Physical Layer Security For Dual-hop SWIPT-Enabled CR Networks

Mounia Bouabdellah[1], Faissal El Bouanani[1], Paschalis C. Sofotasios[2,3], Daniel Benevides da Costa[4], Kahtan Mezher[2], Hussain Ben-azza[5], Sami Muhaidat[2], and George K. Karagiannidis[6]

[1]ENSIAS, Mohammed V University in Rabat, Rabat 10000, Morocco
[2]Center for Cyber-Physical Systems, Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi 127788, UAE
[3]Department of Electrical Engineering, Tampere University, 33101 Tampere, Finland
[4]Department of Computer Engineering, Federal University of Ceará (UFC), Sobral 62010-560, Brazil
[5]ENSAM, Moulay Ismail University in Meknes, Meknes 50500, Morocco
[6]Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, GR-51124, Thessaloniki, Greece
Emails: mounia_bouabdellah@um5.ac.ma, f.elbouanani@um5s.net.ma, p.sofotasios@ieee.org, danielbcosta@ieee.org, kahtan.mezher@ku.ac.ae, hbenazza@yahoo.com, muhaidat@ieee.org, geokarag@auth.gr

***Abstract*—We investigate the physical layer security of a relay-assisted underlay cognitive radio network with simultaneous wireless information and power transfer (SWIPT). To this end, we consider a secondary network comprising a secondary source S, one secondary user (SU) relay R, one SU destination D, one primary user (PU) transmitter, and one PU receiver. In addition, we consider an eavesdropper E which can overhear both communications of the $S \to R$ and $R \to D$ links whereas power constraints are imposed on the secondary network in order to maintain a tolerable interference level at the primary network. Under these constraints, we derive a closed-form expression for the secrecy outage probability assuming uncorrelated Rayleigh fading channels. Numerical and simulation results are presented to corroborate the corresponding analysis. It is shown that the harvested energy, energy conversion efficiency, and maximum tolerable interference level imposed on the primary receiver impact considerably the overall system's security.**

I. Introduction

In recent years, the proliferation of mobile devices has led to unprecedented demand for the wireless spectrum and energy efficient solutions. In this regard, energy harvesting (EH) and cognitive radio notions have been proposed as promising solutions to ensure energy and spectrum efficiency. Specifically, EH enabled devices harvest energy from either ambient RF signals or dedicated RF sources, while cognitive radio allows an efficient utilization of spectrum [1], [2]. Simultaneous wireless information and power transfer (SWIPT) is an EH technique that has been proposed in the context of two variants: (i) time switching (TS) and (ii) power splitting (PS) [3]. Specifically, the PS scheme splits the received signal into two streams, one for EH and the other for information decoding, while TS receivers allocate portion of the time to EH and dedicates the rest to information processing. Likewise, in underlay CRN, the secondary users (SUs) share the spectrum with primary users (PUs) under the condition of meeting the PUs' security and quality of service (QoS) requirements.

Recently, physical layer security (PLS) of CRNs gained a significant attention as an enhancing security technique, complementary to cryptography. In this context, several approaches have been proposed to enhance the security of such networks. For instance, a cooperative relaying technique was proposed to achieve a secure transmission in [4]-[10]. In these contributions, closed-form expressions for the SOP were derived by considering either a single multi-antenna relay [4]-[6] or multiple relays [7]-[10]. In [11]-[12], the authors considered the use of artificial noise to disrupt the eavesdroppers where several SOP expressions were derived assuming Rayleigh fading channels. Likewise, the PLS of non-cooperative CRNs was investigated in [13]-[16]. Closed-form as well as asymptotic expressions of the SOP were derived under Nakagami-m [13], [14] and Rayleigh fading conditions [15], [16], respectively. Also, the PLS of a non-cooperative EH-CRNs has been investigated in [17]-[20]. In these contributions, the authors assumed the presence of a direct communication link between the transmitter and the receiver. Additionally, the SUs are assumed to harvest energy from the PUs' signals. In [17]-[19], by considering Rayleigh fading channels, the SOP was derived while the IP was considered in [20]. However, to the best of our knowledge, the PLS of cooperative EH-CRNs has not been investigated in the open literature.

Motivated by the above, we investigate PLS of a cooperative EH-CRNs consisting of one SU source (S) that communicates with a SU destination (D) through a SWIPT-enabled relay (R) in the presence of an eavesdropper (E) who attempts to intercept communication at both hops. We also assume that the relay is not causing any interference to the PUs. In order to gain meaningful insights into the performance of PLS in SWIPT-enabled CRNs, we derive a closed-form expression for the SOP and demonstrate that the security of such communication systems is improved for certain values of the energy harvesting parameters as well as the maximum tolerable interference power at the PU receiver.

The remainder of this paper is organized as follows: Section II presents the system and channel models. In Section III, we derive a closed-form expression for the SOP of the considered EH-CRNs. Numerical results are provided and discussed in Section IV. while closing remarks are given in Section V.

II. System and channel models

In the aforementioned EH-CRN system illustrated in Fig. 1, SUs share the same spectrum with PUs under the requirement of respecting the PUs' quality of service (QoS). Therefore, node S has to continuously adapt its transmission power in order to avoid interfering with PUs. For the considered system, the communication is carried out in two phases as follows:

- Phase 1: The source S transmits data with power P_S. In order to avoid interference with the PU signal, the transmit power P_S should fall below the maximum tolerated interference level at PU_{Rx} (i.e., P_I). It follows that the transmission power of S is constrained by its maximum transmit power $P_S^{\max}$ and the tolerated P_I at the PU receiver:

$$P_S = \min\left(P_S^{\max}, \frac{P_I}{g_{SP}}\right), \tag{1}$$

  where $g_{SP} = |h_{SP}|^2$ with h_{SP} standing for the fading amplitude of the S-P link.
- Phase 2: The relay R harvests energy from RF signals transmitted by S. In the considered setup, it is assumed that the relay performs power splitting (PS) for energy harvesting. Hence, R harvests a fraction of power θ (i.e., $0 \leq \theta \leq 1$), from the received signal. The remaining power $(1-\theta)P_S$ is used to carry out information processing. If R harvests energy from the received signal for a duration of T, then the harvested energy at R is

$$E_H = T\eta\theta P_S g_{SR}, \tag{2}$$

  where η denotes the energy conversion efficiency coefficient ($0 \leq \eta \leq 1$). Importantly, all the harvested energy by R is assumed to be used for forwarding the information to its destination during the same time slot considered at the first hop. Therefore, the transmission power of R is given by

$$P_R = \frac{E_H}{T} = \eta\theta P_S g_{SR}. \tag{3}$$

Without loss of generality, we assume that the relay is located away from the primary network. Therefore, it is not required by the relay to adopt the power adaption policy as it does not impact the PU's QoS.

Also, all fading amplitudes are assumed to be Rayleigh distributed. Consequently, the channel power gains $g_q = |h_q|^2$, with $q = \{SR, SE, RD, RE\}$, are exponentially distributed with parameters λ_q that are inversely proportional to the average SNRs of the associated inks.

Accordingly, the received signal at R and D are given by

$$y_R = \sqrt{(1-\theta)P_S} h_{SR} x_s + n_R, \tag{4}$$

and

$$y_D = \sqrt{P_R} h_{RD} x_r + n_D, \tag{5}$$

respectively, where n_R and n_D denote the additive white Gaussian noise (AWGN) of zero mean and variance N_R and N_D, respectively. Likewise, x_s and x_r stand for the transmitted signals from S and R, respectively.

The received signals at the eavesdropper at the first and the second hop, respectively, are expressed as

$$y_{1E} = \sqrt{(1-\theta)P_S} h_{SE} x_s + n_E, \tag{6}$$

and

$$y_{2E} = \sqrt{P_R} h_{RE} x_r + n_E, \tag{7}$$

where n_E is the AWGN with zero mean and variance N_E. Without loss of generality, we also consider that all noise powers are identical, i.e., $N_E = N_R = N_D = N$.

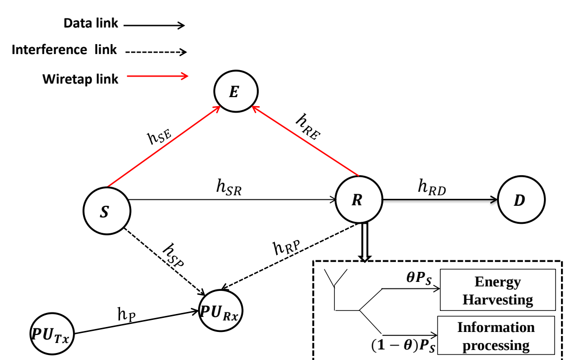

Fig. 1: The considered EH-CRN system.

III. Secrecy outage probability

The SOP stands for the probability that the secrecy capacity C_S falls below a predefined security rate R_s.

$$\text{SOP} = \Pr\left(C_S < R_s\right). \tag{8}$$

It is clearly seen from (8) that a secure system from the PLS prospect corresponds to great values of C_S.

A. Secrecy capacity

The secrecy capacity is defined as the maximum rate of the confidential information that is transmitted from a given source node to a given destination. Therefore, sufficient security is achieved when the capacity of the legitimate link i,e., S-R, is maximized. In the considered EH-CRN system, the eavesdropper is assumed to be intercepting communication at both hops i.e., S-R and R-D. Hence the secrecy capacity can be considered as the minimal capacity of the two hops i.e.

$$C_S = \min(C_{1S}, C_{2S}), \quad (9)$$

where C_{1S} and C_{2S} account for the secrecy capacities at the first and the second hop, respectively [15, Eq. (4)]

$$C_{1S} = \begin{cases} \log_2\left(\dfrac{1+\gamma_R}{1+\gamma_{1E}}\right) & , \ \gamma_R > \gamma_{1E} \\ 0 & , \ \text{elsewhere} \end{cases} \quad (10)$$

and

$$C_{2S} = \begin{cases} \log_2\left(\dfrac{1+\gamma_D}{1+\gamma_{2E}}\right) & , \ \gamma_D > \gamma_{2E} \\ 0 & , \ \text{elsewhere} \end{cases} \quad (11)$$

where γ_R consists of the combined signal-to-noise ratio at the relay R and is given by

$$\gamma_R = (1-\theta)\min\left(\overline{\gamma}_s, \frac{\overline{\gamma}_P}{g_{SP}}\right) g_{SR}. \quad (12)$$

Likewise, γ_D represents the SNR at D and it can be expressed as $\gamma_D = \rho_R g_{RD}$, with

$$\rho_R = \eta\theta\min\left(\overline{\gamma}_s, \frac{\overline{\gamma}_P}{g_{SP}}\right) g_{SR}, \quad (13)$$

and $\overline{\gamma}_s = P_S^{max}/N$, and $\overline{\gamma}_P = P_I/N$.

Finally, the SNRs at the eavesdropper γ_{1E} and γ_{2E} of the links S-E and R-E, are given by

$$\gamma_{1E} = (1-\theta)\min\left(\overline{\gamma}_s, \frac{\overline{\gamma}_P}{g_{SP}}\right) g_{SE}, \quad (14)$$

and $\gamma_{2E} = \rho_R g_{RE}$, respectively.

B. Closed-form secrecy outage probability

Using (8) along with (9), a closed-form expression for the SOP is derived in Theorem 1.

Theorem 1. *The SOP of the considered EH-CRN system subject to flat Rayleigh fading channels is given by (10), as shown at the top of next page, where* $\chi = \lambda_{SR}\gamma/\lambda_{SE}$, $\rho = \lambda_{SR}(\gamma-1)/(1-\theta)$, $\phi = \lambda_{SP}\overline{\gamma}_P/\overline{\gamma}_S$, $\omega_v = \lambda_{SR}/(\eta\theta\overline{\gamma}_s)$, $v \in \{S, P\}$, $\xi = \lambda_{RD}(\gamma-1)$, *whereas*

$$\Xi_1 = \xi^{-2} G_{2,1}^{1,2}\left(\frac{\lambda_{SP}}{\omega_P \xi}\middle| \begin{matrix} -1, 0; - \\ 0; - \end{matrix}\right), \quad (11)$$

and

$$\Omega = G_{0,1:1,1:1,2}^{1,0:1,1:1,1}\left(\frac{\omega_P\xi}{\lambda_{SP}}, \xi\omega_S \middle| \begin{matrix} -; - : 1; - : 1; - \\ 2; - : 1; - : 1; 0 \end{matrix}\right), \quad (12)$$

with $G_{p,q}^{m,n}\left(z \middle| \begin{matrix} (a_i)_{i\le p} \\ (b_k)_{k\le q} \end{matrix}\right)$ denoting the Meijer G-function [21, Eq. (9.301)], and $G_{p_1,q_1:p_2,q_2:p_3,q_3}^{0,n_1:m_2,n_2:m_3,n_3}(x, y|\Upsilon)$, with $\Upsilon = \left(\begin{matrix} (a_i)_{i=1:p_1} : (c_i)_{i=1:p_2} : (e_i)_{i=1:p_3} \\ (b_j)_{j=1:q_1} : (d_j)_{j=1:q_2} : (f_j)_{j=1:q_3} \end{matrix}\right)$ denoting the bivariate Meijer G-function [22, Eqs. (1.14)-(1.16)].

Proof: Substituting (9) into (8), the SOP becomes

$$\begin{aligned} \text{SOP} &= 1 - \Pr(C_{1S} > R_s)\Pr(C_{2S} > R_s) \quad (13) \\ &= 1 - [1 - \text{SOP}_1][1 - \text{SOP}_2], \end{aligned}$$

where SOP_1 and SOP_2 denote the SOP of either the first or the second hop.

1) Expression of SOP_1*:* By using (10), SOP_1 can be expressed as

$$\begin{aligned} \text{SOP}_1 &= \Pr(\gamma_R \le \gamma_{1E}) + \Pr(\gamma_R > \gamma_{1E}) \quad (14) \\ &\quad \times \Pr(C_{1S} < R_s | \gamma_R > \gamma_{1E}). \end{aligned}$$

Utilizing [21, Eq. (12)], one can obtain

$$\begin{aligned} \text{SOP}_1 &= \int_{x=0}^{\infty}\int_{y=0}^{\infty} F_{\gamma_R|g_{SP}=x}(\gamma y + \gamma - 1) \quad (15) \\ &\quad f_{\gamma_{1E}|g_{SP}=x}(y) f_{g_{SP}}(x)\,dy\,dx. \end{aligned}$$

The CDFs of γ_R and γ_{1E} for a given g_{SP} are expressed as

$$\begin{aligned} F_{\gamma_R|g_{SP}=x}(z) &= \Pr(\gamma_R \le z | g_{SP} = x) \quad (16) \\ &= F_{g_{SR}}\left(\frac{z}{(1-\theta)\Phi(x)}\right), \end{aligned}$$

and

$$\begin{aligned} F_{\gamma_{1E}|g_{SP}=x}(y) &= \Pr(\gamma_{1E} \le y | g_{SP} = x) \quad (17) \\ &= F_{g_{SE}}\left(\frac{y}{(1-\theta)\Phi(x)}\right). \end{aligned}$$

respectively, with $\Phi(x) = \overline{\gamma}_S$ for $x \le \overline{\gamma}_P/\overline{\gamma}_S$ and $\Phi(x) = \overline{\gamma}_P/x$ for $x > \overline{\gamma}_P/\overline{\gamma}_S$.

Hence, substituting the derivative of (17) alongside with (16) yields

$$\begin{aligned} \text{SOP}_1 &= \int_0^{\infty} \frac{f_{g_{SP}}(x)}{(1-\theta)\Phi(x)} \left[\begin{matrix} \int_0^{\infty} F_{g_{SR}}\left(\frac{\gamma y+\gamma-1}{(1-\theta)\Phi(x)}\right) \\ \times f_{g_{SE}}\left(\frac{y}{(1-\theta)\Phi(x)}\right) dy \end{matrix}\right] dx \\ &= \int_{x=0}^{\infty} f_{g_{SP}}(x)\left(1 - \frac{e^{-\frac{\rho}{\Phi(x)}}}{\chi+1}\right) dx. \quad (18) \end{aligned}$$

By also using the definition of $\Phi(x)$, we obtain

$$\begin{aligned} \text{SOP}_1 &= \left(1 - \frac{e^{-\frac{\rho}{\overline{\gamma}_S}}}{\chi+1}\right)\int_{x=0}^{\frac{\overline{\gamma}_P}{\overline{\gamma}_S}} f_{g_{SP}}(x)\,dx \quad (19) \\ &\quad + \int_{x=\frac{\overline{\gamma}_P}{\overline{\gamma}_S}}^{\infty} f_{g_{SP}}(x)\left(1 - \frac{e^{-\frac{\rho x}{\overline{\gamma}_P}}}{\chi+1}\right) dx \\ &= 1 - \frac{e^{-\frac{\rho}{\overline{\gamma}_S}}}{\chi+1}\left\{1 - e^{-\phi} + \frac{e^{-\phi}}{\frac{\rho}{\overline{\gamma}_P\lambda_{SP}}+1}\right\}. \end{aligned}$$

$$\mathrm{SOP} = 1 - \frac{1}{\delta}\left[\frac{e^{-\frac{\rho}{\overline{\gamma}_S}}}{\chi+1}\left(1 - e^{-\phi} + \frac{e^{-\phi}}{\frac{\rho}{\overline{\gamma}_P \lambda_{SP}}+1}\right)\right]\left[\left(1-e^{-\phi}\right) G_{0,2}^{2,0}\left(\omega_S \xi \,\middle|\, \begin{matrix} -;- \\ 0,1;- \end{matrix}\right) + \frac{\lambda_{SP} e^{-\phi}}{\xi \omega_P}\left[\xi^2 \Xi_1 - \Omega\right]\right]. \quad (10)$$

2) Expression of SOP_2*:* Using (11), SOP_2 can be expressed as

$$\begin{aligned} \mathrm{SOP}_2 &= \Pr\left(\gamma_D \le \gamma_{2E}\right) + \Pr\left(\gamma_D > \gamma_{2E}\right) \\ &\quad \Pr\left(C_{2S} < R_s \left| \gamma_D > \gamma_{2E}\right.\right). \end{aligned} \quad (20)$$

To this effect, by using [15, Eq. (12)], we obtain

$$\begin{aligned} \mathrm{SOP}_2 &= \int_{x=0}^{\infty}\int_{y=0}^{\infty} F_{\gamma_D|\rho_R=x}\left(\gamma y + \gamma - 1\right) \\ &\quad \times f_{\gamma_{2E}|\rho_R=x}(y) f_{\rho_R}(x) dy dx. \end{aligned} \quad (21)$$

The CDFs of γ_D and γ_{2E} for a given ρ_R can be expressed as

$$F_{\gamma_D|\rho_R=x}\left(z\right) = \Pr\left(\gamma_D \le z \left|\rho_R = x\right.\right) = F_{g_{RD}}\left(\frac{z}{x}\right), \quad (22)$$

and

$$F_{\gamma_{2E}|\rho_R=x}\left(z\right) = \Pr\left(\gamma_{2E} \le z \left|\rho_R = x\right.\right) = F_{g_{RE}}\left(\frac{z}{x}\right), \quad (23)$$

respectively. Based on this, the CDF of ρ_R is given by

$$\begin{aligned} F_{\rho_R}\left(z\right) &= \Pr\left(\min\left(\overline{\gamma}_s, \frac{\overline{\gamma}_P}{g_{SP}}\right) g_{SR} \le \frac{z}{\eta\theta}\right) \\ &= \underbrace{\Pr\left(g_{SR} \le \frac{z}{\eta\theta\overline{\gamma}_s}, \frac{\overline{\gamma}_P}{g_{SP}} \ge \overline{\gamma}_s\right)}_{\mathcal{I}_1} \\ &\quad \underbrace{+\Pr\left(\frac{g_{SR}}{g_{SP}} \le \frac{z}{\eta\theta\overline{\gamma}_P}, \frac{\overline{\gamma}_P}{g_{SP}} \le \overline{\gamma}_s\right)}_{\mathcal{I}_2}, \end{aligned} \quad (24)$$

where the two terms $\mathcal{I}_1$ and $\mathcal{I}_2$ can be rewritten as

$$\mathcal{I}_1 = F_{g_{SR}}\left(\frac{z}{\eta\theta\overline{\gamma}_s}\right) F_{g_{SP}}\left(\frac{\overline{\gamma}_P}{\overline{\gamma}_s}\right), \quad (25)$$

and

$$\begin{aligned} \mathcal{I}_2 &= \int_{\frac{\overline{\gamma}_P}{\overline{\gamma}_s}}^{\infty} F_{g_{SR}}\left(\frac{z}{\eta\theta\overline{\gamma}_P} y\right) f_{g_{SP}}\left(y\right) dy \\ &= \lambda_{SP}\int_{\frac{\overline{\gamma}_P}{\overline{\gamma}_s}}^{\infty}\left(1 - e^{-\omega_P z y}\right) e^{-\lambda_{SP} y} dy \\ &= e^{-\phi} - \frac{\lambda_{SP} e^{-(\omega_S z + \phi)}}{\omega_P z + \lambda_{SP}}. \end{aligned} \quad (26)$$

Then, by replacing (25) and (26) into (24), yields

$$F_{\rho_R}\left(z\right) = 1 - e^{-\omega_S z}\left(1 - e^{-\phi}\right) - \frac{\lambda_{SP} e^{-(\omega_S z + \phi)}}{\omega_P z + \lambda_{SP}} \quad (27)$$

whreas by differentiating (27), it follows that

$$\begin{aligned} f_{\rho_R}\left(z\right) &= \left(1 - e^{-\phi}\right)\omega_S e^{-\omega_S z} \\ &\quad + \frac{\lambda_{SP} e^{-\phi}}{\omega_P}\left(\frac{\omega_S e^{-\omega_S z}}{z + \frac{\lambda_{SP}}{\omega_P}} + \frac{e^{-\omega_S z}}{\left(z + \frac{\lambda_{SP}}{\omega_P}\right)^2}\right). \end{aligned} \quad (28)$$

Based on the above, substituting (22), (28), and the derivative of (23) into (21), yields

$$\begin{aligned} \mathrm{SOP}_2 &= 1 - \frac{1}{\delta}\int_{x=0}^{\infty} f_{\rho_R}(x) e^{-\frac{\xi}{x}} dx \\ &= 1 - \frac{1}{\delta}\left[\left(1 - e^{-\phi}\right)\Phi_1 + \frac{\lambda_{SP} e^{-\phi}}{\omega_P}\left(\Phi_2 + \Phi_3\right)\right], \end{aligned} \quad (29)$$

where

$$\Phi_1 = \omega_S \int_0^{\infty} e^{-\left(\frac{\xi}{x} + \omega_S x\right)} dx, \quad (30)$$

$$\Phi_2 = \omega_S \int_0^{\infty} \frac{e^{-\left(\omega_S x + \frac{\xi}{x}\right)}}{x + \frac{\lambda_{SP}}{\omega_P}} dx, \quad (31)$$

and

$$\Phi_3 = \int_0^{\infty} \frac{e^{-\left(\omega_S x + \frac{\xi}{x}\right)}}{\left(x + \frac{\lambda_{SP}}{\omega_P}\right)^2} dx \quad (32)$$

which need be evaluated. To this end, using [21, Eq. (3.324.1)] alongside with [23, Eq. (03.04.26.0006.01)], it follows that

$$\begin{aligned} \Phi_1 &= \omega_S \sqrt{\frac{\xi}{\omega_S}} G_{0,2}^{2,0}\left(\omega_S \xi \,\middle|\, \begin{matrix} -;- \\ \frac{1}{2}, \frac{-1}{2}; - \end{matrix}\right) \\ &= G_{0,2}^{2,0}\left(\omega_S \xi \,\middle|\, \begin{matrix} -;- \\ 0,1;- \end{matrix}\right). \end{aligned} \quad (33)$$

By performing integration by parts, Φ_3 can re-written as

$$\Phi_3 = \int_0^{\infty}\left(-\omega_S + \frac{\xi}{x^2}\right)\frac{e^{-\left(\omega_S x + \frac{\xi}{x}\right)}}{x + \frac{\lambda_{SP}}{\omega_P}} dx. \quad (34)$$

On the other hand, using [23, Eqs. (07.34.03.0271.01), (01.03.26.0007.01)] along with (34), yields $\Phi_2 + \Phi_3 = \xi\left[\Xi_1 - \Xi_2\right]$, where

$$\Xi_1 = \int_0^{\infty} y e^{-\xi y} G_{1,1}^{1,1}\left(\frac{\lambda_{SP}}{\omega_P} y \,\middle|\, \begin{matrix} 0;- \\ 0;- \end{matrix}\right) dy, \quad (35)$$

and

$$\Xi_2 = \int_0^{\infty} \frac{y}{e^{\xi y}} G_{1,1}^{1,1}\left(\frac{\lambda_{SP}}{\omega_P} y \,\middle|\, \begin{matrix} 0;- \\ 0;- \end{matrix}\right) G_{1,2}^{1,1}\left(\frac{\omega_S}{y} \,\middle|\, \begin{matrix} 1;- \\ 1;0 \end{matrix}\right) dy. \quad (36)$$

Using [23, Eq. (07.34.21.0088.01)], (11) is attained.

On the other hand, (36) can be rewritten using Mellin-Barnes integrals as

$$\begin{aligned} \Xi_2 &= \frac{1}{\left(2\pi j\right)^2}\int_{\mathcal{C}_1}\Gamma\left(s\right)\Gamma\left(1-s\right)\left(\frac{\lambda_{SP}}{\omega_P}\right)^{-s} \\ &\quad \times \int_{\mathcal{C}_2}\frac{\Gamma\left(1+v\right)\Gamma\left(-v\right)}{\Gamma\left(1-v\right)\omega_S^v} ds dv \int_0^{\infty}\frac{y^{v-s+1}}{e^{\xi y}} dy \end{aligned} \quad (37)$$

which becomes $\Xi_2 = \Omega/\xi^2$, where $j = \sqrt{-1}$, $\Gamma\left(.\right)$ denotes the Euler Gamma function [21, Eq. (8.310.1)], $\mathcal{C}_1$ whereas and $\mathcal{C}_2$ are two complex contours of integration ensuring the convergence of the above bivariate Meijer G-functions.

Next, substituting (11) and (37) into (III-B2), yields

$$\Phi_2 + \Phi_3 = \frac{1}{\xi}\left[G_{2,1}^{1,2}\left(\frac{\lambda_{SP}}{\omega_P \xi}\middle| \begin{array}{c} -1, 0; - \\ 0; - \end{array}\right) - \Omega\right]. \quad (38)$$

By also substituting (33) and (38) into (29), yields

$$\mathrm{SOP}_2 = 1 - \frac{1}{\delta}\left[\begin{array}{c} \left(1 - e^{-\phi}\right)\Phi_1 + \\ \frac{\lambda_{SP} e^{-\phi}}{\omega_P \xi}\left(G_{2,1}^{1,2}\left(\frac{\lambda_{SP}}{\omega_P \xi}\middle| \begin{array}{c} -1, 0; - \\ 0; - \end{array}\right) - \Omega\right) \end{array}\right] \quad (39)$$

Finally, substituting (19) and (39) into (13), leads to (10) which concludes the proof. ■

IV. Results and discussion

In this section we evaluate the security performance of the considered EH-CRN setup. The derived SOP expression in (10) is validated through corresponding Monte-Carlo simulation by generating 10^6 exponentially distributed random values. The simulation parameters are depicted in Table I.

TABLE I: Simulation parameters.

Parameter	λ_q	$\overline{\gamma}_P$ (dB)	$\overline{\gamma}_S$ (dB)	R_S (bit/s/Hz)	θ
value	0.5	10	10	1	0.5

Fig. 2 illustrates the SOP as a function of $\overline{\gamma}_P$ for various values of η. It can be observed that SOP decreases with the increasing values of $\overline{\gamma}_P$ and η. Indeed, under the assumption that fading severity parameters of the legitimate links i.e., λ_{SR} and λ_{RD} are smaller than those of the wiretap channels, i.e., λ_{SE} and λ_{RE}, the greater $\overline{\gamma}_P$, the greater the SNRs γ_R and γ_{1D}. Consequently, the capacity of the legitimate links is greater than the one of the wiretap links, which ultimately leads to an enhanced system security.

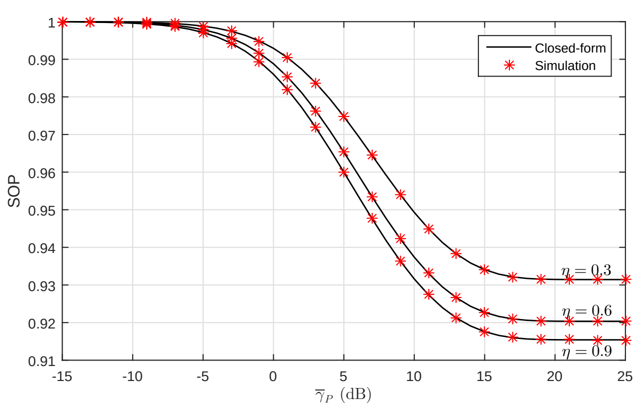

Fig. 2: SOP vs $\overline{\gamma}_P$ for various values of η.

Fig. 3 shows the SOP versus the energy harvesting ratio θ for different values of η. Clearly, the SOP is a concave function of θ. This behavior can be construed by the fact that as θ tends to 0 the instantaneous SNRs given in (III-A), also approach 0. Hence, C_S tends to 0 leading to the highest value of the SOP. Similarly, as θ tends to 1 the instantaneous SNRs given in (12) and (14) approach 0. Consequently, both C_{1S} and C_S approach 0, and thus the SOP increases accordingly.

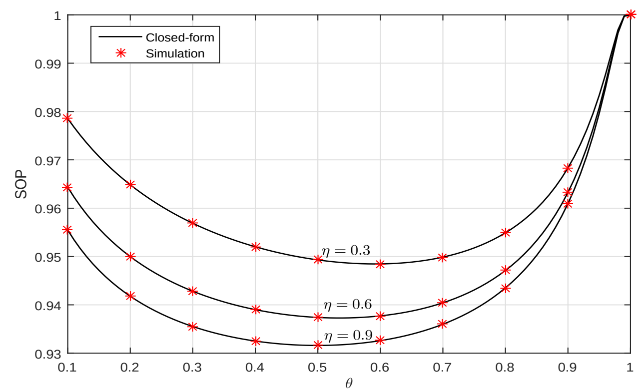

Fig. 3: SOP vs θ for various values of η.

Finally, Fig. 4 demonstrates the SOP versus both $\overline{\gamma}_P$ and θ. Evidently, the parameters $\overline{\gamma}_P$ and θ admit certain values for which a better security is achieved. For instance, one can infer that a higher secrecy is achieved for $0.4 \leq \theta \leq 0.6$ and $\overline{\gamma}_P \geq 15$dB.

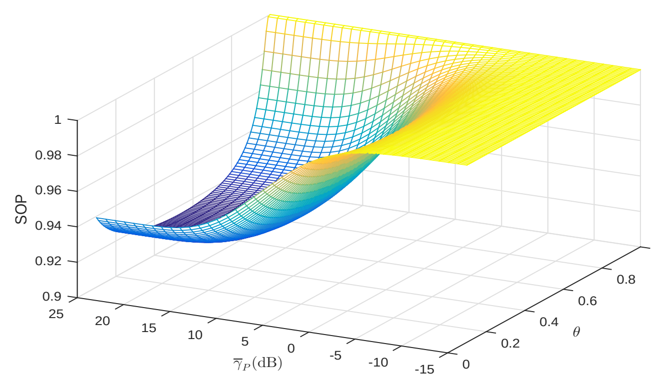

Fig. 4: SOP versus θ and $\overline{\gamma}_P$ for $\eta = 0.9$.

V. Conclusion

The secrecy performance of an EH-CRN system was analyzed. In particular, a power splitting based scheme was considered for energy harvesting at the relay. A closed-form expression for SOP was then derived and subsequently used in quantifying the impact of the involved parameters on the overall secrecy performance. The offered results provide useful theoretical and technical insights that will be useful in the design of EH-CRN systems. For example, it was shown that a better secrecy is achieved when the tolerated interference power at the PU receiver is higher and when the coefficient of the energy efficiency coefficient tends to 1. In addition, it was shown that the system's security is enhanced when the fraction of the harvested power is between 0.4 and 0.6.

REFERENCES

[1] M. Bouabdellah, N. Kaabouch, F. El Bouanani and H. Ben-azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey", *Journal of Information Security and Applications*, vol. 38, pp. 40-49, Dec. 2017.

[2] Y. Saleem and M. Rehmani, "Primary radio user activity models for cognitive radio networks: A survey", *Journal of Network and Computer Applications*, vol. 43, pp. 1-16, April 2014.

[3] Y. Gu and S. Aissa, "RF-Based Energy Harvesting in Decode-and-Forward Relaying Systems: Ergodic and Outage Capacities", *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6425-6434, 2015.

[4] M. Bouabdellah, F. E. Bouanani, and H. Ben-azza, "Secrecy outage performance for dual-Hop underlay cognitive radio system over Nakagami-m fading," *International Conference on Smart Digital Environment (ICSDE'18)*, Oct. 2018.

[5] M. Bouabdellah, F. E. Bouanani, and H. Ben-azza, "Secrecy outage probability in cognitive radio networks subject to Rayleigh fading channels," *2018 International Conference on Advanced Communication Technologies and Networking (CommNet)*, p. 1-5, April 2018.

[6] T. Zhang, Y. Huang, Y. Cai and W. Yang, "Secure Transmission in Spectrum Sharing Relaying Networks With Multiple Antennas", *IEEE Wireless Commun. Lett.*, vol. 20, no. 4, pp. 824-827, March 2016.

[7] H. Lei, H. I. S. Zhang, Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M. S. Alouini, "On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-m fading channels", *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no 4, pp. 614-627, Dec. 2017.

[8] H. Sakran, O. Nasr, S. El-Rabaie, A. El-Azm and M. Shokair, "Proposed relay selection scheme for physical layer security in cognitive radio networks", *IET Commun.*, vol. 6, no. 16, pp. 2676-2687, 2012.

[9] K. Ho-Van and T. Do-Dac, "Analysis of security performance of relay selection in underlay cognitive networks", *IET Commun.*, vol.12, no. 1, pp. 102-108, January 2018.

[10] S. Jia, J. Zhang, H. Zhao, Y. Lou and Y. Xu, "Relay Selection for Improved Physical Layer Security in Cognitive Relay Networks Using Artificial Noise", *IEEE Access*, vol. 6, pp. 64836-64846, 2018.

[11] Y. Zou, "Physical-Layer security for spectrum sharing systems", *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319-1329, Feb. 2017.

[12] Y. Liu, L. Wang , T. Duy, M. Elkashlan, and T. Duong. "Relay selection for security enhancement in cognitive relay networks". *IEEE Wireless Commun. Lett.*, vol. 4, no 1, pp. 46-49, Feb. 2015.

[13] H. Lei, C. Gao, I. Ansari, Y. Guo, Y. Zou, G. Pan and K. Qaraqe, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami- m channels",*IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237-2250, March 2017.

[14] N. Nguyen, T. Thanh, T. Duong and A. Nallanathan, "Secure communications in cognitive underlay networks over Nakagami-m channel", *Physical Commun.*, vol. 25, pp. 610-618, June 2017.

[15] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks", *IEEE Trans. Veh. Technol.*, vol. 64, no 8, pp. 3790-3795, Aug. 2015.

[16] H. Tran, G. Kaddoum, F. Gagnon and L. Sibomana, "Cognitive radio network with secrecy and interference constraints", *Physical Commun.*, vol. 22, pp. 32-41, Dec. 2016.

[17] M. Hanif, H. Yang and M. Alouini, "Transmit Antenna Selection for Power Adaptive Underlay Cognitive Radio With Instantaneous Interference Constraint", *IEEE Trans. on Commun.*, vol. 65, no. 6, pp. 2357-2367, June 2017.

[18] J. Zhang, G. Pan and H. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system", *IEEE Access*, vol. 4, pp. 3887-3893, July 2016.

[19] H. Lei, M. Xu, I. Ansari, G. Pan, K. Qaraqe and M. Alouini, "On Secure Underlay MIMO Cognitive Radio Networks With Energy Harvesting and Transmit Antenna Selection", *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 2, pp. 192-203, 2017.

[20] P. Yan, Y. Zou and J. Zhu, "Energy-Aware Multiuser Scheduling for Physical-Layer Security in Energy-Harvesting Underlay Cognitive Radio Systems", *IEEE Trans. on Vehicular Technology*, vol. 67, no. 3, pp. 2084-2096, March 2018.

[21] I. Gradshteyn, I. Ryzhik, A. Jeffrey and D. Zwillinger, Table of integrals, series and products. Oxford: Academic, 2007.

[22] T. Nguyen and S. Yakubovich, The double Mellin-Barnes type integrals and their applications to convolution theory. Singapore: World Scientific, 1992.

[23] Wolfram Research, Inc. "Mathematica", Edition: Version 10.0, Champaign, Illinois, Wolfram Research, Inc., 2014.