Secrecy Outage Probability in Cognitive Radio Networks Subject to Rayleigh Fading Channels

Mounia Bouabdellah [1] , Faissal El Bouanani [1] , Hussain Ben-azza [2]
[1] ENSIAS, Mohammed V University in Rabat, Morocco
[2] ENSAM, Moulay Ismail University in Meknes, Morocco
Emails: mounia_bouabdellah@um5.ac.ma, f.elbouanani@um5s.net.ma, hbenazza@yahoo.com

***Abstract*—Wireless communication systems are vulnerable to eavesdropping attack in which the attacker overhear the transmitted data in the network. Hence, the physical-layer security is of utmost importance to protect the wireless communications against the eavesdropping attack. In this paper, we study the physical-layer security of a two-hops cognitive radio-based communication system where the secondary user sends some confidential information to a destination through a relay. This relay is assumed to be equipped with multiple antennas for reception, applies the maximum-ratio combining technique for the received signals, and uses only one antenna to forward the combined signal to the destination. The transmission is performed under the eavesdropper's attempt to listen to the communication channel. The secrecy outage probability and the intercept probability are both derived based on the statistical characteristics of the channels and under the constraint of avoiding the communication outage of the primary user. All results have been validated using Monte Carlo method.**

***Index Terms*—Cognitive radio networks, physical layer security, secrecy outage probability, intercept probability, maximum ratio combining.**

I. Introduction

With the proliferation of mobile devices, the demand for wireless radio has increased which leads to a spectrum scarcity problem. As the static spectrum allocation technique is unable to solve this issue, cognitive radio (CR) has been proposed to allow a dynamic spectrum access and increase the efficiency of spectrum utilization. In cognitive radio networks (CRN), unlicensed users, also called secondary users (SUs), share the licensed spectrum bands with primary users (PUs) [1], [2]. Indeed, the SUs sense the spectrum in order to determine the availability of unused bands and opportunistically use them without causing any harmful interference to the PUs signals.

Like any traditional wireless network, CRN can be vulnerable to several attacks that can disrupt their operation [3]. Eavesdropping attack is one of the security threats that can occur at the physical layer. Therein, unauthorized users try to listen to the communication between legitimate users. Thus, under the constraint of eavesdropping risks as well as the potential interference to PU communication, the SUs have to adjust their transmission powers in order to avoid these risks. The physical layer security in the context of CRN has been studied in [4]-[9]. Most of these research papers focused on the direct transmission between the SU source and the SU destination. However, few papers considered the case of a cooperative transmission in which the data is transmitted from a source node to a destination through relays.

In the direct transmission, the source node sends directly the confidential messages to the destination without relying on any intermediate nodes. Hence, this type of communication system assumes that the transmitter, the receiver, and the eavesdropper are in the same transmission range. The secrecy outage probability (SOP) for CR communication system over Nakagami-*m* fading channels were derived in [4]-[6]. In [5], the authors assumed that the source uses one antenna for transmission and both the destination and the eavesdropper use one antenna for reception. In addition to the SOP, the authors derived also the probability of non- zero secrecy capacity (PNSC). A communication system consisting of an SU source node, a legitimate SU receiver, and an eavesdropper that are equipped all with multiple antennas is studied in [4]. The generalized selection combining scheme has been used to combine the multiple copies of signals. In [6], both the receiver and the eavesdropper are supposed to be equipped with multiple antennas, while the transmitter uses a single antenna. The SOP of a system consisting of a transmitter, receiver, and eavesdropper equipped with a single antenna under Rayleigh and log-normal fading channels has been investigated in [8]. In [7], the studied CR communication system consists of primary and secondary transmitters that are equipped with single antenna whereas the primary and secondary receivers use multiple antennas. The communication is performed in the presence of two eavesdroppers, one is overhearing the communication of the primary network whereas the second is listening to the communication of the secondary network. The SOP, in this case, has been derived under the Rayleigh fading channels.

However, direct transmission is not always practical in wireless networks. Hence, the cooperative communication seems to be an efficient solution when no direct communication link exists between the source and the destination [10]. The SOP of two-hops CR cooperative communication system was derived under the Rayleigh fading channels in [9] by taking into consideration the self-interference at the relays. Such system consists of a single SU source that communicates with a unique destination through multiple SU relays in the presence of PUs and one eavesdropper that is assumed to be listening to both communication hops.

In this paper, we investigate the SOP as well as the intercept

978-1-5386-4609-0/18/$31.00

probability over Rayleigh fading channels for two-hops CR communication system in which the data transmitted by an SU source node is forwarded to the destination through an SU relay under the malicious attempt of a single eavesdropper. In this scheme, we assume that the relay performs the maximum-ratio combining (MRC) technique at the reception and uses one antenna to forward the message to the final destination. To the best of our knowledge, none of the existing work studied the case of a CR-based communication system with a relay node equipped with multiple antennas.

The remainder of this paper is organized as follows. In Section II we derive the secrecy outage probability and the intercept probability of the studied system. In Section III, we discuss the numerical and simulation results. Finally, in Section IV, we give a brief conclusion.

II. Methodology

In this paper, we are considering the CR-based system represented in Fig.1. It consists of a two-hops communication system in which one SU source node S is transmitting data to an SU destination node D through an SU relay R under the eavesdropping attempt of E. For simplicity, the eavesdropper is assumed to be equipped with only one antenna. In the first transmission hop, the relay receives the signal on its n branch MRC combiner. In the second transmission hop, the relay R uses only one antenna to forward the data to the destination. During the data transmission, the PU P_{Rx} can be subjected to the interference signals coming from both S and R. Hence, the data transmitted from S to D through R should not cause any harmful interference at the PU receiver. Thus, the node S and the relay R have to adjust their transmission powers in order to satisfy the PUs' quality of service. The transmission powers P_S and P_R of both nodes S and R are adapted to the channel conditions and their expressions are given, respectively, by [9]

$$P_S = \frac{P_P \lambda_{SP}}{\gamma_{Pth} \lambda_P} \left[\frac{1}{1 - \frac{\varepsilon}{2}} exp\left(-\frac{\gamma_{Pth} \lambda_P}{\alpha} \right) - 1 \right], \quad (1)$$

$$P_R = \frac{P_P \lambda_{RP}}{\gamma_{Pth} \lambda_P} \left[\frac{1}{1 - \frac{\varepsilon}{2}} exp\left(-\frac{\gamma_{Pth} \lambda_P}{\alpha} \right) - 1 \right], \quad (2)$$

where $\alpha = \frac{P_P}{N}$, $0 < \varepsilon < 1$ is the desired outage probability for the link $P_{Tx} \rightarrow P_{Rx}$, and γ_{Pth} is the threshold value of the signal-to-noise ratio (SNR). If the SNR of the primary receiver is less than γ_{Pth}, then a communication outage is occurring.

Without loss of generality, the communication between the transmitters and the receivers is assumed to be established in a non-line-of-sight environment, therefore, all links' fading amplitudes are Rayleigh distributed, i.e the channel coefficients of links $S \rightarrow R_k$, $R \rightarrow D$, $S \rightarrow E$, $R \rightarrow E$, $P_{Tx} \rightarrow P_{Rx}$, $R \rightarrow P_{Rx}$, $S \rightarrow P_{Rx}$ are h_{SR_k}, h_{RD}, h_{SE}, h_{RE}, h_P, h_{RP}, h_{SP}, respectively. For simplicity, we write the channel power gains as $g_{SR_k} = |h_{SR_k}|^2$, $g_{RD} = |h_{RD}|^2$, $g_{SE} = |h_{SE}|^2$, $g_{RE} = |h_{RE}|^2$, $g_P = |h_P|^2$, $g_{RP} = |h_{RP}|^2$, $g_{SP} = |h_{SP}|^2$. We assume that all fading amplitudes are normalized. Thus, all coefficients λ_{SR_k}, λ_{RD}, λ_{SE}, λ_{RE}, λ_P, λ_{RP}, λ_{SP} of the exponential distribution are equal to one.

Moreover, each input signal at the relay arrives with a certain delay related to the one received by its first branch. As we set up MRC as our receiver, all these delays will be eliminated and the interference of these signals will be canceled as well. According to [11], the signal at the MRC output of the relay R can be expressed as

$$y_R = \sqrt{P_S} ||h_{SR}|| x_s + w_R n_R, \quad (3)$$

where P_S is the transmission power of S, h_{SR} denotes the $n \times 1$ channel vector from the SU source node to the relay R, x_s is the transmitted signal of S, and n_R stands for the additive white Gaussian noise (AWGN) $n \times 1$ channel vector whose entries have variance N and mean zero. The MRC weight vector is given by $w_R = \frac{h_{SR}^{\dagger}}{||h_{SR}||}$, the symbol $\dagger$ denotes the transpose conjugate.

The received signal at the destination D is given by

$$y_D = \sqrt{P_R} h_{RD} x_r + n_D, \quad (4)$$

where P_R is the transmission power of R, x_r is the transmitted signal of R after performing the relaying technique, and n_D is the AWGN of mean zero and variance N.
The received signals at the eavesdropper from the source and from the relay are, respectively, written as

$$y_{1E} = \sqrt{P_S} h_{SE} x_s + n_E, \quad (5)$$

$$y_{2E} = \sqrt{P_R} h_{RE} x_r + n_E, \quad (6)$$

where n_E is the additive noise assumed to be AWGN of variance N_E and mean zero.

In what follows, we are interested in deriving the secrecy capacity, the secrecy outage probability, and the intercept probability of the system under the constraint of avoiding, as possible, the interference at the PU receiver.

A. Secrecy capacity

The secrecy capacity of the communication system in which the eavesdropper E is trying to listen to both transmission hops can be expressed as

$$C_S = \min(C_{S1}, C_{S2}), \quad (7)$$

where C_{S1} and C_{S2} are the secrecy capacities at the first and second hop, respectively. These secrecy capacities can be written as

$$C_{S1} = \log_2(\gamma_1), \quad (8)$$

$$C_{S2} = \log_2(\gamma_2), \quad (9)$$

where

$$\gamma_1 = \frac{1 + \gamma_R}{1 + \gamma_{1E}}. \quad (10)$$

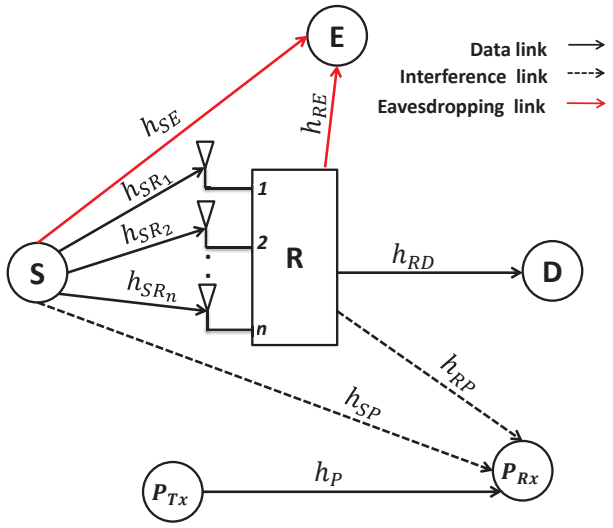

Fig. 1. The studied CRN system model.

and

$$\gamma_2 = \frac{1+\gamma_D}{1+\gamma_{2E}}. \tag{11}$$

Hence, the secrecy capacity of the system can be written as

$$C_s = \log_2\left(\min[\gamma_1, \gamma_2]\right). \tag{12}$$

On the other hand, the combined SNR at the relay R can be written as

$$\gamma_R = \sum_{k=1}^{n} \gamma_{k,R}, \tag{13}$$

while the SNR at the destination D is

$$\gamma_D = \frac{P_R g_{RD}}{N}, \tag{14}$$

By substituting the transmission power P_P of the PU in the equations (13) and (14), the SNR at the relay R and the destination D can be, respectively, expressed as:

$$\gamma_R = \sum_{k=1}^{n} \frac{P_S}{P_P} \alpha g_{SR_k}, \tag{15}$$

$$\gamma_D = \frac{P_R}{P_P} \alpha g_{RD}, \tag{16}$$

where $\alpha = \frac{P_P}{N}$. We refer the reader to [9] for the detailed expressions of P_S and P_R.

Finally, the SNRs at the eavesdropper from the source S and the relay R are γ_{1E} and γ_{2E}, respectively and are expressed as follows

$$\gamma_{1E} = \frac{P_S g_{SE}}{N_E}. \tag{17}$$

$$\gamma_{1E} = \frac{P_R g_{RE}}{N_E}. \tag{18}$$

B. Secrecy outage probability

The SOP is an important metric that is used to evaluate the security performance and it consists of the probability that the secrecy capacity C_S falls below a predefined security rate R_s.

$$SOP = Pr\left(C_S < R_s\right), \tag{19}$$

By using equation (12), the SOP can be written as:

$$\begin{aligned} SOP(\gamma) &= Pr\left(\min[\gamma_1, \gamma_2] < \gamma\right) \\ &= 1 - Pr\left(\gamma_1 > 2^R\right).Pr\left(\gamma_2 > \gamma\right) \\ &= 1 - \left[1 - F\gamma_1(\gamma)\right]\left[1 - F\gamma_2(\gamma)\right], \end{aligned} \tag{20}$$

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

From Eq. (20), we see that to obtain the SOP of the considered system we need to derive $F\gamma_1(\gamma)$ and $F\gamma_2(\gamma)$.

By using Eq. (10) the CDF of γ_1 can be written as

$$\begin{aligned} F\gamma_1(\gamma) &= Pr\left(\frac{1+\gamma_R}{1+\gamma_{1E}} < \gamma\right) \\ &= Pr\left(\gamma_R < \gamma(1+\gamma_{1E}) - 1\right), \end{aligned} \tag{21}$$

According to [13], the Eq. (21) can be written as

$$F\gamma_1(\gamma) = \int_0^{\infty} F_{\gamma_R}(\gamma(1+y) - 1) f_y(y) dy, \tag{22}$$

where $y = \gamma_{1E}$.

From Eq. (22), we notice that to calculate $F\gamma_1(\gamma)$, we have to calculate first the CDF of γ_R which can be computed according to [13] as follows

$$F_{\gamma_R}(x) = \left(\frac{1}{\prod_{i=1}^{n} \overline{\gamma}_{i,R}}\right) \sum_{j=1}^{n} \frac{1 - e^{-\frac{1}{\overline{\gamma}_{j,R}} x}}{\frac{1}{\overline{\gamma}_{j,R}} \prod_{k=1, k\neq j}^{n} \left(\frac{1}{\overline{\gamma}_{k,R}} - \frac{1}{\overline{\gamma}_{j,R}}\right)}. \tag{23}$$

Hence, using Eq. (23) the CDF of γ_1 is derived in Eq. (26), as it is shown in the top of the next page.

The CDF of γ_2 is expressed as follows

$$\begin{aligned} F\gamma_2(\gamma) &= Pr\left(\frac{1+\gamma_D}{1+\gamma_{2E}} < \gamma\right) \\ &= \int_0^{\infty} F_{\gamma_D}\left(\gamma(1+z) - 1\right) f_z(z) dz, \end{aligned} \tag{24}$$

where $z = \gamma_{2E}$

$$F\gamma_2(\gamma) = 1 - \frac{\overline{\gamma}_D}{\overline{\gamma}_D + \gamma\overline{\gamma}_{2E}} e^{-\frac{1}{\overline{\gamma}_D}(\gamma-1)}. \tag{25}$$

C. Intercept probability

According to [12], when the channel capacity of the main link is less than that of the wiretap link, then the eavesdropper, in this case, most likely succeeds in decoding and intercepting the source message. Thus, an intercept event is considered to be occurring. The intercept probability consists of the

$$
\begin{aligned}
F\gamma_1(\gamma) &= \left(\frac{1}{\overline{\gamma}_{1E}\prod_{i=1}^{n}\overline{\gamma}_{i,R}}\right)\sum_{j=1}^{n}\frac{\overline{\gamma}_{j,R}}{\prod_{k=1,k\neq j}^{n}\left(\frac{1}{\overline{\gamma}_{k,R}}-\frac{1}{\overline{\gamma}_{j,R}}\right)}\int_0^{\propto}\left[e^{-\frac{1}{\overline{\gamma}_{1E}}y}-e^{-\left(\frac{1}{\overline{\gamma}_{j,R}}+\frac{1}{\overline{\gamma}_{1E}}\right)y-\frac{\gamma-1}{\overline{\gamma}_{j,R}}}\right]dy \\
&= \left(\frac{1}{\prod_{i=1}^{n}\overline{\gamma}_{i,R}}\right)\sum_{j=1}^{n}\frac{\overline{\gamma}_{j,R}\left(1-\frac{\overline{\gamma}_{j,R}}{\overline{\gamma}_{j,R}+\overline{\gamma}_{1E}\gamma}e^{-\frac{\gamma-1}{\overline{\gamma}_{j,R}}}\right)}{\prod_{k=1,k\neq j}^{n}\left(\frac{1}{\overline{\gamma}_{k,R}}-\frac{1}{\overline{\gamma}_{j,R}}\right)}.
\end{aligned}
\tag{26}
$$

probability when the secrecy capacity becomes non-positive and can be expressed as

$$
P_{int} = Pr(C_S < 0), \tag{27}
$$

By substituting the value of C_S given in Eq. (8) the intercept probability can be written as

$$
\begin{aligned}
P_{int} &= Pr(\log_2(\min[\gamma_1,\gamma_2]) < 0) \\
&= 1 - Pr\left(\gamma_1 > 1\right).Pr\left(\gamma_2 > 1\right) \\
&= 1 - \left[1 - F\gamma_1(1)\right]\left[1 - F\gamma_2(1)\right],
\end{aligned}
\tag{28}
$$

III. Results and Discussion

In this section, we present the analytical and simulation results for the considered communication system. We study the impact of the transmission power of the PU transmitter in terms of $\alpha = \frac{P_P}{N}$, the secrecy rate R_s, and the number of the relay's antennas on the secrecy outage probability for the SU transmission. The simulation has been performed by using the Monte Carlo method.

Fig.2 shows the secrecy outage probability as a function of the secrecy rate R_s for different values of the number of the relay's antennas. As one can see, the SOP increases with the increasing values of R_s. In other words, when a higher secrecy rate R_s is used by SUs for better throughput performance, it is less likely to achieve the perfect secure transmission against eavesdropping attacks. In addition and as expected, the SOP is less when using multiple antennas at the relay instead of a single antenna. For instance, for $R_s = 1$ bits/s, the SOP is almost equal to 0.78 when using only two antenna ($n = 2$) and 0.82 when using 4 antennas.

Fig. 3 illustrates the SOP as a function of α for different numbers of the relay antennas. As it is observed, this probability decreases with the increasing values of α. Moreover, it is clear that using multiple antennas at the relay improves the secrecy of the system. For instance for $\alpha = 40$ dB, the SOP is almost equal to 0.57 for $n = 2$ whereas for $n = 4$ the SOP is almost equal to 0.62.

Fig. 4 depicts the SOP as a function of ϵ for different numbers of the relay's antennas. As it is observed, the SOP has high values for the small values of ϵ. According to [9], ϵ is the desired outage probability for the link $P_{TX} \rightarrow P_{RX}$. In other words when ϵ is very small the transmission powers of the source S and relay R tend to be small which affect the secrecy performance of the system.

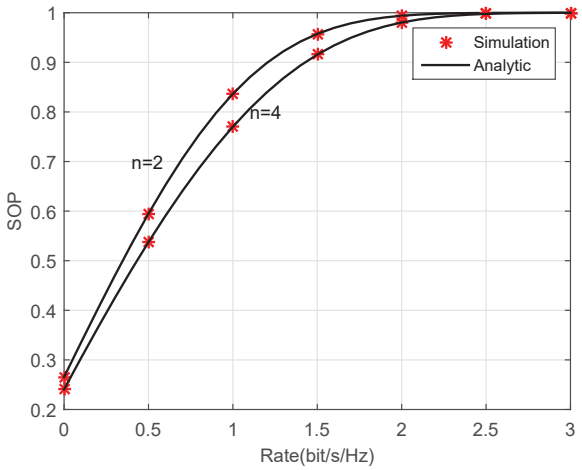

Fig. 2. Secrecy outage probability versus secrecy rate for $\gamma_P = 15$ dB and $\epsilon = 10^{-4}$

Fig. 5 shows the intercept probability as a function of α for different numbers of the relay's antennas. As one can see, the intercept probability decreases with increasing values of α and it becomes null once the PU's transmission power is high. Furthermore, using multiple antennas at the relay enhance the secrecy of the system as the intercept probability tends to be smaller than the case of using a relay with a single antenna.

IV. Conclusion

In this paper, we studied the physical layer security in CRN where the data transmission from an SU source to an SU destination through an SU relay is under the risk of eavesdropping attack and under the constraint of the interference to the PU's transmission. In the studied CR-based communication system, we considered the case of an SU relay with multiple-input antennas for reception and single antenna for transmission. We analyzed the secrecy outage probability of the considered system under different circumferences. The results showed

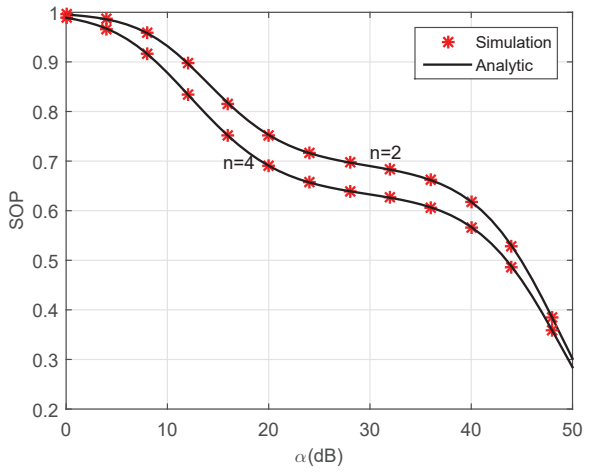

Fig. 3. Secrecy outage probability versus transmission power of the PU for $R_s = 1$ bit/s/Hz and $\epsilon = 10^{-4}$

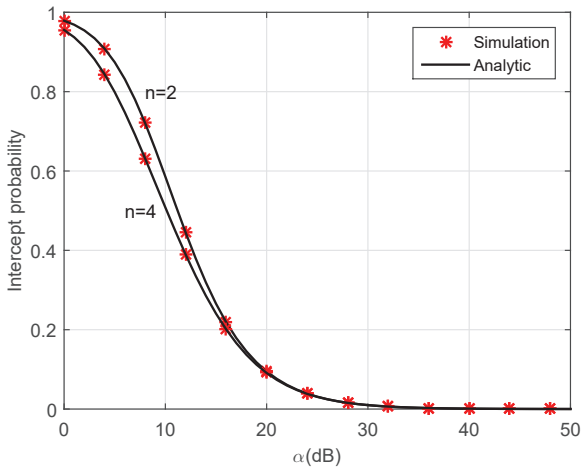

Fig. 5. Intercept probability versus transmission power of the PU for $\epsilon = 10^{-4}$

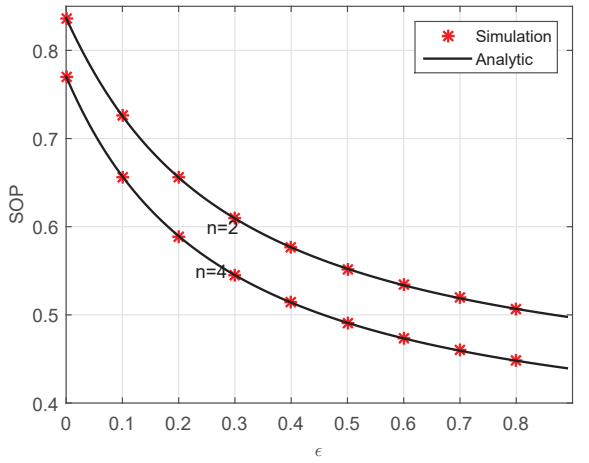

Fig. 4. Secrecy outage probability versus ϵ for $R_s = 1$ bit/s/Hz and $\alpha = 15$ dB

that the system has better secrecy performance when using a relay with multiple antennas instead of using only one antenna. As a future work, we intend to study the physical layer security of a CR-based communication system consisting of multiple sources and multiple eavesdroppers where each one is equipped with multiple antennas.

REFERENCES

[1] I. Akyildiz, W. Lee, M. Vuran, S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer networks*, vol. 50, no 13, p. 2127-2159, 2006.

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

[3] M. Bouabdellah, N. Kaabouch, F. El Bouanani, H. Ben-Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey," *Journal of Information Security and Applications*, vol. 38, p. 40-49, 2018.

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

[5] C. Tang, G. Pan, T. Li, "Secrecy Outage Analysis of Underlay Cognitive Radio Unit Over Nakagami- Fading Channels," *IEEE Wireless Communications Letters*, vol. 3, no 6, p. 609-612, 2014.

[6] N. Nguyen, T. Thanh, T. Duong, "Secure communications in cognitive underlay networks over Nakagami-m channel," *Physical Communication*, vol. 25, p. 610-618, 2017.

[7] H. Tran, G. Kaddoum, F. Gagnon, "Cognitive radio network with secrecy and interference constraints," *Physical Communication*, vol. 22, p. 32-41, 2017.

[8] H. Liu, H. Zhao, C. Tang, G. Pan, T. Li, "Physical-layer secrecy outage of spectrum sharing CR systems over fading channels," *Science China Information Sciences*, vol. 59, no 10, p. 102308, 2016.

[9] M. A. bin Azaman, N. P. Nguyen, D. B. Ha and T. V. Truong, "Secrecy outage probability of full-duplex networks with cognitive radio environment and partial relay selection," *International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom)*, pp. 119-123, Da Nang, 2017.

[10] M. Bouabdellah, F. E. Bouanani and H. Ben-azza, "A secure cooperative transmission model in VANET using attribute based encryption," *International Conference on Advanced Communication Systems and Information Security (ACOSIS)*, pp. 1-6, Marrakesh, 2016.

[11] Y. R. Ortega, P. K. Upadhyay, D. B. da Costa, P. S. Bithas, A. G. Kanatas, U. S. Dias, and R. T. de Sousa Jr., "Joint Effect of Jamming and Noise on the Secrecy Outage Performance of Wiretap Channels with Feedback Delay and Multiple Antennas", *Transactions on Emerging Telecommunications Technologies*, vol. 28, no 11, 2017.

[12] Y. Zou, G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Transactions on Industrial Informatics*, vol. 12, no 2, p.780-787, 2016.

[13] S. M. Ross, "Introduction to probability models," *Academic press*, 2014.