Intercept Probability of Underlay Uplink CRNs with Multi-Eavesdroppers

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

[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, United Arab Emirates
[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
Emails: mounia_bouabdellah@um5.ac.ma, f.elbouanani@um5s.net.ma, p.sofotasios@ieee.org, danielbcosta@ieee.org, hbenazza@yahoo.com, kahtan.mezher@ku.ac.ae, muhaidat@ieee.org

***Abstract*—The present contribution investigates the physical layer security in a cognitive radio network (CRN). To this end, we consider an underlay uplink CRN consisting of multiple secondary sources, a single-antenna secondary base station, and multiple eavesdroppers. In addition, we assume that the secondary sources transmit their data sequentially and that a jammer is randomly chosen from the remaining source nodes to send a jamming signal to the eavesdroppers. However, in an uplink underlay CRN, a friendly jammer is not always allowed to use its maximal transmit power as the secondary users are required to continuously adapt their power in order to avoid causing interference to the primary users. As a consequence, enhancing the system security using a jammer with low transmit power in the presence of numerous eavesdroppers turns out to be questionable. In this regard, we derive novel analytic expressions that assist in quantifying the achievable security levels and the corresponding limitations. This leads to the development of useful insights on the impact of network parameters on the performance of the system's security. The offered analytic results are corroborated through Monte Carlo simulation. It is shown, that for a low transmit power of the friendly jammer, the system's security can only be enhanced for a small number of eavesdroppers.**

I. Introduction

The proliferation of mobile users brought a tremendous demand for the radio spectrum leading to the currently witnessed spectrum scarcity problem. To solve this issue, cognitive radio networks (CRNs) have been proposed as an efficient solution to increase the currently underutilized spectrum resources. In these networks, licensed primary users (PUs) and unlicensed secondary users (SUs) share the same spectrum under the assumption that the SUs signals do not cause interference to the PUs. Consequently, the SUs have to continuously adapt their transmission power in order to avoid causing interference to the PUs. For this reason, the physical layer security under such constraint becomes rather challenging.

The physical layer security of multi-antenna non-cooperative CRNs has been considered in [1]- [4]. In [1], [2], the authors derived closed-form and asymptotic expressions of the secrecy outage probability (SOP) of CRNs subject to Nakagami-m fading channels, whereas Rayleigh fading conditions were considered in [3], [4]. In [1], the authors assumed that all nodes were equipped with multiple antennas and that the source adopts the transmit antenna selection (TAS) method, while the receivers use the selection combining (SC) technique. In [1]- [4], the authors considered that only the destination and eavesdroppers are multiple antennas nodes performing SC diversity. Particularly in [4], the presence of two eavesdroppers equipped with multiple-antennas, where the first one is assumed to intercept the communication of SUs, whereas the second one intercepts the one of PUs.

It is recalled that cooperative relay communication systems have been studied in [5]- [9], in which the SOP has been investigated as a performance metric for Nakagami-m fading channels [5], [6] as well as Rayleigh fading channels [7]- [9]. In [5], [7], the authors derived the SOP by considering the existence of only one multi-antenna relay, whereas in [6], [7], [8], [9] the authors assumed the existence of multiple relays and derived closed-form as well as asymptotic expressions for the SOP by considering different relay selection policies. In [9], the authors derived the intercept probability as a useful performance metric.

In the same context, the physical layer security of a CRN considering a friendly jammer transmitter was investigated in [10], [11]. Specifically, direct communication between multiple source-destination pairs were studied in [10]. In [11], a cooperative transmission through multiple relays was analyzed where one relay is selected to forward the data to its destination and another one is selected to send a jamming signal to disrupt the eavesdropper. The corresponding SOP was derived by investigating different selection policies of the jammer. However, the power adaptation of the SUs was not been considered despite its paramount importance since the SUs are required to avoid interfering with PUs.

Motivated by the aforementioned observations, in this paper

we investigate the physical layer security of an uplink CRN consisting of multiple sources and multiple eavesdroppers. In this context, it is assumed that only one SU is communicating with a single-antenna secondary base station (SBS) under the condition of not causing any interference to the primary network. Moreover, a friendly jammer is randomly chosen among the remaining SUs to disrupt the eavesdroppers. Under the power adaptation constraint of the SUs, the present work aims at investigating the impact of the friendly jammer transmit power as well as the number of eavesdroppers on the overall system's security. Specifically, the main contributions of this paper can be summarized as follows:

- By considering the power adaptation constraint of SUs, a closed-form expression for the intercept probability (IP) is derived for two scenarios: (i) presence and (ii) absence of a friendly jammer transmitter. These exact analytic results constitute the basis for the derivation of simpler, more tractable, and more insightful asymptotic expression.
- We develop useful insights into the secrecy performance of the considered communication system. Specifically, we conclude that for a high number of eavesdroppers and a low transmit power of the friendly jammer, the security performance of the system becomes the same for both scenarios.

The remained of this paper is organized as follows: In Section II, we present the system and channel model whereas the closed-form expression for the IP is derived in Section III. In Section IV, we provide and discuss the numerical and simulation results. Finally, Section V concludes this work and discusses related future work.

II. System and Channel Models

We consider an uplink CRN, illustrated in Fig.1, composed by multiple SUs $(S_i)_{i\leq N}$, multiple eavesdroppers $(E_k)_{k\leq M}$, one single-antenna secondary base station (B_s), one PU transmitter (PU_{Tx}), and one primary base station (PBS) (B_P). Multi-user scheduling is considered such that, at the time instant t, only one source (S_c) is selected according to the round-robbing scheduling algorithm for data transmission. Additionally, a jammer among the $N-1$ remaining sources is selected by the current transmitter to send an artificial noise (AN) that is added to the kth eavesdropper's signal. Indeed, the AN is considered as a signal designed in the null space of the legitimate channel i.e., $S_c - D$, and is transmitted to interfere with the eavesdroppers without affecting the legitimate destination. We also consider that the AN is generated from a pseudo-random sequence. This sequence is known to the legitimate receiver while it is unknown to the eavesdroppers. Consequently, the destination is able to cancel out the AN while the eavesdroppers is not.

For the sake of simplicity but without loss of generality, we denote the channel power gains by $g_q = |h_q|^2$ and their corresponding coefficients are λ_q, where $q = \{S_iB_S,\ S_iE_k,\ S_iB_P\}$. As the fading amplitudes for all links are Rayleigh distributed, it follows that the channel gains are exponentially distributed. Moreover, under the power adaptation policy, the instantaneous signal-to-noise ratio (SNR) of the main channel $S_c - D$ and the wiretap link $S_c - E_k$ are given by

$$\gamma_m^{(c)} = \min\left(\overline{\gamma}_{S_c}, \frac{\overline{\gamma}_P}{g_{S_cP}}\right) g_{S_cR}, \tag{1}$$

and

$$\gamma_{e_k}^{(c,\epsilon J)} = \frac{\min\left(\overline{\gamma}_{S_c}, \frac{\overline{\gamma}_P}{g_{S_cP}}\right) g_{S_cE_k}}{\epsilon \min\left(\overline{\gamma}_{S_J}, \frac{\overline{\gamma}_P}{g_{S_JP}}\right) g_{S_JE_k} + 1}, \tag{2}$$

respectively, where

$$\epsilon = \begin{cases} 0 & : \text{without jammer} \\ 1 & : \text{with jammer} \end{cases}, \tag{3}$$

and $\overline{\gamma}_{S_c} = P_{S_c}^{max}/N_0$, $\overline{\gamma}_{S_J} = P_{S_J}^{max}/N_0$, $\overline{\gamma}_P = P_I/N_0$, with $P_{S_c}^{max}$ and $P_{S_J}^{max}$ denoting the maximal transmit power of S_c and S_J, respectively. Also, P_I accounts for the maximum tolerated interference power at PU_{Rx}, and N_0 is the variance of the additive white Gaussian noise, assumed the same at each receiver.

It is worth mentioning that when P_I increases, the source nodes are able to use their maximal transmission power resulting in increasing the signal-to-noise (SNR) at D, which leads the enhancement of the system's security.

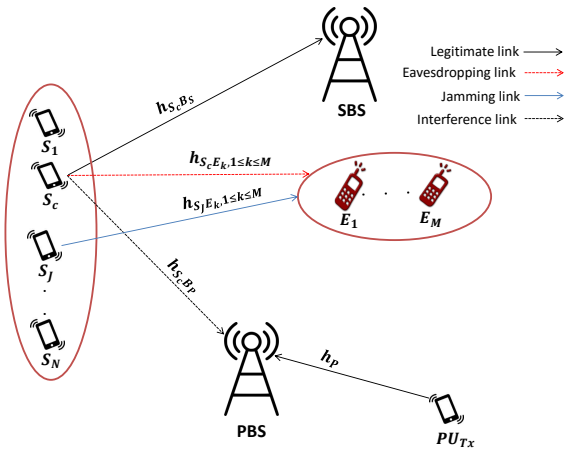

Fig. 1: System setup.

III. Intercept Probability

In this section, the intercept probability analysis of an underlay uplink CRN is presented by considering the presence and absence of a friendly jammer. In addition, the IP of the considered CRN in the presence of a friendly jammer can be expressed as

$$P_{\text{int}} = \frac{1}{N(N-1)} \sum_{c=1}^{N} \sum_{\substack{J=1 \\ J\neq c}}^{N} P_{\text{int}}^{(c,J)}, \tag{4}$$

while the IP in the absence of a friendly jammer is given by

$$P_{\text{int}} = \frac{1}{N}\sum_{c=1}^{N} P_{\text{int}}^{(c)}. \tag{5}$$

For the considered system, the IP can be defined as the probability that at least one of the wiretap links capacities is above the legitimate one, namely

$$P_{\text{int}}^{(c,J)} = 1 - \prod_{k=1}^{M} \Pr\left(C_S^{(c,\,k,\epsilon J)} > 0\right), \tag{6}$$

and $C_S^{(c,\,k,\epsilon J)}$ denotes the secrecy capacity of the c^{th} source when E_k is intercepting the channel, namely

$$C_S^{(c,\,k,\epsilon J)} = \log_2\left(1+\gamma_m^{(c)}\right) - \log_2\left(1+\gamma_{e_k}^{(c,\epsilon J)}\right). \tag{7}$$

Remark 1. *It is worth mentioning that by considering identical parameters, the IPs given in (4) and (5) become $P_{int}^{(c,J)}$ and $P_{int}^{(c)}$, respectively for any user c.*

A. Closed-form intercept probability

According to (4), in order to derive the IP of the considered system, we first have to determine the expression of $P_{int}^{(c,J)}$.

Theorem 1. *The IPs of c^{th} source in presence and absence of a friendly jammer are given by*

$$P_{int}^{(c,J)} = 1 - \prod_{k=1}^{M}\left[\times\left(\begin{array}{c} 1-\lambda_{S_cD} \\ \times \\ \frac{e^{-\varphi_J}}{\varpi_k^{(c)}} - \chi_c^{(k,J)} \\ \times \\ \left[\begin{array}{c} \mathcal{M}_c^{(k,J)} \\ \times\left[e^{-\varphi_J}-1\right] \\ +e^{\theta_c^{(k,J)}-\varphi_J} \\ \times\Delta_c^{(k,J)} \end{array}\right] \end{array}\right)\right], \tag{8}$$

and

$$P_{int}^{(c)} = 1 - \prod_{k=1}^{M}\left[\frac{\lambda_{S_cE_k}}{\lambda_{S_cE_k}+\lambda_{S_cD}}\right], \tag{9}$$

respectively, where $\varphi_J = \lambda_{S_JP}\overline{\gamma}_P/\overline{\gamma}_{S_J}$, $\varpi_k^{(c)} = \lambda_{S_cE_k} + \lambda_{S_cD}$, $\varepsilon_c^{(k,J)} = \lambda_{S_JE_k}/\lambda_{S_cE_k}$, $\chi_c^{(k,J)} = \varepsilon_c^{(k,J)}/\overline{\gamma}_{S_J}$, $\theta_c^{(k,J)} = \varpi_k^{(c)}\chi_c^{(k,J)}$, $\Delta_c^{(k,J)} = \left(A_1^{(c,k,J)}/\varphi_J - A_0^{(c,k,J)}\right)$, $A_v^{(c,k,J)} = \left(\varphi_J/\theta_c^{(k,J)}\right)^{v+1}\Omega_c^{(k,J)}, v\in\{0,1\}$,

$$\Omega_c^{(k,J)} = G_{2,2}^{2,2}\left(\varphi_J/\theta_c^{(k,J)}\,\middle|\,\begin{array}{c}(0,0),(-v,\theta_c^{(k,J)});-\\(0,0),(0,0);-\end{array}\right),$$

$$\mathcal{M}_c^{(k,J)} = G_{1,2}^{2,1}\left(\theta_c^{(k,J)}\,\middle|\,\begin{array}{c}0;-\\0,0;-\end{array}\right),$$

and $G_{p,q}^{m,n}\left(z\,\middle|\,\begin{array}{c}(a_i)_{i\le p}\\(b_k)_{k\le q}\end{array}\right)$ denotes the Meijer-G's function [12, Eq. (9.301)], while $G_{p,q}^{m,n}\left(z\,\middle|\,\begin{array}{c}(a_i,\alpha_i)_{i\le p}\\(b_k,\beta_k)_{k\le q}\end{array}\right)$ accounts for the upper incomplete Meijer-G's function [14, Eq. (1.1.1)].

Proof: In the following, two cases are distinguished, namely the presence and absence of a friendly jammer.

- *Case 1: Presence of a jammer*

The IP corresponding to the links $S_c - D$ and $S_c - E_k$ can be expressed as

$$\Pr\left(C_S^{(c,\,k,J)} \le 0\right) = \int_0^{\infty} F_{g_{S_cD}}(z)\, f_{W_c^{(k,J)}}(z)\, dz, \tag{10}$$

where $W_c^{(k,J)} = g_{S_cE_k}/\left(Y_J^{(k)}+1\right)$,

$$Y_J^{(k)} = \min\left(\overline{\gamma}_{S_J}, \frac{\overline{\gamma}_P}{g_{S_JP}}\right) g_{S_JE_k}, \tag{11}$$

and f_X and F_X denote the probability density function (PDF) and the cumulative density function (CDF) of the distribution X, respectively.

On the other hand, the CDF of $W_c^{(k,J)}$ is given by

$$F_{W_c^{(k,J)}}(\xi) = \int_0^{\infty} F_{g_{S_cE_k}}\left(\xi(z+1)\right) f_{Y_J^{(k)}}(z)\, dz, \tag{12}$$

where the CDF of $Y_J^{(k)}$ is expressed as

$$\begin{aligned} F_{Y_J^{(k)}}(\vartheta) &= \underbrace{\Pr\left(\overline{\gamma}_{S_J} g_{S_JE_k} \le \vartheta, \overline{\gamma}_{S_J} \le \frac{\overline{\gamma}_P}{g_{S_JP}}\right)}_{\mathcal{I}_1^{(k,J)}} \\ &\quad + \underbrace{\Pr\left(\frac{g_{S_JE_k}}{g_{S_JP}} \le \frac{\vartheta}{\overline{\gamma}_P}, \overline{\gamma}_{S_J} > \frac{\overline{\gamma}_P}{g_{S_JP}}\right)}_{\mathcal{I}_2^{(k,J)}}. \end{aligned} \tag{13}$$

The first term $\mathcal{I}_1^{(k,J)}$ can be rewritten as

$$\mathcal{I}_1^{(k,J)} = F_{g_{S_JE_k}}\left(\frac{\vartheta}{\overline{\gamma}_{S_J}}\right) F_{g_{S_JP}}\left(\frac{\overline{\gamma}_P}{\overline{\gamma}_{S_J}}\right), \tag{14}$$

while the second term $\mathcal{I}_2^{(k,J)}$ can be re-expressed as

$$\begin{aligned} \mathcal{I}_2^{(k,J)} &= \int_{\frac{\overline{\gamma}_P}{\overline{\gamma}_{S_J}}}^{\infty} f_{g_{S_JP}}(y)\, F_{g_{S_JE_k}}\left(\frac{\vartheta}{\overline{\gamma}_P}y\right) dxdy \\ &= e^{-\varphi_J} - \frac{e^{-\varphi_J\left(\vartheta\varrho_k^{(J)}+1\right)}}{\vartheta\varrho_k^{(J)}+1}, \end{aligned} \tag{15}$$

with $\varrho_k^{(J)} = \lambda_{S_JE_k}/\lambda_{S_JP}\overline{\gamma}_P$. By replacing (14) and (15) into (13), we obtain the CDF of $Y_J^{(k)}$ as

$$F_{Y_J^{(k)}}(\vartheta) = 1 - e^{-\varphi_J\varrho_k^{(J)}\vartheta}\left(1-e^{-\varphi_J}\right) - \frac{e^{-\varphi_J\left(\vartheta\varrho_k^{(J)}+1\right)}}{\varrho_k^{(J)}\vartheta+1}. \tag{16}$$

Based on the above and by integrating by parts and substituting (16) into (12), it follows that

$$\begin{aligned} F_{W_c^{(k,J)}}(\xi) &= 1 - \xi\int_0^{\infty} f_{g_{S_cE_k}}\left(\xi(z+1)\right) F_{Y_J^{(k)}}(z)\, dz \\ &= 1 - \Xi_k^{(c)}(\xi)\left[\begin{array}{c}\frac{1}{\xi} + \frac{e^{-\varphi_J}-1}{\mu_c^{(k,J)}} \\ -\lambda_{S_cE_k} e^{-\varphi_J}\Theta_c^{(k,J)}(z)\end{array}\right], \end{aligned} \tag{17}$$

where $\Xi_k^{(c)}(\xi) = \xi e^{-\xi\lambda_{S_cE_k}}$, $\Theta_c^{(k,J)}(z) = \int_0^\infty \frac{e^{-\beta_c^{(k,J)}z}}{\varrho_k^{(J)}z+1}dz$, $\beta_c^{(k,J)} = \lambda_{S_cE_k}\mu_c^{(k,J)}$, and $\mu_c^{(k,J)} = \frac{\varphi_J\varrho_k^{(J)}}{\lambda_{S_cE_k}}+\xi$.

Next, using Eqs. (07.34.03.0456.01) (07.34.21.0088.01) of [13], the term $\Theta_c^{(k,J)}$ is given by

$$\begin{aligned}\Theta_c^{(k,J)} &= \frac{1}{\varrho_k^{(J)}}G_{3,2}^{1,3}\left(\frac{\varrho_k^{(J)}}{\beta_c^{(k,J)}}\middle|\begin{matrix}0,1,1;-\\1;0\end{matrix}\right) \\ &= \frac{1}{\varrho_k^{(J)}}G_{1,2}^{2,1}\left(\frac{\beta_c^{(k,J)}}{\varrho_k^{(J)}}\middle|\begin{matrix}0;-\\0,0;-\end{matrix}\right).\end{aligned} \quad (18)$$

Now, substituting (18) into (17) yields

$$F_{W_c^{(k,J)}}(\xi) = 1 - e^{-\lambda_{S_cE_k}\xi}\left[1+\Upsilon_c^{(k,J)}(\xi)\right], \quad (19)$$

where

$$\begin{aligned}\Upsilon_c^{(k,J)}(\xi) &= \frac{\xi\left(e^{-\varphi_J}-1\right)}{\chi_c^{(k,J)}+\xi} - \frac{\xi\lambda_{S_cE_k}}{\varrho_k^{(J)}}e^{-\varphi_J} \\ &\quad\times G_{1,2}^{2,1}\left(\varphi_J + \frac{\varphi_J}{\chi_c^{(k,J)}}\xi\middle|\begin{matrix}0;-\\0,0;-\end{matrix}\right).\end{aligned} \quad (20)$$

By using the integration by parts and incorporating (19) into (10), we obtain

$$\begin{aligned}\Pr\left(C_S^{(c,\,k,J)}\le 0\right) &= 1-\int_0^\infty f_{\,g_{S_cD}}(z)\,F_{W_c^{(k,J)}}(z)\,dz, \\ &= \lambda_{S_cD}\left[\frac{1}{\varpi_k^{(c)}}+\mathcal{I}_3^{(c,k,J)}\right].\end{aligned} \quad (21)$$

The term $\mathcal{I}_3^{(c,k,J)} = \int_0^\infty e^{-\varpi_k^{(c)}z}\Upsilon_c^{(k,J)}(z)\,dz$ can be rewritten using (20) as

$$\mathcal{I}_3^{(c,k,J)} = \left(e^{-\varphi_J}-1\right)\Phi_1^{(c,k,J)} - \frac{\lambda_{S_cE_k}}{\varrho_k^{(J)}}e^{-\varphi_J}\Phi_2^{(c,k,J)}, \quad (22)$$

with

$$\begin{aligned}\Phi_1^{(c,k,J)} &= \int_0^\infty \frac{ze^{-\varpi_k^{(c)}z}}{\chi_c^{(k,J)}+z}dz \\ &= \frac{1}{\varpi_k^{(c)}} - \chi_c^{(k,J)}G_{1,2}^{2,1}\left(\theta_c^{(k,J)}\middle|\begin{matrix}0;-\\0,0;-\end{matrix}\right),\end{aligned} \quad (23)$$

and

$$\begin{aligned}\Phi_2^{(c,k,J)} &= \int_0^\infty \frac{z}{e^{\varpi_k^{(c)}z}}G_{1,2}^{2,1}\left(\varphi_J+\frac{\varphi_J}{\chi_c^{(k,J)}}z\middle|\begin{matrix}0;-\\0,0;-\end{matrix}\right)dz \\ &= \frac{\left(\chi_c^{(k,J)}\right)^2}{\varphi_J}e^{\theta_c^{(k,J)}}\left[\frac{A_1^{(c,k,J)}}{\varphi_J}-A_0^{(c,k,J)}\right],\end{aligned} \quad (24)$$

where the two functions $\left(A_v^{(c,k,J)}\right)_{v=0,1}$ are defined by

$$\begin{aligned}A_v^{(c,k,J)} &= \int_{\varphi_J}^\infty y^v e^{-\frac{\theta_c^{(k,J)}}{\varphi_J}y}G_{1,2}^{2,1}\left(y\middle|\begin{matrix}0;-\\0,0;-\end{matrix}\right)dy \\ &= \frac{1}{2\pi j}\int_{\mathcal{C}}\frac{\Gamma^2(s)\,\Gamma(1-s)\,\Gamma\left(\varsigma_v,\theta_c^{(k,J)}\right)}{\left(\eta_k\right)^{s-v-1}}ds,\end{aligned} \quad (25)$$

where $\eta_k = \varphi_J/\theta_c^{(k,J)}$, $\varsigma_v = v+1-s$, $\Gamma(\cdot,\cdot)$ denotes the upper incomplete Gamma function [12, Eq. (8.350.2)], $j=\sqrt{-1}$, $\mathcal{C}$ represents a complex contour of integration ensuring the convergence of the Mellin-Barnes integral, and $\Gamma(\cdot)$ denotes the Euler Gamma function [12, Eq. (8.310.1)].

Finally, by substituting (25) into (24) alongside inserting (23) and (24) into (22), and using (6), yields (8).

- *Case 2: Absence of jammer*

Under this assumption, it immediately follows that

$$\begin{aligned}\Pr\left(C_S^{(c,\,k)}\le 0\right) &= \int_0^\infty F_{g_{S_cD}}(z)f_{g_{S_cE_k}}(z)\,dz \\ &= 1-\frac{\lambda_{S_cE_k}}{\lambda_{S_cE_k}+\lambda_{S_cD}}.\end{aligned} \quad (26)$$

Substituting (26) into (6), we get the expression of IP given in (9), which concludes the proof of Theorem 1. ■

B. Asymptotic intercept probability

It can be noticed from (8) that the closed-form expression of the IP depends on the average SNRs $\overline{\gamma}_P$ and $\overline{\gamma}_{S_J}$. Consequently, the asymptotic expression for the IP can be derived for high SNR regime by considering either $\overline{\gamma}_P\to\infty$ or $\overline{\gamma}_{S_J}\to\infty$. Analogously to [6], we assume that $\overline{\gamma}_P$ is proportional to $\overline{\gamma}_{S_J}$ i.e., $\sigma = \overline{\gamma}_P/\overline{\gamma}_{S_J}$.

Proposition 1. *The asymptotic expression for the IP of the considered communication system subject to flat Rayleigh fading channels can be expressed as*

$$P_{int}^{(c,J)} \sim 1-\prod_{k=1}^{M}\left[1-\lambda_{S_cD}\left(1+\frac{e^{-\varphi_J}}{\varphi_J}\right)\frac{\varepsilon_c^{(k,J)}}{\overline{\gamma}_{S_J}}\log\left(\overline{\gamma}_{S_J}\right)\right]. \quad (27)$$

Proof: In order to derive the asymptotic expression for the IP, the residues theorem is used to approximate the Meijer G-function.

First, by using the Maclaurin series and performing some algebraic manipulations, the term Φ_2 in (24) can be approximated for high values of $\overline{\gamma}_{S_J}$ as

$$\begin{aligned}\Phi_2^{(c,k,J)} &\sim \frac{1}{2\pi j}\int_0^\infty ze^{-\varpi_k^{(c)}z}\int_C\Gamma^2(s)\,\Gamma(1-s) \\ &\quad\times\left(\frac{\varphi_Jz}{\chi_c^{(k,J)}}\right)^{-s}\left(1-\frac{\chi_c^{(k,J)}}{z}s\right)dsdz \\ &\sim \frac{1}{\left(\varpi_k^{(c)}\right)^2}\Upsilon_1(v) - \frac{\chi_c^{(k,J)}}{\varpi_k^{(c)}}\Upsilon_2(v),\end{aligned} \quad (28)$$

where $\Upsilon_1(v) = G_{2,2}^{2,2}\left(v\middle|\begin{matrix}1,1;-\\1,2;-\end{matrix}\right)$, $\Upsilon_2(v) = G_{2,2}^{2,2}\left(v\middle|\begin{matrix}0,1;-\\1,1;-\end{matrix}\right)$, and $v = \chi_c^{(k,J)}\varpi_k^{(c)}/\varphi_J$.

The terms $\Upsilon_1(v)$ and $\Upsilon_2(v)$ given in (28) can be written in terms of complex integral as

$$\Upsilon_1(v) = \frac{1}{2\pi j}\int_{\mathcal{C}_1}\Gamma(1+s)\,\Gamma(2+s)\,\Gamma^2(-s)\,v^{-s}ds, \quad (29)$$

and

$$\Upsilon_2(\upsilon) = \frac{1}{2\pi j}\int_{\mathcal{C}_2} \Gamma^2(1+s)\,\Gamma(1-s)\,\Gamma(-s)\,\upsilon^{-s} ds. \quad (30)$$

By considering the left half planes of both $\mathcal{C}_1$ and $\mathcal{C}_2$, it can be noticed that (29) has simple pole at -1 and admits poles of second order at $-l-2$, $l \in \mathbb{N}$, while (30) has poles of second order at $-l-1$, $l \in \mathbb{N}$.

By making use of [14, Theorem 1.5], (29) is given by

$$\begin{aligned}\Upsilon_1(\upsilon) &= \lim_{s\to -1}(s+1)\,\Gamma(1+s)\,\Gamma(2+s)\,\Gamma^2(-s)\,\upsilon^{-s} \\ &\quad + \sum_{l=0}^{\infty}\lim_{s\to -(l+2)}\frac{\partial \mathcal{G}_1(s,\upsilon)}{\partial s}, \end{aligned} \quad (31)$$

where

$$\mathcal{G}_1(s,\upsilon) = (s+l+2)^2\,\Gamma^2(1+s)\,(s+1)\,\Gamma^2(-s)\,\upsilon^{-s}. \quad (32)$$

It is evident that, the first term in (31) is equal to υ , while the partial derivative of $\mathcal{G}_1(s,\upsilon)$ with respect to s is given by

$$\begin{aligned}\frac{\partial \mathcal{G}_1(s,\upsilon)}{\partial s} &= (s+l+2)^2\,(s+1)\,\Gamma^2(1+s)\,\Gamma^2(-s)\,\upsilon^{-s} \\ &\quad \times \begin{bmatrix} -\log(\upsilon) + \frac{2[1+(s+l+2)\psi(1+s)]}{s+l+2} \\ +\frac{1-2(s+1)\psi(-s)}{s+1}\end{bmatrix}, \end{aligned} \quad (33)$$

where $\psi(.)$ stands for Polygamma function [13, Eq. (06.14.02.0001.01)].

The limit of $\frac{\partial \mathcal{G}_1(s,\upsilon)}{\partial s}$ can be expressed using [13, Eq. (06.14.06.0026.01)] as follows

$$\lim_{s\to -(l+2)}\frac{\partial \mathcal{G}_1(s,\upsilon)}{\partial s} = \upsilon^{l+2}\left[(l+1)\log(\upsilon)+1\right]. \quad (34)$$

By substituting (34) into (31), we get

$$\Upsilon_1(\upsilon) = \upsilon + \sum_{l=0}^{\infty}\upsilon^{l+2}\left[(l+1)\log(\upsilon)+1\right]. \quad (35)$$

In the same manner to $\Upsilon_1(\upsilon)$, the term $\Upsilon_2(\upsilon)$ can be written using the residues theorem as

$$\Upsilon_2(\upsilon) = \sum_{l=0}^{\infty}(l+1)\,\upsilon^{l+1}\left[\psi(1+l) - \psi(2+l) - \log(\upsilon)\right]. \quad (36)$$

Using [13, Eq. (06.14.03.0001.01)], the term $\Upsilon_2(\upsilon)$ can be simplified as

$$\Upsilon_2(\upsilon) = \sum_{l=0}^{\infty} -(l+1)\,\upsilon^{l+1}\left[\frac{1}{l+1} + \log(\upsilon)\right]. \quad (37)$$

On the other hand, the Meijer G function given in (23) can be written in term of complex integral as

$$G_{1,2}^{2,1}\left(\kappa \middle| \begin{matrix} 0;- \\ 0,0;- \end{matrix}\right) = \frac{1}{2\pi j}\int_{\mathcal{C}} \Gamma^2(s)\,\Gamma(1-s)\,\kappa^{-s} ds, \quad (38)$$

with $\kappa = \theta_c^{(k,J)}$.

It can be noticed that the above integrand function has poles of second order at $-l$, $l \in \mathbb{N}$. Hence, by using the residues theorem, (38) can be expressed as

$$G_{1,2}^{2,1}\left(\kappa \middle| \begin{matrix} 0;- \\ 0,0;- \end{matrix}\right) = \sum_{l=0}^{\infty}\lim_{s\to -l}\frac{\partial \mathcal{G}_2(s,\kappa)}{\partial s}, \quad (39)$$

with

$$\mathcal{G}_2(s,\kappa) = (s+l)^2\,\Gamma^2(s)\,\Gamma(1-s)\,\kappa^{-s}. \quad (40)$$

The partial derivative of $\mathcal{G}_2(s,\upsilon)$ with respect to s is given by

$$\begin{aligned}\frac{\partial \mathcal{G}_2(s,\kappa)}{\partial s} &= (s+l)\,\Gamma^2(s)\,\Gamma(1-s)\,\kappa^{-s} \\ &\quad \times \begin{bmatrix} -(s+l)\log(\kappa) \\ +2[1+(s+l)\,\psi(s)] \\ -(s+l)\,\psi(1-s)\end{bmatrix}. \end{aligned} \quad (41)$$

By making use of [13, Eq. (06.14.06.0026.01)], the limit of (41) can be expressed as

$$\lim_{s\to -l}\frac{\partial \mathcal{G}_2(s,\kappa)}{\partial s} = \frac{\kappa^l}{l!}\left[\psi(1+l) - \log(\kappa)\right]. \quad (42)$$

Now, replacing (42) into (39), yields

$$G_{1,2}^{2,1}\left(\kappa \middle| \begin{matrix} 0;- \\ 0,0;- \end{matrix}\right) = \sum_{l=0}^{\infty}\frac{\kappa^l}{l!}\left[\psi(1+l) - \log(\kappa)\right]. \quad (43)$$

Now, by substituting (35) and (36) into (28) and replacing (28) and (43) into (21) and by considering only the first and second terms of the infinite sum, we get

$$\Pr\left(C_S^{(c,\,k,J)} \le 0\right) \sim \lambda_{S_c D}\left[1 + \frac{e^{-\varphi_J}}{\varphi_J}\right]\frac{\varepsilon_c^{(k,J)}}{\overline{\gamma}_{S_J}}\log\left(\overline{\gamma}_{S_J}\right). \quad (44)$$

Finally, by replacing (44) into (6) we get the asymptotic expression for $P_{int}^{(c,J)}$ given in (27). ■

IV. Results and discussion

In this section, the derived IP expression is validated through corresponding Monte-Carlo simulation by generating 10^6 exponentially distributed random values. The considered simulation parameters are given in Table. 1. We clearly see from the obtained figures that the analytical results perfectly match the simulation results.

TABLE I: Simulation parameters.

Parameter	λ_q	M	$\bar{\gamma}_P$ (dB)
value	0.5	4	10

Fig. 2 shows the IP as a function of $\overline{\gamma}_P$ for various values of M, respectively. Obviously, the greater $\overline{\gamma}_P$, the smaller the IP. According to (1), when $\overline{\gamma}_P$ increases, the SNR of the main link increases as well. This leads to the improvement of the main link capacity and consequently the system's secrecy capacity enhances, which ensure secure transmission. Additionally, according to (6), as M increases, the IP increases as well as.

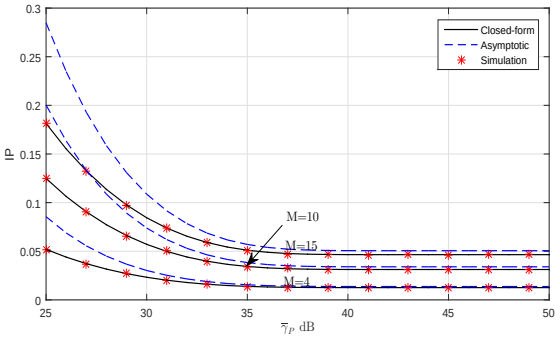

Fig. 2: Intercept probability vs $\overline{\gamma}_P$ for $\overline{\gamma}_{S_J} = 30$ dB.

Fig. 4 depicts the IP as a function of the number of eavesdroppers M for various values of $\overline{\gamma}_{S_J}$ by considering the case of the presence and absence of a friendly jammer. As one can see, as the number of eavesdroppers increases the probability of intercepting communication increases as well. Moreover, it can be also noticed that when $\overline{\gamma}_{S_J}$ is significantly small i.e., $\overline{\gamma}_{S_J} \leq -2$ dB and $M \geq 10$, the friendly jammer does not contribute to improving the security of the system.

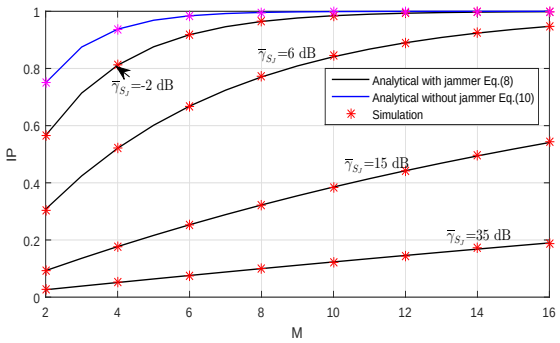

Fig. 3: Intercept probability vs the number of eavesdroppers for $\overline{\gamma}_P = 25$dB.

Fig. 5 depicts the IP versus $\overline{\gamma}_{S_J}$ and the number of eavesdroppers M. It is clearly seen that a better security is achieved for a small number of eavesdroppers and high transmission power of the friendly jammer. However, for a high number of eavesdroppers, the presence of a friendly jammer with low power does not have any significant impact on the system's security as the intercept probability tends to be high.

V. Conclusion

In this paper, the impact of the transmit power of the friendly jammer in the presence of multiple eavesdroppers on the security performance of an uplink underlay cognitive radio has been investigated. Specifically, closed-form and asymptotic expressions of the intercept probability have been derived by considering multiple sources, multiple eavesdroppers, equipped by a single antenna. Two scenarios have been considered: (i) presence or (ii) absence of a friendly jammer. The obtained results show that the system has a good secrecy

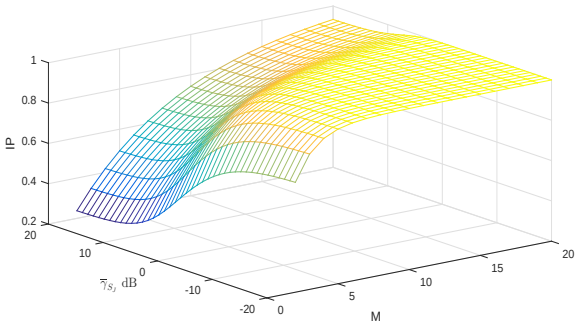

Fig. 4: Intercept probability vs the number of eavesdroppers and $\overline{\gamma}_{S_J}$.

performance in the presence of a friendly jammer and that security is enhanced for high values of the jammer's transmit power.

Acknowledgment

This work was supported in part by Khalifa University under Grant No. KU/RC1-C2PS-T2/8474000137 and Grant No. KU/FSU-8474000122.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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. Cog. Commun. and Netw.*, vol. 3, no 4, pp. 614-627, Dec. 2017.

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

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

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

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

[13] Wolfram Research, Inc. "Mathematica", Edition: Version 11.3, Champaign, Illinois, Wolfram Research, Inc., 2018.

[14] A. Kilbas, "H-Transforms: Theory and applications," Analytical Methods and Special Functions, Taylor and Francis, 2004.