MODELING BASED APPROACH FOR THE PRIMARY USER EMULATION ATTACK USING LOCATION, FEATURE DETECTION TECHNIQUE & POWER ESTIMATION METHODS IN COGNITIVE RADIO NETWORKS

[1] Mahesh Kumar N. & [2] Siddesh G.K.

[1] *Research Scholar, VTU Research Centre,*
Department of Electronics & Communication Engineering,
Dayananda Sagar College of Engineering, Bangalore-78
&
Assistant Professor, Electronics & Communication Engineering Dept.,
Dayananda Sagar College of Engineering, Bangalore-78
E-mail : mkumar.n19@gmail.com

[2] *Department of Electronics & Communication Engineering,*
JSS Academy of Technical Education, JSSATE-Bangalore Campus,
Uttarahalli-Kengeri Road, Bengaluru - 560060, Karnataka
E-mail : siddeshgundagatti@gmail.com

Abstract

Cognitive radio technology addresses the problem of the spectrum scarcity by allowing secondary users to use the vacant spectrum bands without causing interference to the primary users. However, several attacks could disturb the normal functioning of the cognitive radio network. Primary user emulation attack is one of the most severe attacks in which a malicious user emulates the primary user signal characteristics to either prevent other legitimate secondary users from accessing the idle channels or causing harmful interference to the primary users. There are several proposed approaches to detect the primary user emulation attackers. However, most of these techniques assume that the primary user location is fixed which does not make them valid when the primary user is mobile. The growth in wireless communication has increased the demand for wireless radio spectrum to utilize many social and individual benefits. Cognitive radio is a technology that provides a possible solution for improving spectrum efficiency by allowing opportunistic access to the spectrum for unlicensed users (CRs). In this work, we mainly focus on Primary User Emulation attack (PUEA) is one such major threat posed on spectrum sensing, which decreases the spectrum access probability. We propose a mathematical model of the mitigation techniques based transmitter location using received signal strength (RSS) and based on feature detection, which employs a cyclostationary calculation to represent the modulation features of the user signals & use the model to simulate the results, which would be taken as a future work initiative.

Keywords: *Cognitive Radio Networks, Spectrum Sensing, Primary User Emulation Attack, Received Signal Strength, Power Spectral Density, Model.*

1. Introduction

The *Frequency Spectrum* is a vital wireless communication tool and used for military purposes, governments sell a few frequency bands for commercial use to broadcasters and mobile communications companies, others such as ISM (Industrial, Scientific, and Medical) bands are available to the public at nominal charge or Free [1]. As the spectrum is overcrowded, two possible solutions appear: increasing the frequency limits higher to and above 60 GHz frequencies, or re-aggregating the heavily used licensed frequency bands. The new approach to cognitive radio (CR) comes with a feasible solution to the shortage of bandwidth. The CR is an excellent technology to deal with spectrum scarcity by allowing unlicensed CR users to coexist with existing users in licensed spectrum bands without interfering with binding communications. Cognitive technology provides the spectrum ability to be shared with licensed networks [2][3]. This radio system can adjust its transmitter and recipient parameters on the basis of interaction with the current conditions in the environment. From the description, there are two key aspects of cognitive radio [4], which are mentioned as under 2 sub-headings as

First one is Cognitive capacity : with parts of the spectrum accessible at a certain point or physical location, effective communication with the radio atmosphere is important. A CR user can use the temporary unused spectrum band known as the spectrum hole or the white space.

*Second one is Re-configurability***:** The cognitive radio parameter could be adjusted for transmitting and receiving at different frequency ranges and using different hardware-powered access techniques. With this feature, the best frequency band available and the most acceptable operating channel parameters for use can be selected and reconfigured [5].

Successfully implementing CR networks and understanding their advantages will rely on putting critical security mechanisms in sufficiently robust shape to avoid device misuse. The need for confidentiality of the spectrum sensing process is particularly vital. The secret towards this issue is that primary user signals can be strongly separated from secondary user signals [6]. This scheme underlines the significance of the CR's ability to distinguish primary user signals from secondary user signals. The differentiation between the two signals is computationally costly, but it is very difficult to distinguish when CR operates under extreme conditions [40].

The attacker can change the Air-CR functionality in a hostile environment to imitate the aspect of the primary user signal and cause the malicious user to be misidentified by the legitimate secondary user, called as Primary User Emulation Attack (PUEA). This attacks are feasible because their software-driven air interface makes CRs extremely reconfigurable [7]. An approach is required, that can truly differentiate incumbent signal transmitters and SU signal transmitters, which masks these attacks as primary users. In order to improve the reliability of the outcome, such a framework should be incorporated into the spectrum sensing mechanism in hostile environments [39].

The paper is well organized in a structured manner as follows. An introductory note w.r.t. the related work was presented in the previous paragraphs in this introductory section. The review of the related literature work is discussed in the section II. The spectrum management process is discussed in the section III followed by the spectrum sensing model in the section IV. The non-cooperative sensing techniques & the challenges of non-cooperative sensing is portrayed in the section V & VI respectively followed by the cooperative sensing & its challenges followed by spectrum decision & its challenges in the section VIII. The section IX gives a brief idea about the spectrum mobility & its challenges. The attacks that takes place in the CRN's is presented in the section X. The primary user emulation (PUE) attack & its detection and countermeasure techniques is presented in the section XI & XII respectively. Here, we discuss about the localization-based methods, cryptographic approaches, watermarking-based methods, belief propagation-based methods, radio fingerprinting & the game theory based methods. The mathematical model that is used is presented in the section XIII using the references [1]-[40]. The future work that could be carried out in this exciting field of CRNs is depicted in the section XIV followed by the conclusive remarks in the section XV. The paper concludes with the exhaustive list of references used in developing the model followed by the author's biographies at the end.

2. Review of the related literature work

A large quantity of researchers had worked w.r.t. related topic so far till date and a brief review of the literature is presented in this context here. Quite a substantial amount of research has been conducted to prevent this attack of detecting the P U E attack using various the concept of sensing of the spectrum's techniques & in this work we have addressed few of them. Those are Location based, Cryptography based, Watermarked based and Radio Fingerprinting based type of spectrum sending methodologies. Radio location systems are the most common technologies that are used for identifying a primary user transmitter by measuring the distance between the transmitter and receivers. These techniques are dependent on the signal strength which is being received, i.e., (RSS) or the Received-Signal-Strength, the arrival angle (AOA), viz., the Angle-of-the-Arrival, time of the arrival (TOA) or the difference of the time of the arrival (TDOA). Cryptography based techniques are mainly used encryption techniques, authentication techniques like Advanced Encryption Standard, RSA, Digital Signature and the Hash Function.

Li, Bowen and Panlong worked on the optimal frequency-temporal opportunity exploitation for multichannel ad hoc networks & produced astonishing results in their research paper in [1]. Liang *et.al.* wrote a guest article in a IEEE journal, the topic being titled as Cognitive Radio - Theory and Application in [2]. Mustonen *et.al.* produced an excellent paper on the topic of an evolution toward cognitive cellular systems: licensed shared access for network optimization in [3], but had couple of disadvantages. Kovarik worked on the Cognitive Research: Knowledge Representation and Learning in [4] & produced excellent results. Recent advances on radio-frequency design in cognitive radio was presented by Misilmani *et.al.* in [5].

Defense against Primary User Emulation Attacks in Cognitive Radio Networks was worked upon by the combination of Chen & Park in [6]. Sharma Rajesh & Rawat Danda studied on the Advances on Security Threats and Countermeasures for Cognitive Radio Networks & produced an excellent survey paper in [7]. A Spectrum Decision Framework for Cognitive Radio Networks was developed by Lee *et.al.* in [8]. Spectrum mobility in cognitive radio networks was projected in a elaborative manner by Christian *et.al.* in [9]. Fathima *et.al.* in [11] developed a Bayesian Recovery with Toeplitz Matrix for Compressive Spectrum Sensing in Cognitive Radio Networks with very good experimental results. The same authors further carried out an extensive survey on Compressive Sensing Techniques for Cognitive Radio Networks in their review article published in [12].

Further, Arjoune and Kaabouch carried out comprehensive surveys on spectrum sensing in cognitive radio networks w.r.t. the Recent advances, new challenges, and future research directions in [13]. A survey on the Cooperative Spectrum Sensing in Cognitive Radio Networks was put forth by the group of researchers led by Akyildiz *et.al*. in [14]. The Performance Evaluation of Spectrum Sensing Techniques for Cognitive Radio Systems by Manesh *et.al.* in [15] which was a part of the work from the Cooperative Spectrum Sensing article put forth in [16].

Compressive Wideband Spectrum Sensing in Cognitive Radio Systems Based on Cyclostationary Feature Detection was studied with simulation approaches in [17] by the team of authors led by Damavandi *et.al*. & the same authors published another excellent article on the cognitive radio network security status and challenges in [18]. Countermeasures for layered security attacks on cognitive radio networks based on modified digital signature scheme was studied by John Soliman *et.al.* in [19] and presented in an international conference. A survey of security issues in Cognitive Radio Networks was conducted by the group of authors led by Fend *et.al*. in [20] in an review article. Security threats and countermeasures of MAC layer in cognitive radio networks was presented by Manesh *et.al*. in [21], this work was extended to the detection of the primary user emulation (PUE) attacks utilizing various spectrum sensing techniques in cognitive radio networks in [22].

A book chapter was published by Jung-Min titled as Cognitive radio network security, Cognitive Radio Communications and Networks in [23]. Sharma studied the Primary User Emulation Attack Analysis on Cognitive Radio & published it in [24]. The Performance Comparison of TOA and TDOA Based Location Estimation Algorithms in LOS Environment was projected in [26]. Locating the nodes in an Cooperative localization in WSNs was studied by Patwari *et.al.* in his journal paper in [27]. The work was extended to Range-based Primary User Localization in Cognitive Radio Networks by the Singh brothers in [28]. A Location Estimation Algorithm Based on RSSI Vector Similarity Degree was put forth by a excellent team of authors in [29]. In the work done by the authors in [26]-[29] suggested various location methods for the detection of PUEA using Time of Arrival (TOA),Time Difference of arrival (TDOA), Angle of Arrival (AOA) and Received Signal Strength (RSS) to detect the transmitter location.

Defense against PUE Attacks in CRNs Using Advanced Encryption Standard was developed by Alahmadi in [30]. The Analysis and Implementation of the Physical Layer Spectrum Usage Authentication in Cognitive Radio was carried out by Borle *et.al.* in [31]. Detecting Primary User Emulation Attacks in CRNs via PLNC was developed by the Xiongwei Xie *et.al*. in [32]. Chin-Shiuh Shieh. et.al, worked on the genetic watermarking based on transform-domain techniques using some sort of networking concepts in [33]. Defeating Primary User Emulation Attacks Using Belief Propagation in CRNs was developed by Yuan *et.al*. in their result oriented paper in [34]. In [30]-[34], the authors investigated the defense techniques for preventing PUEA using cryptographic technique like advanced Encryption Standard, Digital signature and Hash functions. Thus, the localization is a way of preventing this attack, by finding the location of incumbent user [30]-[34].

A system called radio frequency fingerprinting [35] has been addressed in one of the research papers. All of these methods generally require several computations, so overhead time is costly for networks. In a short time, this approach contributed to the discovery of

PUs with signals sampling and signal processing. In [35], the work based on the Radio Fingerprinting technique to identify the location of source and characteristics of the signal methods that are adopted to detect the PUEA was presented by the group of authors led by Mr. Rehman & their group, who carried out extensive work on the radio-frequency (RF) fingerprinting for mitigating primary user emulation attack in low-end cognitive radios in their lengthy paper in [35], which was used by many people across the world who were pursuing research on WSNs. Vaziri *et.al.* gave a brief review on the Countermeasure with Primary User Emulation Attack in this book in [36].

In [36]-[37], the game theory approach is used to describe the node of selfishness in a non-zero- sum game. The concept of employing Game Theory and TDMA Protocol to Enhance Security and Manage Power Consumption in WSNs-Based Cognitive Radio was studied by Abdalzaher in [37]. Celebi *et.al.* in utilization of location information in CRNs was in their paper in [38]. In [38] GPS, the location of the primary user was detected based on GPS system, but the main drawback of this system is due to weather conditions, obstacles affect GPS localization. In [39] the author proposed the TDoA techniques to identify the malicious user by measuring the transmitted signal's time difference. However, TDoA based technique requires a perfect synchronization between the users which is difficult to achieve. Further, Olga León. *et.al*., did some works on the cooperative detection of primary user emulation attacks in CRNs in [39] which was extended by Wild & Ramachandrdan in [40] to use it for detecting the primary receives for any type of CRN applications.

Like this, a large number of researchers had worked on the cognitive radio systems and in fact, only the important works have been presented in this literature survey [1]-[40]. In majority of the work done by the different researchers / authors presented in the previous references, there were lot of disadvantages / burdens / lacunas / drawbacks / deficiencies. Few of the drawbacks [1] – [40] of the works that were carried out by the earlier researchers were considered in our research work, studied in brief & algorithms were developed in order to overcome some of the deficiencies of the existing algorithms. The research work is verified through effective simulation results in the Matlab environment in order to substantiate the research problem undertaken in comparison with the work done by the earlier authors in the relevant field, in the sense to solve the desired objective (question – *Modeling based approach for the primary user emulation attack using location, feature detection technique & power estimation methods in Cognitive Radio Networks*) & arrive at the outcome (answer/solution – *Development of the mathematical model*) of the chosen research work [1]-[40].

3. Spectrum management process

Cognitive radio networks face many problems due to their coexistence with the primary network as well as the varying criteria for quality of service. Therefore new spectrum management functions should avoid primary user signal interference and to provide Quality of service. To address these obstacles, various functionalities in cognitive radio networks needed for spectrum management. Management method for spectrum consists of four major parts [8][9] as shown in Figure 1 as

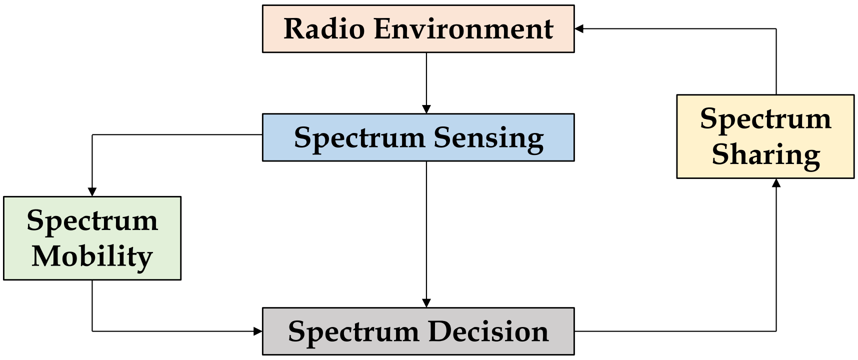

Figure 1 : Spectrum management process [10]

4. Spectrum sensing model

A CR users are designed to recognize changes in their environment and to make spectrum sensing an essential criterion for the feasibility of a cognitive network. Spectrum sensing allows users of cognitive radio to automatically adapt to changes in climate and operation by identifying spectrum holes that are not intended to cause conflict to primary user signals. Spectrum sensing is one of the most key functions of a cognitive transmitter, as it detects the use of spectrum in the surroundings. In real time, a cognitive radio must decide which band to sense, how long and when [11]. The general block-diagrammatic model of spectrum sensing is displayed as illustrated in the figure no. 2.

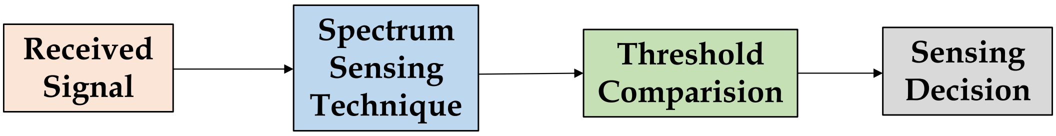

Figure 2 : General model of spectrum sensing

Existing approaches for spectrum sensing rely on detecting the primary transmitter activities. These schemes are generally classified into three main categories as shown in figure no. 3 as cooperative sensing, non-cooperative sensing, and interference-based detection [12]-[17], which are discussed one after the other in succession in the following paragraphs.

5. Non-cooperative sensing techniques

This strategy is also called local sensing, each SU seeks its own targets and does not take the decisions of other SUs into consideration. Since there is no contact or coordination between the various SUs which senses the same frequency band, the decision on spectrum sensing is made locally. The non-cooperative strategies are simple and require no high cost of processing time and hardware. But due to shadowing, fading, interferences and noise instability, they are subject to errors. These are implemented mainly when only one sensing terminal is available or when no contact between the SUs is possible. In order to identify the location of the primary user signal transmission, many non-cooperative sensing techniques have been suggested. Such techniques give the SUs more spectrum use possibilities without interruption or intrusiveness to the PUs. Examples of these techniques are presented in figure no. 3, namely Energy Detection, Matched Filter, Cyclostationary Detection, Waveform based sensing, Wavelet, Radio Identification and Eigenvalue detection.

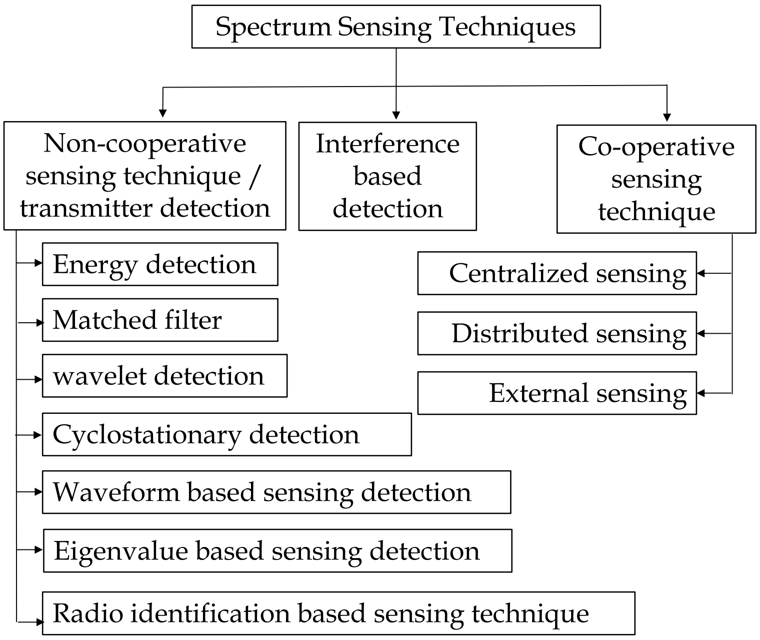
Spectrum Sensing Techniques
Non-cooperative sensing technique / transmitter detection
Interference based detection
Co-operative sensing technique
Energy detection
Matched filter
wavelet detection
Cyclostationary detection
Waveform based sensing detection
Eigenvalue based sensing detection
Radio identification based sensing technique
Centralized sensing
Distributed sensing
External sensing

Figure 3 : Existing spectrum sensing techniques

6. Challenges of Non-Cooperative Sensing

Cognitive radio (CR) technology is a promising solution to the inevitable problem of spectrum scarcity and underutilization. Cognitive radios can perform spectrum sensing, dynamically identify unused spectrum, and opportunistically utilize those spectrum holes for their own transmission. Cognitive radio technology is also a key concept suggested to be part of the fifth generation of cellular wireless standards (5G). Efficient spectrum sensing is crucial to the effective deployment of CR networks. Cooperative spectrum sensing (CSS) schemes can significantly improve the sensing accuracy of CR networks by exploiting multiuser spatial diversity. However, the cooperative gain can be impacted by factors such as the detection performance of each secondary user (SU) and the fusion techniques used to combine the secondary users' decisions. Moreover, CSS incurs cooperation overhead that may deteriorate its overall performance. Some of the Challenges of Non-Cooperative Sensing are listed as …

- *Measurement of Interference*: A cognitive radio does not completely know the position of primary receivers due to the weak inter-communication among primary users and cognitive radios. Therefore, modern methods are needed to complete the interference measurement at the primary networks.
- *Multi-user network spectrum sensing*: In the case of multiple secondary users and primary users it becomes more complex to sense the bands and measure interference. Thus, new efficient procedures need to be built for band sensing in case of multi-user networks.
- *Efficient spectrum sensing*: The cognitive radio is not able to implement both sensing and transmit data simultaneously. It is known as sensing efficiency problem. Appropriately, transmitting should not take place while sensing the spectrum. Also, specific algorithms must be developed so that the time to sense the spectrum should be reduced under the sensing preciseness.

7. Cooperative sensing & its challenges

Cooperative sensing is a solution to noise distortion, fading and shadowing issues in the spectrum sensing. The risk of misdetection and false alarm is significantly reduced by cooperative sensing and also overcome the hidden primary user problem. Cooperative sensing problems include the development of effective algorithms for sharing information and increased complexity. For cooperative sensing, there are three essential methods which could be listed as

1) Centralized sensing
2) Distributed sensing &
3) External sensing

There are several factors which make the sensing problem difficult to solve, some of them are

1) Very low signal-to-noise ratio (SNR)
2) Wireless channel fade and time dispersion can complicate the sensing problem
3) Noise uncertainty problem.

8. Spectrum decision & its challenges

Spectrum decision is defined as the ability to decide whether to use the spectral band within the available frequency bands according to the quality of service requirements. Spectrum decision typically involves each secondary user’s local sensing report and analysis of the primary user network. This involves two important points, viz., the reconfiguring aspect and the spectrum bank aspects.

- Reconfigure: The methods of cognitive radio networks reconfigure certain features of transportation for the ideal performance in a specific spectrum.
- The decision of spectrum band between dissimilar bands: The CRs are have to decide which spectrum band to select between authorized and unauthorized spectrum bands.

9. Spectrum Mobility & its Challenges

The secondary users should handover the occupied spectrum bands when primary user (authorized user) wants to utilize the spectrum bands. The primary objective of this spectrum mobility is to provide accurate transitions while handling the spectrum. This

- Time-domain mobility: Based on the possibility of unused spectrum bands cognitive radio adapts to the band. Due to the changing nature of the unused spectrum bands, the quality of service here must turn out to be a threat.

- Space mobility: As the secondary users change from point to point over time the presence of accessible bands also switches over time. Thus, regular allotment of unused bands in these networks is a challenging problem.

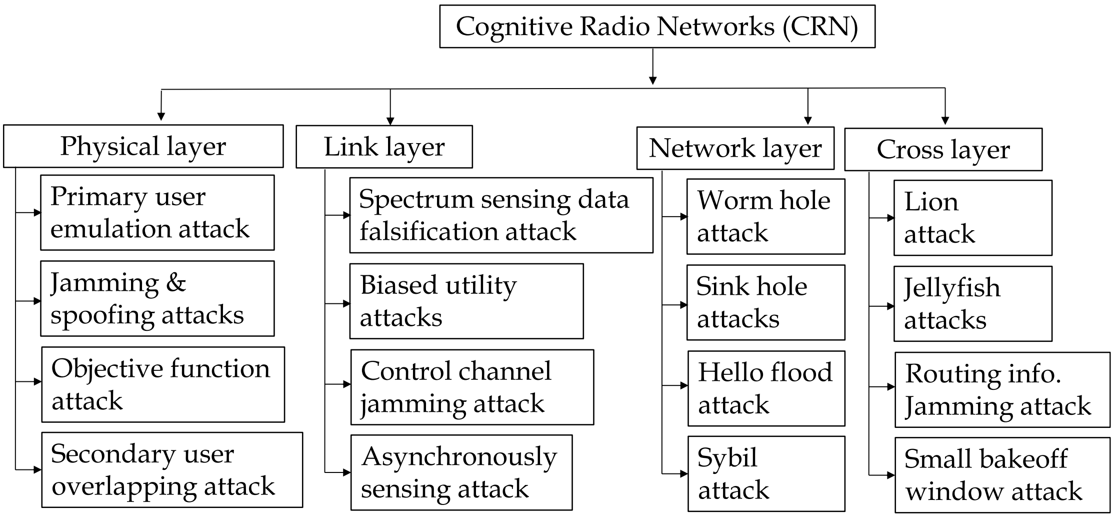
Cognitive Radio Networks (CRN)
Physical layer
Primary user emulation attack
Jamming & spoofing attacks
Objective function attack
Secondary user overlapping attack
Link layer
Spectrum sensing data falsification attack
Biased utility attacks
Control channel jamming attack
Asynchronously sensing attack
Network layer
Worm hole attack
Sink hole attacks
Hello flood attack
Sybil attack
Cross layer
Lion attack
Jellyfish attacks
Routing info. Jamming attack
Small bakeoff window attack

Figure 4 : Attacks taking place in the CRNs [22]

10. Cognitive Radio Networks Attacks

CR Networks solve the spectrum utilization problem by allowing unlicensed users to access licensed users spectrum bands without any interference. Due to this flexibility, CR Networks are exposed to different types of security threats and attacks from the unauthorized users, and this causes severe performance degradation of the network. There are various detection and mitigation techniques to protect the cognitive radio networks. To design a secure framework for cognitive radio networks the following aspects to be considered [18]. The different types of attacks taking place in the CRNs is best explained using a block diagrammatic approach as shown in the Fig. 4.

- *Data Integrity* : Data integrity is the fundamental security component in the case of wireless networks as compared to networks that use wires, Data integrity guards the data against modification that is being transferred; there is no inserting of data or deleting of data etc.
- *Data Confidentiality* : Data confidentiality makes the data or information, which is being transferred is not readable to malicious users.
- *Authentication* : Authentication makes sure that the unlicensed users cannot approach to sensitive data. Authentication is considered as one of the elemental security requisites for CRNs because to differentiate secondary users from primary users in CRN.
- *Availabili*ty : Availability is a process where authorized and non-authorized users can utilize the frequency spectrum in CRNs. In the case of authorized or primary users, it means using the accessible band to transfer data and not being intervened by secondary users and in case of secondary user, it means using the accessible holes of the spectrum band to transfer data and not causing any disturbance to licensed users of that band. This component helps to prohibit DoS outbreaks.
- *Non-repudiation* : Non-repudiation prohibits the transmitter or receiver from refusing the transferred data. The non-repudiation method is useful to validate the misdeed and restrict the invader from the network if an invader is recognized as disobeying the rules.

In this section, we mainly focusing on different types of security attacks specially targeting at cognitive radio networks and we categorized the security attacks based on the layers they are targeting as shown in the Figure No. 4. Primary User Emulation Attack, Jamming and spoofing Attacks, Objective function Attack (OFA), Secondary user overlapping attack in the Physical Layer. Spectrum Sensing Data Falsification Attack (SSDF), Biased Utility Attacks, Control Channel Jamming Attack, Asynchronously Sensing Attack in the Link Layer (MAC layer). Hello flood attack, Wormhole Attack, Sinkhole attack, Sybil Attack in the Network layer. Lion Attack. Jellyfish Attack, Routing Information Jamming and Small Bakeoff Window in the Cross Layer [19]-[21].

11. Primary user emulation (PUE) attack

One of the most extreme attacks is a primary user emulation attack (PUEA), whose objective focuses on the layers of physical CR and MAC. In this attack the malicious node deludes other secondary users by mimicking the transmission features of the incumbent user (PU). It produces a negative threat to the incumbent user, and thwarts other secondary users' use of idle frequency bands. Furthermore, the emulation of the incumbent user signal in multiple channels extends the SU handoff, leading to reduced network performance [6], [23]-[25]. The figure no. 5 shows an example of a primary user emulation attack. The malicious user (PUE attacker) mimic as a PU and other legitimate SUs considered, this as incumbent primary user. Then they send false information to the Fusion Centre, these can increase the probability of false detection. Due to some of the problems that are hidden in the primary users, the primary signal position may not be recognized by the secondary user which would affect the other legitimate user of the CR system.

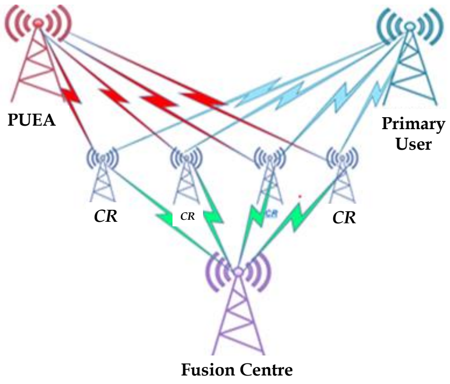

Figure 5 : Primary User Emulation Attack [10]

When the communication aspects in the CR system are taken into consideration, there are lot of chances of signal fading and shadowing effect, etc., which causes the interference with the primary signal. There are mainly attacks like Byzantene attackers, Primary user's emulation attacker (PUEA), where as in this work, we mainly stress on PUEA, which is one of the major attacking effects on the spectrum sensing detection method. In a CR network, the authorized user is being referred to as the primary user (PU) to have the highest priority over unauthorized users, which are being called as secondary the users (SU) for utilizing the band of frequencies. Hence, some of the secondary users are taking advantage of this opportunity by imitating as the authorized user characteristics, to utilize a frequency band with priority over other users [8]-[10].

This scenario is referred as PUEA, which is pictorially illustrated in the Figure No. 5. In this figure no. 5, the red coloured lines indicated that the legitimate secondary user misinterpreted as the primary signal is present.

12. Detection and countermeasure techniques

There are several researches that have been conducted to mitigate the PUE attack. In this section we addressed few of them as illustrated in the figure no. 6.

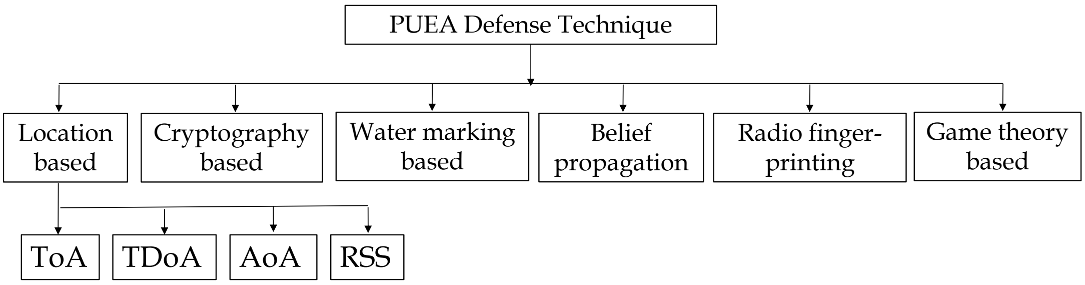

Figure 6 : PUEA detection and countermeasure techniques.

Localization-based methods

In this technique, the position and signal properties of the signal transmitter can be used to verify the primary user signal. In conventional methods for finding the location of PU signals, the time of arrival (TOA), time differential (TDOA), angle of arrival (AOA) and Received signal strength (RSS) are used. The detection technique is based on the RSS measurements, the CR users obtain the RSS peak and determine the location of the primary user or malicious user position by comparing the primary user's known location. When the grid size is small, this technique is more effective. But the main drawback of the technique is that location error increases due to the network size increases [26]-[29].

Cryptographic approaches

In this technique the PUEA can be mitigated using cryptographic techniques like public key encryption, digital signatures, Hash functions, and other authentication techniques for communications between primary and secondary users. The main issue here is that the solutions do not meet requirements of the FCC, which notes that “secondary users should be able to use the available spectrum without altering the primary users and their signals”. Therefore, PU authentication is a challenging issue, and existing proposals are subject to practical limitations [30]-[32].

Watermarking-based methods

In this technique, every PU signal is watermarked for authentication before transmission in order to prevent the PUEA problem. One of the benefits is that no modifications are required in digital television systems and their existing protocols. This method is based on hash functions, it reduces bit error rate in the networks [33].

Belief propagation-based methods

ISSN: 2233-7857 IJFGCN

In this techniques , each SUs calculate the location and compatibility functions of the primary or malicious user, and then exchange messages with other SU's to calculate a belief function in an iterative manner. The main drawback of this approach is that position and efficiency calculations are more complicated [34].

Radio fingerprinting

Fingerprinting radio is a method to identify the source of signal through location of the radio transmission and by analyzing the transmission characteristics, including specific radio frequencies. Each source has own specific "fingerprint" based on location and their configuration parameters. The main drawback of this techniques is that it requires physical proximity to the PU to check its fingerprints and to make them costly [35].

Game theory based

This technique is based on mathematics and economics to prevent malicious user for utilize the spectrum bands. In this method, each secondary user maintain an internal table called Trust list able which consists of authentication ID of the propagating user. Based on this table each secondary user decide the primary user or malicious user. In CRN, attackers try to use the channel by violating the rules all the time. Therefore game theory is a good solution for preventing this type of users [36].

13. System Mathematical Model development

In the development of the mathematical model, we have used two important concepts, viz.,

(a). Primary user localization based PUEA mitigation technique

(b). Power estimation based PUEA mitigation technique

which could be used to develop the system mathematical model for a typical CRN system as shown in the Fig. No. 7.

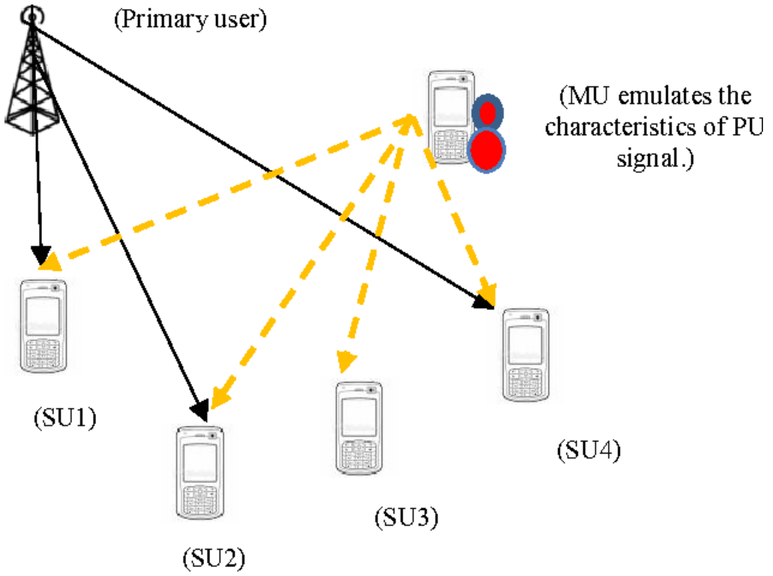

Figure 7 : PUE Emulation Attacking Model

In this paper, first we summarize traditional localization techniques in wireless networks before presenting the new localization method, and then analyze how these techniques should be enhanced to solve the primary signal localization issue in CR networks. The traditional approaches to localization are based on one or more of the following techniques: Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), and Received signal strength (RSS). The traditional methods like ToA, AoA and TDoA are required the expensive hardware to address location of PU signal. In this work, we proposed RSS based location to identification of transmitter or receiver signals. The RSS also referred to as RSSI (Received Signal Strength Indicator) is a measure of the strength present in a radio signal received. Measured in dBm, the RSS values have typical negative values ranging from 0 dBm (excellent signal) to –110 dBm (extremely poor signal). The localization techniques using RSS measurements are primarily classified into (1) range-based positioning, (2) RF fingerprinting, and (3) proximity-based positioning. RSS will solve the following two problems

1) Path fading over time and PUE attackers which are continuously changing, it in turn vary the transmission power to locate the location.
2) Continuously variations in receiver signal strength magnitude, it is usually larger i.e 30 to 40 dB over a distance.

RSS-based techniques are relatively inexpensive and simple to implement in hardware, but they are susceptible of high errors due to the dynamics of indoor/outdoor environments, mainly due to multipath signals and shadowing.

Before discussing PUEA mitigation techniques, we state some of the assumptions which form the basis for the technique. A network consisting of the television signal transmissions (i.e. the stationary television broadcasters) and receivers is expected to be the primary user. The transmitting power of a television tower is typically hundreds of thousands of watts [27]. Depending on the height of the transmitter station the transmissions range differ between 40 to 60 milles. We believe that the secondary users are smart devices and each equipped with a handheld CR unit. The Cognitive radios are considered as self-locating and has a maximum output power from hundred milli watts (mW) to few watts (W), usually equivalent to a transmission range of several hundred metres (*m*). A malicious user can alter modulation technique, frequency and transmission output power.

In the first step each receiver compare the signal characteristics with secondary users signal characteristics like signal energy level, modulation technique, Frequency etc. if this characteristics matches the characteristics of secondary user then conclude that is secondary user. In this case all the receivers have a prior knowledge about secondary user signal characteristics. In this paper we considered frequency modulation technique for primary user signal and QPSK technique for malicious user signal. We analyzed and distinguish these two signals based on their modulation scheme using cyclostationary feature detection techniques. This detection techniques classifies the signals based on position of the peaks in spectral autocorrelation function.

Power spectral density function (PSD) shows the strength of the variations (energy) as a function of frequency. In other words, it shows at which frequencies variations are strong and at which frequencies variations are weak. The unit of PSD is energy (variance) per frequency (width) and you can obtain energy within a specific frequency range by integrating PSD within that frequency range. PSD is a very useful tool to identify the frequencies and amplitudes of transmitted signals. The power spectral density (PSD) of the signal describes the power present in the signal as a function of frequency, per unit frequency. Power spectral density is a key term in sensing spectrum. In order to evaluate a signal in the frequency domain, the power spectral density (PSD), $S_{XX}(f)$, is used to characterize the signal obtained by taking the $R_{XX}(f)$ autocorrelation Fourier transformation of the x(t) random wide-sense stationary (WSS) phase. The PSD and the autocorrelation of a function are mathematically related by the Einstein - Wiener - Khinchin (EWK) relations given by the equations (1) & (2) as

$$R_{xx}(f)=\int_{-\infty}^{\infty} S_{xx}(\tau).e^{+j2\pi f t}df \tag{1}$$

$$S_{xx}(f)=\int_{-\infty}^{\infty} R_{xx}(\tau).e^{-j2\pi f t}d\tau \tag{2}$$

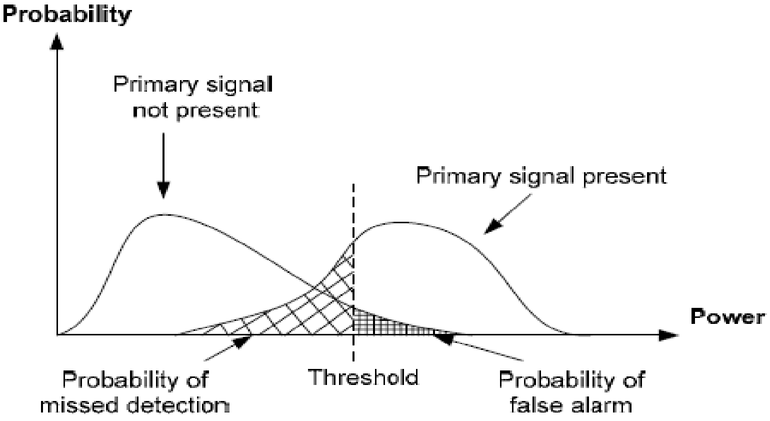
Probability
Primary signal not present
Primary signal present
Power
Probability of missed detection
Threshold
Probability of false alarm

Figure 8 : The probability density functions of the received signal.

In the Figure No. 8, where the probability density functions of the received signal can be identified with and without the primary signal. If we want to keep the likelihood of missed detections very low, the likelihood of false alarms increases and this would lead to low spectrum usage. On the other hand, a low probability of false alarms would result in a high probability of missed detection which increases the primary user interference. This trade-off must be looked into carefully. Typically the primary signal detection sensing can be formulated as a question of binary hypothesis as given by the equation no. (3) as

$$x(t)=\begin{cases} n(t) & H_0 \\ h(t)*s(t)+n(t) & H_1, \end{cases} \tag{3}$$

where $x(t)$ is the received signal at the secondary user, $s(t)$ is the Primary user signal, $h(t)$ is the channel gain, $n(t)$ is the zero-mean additive white Gaussian noise (AWGN), H_0 and H_1 denote the test hypothesis, H_0 denoting the absence of the PU signal. H_1 denoting the presence of the PU signal. Detection mechanisms are tested by means of two parameters, viz., the primary and the secondary signals are missing due to additive white Gaussian noise (AWGN) to classify positions during simulation or operation to detect these two signals or not, the following two equations in (4) & (5) could be used.

$$P_d = \text{Probabilities ofdetection} = \frac{H_1}{H_1} = P_r\left(y > \frac{\rho}{H_1}\right) \tag{4}$$

where *y* is decision statistics and *ρ* is threshold, which is used for decision and depending on

$$P_d = Q_m\sqrt{2r}.\sqrt{\rho} \tag{5}$$

$$P_{f\,a} = \frac{m.\frac{\rho}{2}}{m} \tag{6}$$

where

$$P_{f\,a} = P_r\left(y > \frac{\rho}{H_0}\right) \tag{7}$$

We assume a network area of 1500 × 1500 m^2. Two TV transmitters (Primary users) are fixed location, one is placed at (800 m, 1000 m) and (300 m, 550 m) as second. The transmitting power of the primary users are 100 kw and 50 kw respectively. We deployed 30 secondary users including both (legitimate secondary users and the attackers) are randomly and uniformly distributed in the network with transmitting power 40kw and radius 30 m. First we calculated the distance between primary users and malicious users at secondary receivers using Eqn. (8).

$$d_i = \sqrt{\left(x - x_i\right)^2 + \left(y - y_i\right)^2}\ . \tag{8}$$

Then we evaluated power of the primary users and malicious users at each secondary users using the following equation (9):

$$P_r = \frac{P_t G_t}{d^2}\,. \tag{9}$$

To locate exact location of primary users the following equation (10) is used

$$M = P_t + \alpha_0 + \alpha_1 \ln\left(d\right), \tag{10}$$

where *M* is mean of RSS which is measured from Gaussian random model, α_0 & α_1 are constants and *d* is distance between Transmitter and Receiver. For path propagation and subsequent power loss:

$$Mean = 10.\log_{10}\left(P_m\right) - 40.\log_{10}\left(d_j\right), \tag{11}$$

where d_j is the distance between the j^{th} malicious user and the secondary user. Transmission loss for distance metrics:

$$\mu_p = 10.\log_{10}\left(P_t\right) - 20.\log_{10}\left(d\right) \tag{12}$$

Resilient spectrum sensing method is a cyclostationary feature recognition as modulated information is a cyclostationary operation. As a consequence, even in low-SNR conditions, cyclic detectors can work successfully.

14. Future work

In the future work, we are using this mathematical model in the algorithm that is being developed as a ***.m*** code in the Matlab environment to simulate the various results, have a brief discussion on the various aspects of the chosen research work and compare the work that is being carried out with the work done by other researchers in order to establish the supremacy of the work done showing the effectivity and the profoundness. This would be taken up as a simulation work of another paper in the forthcoming days.

15. Conclusive remarks

In this concluding section, the conclusive remarks about the work done in this paper is being presented in a nutshell. Cognitive Radio Technology is a developing technology that makes the opportunistic use of spectrum holes in the licensed band by the unlicensed users without causing any interference among the licensed users. These networks mainly depend on spectrum sensing to search for spectrum holes in the licensed spectrum not used by the incumbent users. The Primary User Emulation (PUE) attacks can utilize this feature by mimicking as incumbent signals and results decrease the effectiveness of CRN performance. In this mathematical modelling paper, we have analyzed the PUE attack and distinguished whether the transmitter is a primary user transmitter or a PUE attacker transmitter based on localization and power detection techniques. Location based techniques are relatively inexpensive and simple to implement in hardware, but they are Location based techniques are relatively inexpensive and simple to implement in hardware, but they are susceptible of high errors due to multipath signals and shadowing. The location based technique has more number of false detection and misdetection compare to PSD technique. Using the basic concepts of the CRNs from the research articles from the papers [1]-[40], a mathematical model is being developed in this research paper. Further, the mathematical model developed in this research paper is going to be used in our future work (*concept that is used for another paper*) for the simulation experiments to show the disruptive effects of primary user emulation attacks & the tool that is going to be used for performing the simulations in the Matlab 2018a.

References

[1]. Li, Bowen, and Panlong, "Optimal Frequency-Temporal Opportunity Exploitation for Multichannel Ad Hoc Networks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, issue 12, (Dec 2012), pp. 2289-2302.

[2]. Liang, Ying-Chang & Chen, Hsiao-Hwa & III, Joseph & Mähönen, Petri & Kohno, Ryuji & Reed, Jeffrey & Milstein, Laurence. (2008), Guest Editorial – "Cognitive Radio: Theory and Application", *IEEE Journal on Selected Areas in Communications*, vol. 26, (2008), pp. 1-4. 10.1109 / JSAC.2008.080101.

[3]. M. Mustonen, M. Matinmikko, M. Palola, S. Yrjölä and K. Horneman, "An evolution toward cognitive cellular systems: licensed shared access for network optimization," *IEEE Communications Magazine*, vol. 53, no. 5, (May 2015), pp. 68-74.

[4]. V. Kovarik, Jr., “Cognitive Research: Knowledge Representation and Learning”, in B. Fette (ed.), *Cognitive Radio Technolog*y, Burlington, (2006), MA: Elsevier, Inc..

[5]. H. M. E. Misilmani, M. Y. Abou-Shahine, Y. Nasser, and K. Y. Kabalan, “Recent advances on radio-frequency design in cognitive radio,” *Int. J. Antennas and Propagation*, vol. 2016, Article ID 9878475, (Jan. 2016), pp. 1–16.

[6]. R. Chen, J. Park and J. H. Reed, “Defense against Primary User Emulation Attacks in Cognitive Radio Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, (Jan. 2008), pp. 25-37.

[7]. Sharma, Rajesh & Rawat, Danda B., “Advances on Security Threats and Countermeasures for Cognitive Radio Networks : A Survey”, *IEEE Communications Surveys and Tutorials*, (2015), 10.1109 / COMST.2014.2380998.

[8]. Lee, Won-Yeol & Akyldiz, I.. “A Spectrum Decision Framework for Cognitive Radio Networks, *IEEE Trans. Mob. Comput*., vol. 10, (2011), 161-174.

[9]. I. Christian, S. Moh, I. Chung and J. Lee, “Spectrum mobility in cognitive radio networks”, *IEEE Communications Magazine*, vol. 50, no. 6, (June 2012), pp. 114-121.

[10]. Mr. Mahesh Kumar N., Dr. Siddesh G.K., “Detection of the primary user emulation (PUE) attacks utilizing various spectrum sensing techniques in cognitive radio networks”, *Web of Science’s - International Journal of Grid and Distributed Computing*, IJGDC, Indexed in EBSCO, Vol. 13, No. 1, (2020), ISSN: 2005-4262, (6 March 2020) pp. 256-271.

[11]. F. Salahdine, N. Kaabouch, and H. El Ghazi, “A Bayesian Recovery with Toeplitz Matrix for Compressive Spectrum Sensing in Cognitive Radio Networks,” *Wiley’s International Journal of Communication Systems*, (2017), pp. 1–13.

[12]. F. Salahdine, N. Kaabouch, and H. El Ghazi, “A Survey on Compressive Sensing Techniques for Cognitive Radio Networks,” *Phys. Commun*., vol. 20, (2016), pp. 61–73.

[13]. Y. Arjoune and N. Kaabouch, “A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions,” Sensors, vol. 19, no. 1, (2019), p. 126.

[14]. Akyildiz, Ian & Lo, Brandon & Balakrishnan, Ravikumar. “Cooperative Spectrum Sensing in Cognitive Radio Networks: A Survey”, *Physical Communication*, vol. 4, (2011), pp. 40-62. 10.1016 / j.phycom.2010.12.003.

[15]. M. R. Manesh, S. Apu, N. Kaabouch, and W. Hu, “Performance Evaluation of Spectrum Sensing Techniques for Cognitive Radio Systems,” Ubiquitous Computing, Electronics & Mobile Commun. Conf., IEEE Annual, (2016), pp. 1–6.

[16]. K. Ben Letaief and W. Zhang, “Cooperative Spectrum Sensing,” *Cognitive Wireless Communication Networks*, (2007), pp. 115–138.

[17]. Damavandi, M.A.; Nader-Esfahani, S., “Compressive Wideband Spectrum Sensing in Cognitive Radio Systems Based on Cyclostationary Feature Detection”, *Proceedings of the International Conference on Next Generation Mobile Applications, Services, and Technologies*, Cambridge, UK, (9–11 September 2015), pp. 282–287.

[18]. Sameer, Ameer & Sadkhan, Eng. Sattar B., “Cognitive radio network security status and challenges”, *2017 Annual Conference on New Trends in Information & Communications Technology Applications* (NTICT) (Mar. 2017), pp. 1-6, 10.1109/NTICT.2017.7976105.

[19]. John N. Soliman, Tarek Abdel Mageed, Hadia M. El-Hennawy, “Countermeasures for layered security attacks on cognitive radio networks based on modified digital signature scheme”, *Eighth International Conference on Intelligent Computing and Information Systems* (ICICIS), (2017 .

[20]. J. Li, Z. Feng, Z. Feng and P. Zhang, “A survey of security issues in Cognitive Radio Networks,” *China Communications*, vol. 12, no. 3, (Mar. 2015), pp. 132-150.

[21]. Manesh, M. R., & Kaabouch, N., “Security threats and countermeasures of MAC layer in cognitive radio networks”, *Ad Hoc Networks*, vol. 70, (2018), pp. 85-102.

[22]. Mr. Mahesh Kumar N., Dr. Siddesh G.K., “Detection of the primary user emulation (PUE) attacks utilizing various spectrum sensing techniques in cognitive radio networks”, *Web of Science’s - International Journal of Grid and Distributed Computing*, *IJGDC*, Indexed in EBSCO, ProQuest, ULRICH, DOAJ, J-Gate, Cabell, Emerging Sources Citation Index (ESCI) from Web of Science (Clarivate Analysis), Vol. 13, No. 1, (2020), ISSN: 2005-4262, (6 March 2020), pp. 256-271.

[23]. Jung-Min Jerry Park, Kaigui Bian, Ruiliang Chen, “Chapter 15 - Cognitive radio network security, Cognitive Radio Communications and Networks”, *Academic Press*, (2010), Pages 431-466, ISBN 9780123747150, https://doi.org/10.1016/B978-0-12-374715-0.00015-0.

[24]. Sharma, Himanshu; Kumar, Kuldip, “Primary User Emulation Attack Analysis on Cognitive Radio”, *Indian Journal of Science and Technology*, (Apr. 2016). ISSN 0974-5645. doi:10.17485 / ijst / 2016 / v9i14/87432.

[25]. Marinho J, Granjal J, Monteiro E., “A survey on security attacks and countermeasures with primary user detection in cognitive radio networks”, *EURASIP Journal of Information Security*, vol. 1, (2015), pp. 1–14.

[26]. Shen G., Zetik R., & Thorma, R.S., “Performance Comparison of TOA and TDOA Based Location Estimation Algorithms in LOS Environment”, *IEEE Proceedings of the 5th Workshop on Positioning, Navigation and Communication*, (2008).

[27]. Patwari N., Ash J.N., Kyperountas S., Hero A.O., Moses R.L. & Correal N.S., “Locating the nodes: Cooperative localization in wireless sensor networks”, *IEEE Signal Processing Magazine*, vol. 22, no. 4, (2005), pp. 54–69.

[28]. Awadhesh Kumar Singh, A.K. Singh, “Range-based Primary User Localization in Cognitive Radio Networks”, *Procedia Computer Science*, Vol. 93, (2016), pp. 199-206, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2016.07.201.

[29]. Shang, Fengjun & Su, Wen & Wang, Qian & Gao, Hongxia & Fu, Qiang., “A Location Estimation Algorithm Based on RSSI Vector Similarity Degree”, *International Journal of Distributed Sensor Networks*, (2014), pp. 1-22. 10.1155/2014/371350.

[30]. A. Alahmadi, M. Abdelhakim, J. Ren and T. Li, “Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard”, *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, (May 2014), pp. 772-781.

[31]. K.M. Borle, B. Chen and W.K. Du, “Physical Layer Spectrum Usage Authentication in Cognitive Radio: Analysis and Implementation,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, (Oct. 2015), pp. 2225-2235.

[32]. Xiongwei Xie, Weichao Wang, “Detecting Primary User Emulation Attacks in Cognitive Radio Networks via Physical Layer Network Coding”, *Procedia Computer Science*, Volume 21, (2013), Pages 430-435,

[33]. Chin-Shiuh Shieh. *et.al*, “Genetic watermarking based on transform-domain techniques”, *Pattern Recognition*, Volume 37, Issue 3, (2004), Pages 555-565.

[34]. Z. Yuan, D. Niyato, H. Li, J.B. Song and Z. Han, “Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, (November 2012), pp. 1850-1860.

[35]. S. U. Rehman, K. W. Sowerby and C. Coghill, “Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios,” *IET Communications*, vol. 8, no. 8, (22 May 2014), pp. 1274-1284.

[36]. Vaziri Yazdi, S.A., Ghazvini, M., “Countermeasure with Primary User Emulation Attack”, *Cognitive Radio Networks - Wireless Perceive Communications*, ISSN 2261–2277, vol. 108, (2019), https://doi.org/10.1007/s11277-019-06521-9.

[37]. M.S. Abdalzaher and O. Muta, "Employing Game Theory and TDMA Protocol to Enhance Security and Manage Power Consumption in WSNs-Based Cognitive Radio," in IEEE Access, vol. 7, pp. 132923-132936, 2019.

[38]. Celebi, H., & Arslan, H., "Utilization of location information in cognitive wireless networks", *IEEE Wireless Communications*, vol. 14, (2007), pp. 6–13.

[39]. Olga León. *et.al.*, "Cooperative detection of primary user emulation attacks in CRNs", *Computer Networks,* Volume 56, Issue 14, (2012), pages 3374-3384.

[40]. B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *Proc. IEEE DySPAN*, (Nov. 2005), pp. 124–130.