Security Improvement for Energy Harvesting based Overlay Cognitive Networks with Jamming-Assisted Full-Duplex Destinations

Khuong Ho-Van, Paschalis C. Sofotasios, Sami Muhaidat, Simon L. Cotton, Seong Ki Yoo, Yury A. Brychkov, Octavia A. Dobre, and Mikko Valkama

Original citation & hyperlink:
Ho-Van, K., Sofotasios, P.C., Muhaidat, S., Cotton, S.L., Yoo, S.K., Brychkov, Y.A., Dobre, O.A. and Valkama, M., 2021. Security improvement for energy harvesting based overlay cognitive networks with jamming-assisted full-duplex destinations. *IEEE Transactions on Vehicular Technology*, *70*(11), pp.12232-12237.
https://dx.doi.org/10.1109/TVT.2021.3118329

DOI 10.1109/TVT.2021.3118329
ISSN 0018-9545
ESSN 1939-9359

Publisher: IEEE

Security Improvement for Energy Harvesting based Overlay Cognitive Networks with Jamming-Assisted Full-Duplex Destinations

Khuong Ho-Van, Paschalis C. Sofotasios, *Senior Member, IEEE*, Sami Muhaidat, *Senior Member, IEEE*, Simon L. Cotton, *Senior Member, IEEE*, Seong Ki Yoo, *Senior Member, IEEE*, Yury A. Brychkov, Octavia A. Dobre, *Fellow, IEEE*, and Mikko Valkama, *Senior Member, IEEE*

***Abstract*—This work investigates the secrecy capability of energy harvesting based overlay cognitive networks (EHOCNs). To this end, we assume that a message by a licensed transmitter is relayed by an unlicensed sender. Critically, the unlicensed sender uses energy harvested from licensed signals, enhancing the overall energy efficiency and maintaining the integrity of licensed communications. To secure messages broadcast by the unlicensed sender against the wire-tapper, full-duplex destinations – unlicensed recipient and licensed receiver – jam the eavesdropper at the same time they receive signals from the unlicensed sender. To this effect, we derive closed-form formulas for the secrecy outage probability, which then quantify the security performance of both unlicensed and licensed communications for EHOCNs with jamming-assisted full-duplex destinations, namely EHOCNwFD. In addition, optimum operating parameters are established, which can serve as essential design guidelines of such systems.**

***Index Terms*—Energy harvesting, full-duplex jamming, overlay cognitive radio, PHY layer security, secrecy probability.**

I. Introduction

Cognitive radio technology (CRT) permits unlicensed users (UUs) to operate in licensed frequency bands (LFBs) of licensed users (LUs) via three popular principles: underlay, interweave, and overlay [1]. The underlay principle offers UUs access permission to LFBs, whenever UUs guarantee that generated interference by them is below an acceptable level for LUs. In the interweave principle, UUs merely access unused frequencies of LUs, whereas in the overlay principle UUs are allowed to share concurrently LFBs with LUs. The latter is achieved using sophisticated signal processing methods, which ultimately enhance the overall performance of CRT.

Radio frequency (RF) energy harvesting (EH) exploits available energy resources to power wireless terminals, leading to an overall improved energy efficiency [2]. Yet, legal messages in practical communications can be overheard, particularly in CRT where wire-tappers can emulate UUs to access LFBs. Owing to this, recent methods such as physical layer security (PLS) have emerged as efficacious solutions to enhance security in wireless networks [3]. Among various PLS methods, jamming exhibits distinct capabilities of security improvement, without additional complexity [4]. This, along with CRT and RF EH, can assist in addressing the challenges of emerging technologies, such as increased number of wireless services for a massive number of users, efficient spectrum utilization, high energy efficiency, and enhanced security [5].

Several contributions investigated message security for interweave/underlay cognitive networks with EH and jamming; yet, only few have concentrated on the overlay ones [6]–[17]. Specifically, [6] and [7] investigated the scenario in Fig. 1, where the unlicensed sender S scavenges energy in licensed signals for powering its two concurrent activities: send its own message and relay the licensed message. Also, in order to restrict overhearing of the wire-tapper W, the licensed receiver R was assumed to send jamming signals towards W. Different from [6] and [7] where R served as jammer, [8]–[10] proposed a conscientious jammer J. Nonetheless, J in [8] and [9] must scavenge RF energy from the licensed transmitter P while J in [10] was an RF energy supplier for S. To further secure messages in [6]–[10], [11] exploited both R and J to interrupt W, and only S is able to scavenge the RF energy. As an alternative solution to secure EHOCNs with multiple unlicensed sender-recipient pairs and various wire-tappers, [12] considered the joint transmit antenna selection and multiuser scheduling method. However, the considered jammers in [6]–[11] and unlicensed senders in [12] were assumed to operate in half-duplex (HD) mode, which is less efficient than full-duplex (FD) mode [13]–[17]. In [13]–[15], S exploited the FD mode for improved spectral efficiency.

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

K. Ho-Van is with Ho Chi Minh City University of Technology (HCMUT), 268 Ly Thuong Kiet Street, District 10, Ho Chi Minh City, Vietnam and with Vietnam National University Ho Chi Minh City, Linh Trung Ward, Thu Duc District, Ho Chi Minh City, Vietnam (e-mail: hvkhuong@hcmut.edu.vn).

P. C. Sofotasios is with the Center for Cyber-Physical Systems, Department of Electrical Engineering and Computer Science, Khalifa University, P. O. Box 127788, Abu Dhabi, UAE and also with the Department of Electrical Engineering, Tampere University, FI-33720, Tampere, Finland (e-mail: p.sofotasios@ieee.org).

S. Muhaidat are with the Center for Cyber-Physical Systems, Department of Electrical Engineering and Computer Science, Khalifa University, P. O. Box 127788, Abu Dhabi, UAE (e-mail: muhaidat@ieee.org).

S. L. Cotton is with Centre for Wireless Innovation, ECIT Institute, Queen's University Belfast, BT3 9DT, Belfast, UK (e-mail: simon.cotton@qub.ac.uk).

S. K. Yoo is with the Centre for Computational Science and Mathematical Modelling, Faculty of Engineering, Environment and Computing, Coventry University, CV1 2TL, UK (e-mail: ad3869@coventry.ac.uk).

Yu. A. Brychkov is with the Dorodnicyn Computing Center, Russian Academy of Sciences, Moscow 119991, Russia (e-mail: brychkov@ccas.ru).

O. A. Dobre is with the Faculty of Engineering and Applied Science, Memorial University, St. John's, NL A1C 5S7, Canada (e-mail: odobre@mun.ca).

M. Valkama is with the Department of Electrical Engineering, Tampere University, FI-33720, Tampere, Finland (e-mail: mikko.e.valkama@tuni.fi).

Yet, even though [13]–[15] carried out an outage probability analysis, the issue on the message security was bypassed there. In [16] and [17], S assists and secures effectively the FD based licensed communication, which receives P's message and jams W simultaneously. Nonetheless, [16] and [17] did not exploit EH for energy efficiency improvement. Moreover, no security analyses in terms of the corresponding secrecy outage probability (SOP) were carried out in [6]–[17], neither for licensed nor for unlicensed communications in EHOCNwFD.

Motivated by the above observations, this work analyzes EHOCNwFD in which P and R cannot achieve direct communications. Also, S sends its own message and assists licensed communications in exchange for access to LFBs. In this context, jamming-assisted FD destinations (R and unlicensed recipient D) are exploited to protect messages transmitted by S against W through the creation of jamming signals. Also, S is assumed to self-power its operation by extracting energy from licensed signals. Relied on this, closed-form formulas for the corresponding SOPs are derived for the scenario of both unlicensed and licensed communications. To this end, a creative signal generator is assumed for S, which either sends an unlicensed message in the last two phases, or relays a licensed message in Phase 2 and transmits its message in Phase 3, subject to successful recovery of the licensed message.

II. System Description

A. Channel Model

In Fig. 1, $h_{\mathtt{mn}}$ and $d_{\mathtt{mn}}$ denote the channel coefficient and the distance between the corresponding transmitter-receiver pair, respectively, where $\mathtt{m} \in \{p, s, d, r\}$ and $\mathtt{n} \in \{s, d, r, w\}$. Because R and D are FD destinations, they receive signals from S at the same time they transmit jamming signals to W. Due to imperfect self-interference (SI) cancellation of the FD operation at R and D, residual SIs at R and D are represented through loop channels with channel coefficients h_{rr} and h_{dd}, respectively. Notably, for effective wireless power transfer (WPT), the presence of a line-of-sight component is typically necessary. But since only Phase 1 performs WPT, h_{ps} is assumed to follow Rician distribution while other channel coefficients are Rayleigh-distributed. Such an assumption is valid in scenarios where P is placed high above the ground, while other users are located on the ground.

Based on the above, we also let $\alpha_{\mathtt{mn}} = \mathsf{E}\left\{|h_{\mathtt{mn}}|^2\right\}$ represent the fading power, where $\mathsf{E}\{\cdot\}$ denotes statistical expectation. To this effect, we can model $\alpha_{\mathtt{mn}} = \varsigma_0(\mathrm{d}_{\mathtt{mn}}/\mathrm{d}_0)^{-\beta}$, where $\mathrm{d}_0 = 1$ meter (m) is the reference distance, β is the exponent decay, and ς_0 is the fading power at d_0 [15]. For Rayleigh fading, the channel coefficient is indicated by a zero-mean circular symmetric complex Gaussian random variable, namely $h_{\mathtt{mn}} \sim \mathcal{CN}(0, \alpha_{\mathtt{mn}})$. Then, the cumulative distribution function (CDF) and the probability density function (PDF) of the channel gain $g_{\mathtt{mn}} = |h_{\mathtt{mn}}|^2$ are: $F_{g_{\mathtt{mn}}}(z) = 1 - e^{-z/\alpha_{\mathtt{mn}}}$ and $f_{g_{\mathtt{mn}}}(z) = e^{-z/\alpha_{\mathtt{mn}}}/\alpha_{\mathtt{mn}}$, respectively, which hold for $z \geq 0$.

B. Network Model

Fig. 1 illustrates that message transmissions from P and S to R and D are completed in three phases whose duration is

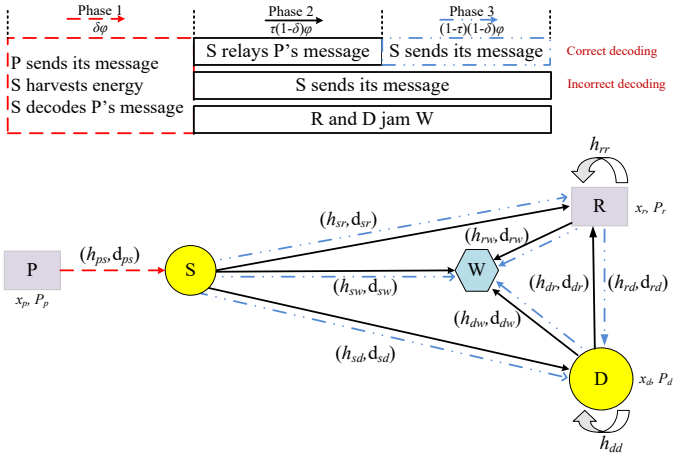


Fig. 1: System model.

denoted as φ. In Phase 1 of $\delta\varphi$, where $0 < \delta < 1$ indicates the time-split factor, P sends the symbol x_p with the transmission power P_p for S to collect energy with the power splitting protocol[1] and to restore the message of P. The power splitting protocol splits the signal received at S into two portions: one portion $\sqrt{\eta}y_s$, $0 < \eta < 1$, indicates the power-split factor and y_s is the signal received at S, for harvesting energy and another portion $\sqrt{1-\eta}y_s$ for restoring the message of P. Depending on the recovery status, S sends dissimilar signals in following phases. Specifically, when S restores the licensed message successfully, it relays it in Phase 2, i.e., it sends $\sqrt{\hat{P}_s}x_p$, and transmits its personal signal, namely $\sqrt{\check{P}_s}x_s$ in Phase 3. Here, x_s is the transmit symbol of S, whereas $\hat{P}_s$ and $\check{P}_s$ denote the transmission powers of S in Phase 2 and Phase 3.

In the scenario that the unlicensed sender fails to restore the licensed message, it instead broadcasts its personal signal $\sqrt{P_s}x_s$ where P_s is the transmission power of S in the last two phases. As illustrated in Fig. 1, R and D concurrently transmit the signals, $\sqrt{P_r}x_r$ and $\sqrt{P_d}x_d$, respectively, in both last phases to jam W, where P_r (or P_d) and x_r (or x_d) are the transmission power and the transmit symbol of R (or D), respectively. It is noted that R and D also suffer from SIs due to the FD operation, whilst three phases are required to avoid mutual interference between x_s and x_p.

C. Signal Model

Based on the considered set up, S receives $y_s = h_{ps}\sqrt{P_p}x_p + n_s$ in Phase 1, where $n_s \sim \mathcal{CN}(0, \epsilon_s)$ is the noise caused by the receive antenna at S. Thus, the harvested[2]

[1]RF EH can be implemented through either time switching (TS) or power splitting (PS) protocols [14]. On the one hand, TS is considered more energy-efficient, yet it achieves a lower throughput. On the other hand, PS appears to be more complicated in terms of implementation, yet it exhibits higher achievable throughput. Based on the latter characteristic, the considered set up is based on the adoption of the PS protocol [6]–[8], [10]–[12], [14].

[2]Similar to the vast majority of reported publications (e.g., [2], [5]–[9], [11], [12], [18]), the present analysis considers the linear energy harvesting model, which still represents the non-linear model over a large range of the input RF power [18]. Therefore, the non-linear energy harvesting model (e.g., [10], [13]–[15], [19]) may not add significant further insights; hence, we defer it to our future works where the achieved performance of the linear energy harvesting model can constitute a benchmark for extensive comparisons.

energy by S in Phase 1 is $E_s = \theta \mathsf{E}\left\{\left|\sqrt{\eta} y_s\right|^2\right\} \delta\varphi = \delta\theta\eta\left(P_p\alpha_{ps}+\epsilon_s\right)\varphi$, where $0 < \theta < 1$ is the energy harvesting efficiency. Therefore, the powers which S can consume in Phase 2, in Phase 3, and in both last phases are $\hat{P}_s = \frac{E_s}{\tau(1-\delta)\varphi} = \frac{\delta\theta\eta(P_p\alpha_{ps}+\epsilon_s)}{\tau(1-\delta)}$, $\check{P}_s = \frac{E_s}{(1-\tau)(1-\delta)\varphi} = \frac{\delta\theta\eta(P_p\alpha_{ps}+\epsilon_s)}{(1-\tau)(1-\delta)}$, and $P_s = \frac{E_s}{(1-\delta)\varphi} = \frac{\delta\theta\eta(P_p\alpha_{ps}+\epsilon_s)}{1-\delta}$, respectively. Also, the message decoder is based on $\check{y}_s = \sqrt{1-\eta} y_s + \check{n}_s$ to recover P's message, where $\check{n}_s \sim \mathcal{CN}\left(0, \check{\epsilon}_s\right)$ indicates the noise owing to down-converting the signal from the passband to the baseband. To this end, by invoking y_s in $\check{y}_s$, one achieves $\check{y}_s = \sqrt{(1-\eta)P_p} h_{ps} x_p + \sqrt{1-\eta} n_s + \check{n}_s$ which establishes the achievable Signal-to-Noise Ratio (SNR) for decoding P's information as $\gamma_s = A g_{ps}$ with $A = \frac{(1-\eta)P_p}{(1-\eta)\epsilon_s + \check{\epsilon}_s}$. Thus, S achieves the channel capacity $C_s = \delta \log_2(1+\gamma_s)$ bps/Hz, where δ is present because of $\delta\varphi$ in Phase 1. Also, S recovers successfully the licensed message only if C_s exceeds the target transmission rate R_T, i.e., $C_s \geq R_\mathsf{T}$.

If S decodes the message of P successfully, it then sends $\sqrt{\hat{P}_s} x_p$ in Phase 2 and $\sqrt{\check{P}_s} x_s$ in Phase 3. Otherwise, it transmits $\sqrt{P_s} x_s$ in both last phases. Furthermore, it is noted that R and D always broadcast $\sqrt{P_r} x_r$ and $\sqrt{P_d} x_d$ in Phase t, $t \in \{2,3\}$. Consequently, the signal received at $\mathtt{L} \in \{\mathtt{D}, \mathtt{W}, \mathtt{R}\}$ in Phase t is represented as

$$y_l^t = \begin{cases} h_{sl}\sqrt{P_t} x_t + h_{rl}\sqrt{P_r} x_r + h_{dl}\sqrt{P_d} x_d + n_l \ , C_s \geq R_\mathsf{T} \\ h_{sl}\sqrt{P_s} x_s + h_{rl}\sqrt{P_r} x_r + h_{dl}\sqrt{P_d} x_d + n_l \ , C_s < R_\mathsf{T} \end{cases} \tag{1}$$

where $P_2 = \hat{P}_s$, $P_3 = \check{P}_s$, $x_2 = x_p$, $x_3 = x_s$, and $n_l \sim \mathcal{CN}(0, \epsilon_l)$ indicates the noise due to the receive antenna at L.

Usually, the jamming signals, x_r and x_d, are purposely generated by R and D to impair the wire-tapping of W without intercepting each other. For example, x_r and x_d are pseudo-random signals [10] and the jamming signal generator at R encrypts its seed with a short secret key and shares it with D and vice versa. Consequently, most reported analyses (e.g., [6]–[11]) assumed that x_r and x_d were totally eliminated at D and R, respectively. Nevertheless, this assumption seems ideal because any regeneration of x_r and x_d is hardly achieved with absolute probability. Therefore, the analysis in the present paper assumes them regenerated at D and R with accuracy of $1-\kappa$, $0 \leq \kappa \leq 1$, which indicates that κx_d and κx_r represent the residual jamming signals due to imperfect jamming cancellation at R and D, respectively. Accordingly, $\mathtt{K} \in \{\mathtt{R}, \mathtt{D}\}$ in Phase t obtains the signal with lower jamming after partly removing the corresponding jamming signal as

$$\check{y}_k^t = \begin{cases} h_{sk}\sqrt{P_t} x_t + h_{kk}\sqrt{P_k} x_k + \kappa h_{jk}\sqrt{P_j} x_j + n_k, C_s \geq R_\mathsf{T} \\ h_{sk}\sqrt{P_s} x_s + h_{kk}\sqrt{P_k} x_k + \kappa h_{jk}\sqrt{P_j} x_j + n_k, C_s < R_\mathsf{T} \end{cases} \tag{2}$$

where $(k,j) = \{(r,d),(d,r)\}$. As a result, the achievable channel capacities for D and R for recovering x_s and x_p are given by

$$C_d = \begin{cases} (1-\tau)(1-\delta)\log_2\left(1+\frac{\check{P}_s g_{sd}}{U+\epsilon_d}\right) & , C_s \geq R_\mathsf{T} \\ (1-\delta)\log_2\left(1+\frac{P_s g_{sd}}{U+\epsilon_d}\right) & , C_s < R_\mathsf{T} \end{cases} \tag{3}$$

and

$$C_r = \begin{cases} \tau(1-\delta)\log_2\left(1+\frac{\hat{P}_s g_{sr}}{Q+\epsilon_r}\right) & , C_s \geq R_\mathsf{T} \\ 0 & , C_s < R_\mathsf{T} \end{cases} \tag{4}$$

where $(\tau(1-\delta)$, $(1-\tau)(1-\delta)$, $1-\delta)$ denote the durations of Phase 2, Phase 3, and both last phases, respectively; $Q = P_r g_{rr} + \kappa^2 P_d g_{dr}$ and $U = P_d g_{dd} + \kappa^2 P_r g_{rd}$.

The knowledge of the jamming signals, x_r and x_d, is merely shared between D and R for protecting x_p and x_s, whilst W is unknown with respect to (w.r.t) it. Thus, the channel capacities attained by W for restoring x_p and x_s follow from (1), yielding

$$C_w^p = \begin{cases} \tau(1-\delta)\log_2\left(1+\frac{\hat{P}_s g_{sw}}{W+\epsilon_w}\right) & , C_s \geq R_\mathsf{T} \\ 0 & , C_s < R_\mathsf{T} \end{cases} \tag{5}$$

and

$$C_w^s = \begin{cases} (1-\tau)(1-\delta)\log_2\left(1+\frac{\check{P}_s g_{sw}}{W+\epsilon_w}\right) & , C_s \geq R_\mathsf{T} \\ (1-\delta)\log_2\left(1+\frac{P_s g_{sw}}{W+\epsilon_w}\right) & , C_s < R_\mathsf{T} \end{cases} \tag{6}$$

where $W = P_r g_{rw} + P_d g_{dw}$. It is evident that R and D purposely produce the amount of jamming power W to corrupt the wire-tapper. Therefore, enlarging W can enhance the overall security performance of both unlicensed and licensed communications. Furthermore, it is noted that the secrecy capacity for restoring x_s represents the subtraction of the capacity at W from that at D, namely $\check{C}_s = [C_d - C_w^s]^+$, where $[z]^+ = \max(z, 0)$. Likewise, the secrecy capacity for decoding x_p indicates the subtraction of the capacity at W from that at R, namely $\check{C}_p = [C_r - C_w^p]^+$.

III. Security Analysis

One of the key indicators to evaluate the security of EHOC-NwFD is the achievable SOP, which quantifies the probability of the secrecy capacity subceeding the target security degree C_T. In the sequel, we derive exact closed-form SOP formulas to straightforwardly determine the achievable security levels for both unlicensed and licensed communications.

A. Licensed SOP

The licensed SOP is defined as $\Phi_p = \Pr\{\check{C}_p < C_\mathsf{T}$ which is decomposed into two cases, depending on whether S decodes successfully the message of P or not, namely

$$\begin{aligned} \Phi_p &= \Pr\{\check{C}_p < C_\mathsf{T} \,|\, C_s \geq R_\mathsf{T}\} \ \Pr\{C_s \geq R_\mathsf{T}\} \\ &\quad + \Pr\{\check{C}_p < C_\mathsf{T} \,|\, C_s < R_\mathsf{T}\} \ \Pr\{C_s < R_\mathsf{T}\} \\ &= \Lambda\Xi + \chi(1-\Xi). \end{aligned} \tag{7}$$

Based on the form of (7), it readily follows that

$$\begin{aligned} \Xi &= \Pr\{\delta\log_2(1+A g_{ps}) \geq R_\mathsf{T}\} = 1 - F_{g_{ps}}\left(\left[2^{R_\mathsf{T}/\delta}-1\right]/A\right) \\ &= \sum_{l=0}^{\infty}\sum_{n=0}^{l} \frac{K^l\left([1+K]\left[2^{R_\mathsf{T}/\delta}-1\right]/[\alpha_{ps}A]\right)^n}{e^{(1+K)\left(2^{R_\mathsf{T}/\delta}-1\right)/(\alpha_{ps}A)+K} l!n!} \end{aligned} \tag{8}$$

where $F_{g_{ps}}(x)$ is the CDF of the P $\rightarrow$ S Rician fading channel gain, which is given in [20, eq. (9)]. Also, K is the Rician factor. As noted in [20], the infinite summation in (8) quickly converges to the finite one.

Using (4) and (5) for the case $C_s < R_\mathsf{T}$, it follows that

$$\chi = \Pr\{0 < C_\mathsf{T}\} = 1 \tag{9}$$

because the target security degree C_T is non-negative. Similarly, using (4) and (5) for the case $C_s \geq R_\mathsf{T}$ yields

$$\Lambda = \Pr\left\{\tau\,(1-\delta)\log_2\frac{X}{Y} < C_\mathsf{T}\right\} = \int_1^\infty F_X(By) f_Y(y)\,dy, \tag{10}$$

where $X = 1 + \frac{\hat{P}_s g_{sr}}{Q+\epsilon_r}$, $Y = 1 + \frac{\hat{P}_s g_{sw}}{W+\epsilon_w}$, $B = 2^{C_\mathsf{T}/\tau(1-\delta)}$.

Evidently, (10) can be derived with the aid of the CDF of X and the PDF of Y. Because X and Y share the same form, we can start with deriving the PDF of Y. It is also noted that Y depends on W and hence, we first derive the PDF of W. By recalling that W is a sum of two independent random variables, its PDF is given by

$$\begin{aligned} f_W(z) &= \int_0^z f_{P_r g_{rw}}(x)\, f_{P_d g_{dw}}(z-x)\,dx \\ &= \int_0^z \frac{e^{-\frac{x}{P_r\alpha_{rw}}}}{P_r\alpha_{rw}} \frac{e^{-\frac{z-x}{P_d\alpha_{dw}}}}{P_d\alpha_{dw}} dx \end{aligned} \tag{11}$$

which can be represented in closed-form as follows:

$$f_W(z) = \begin{cases} \frac{z e^{-\frac{z}{P_d\alpha_{dw}}}}{P_r P_d \alpha_{rw}\alpha_{dw}} & , P_d\alpha_{dw} = P_r\alpha_{rw} \\ \frac{e^{-\frac{z}{P_r\alpha_{rw}}} - e^{-\frac{z}{P_d\alpha_{dw}}}}{P_r\alpha_{rw} - P_d\alpha_{dw}} & , P_d\alpha_{dw} \neq P_r\alpha_{rw} \end{cases}, z \geq 0. \tag{12}$$

To this effect, the CDF of Y can be inferred as

$$\begin{aligned} F_Y(y) &= \mathsf{E}_W\left\{\Pr\left\{1 + \frac{\hat{P}_s g_{sw}}{W+\epsilon_w} < y \middle| W\right\}\right\} \\ &= \mathsf{E}_W\left\{1 - e^{-\frac{(y-1)(W+\epsilon_w)}{\hat{P}_s\alpha_{sw}}}\right\},\ y \geq 1 \end{aligned} \tag{13}$$

whilst invoking (12) in (13), it follows that

$$\begin{aligned} F_Y(y) &= 1 - \int_0^\infty e^{-\frac{(y-1)(z+\epsilon_w)}{\hat{P}_s\alpha_{sw}}} f_W(z)\,dz \\ &= \begin{cases} 1 - \frac{q^2 e^{-\frac{(y-1)\epsilon_w}{\hat{P}_s\alpha_{sw}}}}{P_r P_d \alpha_{rw}\alpha_{dw}} & , P_d\alpha_{dw} = P_r\alpha_{rw} \\ 1 - \frac{(m-q) e^{-\frac{(y-1)\epsilon_w}{\hat{P}_s\alpha_{sw}}}}{P_r\alpha_{rw} - P_d\alpha_{dw}} & , P_d\alpha_{dw} \neq P_r\alpha_{rw} \end{cases}, y \geq 1 \end{aligned} \tag{14}$$

where $\{{}^q_m\} = \left(\frac{y-1}{\hat{P}_s\alpha_{sw}} + \frac{1}{\{{}^{P_d\alpha_{dw}}_{P_r\alpha_{rw}}\}}\right)^{-1}$.

Based on the above, the PDF of Y can be readily deduced by taking the first derivative of $F_Y(y)$ w.r.t y, yielding

$$f_Y(y) = \begin{cases} R e^{-\frac{(y-1)\epsilon_w}{\hat{P}_s\alpha_{sw}}} q^2(\epsilon_w + 2q) & , P_d\alpha_{dw} = P_r\alpha_{rw} \\ J e^{-\frac{(y-1)\epsilon_w}{\hat{P}_s\alpha_{sw}}}\left[\epsilon_w(m-q) + m^2 - q^2\right] & , P_d\alpha_{dw} \neq P_r\alpha_{rw} \end{cases} \tag{15}$$

which is valid for $y \geq 1$, while $R = \left(P_r P_d \hat{P}_s \alpha_{rw}\alpha_{dw}\alpha_{sw}\right)^{-1}$ and $J = \left[\left(P_r\alpha_{rw} - P_d\alpha_{dw}\right)\hat{P}_s\alpha_{sw}\right]^{-1}$.

Likewise, the corresponding CDF of X is computed similarly to (14), yielding

$$F_X(x) = \begin{cases} 1 - \frac{b^2 e^{-\frac{(x-1)\epsilon_r}{\hat{P}_s\alpha_{sr}}}}{P_r P_d \alpha_{rr}\kappa^2\alpha_{dr}} & , P_d\kappa^2\alpha_{dr} = P_r\alpha_{rr} \\ 1 - \frac{(c-b) e^{-\frac{(x-1)\epsilon_r}{\hat{P}_s\alpha_{sr}}}}{P_r\alpha_{rr} - P_d\kappa^2\alpha_{dr}} & , P_d\kappa^2\alpha_{dr} \neq P_r\alpha_{rr} \end{cases}, x \geq 1 \tag{16}$$

where $\{{}^b_c\} = \left(\frac{x-1}{\hat{P}_s\alpha_{sr}} + \frac{1}{\{{}^{P_d\kappa^2\alpha_{dr}}_{P_r\alpha_{rr}}\}}\right)^{-1}$.

To this effect, substituting (15) and (16) in (10) and since $B^{-1} < 1$ and $F_X(x) = 0$ for $x < 1$, yields

$$\Lambda = \begin{cases} 1 - \mathcal{A}_1 & , P_d\kappa^2\alpha_{dr} = P_r\alpha_{rr}\ \&\ P_d\alpha_{dw} = P_r\alpha_{rw} \\ 1 - \mathcal{A}_2 & , P_d\kappa^2\alpha_{dr} = P_r\alpha_{rr}\ \&\ P_d\alpha_{dw} \neq P_r\alpha_{rw} \\ 1 - \mathcal{A}_3 & , P_d\kappa^2\alpha_{dr} \neq P_r\alpha_{rr}\ \&\ P_d\alpha_{dw} = P_r\alpha_{rw} \\ 1 - \mathcal{A}_4 & , P_d\kappa^2\alpha_{dr} \neq P_r\alpha_{rr}\ \&\ P_d\alpha_{dw} \neq P_r\alpha_{rw} \end{cases} \tag{17}$$

where

$$\mathcal{A}_1 = \tilde{A}\left[\epsilon_w \mathcal{G}(L, M, 2, 2) + 2\hat{P}_s\alpha_{sw}\mathcal{G}(L, M, 2, 3)\right], \tag{18}$$

$$\begin{aligned} \mathcal{A}_2 = \breve{A}\,(\epsilon_w\,[\mathcal{G}(N, L, 1, 2) - \mathcal{G}(M, L, 1, 2)] + \\ \hat{P}_s\alpha_{sw}\,[\mathcal{G}(L, N, 2, 2) - \mathcal{G}(L, M, 2, 2)]\Big), \end{aligned} \tag{19}$$

$$\begin{aligned} \mathcal{A}_3 = \bar{A}\,[\epsilon_w\,\{\mathcal{G}(H, M, 1, 2) - \mathcal{G}(I, M, 1, 2)\} \\ + 2\hat{P}_s\alpha_{sw}\,\{\mathcal{G}(H, M, 1, 3) - \mathcal{G}(I, M, 1, 3)\}\Big], \end{aligned} \tag{20}$$

$$\begin{aligned} \mathcal{A}_4 = \widehat{A}\,\{\epsilon_w\,[\mathcal{G}(H, N, 1, 1) - \mathcal{G}(I, N, 1, 1) \\ -\mathcal{G}(H, M, 1, 1) + \mathcal{G}(I, M, 1, 1)] \\ + \hat{P}_s\alpha_{sw}\,[\mathcal{G}(H, N, 1, 2) - \mathcal{G}(H, M, 1, 2) \\ -\ \mathcal{G}(I, N, 1, 2) + \mathcal{G}(I, M, 1, 2)]\}, \end{aligned} \tag{21}$$

with $\tilde{A} = \frac{\hat{P}_s^4 R}{P_r P_d \alpha_{rr}\alpha_{dr}}\left(\frac{\alpha_{sr}\alpha_{sw}}{\kappa B}\right)^2 \exp\!\left(-\frac{(B-1)\epsilon_r}{\hat{P}_s\alpha_{sr}}\right)$, $L = 1 + \frac{\hat{P}_s\alpha_{sr}}{P_d\kappa^2\alpha_{dr}B} - \frac{1}{B}$, $M = \frac{\hat{P}_s\alpha_{sw}}{P_d\alpha_{dw}}$, $\breve{A} = \frac{\hat{P}_s^3\alpha_{sw}J}{P_r P_d\alpha_{rr}\alpha_{dr}}\left(\frac{\alpha_{sr}}{\kappa B}\right)^2 \exp\!\left(-\frac{(B-1)\epsilon_r}{\hat{P}_s\alpha_{sr}}\right)$, $N = \frac{\hat{P}_s\alpha_{sw}}{P_r\alpha_{rw}}$, $\bar{A} = \frac{\hat{P}_s^3\alpha_{sr}\alpha_{sw}^2 R}{(P_r\alpha_{rr} - P_d\kappa^2\alpha_{dr})B}\exp\!\left(-\frac{(B-1)\epsilon_r}{\hat{P}_s\alpha_{sr}}\right)$, $\widehat{A} = \frac{\hat{P}_s^2\alpha_{sw}\alpha_{sr}J}{(P_r\alpha_{rr} - P_d\kappa^2\alpha_{dr})B}\exp\!\left(-\frac{(B-1)\epsilon_r}{\hat{P}_s\alpha_{sr}}\right)$, $H = 1 + \frac{\hat{P}_s\alpha_{sr}}{P_r\alpha_{rr}B} - \frac{1}{B}$, $I = 1 + \frac{\hat{P}_s\alpha_{sr}}{P_d\kappa^2\alpha_{dr}B} - \frac{1}{B}$, $G = \frac{B\epsilon_r}{\alpha_{sr}\hat{P}_s} + \frac{\epsilon_w}{\alpha_{sw}\hat{P}_s}$, $\mathcal{G}(a, b, u, v) = \int_0^\infty \frac{e^{-Gx}}{(x+a)^u(x+b)^v}dx$.

It is apparent that deriving a closed-form formula for (17) needs the analytical evaluation of the integral in $\mathcal{G}$. To this end, we first let $\mathcal{Q}(a, b) = \int_0^\infty \frac{e^{-Gy}}{(y+a)^b}dy$, which is expressed in closed-form as $\mathcal{Q}(a, b) = \frac{(-G)^{b-1}}{(b-1)!}\left[\sum_{k=1}^{b-1}\frac{(k-1)!}{(-aG)^k} - e^{aG}\mathrm{Ei}(-aG)\right]$ upon invoking [21, eq. (3.353.2)], with $\mathrm{Ei}(\cdot)$ denoting the exponential integral. Based on this and upon performing the partial fraction decomposition, the integral in $\mathcal{G}$ is represented as $\mathcal{G}(a, b, u, v) = \sum_{g=1}^{u}\mathcal{U}_g\mathcal{Q}(a, u-g+1) + \sum_{j=1}^{v}\mathcal{T}_j\mathcal{Q}(b, v-j+1)$ where $\mathcal{U}_g = \frac{(-1)^{g-1}\prod_{n=0}^{g-2}(v+n)}{(b-a)^{v+g-1}\prod_{n=1}^{g-1}n!}$ and $\mathcal{T}_j = \frac{(-1)^{j-1}\prod_{n=0}^{j-2}(v+n)}{(a-b)^{u+j-1}\prod_{n=1}^{j-1}n!}$. Therefore, substituting Λ in (17), Ξ in (8), and χ in (9) into (7), one obtains the exact closed-form formula of Φ_p.

B. Unlicensed SOP

Similar to Subsection III-A, the unlicensed SOP can be decomposed as

$$\begin{aligned} \Phi_s &= \Pr\{\check{C}_s < C_\mathsf{T} | C_s \geq R_\mathsf{T}\}\ \Pr\{C_s \geq R_\mathsf{T}\} \\ &\quad + \Pr\{\check{C}_s < C_\mathsf{T} | C_s < R_\mathsf{T}\}\ \Pr\{C_s < R_\mathsf{T}\} \\ &= \Upsilon\Xi + \Omega(1-\Xi). \end{aligned} \tag{22}$$

Substituting (3) and (6) when $C_s \geq R_{\mathsf{T}}$ into $\check{C}_s$ and then inserting $\check{C}_s$ into (22), Υ can be re-written explicitly as

$$\Upsilon = \Pr\left\{ (1-\tau)(1-\delta)\log_2 \frac{1+\frac{\check{P}_s g_{sd}}{U+\epsilon_d}}{1+\frac{\check{P}_s g_{sw}}{W+\epsilon_w}} < C_{\mathsf{T}} \right\}. \quad (23)$$

By comparing (23) with (10), it becomes evident that (23) can be derived from (10) with the appropriate variable transformation: $\Upsilon = \Lambda_{\tau\to 1-\tau,\hat{P}_s\to\check{P}_s,\alpha_{sr}\to\alpha_{sd},P_r\alpha_{rr}\to P_d\alpha_{dd},P_d\alpha_{dr}\to P_r\alpha_{rd},\epsilon_r\to\epsilon_d}$.

Similarly, substituting (3) and (6) for the scenario $C_s < R_{\mathsf{T}}$ into $\check{C}_s$ and then inserting $\check{C}_s$ into (22), it readily follows that

$$\Omega = \Pr\left\{ (1-\delta)\log_2 \frac{1+\frac{P_s g_{sd}}{U+\epsilon_d}}{1+\frac{P_s g_{sw}}{W+\epsilon_w}} < C_{\mathsf{T}} \right\}. \quad (24)$$

Again, comparing (24) with (10) renders evident that (24) can be derived from (10) with the appropriate change of variables: $\Omega = \Lambda_{\tau\to 1,\hat{P}_s\to P_s,\alpha_{sr}\to\alpha_{sd},P_r\alpha_{rr}\to P_d\alpha_{dd},P_d\alpha_{dr}\to P_r\alpha_{rd},\epsilon_r\to\epsilon_d}$.

Hence, plugging the derived closed-form formulas for Ξ, Υ, and Ω into (22), yields a closed-form expression for Φ_s.

To the best of the authors' knowledge, the proposed results have not been reported in the open technical literature. It is also noted that the derived expressions for Φ_s and Φ_p are useful for rapidly evaluating the security capability of both unlicensed and licensed communications in EHOCNwFD and in developing useful insights on the impact of the involved specifications on the overall system behavior and performance.

C. Asymptotic Analysis

Letting $P_r = \psi P_p$ and $P_d = \zeta P_p$, the asymptotic analysis is carried out at high transmission power, i.e. $P_p \to \infty$. When $P_p \to \infty$, S correctly decodes P's message. Therefore, the licensed SOP reduces to $\tilde{\Lambda}$ in (17) where $\tilde{X}$ represents $\lim_{P_p\to\infty} X$; $\tilde{\mathcal{A}}_1 = \frac{\alpha_{sw}}{\alpha_{dw}}\frac{\alpha_{sr}}{\alpha_{dr}}\frac{\alpha_{sr}}{\alpha_{rr}}\frac{\alpha_{sw}}{\alpha_{rw}}\left(\frac{\omega^2\sqrt{2}}{\psi\zeta\kappa B}\right)^2\mathcal{K}$, $\mathcal{K} = \frac{1}{(\tilde{M}-\tilde{L})^3}\left(\frac{1}{\tilde{L}} + \frac{\tilde{M}-\tilde{L}}{2\tilde{M}^2} + \frac{2}{\tilde{M}} - \frac{3\ln(\tilde{M}/\tilde{L})}{\tilde{M}-\tilde{L}}\right)$, $\tilde{M} = \frac{\omega\alpha_{sw}}{\zeta\alpha_{dw}}$, $\tilde{L} = 1 + \frac{\omega\alpha_{sr}}{\zeta\kappa^2\alpha_{dr}B} - \frac{1}{B}$, $\omega = \frac{\delta\theta\eta\alpha_{ps}}{\tau(1-\delta)}$; $\tilde{\mathcal{A}}_2 = \frac{\alpha_{sr}}{\alpha_{dr}}\frac{\alpha_{sr}}{\alpha_{rr}}\frac{\omega^3[\mathcal{W}(\tilde{N})-\mathcal{W}(\tilde{M})]}{\psi\zeta(\kappa B)^2\left(\psi\frac{\alpha_{rw}}{\alpha_{sw}}-\zeta\frac{\alpha_{dw}}{\alpha_{sw}}\right)}$, $\mathcal{W}(a) = \frac{\tilde{L}^{-1}+a^{-1}}{(a-\tilde{L})^2} - \frac{2\ln(a/\tilde{L})}{(a-\tilde{L})^3}$, $\tilde{N} = \frac{\omega\alpha_{sw}}{\psi\alpha_{rw}}$; $\tilde{\mathcal{A}}_3 = \frac{\alpha_{sw}}{\alpha_{dw}}\frac{\alpha_{sr}}{\alpha_{rw}}\frac{2\omega^3[\mathcal{H}(\tilde{H})-\mathcal{H}(\tilde{I})]}{\left(\psi\frac{\alpha_{rr}}{\alpha_{sw}}-\zeta\kappa^2\frac{\alpha_{dr}}{\alpha_{sw}}\right)B\psi\zeta}$, $\mathcal{H}(a) = \frac{1}{(a-\tilde{M})^2}\left(\frac{a-\tilde{M}}{2\tilde{M}^2} - \frac{\ln(\tilde{M}/a)}{a-\tilde{M}} - \frac{1}{\tilde{M}}\right)$, $\tilde{H} = 1 + \frac{\omega\alpha_{sr}}{\psi\alpha_{rr}B} - \frac{1}{B}$, $\tilde{I} = 1 + \frac{\omega\alpha_{sr}}{\zeta\kappa^2\alpha_{dr}B} - \frac{1}{B}$; $\tilde{\mathcal{A}}_4 = \frac{\mathcal{L}(\tilde{H},\tilde{N})-\mathcal{L}(\tilde{H},\tilde{M})-\mathcal{L}(\tilde{I},\tilde{N})+\mathcal{L}(\tilde{I},\tilde{M})}{\omega^{-2}\left(\psi\frac{\alpha_{rr}}{\alpha_{sr}}-\zeta\kappa^2\frac{\alpha_{dr}}{\alpha_{sr}}\right)B\left(\psi\frac{\alpha_{rw}}{\alpha_{sw}}-\zeta\frac{\alpha_{dw}}{\alpha_{sw}}\right)}$, $\mathcal{L}(a,b) = \frac{1}{(a-b)b} - \frac{\ln(a/b)}{(a-b)^2}$. In order to obtain $\tilde{\Lambda}$, we assume: i) $\hat{P}_s \to \omega P_p$; ii) $e^{-Gx} \to 1$ in $\mathcal{G}(a,b)$; iii) $\exp\left(-\frac{(B-1)\epsilon_r}{\hat{P}_s\alpha_{sr}}\right) \to 1$ in $\tilde{A}, \breve{A}, \bar{A}, \widehat{A}$; iv) $\tilde{A}, \breve{A}, \bar{A}, \widehat{A}$ are inversely proportional to P_p; v) $\mathcal{A}_i \to \tilde{\mathcal{A}}_i$ by keeping terms weighted by $\hat{P}_s$, $i \in [1,4]$. Similarly, the unlicensed SOP reduces to $\tilde{\Upsilon} = \tilde{\Lambda}_{\tau\to 1-\tau,\omega\to\omega_3,\alpha_{sr}\to\alpha_{sd},\psi\alpha_{rr}\to\zeta\alpha_{dd},\zeta\alpha_{dr}\to\psi\alpha_{rd},\epsilon_r\to\epsilon_d}$ where $\omega_3 = \frac{\delta\theta\eta\alpha_{ps}}{(1-\tau)(1-\delta)}$. Interestingly, by observing $\tilde{\mathcal{A}}_i$, we find that the licensed SOP $\tilde{\Lambda}$ (or the unlicensed SOP $\tilde{\Upsilon}$) is a function of fading power ratios of channels towards the same receiver, namely $\frac{\alpha_{sw}}{\alpha_{dw}}$, $\frac{\alpha_{sw}}{\alpha_{rw}}$, $\frac{\alpha_{sr}}{\alpha_{dr}}$, $\frac{\alpha_{sr}}{\alpha_{rr}}$ (or $\frac{\alpha_{sd}}{\alpha_{dd}}$, $\frac{\alpha_{sd}}{\alpha_{rd}}$).

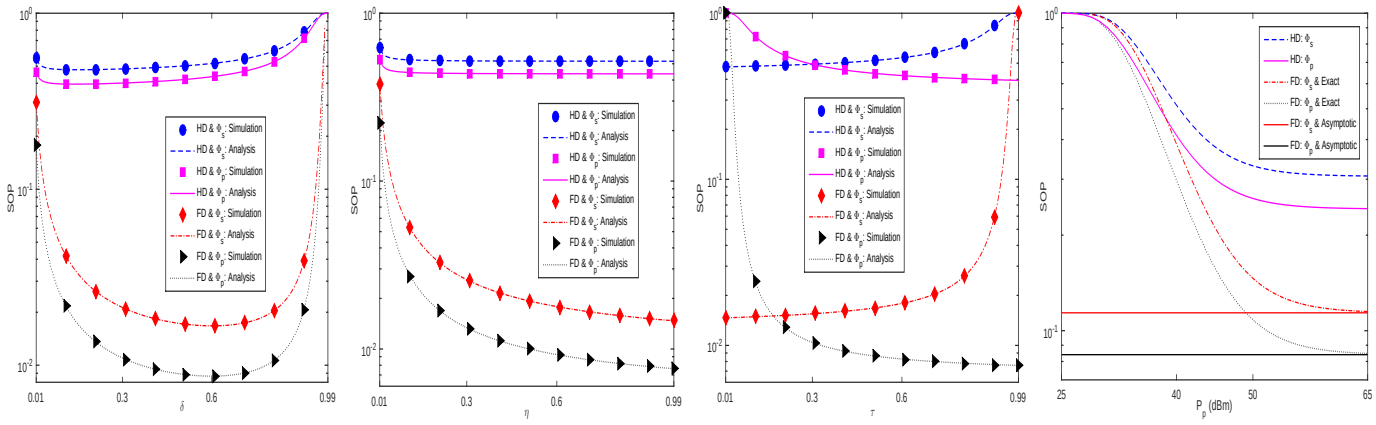
IV. Numerical Results

This section capitalizes on the derived analytic expressions along with results from respective computer simulations to quantify the achievable SOPs of both unlicensed and licensed communications for practical scenarios. All users are assumed to be placed on a two-dimensional plane and hence, the distance between user A at $(x_{\mathtt{A}}, y_{\mathtt{A}})$ and user B at $(x_{\mathtt{B}}, y_{\mathtt{B}})$ is $\mathrm{d}_{\mathtt{AB}} = \sqrt{(x_{\mathtt{A}}-x_{\mathtt{B}})^2 + (y_{\mathtt{A}}-y_{\mathtt{B}})^2}$. Without loss of generality and unless otherwise stated, the following indicative fixed values are assumed as [4], [15]: $\theta = 0.7$, $\beta = 2.6$, $\varsigma_0 = -20$ dB, $\epsilon_d = \epsilon_w = \epsilon_r = \epsilon_s = \check{\epsilon}_s = -70$ dBm, $P_p = 60$ dBm, $P_r = 10$ dBm, $P_d = 5$ dBm, P at $(-10, 0)$ m, S at $(0, 0)$ m, D at $(50, -20)$ m, W at $(60, 0)$ m, R at $(45, 15)$ m, $C_{\mathsf{T}} = 0.1$ bps/Hz, $R_{\mathsf{T}} = 0.1$ bps/Hz, $\alpha_{rr} = \alpha_{dd} = -90$ dB, $\kappa = 0.1$, $K = 2$, $\delta = 0.6$, $\tau = 0.5$, $\eta = 0.7$. To highlight the achievable security improvement of the proposed jamming method, EHOCN with HD destinations, namely EHOCNwHD, is compared with EHOCNwFD. This is straightforwardly realized by setting $P_r = P_d = 0$ in (7) and (22).

Based on the above, Fig. 2 exhibits a perfect match between analytical and simulation results, which corroborates the validity of the proposed analytic formulas in (7) and (22). Moreover, it is clearly observed that EHOCNwFD outperforms EHOCNwHD, proving the achieved security enhancement of the jamming method. In the same context, Fig. 2a demonstrates that the best secrecy performance of both unlicensed and licensed communications in EHOCNwFD occurs at particular values of δ. The optimal values of δ that generate the minimum SOPs are explained as follows: enlarging δ increases energy scavenged at S in Phase 1 and offers higher probability for S to correctly restore the message of P, enhancing the security performance of both unlicensed and licensed communications. Nevertheless, increasing δ decreases the transmission time of the last two phases, which deteriorates unlicensed and licensed secrecy capacities, and ultimately increases the corresponding SOPs. As such, the optimum values of δ exist to trade-off benefits in Phase 1 and in the last two phases.

Fig. 2b demonstrates the achievable SOPs w.r.t η. This figure shows that the achievable security performance of EHOCNwFD is improved as η increases. This stems from the fact that enlarging δ supports S in harvesting more energy in licensed signals, which in turn ultimately decreases Φ_p and Φ_s. Likewise, Fig. 2c illustrates the SOPs w.r.t τ, which reveals that enlarging τ enhances the security capability of the licensed communications and degrades that of the unlicensed communications in EHOCNwFD. This is interpreted from the fact that enlarging τ lingers Phase 2 but decreases Phase 3 for the unlicensed sender to relay the licensed message and then send its own information. As a result, Φ_p reduces while, in turn, Φ_s increases. The opposite performance tendencies of the licensed and unlicensed networks represent the security trade-off between them and hence, their security can be equalized. For example, Fig. 2c illustrates $\Phi_s = \Phi_p$ at $\tau = 0.17$.

Finally, Fig. 2d illustrates the SOPs w.r.t P_p. This figure considers $P_r = P_d = 0.001P_p$ to verify the corresponding asymptotic analysis. Additionally, the SOPs are averaged over 1000 positions of W where $x_{\mathtt{W}}$ and $y_{\mathtt{W}}$ are uniformly distributed



(a) SOPs w.r.t δ (b) SOPs w.r.t η (c) SOPs w.r.t τ (d) SOPs w.r.t P_p

Fig. 2: Impact of adjusting the individual parameters.

in $[50, 70]$ m and $[-10, 10]$ m, respectively, with $(x_{\mathtt{W}}, y_{\mathtt{W}})$ being the coordinate of $\mathtt{W}$. This figure demonstrates the considerable security enhancement of EHOCNwFD when increasing P_p. This occurs because enlarging P_p supports $\mathtt{S}$ in harvesting more energy in the licensed signal as well as aids $\mathtt{S}$ to exactly restore the message of $\mathtt{P}$ with a greater probability. This increases the channel capacities at the corresponding receivers in Phase 2 and Phase 3, which ultimately reduces the involved SOPs. Also, the asymptotic analysis matches the exact results at large P_p, validating the analysis in Subsection III-C. These results justify the usefulness of the proposed setup.

V. Conclusions

This work proposed EHOCNwFD for improved energy efficiency and message security. In this context, we analyzed its licensed/unlicensed SOPs to quantify the achievable security and to develop useful insights on the effect of the involved specifications on the overall system performance. Respective computer simulations also validated the proposed analysis. Moreover, various versatile results showed the superiority of EHOCNwFD to EHOCNwHD, the security trade-off between licensed and unlicensed communications, and the best security performance with appropriate selections of specifications. The offered results are expected to be useful in the design and deployment of future cognitive radio systems and networks.

References

[1] D. H. Tashman *et al.*, "An Overview and Future Directions on Physical-Layer Security for Cognitive Radio Networks," *IEEE Network*, vol. 35, no. 3, pp. 205-211, May/June 2021.

[2] X. Li *et al.*, "Cooperative Wireless-Powered NOMA Relaying for B5G IoT Networks With Hardware Impairments and Channel Estimation Errors," *IEEE IoT Journal*, vol. 8, no. 7, pp. 5453-5467, Apr. 2021.

[3] X. Chen *et al.*, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, pp. 1027-1053, Secondquarter 2017.

[4] X. Chen *et al.*, "Multi-Antenna Covert Communication via Full-Duplex Jamming Against a Warden With Uncertain Locations," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 5467-5480, Aug. 2021.

[5] K. Ho-Van *et al.*, "Relay Selection for Security Improvement in Cognitive Radio Networks with Energy Harvesting," *Wireless Commun. and Mobile Comp.*, Volume 2021, Article ID 9921782, pp. 1-16.

[6] R. Su *et al.*, "Secure Cooperative Transmission in Cognitive AF Relay Systems with Destination-Aided Jamming and Energy Harvesting," in *Proc. IEEE PIMRC*, Turkey, 2019, pp. 1-5.

[7] R. Su *et al.*, "Destination-Assisted Jamming for Physical-Layer Security in SWIPT Cognitive Radio Systems," in *Proc. IEEE WCNC*, Spain, 2018, pp. 1-6.

[8] K. Ho-Van *et al.*, "Overlay Networks with Jamming and Energy Harvesting: Security Analysis," *Ara. J. for Sci. and Eng.*, doi: 10.1007/s13369-021-05492-z.

[9] D. Wang *et al.*, "Primary Privacy Preserving with Joint Wireless Power and Information Transfer for Cognitive Radio Networks," *IEEE Trans. Cogn. Commun. and Netw.*, vol. 6, no. 2, pp. 683-693, Jun. 2020.

[10] F. Wang *et al.*, "Secure Resource Allocation for Polarization-Based Non-Linear Energy Harvesting Over 5G Cooperative CRNs," *IEEE Wireless Commun. Lett.*, doi: 10.1109/LWC.2020.3028585.

[11] M. Xu *et al.*, "Secure Transmission Solutions in Energy Harvesting Enabled Cooperative Cognitive Radio Networks," in *Proc. IEEE WCNC*, Spain, 2018, pp. 1-6.

[12] M. Li *et al.*, "Physical Layer Security in Overlay Cognitive Radio Networks With Energy Harvesting," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11274-11279, Sep. 2018.

[13] Q. N. Le *et al.*, "Full-Duplex Non-Orthogonal Multiple Access Cooperative Overlay Spectrum-Sharing Networks with SWIPT," *IEEE Green Commun. and Netw.*, vol. 5, no. 1, pp. 322-334, Mar. 2021.

[14] K. Agrawal *et al.*, "NOMA With Battery-Assisted Energy Harvesting Full-Duplex Relay," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13952-13957, Nov. 2020.

[15] A. Hakimi *et al.*, "Full-Duplex Non-Orthogonal Multiple Access Cooperative Spectrum-Sharing Networks with Non-linear Energy Harvesting," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 10925-10936, Oct. 2020.

[16] B. Chen *et al.*, "Secure Primary Transmission Assisted by a Secondary Full-Duplex NOMA Relay," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7214-7219, Jul. 2019.

[17] M. Li *et al.*, "Improving the Security and Spectrum Efficiency in Overlay Cognitive Full-Duplex Wireless Networks," *IEEE Access*, vol. 7, pp. 68359-68372, May 2019.

[18] M. Zhang *et al.*, "Energy Efficiency Optimization for Secure Transmission in MISO Cognitive Radio Network With Energy Harvesting," *IEEE Access*, vol. 7, pp. 126234-126252, Sep. 2019.

[19] E. Boshkovska *et al.*, "Practical Non-Linear Energy Harvesting Model and Resource Allocation for SWIPT Systems," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2082-2085, Dec. 2015.

[20] T. Li *et al.*, "Secure UAV-to-Vehicle Communications," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5381-5393, Aug. 2021.

[21] I. S. Gradshteyn *et al.*, *Table of Integrals, Series and Products*, 7th ed., Academic Press, 2007.