On the Secrecy Analysis of Dual-Hop Underlay Multi-Source CRNs with Multi-Eavesdroppers and a Multi-Antenna Destination

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

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

***Abstract*—In this paper, the physical layer security in cognitive radio networks (CRNs) is investigated. We consider an underlay relay assisted CRN consisting of multiple secondary sources, multiple-antenna destination, a single relay, and multiple eavesdroppers. The destination node performs the maximal-ratio combining under uncorrelated Rayleigh fading channels. In more details, we consider, a secondary source is randomly selected to transmit its data, and a jammer is chosen from the remaining source nodes to send a jamming signal to the eavesdroppers. The closed-form expression of the secrecy outage probability is derived, based on the statistical characteristics of the communication channels, under the primary user's quality of service constraint. The derived analysis gives deep insights into the impact of network parameters on the performance of on the secrecy outage performance. Analytic results are corroborated through Monte Carlo simulation.**

I. Introduction

The increasing number of connected devices represents a major challenge for broadband wireless networks that would require a paradigm shift towards the development of key enabling technologies for the fifth generation wireless networks. One of the key challenges towards realizing the next generation wireless networks, however, is the scarcity of spectrum, owing to the unprecedented broadband penetration rate in recent years. A promising solution to the current spectrum crunch is the development of cognitive radio networks (CRNs). In CRNs, unlicensed users, also known as secondary users (SUs), opportunistically access the spectrum of primary (licensed) users (PUs). In underlay networks, the SU signals do not cause interference to the PUs. Accordingly, the physical layer security under such condition is a challenging problem as the SUs have to continuously adapt their transmission power in order to avoid causing interference to the PUs.

It has been shown in [1] that a system is secure if the capacity of the legitimate user is higher than that of the wiretap channel. However, in practical scenarios, the main channel does not always have a higher capacity. Therefore, in order to realize the secrecy of a communication system, several techniques have been proposed in the literature, including, (i) exploiting a friendly jammer to transmit artificial noise to malicious eavesdroppers, (ii) using cooperative transmission through one or multiple relays, or (iii) using multi-antenna nodes.

The friendly jammer approach has not been widely used in cognitive radio networks. In [2], the authors considered a direct communication between multiple source-destination pairs with two jammer selection strategies, namely random and optimal jammer selection. In [3], the authors considered a cooperative communication network in which one relay is selected to forward the transmitted information to the intended destination and another relay is selected as a friendly jammer to disrupt the eavesdropper. The authors derived the secrecy outage probability (SOP) over Rayleigh fading channels for different relay selection policies. However, these works have not considered the power constraints of the SUs, despite that this condition is of paramount importance in order to avoid interference with PUs.

Physical-layer security in cooperative networks was considered in [4-6]. The secrecy performance was investigated by deriving the closed-form expression for the secrecy outage probability (SOP) as well as its asymptotic expression over either Nakagami-m [4] and Rayleigh [5] fading channels. The authors of [4] investigated the optimal and suboptimal relay selection schemes and compared them with multiple relays combining scheme. In [5], the authors considered the presence of multiple PUs and multiple eavesdroppers. In [6], closed-

978-1-5386-8317-0/19/$31.00

form and asymptotic expressions of the intercept probability were derived for Rayleigh fading channels.

A non-cooperative CRN in the presence of a direct communication link between the source and destination has been considered in [7-10]. In these works, the nodes are assumed to be equipped with multiple antennas and perform different diversity technique. For instance, the authors of [7, 8] considered that the source is equipped with only one antenna, whereas the destination and the eavesdropper have multiple antennas. In [9], all nodes are assumed to be equipped with multiple antennas and perform different techniques namely, (i) the optimal antenna selection at the source node and (ii) the generalized selection combining at the destination and eavesdropper. In [10], the authors considered an eavesdropper accordingly, the primary network and another one listening to the SUs transmission. The SOP and its asymptotic expressions have been derived as a performance metric for Rayleigh [7,10] as well as Nakagami-m [8,9] fading channels.

Motivated by above, we investigate, in this paper, the physical layer security of an underlay CRN undergoing Rayleigh fading channels. The main contributions of this paper are:

- We derive a closed-form expression for the SOP by considering the power adaptation constraint of the SUs as well as the presence of multiple eavesdroppers that are intercepting the transmitted data at both communication hops.
- Differently from the previous works, we combine, in this paper, two techniques (i) using a friendly jammer to enhance the security at the first hop, and (ii) considering a multi-antenna destination node that performs MRC technique to improve the security at the second hop as well.
- We give deep useful insights into the secrecy performance of the considered communication system.

The rest of this paper is organized as follows. The system and channel models are described in Section II. In Section III, the closed-form expression for the SOP is derived. The numerical and simulation results are provided and discussed in Section IV. Finally, we conclude this paper and point out some possible research directions in Section V.

II. System and channel models

The considered two-hops CRN, represented in Fig. 1, consists of multiple sources $(S_i)_{i=1,..,n}$, one relay R, multiple eavesdroppers $(E_k)_{k=1,..,m}$, one L-antennas destination D performing MRC diversity technique, one PU transmitter (PU_{Tx}), and one PU receiver (PU_{Rx}). In this scheme, all the nodes except D are assumed to be equipped with only one antenna. Moreover, we consider a multi-user scheduling such that, at the moment t, only one user is transmitting its data. We assume that the source nodes are taking rounds in accessing the spectrum and a friendly jammer S_J is randomly selected among $n-1$ source nodes in order to send an artificial noise to the eavesdroppers. We assume that the primary receiver PU_{Rx} and the relay R are able to cancel out that noise, while the eavesdroppers are not.

In this scheme, we are considering Rayleigh fading model for all links in which the channel gains are exponentially distributed. The channel coefficients of links $S_i \to R$, $R \to D$, $S_i \to E_k$, $R \to E_k$, $PU_{Tx} \to PU_{Rx}$, $R \to PU_{Rx}$, $S_i \to PU_{Rx}$ are denoted by h_{S_iR}, h_{RD}, $h_{S_iE_k}$, h_{RE_k}, h_P,h_{RP}, h_{S_iP}, respectively. The received signals at R, E_k at the first and second hop, D, and the primary receiver PU_{Rx} are, respectively, expressed as

$$y_R = \sqrt{P_{S_i}} h_{S_iR} x_{S_i} + n_R \; i = 1, .., n \tag{1}$$

$$y_{1E_k}^{(i)} = \sqrt{P_{S_i}} h_{S_iE_k} x_{S_i} + \epsilon \sqrt{P_{S_J}} h_{S_JE_k} x_{S_J} + n_{E_k}, \quad k = 1, .., m \; i = 1, .., n \; i \neq J \tag{2}$$

$$y_D = \sqrt{P_R} ||h_{RD}|| x_R + w_D n_D, \tag{3}$$

$$y_{2E_k} = \sqrt{P_R} h_{RE_k} x_r + n_E, k = 1, .., m \tag{4}$$

where

$$\epsilon = \begin{cases} 0, \text{ absence of jammer} \\ 1, \text{ presence of jammer} \end{cases},$$

and P_{S_i}, P_R, and P_{S_J} are the transmission power of S_i, R, and S_J, respectively. The transmitted signals of S_i, R, and S_J are x_{s_i}, x_R, and x_{S_j}, respectively. n_R, n_D, n_E, denote the additive white Gaussian noise at R, D, and E_k, respectively, $w_D = \frac{h_{RD}^\dagger}{||h_{RD}||}$, while h_{RD} denotes $L \times 1$ channel vector of the links R-$(D_j)_{j=1,..,L}$, and the symbol † denotes the transpose conjugate.

For the sake of simplicity, we denote the channel power gains by $g_q = |h_q|^2$ and their corresponding coefficients are λ_q where $q = \{S_iR, \; S_iE_k, \; S_iP, \; RD_j, \; RE_k, \; RP, \; P\}$. As the fading amplitudes of all links are Rayleigh distributed, it follows that the channel gains are exponentially distributed.

During transmission, the nodes S_i, S_J, and R have to set their transmission power in order to avoid causing harmful interference to the PUs. Thus, the transmission power of the source S_i, the jammer S_J, and the relay R can be, respectively, expressed as

$$P_{S_i} = \min \left(P_{S_i}^{max}, \frac{P_I}{g_{S_iP}} \right); i = 1, .., n, \tag{5}$$

and

$$P_R = \min \left(P_R^{max}, \frac{P_I}{g_{RP}} \right), \tag{6}$$

where $P_{S_i}^{max}$, and P_R^{max} are the maximal transmit power at S_i, and R, respectively, while P_I accounts for the maximum tolerated interference power at PU_{Rx}. It is clearly seen from (5), and (6) that when P_I increases, the nodes S_i, S_J, and R will be allowed to use their maximal transmission power. Consequently, the signal-to-noise ratio (SNR) at both R and D will increase while the SNR at eavesdroppers will decrease leading to a system security improvement.

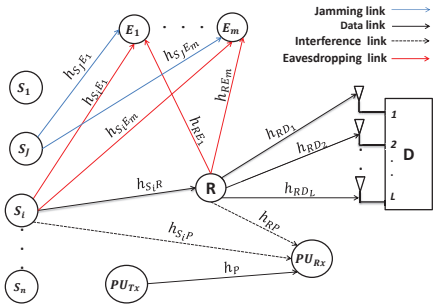

Fig. 1: System setup.

III. Secrecy capacity

The secrecy capacity was first introduced by Wyner [1]. It can be defined as the maximum rate at which the transmitted information can confidentially reach its intended destination. In our considered communication system, we are using a decode-and-forward relaying protocol. Consequently, the secrecy capacity of the ith source when S_J is selected as a friendly jammer can be expressed by

$$C_s^{(i,J)} = \min_{k=1,..,m} \left(C_{1S}^{(i,k,J)}, C_{2S}^{(k)} \right), \tag{7}$$

where

- $C_{1S}^{(i,k,J)}$ denotes the secrecy capacity of the first link, i.e, the difference between the capacity of the main link $S_i - R$ and the one of the wiretap channel $S_i - E_k$ in the presence of the jammer S_J, and can be written as

$$\begin{aligned} C_{1S}^{(i,k,J)} &= \left[C_{1M}^{(i)} - C_{1E}^{(i,k,J)} \right]^+ \\ &= \begin{cases} \log_2 \left(\gamma_{1k}^{(i,J)} \right), & \gamma_R^{(i)} > \gamma_{1E}^{(i,k,J)} \\ 0, & \text{elsewhere} \end{cases}, \end{aligned} \tag{8}$$

  where $\gamma_R^{(i)}$ and $\gamma_{1E}^{(i,k,J)}$ denote the instantaneous SNR at the relay R and the kth eavesdropper E_k, respectively, and are given as

$$\gamma_R^{(i)} = \frac{P_{S_i} g_{S_i R}}{N_R}, \tag{9}$$

$$\gamma_{1E}^{(i,k,J)} = \frac{P_{S_i} g_{S_i E_k}}{P_{S_J} g_{S_J E_k} + N_E}, \tag{10}$$

  and

$$\gamma_{1k}^{(i,J)} = \frac{1 + \gamma_R^{(i)}}{1 + \gamma_{1E}^{(i,k,J)}}. \tag{11}$$

- $C_{2S}^{(k)}$ is the secrecy capacity of the second hop, representing the difference between the capacity of the link $R - D$ and the one of the wiretap channel $R - E_k$

$$C_{2S}^{(k)} = \begin{cases} \log_2 \left(\gamma_{2k} \right), & \gamma_D > \gamma_{2E}^{(k)} \\ 0, & \text{elsewhere} \end{cases}, \tag{12}$$

where γ_D, and $\gamma_{2E}^{(k)}$ denote the instantaneous SNR of the main link $R - D$ and the channel $R - E_k$, respectively and are given as

$$\gamma_D = \frac{P_R \sum_{t=1}^{L} g_{RD_t}}{N_D}, \tag{13}$$

$$\gamma_{2E}^{(k)} = \frac{P_R g_{RE_k}}{N_E}, \tag{14}$$

and

$$\gamma_{2k} = \frac{1 + \gamma_D}{1 + \gamma_{2E}^{(k)}}. \tag{15}$$

IV. Secrecy outage probability

To evaluate the security level of the considered CRN, we consider the SOP as a performance criterion. This metric accounts for the probability that the secrecy capacity is less than a given secrecy rate R_s which can be can be expressed as

$$SOP = \frac{1}{n(n-1)} \sum_{i=1}^{n-1} \sum_{\substack{J=1 \\ J \neq i}}^{n} SOP_i^{(J)}, \tag{16}$$

where

$$SOP_i^{(J)} = \Pr \left(C_s^{(i,J)} < R_s \right), \tag{17}$$

It is clearly seen from (17) that as $C_s^{(i,J)}$ increases SOP decreases resulting in performance enhancement of the system. So, in order to investigate the system's security, it is sufficient to determine the CDF of $C_s^{(i,J)}$.

Substituting (7) into (17), yields

$$\begin{aligned} SOP_i^{(J)} &= 1 - \prod_{k=1}^{m} \Pr \left(\min(C_{1S}^{(i,k,J)}, C_{2S}^{(k)}) \geq R_s \right) \\ &= 1 - \prod_{k=1}^{m} \left[1 - F_{\gamma_{1k}^{(i,J)}}(\gamma) \right] \left[1 - F_{\gamma_{2k}}(\gamma) \right], \end{aligned} \tag{18}$$

where $\gamma = 2^{R_S}$.

One can see from (18) that the computation of $SOP_i^{(J)}$ requires the knowledge of the CDFs of both $\gamma_{1k}^{(i,J)}$ and γ_{2k}.

Theorem 1. *The CDFs of the random variables (RVs) $\gamma_{1k}^{(i,J)}$ and γ_{2k} are given by (19) and (20), respectively, as shown at the top of the next page, where*

$$\Xi_{i,k}^{(J)}(\gamma) = \frac{e^{-\varphi_J}}{h_{i,k}} - \chi_{i,k}^{(J)} \left\{ \Upsilon_{i,k}^{(J)} \left[e^{-\varphi_J} - 1 \right] - e^{\varpi_{i,k}^{(J)} - \varphi_J} \Lambda_{i,k}^{(J)} \right\},$$

$$\varphi_J = \frac{\lambda_{S_J P} P_I}{P_{S_J}^{max}},$$

$$h_{i,k} = \lambda_{S_i E_k} N_E + \lambda_{S_i R} N_R \gamma,$$

$$\chi_{i,k}^{(J)} = \frac{\lambda_{S_J E_k}}{\lambda_{S_i E_k} P_{S_J}^{max}},$$

$$\Upsilon_{i,k}^{(J)} = G_{1,2}^{2,1} \left(\varpi_{i,k}^{(J)} \middle| \begin{matrix} 0; - \\ 0, 0; - \end{matrix} \right),$$

$$F_{\gamma_{1k}^{(i,J)}}(\gamma)=1-\left\{\left(1-\lambda_{S_iR}N_R\gamma\Xi_{i,k}^{(J)}(\gamma)\right)e^{-\frac{\lambda_{S_iR}N_R(\gamma-1)}{P_{S_i}^{max}}}\left(1-\frac{e^{-\frac{\lambda_{S_iP}P_I}{P_{S_i}^{max}}}}{\frac{\lambda_{S_iP}P_I}{\lambda_{S_iR}N_R(\gamma-1)}+1}\right)\right\}. \tag{19}$$

$$F_{\gamma_{2k}}(\gamma)=1-\sum_{h=1}^{L}\prod_{\substack{l=1\\l\neq h}}^{L}\left(\frac{\lambda_{RD_l}}{\lambda_{RD_l}-\lambda_{RD_h}}\right)\frac{e^{-\frac{\lambda_{RD_h}N_D(\gamma-1)}{P_R^{max}}}}{\frac{\lambda_{RD_h}N_D\gamma}{\lambda_{RE_k}N_E}+1}\left[1-\frac{e^{-\frac{\lambda_{RP}P_I}{P_R^{max}}}}{\frac{\lambda_{RP}P_I}{\lambda_{RD_h}N_D(\gamma-1)}+1}\right]. \tag{20}$$

$$\varpi_{i,k}^{(J)}=\chi_{i,k}^{(J)}h_{i,k},$$

$$\Lambda_{i,k}^{(J)}=\frac{A_1^{(i,k,J)}}{\varphi_J}-A_0^{(i,k,J)},$$

$$A_p^{(i,k,J)}=\left(\beta_{i,k}^{(J)}\right)^{p+1}G_{2,2}^{2,2}\left(\beta_{i,k}^{(J)}\middle|\begin{matrix}(0,0),(-p,\varpi_{i,k}^{(J)});-\\(0,0),(0,0);-\end{matrix}\right),$$

and

$$\beta_{i,k}^{(J)}=\frac{\varphi_J}{\chi_{i,k}^{(J)}h_{i,k}},$$

where $G_{p,q}^{m,n}\left(z\middle|\begin{matrix}(a_v)_{v\leq p}\\(b_w)_{w\leq q}\end{matrix}\right)$ denotes the Meijer-G's function [11, Eq. (07.34.02.0001.01)] and $G_{p,q}^{m,n}\left(z\middle|\begin{matrix}(a_l,\alpha_l)_{l\leq p}\\(b_r,\beta_r)_{r\leq q}\end{matrix}\right)$ accounts for the upper incomplete Meijer-G's function [12, Eq. (1.1.1)].

Proof:

A. CDF of $\gamma_{1k}^{(i,J)}$

The CDF of $\gamma_{1k}^{(i,J)}$ can be expressed as

$$\begin{aligned}F_{\gamma_{1k}^{(i,J)}}(\gamma)&=\Pr\left(P_{S_i}\left[\frac{g_{S_iR}}{N_R}-\gamma W_{i,k}^{(J)}\right]\leq\gamma-1\right)\\&=\Pr\left(\left(P_{S_i}\leq Z_{i,k}^{(J)}\text{ and }Z_{i,k}^{(J)}\geq 0\right)\text{or }Z_{i,k}^{(J)}\leq 0\right)\\&=\int_0^\infty F_{P_{S_i}}(z)f_{Z_{i,k}^{(J)}}(z)dz+\int_{-\infty}^0 f_{Z_{i,k}^{(J)}}(z)dz,\end{aligned} \tag{21}$$

where $W_{i,k}^{(J)}=\frac{g_{S_iE_k}}{P_{S_J}g_{S_JE_k}+N_E}$ and $Z_{i,k}^{(J)}=\frac{\gamma-1}{\frac{g_{S_iR}}{N_R}-\gamma W_{i,k}^{(J)}}$. According to (21), it follows that the derivation of $F_{\gamma_{1k}^{(i,J)}}(\gamma)$ requires the knowledge of the CDFs of both P_{S_i} and $Z_{i,k}^{(J)}$. Doing some computations, the CDF of P_{S_i} can be easily shown to be given

$$F_{P_{S_i}}(z)=\begin{cases}1 & :P_{S_i}^{max}\leq z\\ F_{\frac{P_I}{g_{S_iP}}}(z) & :P_{S_i}^{max}>z\end{cases}, \tag{22}$$

where the CDF of $\frac{P_I}{g_{S_iP}}$ can be obtained as

$$F_{\frac{P_I}{g_{S_iP}}}(z)=e^{-\lambda_{S_iP}\frac{P_I}{z}}. \tag{23}$$

On the other hand, the CDF of $Q_{i,k}^{(J)}=\frac{1}{Z_{i,k}^{(J)}}$ can be expressed for positive values of ψ as

$$\begin{aligned}F_{Q_{i,k}^{(J)}}(\psi)&=\Pr\left(g_{S_iR}\leq N_R\left[\psi(\gamma-1)+\gamma W_{i,k}^{(J)}\right]\right)\\&=\int_0^\infty Fg_{S_iR}\left(N_R\left[\psi(\gamma-1)+\gamma z\right]\right)f_{W_{i,k}^{(J)}}(z)\,dz.\end{aligned} \tag{24}$$

In order to derive $F_{Q_{i,k}^{(J)}}(\psi)$ we have to derive the CDF of the RV $W_{i,k}^{(J)}$

$$\begin{aligned}F_{W_{i,k}^{(J)}}(\xi)&=\Pr\left(g_{S_iE_k}\leq\xi\left(g_{S_JE_k}P_{S_J}+N_E\right)\right)\\&=\int_0^\infty F_{g_{S_iE_k}}\left(\xi\left(z+N_E\right)\right)\\&\times\ f_{P_{S_J}g_{S_JE_k}}(z)\,dz.\end{aligned} \tag{25}$$

By using integration by parts, we get

$$F_{W_{i,k}^{(J)}}(\xi)=1-\xi\int_0^\infty f_{g_{S_iE_k}}\left(\xi\left(z+N_E\right)\right)F_{P_{S_J}g_{S_JE_k}}(z)\,dz. \tag{26}$$

By definition, the CDF of the RV $P_{S_J}g_{S_JE_k}$ can be written as

$$\begin{aligned}F_{P_{S_J}g_{S_JE_k}}(z)&=\underbrace{\Pr\left(g_{S_JE_k}\leq\frac{z}{P_{S_J}^{max}},\frac{P_I}{g_{S_JP}}\geq P_{S_J}^{max}\right)}_{I_1^{(k,J)}}\\&+\underbrace{\Pr\left(\frac{g_{S_JE_k}}{g_{S_JP}}\leq\frac{z}{P_I},\frac{P_I}{g_{S_JP}}\leq P_{S_J}^{max}\right)}_{I_2^{(k,J)}}\end{aligned} \tag{27}$$

As the two RVs $g_{S_JE_k}$ and g_{S_JP} are independent, the first term $\mathcal{I}_1^{(k,J)}$ in (27) can be written as

$$\begin{aligned}\mathcal{I}_1^{(k,J)}&=\Pr\left(g_{S_JE_k}\leq\frac{z}{P_{S_J}^{max}}\right)\Pr\left(g_{S_JP}\leq\frac{P_I}{P_{S_J}^{max}}\right)\\&=F_{g_{S_JE_k}}\left(\frac{z}{P_{S_J}^{max}}\right)F_{g_{S_JP}}\left(\frac{P_I}{P_{S_J}^{max}}\right),\end{aligned} \tag{28}$$

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

$$\begin{aligned}\mathcal{I}_2^{(k,J)}&=\int_{\frac{P_I}{P_{S_J}^{max}}}^\infty f_{g_{S_JP}}(y)\int_0^{\frac{z}{P_I}y}f_{g_{S_JE_k}}(x)dxdy\\&=e^{-\varphi_J}-\frac{e^{-\varphi_J\left(z\varrho_k^{(J)}+1\right)}}{z\varrho_k^{(J)}+1},\end{aligned} \tag{29}$$

where $\varrho_k^{(J)} = \frac{\lambda_{S_J E_k}}{\lambda_{S_J P} P_I}$. Then, by plugging (28) and (29) into (27) we obtain

$$F_{P_{S_J} g_{S_J E_k}}(\vartheta) = 1 + e^{-\varphi_J \varrho_k^{(J)} \vartheta} \left(e^{-\varphi_J} - 1\right) - \frac{e^{-\varphi_J \left(\vartheta \varrho_k^{(J)} + 1\right)}}{\vartheta \varrho_k^{(J)} + 1}. \tag{30}$$

Now, the CDF of $W_{i,k}^{(J)}$ can be obtained by incorporating (30) into (26), as

$$F_{W_{i,k}^{(J)}}(\xi) = 1 - e^{-\lambda_{S_i E_k} \xi N_E} \left[\begin{array}{c} 1 + \frac{\lambda_{S_i E_k} \xi \left(e^{-\varphi_J} - 1\right)}{\varphi_J \varrho_k^{(J)} + \lambda_{S_i E_k} \xi} \\ - \frac{\xi \lambda_{S_i E_k} e^{-\varphi_J}}{\varrho_k^{(J)}} \\ \times \underbrace{\int_0^\infty \frac{e^{-\varrho_k^{(J)} \delta_{i,k}^{(J)} z}}{z + \frac{1}{\varrho_k^{(J)}}} dz}_{\mathcal{I}_3^{(i,k,J)}} \end{array} \right], \tag{31}$$

where $\delta_{i,k}^{(J)} = \frac{\varphi_J \varrho_k^{(J)} + \lambda_{S_i E_k} \xi}{\varrho_k^{(J)}}$.

Making use of [11, Eq. (07.34.03.0456.01)] alongside with [11, Eq. (07.34.21.0088.01)], we have

$$\begin{aligned} \mathcal{I}_3^{(i,k,J)} &= \delta_{i,k}^{(J)} \int_0^\infty G_{2,2}^{1,2}\left(z \left| \begin{array}{c} 1,1;- \\ 1;0 \end{array} \right.\right) e^{-\delta_{i,k}^{(J)} z} dz \\ &= G_{3,2}^{1,3}\left(\frac{1}{\delta_{i,k}^{(J)}} \left| \begin{array}{c} 0,1,1;- \\ 1;0 \end{array} \right.\right). \end{aligned} \tag{32}$$

Furthermore,

$$\begin{aligned} G_{3,2}^{1,3}\left(\frac{1}{\delta_{i,k}^{(J)}} \left| \begin{array}{c} 0,1,1;- \\ 1;0 \end{array} \right.\right) &= G_{2,3}^{3,1}\left(\delta_{i,k}^{(J)} \left| \begin{array}{c} 0;1 \\ 1,0,0;- \end{array} \right.\right) \\ &= \frac{1}{2\pi j} \int_{\mathcal{C}} \frac{\Gamma(s+1)\Gamma^2(s)}{\Gamma(s+1)} \\ &\quad \times \Gamma(1-s) \left(\delta_{i,k}^{(J)}\right)^{-s} ds \\ &= G_{1,2}^{2,1}\left(\delta_{i,k}^{(J)} \left| \begin{array}{c} 0;- \\ 0,0;- \end{array} \right.\right), \end{aligned} \tag{33}$$

with $j = \sqrt{-1}$ and $\mathcal{C}$ represents a complex contour of integration ensuring the convergence of the Mellin-Barnes integral.

Then, by performing the substitution (32) into (31) yields

$$\begin{aligned} F_{W_{i,k}^{(J)}}(\xi) &= 1 - e^{-\lambda_{S_i E_k} \xi N_E} \\ &\quad \times \left[\begin{array}{c} 1 + \frac{\lambda_{S_i E_k} \xi \left(e^{-\varphi_J} - 1\right)}{\varphi_J \varrho_k^{(J)} + \lambda_{S_i E_k} \xi} \\ - \frac{\xi \lambda_{S_i E_k} e^{-\varphi_J}}{\varrho_k^{(J)}} \\ \times G_{1,2}^{2,1}\left(\varphi_J + \frac{\varphi_J \xi}{\chi_{i,k}^{(J)}} \left| \begin{array}{c} 0;- \\ 0,0;- \end{array} \right.\right) \end{array} \right], \end{aligned} \tag{34}$$

It follows, by substituting (34) into (24) that

$$F_{Q_{i,k}^{(J)}}(\psi) = 1 - e^{-\phi_i(\psi)} \left(1 - \lambda_{S_i R} N_R \gamma \Xi_{i,k}^{(J)}(\gamma)\right), \tag{35}$$

where

$$\Xi_{i,k}^{(J)}(\gamma) = \int_0^\infty e^{-h_{i,k} z} dz + \left(e^{-\varphi_J} - 1\right) \Theta_{1J}^{(i,k)} - \frac{\varphi_J e^{-\varphi_J}}{\chi_{i,k}^{(J)}} \Theta_2^{(i,k,J)}, \tag{36}$$

$$\Theta_{1J}^{(i,k)} = \int_0^\infty \frac{z e^{-h_{i,k} z}}{\chi_{i,k}^{(J)} + z} dz, \tag{37}$$

$$\Theta_{2J}^{(i,k)} = \int_0^\infty z e^{-h_{i,k} z} G_{1,2}^{2,1}\left(\varphi_J \left(1 + \frac{z}{\chi_{i,k}^{(J)}}\right) \left| \begin{array}{c} 0;- \\ 0,0;- \end{array} \right.\right) dz, \tag{38}$$

and

$$\phi_i(\psi) = \lambda_{S_i R} N_R \psi(\gamma - 1). \tag{39}$$

The term $\Theta_{1J}^{(i,k)}$ can be expressed using the identities (36) and (37) as

$$\begin{aligned} \Theta_{1J}^{(i,k)} &= \int_0^\infty e^{-h_{i,k} z} dz - \chi_{i,k}^{(J)} \int_0^\infty \frac{e^{-h_{i,k} z}}{\chi_{i,k}^{(J)} + z} dz \\ &= \frac{1}{h_{i,k}} - \chi_{i,k}^{(J)} G_{1,2}^{2,1}\left(h_{i,k} \chi_{i,k}^{(J)} \left| \begin{array}{c} 0;- \\ 0,0;- \end{array} \right.\right), \end{aligned} \tag{40}$$

while the term $\Theta_{2J}^{(i,k)}$ can be rewritten, using a change of variable, as

$$\begin{aligned} \Theta_{2J}^{(i,k)} &= \frac{\chi_{i,k}^{(J)}}{\varphi_J} e^{\chi_{i,k}^{(J)} h_{i,k}} \int_{\varphi_J}^\infty \left(\frac{y}{\varphi_J} - 1\right) e^{-\frac{\chi_{i,k}^{(J)} h_{i,k}}{\varphi_J} y} \\ &\quad \times G_{1,2}^{2,1}\left(y \left| \begin{array}{c} 0;- \\ 0,0;- \end{array} \right.\right) dy \\ &= \eta_{i,k}^{(J)} \left[\frac{A_1^{(i,k,J)}}{\varphi_J} - A_0^{(i,k,J)}\right], \end{aligned} \tag{41}$$

where $\eta_{i,k}^{(J)} = \frac{\chi_{i,k}^{(J)}}{\varphi_J} e^{\chi_{i,k}^{(J)} h_{i,k}}$, and the function $\left(A_p^{(i,k,J)}\right)_{p=0,1}$ is defined by

$$\begin{aligned} A_p^{(i,k,J)} &= \int_{\varphi_J}^\infty y^p e^{-\frac{\chi_{i,k}^{(J)} h_{i,k}}{\varphi_J} y} G_{1,2}^{2,1}\left(y \left| \begin{array}{c} 0;- \\ 0,0;- \end{array} \right.\right) dy \\ &= \frac{1}{2\pi j} \int_{\mathcal{C}} \Gamma^2(s) \Gamma(1-s) ds \int_{\varphi_J}^\infty y^{p-s} e^{-\frac{\chi_{i,k}^{(J)} h_{i,k}}{\varphi_J} y} dy \\ &= \frac{\left(\beta_{i,k}^{(J)}\right)^{p+1}}{2\pi j} \int_{\mathcal{C}} \Gamma^2(s) \Gamma(1-s) \Gamma\left(\varsigma_{p,s}, \varpi_{i,k}^{(J)}\right) \left(\beta_{i,k}^{(J)}\right)^{-s} ds, \end{aligned} \tag{42}$$

where $\varsigma_{p,s} = p + 1 - s$. Then, by substituting (42) into (41) alongside with (40), we get the expression of the function $\Xi_{i,k}^{(J)}(\gamma)$ defined above.

In contrast, the CDF of $Z_{i,k}^{(J)}$ is expressed in terms of the one of its inverse as

$$F_{Z_{i,k}^{(J)}}(x) = 1 - F_{Q_{i,k}^{(J)}}\left(\frac{1}{x}\right) + F_{Q_{i,k}^{(J)}}(0). \tag{43}$$

By using (35), the CDF of $Z_{i,k}^{(J)}$ can be rewritten as

$$\begin{aligned} F_{Z_{i,k}^{(J)}}(x) &= e^{-\frac{\lambda_{S_i R} N_R (\gamma - 1)}{x}} \left(1 - \lambda_{S_i R} N_R \gamma \Xi_{i,k}^{(J)}(\gamma)\right) \\ &\quad + \lambda_{S_i R} N_R \gamma \Xi_{i,k}^{(J)}(\gamma). \end{aligned} \tag{44}$$

Then, by performing the appropriate substitutions in (21), we obtain (19).

Remark 1. *For the scenario without any jammer source and by performing some computation we can get easily the CDF at the first hop as*

$$F_{\gamma_{1k}^{(i)}}(\gamma) = 1 + \frac{e^{-\Phi_i}}{\frac{\lambda_{S_iR}N_R\gamma}{\lambda_{S_iE_k}N_E}+1}\left[\frac{\Phi_i e^{-\Omega_i}}{\Omega_i+\Phi_i}-1\right], \quad (45)$$

where $\Omega_i = \frac{\lambda_{S_iP}P_I}{P_{S_i}^{max}}$ *and* $\Phi_i = \frac{\lambda_{S_iR}N_R(\gamma-1)}{P_{S_i}^{max}}$.

B. CDF of γ_{2k}

Using (14), the CDF of γ_{2k} is given as

$$\begin{aligned} F_{\gamma_{2k}}(\gamma) &= \Pr\left(P_R\left[\frac{Y_{RD}}{N_D}-\frac{\gamma g_{RE_k}}{N_E}\right]\le\gamma-1\right) \\ &= \Pr\left(P_R\le V_{R,k}, V_{R,k}\ge 0\right)+\Pr\left(V_{R,k}\le 0\right) \\ &= \int_0^\infty F_{P_R}(z)f_{V_{R,k}}(z)dz+\int_{-\infty}^0 f_{V_{R,k}}(z), \quad (46)\end{aligned}$$

where $Y_{RD}=\sum_{v=1}^{L} g_{RDv}$, and $V_{R,k}=\frac{\gamma-1}{\left(\frac{Y_{RD}}{N_D}-\gamma\frac{g_{RE_k}}{N_E}\right)}$.

In a similar manner, we have to derive first the CDF of the RV $V_{R,k}=\frac{1}{U_{R,k}}$.

$$\begin{aligned} F_{U_{R,k}}(\vartheta) &= \Pr\left(Y_{RD}\le N_D\left(\vartheta(\gamma-1)+\gamma\frac{g_{RE_k}}{N_E}\right)\right) \\ &= \int_0^\infty F_{Y_{RD}}\left(\theta(z)\right)f_{g_{RE_k}}(z)\,dz, \quad (47)\end{aligned}$$

where $\theta(z)=N_D\left(\vartheta(\gamma-1)+\gamma\frac{z}{N_E}\right)$.

According to [6], the CDF of Y_{RD} in the case of i.n.i.d RVs can be expressed as

$$F_{Y_{RD}}(x)=\sum_{h=1}^{L}\psi_h\left(1-e^{-\lambda_{RD_h}x}\right), \quad (48)$$

where $\psi_h=\prod_{\substack{l=1\\ l\neq h}}^{L}\left(\frac{\lambda_{RD_l}}{\lambda_{RD_l}-\lambda_{RD_h}}\right)$.

By substituting the PDF of the exponential RV and (48) into (47), the CDF of $U_{R,k}$ can be derived as

$$F_{U_{R,k}}(\vartheta)=\sum_{h=1}^{L}\psi_h\left(1-\frac{e^{-\lambda_{RD_h}N_D\vartheta(\gamma-1)}}{\frac{\lambda_{RD_h}N_D\gamma}{\lambda_{RE_k}N_E}+1}\right). \quad (49)$$

Similarly to (43), and making use of (49) yields

$$F_{Z_{R,k}}(x)=1-\sum_{h=1}^{L}\psi_h\frac{\left(1-e^{-\frac{\lambda_{RD_h}N_D(\gamma-1)}{x}}\right)}{\frac{\lambda_{RD_h}N_D\gamma}{\lambda_{RE_k}N_E}+1}. \quad (50)$$

TABLE I: Simulation parameters.

Parameter	λ_q	m	n	R_S	N_R
value	0.5	2	2	1	2
Parameter	N_D	N_E	$P_{S_i}^{max}$	P_R^{max}	$P_{S_J}^{max}$
value	2	2	8	8	8

As the CDF of P_R can be expressed similarly to the one of P_{S_i} given by (22) and (23), the CDF of γ_{2k} can be now rewritten as

$$\begin{aligned} F_{\gamma_{2k}}(\gamma) &= \int_0^{P_R^{max}} F_{\frac{P_I}{g_{RP}}}(t)f_{V_{R,k}}(t)\,dt \\ &+ \underbrace{\int_{P_R^{max}}^{\infty} f_{V_{R,k}}(t)\,dt+\int_{-\infty}^{0} f_{V_{R,k}}(t)\,dt}_{=1-\int_0^{P_R^{max}} f_{V_{R,k}}(t)dt}, \quad (51)\end{aligned}$$

Finally, by substituting CDF of $\frac{P_I}{g_{RP}}$, that is similarly to (23), and (50) into (51), we obtain (20) which concludes the proof of Theorem 1. ■

V. Results and Discussion

In this section, we present the analytical and the simulation results for the considered CRN. The setting parameters of the simulation experiment are summarized in Table 1 where the powers are given in dBW.

As seen in Figs. 2-4, all analytical and simulation curves are perfectly matched over the entire ranges of the considered parameters.

Fig. 2 shows the secrecy outage probability as a function of the secrecy rate R_s for various values of destination's antennas number. It can clearly be seen that the SOP increases with the increasing values of R_s, as also noticed by (17). This can be interpreted by the fact that when a high secrecy rate is adopted for a better performance, it is less likely to achieve a perfect secure transmission. Furthermore, the security is enhanced when using multiple antennas at the destination instead of employing only a single one. For instance, for $R_s = 1$ bit/s/Hz we have $SOP \simeq 0.85$ and $SOP = 0.94$ for $L = 4$ and $L = 2$, respectively.

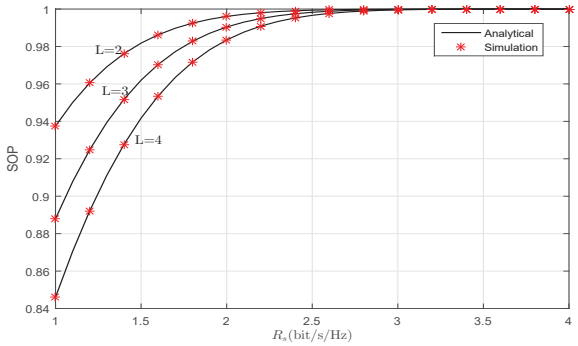

Fig. 2: SOP vs secrecy rate for different values of antennas at the destination.

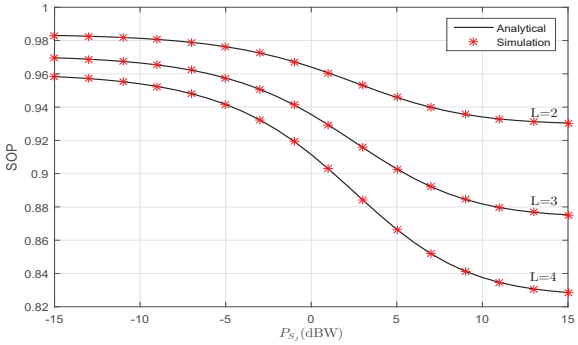

Fig. 3: SOP vs maximum transmission power of the jammer S_J for different values of antennas at the destination.

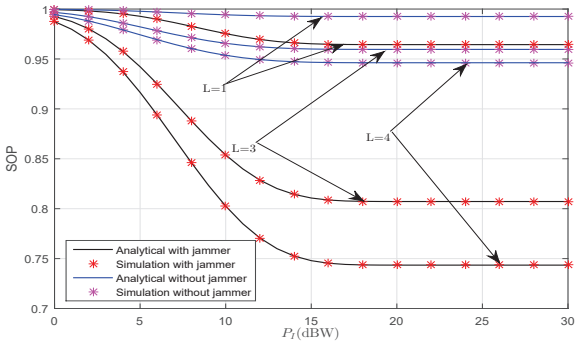

Fig. 4: SOP vs maximum tolerated interference power P_I at PU_{Rx} for different values of antennas at the destination.

The SOP versus the transmission power of the selected jammer $P_{S_J}^{max}$ is illustrated in Fig. 3 for various values of branches number L at the node D. It can be noticed that, the higher $P_{S_J}^{max}$ the smaller the SOP and therefore the system security becomes more reliable. This can be construed as increasing $P_{S_J}^{max}$ leads to a decrease of eavesdroppers' SNRs as it can be seen in (10). Consequently, the wiretap link capacity decreases as well leading to the improvement of the first hop secrecy capacity. Additionally, increasing the number of antennas at the destination enhances the SNR as shown in (13) leading to the enhancement of the main link capacity i.e., $R-D$, and consequently the secrecy performance gets better.

Fig. 4 depicts the SOP versus P_I for different scenarios namely (i) either absence or presence of a friendly jammer and (i) single and multiple antennas destination. It can be noticed that the greater the P_I, the smaller the SOP. This can be justified, from (5) and (6), as increasing P_I above certain threshold, push the sources as well as the relay to transmit with their maximal powers. Also, it is clearly seen that a better secrecy is achieved when using a friendly jammer at the first hop and a destination with multiple antennas. Moreover, it can be noticed that the scenario with absence of jammer and L antennas destination ($L > 2$) is better than the one with presence of friendly jammer and a single antenna destination.

VI. Conclusions

The secrecy outage probability of a CRN under decode-and-forward relaying scheme is investigated by considering either the presence or absence of a friendly jammer at the first hop and a multi-antenna destination at the second hop. A closed-form expression for the SOP is derived, in terms of the upper incomplete Meijer's G-function, based on which the impact of key system parameters on the secrecy performance is investigated. The obtained numerical and simulation results showed that the system's secrecy is enhanced with the increase of both the destination antennas' number and the friendly jammer transmission power. Moreover, it is shown that increasing the number of antennas at the destination without using a friendly jammer yields a more secure communication, compared to the scenario employing a single-antenna destination along with a friendly jammer.

References

[1] A. Wyner, "The Wire-Tap Channel", *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[2] Y. Zou, "Physical-Layer Security for Spectrum Sharing Systems", *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319-1329, Feb. 2017.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

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