Physical-Layer Security for Cognitive Radio Networks over Cascaded Rayleigh Fading Channels

Deemah H. Tashman and Walaa Hamouda
Department of Electrical and Computer Engineering
Concordia University, Montreal, Canada
Email: {d_tashma, hamouda}@ece.concordia.ca

GLOBECOM 2020 - 2020 IEEE Global Communications Conference | 978-1-7281-8298-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/GLOBECOM42002.2020.9348134

***Abstract*—In this paper, physical-layer security (PLS) for an underlay cognitive radio network (CRN) over cascaded Rayleigh fading channels is studied. The underlying cognitive radio system consists of a secondary source transmitting to a destination over a cascaded Rayleigh fading channel. An eavesdropper is attempting to intercept the confidential information of the secondary users (SUs) pair. The secrecy is studied in terms of three main security metrics, which are the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (P_{rnzc}), and the intercept probability (P_{int}). The effects of the path loss and the variation of the distances from the SU transmitter over the secrecy are also analyzed. Results reveal the great effect of the cascade level over the system secrecy. In addition, the effect of varying the interference threshold that the PU receiver can tolerate over the secrecy of the SUs pair is studied. The effect of the channel model parameters of both the main and the wiretap channels is investigated using both simulation and analytical results.**

***Index Terms*—Cascaded fading channels, physical-layer security, underlay cognitive radio networks.**

I. Introduction

COGNITIVE radio networks (CRNs) have emerged as a solution for the spectrum under-utilization issue that is caused by the static spectrum allocation. This issue is growing with the increased demand over the spectrum usage in 5G with the increase in the number of connected devices. CRN helps to opportunistically utilize the frequency bands that are not used by the licensed users [1]. In CRN, the unlicensed users, also called secondary users (SUs) share their information over three different methods; underlay, overlay, and interweave [2], [3]. For the underlay CRN type, the secondary users are allowed to share their transmission over the primary users (PUs) bands simultaneously with the transmission of the PUs. This is under the condition that the SUs transmission power does not exceed a threshold level that is tolerated by the PUs receivers to avoid harmful interference over the licensed users (primary users) transmissions [3].

Due to the broadcast nature of wireless communications, security on the physical layer is a challenging issue. Specifically, for underlay CRN, SUs should continuously sense the PUs transmission and accordingly adapt the transmitting power to ensure that no harm is done over the PUs communication [4]. Hence, attacks such as eavesdropping cannot be prevented when the eavesdroppers exist inside the region of the transmission of SUs or PUs. Therefore, it is necessary to search for methods for securing CRNs against such attacks. Physical-layer security (PLS) has been a promising solution for systems security analysis and enhancement [5]. PLS is based on the idea that enhancing the conditions of the link between the legitimate ends relative to the link between the transmitter and the eavesdropper helps guaranteeing security [6].

Recently, there has been an interest in studying the effect of cascaded fading channels over the secrecy of communication systems. Cascaded fading channel modeling is based on the idea that the channel gain at the receiver end is generated by the multiplication of a large number of rays reflected from the scatters in the path. These rays are represented by random variables that are independent but not necessarily identically distributed. For instance, PLS was studied assuming cascaded $\alpha-\mu$ fading channels in [7] and cascaded κ-μ fading channels in [8]. In addition, cascaded Nakagami-m fading channels were used to study the PLS of a system in [9] and [10]. Cascaded fading channels are important to model channels for different communication systems, such as mobile-to-mobile/vehicle-to-vehicle (M2M/V2V) transmission channels [11], multi-hop relaying systems [9], and keyhole channels for multiple-input-multiple-output (MIMO) systems [12]. Previous works for CRNs have considered the well-known fading channels assumed for all the links to study the PLS. However, no work has considered the effect of cascaded channels over the security of CRNs.

There have been some works in analyzing and enhancing the security of underlay CRNs. In [13], PLS has been studied for an underlay CRN over Rayleigh fading channels in terms of the secrecy outage probability (SOP) and the probability of non-zero secrecy capacity with a multi-antenna legitimate receiver. Results reveal that the secrecy can be improved as the number of antennas increases. PLS analyses have been performed in [14] for a single-input-multiple-output (SIMO) underlay CRN in terms of SOP. Moreover, PLS has been studied for a MIMO underlay CRN in [15] over Nakagami-m fading channels and in [16] over Rayleigh fading channels in terms of the SOP and with the existence of multi-antenna eavesdropper. Moreover, in [17], PLS

978-1-7281-8298-8/20/$31.00 ©2020 IEEE

has been studied for an underlay CRN, where the SU transmitter is equipped with multiple antennas and the SU receiver and the eavesdroppers are equipped with a single antenna over Rayleigh fading channels. Outdated channel state information (CSI) was considered in [17] and in the presence of multiple primary users. In [18], secrecy was studied in terms of the intercept probability with the existence of multiple PUs over Rayleigh fading channels.

To the best of our knowledge, no work considered studying the effect of cascaded fading channels over the PLS of CRNs. Motivated by this, we focus on studying the PLS of a pair of SUs in an underlay CRN. The system model consists of a PU receiver and an eavesdropper attempting to overhear the confidential information transmitted between the SUs through the wiretap channel (the link between the SU transmitter and the eavesdropper). The main channel (the link between the SUs pair) is assumed to follow the cascaded Rayleigh fading, while the wiretap channel and the channel between the SU transmitter and the PU receiver both follow single Rayleigh fading model. Assuming that the main channel follows the cascaded Rayleigh fading model while the wiretap channel follows a single Rayleigh fading is a valid assumption to study the secrecy of the CRN in its worst cases. Moreover, the effect of varying the maximum tolerated interference threshold at the PU receiver over the security of the SUs transmission is studied. Given this system model, the secrecy is studied in terms of the SOP, the probability of non-zero secrecy capacity (P_{rnzc}), and the intercept probability (P_{int}).

The paper is organized as follows; the system model is presented in section II. Physical-layer security analyses are given in section III. Simulations and analytical results are presented in section IV. Finally, conclusions are given in section V.

II. System Model

In our model, we consider a pair of SUs (S, D), a PU receiver (P_R), and an eavesdropper (E) as shown in Fig. 1. We assume that the SU pair, the PU receiver, and the eavesdropper are equipped with a single antenna. The channel h_1 follows cascaded Rayleigh fading model, whereas h_2 and h_3 both follow single Rayleigh fading model. Considering an underlay cognitive radio channel sharing model, the transmitting power at S should be limited by a threshold (I_{th}) that the PU receiver (P_R) can tolerate. The PU transmitter is assumed to be located far away from the SUs pair and does not affect the SUs communication.

Let $h_1 = \prod_i^n x_i$, where x_i follows the Rayleigh channel model. The probability density function (PDF) of h_1 was derived based-on a transformed Nakagami-m distribution in [19] as

$$f_{h_1}(y) \quad = \quad \beta y^{\frac{2m}{n}-1} \exp\left(-\frac{m}{\Omega\sigma^{\frac{2}{n}}} y^{\frac{2}{n}}\right), \tag{1}$$

where n is the cascade level, $\beta = \frac{2\left(\frac{m}{\Omega}\right)^m}{n\Gamma(m)\sigma^{\frac{2m}{n}}}$, σ is the scale parameter of the distribution and $\sigma^2 = \prod_{i=1}^n \sigma_i^2$ for $i = 1, 2, \cdots, n$.

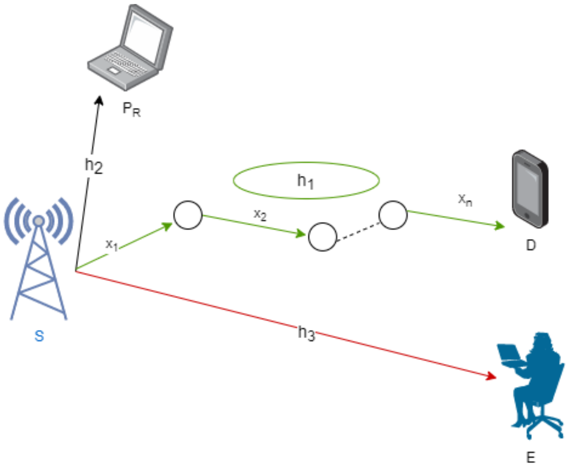

Fig. 1. The system model.

The values of m and Ω are calculated based on the following

$$\begin{aligned} m &= 0.6102n + 0.4263, \\ \Omega &= 0.8808n^{-0.9661} + 1.12. \end{aligned} \tag{2}$$

The PDF of the channel power gain $|h_2|^2$ with the corresponding coefficient λ_p can be expressed as

$$f_{|h_2|^2}(y) \quad = \quad \lambda_p \exp\left(-\lambda_p y\right). \tag{3}$$

The PDF of the channel power gain $|h_3|^2$ with the corresponding coefficient λ_e can be expressed as

$$f_{|h_3|^2}(y) \quad = \quad \lambda_e \exp\left(-\lambda_e y\right). \tag{4}$$

The received message at the SU destination (D) is given by

$$y_D = \sqrt{P_s} h_1 x_s + n_D, \tag{5}$$

where P_s is the transmit power at S, x_s is the transmitted symbol, and n_D is the additive-white-Gaussian-noise (AWGN) at the receiver D with zero mean and variance N_0. Moreover, the intercepted message at the eavesdropper E is given by

$$y_E = \sqrt{P_s} h_3 x_s + n_E, \tag{6}$$

where n_E is the AWGN at E with zero mean and variance N_0.

Given the cognitive underlay model, node S should make sure that the transmitting power (P_s) will not exceed an interference level (I_{th}) that the PU receiver P_R can tolerate as

$$P_s \leqslant \frac{I_{th}}{|h_2|^2}. \tag{7}$$

From (5)-(7), the instantaneous received signal-to-noise-ratios (SNRs) at D and E can be expressed, respectively, as

$$\gamma_D \quad = \quad \frac{I_{th} |h_1|^2}{N_0 |h_2|^2}, \tag{8}$$

$$\gamma_E \;=\; \frac{I_{th}\left|h_3\right|^2}{N_0\left|h_2\right|^2}\cdot \tag{9}$$

III. Physical-Layer Security Analysis

In this section, PLS will be studied in terms of the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (P_{rnzc}), and the intercept probability (P_{int}).

A. Secrecy outage probability

We assume that the eavesdropper (E) in the network is passive. Assuming passive eavesdropping states that the channel state information (CSI) of the eavesdropper is not available at the transmitter S [20]. Hence, there is a probability that the confidential information will be leaked to the eavesdropper through the wiretap channel. The most suitable secrecy metric to be used under these circumstances is the secrecy outage probability (SOP). SOP is defined as the probability that the achievable secrecy capacity falls below a predefined threshold and it can be expressed as

$$SOP = P_r(C_s \leqslant C_{th}), \tag{10}$$

where C_{th} is the target secrecy rate and C_s is the secrecy capacity and it is given by [21]

$$C_s = \begin{cases} C_D - C_E, & \text{if } \gamma_D > \gamma_E \\ 0, & \text{if } \gamma_D \leq \gamma_E \end{cases}, \tag{11}$$

where C_D and C_E are the capacities of the main and the wiretap channels, respectively. The channel capacities C_D and C_E are given, respectively, as

$$\begin{aligned} C_D &= \log_2\left(1+\gamma_D\right), \\ C_E &= \log_2\left(1+\gamma_E\right). \end{aligned} \tag{12}$$

Using (8)-(12) and after doing some mathematical manipulations, the secrecy outage probability can be expressed as

$$\begin{aligned} SOP &= P_r\left(\log_2(1+\gamma_D) - \log_2(1+\gamma_E) \leqslant C_{th}\right) \\ &= P_r\left(\frac{1+\frac{I_{th}|h_1|^2}{N_0|h_2|^2}}{1+\frac{I_{th}|h_3|^2}{N_0|h_2|^2}} \leqslant 2^{C_{th}}\right) \\ &= P_r\left(\frac{(\eta-1)\left|h_2\right|^2 + \eta\rho\left|h_3\right|^2}{\rho\left|h_1\right|^2} \geqslant 1\right), \end{aligned} \tag{13}$$

where $\rho = \frac{I_{th}}{N_0}$ and $\eta = 2^{C_{th}}$. Let $Y = \frac{(\eta-1)|h_2|^2+\eta\rho|h_3|^2}{\rho|h_1|^2}$, $Y_a = (\eta-1)\left|h_2\right|^2 + \eta\rho\left|h_3\right|^2$ and $Y_b = \rho\left|h_1\right|^2$. To find the secrecy outage probability, one needs to find the PDF of the random variable Y. Let $Y_a = A + B$, where $A = (\eta-1)\left|h_2\right|^2$ and $B = \eta\rho\left|h_3\right|^2$.

The PDF of A can be found using (3) as

$$f_A(x) \;=\; \frac{\lambda_p}{(\eta-1)}\exp\left(-\frac{\lambda_p x}{\eta-1}\right)\cdot \tag{14}$$

Using (4), the PDF of B can be given by

$$f_B(x) \;=\; \frac{\lambda_e}{\eta\rho}\exp\left(-\frac{\lambda_e x}{\eta\rho}\right)\cdot \tag{15}$$

Hence, the PDF of Y_a is given by

$$f_{Y_a}(y_a) \;=\; \int_0^{y_a} f_A(x) f_B(y_a - x)dx\cdot \tag{16}$$

Substituting (14) and (15) into (16), the pdf of the random variable Y_a can be expressed as

$$f_{Y_a}(y_a) = a_1\left(\exp\left(-\frac{\lambda_p y_a}{\eta-1}\right) - \exp\left(-\frac{\lambda_e y_a}{\eta\rho}\right)\right), \tag{17}$$

where $a_1 = \frac{\lambda_p\lambda_e}{\mu(\eta-1)(\eta\rho)}$ and $\mu = \left(\frac{\lambda_e}{\eta\rho} - \frac{\lambda_p}{\eta-1}\right)$. The PDF of Y_b cab be found using (1) as

$$f_{Y_b}(y_b) \;=\; \frac{\beta}{2\rho^{\frac{m}{n}}} y_b^{\frac{m}{n}-1}\exp\left(-\frac{m}{\rho^{\frac{1}{n}}\Omega\sigma^{\frac{2}{n}}} y_b^{\frac{1}{n}}\right)\cdot \tag{18}$$

Also, the PDF of Y can be found using the following

$$f_Y(y) \;=\; \int_0^{\infty} y_b f_{Y_a}(y y_b) f_{Y_b}(y_b) dy_b\cdot \tag{19}$$

Using (17), (18), and [22, eq. (2.24.3.1)] and with some mathematical manipulations, (19) can be expressed as

$$\begin{aligned} f_Y(y) = {}& a_3 c_1 y^{\frac{-m}{n}-1} G_{1\ n}^{n\ 1}\left(\left.\begin{matrix} \frac{-m}{n} \\ 0, \frac{1}{n}, \cdots, \frac{n-1}{n} \end{matrix}\right| \frac{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^n}{\rho n^n \frac{\lambda_p y}{\eta-1}}\right) - a_3 \\ & \times c_2 y^{\frac{-m}{n}-1} \\ & \times G_{1\ n}^{n\ 1}\left(\left.\begin{matrix} -\frac{m}{n} \\ 0, \frac{1}{n}, \cdots, \frac{n-1}{n} \end{matrix}\right| \frac{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^n}{\rho n^n y\left(\frac{\lambda_e}{\eta\rho}\right)}\right), \end{aligned} \tag{20}$$

where $a_3 = \frac{a_1\beta}{2\rho^{\frac{m}{n}}}$, $c_1 = \frac{\sqrt{n}\left(\frac{\lambda_p}{\eta-1}\right)^{\frac{-m}{n}-1}}{(2\pi)^{\frac{n-1}{2}}}$, and $c_2 = \frac{\sqrt{n}\left(\frac{\lambda_e}{\eta\rho}\right)^{-\frac{m}{n}-1}}{(2\pi)^{\frac{n-1}{2}}}$.

Given (13) and (20), the secrecy outage probability can be represented as

$$\begin{aligned} SOP &= P_r\left(Y \geqslant 1\right) \\ &= \int_1^{\infty} f_Y(y)dy\cdot \end{aligned} \tag{21}$$

Substituting (20) into (21) and using [23, eq. (26)] with some mathematical manipulations, the SOP can be expressed as

$$SOP \;=\; 1 - \left[S_1 - S_2\right], \tag{22}$$

where

$$S_1 = a_3 c_1 G_{n+1\ \ 2}^{\ \ 1\ \ \ n+1}\left(\left.\begin{matrix} 1, \frac{n-1}{n}, \cdots, \frac{1}{n}, 1+\frac{m}{n} \\ 1+\frac{m}{n}, \frac{m}{n} \end{matrix}\right| \frac{\rho n^n \frac{\lambda_p}{\eta-1}}{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^n}\right) \tag{23}$$

and

$$S_2 = a_3 c_2 G\,{}^{1\;\;n+1}_{n+1\;\;2}\left({}^{1,\frac{n-1}{n},\cdots,\frac{1}{n},1+\frac{m}{n}}_{1+\frac{m}{n},\frac{m}{n}} \middle| \frac{n^n\left(\frac{\lambda_e}{\eta}\right)}{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^n} \right). \tag{24}$$

B. Probability of non-zero secrecy capacity

A secrecy performance metric that is commonly used to study the security of the SUs network is the probability of non-zero secrecy capacity (P_{rnzc}). P_{rnzc} is defined as the probability that the secrecy capacity is positive. In other words, it is the probability that the main channel capacity is larger than the wiretap channel capacity and is given by

$$\begin{aligned} P_{rnzc} &= P_r\left(C_s > 0\right) \\ &= 1 - P_r\left(C_s \leqslant 0\right) \\ &= 1 - P_r\left(\frac{1+\frac{\rho|h_1|^2}{|h_2|^2}}{1+\frac{\rho|h_3|^2}{|h_2|^2}} \leqslant 1\right) \\ &= 1 - P_r\left(|h_1|^2 \leqslant |h_3|^2\right) \\ &= 1 - \int_0^\infty F_{|h_1|^2}(x) f_{|h_3|^2}(x)dx. \end{aligned} \tag{25}$$

In order to evaluate the probability of non-zero secrecy capacity, one needs to find the cumulative distribution function (CDF) of the channel power gain $|h_1|^2$, which can be found using (1), [24, eq. (3.381.3)] and with some mathematical manipulations as

$$F_{|h_1|^2}(x) = 1 - \frac{n\beta\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{-m}}{2}(m-1)!\exp\left(-\frac{m}{\Omega\sigma^{\frac{2}{n}}}x^{\frac{1}{n}}\right) \\ \times \sum_{j=0}^{m-1}\frac{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^j}{j!}x^{\frac{j}{n}}. \tag{26}$$

Using (26) and (4), (25) can be solved as [22, eq. (2.24.3.1)]

$$P_{rnzc} = \sum_{j=0}^{m-1} q\lambda_e^{\frac{-j}{n}} G\,{}^{n\;1}_{1\;n}\left({}^{-\frac{j}{n}}_{0,\frac{1}{n},\cdots,\frac{n-1}{n}} \middle| \frac{\left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^n}{n^n\lambda_e} \right), \tag{27}$$

where $q = \left(\frac{m}{\Omega\sigma^{\frac{2}{n}}}\right)^{-m+j}\frac{n\sqrt{n}\beta(m-1)!}{2j!(2\pi)^{\frac{n-1}{2}}}$.

C. Intercept probability

Intercept probability is one of the useful concepts used to measure the secrecy level of the system, which occurs when the condition of the wiretap channel is better than the main channel condition. This renders the secrecy capacity below zero [25], i.e., most probably the eavesdropper will be able to intercept the confidential information. The intercept probability can be expressed as

$$\begin{aligned} P_{int} &= P_r\left(C_s < 0\right) \\ &= P_r\left(|h_1|^2 < |h_3|^2\right) \\ &= \int_0^\infty F_{|h_1|^2}(x) f_{|h_3|^2}(x)dx \\ &= 1 - P_{rnzc}. \end{aligned} \tag{28}$$

IV. Numerical Results

In this section, analytical results are presented with Monte-Carlo simulations. A perfect match can be noticed between the analytical and the simulation results. To take the path loss effect over the secrecy into consideration, we assume that the transmitter represents the reference location. That is S is located at $(0,0)$ and the other nodes $(D, E, \text{and } P_R)$ are of different distances from S as shown in Fig. 2. Assume $d_{MN}^{-PL} = \frac{1}{2\lambda_J}$, where PL is the path loss exponent, $M \in \{S, d_1, d_2, d_3\}$, $N \in \{P_R, E, d_1, d_2, d_3, D\}$, and $J \in \{e, s, p\}$. $\lambda_s = \frac{1}{2\sigma^2}$ and d_{MN} represents the distance from node M to node N in meters (m). $d_1, d_2,$ and d_3 are the locations of the first, second, and third obstacle in the main channel, respectively. This is to notice the effect of the cascade level between S and D.

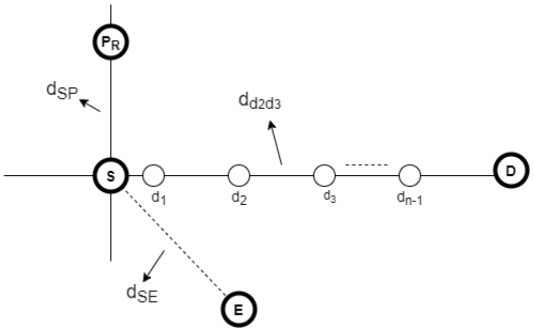

Fig. 2. A representation of the distances between nodes.

Fig. 3 presents the secrecy outage probability versus the interference threshold ρ for different distances between the SU transmitter (S) and the eavesdropper (E), (d_{SE}). One can notice that as the eavesdropper becomes closer to the transmitter S (d_{SE} reduces), there is a higher probability that the wiretap channel's conditions improving, which implies better signal reception at the receiver. That is, the secrecy degrades as the capability of the eavesdropper to intercept the information improves. Moreover, as the interference threshold (ρ) increases, the secrecy improves as the transmitter can enhance the transmitting power. In addition, one can notice that regardless of the distance between S and E, all SOP curves saturate at high values of the threshold level (ρ). This is because as ρ increases to very high values, the system undergoes a non-cognitive state as the limit over the transmit power is ignored and the transmitting power at S can take its maximum value. This can be noticed by setting the threshold ρ to ∞ in (13).

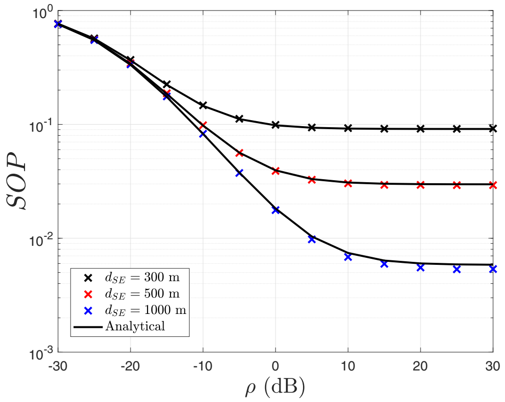

Fig. 3. The secrecy outage probability (SOP) versus the interference level (ρ) for different distances between the transmitter S and the eavesdropper E, (d_{SE}). $d_{SP} = 500$ m, $d_{Sd_1} = 10$ m, $d_{d_1D} = 10$ m, $C_{th} = 0.7$ bit/sec/Hz, $PL = 3$, and $n = 2$.

Fig. 4 shows the secrecy outage probability as a function of the target secrecy rate (C_{th}) for different values of the interference threshold (ρ) and for a cascade level $n = 3$. One can notice that when the target secrecy rate increases, the overall achieved system secrecy becomes poorer. Furthermore, the results reveal that the gap between the SOP curves for different values of the interference threshold ρ for low values of C_{th} is lower than the gap for high values of C_{th}. That is, the effect of decreasing the interference level at the PU receiver (P_R) can be reduced for low values of the target secrecy rate.

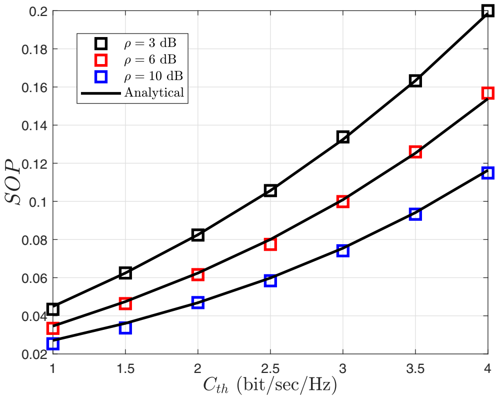

Fig. 4. The secrecy outage probability (SOP) versus the target secrecy rate (C_{th}) for different values of the interference threshold ρ. $n = 3$, $d_{SP} = 500$ m, $d_{SE} = 1000$ m, $PL = 3$, $d_{Sd_1} = 5$ m, $d_{d_1d_2} = 5$ m, and $d_{d_2D} = 5$ m.

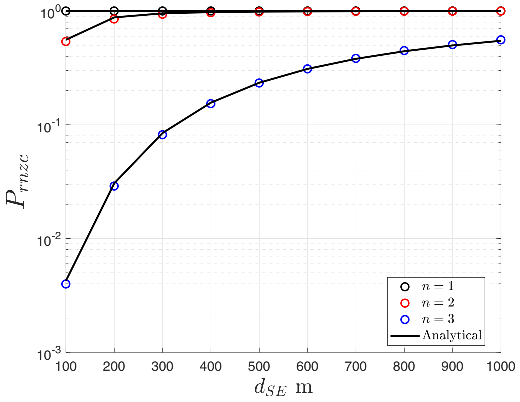

Fig. 5. The probability of non-zero secrecy capacity (P_{rnzc}) versus the distance between S and E, (d_{SE}) for several values of cascade level (n). $PL = 3$, $d_{Sd_1} = 10$ m, $d_{d_1d_2} = 10$ m, and $d_{d_2D} = 10$ m.

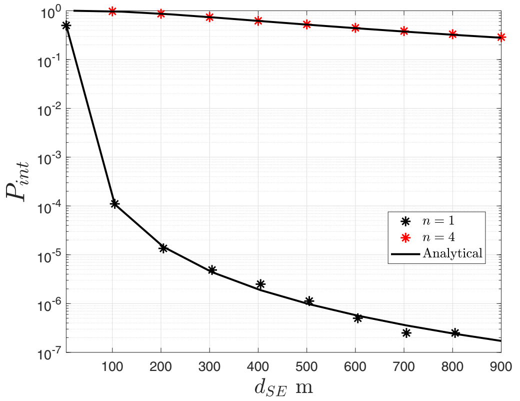

Fig. 6. The intercept probability versus the distance between S and E, (d_{SE}) for single and cascaded Rayleigh fading channels. $PL = 3$, $d_{Sd_1} = 5$ m, $d_{d_1d_2} = 5$ m, $d_{d_2d_3} = 5$ m, and $d_{d_3D} = 5$ m.

Fig. 5 represents the effect of the cascade level n, i.e., the number of keyholes in the channel, over the probability of non-zero secrecy capacity (P_{rnzc}). We assume that the distance from the transmitter S to the next object blocking the path to D (d_{Sd_1}) equals the distance between the node d_1 to d_2 $(d_{d_1d_2})$ and also the distance between node d_2 and the final destination D (d_{d_2D}). It can be noticed that as the distance between S and E increases, the system becomes more robust against this passive eavesdropping. This occurs because the received SNR reduces as the eavesdropper moves away from the transmitting node S, which results in a degradation in the strength of the signal received at the eavesdropper E as well as in the ability of E to intercept and decode the information correctly. Furthermore, as the cascade level n increases, the secrecy degrades since more severe fading conditions emerge as the level of the cascade (the number of keyholes) rises. Moreover, one can notice that the gap between the curves of the probability of non-zero secrecy capacity for a closer eavesdropper E is wider than the gap when d_{SE} gets larger. That is, the effect of the cascade level at the main channel can be reduced as d_{SE} increases.

Fig. 6 shows the effect of the cascade degree of the main channel over the intercept probability for a single $(n = 1)$ and a cascaded Rayleigh fading channels $(n = 4)$. It can be observed that for a single Rayleigh fading channel, when $d_{SE} \geq 300$ m, the communication secrecy is considered to be acceptable. However, if the eavesdropper is at distance $d_{SE} < 300$, the probability that the eavesdropper can intercept and decode the confidential information correctly increases. On the other hand, when the main channel becomes poorer for higher cascade levels as shown for $n = 4$, the secrecy is significantly affected.

V. Conclusions

Physical-layer security for an underlay cognitive radio network over cascaded Rayleigh fading channels is studied. The secrecy is studied in terms of the secrecy outage probability, the probability of non-zero secrecy capacity, and the intercept probability. It is proved that increasing the number of scatters (cascade level) in the main channel degrades the system secrecy as the fading becomes more severe. Moreover, the security is highly affected by the change of the eavesdropper location from the SU transmitter. That is, the secondary users security can be highly degraded when the distance between the transmitter S and the eavesdropper E is short. We have shown that the effect of the interference threshold can be reduced for low values of the target secrecy rate. A perfect match between the analytical and simulation results can be noticed, which proves that the considered system model and the analyses can be used well to model different system models channels, such as M2M/V2V communications and multi-hop relaying systems.

References

[1] Ridhima and A. Singh Buttar, “Fundamental Operations of Cognitive Radio: A Survey,” in *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, India, 2019, pp. 1–5.

[2] A. Sharmila and P. Dananjayan, “Spectrum Sharing Techniques in Cognitive Radio Networks – A Survey,” in *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, India, India, 2019, pp. 1–4.

[3] M. El Tanab and W. Hamouda, “Resource Allocation for Underlay Cognitive Radio Networks: A Survey,” *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1249–1276, Secondquarter 2017.

[4] M. Bouabdellah, F. E. Bouanani, D. B. da Costa, P. C. Sofotasios, H. Bcn-Azza, K. Mezher, and S. Muhaidat, “On the Secrecy Analysis of Dual-Hop Underlay Multi-Source CRNs with Multi-Eavesdroppers and a Multi-Antenna Destination,” in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, Rabat, Morocco, Morocco, April 2019, pp. 1–7.

[5] J. M. Moualeu, W. Hamouda, and F. Takawira, “Secrecy Performance of Generalized Selection Diversity Combining Scheme with Gaussian Errors,” in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, Chicago, IL, USA, 2018, pp. 1–5.

[6] L. H. Ozarow and A. D. Wyner, “Wire-tap channel II,” *AT&T Bell Laboratories technical journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[7] L. Kong, G. Kaddoum, and D. B. da Costa, “Cascaded α-μ fading channels: Reliability and security analysis,” *IEEE Access*, 2018.

[8] D. H. Tashman, W. Hamouda, and I. Dayoub, “Secrecy Analysis Over Cascaded $\kappa - \mu$ Fading Channels With Multiple Eavesdroppers,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8433–8442, 2020.

[9] S. Ö. Ata, “Secrecy performance analysis over cascaded fading channels,” *IET Communications*, vol. 13, no. 2, pp. 259–264, 2018.

[10] R. Singh and M. Rawat, “Unified Analysis of Secrecy Capacity Over N $*$ Nakagami Cascaded Fading Channel,” in *2018 18th International Symposium on Communications and Information Technologies (ISCIT)*. IEEE, 2018, pp. 422–427.

[11] B. Talha and M. Pätzold, “Channel Models for Mobile-to-Mobile Cooperative Communication Systems: A State of the Art Review,” *IEEE Vehicular Technology Magazine*, vol. 6, no. 2, pp. 33–43, June 2011.

[12] A. Kaur and J. Malhotra, “Cascade Fading Channel Models for Wireless Communication-A Survey,” *International Journal of Computer Applications*, vol. 89, no. 14, pp. 22–25, 2014.

[13] H. Zhao, H. Liu, Y. Liu, C. Tang, and G. Pan, “Physical layer security of maximal ratio combining in underlay cognitive radio unit over Rayleigh fading channels,” in *2015 IEEE International Conference on Communication Software and Networks (ICCSN)*, Chengdu, China, June 2015, pp. 201–205.

[14] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, “On the Security of Cognitive Radio Networks,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3790–3795, Aug 2015.

[15] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, “Secrecy Outage Performance of Transmit Antenna Selection for MIMO Underlay Cognitive Radio Systems Over Nakagami-m Channels,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2237–2250, March 2017.

[16] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, “Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 236–10 242, Dec 2016.

[17] S. Chetry and A. Singh, “Physical Layer Security of Outdated CSI Based CRN,” in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bangalore, India, July 2018, pp. 1–5.

[18] A. Singh, M. R. Bhatnagar, and R. K. Mallik, “Physical Layer Security of a Multiantenna-Based CR Network With Single and Multiple Primary Users,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 11 011–11 022, 2017.

[19] H. Lu, Y. Chen, and N. Cao, “Accurate approximation to the PDF of the product of independent Rayleigh random variables,” *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 1019–1022, 2011.

[20] J. M. Moualeu, P. Sofotasios, D. Benevides, S. Muhaidat, W. Hamouda, and U. Dias, “Physical-Layer Security of SIMO Communication Systems over Multipath Fading Conditions,” *IEEE Trans. Sustainable Comput.*, pp. 1–1, 2019.

[21] M. Kamel, W. Hamouda, and A. Youssef, “Physical Layer Security in Ultra-Dense Networks,” *IEEE Wireless Communications Letters*, vol. 6, no. 5, pp. 690–693, 2017.

[22] A. Prudnikov, Y. Brychkov, and O. Marichev, “Integrals Series: More Special Functions, Volume III of Integrals and Series,” *New York: Gordon and Breach Science Publishers*, 1990.

[23] V. Adamchik and O. Marichev, *The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system*, 1990.

[24] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2007.

[25] M. Bouabdellah, F. E. Bouanani, P. C. Sofotasios, D. B. da Costa, H. Benazza, K. Mezher, and S. Muhaidat, “Intercept Probability of Underlay Uplink CRNs with Multi-Eavesdroppers,” in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, Turkey, 2019, pp. 1–6.