*Al-Mukhtar Journal of Sciences* 36 (1): 73-79, 2021

# Performance Metrics in Cognitive Radio Networks

**Mahmoud Ali Ammar**
*Department of Computer Engineering, University of Zawia, Zawia, Libya*

Received: 25 January 2021/ Accepted: 31 January 2021
Doi: https://doi.org/10.54172/mjsc.v36i1.21

**Abstract:** In Cognitive Radio Networks (CRN), the main aim is to allow the secondary users (SUs) to identify the empty bands and use them to transmit or receive data opportunistically. Primary users (PUs) have the priority to use a channel, while the secondary users must vacant this channel once a primary user requests it. An attack known in cognitive radio networks as a Primary User Emulation Attack (PUEA) aims to prevent the SU from using the empty bands. In this paper, an analytical and experimental approach is presented to mitigate the PUEA. This approach is based on obtaining the Probability Density Functions (PDFs) of the received powers at the secondary users from malicious nodes and also from the primary transmitter in the cognitive network. Then, these obtained PDFs are used in Neyman-Pearson composite hypothesis test to measure the performance metrics (probability of false alarm and miss detection in the network). The results proved that the performance metrics were greatly influenced by the network area, where the secondary user is located, and the threshold value λ used in the decision rule. Also, there are boundaries for the λ choices that cannot be overtaken.

**Keywords:** Cognitive Radio (CR); Probability Density Function (PDF); Primary User Emulation Attack (PUEA).

## INTRODUCTION

The four main functions of cognitive radio are spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility. Via these functions the secondary users in the CR must be able to distinguish between the available channels and used channels. For example, if a TV transmitter acts as a primary user, then the users that can use the white spaces (available channels) in the TV band are called cognitive users (Buddhikot & Ryan, 2005).

The major challenge in spectrum sensing is the ability of the cognitive radio to recognize the spectrum bands that are not used by the primary users so the secondary users can coexist with the primary users without any interference to their communication. Recently the operational aspects of CR and its security aspects have gained a great deal of attention (FCC 2003). The reasons that make the cognitive radio vulnerable to new kind of security threats are as follows :-

- The open and dynamic features of the cognitive radio network make the CR systems more vulnerable to various malicious attacks. The new threats such as jamming, primary user emulation (PUE), and Spectrum Sensing Data Falsification (SSDF) (Jin et al., 2009).
- Because the cognitive radio network shares some features of the conventional wireless networks, we have to deal with the conventional wireless security risks in addition to the threats targeting the cognitive radio features. The conventional risks include MAC spoofing, Denial of Service …etc. (Akyildiz et al., 2006).

Based on these vulnerabilities, countermeasures are needed to make the cognitive radio networks robust and secure against any type of threat.

***Corresponding Author:** Mahmoud Ali Ammar m.ammar@zu.edu.ly , Department of Computer Engineering, University of Zawia, Zawia, Libya

Cooperative spectrum sensing can be vulnerable when some malicious nodes share false local sensing reports with others. In such cases, the fused decision may be altered, hence the reliability of cooperative spectrum sensing. Such phenomenon where local sensing results are manipulated is known as spectrum sensing data falsification or Byzantine attack. A malicious radio can advertise 'occupied' as 'available' inducing a policy violation or advertise 'available' as 'occupied' causing a denial of spectrum usage. The environment and changing the parameters in order to improve the quality of service are achieved based on the main functions of the cognitive radio. In adversarial, military, and heterogeneous competitive networks, such actions are not surprising where an adversary wants to cripple the operation of others in the network. Apart from this, there are also cases where a node's permanent spatial orientation is such that its reports are not suitable for use by other nodes. The adversary may vary attack strategies based on different objectives. Hence there is a need to evaluate the trustworthiness of radios before considering their local spectrum sensing reports (Chen & Park, 2006).

The main aim of this research is to obtain the performance metrics in cognitive radio networks. These metrics are crucial in the spectrum detection process to mitigate the attacks that are presented in the cognitive radio networks. Mitigating these attacks leads to improving the spectrum sensing in the cognitive radio network.

## OBJECTIVE OF ADVERSARIAL ATTACKERS

The objectives of an attacker have a direct correlation with the way the attacks are launched, and therefore they determine the nature of attacks. Selfish attacks The attacker's motive is to acquire more spectrum for its own use by preventing others from competing for the channels and unfairly occupying their share. In this type of attack, adversaries will defy the protocols and policies only if they are able to benefit from them (Bhattacharjeea 2013; Mathur & Subbalakshmi, 2007).

**Malicious attacks:** The attackers' only objective is to create hindrance for others and does not necessarily aim at maximizing their own benefits. They do not have any rational objective and identify protocols and policies to just induce losses to others (Jakimoski & Subbalakshmi, 2008).

## IMPACT OF PUE ATTACKS ON CR NETWORKS

The presence of PUE attacks causes several problems for CR networks. The list of potential consequences of PUE attacks is:

1. Bandwidth waste: The ultimate objective of deploying CR networks is to address the spectrum under-utilization that is caused by the current fixed spectrum usage policy. By dynamically accessing the spectrum "holes", the SUs are able to retrieve these otherwise wasted spectrum resources (Cabric et al., 2004).

2. QoS degradation: The appearance of a PUE attack may severely degrade the Quality-of-Service (QoS) of the CR network by destroying the continuity of secondary services (Cabric et al., 2004).

3. Connection unreliability: If a real-time secondary service is attacked by a PUE attacker and finds no available channel when performing spectrum handoff, the service has to be dropped. This real-time service is then terminated due to the PUE attack. In principle, the secondary services in CR networks inherently have no guarantee that they will have stable radio resources because of the nature of dynamic spectrum access. The existence of PUE attacks significantly increases the connection unreliability of CR networks.


*ISSN: online 2617-2186 print 2617-2178*

## SIMULATION MODEL

In practice, the SU aims to identify the signal source, whether it is from a primary transmitter (PT) or malicious users. This scenario model is simulated using Matlab software. Figure 1 shows the cognitive radio network users' distributions where the SUs and malicious users are located in a circular area with radius R.

Some assumptions are considered as follows: The primary user is at a distance $d_p$ from the secondary user. The malicious users are distributed randomly around the good user, as in Figure 1. This model aims to analyze the performance metrics under long-distance $d_p$ = 160 km to the SU. At the same time, the network radios R and $R_o$ are too small, R = 300 m and $R_0$ = 30 m. such parameters for analysis in CR networks are chosen as a novel study of the model under these low - parameters to prove the efficiency of the analytical model.

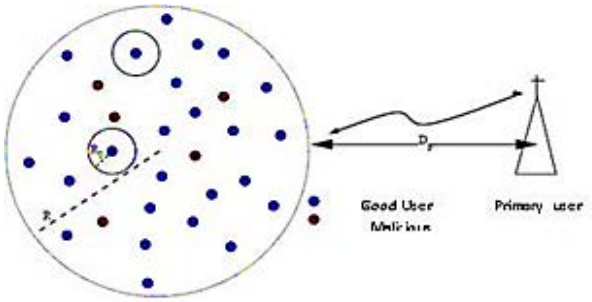


**Figure: (1).** Radio network users' distributions

If M denotes the number of malicious users in the system, $P_t$: Primary transmission power, $P_m$: Malicious transmission power, $\sigma_p$: Variance of Primary users, $\sigma_m$: Variance of Malicious users. The simulation model novel parameters are as in Table 1 below.

**Table: (1).**The simulation model parameters

| Parameter | $d_p$ | R | $R_o$ | M | $P_t$ | $P_m$ | $\sigma_p$ | $\sigma_m$ |
|---|---|---|---|---|---|---|---|---|
| Value | 160 KM | 300 m | 30 m | 20 | 100 KW | 10 W | 8 dB | 5.5 dB |

## MATHEMATIC FUNCTIONS OF THE RECEIVED SIGNALS

To calculate the probability density functions PDFs and use them in the simulated model. The received power Pr is determined first based on the relation below:

$$P_r \propto d^{\gamma} \quad (1)$$

γ is the path loss exponent. Thus, the received power from the primary is:

$$P_r^{(P)} = P_t\, d_p^{-2k} \quad (2)$$

Where k is the path loss $K = 10^{\varepsilon p/10}$

Thus the probability density function of the received power is:

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

$\mu_p$, $\sigma_p$ are the mean and variance of the distribution and given by

$$\mu_p = 10\log_{10} P_t - 20\log_{10} d_p$$

Secondly, the received power from each malicious user $P^{(mi)}$ at the secondary user is calculated according to the equation below:

$$P^{(mi)} = (P_T)_{mi}\, d_i^{-4}\, K \quad (4)$$

Where k is the path loss. $d_i$ is the distance from the secondary user.

Based on the above equations, the decision variable Λ that is used to find the false alarm and miss detection probabilities can be calculated as follows:

$$\Lambda = P^m(\chi) \,/\, P^{\Pr}(\chi) \quad (5)$$

Where $P^{\Pr}(\chi)$ and $P^m(\chi)$ are the pdf of received powers from the primary and all malicious users respectively.

After performing Λ, it is compared with a threshold λ that can be chosen to guarantee a fine false alarm and miss detection probabili-


*ISSN: online 2617-2186 print 2617-2178*

ties as follows:
IF $\Lambda \leq \lambda$ then
The decision is that the transmission is from a primary user.
IF $\Lambda > \lambda$ then
The decision is that the transmission is from a malicious user.

## RESULTS DISCUSSION AND ANALYSIS

The results obtained using Matlab simulation are presented in this section. The performance of the cognitive network under the PUE attack is studied in terms of probability of miss detection and false alarm.

Both the probability of miss detection and false alarms are calculated for 1000 times of simulations to be averaged to offer accurate results. The result obtained first was based on the threshold value $\lambda$=0.45. The network is assumed to be under a high number of malicious attackers M=20. In this case, it is noticed that when $\lambda$ is too small, the achieved false alarm probability is very small, which in this case is about 0.05 as shown in Figure 2 below. At the same time, the miss detection probability is high and is about 0.325, as shown in Figure 3. These values are averaged out of 1000 runs.

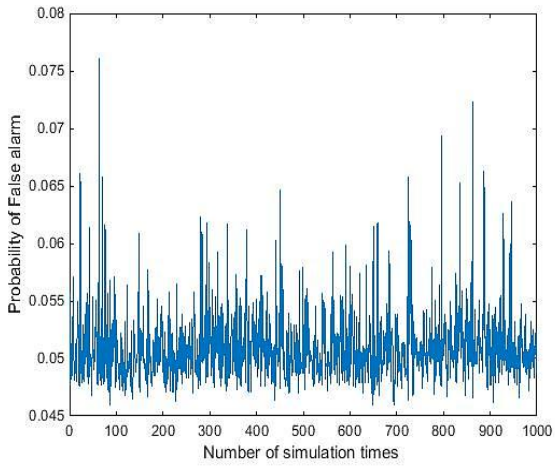


**Figure :(2).** False alarm probability for $\lambda$=0.45

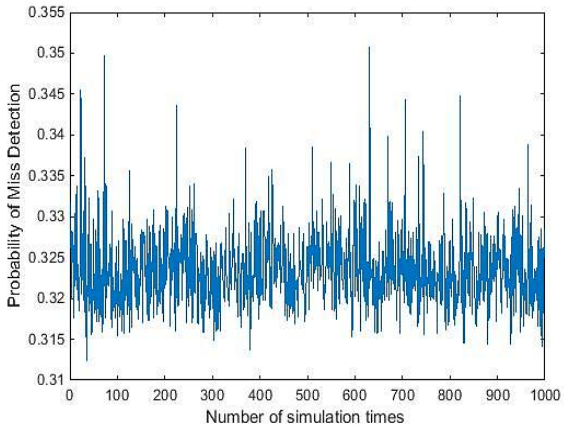


**Figure: (3).** Miss detection probability for $\lambda$=0.45

Furthermore, the model is justified under a high value of $\lambda$, $\lambda$=2.2. Thus the false alarm probability is high, which in this case is 0.43, opposed to the miss detection probability which is very small and is 0.17. These results are summarized in Table 2 as follows.

**Table: (2).** Miss detection and false alarm for different $\lambda$

| Parameter | False Alarm Probability Averaged for 1000 runs | Miss Detection Probability Averaged for 1000 runs |
|---|---|---|
| $\lambda$ =0.45 | 0.05 | 0.325 |
| $\lambda$ =2.2 | 0.43 | 0.17 |

These results mean that the threshold value of the simulated mathematics model must be chosen so that it doesn't exceed 2.2 and not less than 0.45. These boundaries of the threshold value $\lambda$ can guarantee acceptable values of the performance metrics (miss detection and false alarm). In addition, it has proved that at least one of these performance metrics is low because of the mathematic relationship, which forms an inverse correlation. Specifically, there is an inverse correlation between $\lambda$ and miss detection, while a positive correlation exists between $\lambda$ and the false alarm, i.e. as $\lambda$ decreases, false alarm decreases, and miss detection increases.

To sum up, choosing the value $\lambda$ out of the


*ISSN: online 2617-2186 print 2617-2178*

boundaries leads to increasing one of these probabilities, which leads to a wrong decision about the presence of the primary user.

## CDF OF FALSE ALARMS AND MISSED DETECTIONS

In order to testify these results, the cumulative distribution function (CDF) is calculated to display both the false alarms and the missed detection probabilities on the same graph as shown in Figure 4. Notably, the CDF plot is a non-decreasing function, and this indicates that the parameters and assumptions that were considered in the simulation are well-chosen and the results are accurate because these cumulative distributions functions in Figure 4 match and follow the general appearance of the CDF of the continuous variable of the simulated model.

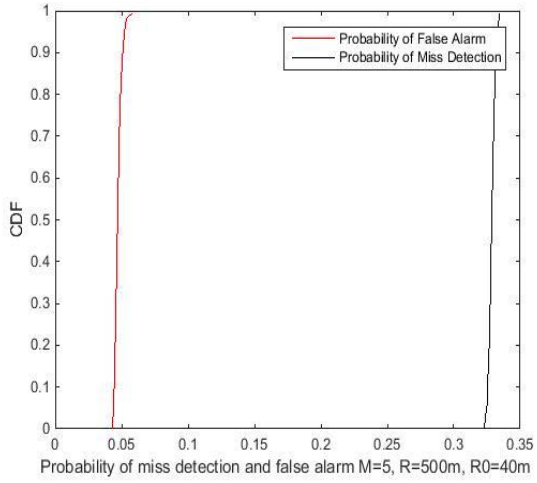


**Figure: (4)**. Cumulative distribution functions for miss detection and false alarm

## CONCLUSION

Due to the limitations and problems in the conventional spectrum sensing and radio network approaches, this paper focused on one of the major threats in the radio networks which is the primary user emulation attack. In this proposed model and using an analytical approach, the security against primary user emulation attacks in radio networks was discussed. The proposed analytical model and its impact on the PUEA attack were investigated.

The performance metrics results (the probability of false alarm and missed detection in the network) proved that the number of malicious nodes in the system has a great impact on the network, and this has led to a reduction in the quality of service due to the transmission from a high number of malicious users.

Also, it has proved that at least one of the performance metrics is low as a result of the inverse correlation between λ and miss detection probability. In other words, there is an inverse correlation between λ and miss detection, while a positive correlation exists between λ and the false alarm. This means if λ decreases, false alarm decreases and miss detection increases. For each model, there is a boundary for the value of λ depending on the parameters used in the model.

## REFERENCES

Akyildiz, I. F., Lee, W.-Y., Vuran, M. C., & Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer networks*, *50*(13), 2127-2159.

Bhattacharjeea, S. (2013). In cognitive radio networks. The International Journal for the Computer and Telecommunications, 01(36) 1387-1398 .

Buddhikot, M. M., & Ryan, K. (2005). Spectrum management in coordinated dynamic spectrum access based cellular networks. First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.,

Cabric, D., Mishra, S. M., & Brodersen, R. W. (2004). Implementation issues in


*ISSN: online 2617-2186 print 2617-2178*

spectrum sensing for cognitive radios. Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.,

Chen, R., & Park, J.-M. (2006). Ensuring trustworthy spectrum sensing in cognitive radio networks. 2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks,

Federal Communications Commission FCC. (2003). NPRM - Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies. FCC, 03-322.

Jakimoski, G., & Subbalakshmi, K. (2008). Denial-of-service attacks on dynamic spectrum access networks. ICC Workshops-2008 IEEE International Conference on Communications Workshops,

Jin, Z., Anand, S., & Subbalakshmi, K. (2009). Detecting primary user emulation attacks in dynamic spectrum access networks. 2009 IEEE International Conference on Communications,

Mathur, C. N., & Subbalakshmi, K. (2007). Security issues in cognitive radio networks. *Cognitive Networks, 25*, 272-290.


*ISSN: online 2617-2186 print 2617-2178*

# مقاييس الاداء في شبكات الراديو المعرفية

**محمود علي عمار**

*قسم الحاسوب، كلية الهندسة، جامعة الزاوية، ليبيا*

تاريخ الاستلام: 25 يناير 2021 / تاريخ القبول: 31 يناير 2021

Doi:https://doi.org/10.54172/mjsc.v36i1.21

**المستخلص:** في شبكات الراديو المعرفية Cognitive Radio Networks( CRN) الهدف الرئيسي هو السماح للمستخدمين الثانويين Secondary users (SUs) بتحديد النطاقات الفارغة، واستخدامها لنقل البيانات، أو استقبالها بشكل انتهازي. يتمتع المستخدمون الأساسيون Primary Users (Pus) بالأولوية في استخدام قناة أو تردد ما بينما يجب على المستخدمين الثانويين إخلاء هذه القناة بمجرد أن يطلبها المستخدم الأساسي. هناك هجوم أمني يُعرف في الراديو المعرفي بأنه هجوم محاكاة المستخدم الأساسي Primary user emulation attack (PUEA) ، ويهدف إلى منع SU من استخدام النطاقات الفارغة. في هذا البحث ، تم تقديم نهج تحليلي وتجريبي للتخفيف من PUEA ، ويستند هذا النهج إلى الحصول على وظائف الكثافة الاحتمالية Probability Density Function (PDF ) للطاقة المتلقية للمستخدمين الثانويين من قبل العقد الخبيثة في الشبكة وكذلك من المرسل الاساسي في الشبكة المعرفية. بعد ذلك يتم استخدام ملفات PDF التي تم الحصول عليها في اختبار الفرضية المركبة Neyman-Pearson لقياس مقاييس الأداء (احتمال الإنذار الخاطئ، واكتشاف الأخطاء الخاطئ في الشبكة). أثبتت النتائج أن مقاييس الأداء تتأثر بشكل كبير بموقع الشبكة، موقع المستخدم الثانوي، وقيمة العتبة المستخدمة في قاعدة القرار. كما أن هناك حدودًا للاختيارات لا يمكن تجاوزها.

**الكلمات المفتاحية:** الراديو المعرفي CR؛ دالة الكثافة الاحتمالية (PDF)؛ هجوم محاكاة المستخدم الأساسي (PUEA).

* محمود علي عمار m.ammar@zu.edu.ly قسم الحاسوب ، كلية الهندسة ، جامعة الزاوية ، ليبيا