Error rate detection due to primary user emulation attack in cognitive radio networks

N. Armi[1], W. Gharibi[2], W. Z. Khan[3]
[1]Indonesian Institute of Sciences, Research Center for Electronics and Telecommunication, Indonesia
[1]Department of Electrical Engineering, Telkom University, Indonesia
[2]Department of Computer Science and Electrical Engineering, University of Missouri-Kansas City, United State
[3]Department of Computer and Network Engineering, Jazan University, Kingdom of Saudi Arabia

Article Info

Article history:

Received Aug 31, 2019
Revised Apr 16, 2020
Accepted Apr 29, 2020

Keywords:

Cognitive radio
False detection
Malicious user
Miss detection
Spectrum sensing

ABSTRACT

Security threat is a crucial issue in cognitive radio network (CRN). These threats come from physical layer, data link layer, network layer, transport layer, and application layer. Hence, security system to all layers in CRN has a responsibility to protect the communication between among Secondary User (SU) or to maintain valid detection to the presence of Primary User (PU) signals. Primary User Emulation Attack (PUEA) is a threat on physical layer where malicious user emulates PU signal. This paper studies the effect of exclusive region of PUEA in CRN. We take two setting of exclusive distances, 30m and 50m, where this radius of area is free of malicious users. Probability of false alarm (Pf) and miss detection (Pm) are used to evaluate the performances. The result shows that increasing distance of exclusive region may decrease Pf and Pm.

Corresponding Author:

Nasrullah Armi,
Research Center for Electronics and Telecommunication,
Indonesian Institute of Sciences,
Cisitu street, No. 21/154 D, Bandung 40135, Indonesia.
Email: nasrullah.armi@gmail.com

1. INTRODUCTION

Besides sensing and access over imperfect channel [1-3], security threat is crucial issue in cognitive radio. It comes from most layer such as physical, data link, network, transport, or application layer [4-10]. Unlike traditional wireless networks where operates in fixed spectrum, cognitive radio networks operate in dynamic spectrum where user opportunistically access available spectrum channel with prior sensing [11-14]. Hence, various factors must be taken into consideration since cognitive radio (CR) deals with the utilization of unused spectrum in opportunistic manner with the unscheduled appearance of primary users [15].

Physical layer is the lowest level which provides an interface to the medium. Security on physical layer is related to some possible attack such as intentional jamming attack, primary receiver jamming attack, primary user emulation attack, and overlapping secondary user attack. Intentional jamming attack means that malicious user transmit signal intentionally in the existing license bands and jams primary and other secondary user. The worst case is occurred when malicious users attack in one geographical area and move to another area very quickly without being identified. The unknown location of primary user is a benefit for attackers to launch primary receiver jamming attack. The attacker may shift to the primary receiver and requests transmission from secondary users. This case causes interference to primary receiver.

In CRN, multiple secondary networks perform sensing for available spectrum to access at the same region with the same time. The transmission from malicious users in one network may cause interference to the primary and secondary users from the other networks. This threat is known as overlapping secondary user attack where a malicious user may also imitate the primary user. The fake primary signal is considered as original signal by secondary user. Hence, secondary user refrain from transmission or terminate the ongoing communication and release the frequency spectrum [16]. This fake signal transmitted by malicious user is known as primary user emulation attack.

Primary user emulation attack is a threat on physical layer. It harms SU to achieve the correct sensing outcome. Malicious user attacks signal detection by transmitting signal whose has the same characteristic as primary signal. It causes SU has a difficulty to identify vacant spectrum. Malicious user does not utilize those vacant bands for its own communication purposes. They only transmit fake primary signal in vacant bands to obstruct SU from detecting original one.

The existing works related to this issue have been done. Smart attacker was introduced in [17]. The authors use Markov chain technique to model the activities of attackers. Then, energy detection of attackers was investigated in [18]. The authors used NI-USRP 2922 devices to derive probability of detection and false alarm. Chen *et al* in [19] investigated the attackers which is considered as interference to result inaccurate position of primary user location. The authors implemented directional antenna to explore position of primary transmitter. The used parameter like angle, arrival time, and strength of signal is explored to detect an accurate position. An analytical of successful probability to attact primary user location was firstly studied by authors in [20]. Fading was considered into account to calculate successful probability of attackers and define a lower limit by applying Fenton's and Markov approximation, respectively. CR signaling was introduced by authors in [21] to ease accessing available spectrum efficiently. The investigation proved that the framework is able to maximize SU transmission rate with low probility of miss detection and probability of false alarm. Using the statistical characteristic of users to prevent PUEA issue was proposed by Ghaznavi et al [22].

The used method on this article was well proved that its technique is able to increase the detection performance compared with the existing works. Investigation of primary user attackers with blind information of users was presented by authors in [23]. They investigated miss detection rate both theoretically and experimentally different number of SU. However, the disavadvantages of this study such as ignoring probability of false detection and the received power performance performance were not clearly presented. The technique to reduce the impact of attackers to primary user due to selfish and malicious users was introduced by authors in [24]. They implemented game strategy to counter the attacker and reduce the error rate detection of primary user. The effect of number of attackers to the performance of detection in PUEA was studied in [25, 26] with Neyman Pearson decision tecnique. They concluded that increasing number of attacker may decrease the performance.

This paper explores more performance affected by radius of exclusive region. Two different radius of exclusive region values is considered with two hypothesis of Neyman Pearson technique to decide the existence of primary user. Error rates detection such as false alarm and miss detection are used to present the derived performance evaluation. The rest of the paper is organized as follows. Section 2 discusses system and numerical model considered in the simulation. The derived result and discussion are presented in section 3. Finally, conclusion is taken briefly in Section 4.

2. PRIMARY USER EMULATION ATTACK MODEL

The major issue in primary signal detection is how SUs can identify fake primary signal. Primary user emulation attack (PUEA) is one threat on physical layer in cognitive radio network where attacker transmit fake primary signal. Two types of well-known PUEA is selfish PUEA and malicious PUEA. Attackers maximize its bandwidth by preventing other SUs to use the spectrum bands in selfish PUEA. Attackers transmit signal to resemble the primary signal. Whereas the aim of attackers in malicious PUEA is obstructing SU to identify the vacant spectrum bands, so that they cannot use those bands. Two type of errors caused by PUEA are probability of false alarm (Pf) and miss detection (Pm). These two detection errors are used as main parameter for performance evaluation.

Figure 1 describes a brief concept of how attackers interfere primary user detection. As figure, there are a number of attackers located on a circular network with radius R and single secondary user located at the center. Each attackers transmit signal among each other. The attackers (M) are distributed randomly covering secondary user with a certain radius R. These attackers transmit signal independently. On the other side, secondary user is located at the center of network with the distance Dp from primary transmitter. Fixed location of primary transmitter possibly to transmit signal with power Pt. Meanwhile, secondary user is free attackers at radius Ro where this region is known as exlusive area of secondary user.

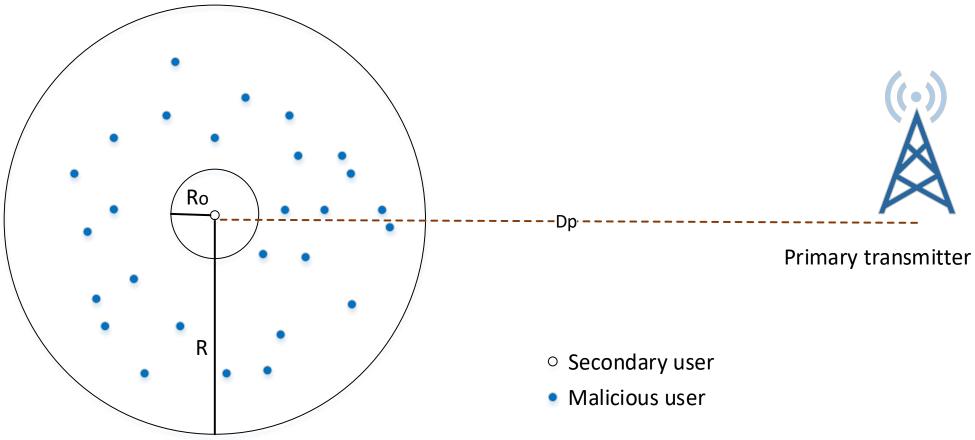

Figure 1. Primary user emulation attack (PUEA) model

As described in figure, we have a number of attackers located at (r_j, θ_j) where j is value with range range 1≤j≤M. Then probability density function (PDF) of r_j is derived as follows [10].

$$p(r_j) = \frac{2r_j}{R^2-Ro^2} \qquad Ro \leq r \leq R \tag{1}$$

where θ_j is equally distributed at range $(-\pi, \pi)$. Then, the received power of transmitted signal from primary transmitter is derived as bellows:

$$Pr^{(p)} = P_t d_p{}^{-2} G_p{}^2 \tag{2}$$

where $Gp^2 = 10^{\frac{\varepsilon p}{10}}, \varepsilon p \sim N(0, \sigma p^2)$. Since P_t and d_p have a fixed values, then the PDF of $pr^{(p)}$ uses a log normal distribution and can be calculated as follows:

$$Pr^{(p)}(\gamma) = \frac{1}{\gamma A \sigma_p \sqrt{2\pi}} exp\left\{\frac{(10log_{10}\gamma - \mu_p)^2}{2\sigma_p{}^2}\right\} \tag{3}$$

where $A = \frac{ln10}{10}$ and $\mu_p = 10log_{10}P_t - 20log_{10}d_p$

The total power received from attackers at the secondary user is derived by:

$$Pr^{(m)} = \sum_{j=1}^{M} P_m D_j{}^{-4} G_j{}^2 \tag{4}$$

where D_j and $G_j{}^2$ are the distance and shadowing between j^{th} malicious user and secondary user, respectively.

$G_j{}^2 = 10^{\frac{\varepsilon_j}{10}}$ where $\varepsilon_j \sim N(0, \sigma^2{}_m)$. The right side of equation (4) above is log normally distributed random variable of the form $10^{\frac{\omega_j}{10}}$ where $\omega_j \sim N(\mu_j, \sigma^2{}_m)$, where μ_j is derived by the following equation:

$$\mu_j = 10log_{10}P_m - 40log_{10}D_j \tag{5}$$

The PDF of $p_r{}^m$ considered as positions of all attackers can be derived as bellows:

$$P_{x|r}{}^{(m)} = \frac{1}{x A \sigma_M \sqrt{2\pi}} exp\left\{\frac{(10log_{10}x - \mu_M)^2}{2\sigma_M{}^2}\right\} \tag{6}$$

r is defined as the vector elements of $r_1, r_2, \ldots, r_m$. Then, $\sigma^2{}_M$ and μ_M are derived as the equation bellows:

$$\sigma_M{}^2 = \frac{1}{A^2} ln\left[1 + \frac{\left(e^{A^2\sigma_m{}^2} - 1\right)\sum_{j=1}^{M} e^{2A\mu_j}}{\left(\sum_{j=1}^{M} e^{A\mu_j}\right)^2}\right] \tag{7}$$

$$\mu_M = \frac{1}{A} ln\left(\sum_{j=1}^{M} e^{A\mu_j}\right) - \frac{A}{2}\left({\sigma_M}^2 - {\sigma_m}^2\right) \tag{8}$$

The PDF of the received power from attackers is calculated as follows:

$$P^m(x) = \int_{Ro}^{R} \prod_{j=1}^{M} P_{x|r}{}^{(m)}(x|r)p(r_j)dr_j \tag{9}$$

Futhermore, calculation of the receiver power from attacker uses log normally distributed random variable with μ_x and σ_x as bellows:

$$p^m(x) = \frac{1}{xA\sigma_x\sqrt{2\pi}} exp\left\{-\frac{(10log_{10}x-\mu_x)^2}{2{\sigma_x}^2}\right\} \tag{10}$$

The values of μ_x and σ_x can be derived when ${p_r}^m$ is considered as a log normally distributed random variable as written in equations bellows:

$${\sigma_x}^2 = \frac{1}{A^2}\left(lnE\left[\left(p_r{}^{(m)}\right)^2\right] - 2lnE\left[p_r{}^{(m)}\right]\right) \tag{11}$$

$$\mu_x = \frac{1}{A}\left(2lnE\left[p_r{}^{(m)}\right]\right) - \frac{1}{2} lnE\left[\left(p_r{}^{(m)}\right)^2\right] \tag{12}$$

From (6), the values of ${p_r}^m$ and $E[{p_r}^m|r]$ is derived by the following equation:

$$E\left[p_r{}^{(m)}|r\right] = Me^{A\mu_j} * e^{\frac{A^2{\sigma_m}^2}{2}} \tag{13}$$

where

$$\mu_j = 10log_{10}\left(P_m * D_j{}^{-4}\right) \tag{14}$$

$$e^{A\mu_j}{=}e^{A10log_{10}\left(P_m * D_j{}^{-4}\right)} = P_m * D_j{}^{-4} \tag{15}$$

Hence,

$$E\left[p_r{}^{(m)}|r\right] = MP_m * D_j{}^{-4} * e^{\frac{A^2{\sigma_m}^2}{2}} \tag{16}$$

By integrating equation over range of $r_1, r_2, \ldots, r_M$, it becomes:

$$\begin{aligned} E\left[P_r{}^{(m)}\right] &= \int_{Ro}^{R} Mp(r_j)P_m * D_j{}^{-4} * e^{\frac{A^2{\sigma_m}^2}{2}} dr_j \\ &= \int_{Ro}^{R} MP_m e^{\frac{A^2{\sigma_m}^2}{2}} \int_{Ro}^{R} \frac{2r_j}{R^2-Ro^2} * D_j{}^{-4} dr_j \end{aligned} \tag{17}$$

If secondary user is located at coordinate (0, 0), meaning that $D_j = r_j$

$$E\left[P_r{}^{(m)}\right] = MP_m e^{\frac{A^2{\sigma_m}^2}{2}} \int_{Ro}^{R} \frac{2r_j}{R^2-Ro^2} * \frac{1}{r_j{}^4} dr_j$$

$$E\left[P_r{}^{(m)}\right] = \frac{MP_m}{R^2 Ro^2} e^{\frac{A^2{\sigma_m}^2}{2}} \tag{18}$$

Using decision criterion of Newman Pearson, we assume that M$_1$ as primary signal transmission in progress, and M$_2$ is emulation attack in progress. This study implements two error rate for performance evaluation, those are false alarm and miss detection. False detection means mistake detection by secondary user where malicious user as attacker signal is detected as primary signal. Meanwhile, miss detection means secondary user detect primary user signal as attacker signal. Hence, secondary user is unaware and loss an opportunity to access available spectrum. The decision variable is derived by including the received signal power as follows:

$$\Lambda = \frac{p^{m}(x)}{p^{(pr)}(x)} \tag{19}$$

The decision is achived by comparing Λ with the threshold as bellows:

$\Lambda \leq \lambda\ D_1$: Primary signal transmission
$\Lambda \geq \lambda\ D_2$: Emulation attack in progress

Then, error rate is determined by the following decision rule:

$P\{D_2|M_1\}$ = probability of missed detection, where decides D_2 when M_1 is true.
$P\{D_1|M_2\}$ = probability of false alarm, where decides D_1 when M_2 is true.

Those mentioned error rate for final decision above can be written mathematically as follows:

$$P\{D_2|M_1\} = \int_{\Lambda\geq\lambda} p^{(pr)}(x)dx = \alpha \tag{20}$$

$$P\{D_1|M_2\} = \int_{\Lambda\leq\lambda} p^{(m)}(x)dx \tag{21}$$

3. RESULTS AND ANALYSIS

This section discusses the derived result and performance analysis for the exclusive region effect of PUEA. We considered two distances for radius of exclusive region, 30 m and 50 m from the center of network cell. As described in Figure 1, a brief concept how malicious user as attacker interfere primary signal detection, with a certain number of malicious users located out of exclusive region transmitting fake primary signal. It is assumed that fix secondary user stand at the center of circular network cell with radius R = 500 m, $P_m = 4\,W$, $\sigma_p = 8\,dB$, $\sigma_m = 5.5\,dB$, primary transmitter power $P_t = 150\,kW$ and the distance from primary transmitter to secondary user D_p = 100 km. Number of attackers is set to M = 10 users.

Firstly, we define radius of exclusive region into Ro = 30m. Simulation is executed by 500 times. Probability of false alarm is derived as shown in Figure 2. Its performance is varied from 0.0046 to 0.0087 as a function of simulation times. The average value is achieved around 0.0057. Meanwhile, the performance of probability of miss detection is shown in Figure 3. Simulation is executed by 500 run times. The derived results are varied from 0.0055 to 0.0075 as function of simulation times. However, the average value is achieved around 0.0063.

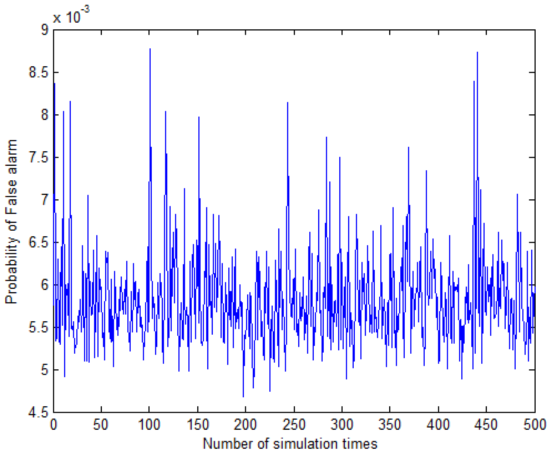

Figure 2. Probability of false alarm during 500 simulation times with parameter R = 500 m, Ro = 30 m and number of attackers M = 10

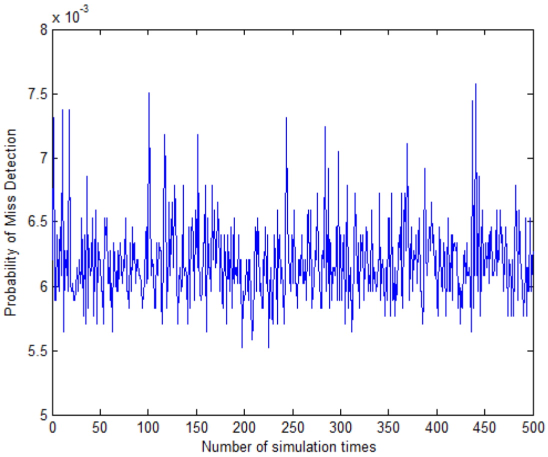

Figure 3. Probability of miss detection during 500 simulation times with parameter R = 500 m, Ro = 30 m and number of attackers M = 10

Secondly, we replace the distance of radius of exclusive region by 50 m. This study observes the effect of exclusive region to the performance of detection due to attackers by changing the radius of exclusive region. The performance results are derived as shown in figures. Figure 4 shows the performance of probability of false detection with radius of exclusive region Ro = 50 m. The values are varied from 0.0025 to 0.0065 as a function of simulation times. The average value is achieved at 0.0033. Probability of false detection decreases when compared with the case of Ro = 30 m. Performance of probability of miss detection is shown in Figure 5. Its result is fluctuated from 0.0029 to 0.0047. However, the average result is achieved around 0.0033. Furthermore, CDF of false alarm and miss detection probability is presented in Figure 6 and Figure 7. The derived results show that the larger radius of exclusive region is used, then achieve less false alarm and miss detection probabilities.

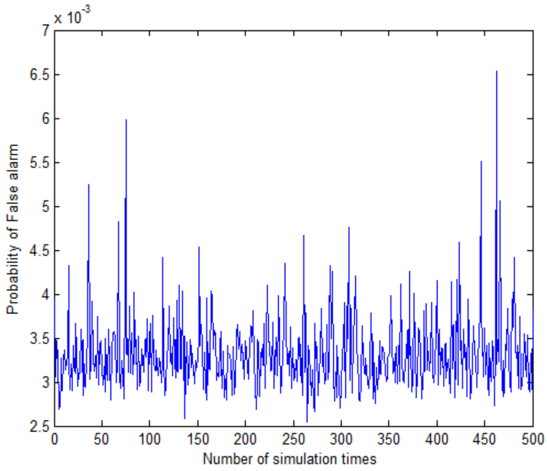

Figure 4. Probability of false alarm during 500 simulation times with parameter R = 500 m, Ro = 50 m and number of attackers M = 10

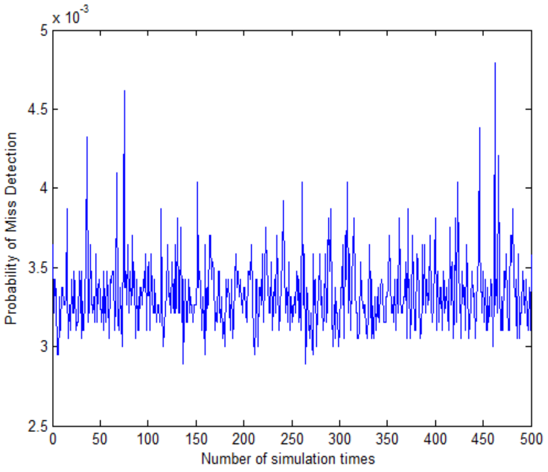

Figure 5. Probability of miss detection during 500 simulation times with parameter R = 500 m, Ro = 50 m and number of attackers M = 10

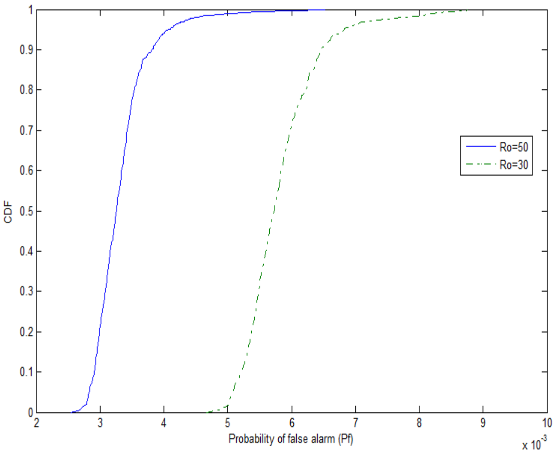

Figure 6. CDF of false alarm probability (Pf)

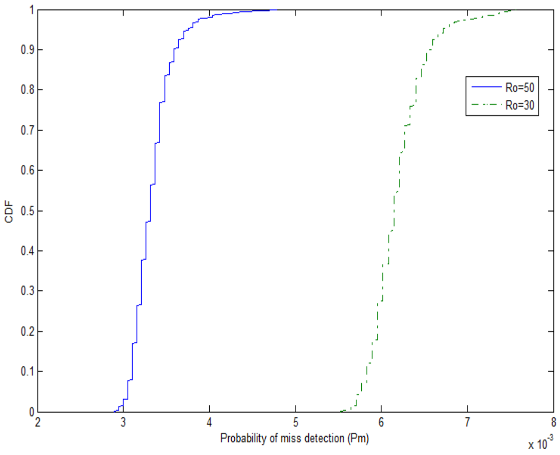

Figure 7. CDF of miss detection probability (Pm)

4. CONCLUSION

The effect of radius of exclusive region in primary user emulation attack under Neyman Pearson techniques has been studied. The statistical model for false alarm and miss detection probability is also discussed. Exclusive region is an area where secondary user free of attackers. The simulation shows that increasing radius of this area can decrease either probability of false detection or miss detection. The larger radius of exclusive region is taken influences to achieve less false alarm and miss detection rate. This study considered one primary transmitter which is located at a certain distance (100 km) away from secondary user. For further study, it will be considered two or multiple primary base station with different distances.

REFERENCES

[1] N. Armi, et al., "Sensing and access over imperfect channel in opportunistic spectrum access system," *2011 National Postgraduate Conference*, Kuala Lumpur, pp. 1-5, 2011.

[2] S. Akin and M. C. Gursoy, “Performance Analysis of Cognitive Radio Systems With Imperfect Channel Sensing and Estimation,” in *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1554-1566, May 2015.

[3] I. U. Ohaeri, et al., “Investigating the Effect of Imperfect Sensing on Spectrum Performance in Cognitive Radio Networks,” *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, pp. 638-644, 2017.

[4] C. N. Mathur and K. P. Subhalakshami, “Security issues in cognitive radio networks,” *Cognitive network: Towards Self-Aware Networks*, John & Wiley, Ltd, pp. 271-291, 2007.

[5] X. Zhang and C. Li, “Constructing secure cognitive wireless networks experiences and challenges,” *Wireless Communications and Mobile Computing*, vol. 10, no. 1, pp. 55-69, 2010.

[6] J. Li, et al., “A survey of security issues in Cognitive Radio Networks,” in *China Communications*, vol. 12, no. 3, pp. 132-150, Mar. 2015.

[7] A. S. Hamood and S. B. Sadkhan, “Cognitive radio network security status and challenges,” *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, Baghdad, pp. 1-6, 2017.

[8] S. Holcomb and D. B. Rawat, “Recent security issues on cognitive radio networks: A survey,” *SoutheastCon 2016*, Norfolk, VA, pp. 1-6, 2016.

[9] S. B. Sadkhan and D. M. Reda, “Security Issues of Cognitive Radio Network,” *2019 2nd International Conference on Engineering Technology and its Applications (IICETA)*, Al-Najef, Iraq, pp. 117-122, 2019.

[10] Y. Yao, et al., “Dynamic Spectrum Access With Physical Layer Security: A Game-Based Jamming Approach,” in *IEEE Access*, vol. 6, pp. 12052-12059, 2018.

[11] A. S. Khobragade and R. D. Raut, “Hybrid Spectrum Sensing Method for Cognitive Radio,” *International Journal of Electrical and Computer Engineering*, vol. 7, no. 5, pp. 2683-2695, 2017.

[12] F. Li, et al., “Dynamic Spectrum Access Networks With Heterogeneous Users: How to Price the Spectrum?” in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5203-5216, Jun. 2018.

[13] K. Umebayashi, et al., “Design of Spectrum Usage Detection in Wideband Spectrum Measurements,” in *IEEE Access*, vol. 7, pp. 133725-133737, 2019.

[14] S. Lien, et al., “Random Access or Scheduling: Optimum LTE Licensed-Assisted Access to Unlicensed Spectrum,” in *IEEE Communications Letters*, vol. 20, no. 3, pp. 590-593, Mar. 2016.

[15] F. Z. El Bahi, et al., “Performance Evaluation of Energy Detector Based Spectrum Sensing for Cognitive Radio using NI USRP-2930,” *International Journal of Electrical and Computer Engineering,* vol. 7, no. 4, pp. 1934-1940, 2017.

[16] R. Chen and J. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” in *Proceedings of IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR)*, pp. 110-119, 2006.

[17] A. Karimi, et al., “Smart Traffic-Aware Primary User Emulation Attack and Its Impact on Secondary User Throughput Under Rayleigh Flat Fading Channel,” in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 66-80, 2020.

[18] E. C. Muñoz, et al., “Detection of Malicious Primary User Emulation on Mobile Cognitive Radio Networks,” *2019 International Conference on Information Systems and Computer Science (INCISCOS)*, Quito, Ecuador, pp. 144-149, 2019.

[19] R. Chen, et al., “Defence against primary user emulation attacks in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications, Special Issue on Cognitive Radio Theory and Applications*, vol. 26, no. 1, Jan. 2008.

[20] S. Anand, et al., “An analytical model for primary user emulation attacks in cognitive radio networks,” in *3rd IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2008.

[21] M. Karimi and S. M. S. Sadough, “Efficient Transmission Strategy for Cognitive Radio Systems Under Primary User Emulation Attack,” in *IEEE Systems Journal*, vol. 12, no. 4, pp. 3767-3774, 2018.

[22] M. Ghaznavi and A. Jamshidi, “Defence against primary user emulation attack using statistical properties of the cognitive radio received power,” in *IET Communications*, vol. 11, no. 9, pp. 1535-1542, 2017.

[23] Z. Jin, et al., “Detecting primary user emulation attacks in dynamic spectrum access networks,” in *2009 IEEE International Conference on Communications (ICC’2009)*, pp. 1-5, 2009.

[24] N. Nguyen-Thanh, et al., “Surveillance strategies against primary user emulation attack in cognitive radio networks,” in *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 4981-4993, Sep 2015.

[25] N. Armi, et al., “Malicious user attack in cognitive radio networks,” *TELKOMNIKA Telecommunication, Computing, Electronics, and Control*, vol. 15, no. 3, pp. 1096-1102, 2017.

[26] D. S. Vernekar, “An Investigation Of Security Challenges In Cognitive Radio Networks,” *Thesis*, University of Nebraska, 2012.