

**Primary User Emulation Attack (PUEA)
In
Cognitive Radio Network (CRN)**



By

Mohammad Hanif Rahman (SID # 2013-1-98-004)
&
Md. Meraz Hossain (SID # 2013-2-98-003)

A Research Project Submitted in Partial Fulfillment of the Requirements
for the Degree of Masters of Science in Telecommunications Engineering

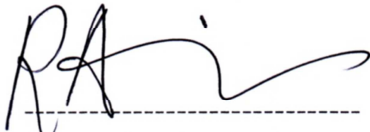
**DEPARTMENT OF ELECTRONICS & COMMUNICATIONS ENGINEERING
EAST WEST UNIVERSITY**

August 2014

APPROVAL

The Research Project Report “Primary User Emulation Attacks (PUEA) in Cognitive Radio Networks (CRN)” submitted by Mohammad Hanif Rahman (SID # 2013-1-98-004) and Md. Meraz Hossain (SID # 2013-2-98-003), to the Department of Electronics & Communications Engineering, East West University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Masters of Science in Telecommunications Engineering and approved as to its style and contents.

Approved By:



(Supervisor)

M. Ruhul Amin, PhD.

Professor

ECE Department

East West University



(Supervisor)

Dr. Md. Imdadul Islam

Professor (Adjunct)

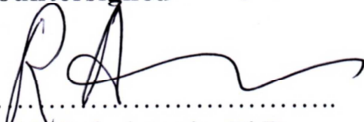
ECE Department

East West University

DECLARATION

We, hereby, declare that the work presented in this Research Project is the outcome of the investigation performed by us under the supervision of M. Ruhul Amin, PhD., Professor, Department of Electronics & Communications Engineering, East West University and Dr. Md. Imdadul Islam, Professor (Adjunct), Department of Electronics & Communications Engineering, East West University. We also declare that no part of this Research Project and thereof has been or is being submitted elsewhere for the award of any degree or diploma.


Countersigned



.....
M. Ruhul Amin, PhD.

(Supervisor)

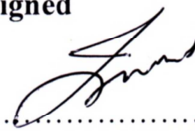
Signature



.....
Mohammad Hanif Rahman

SID # 2013-1-98-004

Countersigned



.....
Dr. Md. Imdadul Islam

(Supervisor)

Signature



.....
Md. Meraz Hossain

SID # 2013-2-98-003

ABSTRACT

In Cognitive Radio Networks the primary goal of the secondary users is to detect the presence of primary user. Different types of detection techniques are prevalent like average energy detection of sample data, matched filter based energy detection and Bayesian approach of prior and posterior modeling of average signal. The situation becomes cumbersome in case of presence of malicious users especially primary user emulator. In this project work we deal with detection of primary user emulator attack (PUEA) based on threshold energy detection model where exponential path loss model is used in a small region, where both secondary user and PUEA are randomly distributed and Okumura-Hata model for long links of secondary user and primary user. Finally we plot the lower bound of probability of PUEA against unoccupied distance of PUEA.

Table of Contents

Chapter 01: Introduction	1
Chapter 02: Cognitive Radio Network	4
2.1 Concept of Cognitive Radio Network	5
2.2 Terminologies	6
2.2.1 Primary User (PU)	6
2.2.2 Secondary User (SU)	6
2.2.3 Malicious User (MU)	6
2.2.4 Spatial False Alarm (SFA)	7
2.2.5 Spectrum Technology	7
2.2.6 White Spaces or Unused Spectrum	8
2.3 Spectrum Sensing Techniques	9
2.3.1 Non Cooperative Sensing	9
2.3.1.1 Energy Detection	9
2.3.1.2 Matched Filter	10
2.3.1.3 Cyclostationary Feature Detection	10
2.3.2 Cooperative Sensing	11
2.3.2.1 Centralized Access	12
2.3.2.2 Distributed Cooperative Sensing	12
2.3.3 Interference Based Detection	13
2.3.3.1 Interference Temperature Management	13
2.3.3.2 Primary Receiver Detection	13
2.3.4 Other Techniques	13
2.4 Malicious User and Their Impacts	14
Chapter 03: System Model	15
3.1 Localization of SU and MU in CR Network	16
3.1.1 Exponential Path Loss Model	16
3.2 Okumura-Hata Model	17
3.3 Assumed Parameters	18
3.4 Received Power Calculation from Path Loss Formula	20
3.5 Substituted Equations and Data in Mathcad Software	21
3.5.1 Input Data for Variation of Lower Bound of PUEA; When, $r_p = 2\text{km}$	21
3.5.2 Input Data for Variation of Lower Bound of PUEA; When, $r_p = 8\text{km}$:	23
Chapter 04: Results	25
4.1 Results and Discussion	26
Chapter 05: Conclusion	29
Reference	31

List of Figures

Chapter 02

Figure 2.1: Licensed & unlicensed users in cognitive radio network	5
Figure 2.2: Penetration capacity of TV white spaces signal	7
Figure 2.3: White spaces inside a used spectrum	9
Figure 2.4: Cooperative Sensing	11

Chapter 03

Figure 3.1: A Typical Cognitive Radio Network in A circular Grid with Secondary & Malicious User.	16
---	----

Chapter 04

Figure 4.1: Variation of lower bound of PUEA; where, $r_p = 2\text{km}$	27
Figure 4.2: Variation of lower bound of PUEA; where, $r_p = 8\text{km}$	28

CHAPTER: 1

INTRODUCTION

Spectrum sharing has always been an important aspect of system design in wireless communication systems due to the scarcity of the available resources/spectrum. Cognitive Radio in wireless communication system that enables unlicensed user (secondary user) to use the free spectrum (white space) for licensed user (primary user).

Although the secondary user can use the free spectrum of licensed user, there is a etiquette (thumbs of rule) to maintain. When licensed users are in use of the spectrum, secondary user cannot use the spectrum and during the usage of the spectrum if the secondary user sensed that primary user is going to use the spectrum, the secondary user is going to evacuate the spectrum [1]. This method of sharing is often called Dynamic Spectrum Access (DSA). There are different sensing mechanisms which could be discussed in detailed in later chapter.

The etiquette of evacuate the spectrum for primary user could be result of denial of service for secondary users if the system is not designed carefully. This happens as follows:

A small group of the secondary user generate enough power to make other secondary users to think that primary user is using or going to use the spectrum. Following the etiquette the maximum secondary users (good secondary users) release the spectrum and let the small group (bad secondary users or malicious users) use the spectrum unconsciously. Such an attack is called Primary User Emulation Attack (PUEA). The main disadvantage of this attack is the poor usage of the spectrum for unauthorized users and unfair advantage for the bad secondary users.

The PUEA depends on the determination of the location of the primary transmitter which is further determined by the direction of signal arrival. But most of the receivers in wireless network are omni directional resulting the detection process more complex.

The project report is organized like:

Chapter 2 gives the basic concept of radio network along with conventional detection technique.

Chapter 3 provides the analytical model of detection of PUEA.

Chapter 4 provides the result based on analytical model.

Chapter 5 Finally concludes the entire analysis.

CHAPTER: 2

COGNITIVE RADIO NETWORK

2.1 Concept of Cognitive Radio Network:

Cognitive Radio (CR) is an adaptive, intelligent radio and network technology that can automatically detect available channels in a wireless spectrum and change transmission parameters enabling more communications to run concurrently and also improve radio operating behavior [2].

Possible functions of cognitive radio include the ability of a transceiver to determine its geographic location, identify and authorize its user, encrypt or decrypt signals, sense neighboring wireless devices in operation, and adjust output power and modulation characteristics. [3]

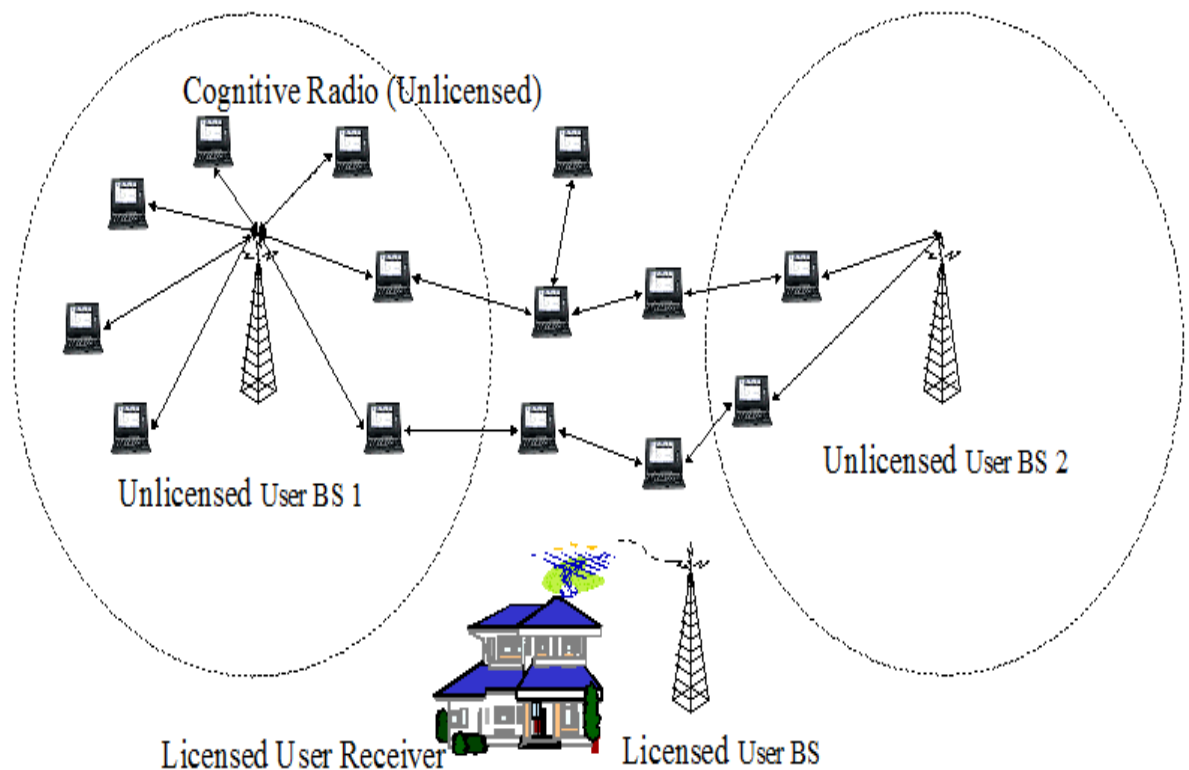


Figure 2.1: Licensed & unlicensed users in cognitive radio network

2.2 Terminologies:

As the Cognitive Radio Network is relatively new concept in the wireless technology, there are a lot of terms which are also new. In order to understand the total concept the following terms should be introduced:

2.2.1 Primary User (PU):

Primary users are the original users of a cognitive radio network. A primary user has higher priority or legacy rights on the usage of a specific part of the spectrum.

2.2.2 Secondary User (SU):

A user who has a lower priority and therefore exploits the spectrum in such a way that it does not cause interference to primary users. Secondary users are not belonging from the same network as the primary users are but wish to use the white spaces for their own communication is called the secondary receivers or transmitters. [4]

2.2.3 Malicious User (MU):

In Cognitive radio network there is a set of secondary users in a system and in the same system there is also a subset of illegal users. If these subset users generate enough power to the secondary user locations which may look like that a primary transmission is occurring. Then according to the rules the secondary users vacate the spectrum. Then the subset users will use those spectrums for their own. These subset bad secondary users are called “malicious users”. A number of good users can lose their access to the network for these types of incidents. All these happen for the malicious users. This occurrence provides poor usage of spectrum to the authorized users and at the same time the malicious users get unfair advantage.

2.2.4 Spatial False Alarm (SFA):

In cognitive radio, secondary user (SU) performs spectrum sensing with a certain sensing range. It is widely considered that a SU is permitted to utilize the primary channel if no primary user (PU) transmits data inside its sensing range. However, it is observed that a busy PU outside the sensing range still can be detected by SU. As a result, the SU misinterprets that this busy PU is inside its sensing range, and hereby loses opportunity to utilize the primary channel. This new sensing issue is termed as Spatial False Alarm (SFA) problem [5].

2.2.5 Spectrum Technology:

TV white spaces are the unused TV channels in any given market that could be used to deliver broadband access, services, and applications. TV white spaces devices and networks will work in much the same way as conventional Wi-Fi, but because the TV signals travel over longer distances and better penetrate walls and other obstacles, they require fewer access points to cover the same area. These excellent range and obstacle penetration characteristics explain why people increasingly refer to TV white spaces as "Super Wi-Fi."

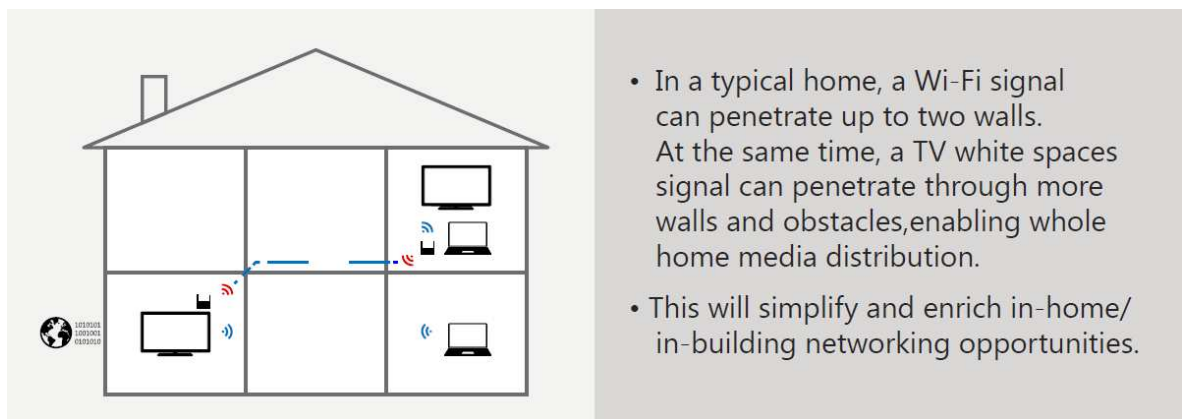


Figure 2.2: Penetration capacity of TV white spaces signal

Regulations in the United States provide for two classes of white space devices [6]:

- Fixed devices are permitted to operate at up to 4 Watts EIRP on second or more adjacent TV channels. They may operate on unused TV channels 2-51, except 3, 4, and 37.
- Personal/portable devices are permitted to operate at up to 40 milliWatts EIRP on adjacent channels and 100 milliWatts EIRP on second or more adjacent TV channels. They may operate on unused TV channels 21-51, except channel 37.

2.2.6 White Spaces or Unused Spectrum:

The term 'White Space' refers to portions of licensed radio spectrum that licensees do not use all of the time or in all geographical locations. Several regulators around the world are moving towards allowing unlicensed access to these frequencies, subject to the proviso that licensed transmissions are not adversely affected. By allowing access to these White Space frequencies, more effective and efficient use of the radio spectrum is envisaged. While the frequencies are unused, they have been specifically assigned for a purpose, such as a guard band. Most commonly however, these white spaces exist naturally between used channels, since assigning nearby transmissions to immediately adjacent channels will cause destructive interference to both. In addition to white space assigned for technical reasons, there is also unused radio spectrum which has either never been used, or is becoming free as a result of technical changes [7].

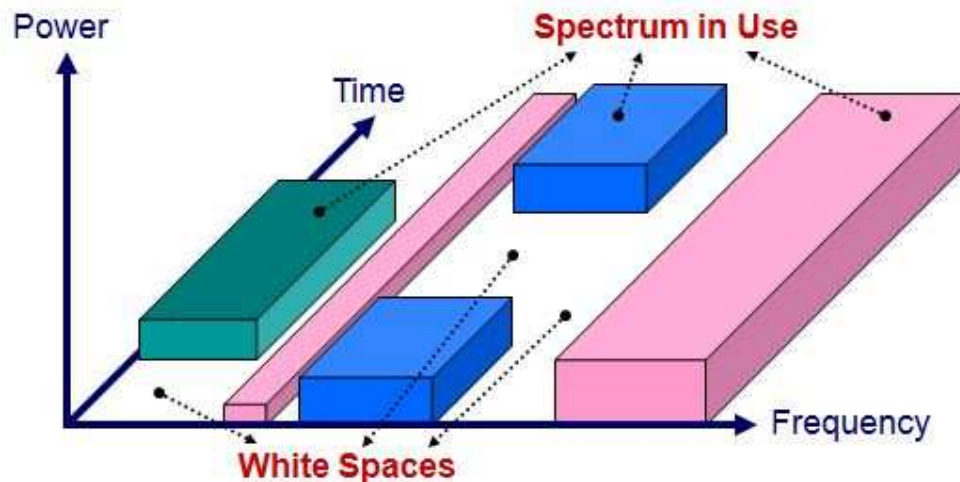


Figure 2.3: White spaces inside a used spectrum

2.3 Spectrum Sensing Techniques:

Cognitive the present literature for spectrum sensing is still in its early stages of development. A number of different methods for identifying the presence of signal transmissions have been proposed. The spectrum sensing techniques are classified broadly into three main types, transmitter detection or non cooperative sensing, cooperative sensing and interference based sensing.

2.3.1 Non Cooperative Sensing:

This form of spectrum sensing occurs when a CR acts on its own. Transmitter detection techniques are classified further into energy detection, matched filter detection and cyclostationary feature detection [10].

2.3.1.1 Energy Detection:

Energy detection (ED) is a non coherent detection method that detects the PU's signal based on the sensed energy [11]. ED is the most popular sensing technique in cooperative sensing because of its simplicity and no requirement for a priori knowledge of the PU's signal [12].

The ED is said to be a blind signal detector because it ignores the structure of the signal. The ED estimates the presence of a signal by comparing the received energy with a known threshold derived from the statistics of the noise. On the other hand, ED is always accompanied by a number of disadvantages: i) the sensing time taken to achieve a given probability of detection may be high; ii) detection performance is subject to the uncertainty of noise power; and iii) ED cannot be used to detect the spread spectrum signals [13].

2.3.1.2 Matched Filter:

Matched-filtering is the optimal method for detecting PUs when the transmitted signal is known. The main advantage of matched filtering is the short time to achieve a certain probability of a false alarm or the probability of miss detection compared to other methods. The required number of samples grows as $O(1/\text{SNR})$ for a target probability of a false alarm at low SNRs for matched-filtering [8].

On the other hand, matched-filtering requires a CR to demodulate the received signals. Therefore, it requires perfect knowledge of the signaling features of PUs, such as bandwidth, operating frequency, modulation type and order, pulse shaping, and frame format. Moreover, because CR needs receivers for all signal types, the implementation complexity of the sensing unit is impractically large [14]. Another disadvantage of matched filtering is the large power consumption by various receiver algorithms needed for detection.

2.3.1.3 Cyclostationary Feature Detection:

Cyclostationary feature detection exploits the periodicity in the received primary signal to identify the presence of the PU's signal. The periodicity is commonly embedded in sinusoidal carriers, pulse trains, spreading code, hopping sequences, or cyclic prefixes of the primary signals. Because of the periodicity, these cyclostationary signals exhibit the features of periodic

statistics and spectral correlation, which are not found in stationary noise and interference. [9]

Therefore, cyclostationary feature detection is robust to noise uncertainty and performs better than ED in low SNR regions. Although it requires a priori knowledge of the signal characteristics, cyclostationary feature detection is capable of distinguishing CR transmissions from various types of PUs' signals [14].

On the other hand, this method has its own shortcomings because of its high computational complexity and long sensing time. Because of these issues, this detection method is less common than ED in cooperative sensing.

2.3.2 Cooperative Sensing:

In this approach, the PU's signals are detected reliably by interacting or cooperating with other users. This method can be implemented as either centralized access to the spectrum coordinated or distributed approach. [15]

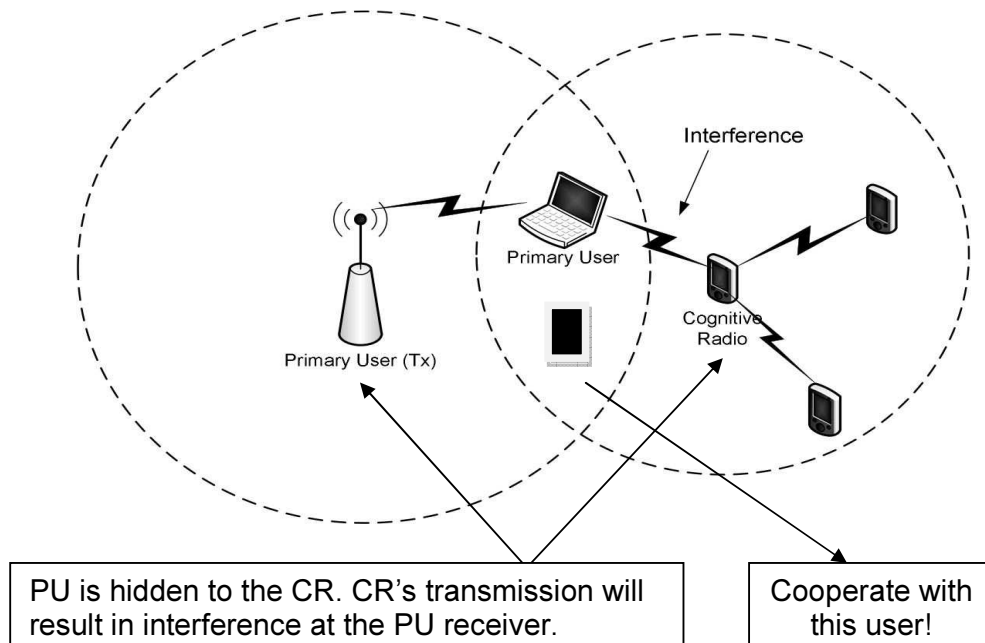


Figure 2.4: Cooperative Sensing

2.3.2.1 Centralized Access:

In centralized cooperative sensing the Fusion Center (FC) controls the processes of cooperative sensing. All cooperating CR users report their sensing results via the control channel. The FC combines the received local sensing information, determines the presence of PUs, and diffuses the decision back to the cooperating CR users. For local sensing, all CR users are tuned to the selected licensed channel or frequency band where a physical point-to-point link between the PU transmitter and each cooperating CR user for observing the PU's signal is called a sensing channel. For data reporting, all CR users are tuned to a control channel where a physical point-to-point link between each cooperating CR user and FC for sending the sensing results is called a reporting channel. In centralized networks, a Base Station (BS) is naturally the FC. Alternatively, in CRNs, where a BS is not present, any CR user can act as a FC to coordinate cooperative sensing and combine the sensing information from the cooperating neighbors. [16, 17]

2.3.2.2 Distributed Cooperative Sensing:

Unlike centralized cooperative-sensing, distributed cooperative-sensing [18] does not rely on a FC to make a cooperative decision. In this case, CR users communicate among themselves and converge to a unified decision on the presence or absence of PUs by iterations. Based on the distributed algorithm, each CR user sends its own sensing data to other users, combines its data with the received sensing data, and determines whether or not the PU is present using a local criterion. If the criterion is not satisfied, the CR users send their combined results to the other users again and repeat this process until the algorithm converges and a decision is reached. In this manner, this distributed scheme may take several iterations to reach a unanimous cooperative decision.

On the other hand, distributed sensing is more advantageous than centralized sensing because there is no need for a backbone infrastructure and it has reduced cost.

2.3.3 Interference Based Detection:

For interference-based spectrum sensing techniques, there are two proposed methods, Interference Temperature Management and Primary Receiver Detection.

2.3.3.1 Interference Temperature Management:

The interference temperature is a measure of the RF power available at a receiving antenna to be delivered to a receiver, reflecting the power generated by the other emitters and noise sources [19].

2.3.3.2 Primary Receiver Detection:

In this method, the interference and/or spectrum opportunities are detected based on the primary receiver's local oscillator leakage power [20].

2.3.4 Other Techniques:

Many other techniques are proposed to enhance the detection of PU's signals in CRNs. As an example, covariance-based detection [21] exploits space-time signal correlation that does not require knowledge of the noise and signal power. This is unlike the energy detection method, which suffers from noise uncertainty problems. Furthermore, hybrid detection methods [22, 23] are proposed to exploit the advantages of covariance-based and energy detection methods for detecting a licensed user.

2.4 Malicious User and their impacts:

The presence of malicious users can significantly affect the performance of a CR cooperative sensing system. A user might be malicious for selfish reasons or due to sensor malfunctioning. In the former case, a CR might detect that the primary signal is absent. However, it might force the access point to erroneously decide that a primary signal is present by sending false sensing data. The malicious user can then selfishly transmit its own signal on the free channel. If the sensor is malfunctioning, it might generate random energy values. There are, generally, two ways in which malicious users can affect the cooperative sensing system. They may send high energy values when there is no primary signal present, thus increasing the probability of a false alarm and decreasing the available bandwidth for the CR system. Malicious users may also send low energy values when the signal is present, thus decreasing the probability of detection of the primary signal and causing increased interference to the PU system. Since most of the data fusion schemes at the access point take into consideration that some of the sensors will have weak channels from the primary transmitter, the impact of malicious users sending low energy values when a primary signal is present will, in general, be low on the performance of the cooperative sensing system. However, when the malicious users send high energy values when no primary signal is present, the impact on the performance of the cooperative sensing system will be much more severe. Thus, malicious user detection schemes should be efficient in identifying malicious users that falsely send high energy values to the access point. At the same time, the scheme chosen to identify these malicious users should not misdetect a non-malicious user as a malicious user. When the primary signal is present, it is especially important that the data of non-malicious users that receive good signal strength from the primary transmitter should not be rejected, as this would severely decrease the probability of detection of the cooperative sensing system leading to severe interference to the PU system. [24]

CHAPTER: 3

SYSTEM MODEL

3.1 Localization of SU and MU in CR Network:

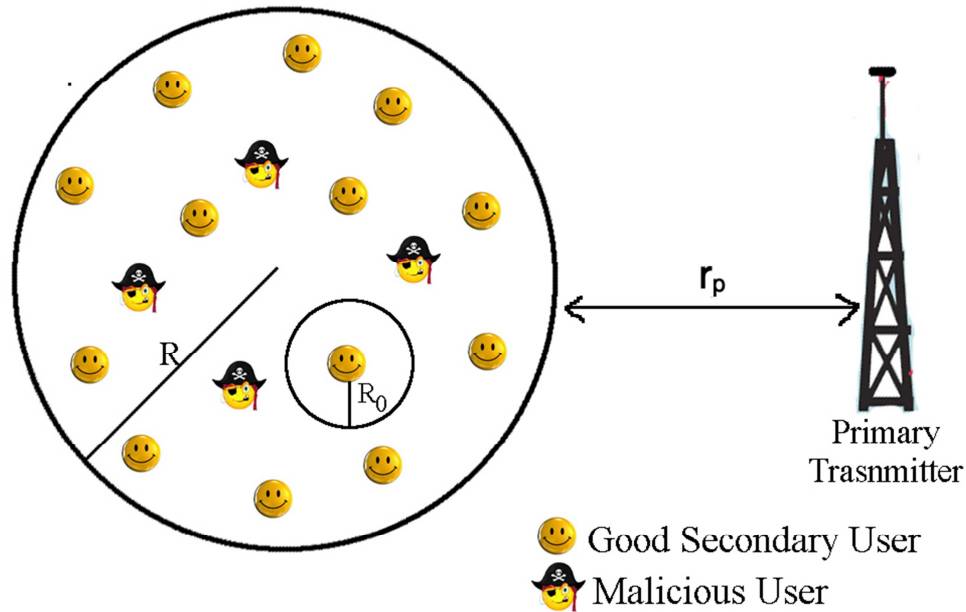


Figure 3.1: A Typical Cognitive Radio Network in A circular Grid with Secondary & Malicious User.

Here we consider the Secondary User (SU) and Malicious User (MU) are distributed within a region of radius R . Each S_u has coverage of R_0 within which there is an MU based on the concept of [1]. The Primary User (PU) is located at a distance of r_p from the reference point. Here we consider exponential path loss model within the range of radius R and the Okumura-Hata model for the distance of r_p .

3.1.1 Exponential Path Loss Model:

If we consider the frequency length of the signal as λ then we can write,

$$k = \left(\frac{\lambda}{4\pi d_0} \right)^2$$

and

$$P_r = P_t \left(\frac{d_0}{d} \right)^\gamma$$

Where P_r is the received power of the signal and P_t is the transmit power of the signal. Here d_0 is a reference distance, Complex analytical models or empirical measurements when tight system specifications must be met:

- Best locations for base stations
- Access point layouts

3.2 Okumura-Hata Model:

This model is an example of a land mobile propagation model that is based on empirical measurements. This model applies to propagation in the frequency band from 150 MHz to 1GHz. The original data were collected by Okumura and others in several areas of Japan. Numerous charts were provided illustrating the many factors that affect land mobile propagation, including building characteristics and antenna height. Hata later provided analytical approximations to these data that captured most of the major effects.

The Okumura-Hata model predicts the standard path loss (not path fading) in three types of environment: urban, suburban and open. The path loss in dB, for the urban environment is given below:

$$L_p = A + B \log_{10} r$$

Where r is the range in kilometer. The parameters in this equation depends on the frequency of operation, f_c the height of the transmitting station, h_b and the height of the receiving station, h_m .

These parameters are given by the empirical formula

$$A = 69.55 + 26.16 \log_{10} f_c - 13.82 \log_{10} h_b - a(h_m)$$

$$B = 44.9 - 6.55 \log_{10} h_b$$

Where f_c is measured in MHz, h_b and h_m are in meters and $a(h_m)$ is correction factor that is defined in what follows. This model is valid for the following range of parameter values:

$$150\text{MHz} < f_c < 1000\text{MHz}$$

$$30 \text{ m} < h_b < 200 \text{ m}$$

$$1 \text{ m} < h_m < 10 \text{ m}$$

$$1 \text{ km} < r < 20 \text{ km}$$

The term $a(h_m)$ is a correction factor based on the mobile antenna height and is a function of the environment. For a large city, it is given by

$$a(h_m) = 8.29 (\log 1.54h_m)^2 - 1.1\text{dB} \quad \text{for } f_c \leq 300 \text{ MHz}$$

$$a(h_m) = 3.2(11.75 h_m)^2 - 4.97\text{dB} \quad \text{for } f_c > 300 \text{ MHz}$$

3.3 Assumed Parameters:

The following assumptions were made for the analysis:

- There are M malicious users and S good secondary users in the system.
- The primary transmitter is at a minimum distance of r_p from all the users.
- The primary transmitter transmits at a power P_t .
- The malicious users transmit at a power P_m . (Typically, $P_m \ll P_t$)
- The malicious users received power P_r^m and primary users received power P_r^p .
- The positions of the good and malicious users are uniformly distributed in the circular grid of radius R .
- The co-ordinates of the primary transmitter are fixed at a point (r_p, θ_p) and this position is known to all the users in the grid.

- The positions of the good users and the malicious users are statistically independent of each other.
- Each secondary user measures the received signal and compares the measured energy with a threshold, ϵ .
- The variance of path loss of PU σ_p and the variance of path loss of MU σ_m .
- We consider a free space propagation model for the signal from the primary transmitter and a two-ray ground model for the signal from the malicious users thus resulting in a path loss exponent of 2 for the propagation from the primary transmitter and a path loss exponent of 4 for the propagation from the malicious users. This is because the primary transmitter is so far away from the secondary and malicious users that the signal due to multi-path can be neglected. However, the distances from malicious users are not large enough to ignore the effects of multi-path.

For any secondary user fixed at co-ordinates (r, θ) , no malicious users are present within a circle of radius R_θ centered at (r, θ) . If this restriction is not posted, then the power received due to transmission from any subset of malicious users present within this grid will be much larger than that due to a transmission from a primary transmitter thus resulting in a failed PUEA all the time. On the other hand, if the malicious users deploy power control, then the malicious user present in this grid can modify its transmit power in such a way so that the PUEA is successful all the time. The distance R_θ is called the “exclusive distance from the secondary user”

3.4 Received Power Calculation from Path Loss Formula:

Here we have derived the received power from the path loss formula by using Okumura-Hata model. We have calculated all the dB terms in absolute form and we have taken their absolute values.

$$L_p = A + B \log_{10} r$$

$$= 69.55 + 26.16 \log_{10} f_c - 13.82 \log_{10} h_b - 8.29(\log_{10} 1.54h_m)^2 + 1.1 \text{ dB} + (44.9 - 6.55 \log_{10} h_b) \log_{10} r$$

$$= \log_{10} 10^{69.55} + \log_{10} f_c^{26.16} - \log_{10} h_b^{13.82} - (\log_{10} 1.54h_m^{\sqrt{8.29}})^2 + \log_{10} 10^{1.1} + k \log_{10} r$$

$$K = 44.9 - \log_{10} h_b^{6.55}$$

$$= 31.8 \text{ [if } h_b = 100 \text{ m]}$$

$$= \log_{10} \left(\frac{10^{69.55} \times f_c^{26.16}}{h_b^{13.82}} \right) - (\log_{10} 1.54h_m^{\sqrt{8.29}})^2 + \log_{10} 10^{1.1} + k \log_{10} r$$

$$= \log_{10}(k' f_c^{26.16}) - (\log_{10} 1.54h_m^{\sqrt{8.29}})^2 + \log_{10} 10^{1.1} + k \log_{10} r$$

$$k' = \frac{10^{69.55}}{h_b^{13.82}}$$

$$= 8.13 \times 10^{41} \text{ [} h_b = 100 \text{ m]}$$

$$= \log_{10}(k' f_c^{26.16} \times 10^{1.1}) + k \log_{10} r - (\log_{10} 1.54h_m^{\sqrt{8.29}})^2$$

$$= \log_{10}(k'' f_c^{26.16} \times r^k) - \log_{10} 10^{(\log_{10} 1.54h_m^{\sqrt{8.29}})^2}$$

$$L_p = \log_{10} \left(\frac{k'' f_c^{26.16} \times r^k}{10^{(\log_{10} 1.54h_m^{\sqrt{8.29}})^2}} \right)$$

$$k'' = k' \times 10^{1.1}$$

$$= 8.13 \times 10^{41} \times 10^{1.1} \text{ [} h_b = 100 \text{]}$$

$$L_{p_{abs}} = \frac{k'' f_c^{26.16} \times r^k}{10^{(\log_{10} 1.54h_m^{\sqrt{8.29}})^2 + 1}}$$

Now, for received power formula we know,

$$P_r = \frac{P_t}{L_{p_{abs}}}$$

$$P_r = \frac{P_t \times 10^{(\log_{10} 1.54 h_m \sqrt{8.29})^2 + 1}}{k'' f_c^{26.16} \times r^k}$$

$$P_r = k''' \times r^{-k}$$

$$k''' = \frac{P_t \times 10^{(\log_{10} 1.54 h_m \sqrt{8.29})^2 + 1}}{k'' f_c^{26.16}}$$

which is the received power (P_r) at the particular secondary user from the primary transmitter P_t .

3.5 Substituted Equations and Data in Mathcad Software:

In Mathcad software we have put following equations and data for plotting the graph to observe the lower bound of Primary User Emulation Attack (PUEA).

3.5.1 Input Data for Variation of Lower Bound of PUEA Against the Distance R_0 ; When, $r_p = 2\text{km}$:

$$a = \frac{\ln(10)}{10} \quad \sigma_p = 8 \quad \sigma_m = 5.5 \quad M = 2 \quad r_p = 2000 \quad R = 700$$

$$P_t = 12 \quad R_0 = 40, 50..100 \quad P_m = 1$$

$$\hat{\sigma} = \frac{1}{a^2} \ln\left(1 + \frac{e^{a^2 \times \sigma_m^2} - 1}{M}\right)$$

$$P_{mr}(R_0) = \frac{MP_m}{2R_0^2(R^2 - R_0^2)} e^{\frac{1}{2}a^2\hat{\sigma}^2}$$

$$P_r = \frac{P_t}{r_p^2} e^{\frac{1}{2}a^2\sigma_p^2}$$

$$\varepsilon = 0.0002$$

CHAPTER: 4

RESULTS

4.1 Results and Discussion:

In this section we determine the lower bound of probability of Emulation Attack against the distance R_0 (the radius of a circle within which a SU assumes that there is no MU) for both the case of flat fading environment of [1] and our proposed model.

Here we consider a circular area of radius $R=0.5$ km, where the SU and MU are randomly distributed. The link between SU and MU are short therefore exponential path loss model is used to determine the received power of SU from the MU. Probability of emulation attack increases with increase in R_0 for both the cases. From the profile of PUEA the curve reveals that the parameter is heavily depends on path loss exponent. With increasing path loss exponent γ , the receive signal of emulator decreases more prominently, hence the receive signal of primary user is found more prominent. Therefore PUEA decreases with increasing of γ from 3 to 3.1.

Here we use, $\lambda=10^{-6}$ meter, $d_0=100$ meter and path loss exponent $\gamma=3$ and 3.1 to determine the received power from MU. Taking the distance between PU and the test SU, $r_p=2$ km, hence we can use Okumura-Hata Model to determine the received signal at the test SU from the PU. The parameters used for Okumura-Hata model:

Base Station Height, $h_b= 200$ meter,

Mobile Antenna Height, $h_m= 10$ meter,

Carrier Frequency, $f_c= 900$ MHz and

Transmit Power, $P_t = 12$ dBw.

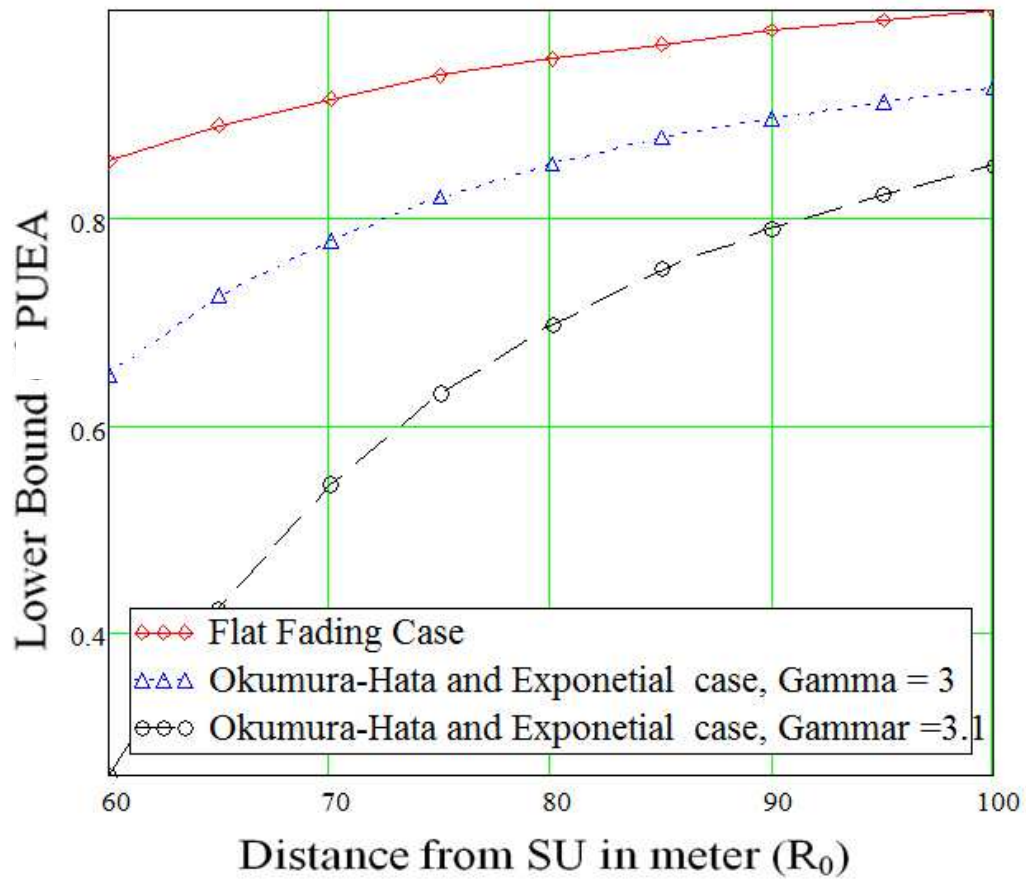
In existing model of Flat Fading we use the typical parameter

$$\sigma_p = 8,$$

$$\sigma_m = 5.5 \text{ and}$$

$$m = 2$$

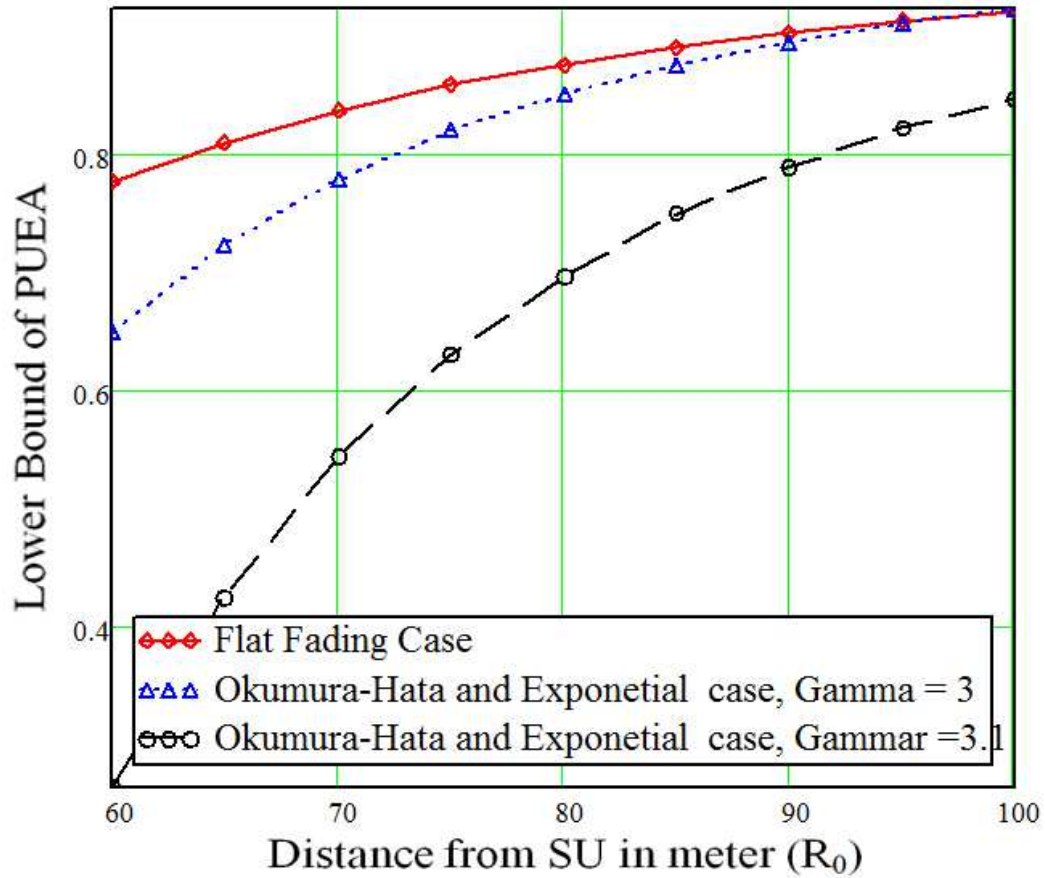
Varying R_0 from 60 to 100 meter we plot the lower boundary of PUEA shown in figure.



**Figure 4.1: Variation of lower bound of PUEA against the distance R_0 ;
where, $r_p=2\text{km}$**

Lower bound of PUEA is smaller under the proposed model (where the combination of Okumura-Hata (between PU and SU) and exponential (between SU and MU) are used) compared to the existing flat fading model.

Lower bound of Emulation attack further reduced with increment of path loss exponent from 3 to 3.1 for the link between MU and SU.



**Figure 4.2: Variation of lower bound of PUEA against the distance R_0 ;
where, $r_p=8\text{km}$**

Summarizing the two graphs it is visualized that PUEA increases with increasing distance between primary user and location of measurement.

With increase in r_p to 8 km the lower boundary of PUEA is decrease for all the two curves because of weaker signal received from the PU.

CHAPTER: 5

CONCLUSION

The CR system is an effective way to improve the efficiency of spectrum uses with respect to the conventional wireless network traffic. In this paper, we show the profile of lower bound of PUEA with respect to the distance R_0 (the radius of an area within which there is no emulator attacker). We have found that lower bound of PUEA increases with increasing R , that is, probability of emulator attack decreases with the decrease in density of the attackers. It is also found that, use of Okumara-Hata model, for long link between SU and PU, decreases the performance of the network with respect to the exponential path loss model of [1]. The entire work can be extended including small scale fading like Rayleigh and Nakagami-m fading, to get more realistic scenario of dense urban area.

REFERENCES

- [1] S. Anand, Z. Jin and K. P. Subbalakshmi, “An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks”
- [2] http://www.webopedia.com/TERM/C/cognitive_radio.html
- [3] <http://searchnetworking.techtarget.com/definition/cognitive-radio>
- [4] A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications “Tevfik Yucek and Huseyin Arslan” EE-360 Presentation: Ceyhun Baris Akcay ,Stanford University
- [5] <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6397631>
- [6] <http://research.microsoft.com/en-us/projects/spectrum/technology.aspx>
- [7] <http://www.wirelesswhitespace.org/about-us/what-is-white-space.aspx>
- [8] R. Tandra and A. Sahai, “Fundamental limits on detection in low SNR Under noise uncertainty,” in Proc. of IEEE International Conference on Wireless Networks, Communication and Mobile Computing, pp. 464–469, June, 2005. Article (CrossRef Link)
- [9] A. Al-Dulaimi, N. Radhi, N., H. S. Al-Raweshidy, “Cyclostationary Detection of undefined secondary users,” Third International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 230–233, 2009. Article (CrossRef Link)
- [10] D. Bhargavi and C.R. Murthy, “Performance comparison of energy, matched-filter and cyclostationarity-based spectrum sensing,” IEEE Eleventh International Workshop of Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-5, June, 2010. Article (CrossRef Link)
- [11] A. Shahzad, “Comparative analysis of primary transmitter detection based Spectrum sensing techniques in cognitive radio systems,” Australian Journal of Basic and Applied Sciences, INSInet Publication, vol 4, no. 9, pp. 4522-4531, 2010. Article (CrossRef Link)

- [12] D. Cabric, A. Tkachenko, and R. Brodersen, "Spectrum sensing Measurements of pilot, energy, and collaborative detection," in Proc. of IEEE Military Communication Conference, pp. 1–7, October, 2006. Article (CrossRef Link)
- [13] Ian F. Akyildiz and Brandon F. Lo, Ravikumar, "Cooperative spectrum Sensing in cognitive radio networks: A survey," *Physical Communication* (Elsevier), vol. 4, no. 1, pp: 40-62, 2011. Article (CrossRef Link)
- [14] D. Cabric, S. Mishra and R. Brodersen, "Implementation issues in Spectrum sensing for cognitive radios," in Proc. of Asilomar Conference On Signals, Systems and Computers, pp. 772–776, November, 2004. Article (CrossRef Link)
- [15] I. F. Akyildiz, W. Y. Lee, M. C. Vuran and S. Mohanty, "Next generation / dynamic spectrum access / cognitive radio wireless networks: A survey," *Computer Networks Journal* (Elsevier), vol. 50, no. 13, pp. 2127–2159, September, 2006. Article (CrossRef Link)
- [16] C. Sun, W. Zhang and K. B. Letaief, "Cooperative spectrum sensing for Cognitive radios under bandwidth constraints," in Proc. of IEEE Wireless Communication and Networking Conference, pp. 1–5, March, 2007. Article (CrossRef Link)
- [17] J. Lund'én, V. Koivunen, A. Huttunen and H. V. Poor, "Spectrum sensing in cognitive radios based on multiple cyclic frequencies," in Proc. of IEEE International Conference on Cognitive Radio Oriented Wireless Networks And Communication (Crowncom), July-August, 2007. Article (CrossRef Link)
- [18] M. Gandetto and C. Regazzoni, "Spectrum sensing: A distributed Approach for cognitive terminals," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 546–557, April, 2007. Article (CrossRef Link)

- [19] O. Simeone, J. Gambini, U. Spagnolini and Y. Bar-Ness, “Cooperation and cognitive radio,” in Proc. of IEEE CogNet Workshop, pp. 6511 – 6515, August, 2007. Article (CrossRef Link)
- [20] B. Wild and K. Ramchandran, “Detecting primary receivers for cognitive Radio applications,” in Proc. of IEEE New Frontiers in Dynamic Spectrum Access Networks DySPAN, pp. 124–130, December, 2005. Article (CrossRef Link)
- [21] T. Dhope and D. Simunic, “Performance analysis of covariance based detection in cognitive radio,” in Proc. Of 35th Jubilee International Convention MIPRO, pp. 737 - 742, May, 2012. Article (CrossRef Link)
- [22] T. Dhope and D. Simunic, “Hybrid detection method for cognitive radio,” 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp: 1-5, September, 2011. Article (CrossRef Link)
- [23] T. Dhope and D. Simunic, “Hybrid detection method for spectrum sensing in cognitive radio,” 35th Jubilee International Convention MIPRO, pp. 765 – 770, May, 2012. Article (CrossRef Link)
- [24] <http://www.ualberta.ca/~mkhabbaz/Publications/Cognitive-TWC.pdf>