PRIMARY USER EMULATION ATTACK MITIGATION IN COGNITIVE RADIO NETWORKS

By

EFE FRANCIS ORUMWENSE

DURBAN, SOUTH AFRICA

AUGUST 2014

TITLE

PRIMARY USER EMULATION ATTACK MITIGATION IN COGNITIVE RADIO NETWORKS

By

EFE FRANCIS ORUMWENSE

Submitted in completion of the academic requirements for the degree of M.Sc. Engineering

School of Engineering, Discipline of Electrical, Electronic and Computer Engineering

University of KwaZulu-Natal, Durban, South Africa

August 2014

Supervisor

Professor Stanley H. Mneney

Co- Supervisor

Dr. Olutayo O. Oyerinde

I hereby approve the submission of this thesis, as the candidate supervisor.

Name: Professor Stanley H. Mneney

Signed: ……

Date: …….

DECLARATION

I, Efe F. Orumwense, declare that:

i. The research reported in this thesis, except where otherwise indicated, is my original work.

ii. This thesis has not been submitted for any degree or examination at any other University.

iii. This thesis does not contain other persons' data, pictures, graphs, or information, unless specifically acknowledged as being sourced from other persons.

iv. This thesis does not contain other person's writings, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

   a) Their words have been re-written but the general information attributed to them has been referenced;

   b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself and alone and have fully referenced such publication.

vi. This thesis does not contain text, graphics or tables copied and pasted from the internet unless specifically acknowledged, the source being detailed in the thesis and in the reference section.

Signed: ……

DEDICATION

To God Almighty – The Great Architect of the Universe

"Immortal, Invisible, God only wise" – 1 Timothy 1:17

PREFACE

The research work in this thesis was implemented by Efe Orumwense, under the supervision of Professor S.H. Mneney and co-supervised by Dr. O.O Oyerinde at the Discipline of Electrical, Electronic and Computer Engineering, University of KwaZulu-Natal, Howard College, Durban. This research work was sponsored by Telkom South Africa, Alcatel-Lucent and THRIP through the Center for Radio Access and Rural Technologies (CRART).

Parts of this thesis have been published in the International Journal on Communications Antenna and Propagation and also currently under review for publication by the Institution of Electronics and Telecommunication Engineers (IETE Journal of Research). Also part of this thesis has been presented at Southern Africa Telecommunication Networks and Applications Conference held at The Boardwalk, Port Elizabeth**,** Eastern Cape, South Africa.

ACKNOWLEDGEMENT

First and foremost, I am ever grateful to the Almighty God for His guidance, blessings and inspiration and for having made this work possible.

I would like to thank my supervisor, Professor Stanley Mneney, for all his guidance during my research. As his student, I have had the freedom to seek my trajectory, while always having access to his support and advice. In every sense, none of this work would have been possible without him.

My sincere gratitude and appreciation also goes to Co-supervisor, Dr. Olutayo Oyerinde for his enlightening advice on my research, his time spent discussing with me and his prompt response anytime I needed him. His enthusiasm and diligence in research have motivated me greatly.

Special appreciation goes to my loving mum, Mrs Elizabeth Orumwense whose constant prayers and blessing have thus led me this far.

Special thanks to Miss Adesuwa Ahanor for her support and encouragement throughout the entire period and also to my cousin Uyi Osariyekemwen.

Finally, I acknowledge the support of Telkom South Africa, Alcatel-Lucent and THRIP for the financial support through the Centre of Excellence (CoE) in the School of Engineering, Discipline of Electrical, Electronics and Computer Engineering, University of KwaZulu-Natal, Durban. I also acknowledge the financial support from the Centre of Postgraduate Study (CEPS) and the German Academic Exchange Service (DAAD).

ABSTRACT

The rapid progress in the number of users and applications in wireless communication have led to the problem of growing spectrum scarcity in recent years. This imminent spectrum scarcity problem is in part due to a rapidly increasing demand for wireless services and in part due to the inefficient usage of currently licensed spectrum bands. Cognitive radio (CR) is a new technology that is proposed to improve spectrum efficiency by allowing unlicensed secondary users to access the licensed frequency bands without interfering with the licensed primary users. A malicious secondary user can decide to exploit this spectrum access etiquette by mimicking the spectral characteristics of a primary user, and gain priority access to a wireless channel over other secondary users. This scenario is referred to in literature as Primary User Emulation Attack (PUEA).

Though quite a lot of research efforts have been focused on the detection and defense strategy of PUEA in cognitive radio networks, less attention have been given to combating and mitigating PUEA in a cooperative spectrum sensing environment. This dissertation seeks to contribute to research in the field of cognitive radio networks through an investigation into the impacts of Primary User Emulation Attacks (PUEA) on cognitive radio networks, the problem of trust amongst users in the networks and also mitigating the activities of PUEA in the network.

An analytical and system model for PUEA in cognitive radio networks is presented and its impacts are also studied using Neyman-Pearson Composite Hypothesis Test. The intention is to evict malicious users from the network and maximize spectrum utilization efficiency. To achieve this, techniques to verify that the source of spectrum occupancy information is from a genuine user are proposed.

In a primary user emulation attack, malicious users tend to destruct the spectrum sensing process of a cognitive radio network by imitating the primary signal and deceive other secondary users from accessing vacant frequency bands. An energy detection cooperative spectrum sensing technique is proposed to mitigate this attack. This technique assists in the reduction of errors made by secondary users in detecting primary user signals in frequency

bands considering the existence of PUEA in the network. The performance of our proposed method is compared to an existing energy detection spectrum sensing method that does not consider the existence of PUEA in the network. Simulated results show that the proposed method can effectively mitigate PUEA in a cognitive radio network.

Table of Contents

List of Figures

List of Acronyms

2-D	Two Dimensional
CAF	Cyclic Autocorrelation Function
CN	Complex Normal Distribution
CR	Cognitive Radio
CRN	Cognitive Radio Network
CSD	Cyclic Spectrum Density
DSA	Dynamic Spectrum Access
ED	Energy Detector
FC	Fusion Center
FCC	Federal Communications Commission
GPS	Global Positioning System
ITU-R	International Telecommunication Union Radio Communication Sector
MAC	Medium Access Control
OfCom	Independent Regulator and Competition Authority
PDF	Probability Density Function
PER	Primary Exclusive Region
PU	Primary User
PUEA	Primary User Emulation Attack(s)
RSS	Received Signal Strength
SCF	Spectral Correlation Function
SDR	Software Defined Radio
SNR	Signal to Noise Ratio
SU	Secondary User
TV	Television

List of Symbols

A_0	Absence of PUEA
A_1	Presence of PUEA
d	Distance
d_0	Reference distance
d_M	Distance between malicious user and primary user
d_p	Distance between the primary transmitter & other users
G_t	Gain of transmitter
G_r	Gain of receiver
G_P^2	Shadowing between the primary user & secondary users
G_J^2	Shadowing between the malicious user & secondary user
h_a^k	Channel gain between PUEA and secondary user
h_p^k	Channel gain between primary user and secondary user
H_0	Absence of primary user
H_1	Presence of primary user
H_t	Height of transmitter
H_r	Height of receiver
L	Factor loss
n_i^k	Additive white Gaussian noise
P_m	Malicious user transmitting power
P_r	Received power level
P_t	Primary user transmitting power
p_d^i	Probability of detection

p_f^i	Probability of false alarm
p_d^{OR}	Probability of detection in the OR rule
p_d^{AND}	Probability of detection in the AND rule
p_f^{OR}	Probability of false alarm in the OR rule
p_f^{AND}	Probability of false alarm in the AND rule
p_e^{OR}	Probability of error in the OR rule
p_e^{AND}	Probability of error in the AND rule
(r_0, θ_0)	Polar coordinates
R	Radius of the circular grid
(R_0, R)	Radii of annular region
X_t	Received signal
y_i^k	Received signal
σ_m^2	Variance of malicious user
σ_p^2	Variance of primary user

CHAPTER 1

INTRODUCTION

1.0 Background

Wireless communication has indeed been one of the fastest developing sector of the communications industry in recent years due to the fact that wireless applications has steadily been on the increase. As a result, many wireless applications and systems operating in unlicensed spectrum bands have gradually led to the overcrowding of the spectral bands making them scarce and unavailable. However, investigation into the spectrum scarcity problems by numerous regulatory bodies around the world, including the United States Federal Communication Commission (FCC) and the Independent Regulator and Competition Authority (OfCom) in the United Kingdom, have reported that although the demand for spectrum will significantly increase in the near future the major problem is not the spectrum scarcity but the inefficiency in spectrum usage [1], [2], [3].

Hence to address the inefficient spectrum usage and spectrum scarcity problems, a new approach for spectrum management is required. This approach should be capable of providing wireless access to unlicensed users, also known as secondary users (SUs), by allowing them to opportunistically gain access to unoccupied licensed spectrum while simultaneously guarantying the rights of incumbent users, also known as primary users (PUs) who possesses a "*first class*" access or legacy rights across the spectrum [4]. This implies that a licensed spectrum band can be accessed by a secondary user only if not in use by a primary user. This new approach is referred to as Dynamic Spectrum Access (DSA) [5].

The cognitive radio technology [7] [15] [17], plays an important role in ensuring the realisation of this DSA paradigm. The concept of cognitive radio was first proposed in 1999 by Joseph Mitola [7] where cognitive radio was described as software defined radio (SDR) [8] which possesses a more flexible approach to wireless communication. A cognitive radio has the ability to learn from its environment and intelligently adjust its parameters based on what has been learned. So in DSA, a cognitive radio can learn about the spectrum usage status of a band and automatically decides if the band is occupied by the primary user or not.

The process of learning about the spectrum usage status of a band is called spectrum sensing [16] [18] and this spectrum sensing technique plays a pivotal role to ensure a successful DSA. During a spectrum sensing process, if a primary user begins to transmit across a specific spectrum band occupied by a secondary user, the secondary user is ideally required to vacate the spectral band immediately and automatically search for a vacant band. But when there is no active primary user activity in the spectrum, all secondary users can enjoy equal rights to access the unoccupied spectral band.

For a secondary user to gain equal rights as the primary user, the secondary user imitates the characteristics of a primary user causing the secondary user to behave maliciously. The result of this is that other secondary users will identify the '*malicious'* secondary user as a primary user and vacate the occupied spectrum for the malicious secondary user believing it is a primary user. In this way, the malicious user gets unrivalled access to the primary user's spectral band. This kind of attack is considered as a Primary User Emulation Attack (PUEA) [9].

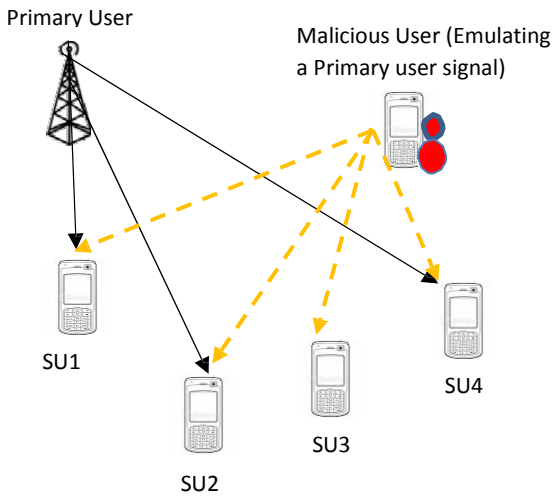

Figure 1-1 :- Illustration of primary user emulation attacks in cognitive radio networks

The term primary user emulation attack was first introduced in [10]. Figure 1.1 shows a typical scenario of a PUEA in cognitive radio network environment where the appearance of an attacker may block the secondary users (SUs) from accessing the idle channel. The

presence of PUEA may severely influence the performance of cognitive radio network and these calls for some kind of strong security mechanism in the network.

1.1 Overview of Dissertation

1.1.1 Objectives and Motivation

Cognitive radio technology is seen as a practical potential solution for efficient spectrum utilization. A major process in the implementation of cognitive radio network is spectrum sensing to determine the existence of spectral holes or the activity of a primary user. But one of the main challenges associated to spectrum sensing is the problem of secondary users to accurately distinguish primary user signals from PUEA signals. Based on the principle that primary users signal possess the priority to access a spectral band, while secondary users must always give up access of the spectral band over to the primary user and ensure that no interference is caused, there exist the potential for malicious secondary users to mimic the spectral characteristics of the primary users in order to gain access to the spectral bands occupied by other secondary users.

In order to resolve the security problems arising from PUEA in cognitive radio (CR) networks, the main objective of this research is to develop an efficient technique and defense mechanism to mitigate the activities of PUEA in CR networks. This will help in reducing the errors made by secondary users in the network and also assist secondary users in successfully detecting primary user signals in frequency spectral bands while limiting interference between users in the system. This work also aims at improving trustworthiness amongst secondary users in the network by proposing a technique to verify if the source of spectrum occupancy information is from a genuine primary user in order to identify and evict malicious users from the network and maximise spectrum utilization efficiency. This will also assist in building a healthy relationship amongst secondary users in the network.

1.1.2 Research Contribution

This research focuses on the major potential attack that is associated to CR networks which is PUEA. The aforementioned attack can wreak havoc to the normal spectrum sensing etiquette of a CR network. After identifying and analysing the attack, we discuss methods to mitigate it.

The contribution this research makes to the field of CR networks is grouped into three categories. Firstly, the threats that this attack poses to cognitive radio networks are examined and analysed because identifying and understanding these threats are the two important initial steps in ensuring a secured CR network. This is achieved by investigating the impacts of this attack on the network using analytical method and extensive Matlab simulations.

Secondly, since spectrum sensing occupancy information is being received by secondary users in a CR network, it is imperative to verify if this information is actually from a genuine primary user. Without this verification, a malicious user may be able to falsify this spectrum sensing information thus denying access to the vacant spectral bands to other secondary users. So a technique is proposed to verify if the spectrum occupancy information is from a genuine primary user.

Finally, this research helps to strengthen and increase the performance of secondary users' spectrum sensing by proposing a novel technique to effectively mitigate the activities of PUEA in a CR network and compare with other existing published techniques.

The results of this research will help to control the activities of PUEA and eliminate spectrum sensing errors encountered by secondary users in a CR network and also aid in the design and implementation of secured and trustworthy CR networks.

1.1.3 Dissertation Review

This dissertation has been organised into six chapters. In chapter 2, an overview of the technical background of cognitive radio networks and its security threats is discussed. In chapter 3, the concept of primary user emulation attack is introduced and its impacts on cognitive radio networks is investigated and analysed.

Chapter 4 presents a proposed technique in ensuring trust amongst secondary users in cognitive radio networks. Simulation setup and results are also presented. Another technique using an effective energy detection cooperative spectrum sensing in eliminating and mitigating PUEA in CR networks is proposed in chapter 5.

In chapter 6, a summary of the dissertation is presented and recommendations for possible future research related to this work are discussed.

1.1.4 Resulting Peer Reviewed Publications

The following peer reviewed publications have been derived from the work undertaken during this research. These publications are related to the topic chapters covered in this dissertation. They are as follows:

Conference Proceedings

1. E. Orumwense, O. Oyerinde and S. Mneney, "Improving trustworthiness amongst nodes in cognitive radio network" *Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC),* Eastern Cape, South Africa. August 2014.

Journal Publications

1. E. Orumwense, O. Oyerinde and S. Mneney, "Impact of primary user emulation attacks on cognitive radio networks" *International Journal on Communications Antenna and Propagation,* Vol. 4, No. 1, April 2014. pp. 19 – 26.

2. E. Orumwense, O. Oyerinde and S. Mneney, Mitigating primary user emulation attacks in cognitive radio networks using cooperative spectrum sensing. *IETE Journal of Research,* Submitted June, 2014.

CHAPTER 2

AN OVERVIEW OF COGNITIVE RADIO

2.0 Objective

The primary objective of this chapter is to introduce and review cognitive radio, cognitive radio network architecture and the various spectrum sensing techniques in cognitive radio networks. The chapter also aims at examining the various key areas that are associated with this work.

2.1 Introduction to Cognitive Radio

The demand for wireless communication services has drastically increased and most of the available part of the spectrum is being used by different licensed applications. With the recent advances in the world of wireless communication, cognitive radio technology is seen as a potential solution for efficient spectrum utilization by unlicensed users which we may also call secondary users (SUs). It has given the opportunity for the secondary users to transmit in several licensed bands without causing harmful interference to the primary users. As cognitive radio is been actualized and put to practice for our modern day use, a major problem it faces is security threats and attacks. Since cognitive radio works on the basis of its two main characteristics; capability and reconfigurability, security threats often build around these characteristics. Most threats that are associated with cognitive radio capabilities are those threats that are launched to mimic the primary transmitters and also threats which emanates from sending false information or observations related to spectrum sensing. These reconfiguration characteristics can be taken advantage of by an attacker whose main purpose is to selfishly acquire the spectral band.

Since cognitive radio is seen as a promising technology in alleviating the spectrum shortage problem in wireless communications, we are now faced with new type of security. However, it is also important to note that cognitive radio networks face other classic threats which are present in other conventional wireless networks. The main difference is in the security threats in Cognitive Radio Networks (CRNs) resulting from the issue of spectrum access rights [11].

Primary user emulation attacks, spectrum sensing data falsification, objective function attacks and Sybil attacks are examples of attacks on a cognitive radio network.

Spectrum sensing data falsification attacks also referred to as Byzantine attacks is an attack against routing protocols, in which two or more routers collude to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services in a cognitive radio network [58]. An objective function attack is usually launched at the physical layer of a cognitive radio. When the cognitive radio is running to find the radio parameters suitable for that environment, the attacker launches an attack to manipulate the parameters it has control over so as to enable the results favour its interest. A Sybil attack is a pervasive security threat in cognitive radio networks where a single malicious node masquerades multiple identities, and behaves like multiple geographically distinct nodes [59].

Attacks inherited from the traditional wireless networks include Medium Access Control (MAC) spoofing, congestion attacks, jamming attacks, beacon falsification attacks, hole attacks, jelly fish attacks, hello flood attacks and lion attacks. A description of CRs and CR networks, analytical survey of the threats and attacks associated with CR networks will be discussed in this chapter.

2.2 Cognitive Radio and Cognitive Radio Networks

The term Cognitive Radio was first presented by Mitola and Maguire in 1999 [7]. Their original report has received several opinions and results and since then, the term cognitive radio has become overloaded with many potential meanings.

"*Cognitive Radio: A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets*".

That definition was adopted by the Federal Communication Commission (FCC) [12], a body set up to regulate spectrum usage in the US. Similarly, the International Telecommunication Union Radio Communication sector (ITU-R) [13] also defines Cognitive Radio as

"A radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained."

Cognitive Radio is based on Software Defined Radio (SDR), which is a radio communication system that can potentially tune to any frequency band and receive any modulation across a large frequency spectrum by means of as little hardware as possible and processing these signals though software. Spectrum can be significantly utilized by granting permission to the secondary users to utilize a licensed spectrum when the primary user is not present. The practical implementation of this cognitive radio technology enables secondary users to sense which portion of the spectrum is available, select best available channel, coordinate spectrum access with other users and vacate the channel when a primary user reclaims the spectrum usage rights [14].

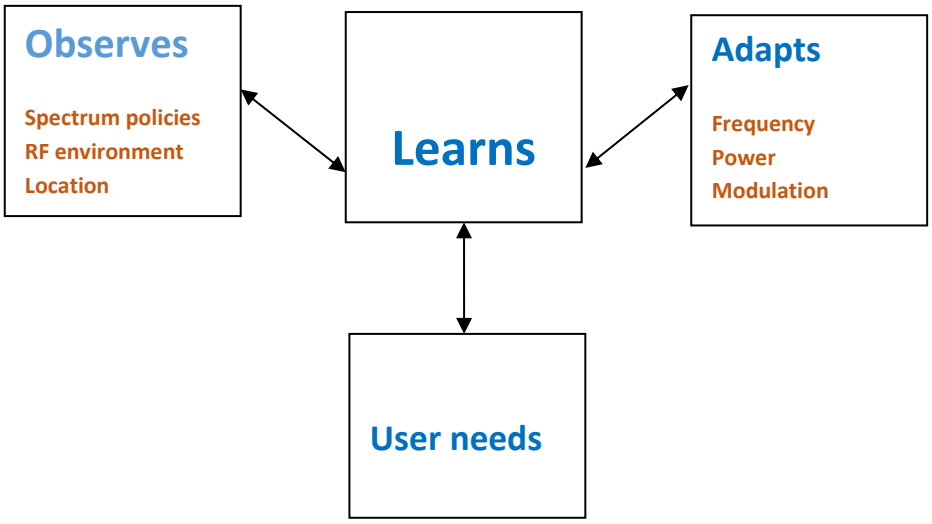

Figure 2-1:- Key functions of a cognitive radio

What differentiate cognitive radio from other traditional communication paradigms are its key functions as shown in figure 2-1.

Observes -: Which can also be referred to as self-awareness, a cognitive radio have the ability to scan and sense the RF environment for detection of RF activity across multiple bands, standards and channels, followed by classification of detection signals.

Learns -: A cognitive radio can also learn the RF environment, from past decisions and observations, so as to be able to anticipate, predict and correct communication standard, mode of operation, and RF parameters. Machines learning techniques such as neural networks and support vector machines can be used to train these devices not to only learn how to adapt, but also how to predict changes in the RF environment.

Adapts -: A cognitive radio/device can adapt their operating parameters, such as frequency, transmission power, modulation type, etc., to the variations of the surrounding radio environment. Before CRs adjust their operating mode to environment variations, they must first gain necessary information from the radio environment, a characteristic known as cognitive capability. This characteristic enables CR devices to be aware of the transmitted waveform, radio frequency (RF) spectrum, communication network type/protocol, geographical information, locally available resources and services, user needs, security policy, and so on.

User needs -: Reconfiguring a CR to provide enhanced communication quality with respect to user-defined goals. Such configuration can be, for instance, the choice of wireless radio interface to be used for communication, or tuning of the communication system's parameters to suit the user.

After CR devices gather their needed information from the radio environment, they can dynamically change their transmission parameters according to the sensed environment variations and achieve optimal performance, a characteristic known as reconfigurability. A cognitive radio incorporates multiple sources of information, determines its current operation settings, and collaborates with other cognitive radios in a wireless network. So when CRs are interconnected, they form Cognitive Radio Networks (CRNs).

2.3 Cognitive Radio Network Architecture

A cognitive radio network (CRN) is not just a network of interconnected cognitive radios but CRN are composed of various kinds of communication systems and networks that can be viewed as a sort of heterogeneous network. Cognitive radios in a CRN, has the ability to sense available networks and communication systems around it. A typical CRN environment

also consists of a primary user or a number of primary radio networks that coexist within the same geographical location of a cognitive radio network. A primary network is an existing network that is licensed to operate in a certain spectrum band. Hence, a primary network is also referred to as a licensed network. The design of cognitive radio network architecture has the objective of optimising the entire network utilization, rather than only maximising spectral efficiency.

CRNs can be deployed in centralized, distributed, ad-hoc or mesh architectures, and serve the needs of both licensed and unlicensed user applications. The basic components of CRNs are cognitive users, the primary user, base stations and core networks. These four basic components compose three kinds of network architectures in CRNs which are infrastructure, ad-hoc and mesh architectures [15].

2.3.1 Infrastructure Architecture – In an infrastructural based architecture as shown in figure 2.2, the cognitive radio base station controls and coordinates the transmission activities of the secondary cognitive radio users. The cognitive radio base stations control the secondary transmissions over both the licensed and unlicensed bands by collecting all the spectrum-related information from the cognitive radio user.

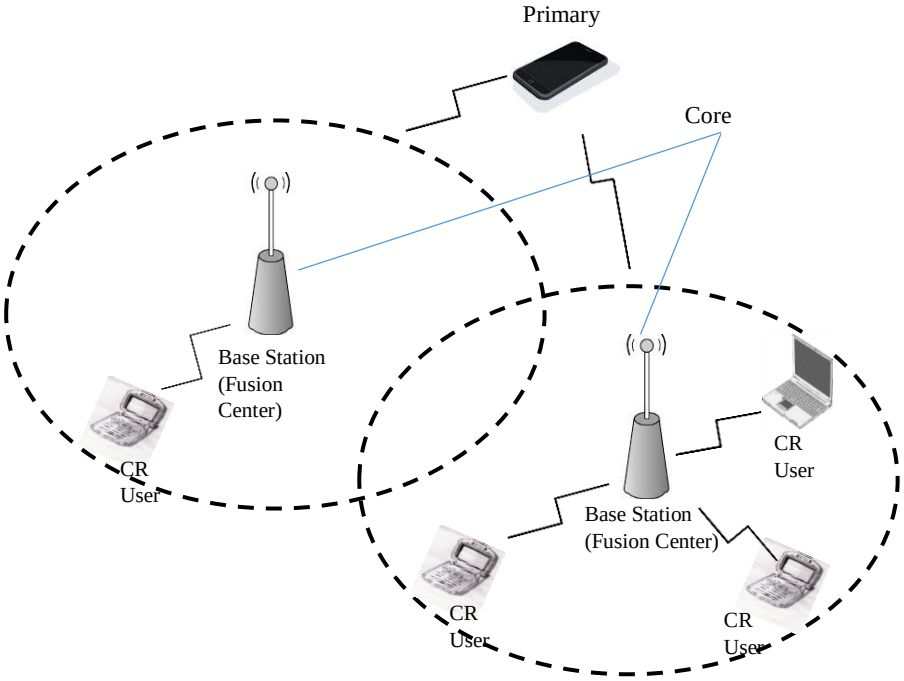

Figure 2-2:- Infrastructure architecture

Based on these collected information, the base stations take a final access decisions for all the nodes. The cognitive user can only access the base station in a one-hop manner. Cognitive users under the transmission range of the same base station communicate with each other through that base station. Communication between different cells is routed through core networks and the base stations have the ability to execute multiple communication protocols in order to fulfil the various demands from cognitive users. The channel between the primary user and the secondary user is the sensing channel and the channel between the CR user and the base station is the reporting channel.

2.3.2 Ad-hoc Infrastructure - In Ad-hoc architecture, as shown in figure 2-3, there is no infrastructural support. The CR users communicate directly with each other in an ad-hoc manner and information is shared between the cognitive radio users who fall within this communication range. Cognitive radio users can either communicate with each other using existing communication protocols or by dynamically using spectrum holes. The cognitive radio users do not have direct communication channel with the primary user and rely on their local observation during their operation.

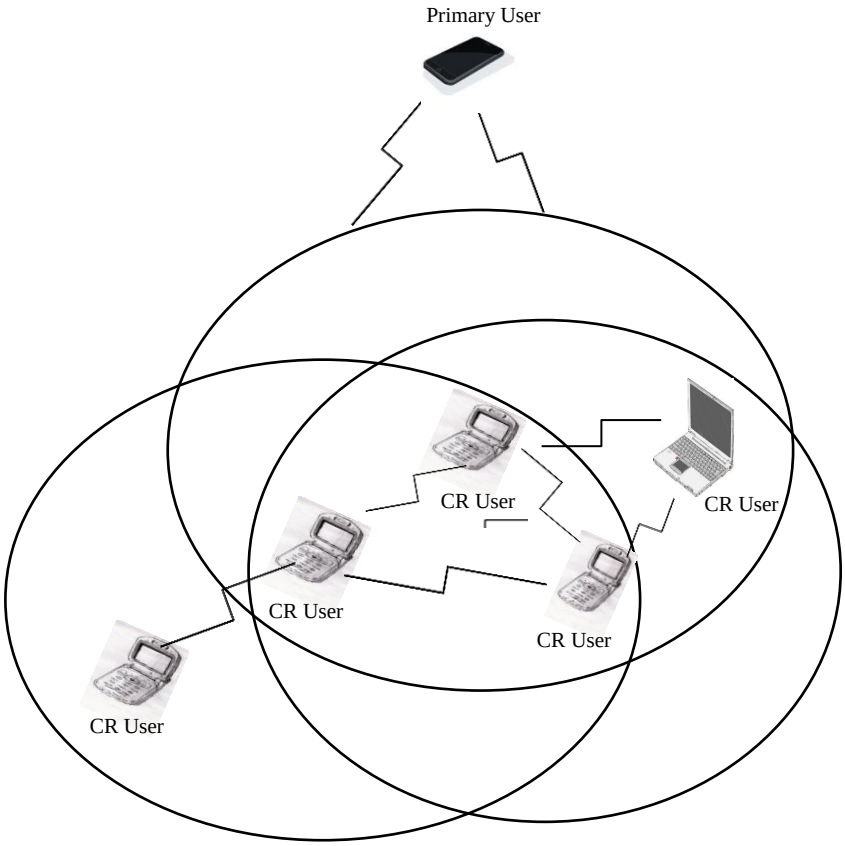

Figure 2-3:- Ad-hoc Architecture

2.3.3 Mesh Architecture – This architecture is a combination of both the infrastructure and ad-hoc architectures. Cognitive radio users can either access the base stations directly or use other cognitive radio users as multi-hop relay nodes. Some base stations may also connect to the core networks and function as gateways and since base stations can be positioned without necessarily connecting to the core networks, it is more flexible and less costly in planning the locations of base stations.

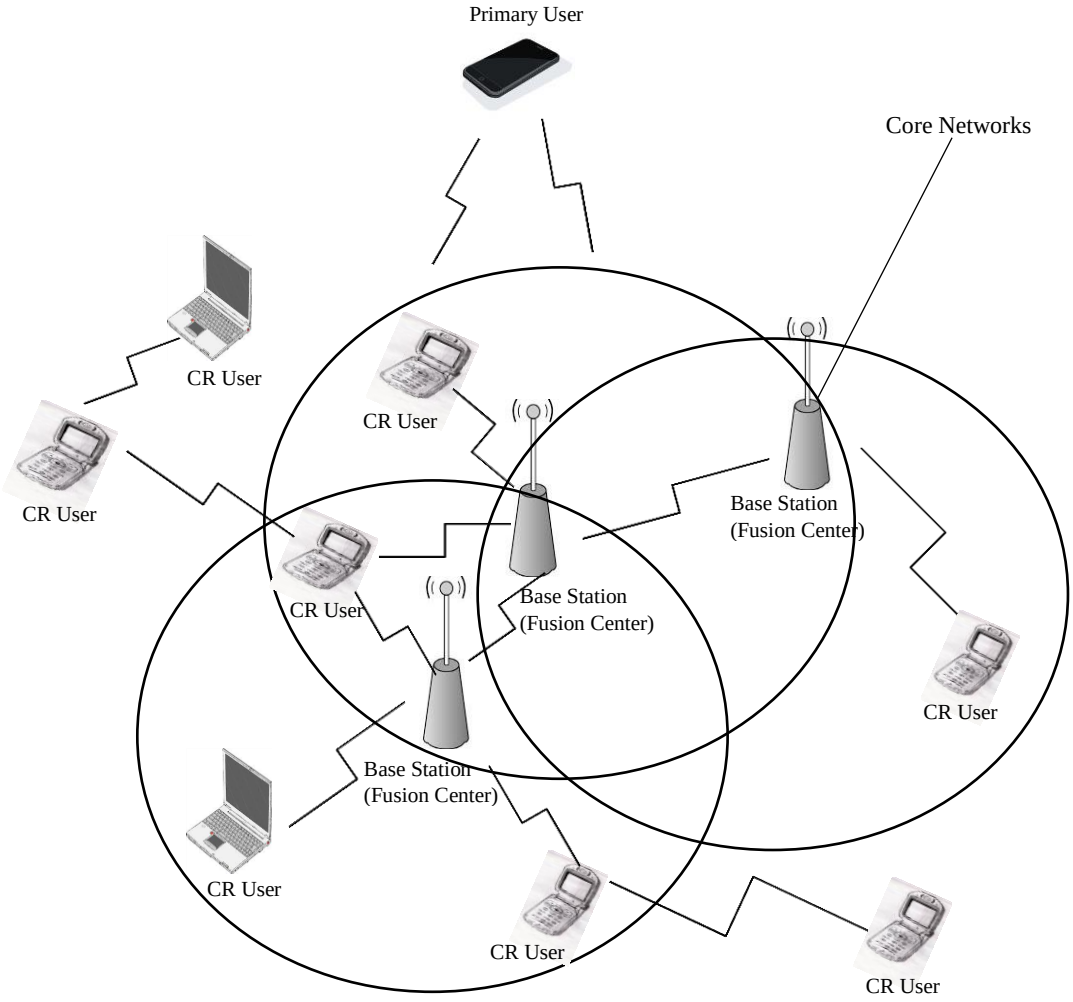

Figure 2-4:- Mesh Architecture

2.4 Spectrum Sensing in Cognitive Radio Networks

Due to the steadily increasing number of wireless applications, the demand for radio spectrum has also been on the increase. This radio spectrum has gradually become a scarce resource and therefore it is necessary to proffer methods to effectively utilize the scarce spectral band. The cognitive capabilities of a CR are realised in the form of a spectrum sensing. This basic function helps CR to learn about the occupancy of spectral bands in its environment. In cognitive radio networks, spectrum sensing is performed by secondary users to determine which frequency spectral band is available for use without creating any type of interference to the primary user.

Currently, there are several existing spectrum sensing techniques in literature [16] [18], but they can be classified or categorized into the non-cooperating spectrum sensing technique or local spectrum sensing technique and the cooperative spectrum sensing technique. The Non-cooperative sensing technique exploits the physical layer characteristics of primary user transmissions such as energy, spectral density modulation and cyclostationary properties [19] while the cooperative sensing technique tends to improve on the non-cooperative spectrum sensing technique by permitting secondary user nodes to exchange spectrum sensing information among each other. The local spectrum sensing technique is further categorized into energy detection, cyclostationary feature detection and matched filter detection based on the sensing method employed in the signal detection process.

2.4.1 Energy Detection

Energy detection (ED) is the simplest and the most commonly used local spectrum sensing technique. Signal detection is achieved by comparing the energy detector's output to a predetermined threshold. Mathematically, the signal detection process can be represented by the following signal model of figure 2-5.

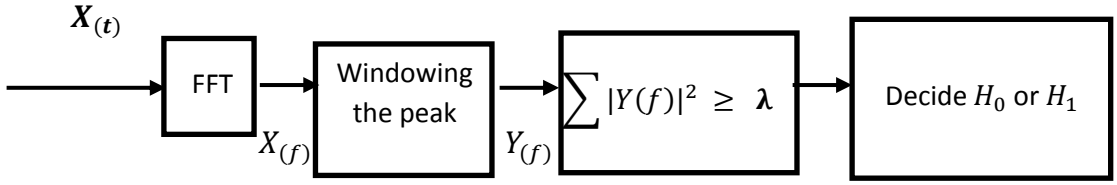

Figure 2-5:- Block diagram of Energy Detection

The received signal $X_{(t)}$ sampled in a time window is then passed through an FFT device, in order to get the power spectrum $X_{(f)}$. Then the peak of this power spectrum is located and after windowing the peak of the spectrum $Y_{(f)}$ is obtained. Then the signal energy in the frequency domain is collected and a binary decision is made.

2.4.2 Matched Filter Detection

Matched filter detection technique is the finest detection technique as it has the ability to maximize the signal to ratio noise (SNR) of the received signal in the presence of additive Gaussian noise [20]. It is achieved by correlating a known signal with an unknown signal in order to detect the existence of the known signal in the unknown signal. In figure 2-6, the matched filter input is convolved with the impulse response of the matched filter and the matched filter output is then compared with the threshold for primary detection. The threshold is calculated by computing the standard deviation of the signal and determining its mean and uses it as the threshold. Its usage in cognitive radio is very limited because it requires a *priori* knowledge about the primary user signal.

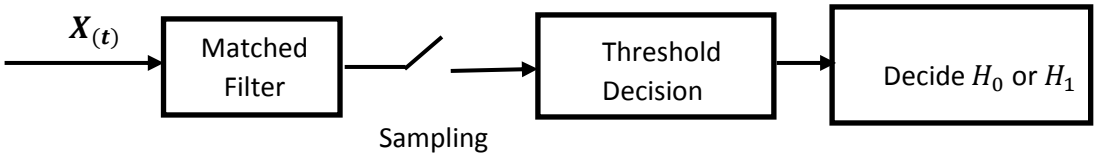

Figure 2-6:- Block diagram of Matched Filter Detection

2.4.3 Cyclostationary Feature Detection

This feature introduces built in periodicity into the modulated signals because of its sine wave carriers. Cyclostationary feature detection utilizes the cyclic feature of a signal to detect it by analysing a spectral correlation function. For example, the cyclic autocorrelation function (CAF) and the cyclic spectral density (CSD) can both be used to detect signal features [21].

The signal of a primary user can be detected at low SNR values if the signal exhibits cyclostationary properties.

Figure 2.7 shows the block diagram of cyclostationary feature detection. The cyclic spectrum or spectral correlation function (SCF) which is denoted by $S\ (f, a)$ is obtained by calculating the discrete Fourier transformation of the cyclic auto correlation function (CAF), where a is the cyclic frequency. Detection is finally completed by searching for the unique cyclic frequency corresponding to the peak in the SCF plane. The main disadvantage of cyclostationary feature detection is its computational complexity and long observational time.

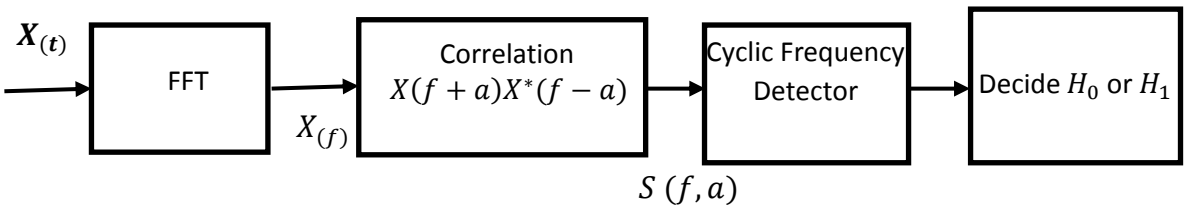

Figure 2-7:- Block diagram of Cyclostationary Feature Detection

2.4.4 Cooperative Spectrum Sensing

One of the most pressing issues relating to local spectrum sensing is channel sensing reliability [22], which becomes more difficult especially when a secondary user is shadowed or in deep fade. To improve on this issue, multiple secondary users can be coordinated to perform cooperative spectrum sensing and several recent works have shown that cooperative spectrum sensing significantly increases the probability of detection in a cognitive radio network. [23] – [25]. Cooperative spectrum sensing is more accurate in detection since the problems of multipath fading and shadowing encountered by a single secondary user detection has been minimised by secondary users sharing information with each other about their individual spectrum sensing results. Figure 2-8 shows a cooperative spectrums sensing scheme.

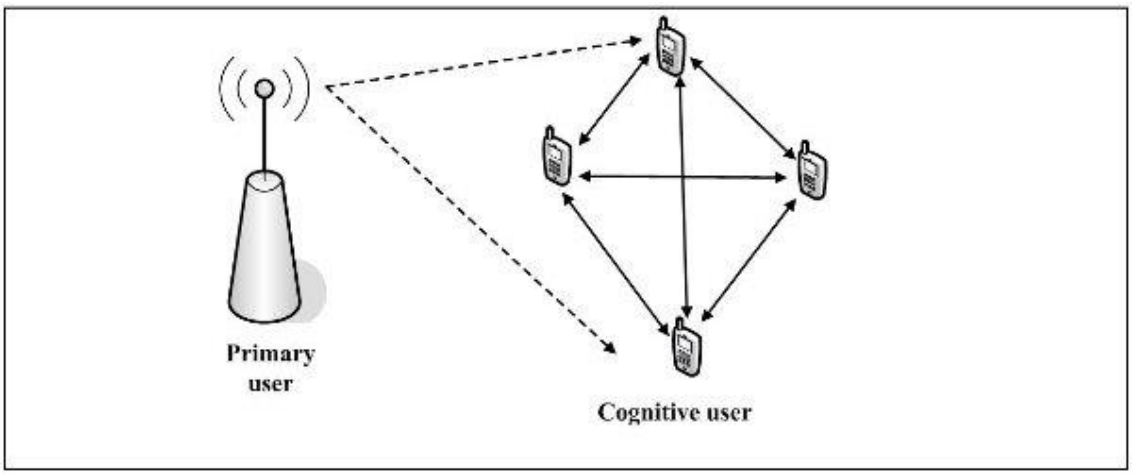

Figure 2- 8:- Cooperative Spectrum Sensing Scheme

Cooperative spectrum sensing can be implemented either in a centralized or a distributed fashion [23]. In the centralized sensing, a fusion center (FC) collects the entire spectrum sensing information from different secondary users and identifies the available spectrum holes and broadcast this information to the secondary users. In the case of distributed sensing, the secondary users exchange spectrum sensing information among each other and collectively make their own decision on which part of the spectrum is available.

The final decision about the channel occupancy is decided following fusion rules. There are many fusion rules that can be applied at the fusion center [17]. The most popular fusion rules are the logic OR rule and the logic AND rules. In the logic OR rule, even if one of the secondary users reports the channel to be busy, the decision about the channel status will be "busy". In the logic AND rule, a channel is decided to be "busy" if all the secondary users report it to be busy and it will be "vacant" if all the secondary users do not sense any activity on the channel.

2.5 Security Threats in Cognitive Radio Networks

There are more intruding opportunities open to attackers in cognitive radio technology when compared with the traditional wireless networks and as a result of this, security in cognitive radio networks has become a more challenging task. Adversaries can now take advantage of several vulnerabilities associated with this new technology and cause severe performance

degradation. Cognitive radio networks is very similar to other wireless networks, since the operational nature of wireless media is the open air, but it is more vulnerable to attacks compared to wired networks. It is also important to note that CRNs faces other classic and common threats found in the traditional and conventional wireless networks. The data in wireless network maybe eavesdropped without prior notice or the channel maybe jammed or overused by adversaries [26], but cognitive radio technology opens more chances to threats and attacks due to its intrinsic nature. That means that these new threats and attacks face by CRNs arise due to their unique cognitive characteristics. Like any other wireless communication technology, a comprehensive analysis of reliability and security challenges in CRNs is a very vital step towards the realization of lasting practical solutions.

Although there exist several types of attacks and threats in cognitive radio networks [56] [57], primary user emulation attacks is considered to be one of the severe threats to cognitive radio systems because of the dangers it poses to spectrum sensing. This attack will be the focus of the next chapter.

2.6 Chapter Summary

This chapter introduced and reviewed cognitive radio and its architecture and primary functionality. The fact that cognitive radio promises to be one of the favourable solution to spectrum scarcity in wireless networks was also examined. Spectrum sensing techniques, a major operational aspect of CRNs was briefly looked at. The security threats associated to cognitive radio networks was also studied and PUEA which potentially combine all these topics together was introduced. Various key areas that are of importance to this work as described in the following chapters were also introduced.

CHAPTER THREE

PRIMARY USER EMULATION ATTACKS

3.0 Objective

The main objective of this chapter is to create an overview of primary user emulation attacks and investigate the impacts it has on cognitive radio networks. This will be achieved by presenting a mathematical formulation for the attack and determining the probability density function of the received signals from both the malicious user and the primary user before presenting a test to examine the impacts of the attack.

Identifying the impacts of PUEA on cognitive radio networks is one of the important steps in modelling techniques to mitigate it.

3.1 Introduction

Lately, security issues, in cognitive radio, are gaining more attention from researchers and one of the most prominent security issue associated with cognitive radio networks is the primary user emulation attacks. This attack was first discussed by Chen *et al* in [9] and [10] and found to pose a great threat to the Dynamic Spectrum Access (DSA) paradigm of cognitive radio networks. In a typical DSA paradigm, primary user possess the priority to access the spectrum band, while the secondary users must always relinquish access of the spectrum band over to the primary users and ensure that no interference is caused. Subsequently, if a primary user begins to transmit across a frequency band occupied by a secondary user, the secondary user is ideally required to immediately vacate that specific spectral band. But when there is no active primary user communication in the spectrum, all other users enjoy equal rights to access the unoccupied spectral band. For a secondary user to gain equal rights as the primary user, the secondary user has to maliciously modify the air interface so as to mimic the primary user's characteristics. The resultant effect of this is that the other secondary users will identify the malicious user as a primary user and as a result

vacate the occupied spectral band for the malicious user. In this way, the malicious user gets unrivalled access to the primary user's spectral band. In literature, this kind of attack against cognitive radio networks is what is considered as a Primary User Emulation Attack (PUEA) [27].

Therefore, we can define primary user emulation attack as an attack in cognitive radio networks where the malicious user pretends to be the primary user to obstruct idle channels by transmitting a similar signal as the primary user [28]. Due to the good (non-malicious) secondary user being forced to vacate the spectral band, the network becomes untrustworthy because the information regarding the occupancy of the spectrum is now being provided by a malicious user.

In the vein of mitigating PUEA in cognitive radio networks, some research advances have been made in countering this attack. Examples are the distance ratio test and the distance difference test proposed by Chen and Park in [10], the localization based defense method proposed by Chen *et al* in [9] and the authentication of primary user signal using cryptographic and wireless link signatures proposed in [45]. Also is the single-attacker-defender-scenario in [37] where both the attacker and the defender can apply estimation techniques and learning methods to obtain key information of the environment.

A PUEA can be launched while the spectrum is being sensed or detected by using the energy detection method, cyclostationary detection method or matched filter detection method [29]. Among these, the energy based detection method is more popular and easier to implement. There are two types of primary user emulation attacks which are associated with the primary user depending on the aim and purpose of the attack.

- **Selfish PUEA**: - The aim of this attack is to maximize attacker's bandwidth by preventing other secondary users from using it. For instance when a malicious user identifies a vacant band, it will prevent other secondary users from using that band by transmitting signals that resembles the primary signal.

- **Malicious PUEA**: - This attack aims at obstructing the secondary users from identifying and using the vacant spectral bands which causes a complete destruction to spectrum sensing process of the cognitive radio network [9] [10].

It should also be noted that PUEA is quite different from jamming attacks because in PUEA the malicious user cause secondary users to vacate the spectrum not by creating large interference on the spectrum but by transmitting signals that resemble that of a primary user thus making them believe that the primary user is transmitting.

3.2 Impacts of Primary User Emulation Attacks in Cognitive Radio Networks

From the discussion about PUEA in section 3.1, there are several ways PUEA can negatively influence a cognitive radio network thereby causing chaos and disrupting the good working order of the network. In this section, we present a system model of a cognitive radio network which is used to perform our analysis.

3.2.1 System Model of Primary User Emulation Attacks

Considering a system as in Figure 3.1, where all secondary users are distributed in a circular grid of radius R and the primary transmitter is present at a distance of at least d_p from all the users. We consider energy based detection mechanisms to detect the presence of the primary user by measuring the energy signal level in the band and comparing it with a pre-set threshold. It order to determine the probability of a PUEA in the system, we make the following assumption to simplify our analysis:

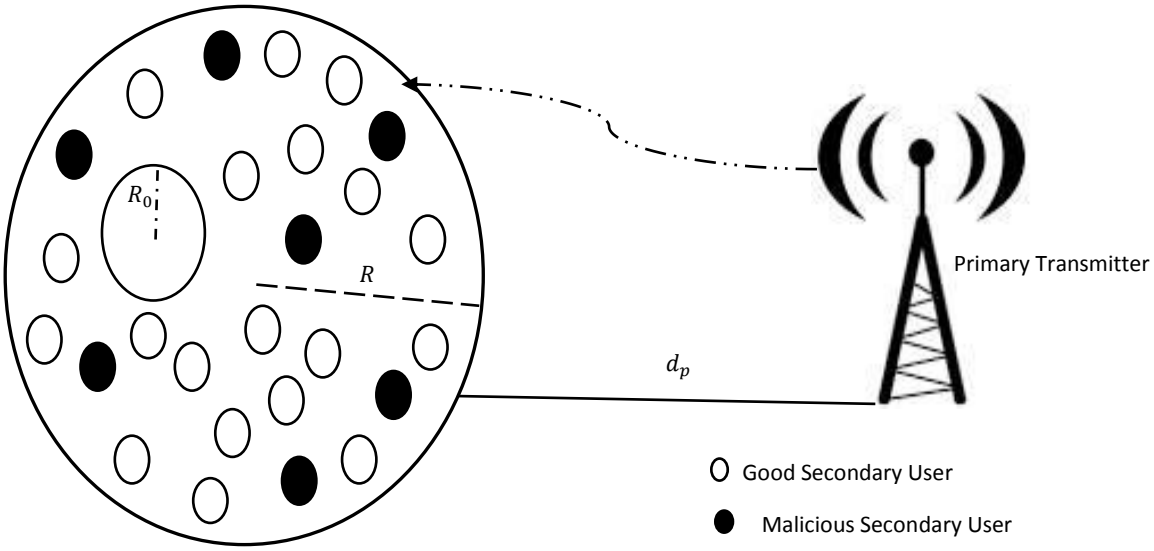

Figure 3-1:- A typical cognitive radio network in a circular grid of radius R consisting of good secondary and malicious users

- That there are M malicious users in the system.
- There is absence of communication or co-operation between the secondary users in the system. In this way, the impact of PUEA on each secondary user can be independently analysed.
- The primary transmitter is at a minimum distance of d_p from all users and it transmits at a power p_t and the malicious users transmit at a power p_m. Typically, $p_m << p_t$ and also the co-ordinates of the primary transmitter are known to the malicious users in the system.
- The positions of the secondary and the malicious users are randomly distributed in the circular grid of radius R and their positions are statistically independent of each other.
- For any secondary user fixed at polar coordinates (r_0, θ_0), no malicious users are present within a circle of radius R_0 (i.e. Primary Exclusive Region) centered at (r_0, θ_0). If the restriction is not posted then the power received from any subset of malicious users present within this grid will be much larger than that due to the transmission from a primary transmitter [30].
- The RF signals from the primary transmitter and the malicious users undergo path loss, log-normal shadowing and Rayleigh fading.
- The Rayleigh fading is assumed to be averaged out and can hence be ignored [36].
- The shadowing random variable from the primary transmitter is $G_P^2 = 10^{\frac{\varepsilon P}{10}} = e^{A\varepsilon p}$ where $A = \frac{ln10}{10}$, εp represents the logarithmic shadowing in dBs with a zero mean and variance σ_p^2 following a normal distribution, $\varepsilon p \sim N(0, \sigma_p^2)$.
- The shadowing random variable from the malicious user is $G_j^2 = 10^{\frac{\varepsilon j}{10}} = e^{A\varepsilon j}$ where $A = \frac{\ln 10}{10}$, ε_j represents the logarithmic shadowing in dBs with a zero mean and variance σ_j^2 following a normal distribution, $\varepsilon_j \sim N(0, \sigma_j^2)$.
- We consider a free space propagation model for the signal from the primary transmitter with a path loss exponent of 2 and a two-ray ground model for the signal from the malicious user with a pass loss exponent of 4. That is the received signal energy of the secondary user from the primary user $P_r^{(p)}$, is proportional to d_p^{-2} while the received signal energy of the secondary user from the malicious users $p_r^{(m)}$, is proportional to d_j^{-4}.

- The PDF of received powers follows a log-normal distribution because a random variable which has a log-normal distribution takes only positive real values.

3.2.2 Primary Exclusive Region

The primary exclusive region (PER), which is also known as the keep out region, serves as a safety mechanism for primary receivers in a cognitive radio network. It practically gives primary receivers an upper hand over other secondary users in the network as the region serves as a protection area. This region is void of cognitive transmitters, that is, the secondary user network must be deployed outside PER in order to guarantee a certain performance for the primary receivers in the region and also ensure there is no interference in the network [32]. This type of deployment scheme is suitable to broadcast networks. An example is a TV network in which the TV station broadcast in a currently licensed band. Since the TV bands are wasted in geographic locations barely covered by the TV signal, secondary devices which are cognitive radio users can be able to dynamically access the spectrum provided they do not cause any interference to the primary users of the bands. The primary transmitter may be seen as the TV broadcaster, and the primary receivers or users as the TV subscribers. It can also apply to any other network in which there is one primary transmitter communicating with multiple receivers and other scenarios, such as the downlink in a cellular network. Such a primary exclusive region has been proposed for the upcoming spectrum sharing of the TV band [33]. The secondary users are randomly and uniformly distributed within a network radius from the primary transmitter, outside the PER.

3.2.3 An Analytical Model of Primary User Emulation Attacks

Due to the absence of cooperation between secondary users, the probability of PUEA on any user in the network is the same. Hence, without loss of generality, we analyse the Probability Density Function (PDF) of the received signal of one secondary user. It is often necessary to calculate the PDF of the total received signal power, which is the “power sum” of a number of simultaneously received signal power. When signal power is on a linear scale, the probability density functions (PDFs’) of the individual signal, either from the secondary users

or from the malicious users, can be convolved to give the PDF of the received power of all the signals all together.

In figure 3.2, we transform the coordinates of all malicious users such that the secondary user of interest lies on the origin. The transformed co-ordinates of the primary will then be (d_p, θ_p). It is important to note that this transformed co-ordinates of the primary user will also depend on the actual location of the secondary user of interest and will not be (d_p, θ_p) for all the secondary users. The received power at the secondary user from each of the malicious user is independently and identically distributed (i.i.d). This is valid due to the symmetry of the system and the fact that the malicious users can be present uniformly in an annular region between the centered at (0,0) and radii (R_0, R). Such approximations for analysis of other parameters in cognitive radio networks are also made in [27], [31], [32], [34] and [35]. The PDF of the received signal at the secondary user due to the primary transmitter and the PDF of the received signal at the secondary user due to the malicious user are calculated.

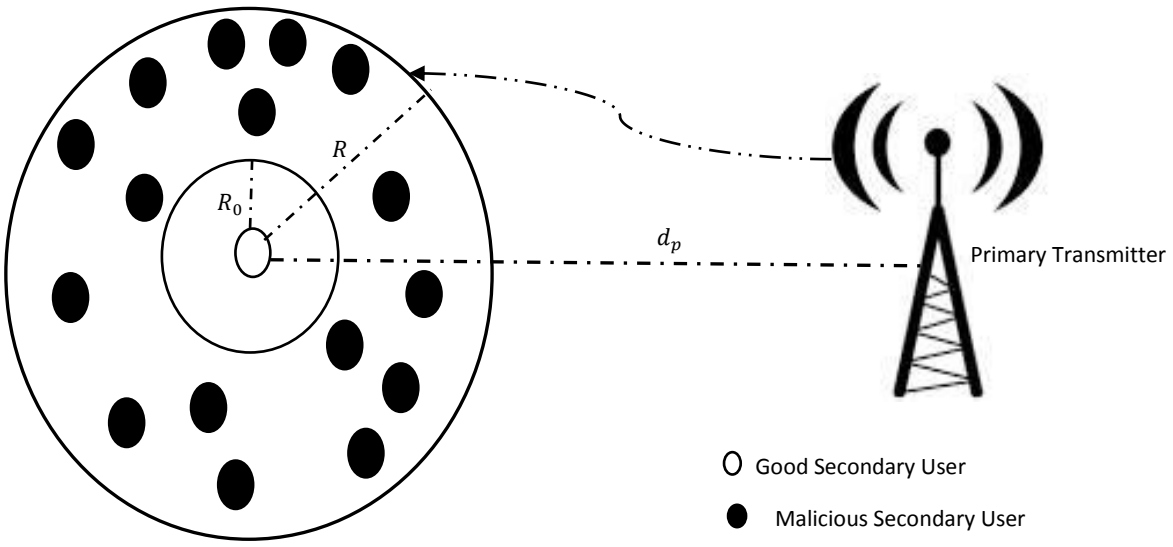

Figure 3-2:- A scenario with transformed coordinates. The secondary user of interest is at (0,0). Malicious users are uniformly distributed in an annular region.

3.2.4 Probability Density Function of Received Signal

In the circular grid, we consider M malicious users to be at the coordinates (r_j, θ_j), $1 \leq j \leq M$. From assumptions stated in section 3.2.1, the position of the j^{th} malicious user is uniformly distributed in the annular region between R_0 and R, $r_j$and θ_j are statistically independent $\forall j$. The PDF of r_j, $p(r_j)$ $\forall j$ is given by [32]

$$p(r_j) = \begin{cases} \frac{2r_j}{R^2 - R_0^2}, & r_j \in [R_0, R] \\ 0 & otherwise, \end{cases} \tag{3.1}$$

and θ_j is uniformly distributed in $(-\pi, \pi), \forall j$. The received power at the secondary user from the primary transmitter, $P_r^{(p)}$ is given by

$$P_r^{(p)} = p_t d_p^{-2} G_p^2, \tag{3.2}$$

where the shadowing at the secondary user from the primary transmitter $G_p^2 = 10^{\frac{\varepsilon_p}{10}}$, with ε_p having a mean of zero and variance of σ_P^2, $\varepsilon_p \sim N(0, \sigma_p^2)$ as mentioned in section 3.2.1. Since p_t and d_p are fixed, the PDF of the received power at the secondary user from the primary transmitter,$P_r^{(p)}(\gamma)$, follows a log-normal distribution and can be written as [60]

$$P_r^{(p)}(\gamma) = \frac{1}{A\sigma_p\sqrt{2\pi}\gamma} exp\left\{-\frac{(10\log_{10}\gamma - \mu_p}{2\sigma_p^2}\right\}, \tag{3.3}$$

where γ is the random variable, $A = \frac{\ln 10}{10}$ and

$$\mu_p = 10\log_{10} p_t - 20\log_{10} d_p. \tag{3.4}$$

The total received power at the secondary node from all *M* malicious users is given by

$$p_r^{(m)} = \sum_{j=1}^{M} p_m d_j^{-4} G_j^2, \tag{3.5}$$

where d_j is the distance between the j^{th} malicious user and the secondary user and G_j^2 is the shadowing between the j^{th} malicious user and the secondary user, $G_j^2 = 10^{\frac{\varepsilon_j}{10}}$, where $\varepsilon_j \sim N(0, \sigma_m^2)$ as previously explained. Conditioned on the positions of all the malicious users, each term in the summation in the right hand of equation (3.5) is a log-normal distributed random variable of the form $10^{\frac{w_j}{10}}$, where $w_j \sim N(\mu_j, \sigma_m^2)$ and where

$$\mu_j = 10\log_{10} p_m - 40\log_{10} d_j \ . \tag{3.6}$$

As explained in [36], $p_r^{(m)}$ can be approximated as a log normal distributed variable whose mean and variance can be obtained by the Fenton's method [33].

Therefore the PDF of $p_r^{(m)}$ conditioned on the positions of all *M* malicious user, $p_{x|r}^m\ (x|\boldsymbol{r})$, can be written as

$$p_{x|r}^m(x|\boldsymbol{r}) = \frac{1}{Ax\sigma\sqrt{2\pi}} exp\left\{-\frac{(10\log_{10} x - \mu_M)^2}{2\sigma_M^2}\right\}, \tag{3.7}$$

where **r** is the vector with elements $r_1 \ldots r_M$ and σ_M^2 and μ_M using Fenton's approximation are given as

$$\sigma_M^2 = \frac{1}{A^2}\ln\left[1 + \frac{(e^{A^2\sigma_m^2} - 1)\sum_{j=1}^{M} e^{2A\mu_J}}{(\sum_{j=1}^{M} e^{A\mu_J})^2}\right], \tag{3.8a}$$

and

$$\mu_M = \frac{1}{A}\ln\left(\sum_{j=1}^{M} e^{A\mu_j}\right) - \frac{A}{2}(\sigma_M^2 - \sigma_m^2)\ . \tag{3.8b}$$

The PDF of the received power from all *M* malicious users, $p^{(m)}(x)$, can be obtained by averaging equation (3.7) over $r_1, r_2 \ldots r_M$ and is given as

$$p^{(m)}(x) = \int_{R_0}^{R} \prod_{J=1}^{M} p_{x|r}^m(x|\boldsymbol{r})\, p(r_j) dr_j, \tag{3.9}$$

where $p(r_j)$ can be obtained in equation (3.2). Evaluating equation (3.9) is very complex, but however, it is seen as a weighted sum of conditional PDF's, each of which is log-normal distributed. Therefore, equation (3.9) above can be approximated as a log-normal distribution with parameters μ_x and σ_x^2 obtained by applying Fenton's approximation for the weighted sum. The expression for the PDF $p^{(m)}(x)$ in equation (3.9) is now of the form

$$p^{(m)}(x) = \frac{1}{Ax\sigma_x\sqrt{2\pi}} exp\left\{-\frac{(10\log_{10} x - \mu_x)^2}{2\sigma_x^2}\right\}, \tag{3.10}$$

If $p_r^{(m)}$ is a log-normal distributed random variable then μ_x and σ_x^2 can be obtained as

$$\sigma_x^2 = \frac{1}{A^2}\left(\ln \mathrm{E}\left[\left(p_r^{(m)}\right)^2\right] - 2\ln \mathrm{E}\left[p_r^{(m)}\right]\right), \tag{3.11}$$

$$\mu_x = \frac{1}{A}\left(2\ln E\left[p_r^{(m)}\right] - \frac{1}{2}\ln E\left[\left(p_r^{(m)}\right)^2\right]\right), \tag{3.12}$$

From equation (3.7), the conditional expectations, $E\left[p_r^{(m)}|\boldsymbol{r}\right]$, and $E\left[\left(p_r^{(m)^2}\right)|\boldsymbol{r}\right]$, can both be evaluated using the Fenton's approximation analysis. $E\left[p_r^{(m)}\right]$ and $E\left[\left(p_r^{(m)}\right)^2\right]$ are obtained by averaging $E\left[p_r^{(m)}|\boldsymbol{r}\right]$ and $E\left[\left(p_r^{(m)^2}\right)|\boldsymbol{r}\right]$ over $r_1, r_2 \ldots r_M$. So the average probability of $p_r^{(m)}$, can be written as,

$$E\left[p_r^{(m)}|\boldsymbol{r}\right] = e^{A\mu_M + A^2\sigma_M^2},$$

$$= e^{A\left(\mu_j - \frac{A}{2}\sigma_M^2 + \frac{A}{2}\sigma_m^2 + \frac{1}{A}ln\mathrm{M}\right) + \frac{1}{2}A^2\sigma_M^2},$$

$$= e^{A\mu_j + \frac{A^2}{2}\sigma_m^2 + ln\mathrm{M}},$$

$$E\left[p_r^{(m)}|\boldsymbol{r}\right] = Me^{A\mu_j}.e^{\frac{A^2\sigma_m^2}{2}}. \tag{3.13}$$

where,

$$\mu_j = 10\log_{10}p_m - 40\log_{10}d_j = 10\log_{10}(p_m.d_j^{-4}).$$

Substituting μ_j in equation (3.13) results

$$E\left[p_r^{(m)}|\boldsymbol{r}\right] = Mp_m.d_j^{-4}.e^{\frac{A^2\sigma_m^2}{2}}\ . \tag{3.14}$$

Integrating equation (3.14) over $r_1, r_2 \ldots r_M$,

$$E\left[p_r^{(m)} \right] = \int_{R_0}^{R} Mp(r_j) P_m d_j^{-4} e^{\frac{A^2\sigma_m^2}{2}} dr_j,$$

we get

$$E\left[p_r^{(m)} \right] = MP_m e^{\frac{A^2\sigma_m^2}{2}} \int_{R_0}^{R} \frac{2r_j}{R^2 - R_0^2} . d_j^{-4} dr_j . \tag{3.15}$$

Since secondary user is at position (0,0), $d_j = r_j$.

$$E\left[p_r^{(m)} \right] = \frac{MP_m e^{\frac{A^2\sigma_m^2}{2}}}{R^2 - R_0^2} . 2 \int_{R^0}^{R} \frac{1}{r_j^2} \, dr_j \tag{3.16}$$

$$= \frac{MP_m e^{\frac{A^2\sigma_m^2}{2}}}{R^2 - R_0^2} . 2 \left[\frac{1}{2} \left[\frac{1}{R^2} - \frac{1}{R_0^2} \right] \right],$$

$$= \frac{MP_m e^{\frac{A^2\sigma_m^2}{2}}}{R^2 - R_0^2} \left[\frac{R^2 - R_0^2}{R^2 R_0^2} \right],$$

and simplifies to

$$E\left[p_r^{(m)} \right] = \frac{MP_m}{R_0^2 R^2} e^{\frac{A^2\sigma_m^2}{2}}, \tag{3.17}$$

From the analysis above, it is seen that the received power at the secondary user from the primary transmitter, equation (3.2), the received power at the secondary user from the malicious users, equation (3.5), and their respective PDFs, equations (3.3) and (3.10) have been derived.

3.2.5 Using Neyman-Pearson Composite Hypothesis Test to Investigate the Impact of PUEA

This test can be used to distinguish between two hypotheses H_1 which indicates that Primary transmission is in progress and H_2 which indicates that emulation attack is in progress by simply minimizing the probability of successful PUEA for a fixed probability of missed detection at a desired threshold. There are two types of errors that the secondary user can make in this hypothesis test which are:

False Alarm: This type of error occurs when the actual transmission is made by malicious user but the secondary user decides that the transmission is due to the primary user [61] [62] [63]. Too many false alarms in the system results in an inefficient spectrum reuse, so controlling the false alarm probability in a network is crucial for efficient spectrum usage.

Missed Detection: The type of error occurs when the actual transmission is made by the primary user but the secondary user makes a decision that the transmission is from a malicious user [61] [62] [63]. Too many missed detection may lead to collisions of primary and secondary user transmission causing inference, so controlling the missed detection probability is crucial for keeping interference to the primary user under the permissible limits.

Neyman Pearson Composite Hypothesis test calculates the PDF of received power at the secondary nodes due to the primary transmitter and also the PDF of received power at the secondary nodes due for the malicious users and the division gives the decision variable z.

$$z = \frac{p^{(m)}(x)}{p^{(pr)}(x)}, \tag{3.19}$$

where $p^{(pr)}(x)$ is the PDF of the received power at the secondary receiver from the primary transmitter following a log normal distribution and $p^{(m)}(x)$ is the PDF of received power at the secondary receiver from malicious users following a log normal distribution.

The quotient z which is the decision variable is compared with the predefined threshold and the secondary user makes its decisions based on the following criterion:

$$\begin{aligned} z \leq \boldsymbol{\lambda} \quad & D_1 : \text{Primary user is transmitting} \\ z \geq \boldsymbol{\lambda} \quad & D_2 : \text{PUEA in progress} \end{aligned} \tag{3.20}$$

The secondary user may take the decision of D_1 when H_2 is true and the secondary user may also take the decision of D_2 when H_1 is true. Each of these errors has a probability associated with it which depends on the decision rule.

The equation of the probability of false alarm where $\boldsymbol{\lambda}$ satisfies the constraint of the probability of the false alarm can be written as

$$\Pr\{D_1|H_2\} = \int_{Z \leq \boldsymbol{\lambda}} p^{(m)}(x)dx. \tag{3.21a}$$

While the equation of probability of missed detection where $\boldsymbol{\lambda}$ satisfies the constraint of missed probability is given as,

$$\Pr\{D_2|H_1\} = \int_{Z \geq \boldsymbol{\lambda}} p^{(m)}(x)dx = \alpha. \tag{3.21b}$$

Equation (3.21a) can also be seen as the probability of making decision D_1 when H_2 is true and Equation (3.21b) as the probability of making decision D_2 when H_1 is true.
Both equations can also be represented in a shorthand form as

$$z \underset{D_1}{\overset{D_2}{\gtrless}} \boldsymbol{\lambda}. \tag{3.33}$$

We will only be concerned with the probability of false alarm since in the scenario of the probability of miss detection, the malicious user is not transmitting.

3.2.6 Simulations Setup and Results

Table 3.1

Values of Parameters used in the simulation

Parameter	**Value**
R_0	50 m
R	1 km
P_t	500 w
P_m	40 w
d_p	10 km
σ_p	8 dB [37]
σ_m	5.5 dB [37]

The theoretical results in figure 3.3 and figure 3.4 are obtained by setting the transmitting power of the primary transmitter to 500 w, the distance between the primary transmitter and the good secondary user to 10 km, the transmitting power of the malicious user to 40 w. The radius of our circular grid is set to 1 km, the secondary user exclusive region to 50 m, the variances of the primary and malicious transmissions are taken to be 8 and 0.5, respectively, since it is to be modelled as if it is occurring in an urban and suburban environments [38]. The number of malicious users is assumed to be randomly distributed around the circular grid. The simulation is set to run at 10000 testing times.

To simulate the PUEA in the network, we consider the same values of the system parameters in table 1 with different values of R_0 which is the exclusive distance from the secondary user and also making sure that the probability of missing the primary signal stays strictly below the required threshold. Increasing number of M(number of malicious users), is keyed into the network and these malicious users are independent and identically distributed (i.i.d) in the annulus of the circular grid with radii R_0 and R. The probability density function of the received power from the transmission of all M malicious users is calculated based on Equation (3.10), including path loss and i.i.d shadowing.

For each number of malicious users M, we ran 1,000 simulations. We calculated the false alarm probabilities by observing the number of times that the decision statistic meets the corresponding decision criterion.

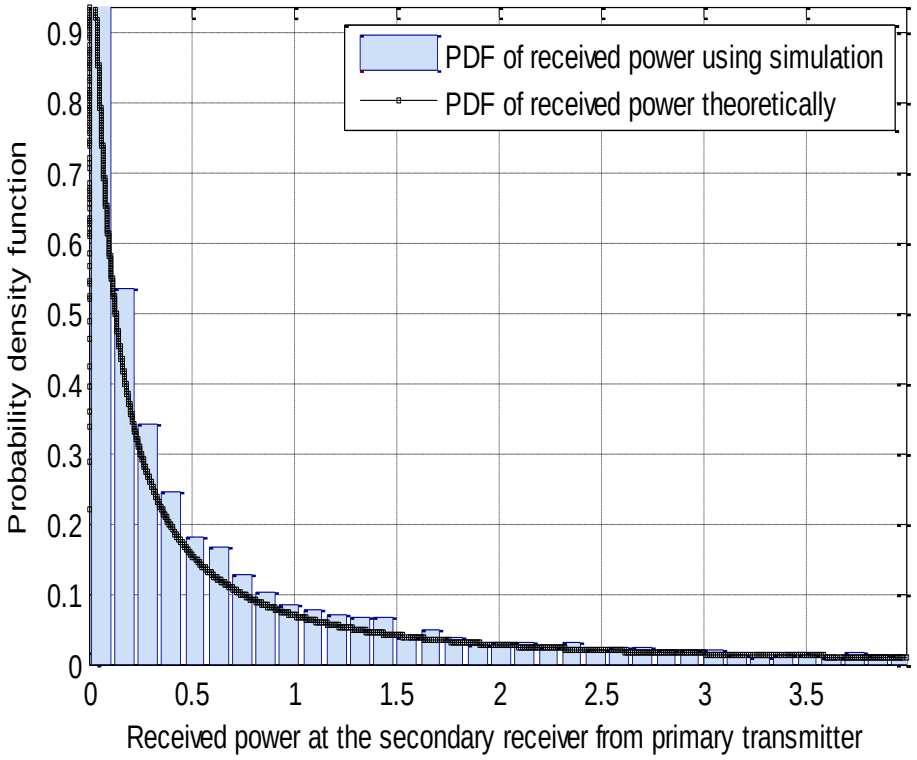

Figure 3-3:- Probability density function of received power at the secondary receiver due to the primary transmitter

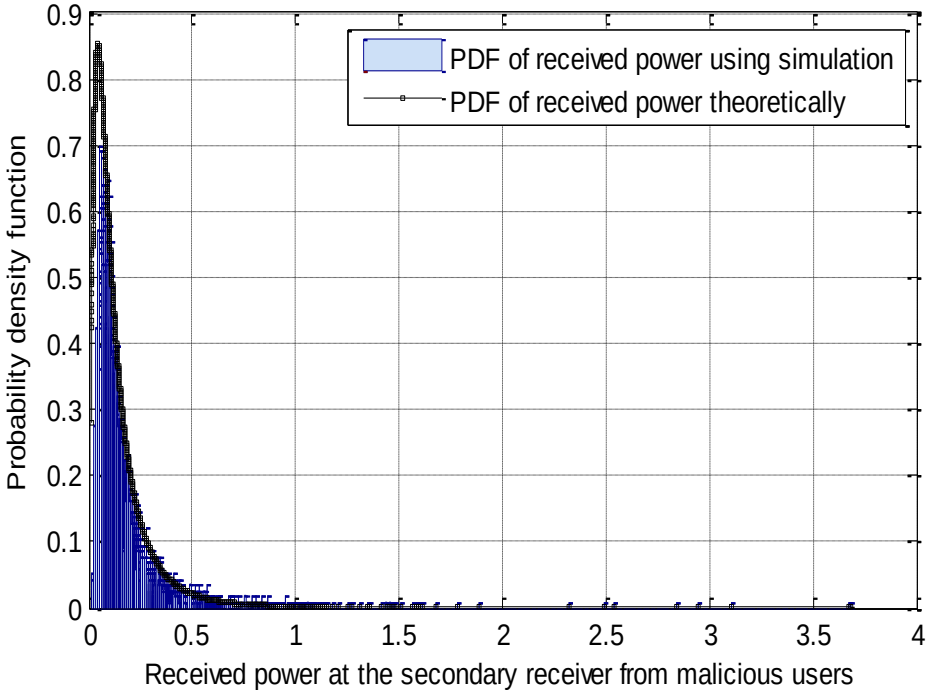

Figure 3-4:- Probability density function of received power at the secondary receiver due to the malicious user

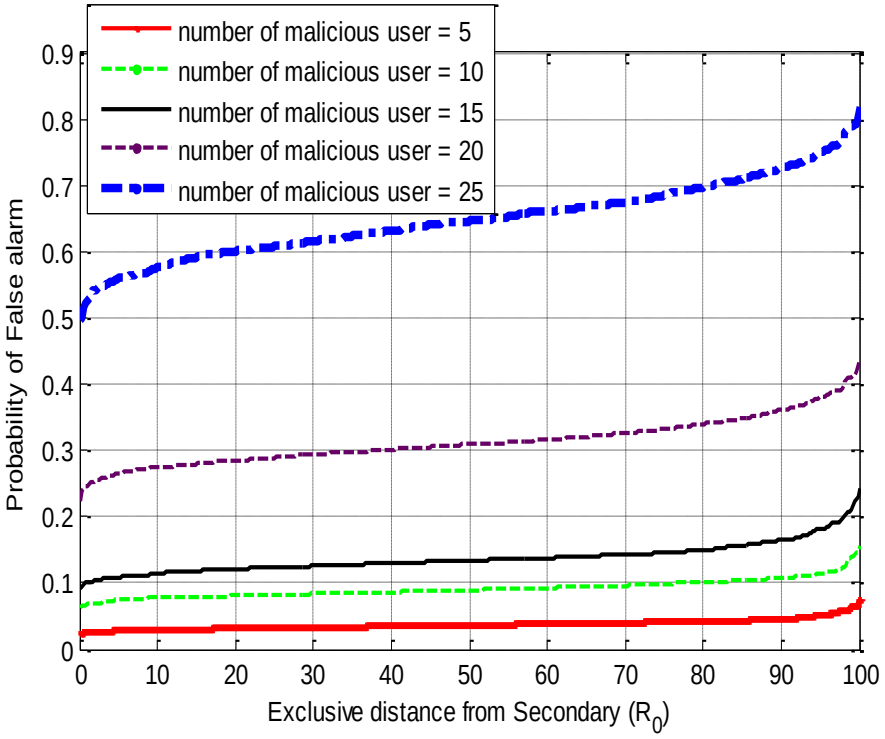

Figure 3-5:- Probability of false alarm at different number of malicious users acting on the system.

3.2.7 Observation and Discussion

Figure 3.3 and figure 3.4 show the results obtained using Matlab simulations and also the theoretical results for the similar setup for the probability density function of the received power at the secondary users due to the primary transmitter and the received power at the secondary users due to the malicious users.

From the figure 3.3 and figure 3.4, we can see that result of the probability density function using simulations considerably match with the one derived theoretically. The reason for the slight mismatch is that the theoretical derivation is for ideal setup and over an unlimited duration of time. On the other hand, the testing times for the simulation are limited in number and therefore will always have an effect on the simulation settings and also the inherent limitations of the Matlab environment should be put into consideration.

It can also be seen from figures 3.4 and 3.5 that the probability density functions of the received power at the secondary user from the primary transmitter and the received power at the secondary user from the malicious user differ from one another. As a result, these

probability density functions can be used in Neyman-Pearson's Composite Hypothesis Test or any other statistical test to identify intruders and impostors in cognitive radio networks. They can also be used to investigate the impact of PUEA in the network.

From results shown in Figure 3.5, it is observed that the probability of false alarm increases as the number of malicious users present in the network is increased. This is because for a large value of R_0 , R tends to be smaller therefore, the malicious users become closer to the good secondary users and the total received power from all the malicious users become close to that received from the primary. Thus, for a large R, the total received power from the malicious users may not be enough to successfully launch a PUEA in the network. When the malicious user M, is set at 5, we can see that the total power all the malicious users generate gives rise to a lower probability than when compared to when M is set to a larger value. The higher the number of malicious users present in the network, the more power it generates resulting good secondary users making erroneous decisions causing a large probability of PUEA in the network. From the results shown, we can therefore deduce that for large values of R_0, there is an increase in the probability of false alarm with a corresponding increase of the number of malicious users this means that high values of R_0 increases the chances of the presence of PUEA in the network, so one can find a convenient range of R_0 in which an attack would be minimized.

3.3 Chapter Summary

In this chapter, primary user emulation attack was studied and its impact on cognitive radio networks was investigated. This was done by presenting an analytical and experimental approach to obtain the probability Density Function (PDF) of the received powers at the secondary users due to the malicious users and also due to the primary transmitter in a cognitive radio network by a set of co-operating malicious users. The PDF obtained was used in Neyman-Pearson Hypothesis Test to show the probability of false alarm in the network.

Results obtained show that the number of malicious users in the system has a great impact on the network causing the good secondary users to suffer degradation in the quality of their communication due to the transmission from malicious users. PUEA will be further explored in chapter 5 and defensive mechanisms to mitigate it will be employed.

CHAPTER FOUR

ENSURING TRUST AMONGST SECONDARY USERS IN COGNITIVE RADIO NETWORKS

4.0 Objective

The objective of this chapter is to examine the concept of trustworthiness in cognitive radio networks and propose techniques to verify if the source of spectrum occupancy information in a cognitive radio network is from a true and genuine primary user in order to evict malicious users from the network thereby maximising spectrum efficiency.

4.1 Introduction

Secondary users' ability to sense and exploit the spectrum in cognitive radio networks imposes a type of attack called primary user emulation attack and also provides an opportunity for malicious users to intrude the network and disrupt the performance of cognitive radio spectrum sensing [10]. To mitigate such an attack, a trustworthy network can be established whereby the trust level of every secondary user node in the system can be assessed individually or through a combination with other nodes. A verification process can be carried out to enable secondary user nodes identify the information provided by genuine users in the network. This way, the secondary user is sure that the information regarding the occupancy of the spectrum is provided by a genuine user and the nefarious activities of malicious users are being thwarted.

In the chapter, a new technique is proposed and analysed to verify the genuineness of spectrum sensing information provided by secondary users in a cooperative spectrum sensing environment so as to identify malicious users in the system and create a trustworthy network. This aims at building a healthy relationship amongst secondary user nodes in cognitive radio networks.

4.2 Creating a Trustworthy Cognitive Radio Network

Trust is an important factor that cuts across many facets of disciplines and based upon it many relationships are formed. Whether it is used for security on recommended systems, the issue of trust will help in successful message transmission among network entities. In a cognitive radio network, trust amongst its nodes will improve the reliability of the spectrum occupancy information of the primary users and ease the decision making process of the fusion center in terms of cooperative spectrum sensing. A malicious user node might detect the absence of primary signal and sends false information that shows the presence of a primary signal to the fusion center. The fusion center erroneously decides that the primary signal is present, this way the malicious user selfishly uses the entire free spectral band [39].

To curb this menace, a trust value is assigned to secondary user nodes where it will be measured by other nodes in terms of the expected genuineness of its information amongst other decisions made from the collective information. This can be achieved when a secondary node sensing result is always different from all other nodes sensing results. A specific scenario is when all secondary user nodes report the absence of a primary user and a specific node reports the presence of a primary user. That node is then regarded as a malicious node and its sensing result is removed before a final decision is taken by the fusion center. In this way, a trustworthy network will be created where by the trust level of every component can be assessed individually or through a combination with other nodes.

In another sense, secondary nodes of a cognitive radio network form a social relationship between themselves to help build trust in the network. A set of nodes can form a sub group and give positive or negative rating of each other based on their previous encounters in order to determine and assess the trust rating of each other. In this way, malicious or untrustworthy nodes can easily be detected cooperatively because of their low trust rating. Therefore the information originating from these malicious nodes can either be ignored or disregarded before the fusion center makes a final decision. Also in a cooperative scenario, a node can change its association with a neighbouring node when it finds out that the level of trust value of that node has drastically been reduced thus ensuring the network operates in a trustworthy manner.

In order to ensure a trustworthy cognitive radio network, a robust transmitter verification scheme [10] that can distinguish between trustworthy secondary users and malicious secondary users is also necessary. In hostile environments, such a mechanism can be integrated into the spectrum sensing process of a cognitive radio network to enhance its trustworthiness.

4.3 System Model of a Cognitive Radio Network

Considering a system as in Figure 4.1, where all the secondary and malicious users are distributed across a circular grid, with a distance d_P between the particular good secondary user and a primary user and a distance d_M between a malicious secondary user and a good secondary user and the primary user is located at the center of the circular grid. We consider a cooperative cognitive radio environment where all secondary users can share their spectrum occupancy information and send this information to the fusion center for final decision. The secondary users broadcast their location information in order to detect unused spectrum bands. We assume that the secondary users can employ some positioning mechanisms to acquire positions, e.g., by using the global positioning system (GPS) [54]. The cognitive radio user calculates the distance between the secondary user and other users based on location coordinates and also calculates the distance based on the received power level from the primary user. If the distance calculated using the coordinates considerably matches the distance calculated with received power level, then we can consider the user as trustworthy but if otherwise, the user is regarded as untrustworthy.

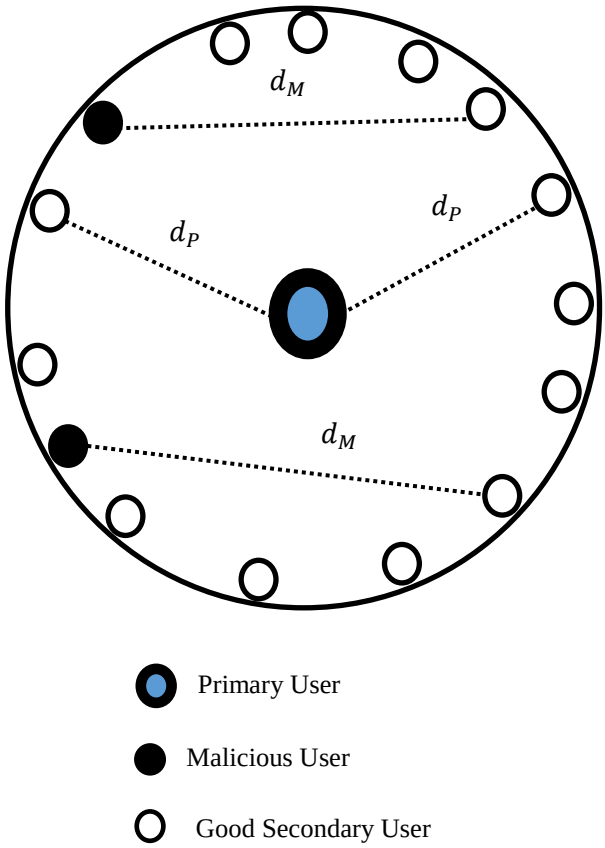

Figure 4-1:- A typical cognitive radio network in a circular grid consisting of all users in the system.

4.4 Proposed Techniques

4.4.1 Distance Estimated Based on Location Coordinates

We analyse the proposed system based on location coordinates whereby all secondary users broadcast their location information. With this information, the distance between the users can be calculated.

For simplification in calculating the distance between users, we consider the location in a (2-D) plane, where $(x_{s\,i}, y_{s\,i})$ are the x and y coordinates of the i^{th} secondary user, (x_P, y_P) are the x and y coordinates of an existing primary user and $(x_{m\,i}, y_{m\,i})$ are the x and y

coordinates of the malicious user. The distance d_P between the i^{th} secondary user and primary user is given by

$$d_P = \sqrt{(x_{s\,i} - x_P)^2 + (y_{s\,i} - y_P)^2}, \quad \text{for } i = 1,2,3 \ldots N. \tag{4.1}$$

where i is the particular secondary user and the distance d_M between the M^{th} malicious user and any good secondary user is also given by

$$d_M = \sqrt{(x_{m\,i} - x_s)^2 + (y_{m\,i} - y_s)^2} \quad \text{for } i = 1,2,3 \ldots M. \tag{4.2}$$

The decision making node can now use the estimated distance obtained using the coordinates to determine how trustworthy any of the secondary user in the system can be.

4.4.2 Distance Measured Based on Received Power Level

The whole idea of distance measurement by means of received power level or received signal strength (RSS) is based on the assumption that the received power level is a function of the transmitting power and distance on the path between two radio devices. The distance between the secondary and other users can also be calculated by measuring the received power level with a known transmit power level. The received power level, P_r, with a given transmit power P_t is given by the equation [40].

$$P_r(d) = P_t G_t G_r \frac{H_t^2 H_r^2}{d^4 L}, \tag{4.3}$$

where P_t is the transmit power level, G_t and G_r are antenna gain of both the transmitter and the receiver respectively, H_t and H_r are the heights of both the transmitter and receiver antennas respectively while L is the system loss factor.

Considering H_t, H_r, G_t, G_r and L are constant and $k = \frac{G_t G_r H_t^2 H_r^2}{L}$, therefore, the received power level will be solely dependent on the transmit power level and distance, expressed as,

$$P_r = \frac{P_t}{d^4} k . \tag{4.4}$$

Based on the received power level the distance between the secondary user and the primary user is given by

$$d = \sqrt[4]{\frac{P_t}{P_r}k}\,. \tag{4.5}$$

Hence, the distance between the users can be estimated based on the received power level. The distance calculated using the received power may not be accurate due to noise and the impact of channel impediments and some other uncertainty caused by the signal propagation environment. However, many researchers still use the received power level based measurement method because of its simplicity and cost efficiency.

The path loss model as proposed in [41] and [42] which is commonly used in received signal power based measurements is written as

$$\frac{P_r(d_0)}{P_r(d)} = \left(\frac{d}{d_0}\right)^n. \tag{4.6}$$

where $P_r(d)$ is the received power at distance d, $P_r(d_0)$ is the received power at the reference distance d_0, n is path loss exponent, d is the distance between the transmitter and the receiver [Km], and d_0 is the reference distance [Km]. Due to the large dynamic range of received power levels, dBm or dBW units can be used to express received power levels.

$$[P_r d] = 10.log\frac{P_r(d)}{0.001(W)} \quad dBm$$

$$\Rightarrow P_r(d) = 10^{\left(\frac{[P_r d]-30}{10}\right)} \quad \text{W},$$

$$\log P_r(d_0) - \log P_r(d) = n.log\left(\frac{d}{d_0}\right)/10,$$

$$\frac{P_r(d_0) - P_r(d)}{10} = n.log\left(\frac{d}{d_0}\right),$$

$$P_r(d) = P_r(d_0) - 10.n.log\left(\frac{d}{d_0}\right) \text{ dB}, \tag{4.7}$$

$$d = d_0.10^{\left(\frac{P_r(d_0)-P_r(d)}{10.n}\right)} \text{ Km} \tag{4.8}$$

$P_r(d)$ and $P_r(d_0)$ are in dBm units. Equation (4.7) is the so-called simplified log-normal shadowing model. Parameters $P_r(d_0), d_0, n,$ are the main parameters for log normal shadowing model formula and they define the properties of radio propagation environment. For this work, n is taken as 2.8 as in [43].

In our proposed technique, the distance between a cognitive user and other users is calculated based on location coordinates and also received power level. If the distance calculated using either proposed methods matches or is extremely close to each other, then the user is regarded as a trustworthy user. If otherwise, then it will be regarded as a malicious user. The trust value is expected to be close to 1 for trustworthy users and low for untrustworthy or malicious users.

4.4.3 Verification of Spectrum Occupancy

In a typical cooperative cognitive radio network, secondary users sense if a particular spectral band is occupied or not before sending its spectrum sensing information to the fusion center for a final decision. During this process, it is imperative that these secondary users correctly sense that the spectrum is occupied by a primary user instead of a malicious user otherwise it will be sending a false spectrum sensing information to the fusion center. As a result, the trust of this particular secondary user node will be compromised.

So to verify the authenticity of the secondary user spectrum sensing information, i.e. to verify if the primary user is indeed using a specific spectral band, we propose a verification tag technique which involves adding a verification tag to the primary user signal. Ideally, there is an FCC rule that says there should be no modification carried out on the incumbent system so as to accommodate opportunistic use of the spectrum by secondary users. But if the FCC's major concern is to ensure spectrum efficiency, then this technique should become very promising even if the FCC rule is not followed. Unlike the other FCC rules, there is no negative impact on the community if this rule is ignored. We strongly believe that if we can demonstrate the significant benefit of this technique, FCC may consider lifting this rule.
After all, by allowing secondary cognitive radios (unlicensed users) to use licensed spectral band, FCC is actually lifting a previously existing rule. Moreover, FCC rules only apply to the United States; other countries may not have such a rule.

So in this technique, a verification tag is added to the primary user signal, the secondary user retrieves these verification tags from the primary user signal and uses the tag to verify whether a spectrum is currently being used by its legitimate owner or not.
The primary signal generates the following one way hash chain:

$$h_n \rightarrow h_{n-1} \rightarrow \ldots \rightarrow h_1 \rightarrow h_0, \tag{3.9}$$

where $h_i = hash(h_{i+1})$ and $hash(.)$ is a hash function.

The last tag h_0 is broadcasted to all users, hence it is known to both the secondary users and the malicious users. The subscript i of h_i indicates the time index during which the primary user will transmit the tag h_i. At time $t = 1$, which is indicative of a short time window, the primary user transmits h_1. Because of the way the one-way hash chain is generated, the disclosure of h_i does not lead to the disclosure of h_j for $j > i$. So between time $t = 1$ and $t = 2$, the verification tag is simply h_1. That is the primary signal embeds h_1 into its signal as shown in figure 4.2 and during $t = 2$ and $t = 3$, h_2 is embedded in the signals and sent out repeatedly. The repetition is necessary because a secondary user might tend to sense the spectrum at any arbitrary moment. Once the secondary user senses the particular spectrum, it retrieves the verification tag from the signals; then using the current time and spectrum owner's h_0 value, the secondary user can verify the validity of h_1.

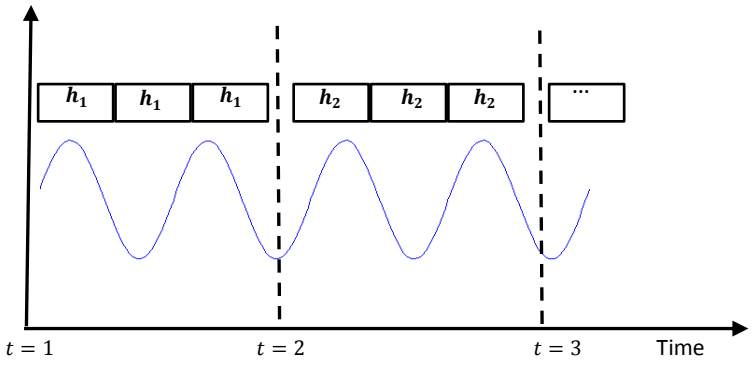

Figure 4-2:- Verification tags

If the malicious user decides to replay the verification tag into its signal so as to emulate the primary user, it will not be successful because the malicious user only replays what is sensed from the primary user. Since the goal of h_1 and h_2 is to prove to the receivers that the primary user is using the current spectrum at a specific time t, so when the specific time window expires, the malicious user will be needing the next verification tag to fool the secondary users which will eventually not be transmitted if the spectrum is no longer in use

by the primary user. That means if the primary user is not using the spectrum, h_{i+1} will not be sent out, so the malicious user will not be able to emulate the primary user hence the spectrum occupancy is verified.

4.5 Relative Trustworthiness of a User

For spectrum occupancy sensing information to be regarded as trustworthy, it has to be received from a trustworthy user. According to the principle of object trust combination, if the final values of an object calculated by using significantly different methods are similar, then the evaluator places a higher level of trust in the results [44].

In an unfriendly environment involving malicious users, trust values are assigned to secondary users to ascertain and evaluate their behaviour in the network. These trust values are assigned to secondary users based on their evaluation of performance using our proposed techniques. Each time after cooperation, the behaviour of the selected secondary users will be evaluated and the trust value will be updated accordingly. Then these trust values will be exchanged periodically between the users in the network. The fusion center often maintains and record identities and their corresponding trust values of all secondary users and keeps these trust values in its domain.

If a malicious user masquerades or poses as a primary user, the trust value assigned to that specific user with the aid of our proposed techniques can enable the fusion center to verify the genuineness of the spectrum occupancy sensing information being carried by that user thereby increasing the legitimacy of spectrum occupancy sensing results in the network and a more accurate detection of primary signals.

4.6 Simulations and Discussion

We use MATLAB simulation in verifying the proposed technique and evaluate the results. To determine the location of both the primary and the malicious user, we considered a 10km by 10km area for our simulation with 4 secondary users and a malicious user present in the network. We assume that each of the 4 secondary users is fixed at 5 km away from the primary user with a line of sight transmission. We also generated 100 instances random

coordinates for 50,000 samples in the case of their trustworthiness and the distance is calculated based on coordinates and received power levels.

Figure 4.3 and figure 4.4 show the actual and estimated locations based on coordinates of the primary user and malicious user, respectively. We can see from figure 4.3 that the estimated location of the primary user closely matches its actual location which is 5km apart from the secondary users, i.e., the distance of the primary user from any of the secondary users is the same. While in figure 4.4, no matter how the malicious user tries to mimic primary user, its distance from the malicious user to each of the secondary users does not match considerably.

Figure 4.5 shows the distance measured between the primary user and a secondary user based on coordinates and the distance measured based on received power level of the primary user from the secondary user. We can see that both distance measurements matches considerably that is an indication that the secondary user is actually communicating with a trustworthy user.

Figure 4.6 shows the trustworthiness of a user in cognitive radio network. As the SNR value increases, correspondingly, the trustworthiness also increases. If the trustworthiness increases to 1, then we can conclude that we are communicating with the primary user and not the malicious or untrustworthy user. If the trustworthiness is approximately equal to 1, we can still conclude that it is a primary user because of some uncertainties which may tend to reduce the trustworthiness. Even as the value of SNR increases we can see from figure 4.6 that the malicious user trustworthiness remains constant at 0.6. Therefore, whatever spectrum occupancy information given by that user is not taken into consideration in the final decision making process of the fusion center.

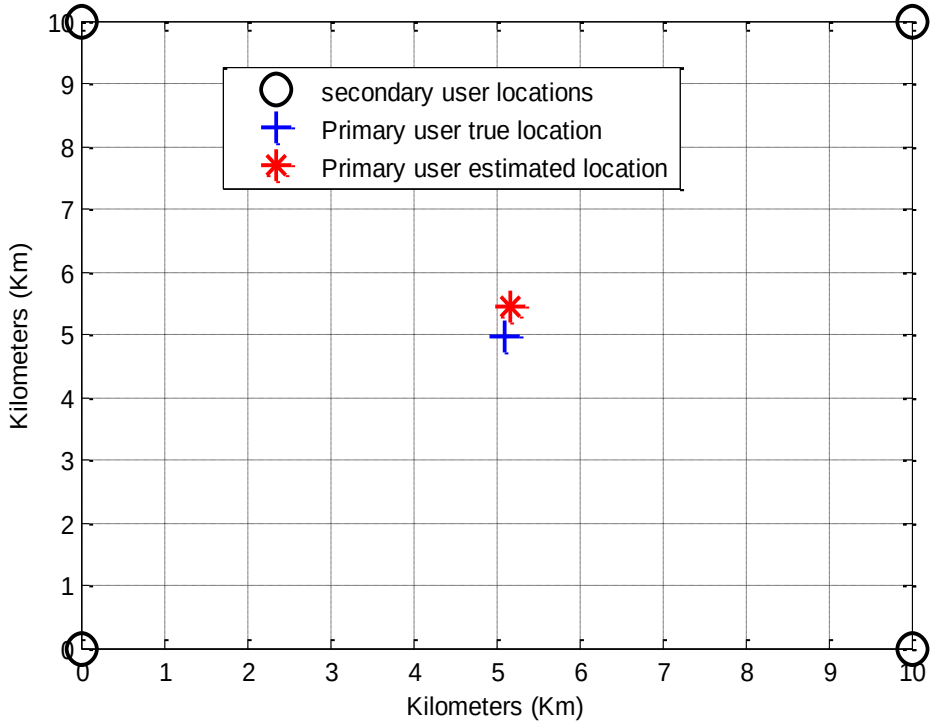

Figure 4-3:- Location of the primary user based on location coordinates

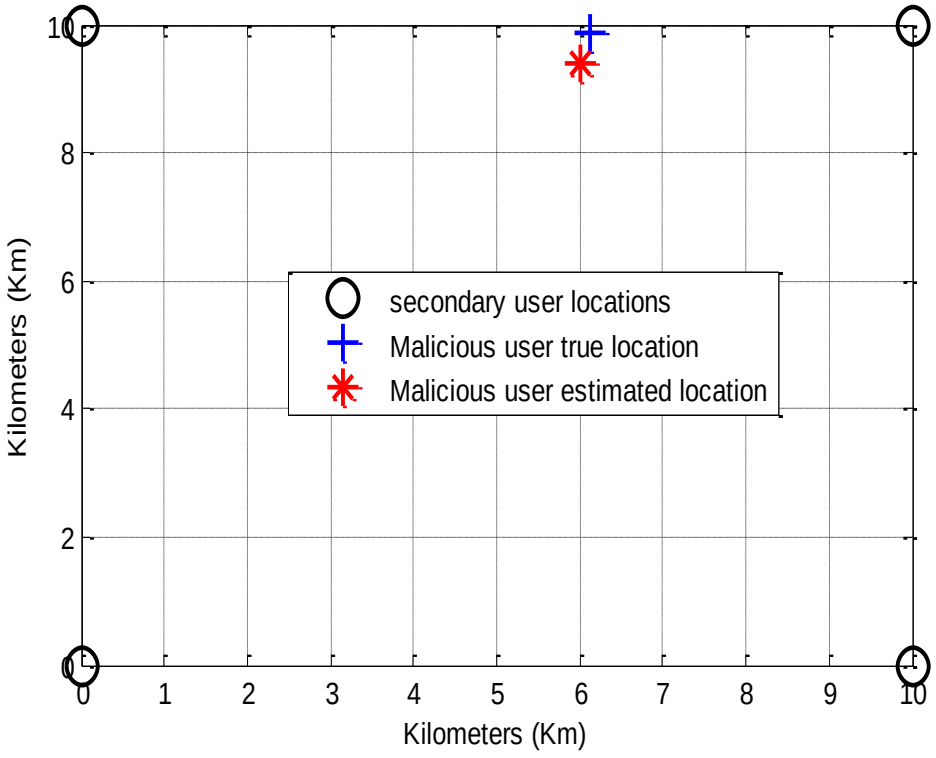

Figure 4-4:- Location of the malicious user based on location coordinates

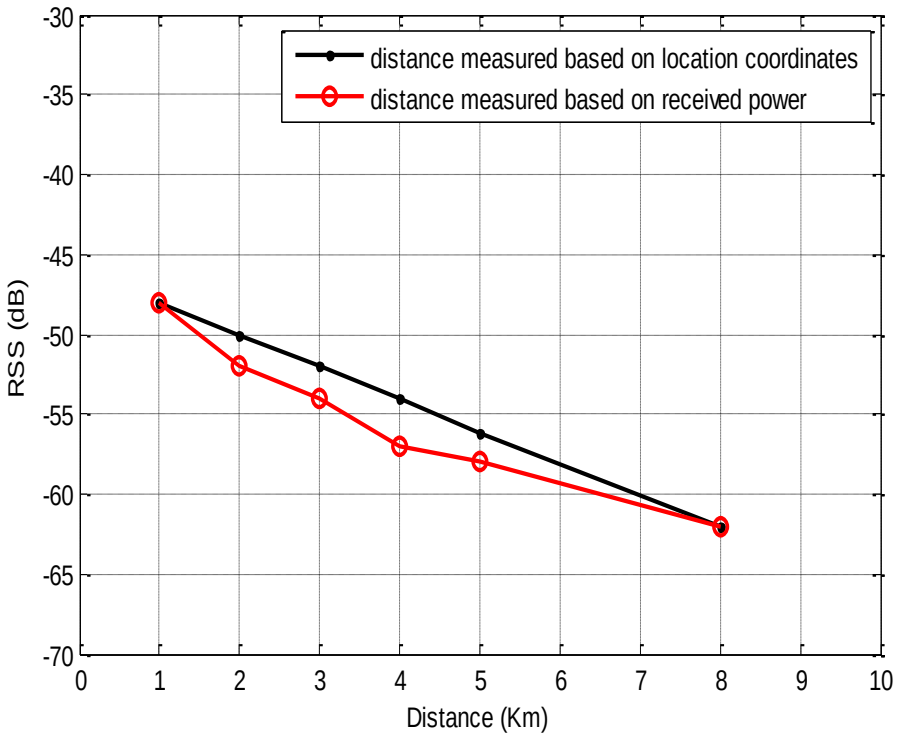

Figure 4-5:- Distance measured between the primary user and secondary user based on location coordinates and received power

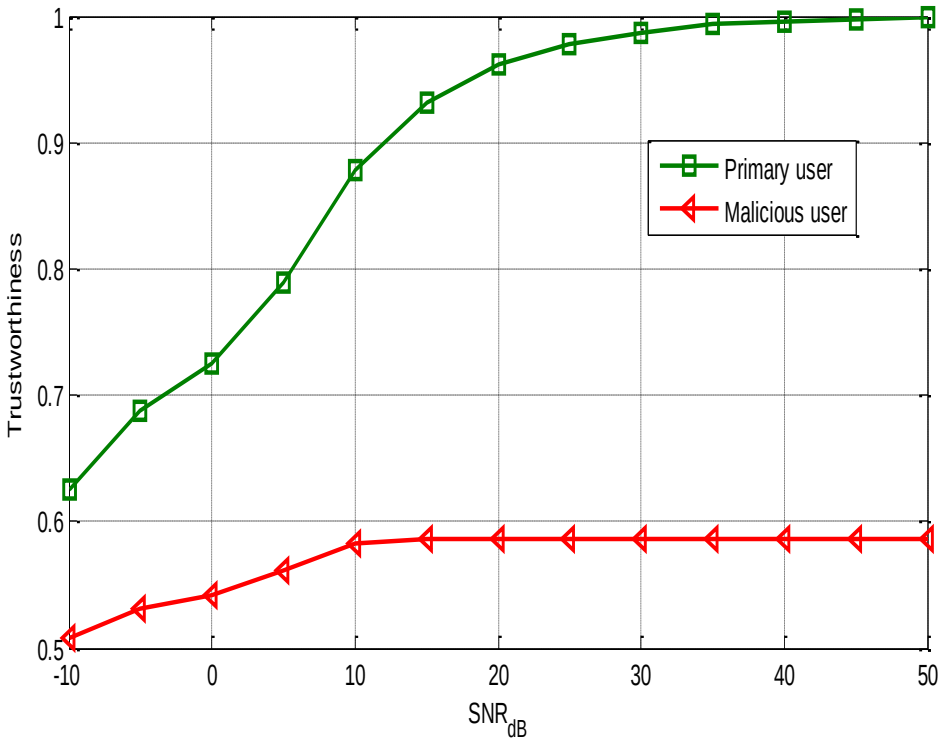

Figure 4-6:- Trustworthiness of a user in a cognitive radio network

4.7 Chapter Summary

Trust and its management are important fields of research due to its employment on trust systems and other security and commercial applications. In this chapter, we propose a technique that can be able to verify that the source of a spectrum sensing occupancy information is from a genuine primary user and not from a malicious secondary user masquerading to be a primary user. This way, malicious users can be evicted from the network and spectrum utilization efficiency will be maximized.

It is seen from our results that high quality and trustworthiness of received spectrum sensing occupancy information is very important to the decision maker (fusion center), in cognitive radio networks, so that any bias or untrue decision can be ignored or avoided.

CHAPTER FIVE

MITIGATING PRIMARY USER EMULATION ATTACKS IN COGNITIVE RADIO NETWORKS

5.0 Objective

The main objective of this chapter is to effectively mitigate primary user emulation attacks in cognitive radio networks. This is achieved by proposing an energy detection cooperative spectrum sensing technique in cognitive radio networks to assist in the reduction of errors made by secondary users in detecting primary user signals in frequency bands considering the existence of PUEA in the network. Our proposed technique is compared to an existing energy detection spectrum sensing technique which does not consider the existence of PUEA in the network to determine its performance.

5.1 Introduction

With the introduction of cooperative spectrum sensing in cognitive radio networks, the performance of spectrum sensing has greatly improved and there is a more accurate detection of primary signals [23]-[25]. However, cooperative spectrum sensing is still vulnerable to primary user emulation attacks which disrupt the entire network and cause performance degradation. Although, several research works have been proposed in literature to counter the various security threats associated to this attack as in [9], [30], [36] – [37],[45] – [47] [66] [67], none have been able to successfully combat PUEA in a cooperative spectrum sensing environment.

In this chapter, we establish a model of cooperative spectrum sensing with a PUEA present in the network. The PUEA, like other cognitive radio users, also perform spectrum sensing and send primary imitative signals when the primary user is absent**.** We propose a new technique to minimize the total error rate in the system by formulating a method of energy detection in secondary nodes to detect vacant bands before the fusion center makes a final decision using the OR/AND fusion rules. This is done so as to maximize primary user signal detection while limiting interference between users in the system. We also determine the optimal decision fusion rule that will minimize the total error rate with PUEA acting in the network. We

further consider a scenario where the PUEA constantly sends fake signals in both vacant and occupied bands in order to selfishly acquire the band thus making the secondary user to vacate the existing band. The results obtained from our proposed energy detection cooperative spectrum sensing technique is compared to a conventional energy detection cooperative spectrum sensing approach which is considered in [48] to determine its performance.

5.2 A System Model of a Cognitive Radio Network with PUEA Present

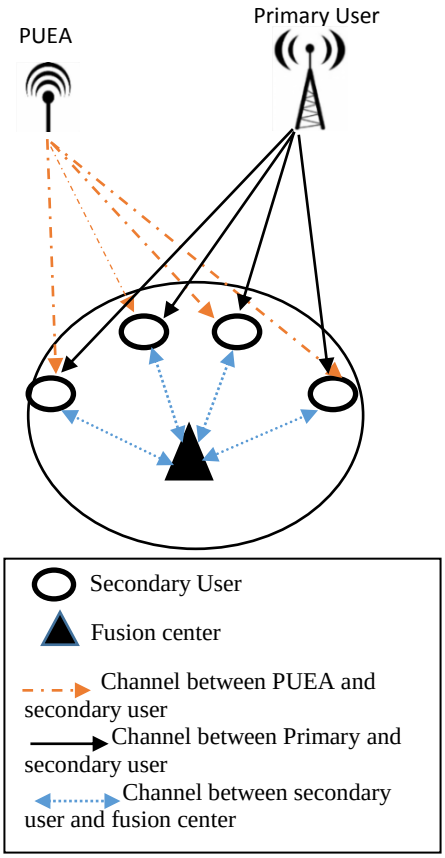

Figure 5-1:- System model of a cognitive radio network with PUEA present.

Our model, as in Figure 5.1, consists of a PUEA existing in a cognitive radio network with N cognitive radio secondary users and a fusion center. A malicious user or a PUEA is present in the network with the objective of deceiving the secondary users. The PUEA is aware of the radio environment and sends fake signals when the primary user is absent. The secondary

users employ energy detection for local spectrum sensing to detect spectrum holes and send its decision about the presence or absence of a primary user to the fusion center. The fusion center receives these decisions from all the secondary users and fuse them by using the OR/AND fusion rules to make a final decision. It is assumed that spectrum sensing for cognitive radio users is perfect.

Since the PUEA tend to send similar signals like the primary user, we can take $\sqrt{P_p}x_p^k$ and $\sqrt{P_a}x_a^k$ as the signals transmitted by the primary user and the PUEA, respectively with a power of $\sqrt{P_p}$ and $\sqrt{P_a}$ at the kth time instant. For simplicity, x_p^k is assumed to be independently and identically distributed (i.i.d.) complex Gaussian random variable with a zero mean and a constantly known variance σ_p^2. x_a^k also follows a complex Gaussian random distribution with a zero mean and a constantly known variance σ_a^2 as well.

We define y_i^k to be the signal received at ith secondary user at the kth time instant. H_0 and H_1 indicates the presence and absence of the primary user signal in our model while A_0 and A_1 indicates the absence and presence of the PUEA signal.
Since it is assumed that the PUEA does not transmit when the primary user is present, there will be three possible outcomes of received signal y_i^k, at the ith secondary user which is labeled: $z_1 = \{A_0, H_1\}$, $z_2 = \{A_1, H_0\}$ and $z_3 = \{A_0, H_0\}$.
Therefore,

$$y_i^k = \begin{cases} \sqrt{P_p}x_p^k\, h_{p,i}^k + n_i^k, & \text{under } z_1 \\ \sqrt{P_a}x_a^k\, h_{a,i}^k + n_i^k, & \text{under } z_2 \\ n_i^k & \text{under } z_3 \end{cases} \tag{5.1}$$

where n_i^k is the additive white Gaussian noise at the ith secondary user with zero mean and variance $\sigma_{n,i}^2$, $h_{p,i}^k$ is the channel gain between the primary user and ith secondary user at kth time instant and $h_{a,i}^k$ is the channel gain between the PUEA and ith secondary user at kth time instant. We assume block fading channels with channel coefficients that can be constant in every detection time [64]. Therefore, k can be omitted from $h_{p,i}^k$ and $h_{a,i}^k$. From equation (5.1), y_i^k will be a complex random variable under z_j for $j \in \{1, 2, 3\}$.

$$y_i^k \sim CN(0, \sigma_{j,i}^2) \quad \text{under } z_j, \quad j \in \{1, 2, 3\}, \tag{5.2}$$

we can easily verify that

$$\sigma_{1,i}^2 = P_P \sigma_p^2 |h_{p,i}|^2 + \sigma_{n,i}^2 ,$$

$$\sigma_{2,i}^2 = P_a \sigma_a^2 |h_{a,i}|^2 + \sigma_{n,i}^2 ,$$

$$\sigma_{3,i}^2 = \sigma_{n,i}^2 .$$

5.3 Proposed Cooperative Spectrum Sensing Technique against PUEA

In this section, we will introduce a spectrum sensing process that takes into account the presence of a PUEA which sends fake primary signals when the primary user is not present. In the cooperative spectrum sensing process, every secondary user independently performs its local spectrum sensing, makes a binary decision and forwards these binary decisions to the fusion center (FC) to make a final decision about the presence or absence of the primary signal in the observed frequency band. There are many fusion rules that can be applied at the fusion center [49]. For this work, we will use the logic OR and logic AND rules because given a targeted probability of detection or a targeted probability of false alarm, each secondary user's threshold can easily be derived. In OR rule, the FC will declare the presence of the primary user when at least one of the secondary users detects the primary signal, otherwise the frequency band is regarded as vacant. In the AND rule, the presence of the primary user is declared by the FC only when all the secondary users detect the primary signal, otherwise the frequency band is regarded as vacant.

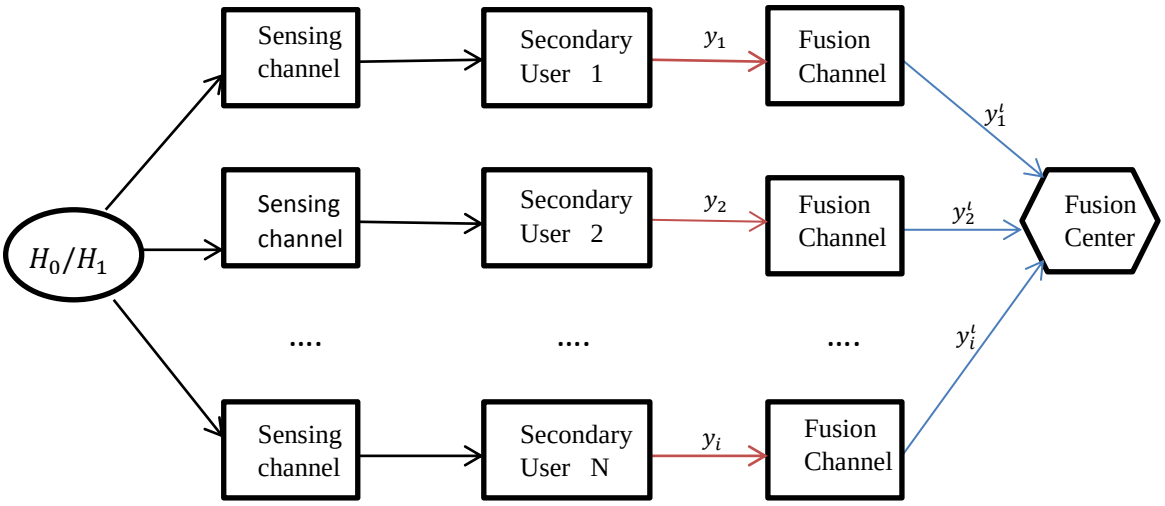

Figure 5-2:- Cooperative spectrum sensing in cognitive radio networks.

Figure 5.2 shows a schematic illustration of cooperative spectrum sensing in cognitive radio networks. To evaluate the performance of cognitive radio spectrum sensing, we use the probability of detection (p_d) and the probability of false alarm (p_f) for both fusion rules. From the cooperative spectrum sensing algorithm in [68], the probability of detection (p_d) and the probability of false alarm (p_f) for OR/AND fusion rules can be derived.

For OR fusion rule, the (P_d^{OR}) and (P_f^{OR}) of the final decision made by the fusion center using the local spectrum decisions can be written as

$$P_d^{OR} = 1 - \prod_{i=1}^{N}(1 - p_d^i)\,, \tag{5.3}$$

$$P_f^{OR} = 1 - \prod_{i=1}^{N}(1 - p_f^i)\,, \tag{5.4}$$

similarly, for AND fusion rule, the (P_d^{AND}) and (P_f^{AND}) of the final decision made by the fusion center using the local spectrum sensing can also be expressed as

$$P_d^{AND} = \prod_{i=1}^{N} p_d^i\,, \tag{5.5}$$

$$P_f^{AND} = \prod_{i=1}^{N} p_f^i\,, \tag{5.6}$$

where p_d^i and p_f^i are the probabilities of detection and false alarm, respectively, in the local spectrum sensing process of any the secondary users in the cognitive radio network. This can be expressed as,

$$p_d^i = p(D_{on}^i|H_1)\,, \tag{5.7}$$

and

$$p_f^i = p(D_{on}^i|H_0)\,, \tag{5.8}$$

where D_{on}^i indicates that ith secondary user has decided that primary signal is present and D_{off}^i indicates that ith secondary user has decided that primary signal is not present.

Since fake signals are sent by the PUEA when the primary signal is not present, that means the PUEA signal will be received by the secondary users under H_0 only. In the event of an attacker, only the probability of false alarm (p_f^i) will be affected. So involving the presence or absence of an attacker A_0 and A_1 respectively in equation (5.8), we then have

$$p_f^i = p\left(D_{\text{on}}^i \middle| A_0, H_0\right)p(A_0|H_0) + p\left(D_{\text{on}}^i \middle| A_1, H_0\right)p(A_1|\, H_0), \quad (5.9)$$

where $p(A_0|H_0)$ and $p(A_1|\, H_0)$ are conditional probabilities regarding the presence and absence of fake PUEA attacker signals which are related to the attacker strategy. If the primary signals are such that their transmission parameters are recognized by all, e.g TV towers, then it is assumed that $p(H_0)$ is known. So we can consider $p(A_0|H_0)$ and $p(A_1|\, H_0)$ as constant values.

For simplicity of notations, we define

$$p(A_1|H_0) = \beta\ , \quad (5.10)$$

and

$$p(A_0|H_0) = 1 - p(A_1|H_0) = \ 1 - \beta\ , \quad (5.11)$$

therefore, we can rewrite equation (5.9) as

$$p_f^i = p\left(D_{\text{on}}^i \middle| A_0, H_0\right)(1 - \beta) + p\left(D_{\text{on}}^i \middle| A_1, H_0\right)\beta \quad (5.12)$$

5.4 Proposed Energy Detection Based Cooperative Spectrum Sensing with PUEA

Energy detection is the most popular sensing technique in cooperative sensing due to its simplicity and no requirement on a prior knowledge of the primary user signal [50]. A local spectrum sensing is performed by the secondary users in the presence of PUEA. It is assumed that every secondary user adopts the energy detection technique in which M samples of the energy of y_i^k are summed during a detection interval,

$$Y_i = \sum_{k=1}^{M} |y_i^k|^2\ . \quad (5.13)$$

Y_i is compared to a threshold which every secondary user decides locally about the presence and absence of a primary user signal. The probability of detection and the probability of false alarm for a ith secondary user in energy detection can be written as:

$$p_d^i = p(Y_i \geq T_i|H_1)\ , \quad (5.14)$$

$$p_f^i = p(Y_i \geq T_i|H_0)\ , \quad (5.15)$$

where T_i is the threshold used in energy detector of the ith secondary user. Based on equation (5.13), Y_i in energy detection is sum of y_i^k squared represented in equation (5.1). From equation (5.2), y_i^k is Gaussian random variable with zero mean and variance $\sigma_{j,i}^2$ under z_j, $j \in \{1, 2, 3\}$. So Y_i will be compliant with the central Chi-square (χ^2) distribution with $2M$ degrees of freedom and parameter $\sigma_{j,i}^2$.

$$Y_i = \begin{cases} \chi_{2M}^2\ (\sigma_{1,i}^2)\,, & \text{under}\ \ z_1 = \{A_0, H_1\} \\ \chi_{2M}^2\ (\sigma_{2,i}^2)\,, & \text{under}\ z_2 = \{A_1, H_0\}\ . \\ \chi_{2M}^2\ (\sigma_{3,i}^2)\,, & \text{under}\ z_3 = \{A_0, H_0\} \end{cases} \tag{5.16}$$

In determining the performance of the analyzed spectrum sensing method from the previous section, we employ Neyman-Pearson criterion [51] to determine the probability of detection using energy detection based cooperative spectrum sensing. Neyman-Pearson technique provides a threshold for detection subject to a constant probability of false alarm p_f^i. Based on equation (5.9), we need the values of $p\left(D_{\text{on}}^i \middle| A_1, H_0\right)$ and $p\left(D_{\text{on}}^i \middle| A_0, H_0\right)$, which can be written in energy detection as

$$p\left(D_{\text{on}}^i \middle| A_1, H_0\right) = p(Y_i \ \geq\ T_i | A_1, H_0)\,, \tag{5.17}$$

$$p\left(D_{\text{on}}^i \middle| A_0, H_0\right) = \ p(Y_i \ \geq\ T_i | A_0, H_0). \tag{5.18}$$

As in [52] we can now rewrite equation (5.7) for energy detection based spectrum sensing as

$$p_d^i = \frac{\Gamma(M, \frac{T_i}{\sigma_{1,i}^2})}{\Gamma(M)}\,, \tag{5.19}$$

where $\Gamma(.)$ and $\Gamma(.,.)$ are Gamma function and upper incomplete Gamma function [53], respectively. Equation (5.12) can also be written as

$$p_f^i = \frac{\Gamma(M, \frac{T_i}{\sigma_{3,i}^2})}{\Gamma(M)}\ (1 - \ \beta) + \frac{\Gamma(M, \frac{T_i}{\sigma_{2,i}^2})}{\Gamma(M)}\beta\ . \tag{5.20}$$

In Neyman-Pearson criterion, it is shown that for a given probability of false alarm, the optimal threshold which maximizes the probability of detection can be obtained if the given probability of false alarm is the actual considered probability of false alarm.

With PUEA considered in our proposed method, we can evaluate the method by comparing it to the conventional energy detection spectrum sensing method that does not consider an attacker in the system like the one proposed in [48]. In evaluating the system performance, a parameter relating to spectrum sensing called probability of error is used. The probability of error defines the probability of making a wrong decision in spectrum sensing. That is declaring the presence of primary user when primary signal is not present or declaring the absence of primary user when primary user is actually sending signals. For OR FC rule, we can express the probability of error as

$$p_e^{OR} = p(H_0, D_{on}^{OR}) + p\left(H_1, D_{off}^{OR}\right),$$

$$= p(H_0)p_f^{OR} + \ p(H_1)p_m^{OR}, \tag{5.21}$$

we can also express the probability of error in AND FC rule as

$$p_e^{AND} = \ p(H_0)p_f^{AND} + \ p(H_1)p_m^{AND} \ . \tag{5.22}$$

5.5 Proposed Technique for the Case of an Always Present Attacker in the Network

There is, an extreme case where a PUEA constantly sends fake signals in the cognitive radio environment irrespective of a band being vacant or occupied. That is, we can assume that the PUEA performs a kind of spectrum sensing to send fake signals both in vacant and occupied frequency band. The effect of these fake signals transmitted constantly by the PUEA will destroy the entire spectrum sensing process and prompting secondary users to make erroneous decisions and also cause interference in the network [65]. In this case, there will be a possible outcome of $z_4 = \{A_1, H_1\}$ where both the primary user and PUEA are both transmitting in the cognitive radio environment. Then,

$$y_i^k = \sqrt{P_p}x_p^k \ h_{p,i}^k + \sqrt{P_a}x_a^k \ h_{a,i}^k + n_i^k, \text{ under } z_4, \tag{5.23}$$

where y_i^k is a complex random variable with a mean of zero and variance of $\sigma_{4,i}^2$.

$$y_i^k \sim CN(0, \sigma_{4,i}^2) \quad \text{under } z_4, \tag{5.24}$$

and

$$\sigma_{4,i}^2 = P_P \sigma_p^2 |h_{p,i}|^2 + P_a \sigma_a^2 |h_{a,i}|^2 + \sigma_{n,i}^2$$

In the presence of a constant attacker sending fake signals over the licensed frequency band, PUEA signal will be received by the secondary users under both H_0 and H_1. The probability of detection (p_d^i) is now affected by the presence of an attacker and (p_f^i) will still be the same as analyzed in equation (5.9). The probability of detection, (p_d^i), is now expressed as

$$p_d^i = p\left(D_{\text{on}}^i \middle| A_1, H_1\right) p(A_1 | H_1) + p\left(D_{\text{on}}^i \middle| A_0, H_1\right) p(A_0 | H_1), \tag{5.25}$$

where $p(A_1 | H_1)$ and $p(A_0 | H_1)$ are now the new conditional probabilities regarding the presence and absence of the attacker. If we take $p(A_1 | H_1)$ to be α for easy notation, then $p(A_0 | H_1)$ will be $1 - \alpha$. Equation (5.25) can now be written as

$$p_d^i = p\left(D_{\text{on}}^i \middle| A_1, H_1\right) \alpha + p\left(D_{\text{on}}^i \middle| A_0, H_1\right) (1 - \alpha). \tag{5.26}$$

In the same way as in the previous section, formulating the cooperative spectrum sensing technique based on energy detection, Y_i will also be compliant with the central Chi-square (χ^2) distribution with $2M$ degrees of freedom and parameter $\sigma_{4,i}^2$ and is given by

$$Y_i \sim \chi_{2M}^2 \left(\sigma_{4,i}^2\right), \text{ under } z_4 = \{A_1, H_1\}, \tag{5.27}$$

and

$$p\left(D_{\text{on}}^i \middle| A_1, H_1\right) = p(Y_i \geq T_i | A_1, H_1) = \frac{\Gamma\left(M, \frac{T_i}{\sigma_{4,i}^2}\right)}{\Gamma(M)}, \tag{5.28}$$

$$p\left(D_{\text{on}}^i \middle| A_o, H_1\right) = p(Y_i \geq T_i | A_0, H_1) = \frac{\Gamma\left(M, \frac{T_i}{\sigma_{1,i}^2}\right)}{\Gamma(M)}. \tag{5.29}$$

So the probability of detection p_d^i in equation (5.26) can be rewritten as

$$p_d^i = \frac{\Gamma\left(M, \frac{T_i}{\sigma_{4,i}^2}\right)}{\Gamma(M)} \alpha + \frac{\Gamma\left(M, \frac{T_i}{\sigma_{1,i}^2}\right)}{\Gamma(M)} (1 - \alpha). \tag{5.30}$$

5.6 Simulations and Discussion

We implemented the simulations of the proposed energy based cooperative sensing technique with the existence of a PUEA in the network and compare the results with the a conventional energy based spectrum sensing method which does not consider the existence of a PUEA in the network as seen in [48] in order to determine its performance.

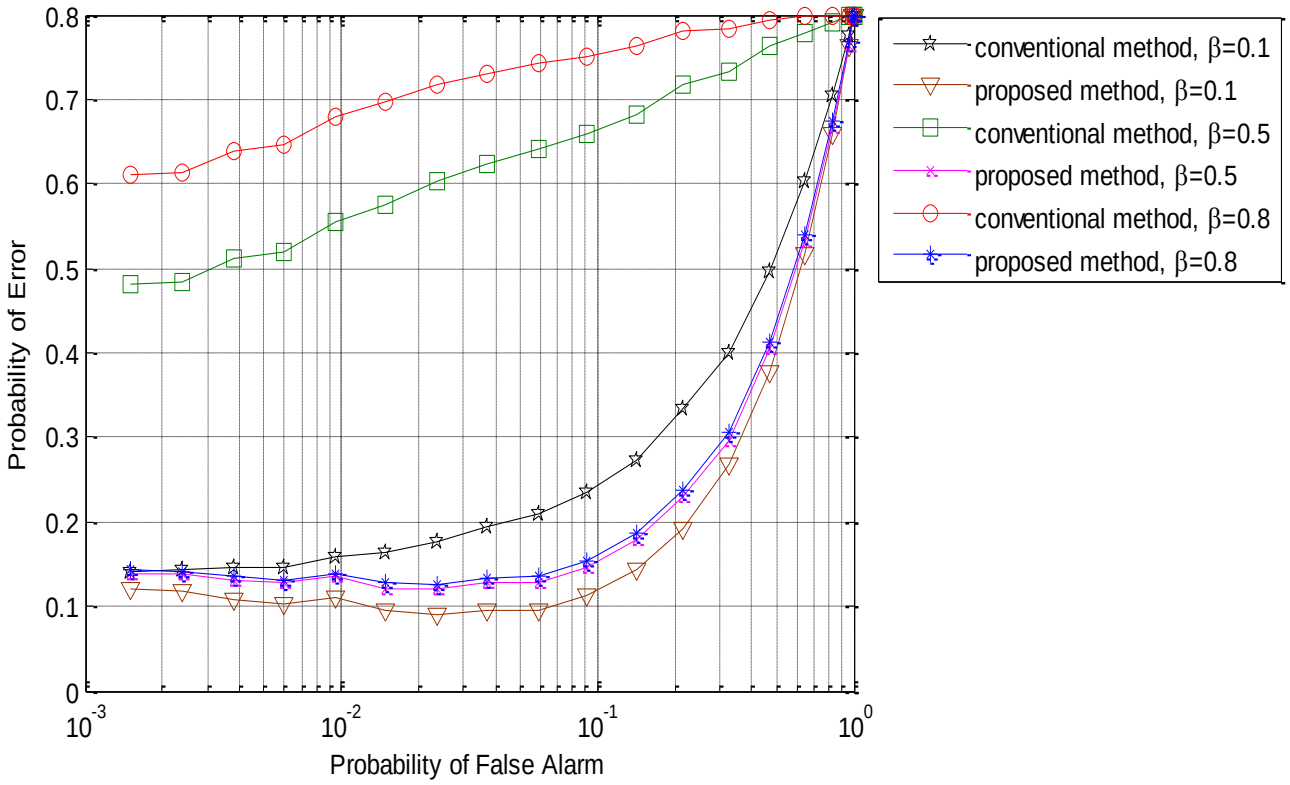

Figure 5-3:- Probability of error against the probability of false alarm for the proposed and the conventional method with N = 6 using the OR fusion rule.

The channels are assumed to be identically and independently distributed block Rayleigh fading and the channel information is assumed to be known to the users in the cognitive radio network. The average SNR at every secondary user is set to 0 dB. The number of samples within a detection interval is $M = 3$. Since we are aware of $p(H_0)$ and $p(H_1)$ even when there is not either CR signal or fake signal, so we consider them as constant known values, so $p(H_0)$ and $p(H_1)$ are taken as 0.8 and 0.2, respectively.

Figure 5.3 shows the performance comparison of the proposed energy detection spectrum sensing method and the conventional energy detection method. The performance of each method is examined by setting N, the number of secondary users present in the network, to 6 and using the OR fusion rule. As seen in the figure, our proposed method tends to have a

lower probability of error when compared to the conventional method of spectrum sensing. The increase of β, which is the probability of PUEA signal occurrence in the network is seen to have a negative effect on the performance of the conventional spectrum sensing method.

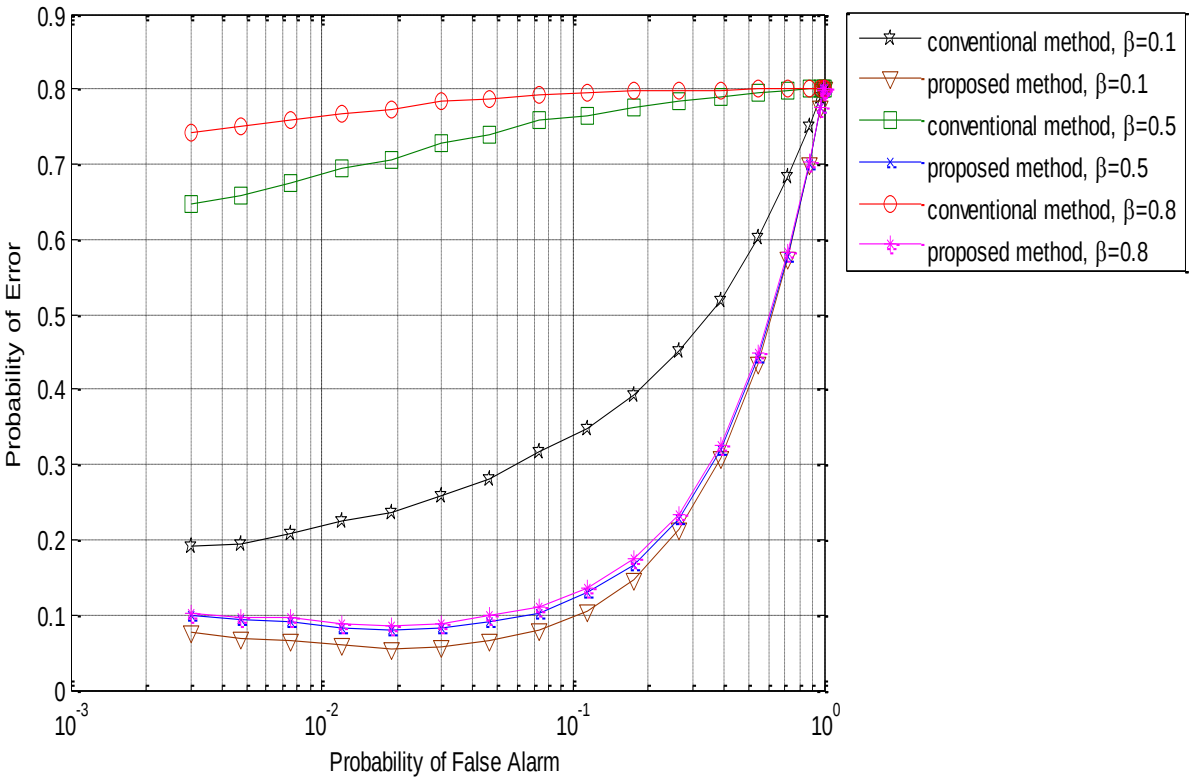

Figure 5-4:- Probability of error against the probability of false alarm for the proposed and the conventional method with N = 12 using the OR fusion rule.

Figure 5.4 also shows the probability of error versus the probability of false alarm for both spectrum sensing methods in the OR fusion rule with the number of secondary users N increased to 12. As already known, if there is an increase in the number of cooperating secondary users in the system, there will be an increase in the probability of detection or a decrease in the probability of error. But it can be observed in the figure that increasing the number of secondary users in the network has not reduced the probability of error for the conventional method while our proposed method still maintains a very low probability of error for different values of β.

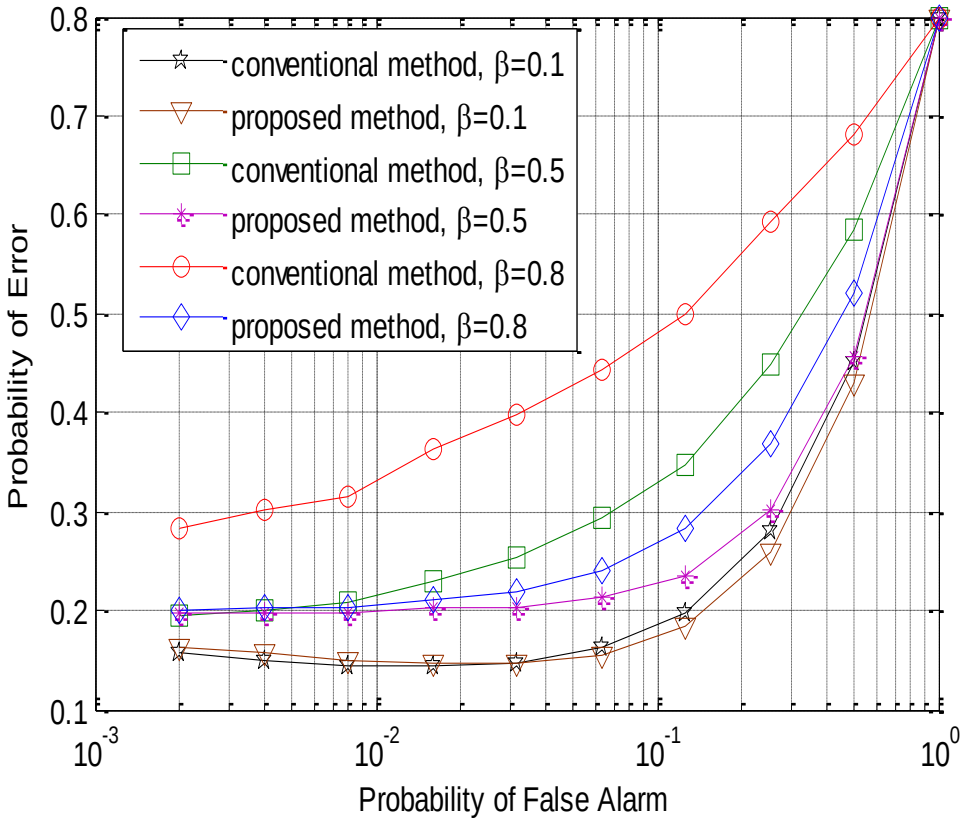

Figure 5-5:- Probability of error against the probability of false alarm for the proposed and the conventional method with N = 6 using the AND fusion rule.

In Figure 5.5, our proposed energy detection spectrum sensing method is also compared with the energy detection spectrum sensing method considered in [48] for the AND fusion rule with number of secondary users N set at 6. We can see that the proposed method performs a lot better than the conventional method due to the secondary users awareness of fake signals in the network hence it has a very low probability of error even when there is an increase in β.

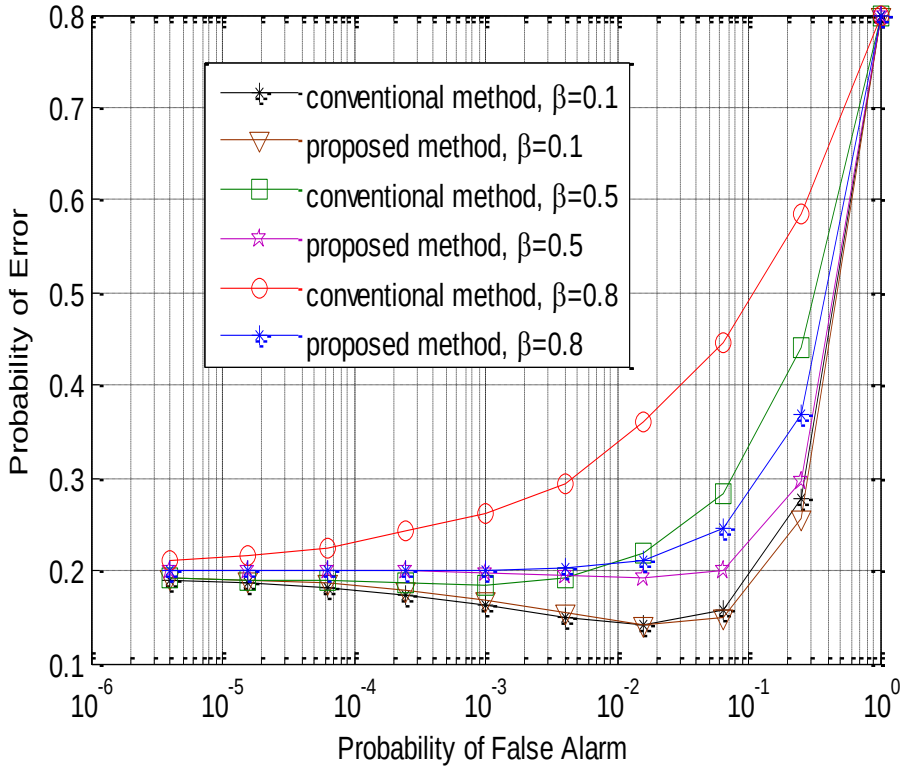

Figure 5-6:- Probability of error against the probability of false alarm for the proposed and the conventional method with N = 12 using the AND fusion rule.

Figure 5.6 also illustrates the probability of error versus the probability of false alarm in the AND fusion rule with the number of secondary users N set at 12. Due to the increase in the number of cooperating users, it is seen that there is an improved performance in our proposed method in the presence of PUEA and the conventional spectrum sensing method is severely compromised by the presence of PUEA in the network. Also as β increases, there is an increase in the probability of error for the conventional spectrum sensing method.

Figure 5.7 and figure 5.8 show the performance of our proposed method in the case of an attacker constantly sending fake signals to the cognitive radio network in the OR and AND fusion rule respectively. Our proposed spectrum sensing method is also compared with the conventional spectrum sensing method and the case of no attacker present in the network. From both figures, as expected, it is observed that there is a greater performance from our proposed method in the presence of a constant attacker compared to the considered conventional method.

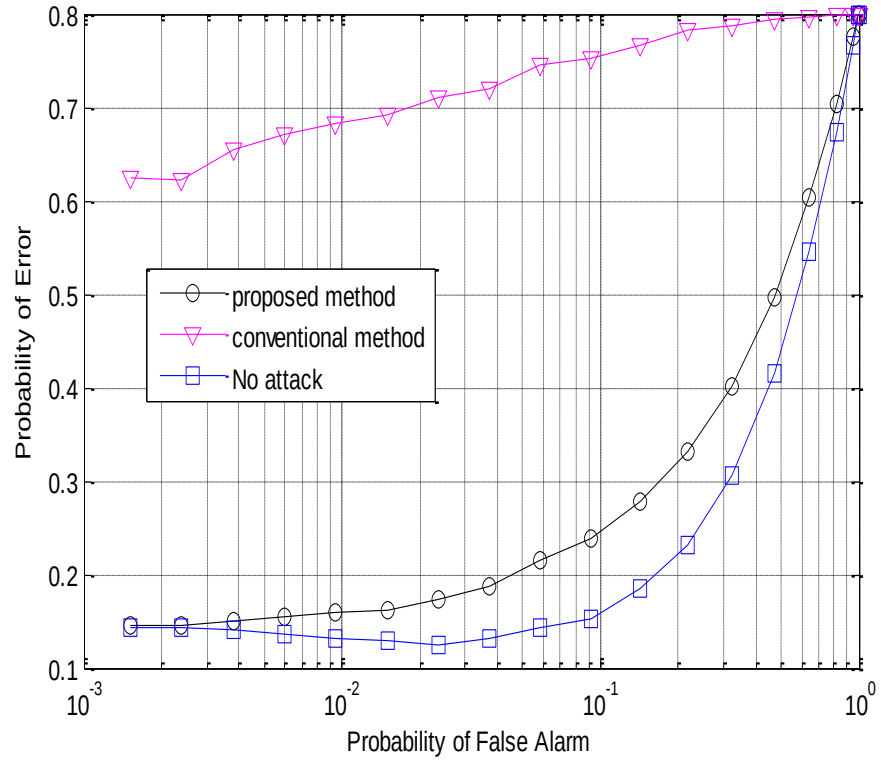

Figure 5-7:- Probability of error against the probability of false alarm for the proposed and the conventional method for an always present attacker using the OR fusion rule.

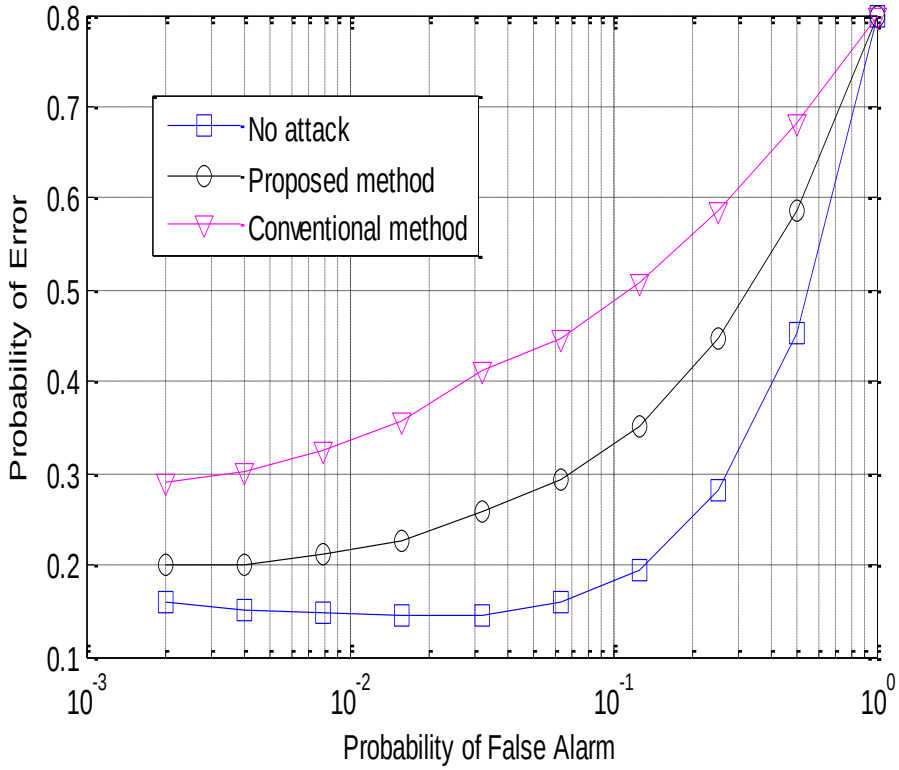

Figure 5-8:- Probability of error against the probability of false alarm for the proposed and the conventional method for an always present attacker using the AND fusion rule.

From all the results, we can deduce that the conventional spectrum sensing method using the AND fusion rule often leads to a low probability of error in the network. This is so because all secondary users must declare the presence of a primary user signal before a final decision will be made about the presence of a primary user. Thus, if the conventional spectrum sensing method must be used, it should be used under the AND fusion rule. But again, our proposed spectrum sensing method has an improved performance over the conventional spectrum sensing method in both the OR and AND fusion rules with a much higher improvement in the OR fusion rule. In conclusion, we can say that the best possible mitigation of PUEA in a cognitive radio network is achieved using the proposed spectrum sensing method in the OR fusion rule.

5.7 Chapter Summary

This chapter focuses on mitigating one of the common and perilous attacks associated to cognitive radio network which is the Primary User Emulation Attack (PUEA). When the primary user is not present, an attacker sends primary-like signals in the network. We therefore introduced a spectrum sensing technique under PUEA which can enable secondary users to make the right decision about the presence or absence of a primary signal in a frequency spectrum band. This spectrum sensing technique employs spectrum sensing rules (OR and AND fusion rules) at the fusion center to make final decisions in the network. The proposed spectrum sensing method is also applied to the case where a PUEA constantly sends fake signals in the cognitive radio network.

The performance of the proposed method is compared with the conventional method which does not acknowledge the presence of PUEA in the network. Our simulation results shows that a greater improvement in the probability of error for both OR and AND fusion rules can be achieved using the proposed method. In order to achieve an optimal performance in mitigating PUEA in cognitive radio networks, the proposed method in the OR fusion rule can be deployed.

CHAPTER SIX

CONCLUSION AND FUTURE WORK

6.1 Conclusion

In recent years, technologies and innovations in wireless networks have gained significant improvements and the competition for access to the electromagnetic spectrum has substantially increased. Thus, wireless technologies needs to cooperate and share the electromagnetic spectrum in a non-interfering manner for useful communication. As the number of wireless technology users increase, there is an increasing scarcity of spectrum resources. Therefore, some regulatory bodies like the Federal Communications Commission (FCC) has decided to permit unlicensed (secondary) users to make use of the spectrum belonging to licensed (primary) users by employing a cognitive radio (CR). Cognitive radio networks (CRNs) monitor available spectrum band, capture their information and automatically identify spectrum holes. The most efficient way to identify these spectrum holes is by a spectrum sensing process. However, existing spectrum sensing techniques are vulnerable to a kind of attack called primary user emulation attack that mimics or impersonates the characteristics of a primary user in order to get unrivalled access to the spectrum band thereby reducing the bandwidth available to the CRN. In the comprehensive research work that has been carried out, we examine the impacts of this attack and propose a technique to mitigate it. This will help to effectively differentiate between honest and malicious users in the network and greatly improve the security of CR networks.

In chapter 2, the concept of cognitive radio was introduced and its architecture and basic functions was presented. Other topics of importance relating to the theoretical foundation of this research were also discussed. These included spectrum sensing techniques that are used by cognitive radio and also the security threats associated to cognitive radio networks.

In chapter 3, the concept of primary user emulation attack (PUEA) was described and its impacts on cognitive radio network were investigated. A system model of PUEA was also

presented. We also presented an analysis to calculate the powers and probability density function (PDF) of both malicious users and good secondary users. The PDF obtained is used in Neyman-Pearsons composite hypothesis test to investigate the impacts of PUEA in the network. Our simulated results show that the number of malicious users in the system can significantly increase the probability of false alarm in the network resulting in secondary users to suffer degradation in the quality of their communication due to the action of malicious users in the network.

In the vein of curtailing the impacts of PUEA in cognitive radio networks, trust among secondary users in the network has been established in chapter 4, whereby verification techniques are carried out to enable secondary user nodes identify whether spectrum occupancy information provided is from genuine users in the network. In our proposed verification techniques, the distance between a cognitive secondary user and other users is calculated based on location coordinates and also based on received power level. If the distance calculated using either proposed methods matches or is extremely close to each other, then the user is regarded as a trustworthy user and hence other users can communicate with the secondary user but if otherwise, then the user is regarded as a malicious user and its spectrum occupancy information will be ignored. We also propose a verification tag technique to enable secondary users verify if a primary user is indeed using a specific spectral band. This was achieved by adding a verification tag to the primary user signal where the secondary user retrieves this tag from the primary user and uses this tag to verify whether a spectrum is currently being used by its legitimate owner or not. From our simulated results, it is seen that the trustworthiness of a primary user tends to be higher than that of a malicious user. That is to say that high quality and trustworthiness of received spectrum sensing occupancy information is very vital to the fusion center which is the decision maker on presence and absence of a primary users in the network.

In chapter 5, we have briefly described the cooperative spectrum sensing principle and benefit of it increasing the agility in CR networks. We have also extensively researched on how PUEA can be extenuated in cognitive radio networks using cooperative spectrum sensing. Firstly, a system model of cognitive radio network in the presence of a PUEA was presented. Since PUEA primarily disrupts the spectrum sensing process of cognitive radio networks, an energy detection cooperative spectrum sensing technique was proposed to evict PUEA from the network and also increase secondary user spectrum sensing performance.

This proposed technique uses the logic OR and logic AND fusion rules in the fusion center to make the final decision about the presence or absence of a primary user in a specific spectral band.

An energy detection based cooperative spectrum sensing technique was also proposed for the case of an always present attacker in the network. Our simulation result which was compared to a conventional defense technique shows that our proposed method tend to have a lower probability of error to that of the conventional method even if the probability of an attacker in the network is increased. Again, in our results it was deduced that our proposed energy detection cooperative spectrum sensing technique using the OR fusion rule is more effective in mitigating PUEA in cognitive radio networks. This can solve the problem of spectrum scarcity and unavailability and thus can save millions of dollars.

6.2 Future work

The focus of this research work has been on security challenges facing cognitive radio networks especially Primary User Emulation Attacks. However, the concept of cognitive radio is relatively new and there is still much work to do in this regard. The other areas of possible research that maybe explored may include the following:

- Further investigations into other threats and attacks that cognitive radios networks face and possibly introduce efficient prevention techniques to mitigate them.
- In this thesis, it was assumed that the secondary users have a perfect knowledge of the channel state information. More work can be done on the case where there exists different channel estimation errors and investigate the corresponding impacts on the detection and mitigation performance.
- Further work can also be done by considering a case when multiple attackers are considered in the cooperative spectrum sensing environment and analyse the corresponding detection performance.
- The incorporation of this work into a complete cognitive radio simulator or a physical cognitive radio test bed.

REFERENCES

[1] E. C. N. Federal Communications Commission (FCC), "03-222", Notice of Proposed Rule Making and Order, *Implementation of the Final ACTS OF THE World Radio Communication Conference (WRC-07),* Geneva, August, 2003.

[2] M. McHenry, "Spectrum white space measurements". Presented to New America Foundation Broadband Forum, Shared Spectrum Company, Tech. Rep., June, 2003.

[3] US Federal Communications Commission, "Spectral policy task force report" Report of the Unlicensed Devices and Experimental Licenses Working Group. Tech. Rep. ET Docket 02 – 155, November, 2002.

[4] D. Cabric, S. Mishra, D Willkomm, R. Brodersen, and A. Wolisz, " A cognitive radio approach for usage of virtual unlicensed spectrum," *in Proceedings of the 14th IST Mobile and Wireless Communications Summit*, Dresden, Germany. June, 2005.

[5] Q. Zhao and B.M. Sadler, "A survey of dynamic spectrum access," IEEE Signal Processing Magazine, Vol. 24, No. 3, 2007. pp. 79-89.

[6] Federal Communications Commission, "Mobile broadband: the benefits of additional spectrum," FCC staff technical paper, Washington, US. October, 2010.

[7] J. Mitola and G.Q. Maguire, Cognitive radio: "Making software radios more personal", *IEEE Communication Magazine*, vol. 6, No 4, August, 1999. pp. 13 – 18.

[8] J. Mitola III, "Software radio architecture: a mathematical perspective," IEEE *Journal on Selected Areas of Communications*., Vol. 17, No 4, April, 1999. pp. 514 – 538.

[9] R. Chen, M. 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, January, 2008. pp. 25-37.

[10] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. IEEE Workshop Networking Technologies for Software Defined Radio Networks (SDR),* September, 2006. pp. 110 – 119.

[11] A. Attar, H. Tang, "A Survey of Security Challenges in Cognitive Radio Networks*" Solutions and Future Research Directions. Proceedings of the IEEE,* Vol. 100, No. 12, December, 2012. pp. 4446 – 4456.

[12] Federal Communications Commission, "Notice of Proposed Rulemaking" First report and order, in the matter of unlicensed operation in the TV broadcast bands," *ET Docket No. 04-186 (FCC 04-113)* May, 2004.

[13] ITU-R, "Definitions of Sofware Defined Radio (SDR) and Cognitive Radio System (CRS)," ITU-R. Tech. Rep. SM.2152, September, 2009.

[14] B. Fette, "Three obstacles to cognitive radio," *EE Times,* August. 2004, quoting Joseph Mitola.

[15] K. C. Chen, Y.C Peng, N. Prasad, Y.C. Liang and S, Sun, "Cognitive radio network architecture; Part 1 – General structure". *Proceedings of the ACM International Conference on Ubiquitous Information Management and Communication*, Seoul, February, 2008.

[16] T. Yucek and Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications. "*IEEE Communication. Survey and Tutorials,* Vol. 11, No 1, March, 2009. pp. 116 – 133.

[17] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal Selected Areas in Communications,* Vol. 23, No. 2, February, 2005. pp. 2015 – 2020.

[18] Y. Zeng, T-C. Liang, A.T. Hoang, and R. Zhang, "A review on spectrum sensing for cognitive radio: challenges and solutions," *EURASIP Journal Advances in Signal Process*, Vol. 20, June, 2010. pp. 1-15.

[19] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios", *IEEE Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol. 1. California, USA. November, 2004, pp. 772–776.

[20] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," *Proceedings of Allerton Conference on Communicaions, Control, and Computing (Monticello)*, Illinois, USA. October 2004. pp. 1549 – 1561.

[21] A. Pandharipande, J. Kim, D. Mazzarese, and B. Ji, IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22, November, 2005. available at: http://www.ieee802.org/22/

[22] A. Famous, Y. Sagduyu and A. Ephremides, "Reliable spectrum sensing and opportunistic access in network-coded communications" *IEEE Journal on Selected Areas in Communications.* Vol. 32, March, 2010. pp. 400 - 410.

[23] G. Ganesan and Y. G. Li, "Cooperative spectrum sensing in cognitive radio networks," *Proceedings IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks* (DySPAN'05), Baltimore, USA, November, 2005. pp. 137-143.

[24] S. M. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios*," Proceedings IEEE International Conference on Communications*, Turkey, June 2006. Vol. 4, pp. 1658-1663.

[25] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," *Proceedings IEEE Symposium. New Frontiers in Dynamic Spectrum Access Networks* (DySPAN'05), Baltimore, USA, November 8 - 11, 2005, pp. 131-136.

[26] X. Zhang, C. Li, "Constructing secure cognitive wireless networks experiences and challenges," *Wireless Communications and Mobile Computing*, vol. 10, October, 2009. pp. 55 - 69.

[27] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," In *Proceedings of the IEEE International Conference on Communications*, Dresden, Germany, June, 2009. pp. 1- 5.

[28] E. Orumwense, O. Oyerinde, S. Meneny, "Impact of primary user emulation attacks on cognitive radio networks," *International Journal on Communications Antenna and Propagation,* Vol. 4, No. 1. April, 2014. pp. 19 – 26.

[29] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," (*Elsevier Journal), on computer Networks*, Vol. 50, no. 13, September 2006. pp. 2127-2159.

[30] T. Clancy, and N. Goergen, **"**Security in Cognitive Radio Networks: Threats and Mitigation," *Third International Conference on Cognitive Radio Oriented Wireless Networks and communications, (*CrownCom). May, 2008. pp. 1 – 8.

[31] Z. Jin, S. Anand, and K. P. Subbalakshmi, **"**Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing" *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 13, Issue 2 April, 2009. pp. 74 – 85.

[32] M. Vu, N. Devroye, and V. Tarokh, "On the Primary Exclusive Region of Cognitive Networks", Proceedings, *IEEE Transactions on Wireless Communications*, Vol. 8, No 7, July, 2009. pp. 3380 – 3385.

[33] L. Fenton, "The sum of log-normal probability distributions in scatter transmission systems", *IRE Transactions on communication Systems, vol. 8,* No 1. , March, 1960. pp. 57-67.

[34] M. Vu, N. Devroye, M. Sharif, and V. Tarokh, "Scaling laws of cognitive networks", Proceedings, *IEEE Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM'2007),* August, 2007. pp. 2–8.

[35] S. Anand, and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," *Proceedings in IEEE Cognitive Radio Oriented Wireless Networks and Communications. (CROWNCOM).* August, 2008. pp. 1 – 5.

[36] S. Anand, Z. Jin, and K. P. Subbalakshmi, **"**An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks", Proceedings, *IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN).* April, 2008. pp. 1 – 6.

[37] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," *Proceedings, IEEE International Performance Computing and Communications Conference (IPCCC'2009),* Arizona, USA. December, 2009, pp. 208–215.

[38] T. S. Rappaport**,** Wireless Communications: *Principle and Practice*. (Prentice Hall Inc., New Jersey, 1996).

[39] E. Taghavi, and M. Abolhassani,"Trustworthy Node detection in Cognitive radio in hostile environment" *International Journal of Information and Electronics Engineering.* Vol 3, No 2, March 2013. pp. 132 -135.

[40] J. Xu, W. Liu, F. Lang, Y. Zhang, and C. Wang, "Distance Measurement model based on RSSI in WSN" *Communications in Wireless sensor Networks.* August, 2010. pp. 606 – 611.

[41] J. Kang, D. Kim, and Y. Kim, "RSS sef-calibration protocol for WSN *localization. In 2nd international symposium on wireless Pervasive Computing ISWPC'07.* San Juan, Puerto- Rico, February 2007.

[42] M. Botta, M. Simek, “Adaptive Distance Estimation Based on RSSI in 802.15.4 network. *International Journal for Radio Engineering,* Vol.22, No. 4. December, 2013. pp. 1162 – 1168.

[43] National Telecommunications and Information Administration, NTIA Special Publication SP-04-409, *Proceedings of the International Symposium on Advanced Radio Technologies March 2-4, 2004*, March, 2004. pp. 101 -105.

[44] Y. Zuo, and B. Panda, “Information trustworthiness evaluation based on trust combination*” in SAC ’06: Proceedings of the 2006 ACM symposium on applied computing,* Dijon, France, April, 2006. pp. 1880-1885.

[45] Y. Liu, P. Ning, H. Dai, “Authenticating Primary Users Signals in Cognitive Radio 1209 networks via integrated cryptographic and wireless link signatures,” *in Proc. Of 1210 IEEE Symposium on Security and Privacy,* 2010, pp. 286–301.

[46] Z. Yuan, D. Niyato, H. Li, and Z. Han, “Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks,” *in IEEE Wireless Communications and Networking Conference (WCNC).* Cancun, Mexico. March, 2011. pp. 599-604.

[47] C. Chen, H. Cheng, Y-D. Yao, “Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack,” *IEEE Transactions on Wireless Communications* Vol. 10 February, 2011. pp. 2135-2141.

[48] N. Armi, N. Saad, Y, Zuki, and M. Arshad, “Cooperative spectrum sensing and signal detection in cognitive radio” *IEEE International Conference on Intelligent and Advanced Systems (ICIAS),* Kuala, Lumpur, Malaysia. June, 2010. Pp 1-5.

[49] S. Kyperountas, N. Correal, and Q. Shi “A Comparison of Fusion Rules for Cooperative Spectrum Sensing in Fading Channels”. *EMS Research, Motorola.* 2009.

[50] I. Akyildiz, B. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: a survey" *Elsevier Journal on Physical Communications,* Vol. 11. June, 2011. pp. 40-62.

[51] S. Kay, "Fundamentals of statistical signal processing: detection theory," Vol. 2, Englewood Cliffs, NJ; Prentice-Hall: 1998. pp595.

[52] F. Digham, M. Alouini, and M. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Transactions on Communications.* Vol. 55, No. 1 January, 2007. pp. 21-24.

[53] I. S. Gradshteyn and I. M. Ryzhik, "Table of integrals, series and products," 6th edition. New York. Academic Press, 2000.

[54] L. C. Wang and A. Chen, "Effects of location awareness on concurrent transmissions for cognitive ad hoc networks overlaying infrastructure based systems," *IEEE Transaction and Mobile Computation,* Vol. 8, No. 5, May, 2009. pp. 577–589.

[55] A. J. Viterbi, *CDMA:* Principles of Spread Spectrum Communication. Reading, MA: Addison-Wesley, 1995.

[56] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks" *IEEE Communications Survey and Tutorials,* Vol 15, No 1. March 2013. pp. 428 – 445.

[57] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks "*Journal of Internet Technology*, Vol 12, No. 2. September, 2011. pp. 181 – 198.

[58] M. Yu, M. Zhou and W. Su, "A secure routing protocol against Byzantine attacks for MANETs in adversarial environments" *IEEE Transactions on Vehicular Technology,* Vol. 58, No. 11, January 2009. pp. 449 – 460.

[59] J.R. Douceur, "The sybil attack", *Proceedings of 1st International Workshop on Peer to Peer Systems (IPTPS),* Massachusetts, USA. March, 2002.

[60] E.L Crow, K. Shimzu, Editor. Log-normal distributions: Theory and Applications. Marcel Dekker, New York, 1998.

[61] S. Chaudhari, "Spectrum sensing for cognitive radio: Algorithms, Performance and Limitations" Ph.D. dissertation, Department of Signal Processing and Acoustics, Aalto University, November, 2012.

[62] B. Acar, M.A Ersoy, H.B Yilmaz, S. Eryigit and T. Tugcu, "Zone-based spectrum sensing in cognitive radio" *IEEE symposium on computers and communications (ISCC),* August, 2012. pp. 696-701.

[63] Y. Liu, C. Zeng, H. Wang and G. Wei, "Energy detection threshold optimization for cooperative spectrum sensing" *IEEE 2nd International Conference on Advanced Computer Control (ICACC).* Shenyang, China. Vol. 4. March, 2010. pp. 566 – 570.

[64] M. Haghighat and S. M. S. Sadough, "Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks, *in proceedings of the 6th International Symposium on Telecommunications (IST'2012),* 6-8 November. 2012. Tehran. pp. 148 – 151.

[65] M. J Saber and S.M.S Sadough, "Optimal energy detection in cognitive radio networks in the presence of malicious users," *in proceedings of the 3rd International Conference on Computer Knowledge Engineering (ICCKE),* October 2013, Mashhad, pp. 173 – 177.

[66] P. Kaligineedi, M. Khabbazian, and V.K Bhargava. "Malicious user detection in a cognitive radio cooperative system." IEEE Transactions on Wireless Communications, Vol. 9, No 8, 2010. pp. 2488 – 2497.

[67] 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. Pp. 772 – 781.

[68] E. Peh, Y-C. Liang, Optimization for cooperative sensing in cognitive radio networks. In: IEEE Wireless Communications and Networking Conference (WCNC). 2007. pp. 27–32.