K.H.Van); hanhdn@hcmut.edu.vn (H.D.Ngoc); thiemdd@tdmu.edu.vn (T.D.Dac); phongsolo@gmail.com (P.N.Huu); sonvq@hcmut.edu.vn (S.V.Que); ngocsond00vta1@gmail.com (S.P.Ngoc); phamhonglien2005@gmail.com (L.P.Hong).

additional energy scavenging equipments (e.g., wind turbines, solar panels) nor depends time-variant energy resources. Accordingly, it is considered in standards of next generation mobile networks which implement it through simultaneous wireless information and power transfer (SWIPT) [6–8] or relaying transmission [9–11].

SUs with self-powering capability by harvesting RF energy contribute higher (energy and spectrum utilization) efficiencies to design of next generation mobile networks thanks to exploiting benefits of both cognitive radio and RF energy harvesting technologies. However, the cognitive radio technology also offers an open access environment and hence, eavesdroppers can emulate legal users (SUs and/or PUs) to wire-tap secret information, causing a serious security problem. Currently, beside conventional cryptographic and encryption solutions, physical layer security (PLS), which takes advantages of wireless channel variations to secure secret information, has attracted research community lately [12]. Many viable methods for implementing PLS can be listed as transmit beam-forming [13], on-off transmission [14], jamming [15], transmit antenna selection [16], opportunistic scheduling [17], and relaying [18]. Among them, jamming is simple, flexible, and efficient for implementation [19]. Accordingly, cognitive radio networks with SUs capable of self-powering and jamming are investigated in this paper, which can achieve simultaneously better spectrum utilization efficiency, energy efficiency and information security.

1.1. Literature review

This paper investigates cognitive radio networks with SUs capable of self-powering and jamming where SUs operate in the overlay mechanism and assist primary transmitters in relaying primary information to primary receivers and also transmit their own information to secondary recipients. SUs' transmission is wire-tapped by eavesdroppers.

Whilst most works have focused on security solutions for cognitive radio networks with SUs capable of harvesting RF energy and operating in the interweave and underlay mechanisms, few publications have studied the overlay mechanism lately [20–24]. More specifically, the almost identical system model as ours was investigated in [20] and [21] but their security solution is to jam the eavesdropper by primary receiver[1]. The authors in [22] deployed a dedicated jammer to interrupt the signal reception of the eavesdropper instead of the primary receiver as in [20] and [21]. To further secure primary network, [23] exploited both the dedicated jammer and the primary receiver to jam the eavesdropper. Nonetheless, [20–23] did not carry out the security analysis in terms of secrecy outage probability (SOP). As alternative security solutions, [24] proposed multi-user scheduling and transmit antenna selection and analyzed the ergodic rate of secondary network and the SOP of primary network. Nevertheless, different from [20–23], the authors in [24] required SUs to relay primary information and send their own information independently in order to simplify the SOP analysis and make it tractable.

[1]The system model in [20] and [21] is the same as that in [25]. Nevertheless, [25] assumed energy harvested from the ambient (e.g., wind, solar) other than RF signals, significantly simplifying the analysis. Moreover, [25] did not exploit the jamming technique. Therefore, references like [25] should not be reviewed.

1.2. Contributions

Although the ergodic rate of secondary network and the SOP of primary network was analyzed in [24], SUs are required to relay primary information and send their own information separately. This demands at least three stages (Stage 1: Primary transmission and energy harvesting; Stage 2: Secondary transmission to PU; Stage 3: Secondary transmission to SU) to finish a transmission process of both SU and PU, dramatically mitigating spectral efficiency. This paper improves spectral efficiency and security capability of [24] by proposing a two-stage transmission scheme with SU capable of jamming. Here are our contributions:

- Propose a novel operation principle of secondary sender that can do multiple tasks simultaneously: i) harvest RF energy from the primary transmitter; ii) decode primary information; iii) network-code three (secondary, primary, jamming) information. This principle is flexibly controlled by various parameters whose appropriate selection can obtain desired security trade-off between primary and secondary networks as well as optimize system performance.

- Propose exact SOP expressions for quickly assessing security capability of both primary and secondary networks without time-consuming simulations.

- Provide optimum parameter sets for maximum security capability and expected performance trade-off between primary and secondary networks.

- Illustrate key results on security capability of primary/secondary network with respect to numerous system parameters.

1.3. Structure

The system model is described in next part which is followed by the derivation of the SOPs of both secondary and primary networks in Part 3. Then, Part 4 demonstrates results while Part 5 concludes the paper.

2. SYSTEM MODEL

Figure 1 illustrates a cognitive radio network with a secondary sender S capable of self-powering by harvesting RF energy from signals of a primary transmitter T and jamming an eavesdropper E to secure information transmission of both S and T. S operates in the overlay mechanism and hence, it not only relays primary signal to a primary receiver R (assuming that T and R cannot communicate directly to each other due to heavy shadowing, long distance,...) but also transmits its own signal to a secondary recipient D.

In Figure 1, channel coefficients between T and S, S and D, S and E, S and R are correspondingly denoted as g_{ts}, g_{sd}, g_{se}, g_{sr}. This paper assumes Rayleigh fading channels and hence, they are respectively modelled as $g_{ts} \sim \mathcal{CN}(0, \vartheta_{ts})$, $g_{sd} \sim \mathcal{CN}(0, \vartheta_{sd})$, $g_{se} \sim \mathcal{CN}(0, \vartheta_{se})$, and $g_{sr} \sim \mathcal{CN}(0, \vartheta_{sr})$. Then, the cumulative distribution function (CDF) and the probability density function (PDF) of the channel gain $h_{\mathtt{mn}} = |g_{\mathtt{mn}}|^2$ are respectively addressed as $F_{h_{\mathtt{mn}}}(x) = 1 - e^{-x/\vartheta_{\mathtt{mn}}}$ and $f_{h_{\mathtt{mn}}}(x) = e^{-x/\vartheta_{\mathtt{mn}}}/\vartheta_{\mathtt{mn}}$, where $x \geq 0$, $\mathtt{m} \in \{t, s\}$ and $\mathtt{n} \in \{s, r, d, e\}$.

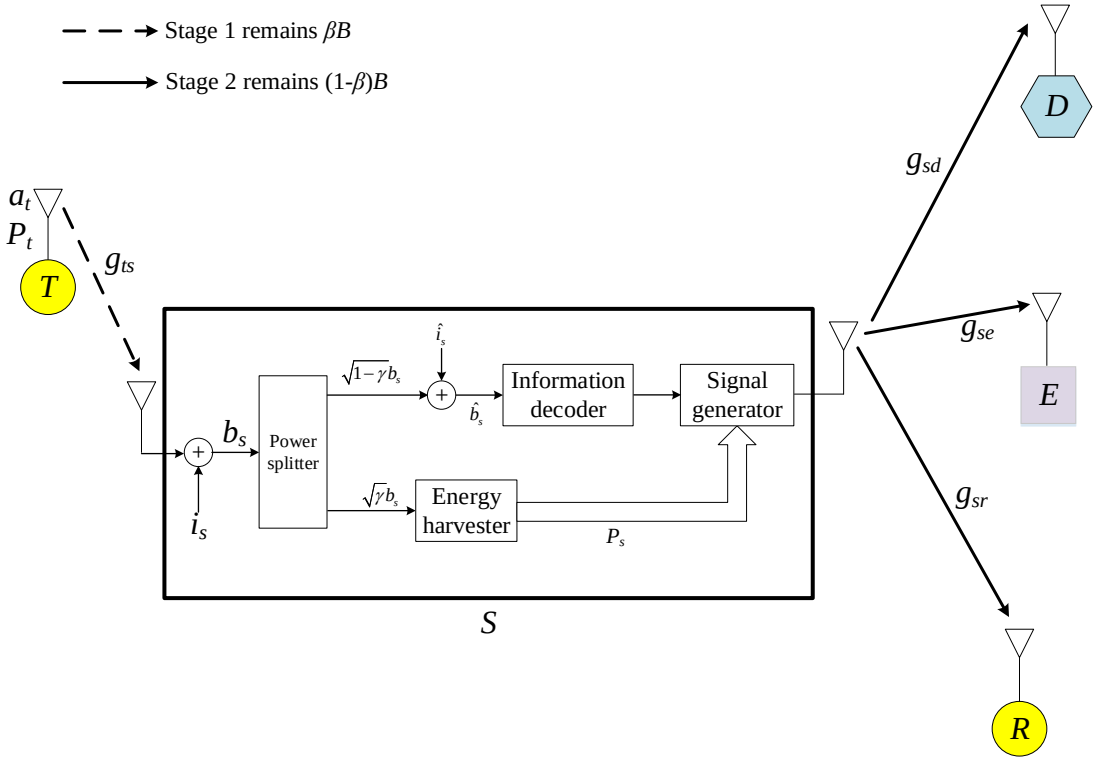

Figure 1. System model

In Figure 1, a complete primary and secondary transmission lasts two stages with total time of B. The stage 1, which remains βB with $\beta \in (0,1)$ being the time allocation factor, is for T to perform SWIPT such that S harvests RF energy from primary signals relied on the power splitting technique [26] and recovers primary information. S firstly partitions its received signal into two parts: One part $\sqrt{\gamma}b_s$ (b_s is the received signal of S and $\gamma \in (0,1)$ is the power allocation factor) for recovering primary information[2] and the other part $\sqrt{1-\gamma}b_s$ for harvesting RF energy; Secondly, based on the decoding result, signal generator of S produces different signal combinations. More specifically, if S correctly restores primary information, it sends a network-coded signal consisting of three (primary, secondary, jamming) information. Otherwise, it transmits a network-coded signal comprising of two (secondary, jamming) information. In the stage 2 which remains $(1-\beta)B$, S broadcasts the network-coded signal to R, D, and E.

The signal which S receives in the stage 1 is

$$b_s = g_{ts}\sqrt{P_t}a_t + i_s, \tag{1}$$

where P_t is the transmit power of T, a_t is the transmit symbol of the unit power, $i_s \sim \mathcal{CN}(0, \kappa_s)$ is the noise produced by the receiving antenna at S.

[2]The current paper assumes that information decoder consumes negligible energy. This assumption is mostly acknowledged in the literature (e.g., [27–33]).

Relied on Figure 1, the total energy which S harvests in the stage 1 is

$$E_s = \lambda \mathcal{E}\left\{\left|\sqrt{\gamma} b_s\right|^2\right\} \beta B = \beta\lambda\gamma \left(P_t h_{ts} + \kappa_s\right) B, \tag{2}$$

where $\mathcal{E}\{\cdot\}$ is the statistical average and $\lambda \in (0,1)$ is the energy conversion efficiency.

The power which S can utilize in the stage 2 is

$$P_s = \frac{E_s}{(1-\beta) B} = \frac{\beta\lambda\gamma}{1-\beta} \left(P_t h_{ts} + \kappa_s\right). \tag{3}$$

Figure 1 exposes the signal for recovering primary information as

$$\hat{b}_s = \sqrt{1-\gamma} b_s + \hat{i}_s, \tag{4}$$

where $\hat{i}_s \sim \mathcal{CN}\left(0, \hat{\kappa}_s\right)$ is the noise induced by the passband-to-baseband signal conversion.

Substituting (1) into (4), one has

$$\hat{b}_s = \sqrt{(1-\gamma) P_t} g_{ts} a_t + \sqrt{1-\gamma} i_s + \hat{i}_s, \tag{5}$$

from which the SNR achievable for recovering primary information is

$$\Gamma_s = \frac{\mathcal{E}\left\{\left|\sqrt{(1-\gamma) P_t} g_{ts} a_t\right|^2\right\}}{\mathcal{E}\left\{\left|\sqrt{1-\gamma} i_s + \hat{i}_s\right|^2\right\}} = A h_{ts}, \tag{6}$$

where

$$A = \frac{(1-\gamma) P_t}{(1-\gamma)\kappa_s + \hat{\kappa}_s}. \tag{7}$$

S can achieve the channel capacity as $C_s = \beta \log_2\left(1+\Gamma_s\right)$ bps/Hz where the constant β before the logarithm is because the stage 1 remains βB. According to the information theory, S precisely recovers primary information merely if C_s is above the target spectral efficiency C_t, i.e., $C_s \geq C_t$. In other words, a_t is precisely recovered at S if $\Gamma_s \geq \Gamma_t$, where $\Gamma_t = 2^{C_t/\beta} - 1$.

The signal generator of S outputs the network-coded signal dependent on the decoding result. If S correctly restores primary information, it transmits a superposition of three signals in the form of $\sqrt{\varepsilon\zeta P_s} a_t + \sqrt{\varepsilon(1-\zeta) P_s} a_s + \sqrt{(1-\varepsilon) P_s} a_j$ in the stage 2, where ε is the power splitting factor for legitimate signals and jamming signal when S correctly restores primary information, ζ is the power splitting factor for secondary and primary signals, a_s is the privacy symbol of the unit power of S, and a_j is the jamming symbol of the unit power. Otherwise, it sends a superposition of only two signals in the form of $\sqrt{\mu P_s} a_s + \sqrt{(1-\mu) P_s} a_j$ in the stage 2, where μ is the power splitting factor for legitimate and jamming signals when S decodes unsuccessfully primary information. Accordingly, $K \in \{R, D, E\}$ receive the following signal in the stage 2

$$b_k = \begin{cases} g_{sk}\left(\sqrt{\varepsilon\zeta P_s} a_t + \sqrt{\varepsilon(1-\zeta) P_s} a_s + \sqrt{(1-\varepsilon) P_s} a_j\right) + i_k, & \Gamma_s \geq \Gamma_t \\ g_{sk}\left(\sqrt{\mu P_s} a_s + \sqrt{(1-\mu) P_s} a_j\right) + i_k, & \Gamma_s < \Gamma_t, \end{cases} \tag{8}$$

where $i_k \sim \mathcal{CN}(0, \kappa_k)$ is the noise caused by the receive antenna at K.

The jamming signal a_j is intentionally generated by S to solely interrupt signal reception of E without mitigating the performance of the legal receiver $L \in \{R, D\}$. This can be implemented by letting S to share a_j with L (e.g., the seed of the jamming signal generator at S is shared with L in a secure manner through a cooperation hand-shaking solely among S and L before information transmission starts). Such a jamming signal generation is widely accepted in most existing works (e.g., [34–43]). Accordingly, the legal receiver L can exactly re-generate the jamming signal and completely take it out of its received signal, intimately obtaining the jamming-free signal at L as

$$\hat{b}_l = \begin{cases} g_{sl}\left(\sqrt{\varepsilon\zeta P_s}a_t + \sqrt{\varepsilon(1-\zeta)P_s}a_s\right) + i_l, & \Gamma_s \geq \Gamma_t \\ g_{sl}\sqrt{\mu P_s}a_s + i_l, & \Gamma_s < \Gamma_t \end{cases} \tag{9}$$

from which SINRs for decoding a_t at R and a_s at D are correspondingly expressed as

$$\Gamma_r = \begin{cases} \dfrac{\varepsilon\zeta P_s h_{sr}}{\varepsilon(1-\zeta)P_s h_{sr} + \kappa_r}, & \Gamma_s \geq \Gamma_t \\ 0, & \Gamma_s < \Gamma_t, \end{cases} \tag{10}$$

$$\Gamma_d = \begin{cases} \dfrac{\varepsilon(1-\zeta)P_s h_{sd}}{\varepsilon\zeta P_s h_{sd} + \kappa_d}, & \Gamma_s \geq \Gamma_t \\ \dfrac{\mu P_s h_{sd}}{\kappa_d}, & \Gamma_s < \Gamma_t. \end{cases} \tag{11}$$

It is recalled that the jamming signal a_j is solely shared among S, R, and D for securing a_s and a_t but unknown at E. Accordingly, the SINRs at E for decoding a_t and a_s are inferred from (8), correspondingly, as

$$\Gamma_{Et} = \begin{cases} \dfrac{\varepsilon\zeta P_s h_{se}}{(1-\varepsilon\zeta)P_s h_{se} + \kappa_e}, & \Gamma_s \geq \Gamma_t \\ 0, & \Gamma_s < \Gamma_t, \end{cases} \tag{12}$$

$$\Gamma_{Es} = \begin{cases} \dfrac{\varepsilon(1-\zeta)P_s h_{se}}{(\varepsilon\zeta + 1 - \varepsilon)P_s h_{se} + \kappa_e}, & \Gamma_s \geq \Gamma_t \\ \dfrac{\mu P_s h_{se}}{(1-\mu)P_s h_{se} + \kappa_e}, & \Gamma_s < \Gamma_t. \end{cases} \tag{13}$$

It is remarked from (12) and (13) that Γ_{Et} and Γ_{Es} are inversely proportional to the jamming signal power which can be flexibly controlled by ε, ζ, μ. Accordingly, increasing the amount of the jamming signal improves security performance for a_s and a_t.

R and D achieve correspondingly the channel capacities in the stage 2 which are computed from (10) and (11)

$$C_r = (1-\beta)\log_2(1+\Gamma_r), \tag{14}$$

$$C_d = (1-\beta)\log_2(1+\Gamma_d), \tag{15}$$

where $1-\beta$ before the logarithm is because the stage 2 remains $(1-\beta)B$.

Similarly, E achieves the channel capacities for decoding a_t and a_s in the stage 2 which are computed from (12) and (13), correspondingly

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

$$C_{Es} = (1-\beta)\log_2(1+\Gamma_{Es}). \tag{17}$$

The secrecy capacity for a_s is the gap between the capacities at D and E for recovering a_s, i.e.,

$$\tilde{C}_s = [C_d - C_{Es}]^+ = (1-\beta)\left[\log_2\frac{1+\Gamma_d}{1+\Gamma_{Es}}\right]^+, \tag{18}$$

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

Similarly, the secrecy capacity for a_t is the gap between the capacities at R and E for recovering a_t, i.e.,

$$\tilde{C}_t = (1-\beta)\left[\log_2\frac{1+\Gamma_r}{1+\Gamma_{Et}}\right]^+. \tag{19}$$

3. SECURITY PERFORMANCE ANALYSIS

This section suggests accurate SOP expressions for promptly assessing security performance for a_s and a_t without exhaustive simulations. The SOP is the possibility that the secrecy capacity is below the predetermined security level C_0. Accordingly, the SOP is an essential metric to evaluate the security capability of both primary and secondary networks.

3.1. Primary SOP

The primary SOP measures the security performance for protecting a_t, which is addressed as

$$SOP_p = \Pr\left\{\tilde{C}_t < C_0\right\}. \tag{20}$$

Because $\tilde{C}_t$ takes two values dependent on whether S correctly recovers primary information or not, SOP_p must be decomposed into two cases as

$$SOP_p = \Pr\left\{\tilde{C}_t < C_0, C_s \geq C_t\right\} + \Pr\left\{\tilde{C}_t < C_0, C_s < C_t\right\}. \tag{21}$$

According to the operation principle of the signal generator at S, if S correctly recovers primary information, it does not relay primary information and hence, the SINR at R for decoding a_t is zero (i.e., $\Gamma_r = 0$ for $\Gamma_s < \Gamma_t$ as seen in (10)). Accordingly, this case induces zero secrecy capacity for a_t (i.e., $\tilde{C}_t = 0$ conditioned on $\Gamma_s < \Gamma_t$) and hence, the event $\tilde{C}_t < C_0$ always happens. Therefore, (21) is further simplified as

$$SOP_p = \mathcal{E}_{|\Gamma_s \geq \Gamma_t}\left\{\underbrace{\Pr\left\{\tilde{C}_t < C_0 \middle| \Gamma_s \geq \Gamma_t\right\}}_{\Delta}\right\} + \Pr\{\Gamma_s < \Gamma_t\}, \tag{22}$$

where $\mathcal{E}_{|Z}$ denotes the conditional expectation on Z.

Invoking $\tilde{C}_t$ in (19), one obtains

$$\Delta = \Pr\{1+\Gamma_r < U(1+\Gamma_{Et}) | \Gamma_s \geq \Gamma_t\}, \tag{23}$$

where

$$U = 2^{C_0/(1-\beta)}. \tag{24}$$

Invoking (10) and (12) for the case of $\Gamma_s \geq \Gamma_t$, Δ in (23) is rewritten as

$$\Delta = \Pr\left\{ X_{sr} < UX_{se} | \, \Gamma_s \geq \Gamma_t \right\}, \tag{25}$$

where

$$X_{sr} = 1 + \frac{Dh_{sr}}{G_{sr}h_{sr} + \kappa_r}, \tag{26}$$

$$X_{se} = 1 + \frac{Dh_{se}}{G_{se}h_{se} + \kappa_e}, \tag{27}$$

with

$$D = \varepsilon\zeta P_s, \tag{28}$$

$$G_{sr} = \varepsilon\left(1-\zeta\right)P_s, \tag{29}$$

$$G_{se} = \left(1-\varepsilon\zeta\right)P_s. \tag{30}$$

Before solving (25) in closed-form, some preliminary results are prepared in the following lemmas.

Lemma 1. *The PDFs of X_{sr} and X_{se} are correspondingly expressed as*

$$f_{X_{sr}}\left(x\right) = \frac{M_{sr}}{\left(x-K_{sr}\right)^2} e^{H_{sr}\frac{x-1}{x-K_{sr}}}, \; 1 \leq x < K_{sr} \tag{31}$$

and

$$f_{X_{se}}\left(y\right) = \frac{M_{se}}{\left(y-K_{se}\right)^2} e^{H_{se}\frac{y-1}{y-K_{se}}}, \; 1 \leq y < K_{se} \tag{32}$$

where

$$K_{sr} = D/G_{sr} + 1, \tag{33}$$

$$H_{sr} = \kappa_r / \left(\vartheta_{sr} G_{sr}\right), \tag{34}$$

$$M_{sr} = H_{sr} D/G_{sr}, \tag{35}$$

$$K_{se} = D/G_{se} + 1, \tag{36}$$

$$H_{se} = \kappa_e / \left(\vartheta_{se} G_{se}\right), \tag{37}$$

$$M_{se} = H_{se} D/G_{se}. \tag{38}$$

Proof. Using (26), one infers

$$h_{sr} = \frac{\left(X_{sr}-1\right)\kappa_r}{D + G_{sr} - G_{sr}X_{sr}}. \tag{39}$$

Because $h_{sr} \geq 0$, X_{sr} is constrained by $1 \leq X_{sr} < \frac{D}{G_{sr}} + 1$. The Jacobian coefficient is computed as

$$\frac{dh_{sr}}{dX_{sr}} = \frac{D\kappa_r}{\left(D + G_{sr} - G_{sr}X_{sr}\right)^2}. \tag{40}$$

Given the variable substitution in (26), the PDF of X_{sr} can be inferred from the PDF of h_{sr} as

$$f_{X_{sr}}\left(x\right) = f_{h_{sr}}\left(\frac{\left(x-1\right)\kappa_r}{D + G_{sr} - G_{sr}x}\right)\left|\frac{dh_{sr}}{dX_{sr}}\right|_{X_{sr}=x}. \tag{41}$$

Inserting $f_{h_{sr}}(x) = e^{-x/\vartheta_{sr}}/\vartheta_{sr}$ and the Jacobian coefficient into (41), the PDF of X_{sr} is obtained as (31). By following the proof of (31), the PDF of X_{se} can be inferred as (32). This finishes the proof. ∎

Lemma 2. *The exact closed-form representation of*

$$\mathcal{A}(a,b,L_{sr}) = \int_a^b f_{X_{sr}}(x)\,dx, \tag{42}$$

is

$$\mathcal{A}(a,b,L_{sr}) = e^{H_{sr}}\left(e^{\frac{M_{sr}}{a-K_{sr}}} - e^{\frac{M_{sr}}{b-K_{sr}}}\right) \tag{43}$$

where $L_{sr} = \{H_{sr}, M_{sr}, K_{sr}\}$ is the set of parameters relating the transmission from S to R, $1 \le a < b \le K_{sr}$.

Proof. Plugging $f_{X_{sr}}(x)$ in (31) into (42) and performing the variable changes, one obtains

$$\begin{aligned}
\mathcal{A}(a,b,L_{sr}) &= \int_a^b \frac{M_{sr}}{(x-K_{sr})^2} e^{H_{sr}\frac{x-1}{x-K_{sr}}}\,dx \\
&\overset{y=\frac{1}{x-K_{sr}}}{=} -M_{sr}\int_{\frac{1}{a-K_{sr}}}^{\frac{1}{b-K_{sr}}} e^{H_{sr}y\left(\frac{1}{y}+K_{sr}-1\right)}\,dy \\
&= e^{H_{sr}}\int_{\frac{1}{b-K_{sr}}}^{\frac{1}{a-K_{sr}}} M_{sr}e^{M_{sr}y}dy.
\end{aligned} \tag{44}$$

The last integral is straightforwardly computed, reducing (44) to (43). This finishes the proof. ∎

The preliminary results in two above lemmas are convenient to represent Δ in (25) in a compact form as follows.

Theorem 1. *Δ is expressed in an exact closed form as*

$$\Delta = \begin{cases} 1 - M_{se}e^{H_{sr}+H_{se}}\mathcal{G}, & K_{se} < V \\ 1 - M_{se}e^{H_{sr}+H_{se}}\mathcal{K}, & 1 \le V < K_{se} \\ 1, & V < 1 \end{cases} \tag{45}$$

where

$$V = K_{sr}/U, \tag{46}$$

$$J = M_{sr}/U, \tag{47}$$

$$I = (K_{se}-1)^{-1} - (K_{se}-V)^{-1}, \tag{48}$$

$$\mathcal{G} = e^{\frac{J}{K_{se}-V}} \left\{ \frac{e^{-H_{se}}}{M_{se}} - \frac{J}{(K_{se}-V)^2} e^{\frac{M_{se}}{V-K_{se}}} Ei\left(-M_{se}I\right) + \sum_{n=2}^{\infty} \frac{J^n(-M_{se})^{n-1}}{n!\,(n-1)!(K_{se}-V)^{2n}} \left[e^{-H_{se}} \sum_{k=1}^{n-1} \frac{(k-1)!}{(-M_{se}I)^k} - e^{\frac{M_{se}}{V-K_{se}}} Ei\left(-M_{se}I\right) \right] \right\}, \tag{49}$$

$$\mathcal{K} = e^{\frac{J-M_{se}}{K_{se}-V}} \left\{ \frac{e^{-M_{se}I}-1}{M_{se}} + \sum_{n=1}^{\infty} \frac{J^n}{(K_{se}-V)^{2n} n!} \times \left(e^{-M_{se}I} \sum_{k=1}^{n-1} \frac{(-M_{se})^{k-1}}{I^{n-k} \prod_{i=1}^{k} (n-i)} - \frac{(-M_{se})^{n-1}}{(n-1)!} Ei\left(-M_{se}I\right) \right) \right\}, \tag{50}$$

with $Ei(\cdot)$ being the exponential-integral function [44].

Proof. Please refer to Appendix A. ∎

For convenience of presentation, let $\bar{\Delta} = 1 - \Delta$. Then

$$\bar{\Delta} = \begin{cases} M_{se} e^{H_{sr}+H_{se}} \mathcal{G}, & K_{se} < V \\ M_{se} e^{H_{sr}+H_{se}} \mathcal{K}, & 1 \le V < K_{se} \\ 0, & V < 1. \end{cases} \tag{51}$$

Plugging Δ in (45) into (22) results in

$$\begin{aligned} SOP_p &= \mathcal{E}_{|\Gamma_s \ge \Gamma_t} \left\{ 1 - \bar{\Delta} \right\} + \Pr\left\{ \Gamma_s < \Gamma_t \right\} \\ &= \mathcal{E}_{|\Gamma_s \ge \Gamma_t} \left\{ 1 \right\} + \Pr\left\{ \Gamma_s < \Gamma_t \right\} - \mathcal{E}_{|\Gamma_s \ge \Gamma_t} \left\{ \bar{\Delta} \right\} \\ &= \Pr\left\{ \Gamma_s \ge \Gamma_t \right\} + \Pr\left\{ \Gamma_s < \Gamma_t \right\} - \mathcal{E}_{|\Gamma_s \ge \Gamma_t} \left\{ \bar{\Delta} \right\} \\ &= 1 - \mathcal{E}_{|\Gamma_s \ge \Gamma_t} \left\{ \bar{\Delta} \right\}. \end{aligned} \tag{52}$$

Because $\bar{\Delta}$ is a function of a random variable P_s (or $h_{ts} = x$) according to (3) and the condition $\Gamma_s \ge \Gamma_t$ is equivalent to $h_{ts} \ge \Gamma_t / A$, (52) can be expressed in terms of a single-variable integral as

$$\begin{aligned} SOP_p &= 1 - \int_{\Gamma_t/A}^{\infty} \bar{\Delta} f_{h_{ts}}(x)\, dx \\ &= \begin{cases} 1 - \frac{1}{\vartheta_{ts}} \int_{\Gamma_t/A}^{\infty} M_{se} e^{H_{sr}+H_{se}-x/\vartheta_{ts}} \mathcal{G} dx, & K_{se} < V \\ 1 - \frac{1}{\vartheta_{ts}} \int_{\Gamma_t/A}^{\infty} M_{se} e^{H_{sr}+H_{se}-x/\vartheta_{ts}} \mathcal{K} dx, & 1 \le V < K_{se} \\ 1, & V < 1. \end{cases} \end{aligned} \tag{53}$$

3.2. Secondary SOP

The secondary SOP measures the security performance for protecting a_s, which is addressed as

$$SOP_s = \Pr\left\{ \tilde{C}_s < C_0 \right\}. \tag{54}$$

Because $\tilde{C}_s$ takes two values dependent on whether S correctly recovers primary information or not, SOP_s must be decomposed into two cases as

$$SOP_s = \Pr\left\{\tilde{C}_s < C_0, C_s \geq C_t\right\} + \Pr\left\{\tilde{C}_s < C_0, C_s < C_t\right\}. \tag{55}$$

Inserting $\tilde{C}_s$ in (18) into (55), one obtains

$$\begin{aligned} SOP_s = \mathcal{E}_{|\Gamma_s \geq \Gamma_t} & \left\{ \overbrace{\Pr\left\{1+\Gamma_d < U\left(1+\Gamma_{Es}\right) | \, \Gamma_s \geq \Gamma_t\right\}}^{\Psi_1} \right\} \\ + \mathcal{E}_{|\Gamma_s < \Gamma_t} & \left\{ \underbrace{\Pr\left\{1+\Gamma_d < U\left(1+\Gamma_{Es}\right) | \, \Gamma_s < \Gamma_t\right\}}_{\Psi_2} \right\}. \end{aligned} \tag{56}$$

The explicit form of Ψ_1 in (56) is obtained after invoking (11) and (13) for the case of $\Gamma_s \geq \Gamma_t$ as

$$\Psi_1 = \Pr\left\{ 1 + \frac{\varepsilon\left(1-\zeta\right) P_s h_{sd}}{\varepsilon\zeta P_s h_{sd} + \kappa_d} < U\left(1 + \frac{\varepsilon\left(1-\zeta\right) P_s h_{se}}{\left(\varepsilon\zeta + 1 - \varepsilon\right) P_s h_{se} + \kappa_e}\right) \middle| \, \Gamma_s \geq \Gamma_t \right\}. \tag{57}$$

By observing (25) and (57), it is seen that Ψ_1 and Δ have a same form. Accordingly, with appropriate variable substitutions in Δ in (25), one can obtain the exact closed-form expression of Ψ_1. To be more specific, Ψ_1 is achieved from Δ in (45) with $\varepsilon\left(1-\zeta\right) P_s \to D$, $\varepsilon\zeta P_s \to G_{sr}$, $\left(\varepsilon\zeta + 1 - \varepsilon\right) P_s \to G_{se}$, $\vartheta_{sd} \to \vartheta_{sr}$, $\kappa_d \to \kappa_r$. Accordingly, the derivation of Ψ_1 is omitted here for briefness

$$\Psi_1 = 1 - \bar{\Delta}_{\varepsilon(1-\zeta)P_s \to D, \varepsilon\zeta P_s \to G_{sr}, (\varepsilon\zeta+1-\varepsilon)P_s \to G_{se}, \vartheta_{sd} \to \vartheta_{sr}, \kappa_d \to \kappa_r}. \tag{58}$$

Ψ_2 in (56) is given in the following theorem.

Theorem 2. *Ψ_2 is derived in an exact closed form as*

$$\Psi_2 = 1 - \bar{H} \sum_{n=0}^{\infty} \frac{1}{n!} \left(\frac{\bar{Q}\bar{G}}{\sqrt{\bar{E}}}\right)^n e^{-\bar{E}/2} \mathbf{W}_{-\frac{n}{2}, \frac{1-n}{2}}\left(\bar{E}\right), \tag{59}$$

where

$$\begin{aligned} \bar{A} &= \mu P_s / \kappa_d, && (60)\\ \bar{B} &= \mu P_s, && (61)\\ \bar{C} &= \left(1-\mu\right) P_s, && (62)\\ \bar{D} &= 1 + \bar{B}/\bar{C}, && (63)\\ \bar{E} &= \kappa_e / \left(\vartheta_{se}\bar{C}\right), && (64)\\ \bar{G} &= \bar{E}\bar{B}/\bar{C}, && (65)\\ \bar{Q} &= U / \left(\vartheta_{sd}\bar{A}\right), && (66)\\ \bar{H} &= e^{\bar{E} - \bar{Q}\bar{D} + \left(\vartheta_{sd}\bar{A}\right)^{-1}}, && (67) \end{aligned}$$

with $W_{a,b}\left(c\right)$ being the Whittaker function [44, eq. (1087.4)].

Proof. Please refer to Appendix B. ∎

Inserting Ψ_1 in (58) and Ψ_2 in (59) into (56), one achieves

$$\begin{aligned} SOP_s &= \mathcal{E}_{|\Gamma_s \geq \Gamma_t} \left\{1 - \bar{\Delta}_{\varepsilon(1-\zeta)P_s \to D, \varepsilon\zeta P_s \to G_{sr}, (\varepsilon\zeta+1-\varepsilon)P_s \to G_{se}, \vartheta_{sd} \to \vartheta_{sr}, \kappa_d \to \kappa_r}\right\} \\ &\quad + \mathcal{E}_{|\Gamma_s < \Gamma_t} \left\{1 - \bar{H} \sum_{n=0}^{\infty} \frac{1}{n!} \left(\frac{\bar{Q}\bar{G}}{\sqrt{\bar{E}}}\right)^n e^{-\bar{E}/2} \mathbf{W}_{-n/2,(1-n)/2}\left(\bar{E}\right)\right\} \\ &= 1 - \mathcal{E}_{|\Gamma_s \geq \Gamma_t} \left\{\bar{\Delta}_{\varepsilon(1-\zeta)P_s \to D, \varepsilon\zeta P_s \to G_{sr}, (\varepsilon\zeta+1-\varepsilon)P_s \to G_{se}, \vartheta_{sd} \to \vartheta_{sr}, \kappa_d \to \kappa_r}\right\} \\ &\quad - \sum_{n=0}^{\infty} \frac{1}{n!} \mathcal{E}_{|\Gamma_s < \Gamma_t} \left\{\bar{H} \left(\frac{\bar{Q}\bar{G}}{\sqrt{\bar{E}}}\right)^n e^{-\bar{E}/2} \mathbf{W}_{-n/2,(1-n)/2}\left(\bar{E}\right)\right\}. \end{aligned} \tag{68}$$

Because terms inside conditional expectations are functions of the random variable P_s (or $h_{ts} = x$) and the conditions $\Gamma_s \geq \Gamma_t$ and $\Gamma_s < \Gamma_t$ are correspondingly equivalent to $h_{ts} \geq \Gamma_t/A$, and $h_{ts} < \Gamma_t/A$, (68) can be expressed in terms of a single-variable integral as

$$\begin{aligned} SOP_s &= 1 - \frac{1}{\vartheta_{ts}} \int_{\Gamma_t/A}^{\infty} e^{-x/\vartheta_{ts}} \bar{\Delta}_{\varepsilon(1-\zeta)P_s \to D, \varepsilon\zeta P_s \to G_{sr}, (\varepsilon\zeta+1-\varepsilon)P_s \to G_{se}, \vartheta_{sd} \to \vartheta_{sr}, \kappa_d \to \kappa_r} dx \\ &\quad - \frac{1}{\vartheta_{ts}} \sum_{n=0}^{\infty} \frac{1}{n!} \int_{0}^{\Gamma_t/A} e^{-x/\vartheta_{ts} - \bar{E}/2} \bar{H} \left(\frac{\bar{Q}\bar{G}}{\sqrt{\bar{E}}}\right)^n \mathbf{W}_{-n/2,(1-n)/2}\left(\bar{E}\right) dx. \end{aligned} \tag{69}$$

3.3. Remark

The exact single-variable expressions of SOP_p and SOP_s are numerically evaluated by various computation softwares (e.g., Matlab, Mathematica). As such, they are helpful in promptly assessing the security performance of both secondary and primary networks without exhaustive simulations. Upon our understanding, these expressions have not been reported in any publication yet.

4. ILLUSTRATIVE RESULTS

This section demonstrates the SOPs of both secondary and primary networks in key system parameters. Taking path-loss into account, fading power of the $\mathtt{m} - \mathtt{n}$ channel is modelled as $\vartheta_{\mathtt{mn}} = d_{\mathtt{mn}}^{-\phi}$ where $d_{\mathtt{mn}}$ is the $\mathtt{m}$-$\mathtt{n}$ distance and ϕ is the path-loss exponent. For illustration purposes, some system parameters are listed as follows: coordinates of T, R, S, D, E are $(-0.1, 0.3)$, $(0.5, -0.2)$, $(d, 0.0)$, $(0.6, 0.0)$, $(0.6, -0.1)$, correspondingly; $\lambda = 0.9$; $\kappa_s = \kappa_e = \kappa_r = \kappa_d = \hat{\kappa}_s = N_0$; $\phi = 4$. In the following figures, "Sim." and "Ana." correspondingly represent the simulated result and the analytical results in (53) and (69). A common observation from the following figures is that the simulation matches the analysis, confirming the validity of the proposed expressions in (53) and (69).

Figure 2 plots the SOPs with respect to (w.r.t) P_t/N_0 for $C_0 = 0.1$ bps/Hz, $C_t = 0.1$ bps/Hz, P_t/N_0, $\beta = 0.4$, $\gamma = 0.6$, $d = 0.0$, $\varepsilon = 0.7$, $\zeta = 0.6$, $\mu = 0.7$. These results show security performance improvement (i.e., SOPs decrease) with increasing P_t/N_0. This is because increasing P_t/N_0 offers S more harvested energy and higher possibility of decoding

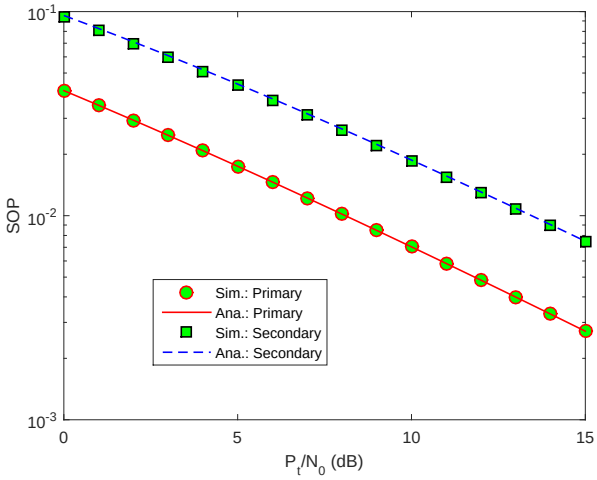

Figure 2. SOPs w.r.t P_t/N_0

successfully primary information and hence, improving the SINRs at corresponding receivers in the stage 2 and mitigating the SOPs. Additionally, the primary network obtains higher security performance than the secondary network. This comes from the fact that the power splitting factor for primary and secondary signals is $\zeta = 0.6$, which means that higher transmit power (60% ($\zeta = 0.6$) of S's total transmit power allotted for secret information (i.e., εP_s)) is allocated for relaying primary information while lower transmit power is for sending secondary information (only 40% ($1 - \zeta = 0.4$) of S's total transmit power allotted for secret information).

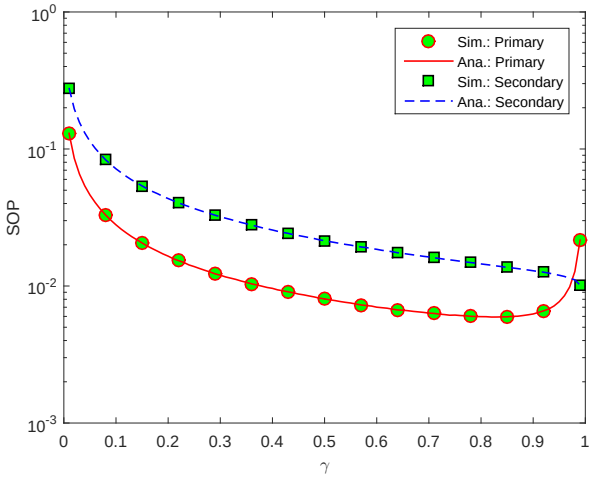

Figure 3. SOPs w.r.t γ

Figure 3 plots the SOPs w.r.t γ with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB. It is seen that the secondary network is more secured with increasing γ. This can be explained as follows. Increasing γ offers S more harvested energy but lower receive power for

decoding primary information. Therefore, the probability of decoding successfully primary information at S is reduced and hence, secondary information is sent with higher power in the stage 2, intimately reducing SOP_s. Nonetheless, the primary network can obtain the best security performance with appropriate selection of γ which aims to balance between harvested energy and probability of decoding successfully primary information at S; for example, SOP_p is minimum at $\gamma = 0.83$ as seen in Figure 3. Furthermore, the best security capability of the primary network is superior to the security performance of the secondary network owing to $\zeta = 0.6$ as explained from Figure 2.

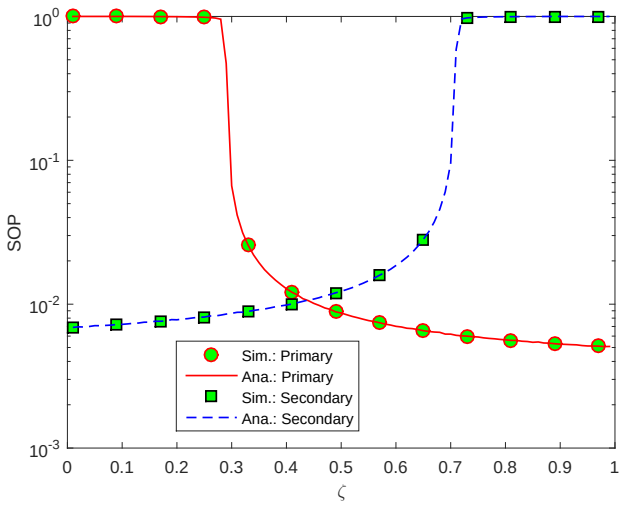

Figure 4. SOPs w.r.t ζ

Figure 4 illustrates the SOPs w.r.t ζ with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB. The results show that the primary network is more secured (i.e., SOP_p reduces) with increasing ζ while security trend is reversed for the secondary network (i.e., SOP_s increases). This makes sense because ζ and $1-\zeta$ are proportional to S's power allotted for primary and secondary information, correspondingly. Accordingly, increasing ζ reduces SOP_p but increases SOP_s. Because of the opposite security tendency of the primary and secondary networks w.r.t ζ, it is possible to balance the security performance of these networks with appropriate selection of ζ; for example, $SOP_p = SOP_s$ when $\zeta = 0.44$ as seen in Figure 4. Furthermore, due to insufficient power, both secondary and primary networks suffer a complete outage in a certain range of ζ; for example, $SOP_s = 1$ and $SOP_p = 1$ when $\zeta \geq 0.77$ and $\zeta \leq 0.24$, respectively.

Figure 5 demonstrates the SOPs w.r.t C_t with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB. It is seen that increasing C_t improves the security performance of the secondary network but degrades that of the primary network. This is attributed from the fact that increasing C_t (i.e., increasing the target spectral efficiency required by T) mitigates the possibility of decoding successfully primary information at S, eventually reducing the chance that primary information is relayed by S and hence, increasing the SOP_p. However, reducing the chance that primary information is relayed by S increases the possibility that secondary information is transmitted with higher power and hence, reducing the SOP_s. Because of

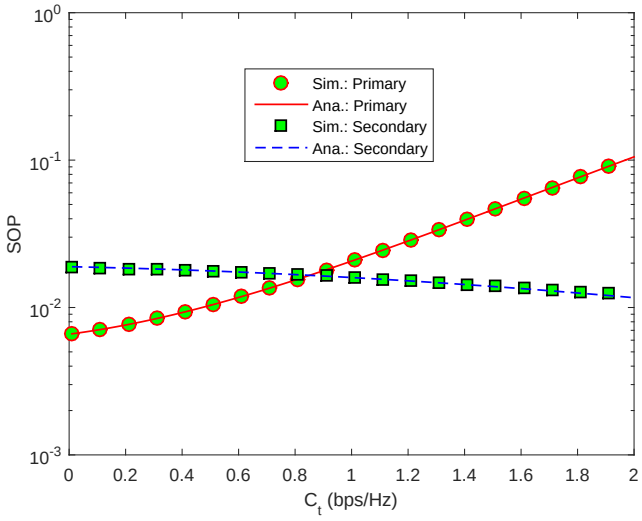

Figure 5. SOPs w.r.t C_t

the opposite security performance tendency of the primary and secondary networks w.r.t C_t, their security capability can be balanced with appropriate selection of C_t; for example, $SOP_p = SOP_s$ when $C_t = 0.85$ bps/Hz as seen in Figure 5.

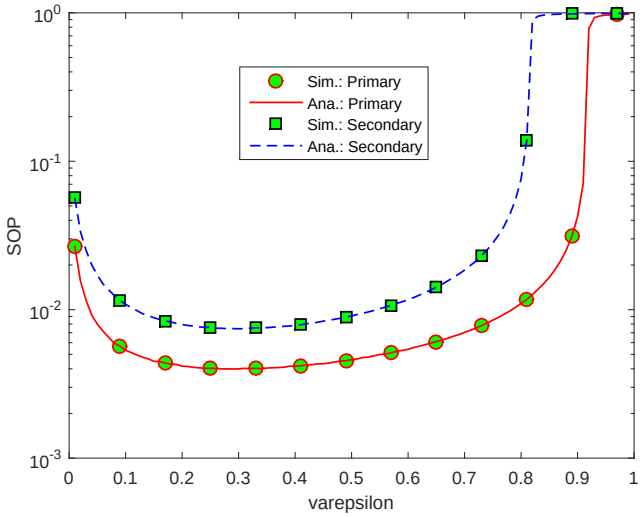

Figure 6. SOPs w.r.t ε. The label "varepsilon" on the x axis is ε

Figure 6 shows the SOPs w.r.t ε with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB. This figure demonstrates that the security performance of both primary and secondary networks can be maximized (i.e., SOPs are minimum) with optimal selection of ε (e.g., $\varepsilon_{opt} = 0.33$ results in minimum SOP_s and SOP_p in Figure 6). This ε_{opt} is to balance transmit powers for secret (primary and secondary) information and jamming information.

Additionally, SOP_p is smaller than SOP_s. This can be explained on basis of $\zeta = 0.6$ as Figure 2.

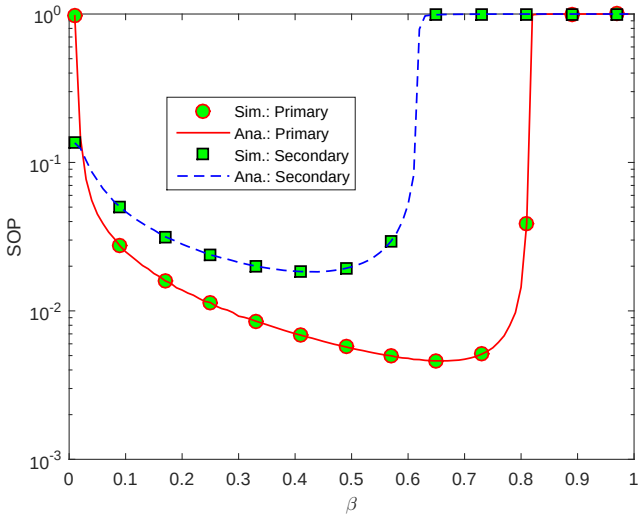

Figure 7. SOPs w.r.t β

Figure 7 shows the SOPs w.r.t β with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB. This figure illustrates that optimum security performance of the primary and secondary networks is achievable with optimum selection of β; for instance, SOP_s and SOP_p are minimum at $\beta = 0.44$ and $\beta = 0.65$, correspondingly. The optimal values of β for maximum security capability can be interpreted as follows. Increasing β helps S harvest more energy from T and decode successfully primary information with a higher probability in the stage 1; hence, increasing SINRs in the stage 2. Nonetheless, this increment also decreases channel capacities in the stage 2 because they are proportional to $1 - \beta$. Therefore, the optimum values of β is to balance benefits in both stages. Furthermore, the security capability of primary network is superior to that of the secondary network. This can be interpreted on basis of $\zeta = 0.6$ as Figure 2. Furthermore, both secondary and primary networks suffer a complete outage in a certain range of β due to insufficient secrecy capacity; for example, $SOP_s = 1$ and $SOP_p = 1$ when $\beta \geq 0.65$ and $\beta \geq 0.83$, respectively.

It is recalled that μ is the power splitting factor for secondary and jamming signals when S fails to decode primary information. Accordingly, to observe the impact of μ clearly, it is good to consider the scenario where S fails to decode primary information. This scenario can be established by choosing a large value of C_t. Figure 8 illustrates the SOPs w.r.t μ, with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB and $C_t = 6$ bps/Hz. It is seen that the primary network suffers a complete outage because the large C_t induces S to decode unsuccessfully primary information all the time and thus, R never receives it for decoding. Moreover, the secondary network can achieve the best security performance with optimum selection of μ, which is to balance power allocation for secondary and jamming signals; for instance, $\mu = 0.25$ maximizes the security performance of the secondary network.

Figure 9 illustrates the SOPs w.r.t C_0 with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB. It is seen that both primary and secondary networks are less secured with increasing C_0

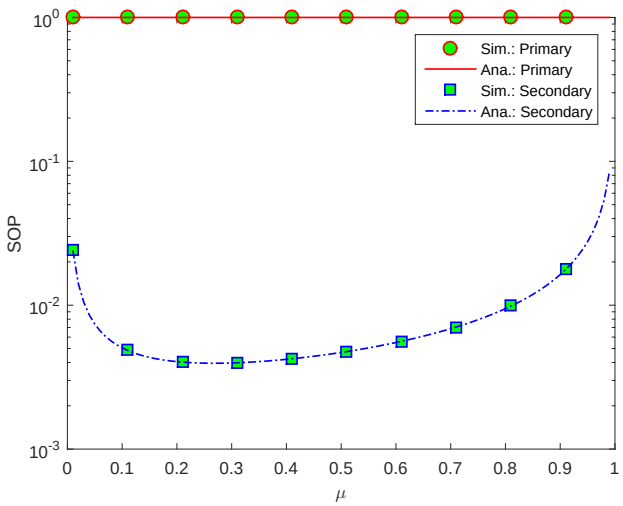

Figure 8. SOPs w.r.t μ

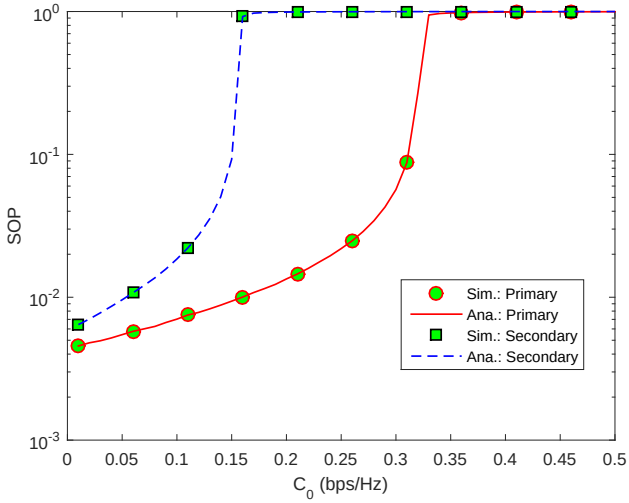

Figure 9. SOPs w.r.t C_0

and suffer a complete outage at large values of C_0 (e.g., $SOP_s = 1$ and $SOP_p = 1$ when C_0 is larger than 0.17 bps/Hz and 0.35 bps/Hz, respectively). Moreover, the primary network is more secured than the secondary network. This can be explained on basis of $\zeta = 0.6$ as Figure 2.

It is noted that locating users in cognitive radio networks affects not only benefits (harvested energy and probability of recovering correctly primary information) in the stage 1 but also secrecy capacities in the stage 2, intimately varying the SOPs. Figure 10 illustrates the SOPs w.r.t S's location with parameters of Figure 2 excepting $P_t/N_0 = 10$ dB. It is seen that the primary network is less secured with increasing d (i.e., S is far away from T but closer to (R, D, E)). This makes sense because of reduction in benefits in the stage

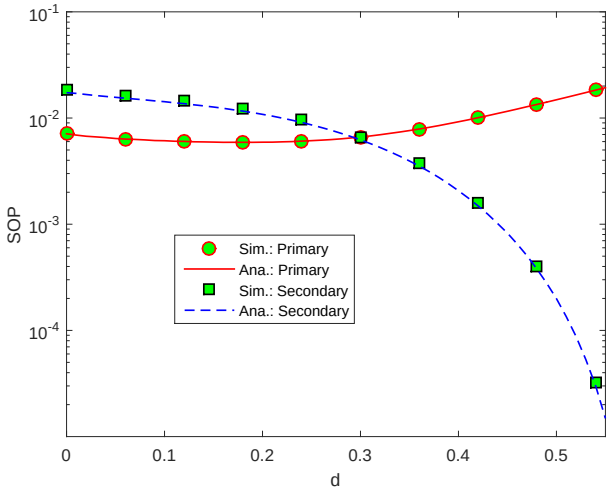

Figure 10. SOPs w.r.t d

1. Nonetheless, the primary network can achieve the best security performance at optimum location of S which balances benefits in both stages; for example, $d = 0.18$ results in mimimum SOP_p. For the secondary network, its security capability is improved with increasing d. This can be explained as follows. Increasing d (i.e., primary information is hardly relayed by S) induces most harvested energy allocated for secondary information with low path-loss to corresponding receivers. Accordingly, secondary secrecy capacity increases, eventually mitigating SOP_s. Furthermore, opposite security performance trend of secondary and primary networks with d exposes their performance compromise, which is flexibly set-up by choosing appropriate location of S.

5. CONCLUSION

This paper investigated cognitive radio networks where secondary users operate in the overlay mechanism and are capable of self-powering to improve energy efficiency and jamming to enhance security performance. Exact secrecy outage probability expressions for both secondary and primary networks were proposed to analyze their security performance in various key specifications. Interestingly, based on these proposed expressions, security capability of both secondary and primary networks can be optimized with appropriate parameter selection through exhaustive searches. Moreover, their security capability as well as their performance trade-off can be flexibly adjusted by numerous specifications (power allocation factor, time allocation factor, power splitting factor,...).

ACKNOWLEDGMENT

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2019.318.

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.

APPENDIX A: PROOF OF Δ

Because X_{sr} and X_{se} are statistically independent, Δ in (25) is computed as

$$\Delta = \iint\limits_{x<Uy} f_{X_{sr}}(x)\, f_{X_{se}}(y)\, dxdy. \tag{70}$$

Since $f_{X_{sr}}(x)$ is non-zero for $x \in [1, K_{sr})$, three cases on Uy in correlation to $[1, K_{sr})$ are considered as

$$\Delta = \underbrace{\iint\limits_{x<Uy} f_{X_{sr}}(x)\, f_{X_{se}}(y)\, dxdy}_{\text{Case 1: } Uy<1} + \underbrace{\iint\limits_{x<Uy} f_{X_{sr}}(x)\, f_{X_{se}}(y)\, dxdy}_{\text{Case 2: } 1\le Uy<K_{sr}} + \underbrace{\iint\limits_{x<K_{sr}} f_{X_{sr}}(x)\, f_{X_{se}}(y)\, dxdy}_{\text{Case 3: } Uy>K_{sr}}. \tag{71}$$

Because $f_{X_{se}}(y)$ is non-zero for $y \in [1, K_{se})$ and "Case 1" means $y < U^{-1} < 1$, $f_{X_{se}}(y) = 0$ in "Case 1" and thus, the first term in (71) is zero. Additionally, "Case 2" and "Case 3" are correspondingly equivalent to $U^{-1} \le y < V$ and $y > V$ where V is defined in (46). Because $f_{X_{se}}(y)$ is non-zero for $y \in [1, K_{se})$, three scenarios on V in correlation to $[1, K_{se})$ are considered as follows.

Scenario 1. $K_{se} < V$

This scenario reduces the last term is (71) to $\underbrace{\int\limits_{y=V}^{\infty} \left[\int\limits_{x=1}^{K_{sr}} f_{X_{sr}}(x)\, dx\right] f_{X_{se}}(y)\, dy}_{\text{Case 3: } y>V}$, which is zero because $f_{X_{se}}(y) = 0$ when $y = V > K_{se}$. Accordingly, (71) is simplified as

$$\Delta = \underbrace{\int\limits_{y=1}^{K_{se}} \left[\int\limits_{x=1}^{Uy} f_{X_{sr}}(x)\, dx\right] f_{X_{se}}(y)\, dy}_{\text{Case 2: } U^{-1}\le y<V}. \tag{72}$$

Invoking (42) to solve the inner integral in (72), one has

$$\begin{aligned} \Delta &= \int\limits_{1}^{K_{se}} \mathcal{A}(1, Uy, L_{sr})\, f_{X_{se}}(y)\, dy \\ &= \int\limits_{1}^{K_{se}} e^{H_{sr}} \left(e^{\frac{M_{sr}}{1-K_{sr}}} - e^{\frac{M_{sr}}{Uy-K_{sr}}}\right) f_{X_{se}}(y)\, dy \\ &= 1 - e^{H_{sr}} \mathcal{B}, \end{aligned} \tag{73}$$

where

$$\mathcal{B} = \int\limits_{1}^{K_{se}} e^{\frac{M_{sr}}{Uy-K_{sr}}} f_{X_{se}}(y)\, dy. \tag{74}$$

It should be noted that the last equality in (73) holds because $\int_1^{K_{se}} f_{X_{se}}(y)\,dy = 1$. Plugging $f_{X_{se}}(y)$ in (32) into (74) and after some simplifications, one have

$$\mathcal{B} = M_{se}e^{H_{se}}\mathcal{G}, \tag{75}$$

where

$$\mathcal{G} = \int_1^{K_{se}} \frac{e^{\frac{J}{y-V}+\frac{M_{se}}{y-K_{se}}}}{(y-K_{se})^2}dy, \tag{76}$$

with J being given in (47).

Substituting (75) into (73), it is seen that Δ in (73) agrees Δ in (45) for $K_{se} < V$. Accordingly, the next step is to show that (76) matches (49). Towards this end, executing some appropriate variable changes, one simplifies (76) to

$$\begin{aligned}
\mathcal{G} &\overset{x=\frac{1}{y-K_{se}}}{=} -\int_{1/(1-K_{se})}^{-\infty} e^{\frac{J}{K_{se}-V+1/x}+M_{se}x}dx \\
&\overset{y=-x}{=} \int_{1/(K_{se}-1)}^{\infty} e^{\frac{J}{K_{se}-V}\frac{y}{y-1/(K_{se}-V)}-M_{se}y}dy \\
&= e^{\frac{J}{K_{se}-V}} \int_{1/(K_{se}-1)}^{\infty} e^{\frac{J/(K_{se}-V)^2}{y-1/(K_{se}-V)}-M_{se}y}dy.
\end{aligned} \tag{77}$$

Executing the series expansion $e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}$ for the term $e^{\frac{J/(K_{se}-V)^2}{y-1/(K_{se}-V)}}$ in (77) results in

$$\begin{aligned}
\mathcal{G} &= e^{\frac{J}{K_{se}-V}} \int_{1/(K_{se}-1)}^{\infty} e^{-M_{se}y}\left(\sum_{n=0}^{\infty}\frac{1}{n!}\left[\frac{J/(K_{se}-V)^2}{y-1/(K_{se}-V)}\right]^n\right)dy \\
&= e^{\frac{J}{K_{se}-V}}\sum_{n=0}^{\infty}\frac{J^n}{(K_{se}-V)^{2n}n!}\int_{1/(K_{se}-1)}^{\infty}\frac{e^{-M_{se}y}}{[y-1/(K_{se}-V)]^n}dy \\
&= e^{\frac{J}{K_{se}-V}}\left\{\int_{1/(K_{se}-1)}^{\infty} e^{-M_{se}y}dy + \frac{J}{(K_{se}-V)^2}\int_{1/(K_{se}-1)}^{\infty}\frac{e^{-M_{se}y}}{y+1/(V-K_{se})}dy\right. \\
&\quad \left. + \sum_{n=2}^{\infty}\frac{J^n}{(K_{se}-V)^{2n}n!}\int_{1/(K_{se}-1)}^{\infty}\frac{e^{-M_{se}y}}{[y+1/(V-K_{se})]^n}dy\right\}.
\end{aligned} \tag{78}$$

Three integrals in the last equality of (78) are solved as follows. The first one is easy to solve. Additionally, the second one is solved in terms of the exponential-integral function

while the third one is computed by invoking [44, eq. (3.353.1)]. Plugging the closed forms of these three integrals into (78), one reduces (78) to (49), finishing the proof of Δ for $K_{se} < V$.

Scenario 2. $1 \leq V < K_{se}$

This scenario simplifies (71) as

$$\Delta = \underbrace{\int_{y=U^{-1}}^{V} \left[\int_{x=1}^{Uy} f_{X_{sr}}(x)\,dx\right] f_{X_{se}}(y)\,dy}_{\text{Case 2: } U^{-1}\leq y<V} + \underbrace{\int_{y=V}^{K_{se}} \left[\int_{x=1}^{K_{sr}} f_{X_{sr}}(x)\,dx\right] f_{X_{se}}(y)\,dy}_{\text{Case 3: } y>V}. \tag{79}$$

Before solving (79), it should be noted that $f_{X_{sr}}(x)$ is non-zero for $x \in [1, K_{sr})$ and thus, $\int_1^{K_{sr}} f_{X_{sr}}(x)\,dx = 1$. Moreover, $\int_1^{Uy} f_{X_{sr}}(x)\,dx$ is solved as $\mathcal{A}(1, Uy, L_{sr})$ according to (42). Accordingly, (79) is simplified as

$$\begin{aligned}
\Delta &= \int_1^V \mathcal{A}(1, Uy, L_{sr})\, f_{X_{se}}(y)\,dy + \int_V^{K_{se}} f_{X_{se}}(y)\,dy \\
&= \int_1^V e^{H_{sr}} \left(e^{\frac{M_{sr}}{1-K_{sr}}} - e^{\frac{M_{sr}}{Uy-K_{sr}}}\right) f_{X_{se}}(y)\,dy + \int_V^{K_{se}} f_{X_{se}}(y)\,dy \\
&= \int_1^V f_{X_{se}}(y)\,dy - e^{H_{sr}}\mathcal{D} + \int_V^{K_{se}} f_{X_{se}}(y)\,dy \\
&= 1 - e^{H_{sr}}\mathcal{D},
\end{aligned} \tag{80}$$

where

$$\mathcal{D} = \int_1^V e^{\frac{M_{sr}}{Uy-K_{sr}}} f_{X_{se}}(y)\,dy. \tag{81}$$

It should be noted that the last equality in (80) is solved since $\int_1^{K_{se}} f_{X_{se}}(y)\,dy = 1$. Plugging $f_{X_{se}}(y)$ in (32) into (81) and after some simplifications, one reduces (81) to

$$\mathcal{D} = M_{se} e^{H_{se}} \mathcal{K}, \tag{82}$$

where

$$\mathcal{K} = \int_1^V \frac{e^{J/(y-V) + M_{se}/(y-K_{se})}}{(y-K_{se})^2} dy. \tag{83}$$

Inserting (82) into (80), one reduces (80) to (45) for $1 \leq V < K_{se}$. Accordingly, the next step is to show that (83) coincides (50). Towards this end, applying some appropriate variable changes and the series expansion (similarly to steps in (77) and (78)), one reduces

(83) to

$$\begin{aligned}\mathcal{K} &= e^{\frac{J-M_{se}}{K_{se}-V}} \sum_{n=0}^{\infty} \frac{J^n}{(K_{se}-V)^{2n} n!} \int_I^0 \frac{e^{-M_{se}x}}{x^n} dx \\ &= e^{\frac{J-M_{se}}{K_{se}-V}} \left\{ \int_I^0 e^{-M_{se}x} dx + \sum_{n=1}^{\infty} \frac{J^n}{(K_{se}-V)^{2n} n!} \int_I^0 \frac{e^{-M_{se}x}}{x^n} dx \right\},\end{aligned} \tag{84}$$

where I is given in (48).

The first integral in (84) is easily solved while the second one is solved by invoking [44, eq. (2.324.2)]. Inserting closed forms of these two integrals into (84), one reduces (84) to (50), completing the proof of Δ for $1 \leq K_{se} < V$.

Scenario 3. $V < 1$

This scenario simplifies (71) as

$$\Delta = \underbrace{\int_{y=U^{-1}}^{V} \left[\int_{x=1}^{Uy} f_{X_{sr}}(x)\, dx \right] f_{X_{se}}(y)\, dy}_{\text{Case 2: } U^{-1} \leq y < V} + \underbrace{\int_{y=1}^{K_{se}} \left[\int_{x=1}^{K_{sr}} f_{X_{sr}}(x)\, dx \right] f_{X_{se}}(y)\, dy}_{\text{Case 3: } y > V}. \tag{85}$$

Since $f_{X_{se}}(y) = 0$ when $y = V < 1$, the first term in (85) is zero. Additionally, $f_{X_{sr}}(x)$ is non-zero for $x \in [1, K_{sr})$ and $f_{X_{se}}(y)$ is non-zero for $y \in [1, K_{se})$ and thus, the second term in (85) is one. Plugging these results into (85), one infers $\Delta = 1$, which matches (45) for $V < 1$. This finishes the proof of Δ for $V < 1$.

By combining the three above scenarios, it is seen that Δ is precisely solved as (45). This completes the proof of Theorem 1.

APPENDIX B: PROOF OF Ψ_2

Let $X_{sd} = 1 + \bar{A} h_{sd}$ and $\bar{X}_{se} = 1 + \frac{\bar{B} h_{se}}{\bar{C} h_{se} + \kappa_e}$ where $\bar{A}$, $\bar{B}$, and $\bar{C}$ are given in (60), (61), and (62), correspondingly. Relied on the variable change, the PDF of X_{sd} is expressed as

$$f_{X_{sd}}(x) = \frac{1}{\vartheta_{sd} \bar{A}} e^{-\frac{x-1}{\vartheta_{sd} \bar{A}}}, \; x \geq 1. \tag{86}$$

Also, by invoking Lemma 1, the PDF of $\bar{X}_{se}$ can be obtained as

$$f_{\bar{X}_{se}}(y) = \bar{G} \frac{e^{\bar{E} \frac{y-1}{y-\bar{D}}}}{\left(y - \bar{D}\right)^2}, \; 1 \leq y < \bar{D}, \tag{87}$$

where $\bar{D}$, $\bar{E}$, and $\bar{G}$ are correspondingly given in (63), (64), and (65).

Invoking (11) and (13) for the case of $\Gamma_s < \Gamma_t$, one rewrites Ψ_2 in (56) as

$$\Psi_2 = \Pr\left\{ 1 + \frac{\mu P_s h_{sd}}{\kappa_d} < U\left(1 + \frac{\mu P_s h_{se}}{(1-\mu) P_s h_{se} + \kappa_e}\right) \middle| \, \Gamma_s < \Gamma_t \right\}, \tag{88}$$

which is also represented in terms of X_{sd} and $\bar{X}_{se}$ as

$$\Psi_2 = \Pr\left\{ X_{sd} < U\bar{X}_{se} \middle| \Gamma_s < \Gamma_t \right\}. \tag{89}$$

Since X_{sd} and $\bar{X}_{se}$ are statistically independent, (89) can be rewritten in terms of the individual PDFs of X_{sd} and $\bar{X}_{se}$ as

$$\Psi_2 = \iint\limits_{x<Uy} f_{X_{sd}}(x)\, f_{\bar{X}_{se}}(y)\, dxdy. \tag{90}$$

Because $f_{X_{sd}}(x)$ is non-zero for $x \geq 1$, two cases on Uy in correlation to 1 are considered as

$$\Psi_2 = \underbrace{\int\limits_{y<U^{-1}} \left[\int\limits_{x<Uy} f_{X_{sd}}(x)\, dx \right] f_{\bar{X}_{se}}(y)\, dy}_{\text{Case 1: } Uy<1} + \underbrace{\int\limits_{y=1}^{\bar{D}} \left[\int\limits_{x=1}^{Uy} f_{X_{sd}}(x)\, dx \right] f_{\bar{X}_{se}}(y)\, dy}_{\text{Case 2: } Uy>1}. \tag{91}$$

The first term in (91) is zero since $\int\limits_{x<Uy} f_{X_{sd}}(x)\, dx = 0$ due to $f_{X_{sd}}(x) = 0$ for $x = Uy < 1$. Accordingly, by substituting (86) into the second term in (91) and after solving the inner integral in (91), one has

$$\Psi_2 = \int\limits_{1}^{\bar{D}} \left(1 - e^{-\frac{Uy-1}{\vartheta_{sd}\bar{A}}} \right) f_{\bar{X}_{se}}(y)\, dy = \underbrace{\int\limits_{1}^{\bar{D}} f_{\bar{X}_{se}}(y)}_{1} - e^{\frac{1}{\vartheta_{sd}\bar{A}}} \underbrace{\int\limits_{1}^{\bar{D}} e^{-\bar{Q}y} f_{\bar{X}_{se}}(y)\, dy}_{\mathcal{H}}, \tag{92}$$

where $\bar{Q}$ is given in (66).

The first integral in the last equality of (92) is one due to the property of the PDF while the second integral can be rewritten after invoking $f_{\bar{X}_{se}}(y)$ in (87) as

$$\begin{aligned} \mathcal{H} &= \int\limits_{1}^{\bar{D}} e^{-\bar{Q}y} \bar{G} \frac{e^{\bar{E}\frac{y-1}{y-\bar{D}}}}{\left(y-\bar{D}\right)^2} dy \\ &\overset{x=\frac{1}{y-\bar{D}}}{=} -\bar{G} e^{\bar{E}-\bar{Q}\bar{D}} \int\limits_{1/\left(1-\bar{D}\right)}^{-\infty} e^{\bar{G}x - \frac{\bar{Q}}{x}} dx \\ &\overset{y=-x}{=} \bar{G} e^{\bar{E}-\bar{Q}\bar{D}} \int\limits_{1/\left(\bar{D}-1\right)}^{\infty} e^{-\bar{G}y + \frac{\bar{Q}}{y}} dy. \end{aligned} \tag{93}$$

Executing the series expansion $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ for the term $e^{\frac{\bar{Q}}{y}}$ in (93), one obtains

$$\begin{aligned}\mathcal{H} &= \bar{G}e^{\bar{E}-\bar{Q}\bar{D}} \int_{1/(\bar{D}-1)}^{\infty} e^{-\bar{G}y}\left(\sum_{n=0}^{\infty}\frac{1}{n!}\left[\frac{\bar{Q}}{y}\right]^n\right)dy \\ &\overset{x=\bar{G}y}{=} e^{\bar{E}-\bar{Q}\bar{D}}\sum_{n=0}^{\infty}\frac{\left(\bar{Q}\bar{G}\right)^n}{n!}\int_{\bar{E}}^{\infty}\frac{e^{-x}}{x^n}dx. \end{aligned} \tag{94}$$

The last integral in (94) is solved by invoking [44, eq. (3.381.6)], which reduces (94) to

$$\mathcal{H} = e^{\bar{E}-\bar{Q}\bar{D}}\sum_{n=0}^{\infty}\frac{\left(\bar{Q}\bar{G}\right)^n}{n!}\bar{E}^{-n/2}e^{-\bar{E}/2}\mathbf{W}_{-\frac{n}{2},\frac{1-n}{2}}\left(\bar{E}\right). \tag{95}$$

Substituting (95) into (92), one reduces (92) to (59), finishing the proof.

REFERENCES

[1] S. K. Sharma, I. Woungang, A. Anpalagan, and S. Chatzinotas, "Towards tactile internet in beyond 5g era: Recent advances, current issues and future directions," *IEEE Access,* vol. 8, pp. 56948–56991, 2020.

[2] M. Tavana, A. Rahmati, V. Shah-Mansouri, and B. Maham, "Cooperative sensing with joint energy and correlation detection in cognitive radio networks," *IEEE Communications Letters,* vol. 21, pp. 132–135, 2017.

[3] D. Feng, C. Jiang, G. Lim, L. J. Cimini, Jr., G. Feng, and G. Y. Li, "A survey of energy-efficient wireless communications ," *IEEE Communications Surveys & Tutorials*, vol. 15, pp. 167-178, 2013.

[4] A. Celik, A. Alsharoa, and A. E. Kamal, "Hybrid energy harvesting cooperative spectrum sensing in heterogeneous CRNs," in *2016 IEEE Globecom Workshops (GC Wkshps)*, Washington, DC, 2016, pp. 1-6. Doi: 10.1109/GLOCOMW.2016.7848925

[5] S. Buzzi, C.-L. I, T. E. Klein, H. V. Poor, C. Yang, and A. Zappone, "A survey of energy-efficient techniques for 5G networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 697–709, 2016.

[6] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT," *IEEE Transactions on Wireless Communications,* vol. 16, pp. 2450–2464, 2017.

[7] G. Pan, H. Lei, Y. Yuan, and Z. Ding, "Performance analysis and optimization for SWIPT wireless sensor networks," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 2291–2302, May 2017. Doi: 10.1109/TCOMM.2017.2676815

[8] T. Liu, X. Wang, and L. Zheng, "A cooperative SWIPT scheme for wirelessly powered sensor networks," *IEEE Transactions on Communications,* vol. 65, no. 6, pp. 2740–2752, June 2017. Doi: 10.1109/TCOMM.2017.2685580

[9] H. Ding, D. B. da Costa, H. A. Suraweera, and J. Ge, "Role selection cooperative systems with energy harvesting relays," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4218–4233, June 2016. Doi: 10.1109/TWC.2016.2536732

[10] Y. Gu and S. Aissa, "RF-based energy harvesting in decode-and-forward relaying systems: Ergodic and outage capacities," *IEEE Transactions on Wireless Communications,* vol. 14, no. 11, pp. 6425–6434, Nov. 2015. Doi: 10.1109/TWC.2015.2453418

[11] A. Rajaram, D. N. K. Jayakody, K. Srinivasan, B. Chen, and V. Sharma, "Opportunistic-Harvesting: RF wireless power transfer scheme for multiple access relays system," *IEEE Access*, vol. 5, pp. 16084–16099, 2017. Doi: 10.1109/ACCESS.2017.2734852

[12] J. Miao and Z. Zheng, "Cooperative Jamming for Secure UAV-Enabled Mobile Relay System," *IEEE Access,* vol. 8, pp. 48943–48957, 2020. Doi: 10.1109/ACCESS.2020.2980242

[13] F. Zhu and M. Yao, "Improving physical layer security for CRNs using SINR-based cooperative beamforming," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1835–1841, March 2016. Doi: 10.1109/TVT.2015.2412152

[14] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013. Doi: 10.1109/TIFS.2013.2284754

[15] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications,* vol. 8, no. 10, pp. 5003–5011, October 2009. Doi: 10.1109/TWC.2009.090323

[16] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Transactions on Wireless Communications,* vol. 13, no. 3, pp. 1656–1667, March 2014. Doi: 10.1109/TWC.2013.013014.131248

[17] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Processing Letters,* vol. 20, no. 2, pp. 141–144, Feb. 2013. Doi: 10.1109/LSP.2012.2234109

[18] L. Jong-Ho, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Communications Letters,* vol. 19, no. 4, pp. 525–528, April 2015. Doi: 10.1109/LCOMM.2015.2401551

[19] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for noma systems against internal and external eavesdropping," *IEEE Transactions on Information Forensics and Security,* vol. 15, pp. 2930–2943, 2020. Doi: 10.1109/TIFS.2020.2980202

[20] 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)*, Istanbul, Turkey, 2019, pp. 1–5. Doi: 10.1109/PIMRC.2019.8904314

[21] 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),* Barcelona, 2018, pp. 1–6. Doi: 10.1109/WCNC.2018.8377306

[22] D. Wang, F. Zhou, and V. C. M. Leung, "Primary privacy preserving with joint wireless power and information transfer for cognitive radio networks," *IEEE Transactions on*

Cognitive Communications and Networking, vol. 6, no. 2, pp. 683–693, June 2020. Doi: 10.1109/TCCN.2019.2952885

[23] 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),* Barcelona, 2018, pp. 1–6. Doi: 10.1109/WCNC.2018.8377071

[24] 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, Nov. 2018. Doi: 10.1109/TVT.2018.2868902

[25] L. Chen, L. Huang, H. Xu, C. Yang, Z. Sun, and X. Wang, "Primary secrecy Is achievable: optimal secrecy rate in overlay CRNs with an energy harvesting secondary transmitter," in *2015 24th International Conference on Computer Communication and Networks (ICCCN)*, Las Vegas, NV, 2015, pp. 1–6. Doi: 10.1109/ICCCN.2015.7288450

[26] 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. 4754–4767, November 2013. Doi: 10.1109/TCOMM.2013.13.120855

[27] P. M. Quang, T. T. Duy, and V. N. Q. Bao, "Performance evaluation of underlay cognitive radio networks over Nakagami-m fading channels with energy harvesting," in *2016 International Conference on Advanced Technologies for Communications (ATC),* Hanoi, 2016, pp. 108–113. Doi: 10.1109/ATC.2016.7764755

[28] J. Zhang, G. Pan, and H.M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access,* vol. 4, pp. 3887–3893, 2016. Doi: 10.1109/ACCESS.2016.2591782

[29] W. Mou, W. Yang, X. Xu, X. Li, and Y. Cai, "Secure transmission in spectrum-sharing cognitive networks with wireless power transfer," in *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*, Yangzhou, 2016, pp. 1–5. Doi: 10.1109/WCSP.2016.7752665

[30] H. Lei, M. Xu, H. Zhang, G. Pan, I. S. Ansari, and K. A. Qaraqe, "Secrecy outage performance for underlay MIMO CRNs with energy harvesting and transmit antenna selection," in *2016 IEEE Globecom Workshops (GC Wkshps)*, Washington, DC, 2016, pp. 1–6. Doi: 10.1109/GLOCOMW.2016.7849037

[31] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Secrecy outage of a simultaneous wireless information and power transfer cognitive radio system," *IEEE Wireless Communications Letters*, vol. 5, no. 3, pp. 288–291, June 2016. Doi: 10.1109/LWC.2016.2544828

[32] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 329–342, Jan. 2016. Doi: 10.1109/TCOMM.2015.2498171

[33] 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 *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI),* Jaipur, 2016, pp. 1622–1627. Doi: 10.1109/ICACCI.2016.7732280

[34] S. Zhihui, Q. Yi, and C. Song, "On physical layer security for cognitive radio networks," *IEEE Network,* vol. 27, no. 3, pp. 28–33, May-June 2013. Doi: 10.1109/MNET.2013.6523805

[35] R. Sharma and D. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 17, no. 2, pp. 1023–1043, Secondquarter 2015. Doi: 10.1109/COMST.2014.2380998

[36] V. D. Nguyen, T. Q. Duong, O. A. Dobre, and O. S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 11, pp. 2609–2623, Nov. 2016. Doi: 10.1109/TIFS.2016.2594131

[37] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and artificial noise design for cognitive MIMOME wiretap channels," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 8, pp. 6753–6758, Aug. 2016. Doi: 10.1109/TVT.2015.2477305

[38] Y. Wu, X. Chen, and X. Chen, "Secure beamforming for cognitive radio networks with artificial noise," in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, Nanjing, 2015, pp. 1–5. Doi: 10.1109/WCSP.2015.7341139

[39] X. Hu, X. Zhang, H. Huang, and Y. Li, "Secure transmission via jamming in cognitive radio networks with possion spatially distributed eavesdroppers," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Valencia, 2016, pp. 1–6. Doi: 10.1109/PIMRC.2016.7794918

[40] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO cooperative cognitive radio networks," in *2015 IEEE International Conference on Communications (ICC)*, London, 2015, pp. 7609–7614. Doi: 10.1109/ICC.2015.7249543

[41] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Transactions on Wireless Communications,* vol. 16, no. 2, pp. 1319–1329, Feb. 2017. Doi: 10.1109/TWC.2016.2645200

[42] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Communications Letters,* vol. 4, no. 1, pp. 46–49, Feb. 2015. Doi: 10.1109/LWC.2014.2365808

[43] P. Chakraborty and S. Prakriya, "Secrecy performance of an idle receiver assisted underlay secondary network," *IEEE Transactions on Vehicular Technology,* vol. 66, no. 10, pp. 9555–9560, Oct. 2017. Doi: 10.1109/TVT.2017.2698162

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

Received on April 16, 2020
Revised on June 22, 2020