CHAPTER 1

INTRODUCTION

1.1 Preface

The recent advances in wireless communication have led to the problem of growing spectrum scarcity. The available wireless spectrum has become scarcer due to increasing demand for new wireless application. The large portion of the allocated spectrum is sporadically used leading to underutilization of signification amount of spectrum. To improve the spectrum efficiency, the idea of cognitive radio technology was introduced. This concept of cognitive radio provides a promising solution for the spectrum scarcity issues in wireless networks. Meanwhile, the security issues of cognitive radio have received more attention recently since the inherent properties of CR networks would pose new challenges to wireless communications. This thesis mainly focus on the security problem arising from Primary User Emulation (PUE) attacks in CR networks. The presence of PUE attacks may severely influence the performance of CR network. This thesis aims at presenting a comprehensive introduction to PUE attack, from attacking principle and its impact on CR network, to the detection and analyzing a defense mechanism that use analytical model.

1.2 Problem Statement

In the spectrum sharing mechanism the CR network need to carry out spectrum sensing to identify empty spectrum bands, that is the spectrum " white spaces". Adversaries (attackers) can exploit the vulnerabilities in spectrum sharing mechanism to attack CR network causing a particular security threat to the

incumbent user coexistence which is PUE attack problem . In hostile electromagnetic environment, an intruder secondary users attempts to gain priority over legitimate secondary users by transmitting signals that emulates the characteristics of the primary user's signals.

The potential impact of PUE attack depends on the attacker's signals and primary user's signals while conducting spectrum sensing. PUE attack can produce serious interference to the spectrum sensing and significantly reduces the available channel resources of legitimate secondary users and drastically decrease the bandwidth available to legitimate secondary users and causing bandwidth waste, quality of service (QoS) degradation, connection unreliability, and denial of service (DoS) problems .

1.3 Objectives

The objectives of this thesis have been identified in the following points :

(1) Analyse of security mechanism for CR network using analytical model against PUE attack problem.

(2) Evaluate the performance of the two cases in the model design with comprehensive comparison .

(3) Implement a simulation that determine the performance using Matlab codes.

1.4 Methodology

The methodology that has been followed in this thesis are shown in the following points:

(1) Define the cognitive radio network in details with brief explanation of its architecture, evolution, applications, and security threats .

(2) Description of the security system under investigation with comprehensive analyzing, the study will carry out with two models, and the performance is

characterized by the received signal strength , number of malicious users , and the radius of the area of deployment.

(3) The major aspect during the methodology stages is the simulation process, the main objective of simulation is to find the optimum configuration and performance, this will not only save time but also provide a clear picture. (based on the code results and the illustrated figures).

(4) The conclusion of the above steps will carry out the final results and recommendations.

1.5 Thesis Scope

This section highlight the scope of the thesis, considering the building blocks of the six areas of the communication security – confidentiality, privacy, integrity, authentication , authorization and non-repudiation – this thesis belong to the authentication field. Further, the only radio- based attacks are considered and non-radio attacks – such as attacks on policy databases over Internet – are not considered. This is under the promise that most of the non- radio attacks can be easily handled by incorporation of cryptographic security in high-layers, while this thesis focus on physical layer security in CR networks. Due to the system complexity and multiplicity of configuration in which CRs may employed, the countermeasures of different security threats will not be included.

1.6 Thesis Outline

The thesis organized as follows, in chapter1, the introduction will be introduced. Chapter2 is dedicated to the literature review. Chapter 3 dive into the description of the two security models for the CR networks in details. Chapter 4 will explain the simulation and results for the two analyzed security models. Chapter 5 contains the conclusion and recommendation.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Spectrum sharing has always been an important aspect of system design in wireless communication systems due to the scarcity of the available resources (spectrum). Cognitive radio network [1] enable usage of unused spectrum in a network, A, by users belonging to another network , B. These users thereby become " secondary users" to the network A. The users that originally subscribed to the network A are called " primary users" of network A. One example of cognitive radio network is usage of white spaces (or unused spectrum) in the television (TV) band . The TV transmitter then becomes a primary transmitter and TV receivers are primary receivers. Other users who are not TV subscribers but wish to use the white spaces in the TV band for their own communications become secondary transmitters/receivers. The IEEE 802.22 working group on wireless regional area networks (WRAN) [2] provide the physical layer (PHY) and medium access control (MAC) specification for usage of the TV white spaces. More details on the IEEE 802.22 can be found in [3] , [4].

The etiquette followed in cognitive radios is that the secondary users evacuate the used spectrum once they detect a primary transmission. The etiquette of spectrum evacuation could however result in denial-of-service attacks on secondary users if the system is not carefully designed.

A subset of users could forge the essential signal characteristics of the primary and generate enough power at the good secondary user locations to confuse the secondaries into thinking that a primary transmission is under way.

Such an attack by malicious users on secondary users is called a primary user emulation attack (PUE attack).

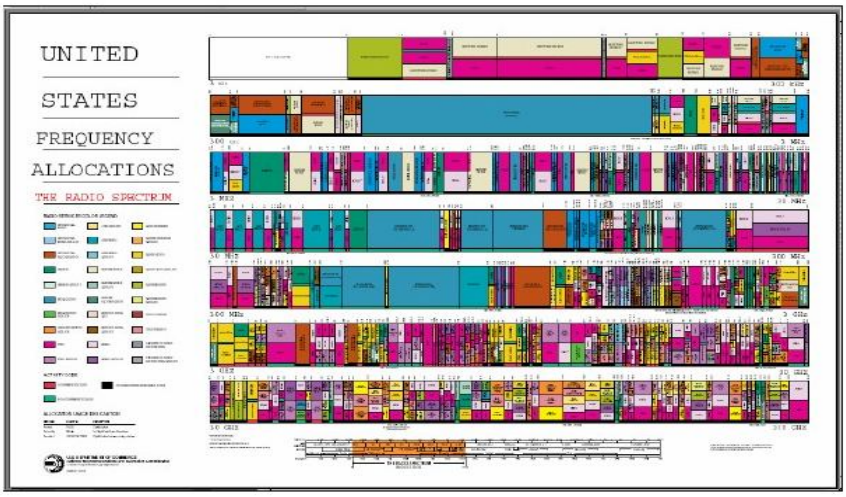


Figure 2.1 Radio Frequency Allocation in US [2]

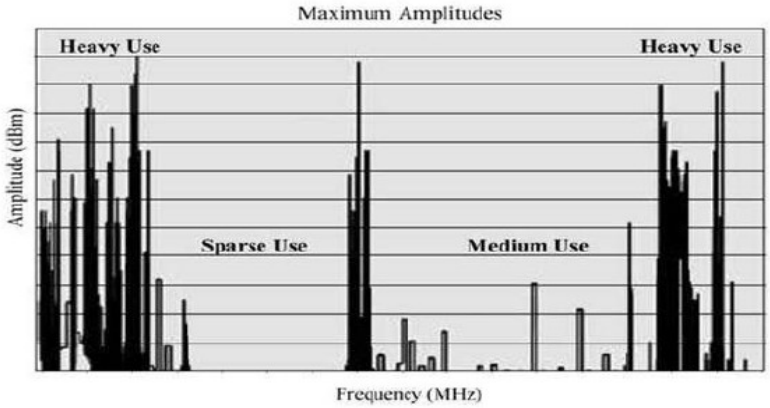


Figure 2.2 Spectrum Utilization [9]

2.2 Cognitive Radio Technology

Cognitive Radio, built on a software radio platform, is a context – aware intelligent radio potentially capable of autonomous reconfiguration by learning from and adapting to the communication environment. Since a CR is a radio that can change its transmitter parameters based on the interaction with its environment, CR should fulfill two main requirements: cognitive capability and reconfigurability .The cognitive capability identifies the spectrum portions that are

available in a specific moment. These available spectrum portions are called spectrum holes or white spaces. In a CR network, it should also be possible to transmit and receive through different frequency values using different access technologies. That way the parameters of a CR can be modified to adapt to the environment and use the best frequency band. This ability is called reconfigurability.

2.2.1 Cognitive Radio Evolution

Cognitive radio technology is the key technology that enables an xG network to use spectrum in a dynamic manner. The term, cognitive radio, can formally be defined as follows:

A ”Cognitive Radio” is a radio that can change its transmitter parameters based on interaction with the environment in which it operates. From this definition, two main characteristics of the cognitive radio can be defined:

- Cognitive Capability Cognitive capability refers to the ability of the radio technology to capture or sense the information from its radio environment. This capability cannot simply be realized by monitoring the power in some frequency band of interest but more sophisticated techniques are required in order to capture the temporal and spatial variations in the radio environment and avoid interference to other users. Through this capability, the portions of the spectrum that are unused at a specific time or location can be identified. Consequently, the best spectrum and appropriate operating parameters can be selected.
- Reconfigurability The cognitive capabilities provide spectrum awareness whereas Reconfigurability enables the radio to be dynamically programmed according to the radio environment. More specifically, the cognitive radio can be programmed to transmit and receive on variety of frequencies and to use different transmission access technologies supported by its hardware design [7].

2.2.2 The XG Network (CR Network) Architecture

Existing wireless network architectures employ heterogeneity in terms of both spectrum policies and communication technologies [1] . Moreover, some portion of the wireless spectrum is already licensed to different purposes while some bands remain unlicensed. For the development of communication protocols, a clear description of the xG network architecture is essential. In this section, the xG network architecture is presented such that all possible scenarios are considered.

The components of the xG network architecture, as shown in Figure .2.3, can be classified in two groups as the primary network and the xG network. The basic elements of the primary and the xG network are defined as follows:

- Primary Network An existing network infrastructure is generally referred to as the primary network, which has an exclusive right to a certain spectrum band. Examples include the common cellular and TV broadcast networks. The components of the primary network are as follows:
    1) Primary user Primary user (or licensed user) has a license to operate in a certain spectrum band. This access can only be controlled by the primary base-station and should not be affected by the operations of any other unlicensed users. Primary users do not need any modification or additional functions for coexistence with xG base-stations and xG users.
    2) Primary base-station: Primary base-station (or licensed base-station) is a fixed infrastructure network component which has a spectrum license such as base-station transceiver system (BTS) in a cellular system. In principle, the primary base-station does not have any xG capability for sharing spectrum with xG users. However, the primary base-station may be requested to have bothlegacy and xG protocols for the primary network access of xG users, which is explained below.

- xG Network xG network (or cognitive radio network, Dynamic Spectrum Access network, secondary network, unlicensed network) does not have license to operate in a desired band. Hence, the spectrum access is allowed only in an opportunistic manner. xG networks can be deployed both as an infrastructure network and an ad hoc network as shown in Figure. 2.1 The components of an xG network are as follows:
    1) xG user xG user (or unlicensed user, cognitive radio user, secondary user) has no spectrum license. Hence, additional functionalities are required to share the licensed spectrum band.
    2) xG base-station xG base-station (or unlicensed base-station, secondary base-station) is a fixed infrastructure component with xG capabilities. xG base-station provides single hop connection to xG users without spectrum access license. Through this connection, an xG user can access other networks.
- Spectrum Broker Spectrum broker (or scheduling server) is a central network entity that plays a role in sharing the spectrum resources among different xG networks. Spectrum broker can be connected to each network and can serve as a spectrum information manager to enable coexistence of multiple xG networks [8, 9, 10] . Thus, in xG networks, there are three different access types as explained next:
    1) xG network access xG users can access their own xG base-station both on licensed and unlicensed spectrum bands.
    2) xG ad hoc access xG users can communicate with other xG users through ad hoc connection on both licensed and unlicensed spectrum bands [13].
    3) Primary network access: The xG users can also access the primary base-station through the licensed band.

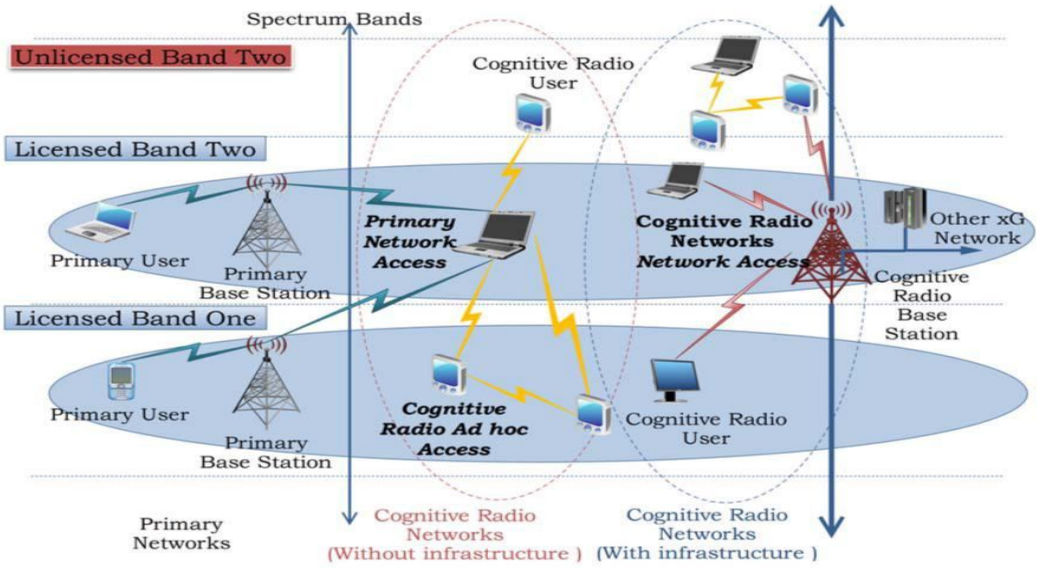


Figure 2.3 Architecture for CR Network

2.2.3 Dynamic Spectrum Access

Today's wireless networks are regulated by a fixed spectrum assignment policy, i.e. the spectrum is regulated by governmental agencies and is assigned to license holders or services on a long term basis for large geographical regions. Although the fixed spectrum assignment policy has generally worked well in the past, there is a dramatic increase in the access to the limited spectrum for mobile services in recent years. Consequently, this increase is straining the effectiveness of the traditional spectrum policies .

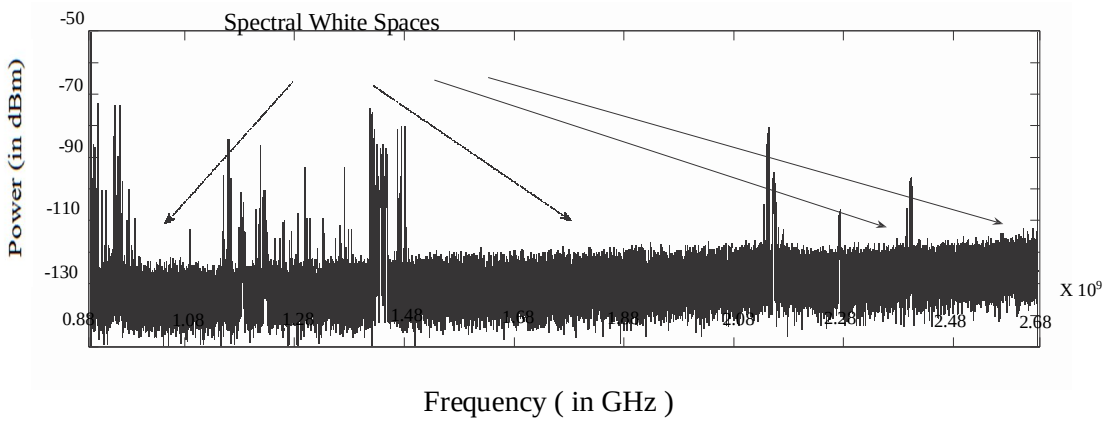


Figure 2.4 A power spectral density snapshot of wireless spectrum ranging from 88 MHz to 2686 MHz measured on July 11, 2008, in Worcester, MA,USA at coordinates 42°16′8″N, 71°48′14″W [5]

It is commonly believed that there is a crisis of spectrum availability at frequencies that can be economically used for wireless communications. This misconception is strengthened by a look at the FCC frequency chart [10], which shows multiple allocations over all of the frequency bands; which is a situation essentially also true worldwide. This has resulted in fierce competition for use of spectra, especially in the bands below 3 GHz. On the other hand, a large portion of the assigned spectrum is used sporadically as illustrated in Figure 2.4, where the signal strength distribution over a large portion of the wireless spectrum is shown. The spectrum usage is concentrated on certain portions of the spectrum while a significant amount of the spectrum remains unutilized. This appears to be a contradiction to the concern of spectrum shortage since in fact we have an abundant amount of spectrum, and the spectrum shortage is partially an artifact of the regulatory and licensing process.

It is this discrepancy between FCC allocations and actual usage, which indicates that a new approach to spectrum licensing is needed. This approach should provide the incentives and efficiency of unlicensed usage to other spectral bands, while accommodating the present users who have higher priority or legacy rights (primary users) and enabling future systems a more flexible spectrum access [13]. This new approach is called dynamic spectrum access.

Dynamic spectrum access is the process of increasing spectrum efficiency via the real time adjustment of radio resources, i.e. via a process of local spectrum sensing, probing, and the autonomous establishment of local wireless connections among cognitive nodes and networks. Cognitive radio envisioned real time spectrum auctions among diverse constituencies, using for one purpose, such as cellular radio, spectrum allocated and in use for another purpose such as public safety, and conversely, in order to multiply

both the number of radio access points for public safety and to more efficiency use public safety spectrum commercially during peak periods.

2.2.4 Dynamic Spectrum Access Models

Standing for the opposite of the current static spectrum management policy, the term dynamic spectrum access has broad connotations that encompass various approaches to spectrum reform .Dynamic spectrum access strategies can be broadly categorized under three models [6]:

- Dynamic Exclusive Use Model This model maintains the basic structure of the current spectrum regulation policy: Spectrum bands are licensed to services for exclusive use. The main idea is to introduce flexibility to improve spectrum efficiency.Two approaches have been proposed under this model: Spectrum property rights and dynamic spectrum allocation. The former approach allows licensees to sell and trade spectrum and to freely choose technology. Economy and market will thus play a more important role in driving toward the most profitable use of this limited resource. Note that even though licensees have the right to lease or share the spectrum for profit, such sharing is not mandated by the regulation policy. The second approach, dynamic spectrum allocation aims to improve spectrum efficiency through dynamic spectrum assignment by exploiting the spatial and temporal traffic statistics of different services. In other words, in a given region and at a given time, spectrum is allocated to services for exclusive use This allocation, however, varies at a much faster scale than the current policy. Based on an exclusive use model, these approaches cannot eliminate white space in spectrum resulting from the bursty nature of wireless traffic.

- Open Sharing Model Also referred to as spectrum commons, this model employs open sharing among peer users as the basis for managing a spectral region. Advocates of this model draw support from the phenomenal success of wireless services operating in the unlicensed industrial, scientific, and medical radio band (e.g., WiFi). Centralized and distributed spectrum sharing strategies have been initially investigated to address technological challenges under this spectrum management model.
- Hierarchical Access Model This model adopts a hierarchical access structure with primary and secondary users. The basic idea is to open licensed spectrum to secondary users while limiting the interference perceived by primary users (licensees). Two approaches to spectrum sharing between primary and secondary users have been considered: Spectrum underlay and spectrum overlay. The underlay approach imposes severe constraints on the transmission power of secondary users so that they operate below the noise floor of primary users. By spreading transmitted signals over a wide frequency band, secondary users can potentially achieve short-range high data rate with extremely low transmission power. Based on a worst-case assumption that primary users transmit all the time, this approach does not rely on detection and exploitation of spectrum white space. Spectrum overlay investigated by the Next Generation (XG) program under the term opportunistic spectrum access. Differing from spectrum underlay, this approach does not necessarily impose severe restrictions on the transmission power of secondary users, but rather on when and where they may transmit. It directly targets at spatial and temporal spectrum white space by allowing secondary users to identify and exploit local and instantaneous spectrum availability in a non intrusive manner. Compared to the dynamic exclusive use and open

sharing models, this hierarchical model is perhaps the most compatible with the current spectrum management policies and legacy wireless systems. Furthermore, the underlay and overlay approaches can be employed simultaneously to further improve spectrum efficiency.

2.2.5 Spectrum Sensing

An important requirement of the xG network is to sense the spectrum holes. As explained in Previous Section, a cognitive radio is designed to be aware of and sensitive to the changes in its surrounding. The spectrum sensing function enables the cognitive radio to adapt to its environment by detecting spectrum holes [18].

The most efficient way to detect spectrum holes is to detect the primary users that are receiving data within the communication range of an xG user. In reality, however, it is difficult for a cognitive radio to have a direct measurement of a channel between a primary receiver and a transmitter. Thus, the most recent work focuses on primary transmitter detection based on local observations of xG users.

- Spectrum Sensing Challenges There exist several open research challenges that need to be investigated for the development of the spectrum sensing function.

1) Interference temperature measurement.
2) Spectrum sensing in multi-user networks.
3) Detection capability.

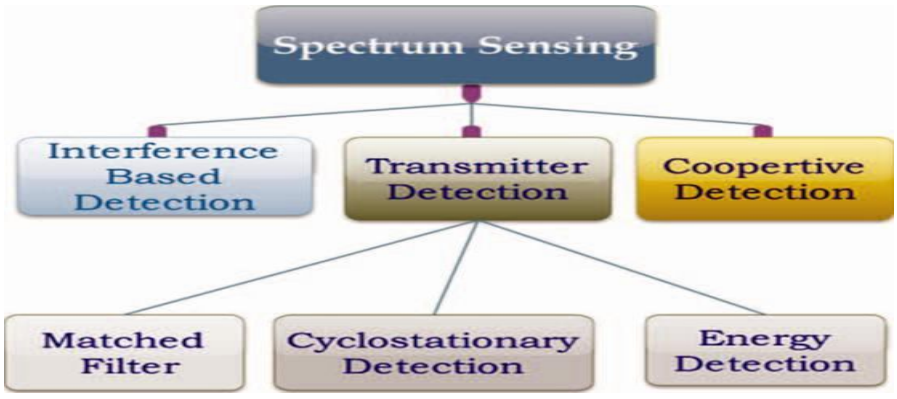


Figure 2.5 Classification of Spectrum Sensing Techniques

2.2.6 Spectrum Management

In xG networks, the unused spectrum bands will be spread over wide frequency range including both unlicensed and licensed bands. These unused spectrum bands detected through spectrum sensing show different characteristics according to not only the time varying radio environment but also the spectrum band information such as the operating frequency and the bandwidth [15].

Since xG networks should decide on the best spectrum band to meet the QoS requirements over all available spectrum bands, new spectrum management functions are required for xG networks, considering the dynamic spectrum characteristics.

These functions classified as spectrum sensing, spectrum analysis, and spectrum decision. While spectrum sensing, which is primarily a PHY layer issue, spectrum analysis and spectrum decision are closely related to the upper layers. In this section, spectrum analysis and spectrum decision are investigated.

- Spectrum Analysis It is essential to define parameters such as interference level, channel error rate, path-loss, link layer delay, and holding time that can represent the quality of a particular spectrum band.
- Spectrum Decision Once all available spectrum bands are characterized, appropriate operating spectrum band should be selected for the current transmission considering the QoS requirements and the spectrum characteristics. Thus, the spectrum management function must be aware of user QoS requirements.
- Spectrum Management Challenges There exist several open research issues that need to be investigated for the development of spectrum decision function.Some of the challenges are :

  1) Decision model.

  2) Multiple spectrum band decision.

3) Cooperation with reconfiguration.

4) Spectrum decision over heterogeneous spectrum bands.

2.2.7 Spectrum Mobility

xG networks target to use the spectrum in a dynamic manner by allowing the radio terminals, known as the cognitive radio, to operate in the best available frequency band. This enables ”Get the Best Available Channel” concept for communication purposes. To realize the ”Get the Best Available Channel” concept, an xG radio has to capture the best available spectrum. Spectrum mobility is defined as the process when an xG user changes its frequency of operation. The following sections describe the spectrum handoff concept in xG networks and discuss open research issues in this new area [16]. Some of the challenges of Spectrum mobility are :

1) Spectrum handoff.

2) Spectrum mobility in multiple users

2.2.8 Spectrum Sharing

In order to provide a directory for different challenges during spectrum sharing, we first enumerate the steps in spectrum sharing in xG networks. The challenges and the solutions proposed for these steps will then be explained in detail. The spectrum sharing process consists of five major steps:

1) Spectrum sensing

2) Spectrum allocation:

3) Spectrum access

4) Transmitter-receiver handshake

5) Spectrum mobility

- Overview of Spectrum Sharing Techniques The existing solutions for spectrum sharing in xG networks can be mainly classified in three aspects: i.e., according to their architecture assumption, spectrum allocation behavior, and spectrum

access technique as shown in Figure 2 .6. In this section, we describe these three classifications and present the fundamental results that analyze these classifications [11]. The analysis of xG spectrum sharing techniques has been investigated through two major theoretical approaches. While some work uses optimization techniques to find the optimal strategies for spectrum sharing, game theoretical analysis has also been used in this area. The first classification for spectrum sharing techniques in xG networks is based on the architecture, which can be described as follows:

1) Centralized spectrum sharing
2) Distributed spectrum sharing
3) Cooperative spectrum sharing
4) Non-cooperative spectrum sharing
5) Overlay spectrum sharing
6) Underlay spectrum sharing

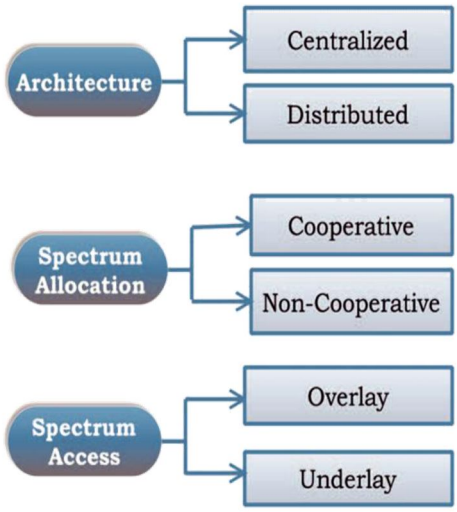


Figure 2.6 Classification of spectrum sharing in xG networks based on architecture, spectrum allocation behavior, and spectrum access technique

or any combination of above types (Figure 2.7)

1) Centralized inter-network spectrum sharing
2) Distributed inter-network spectrum sharing
3) Intra-network spectrum sharing
4) Cooperative intra-network spectrum sharing
5) Non-cooperative intra-network spectrum sharing

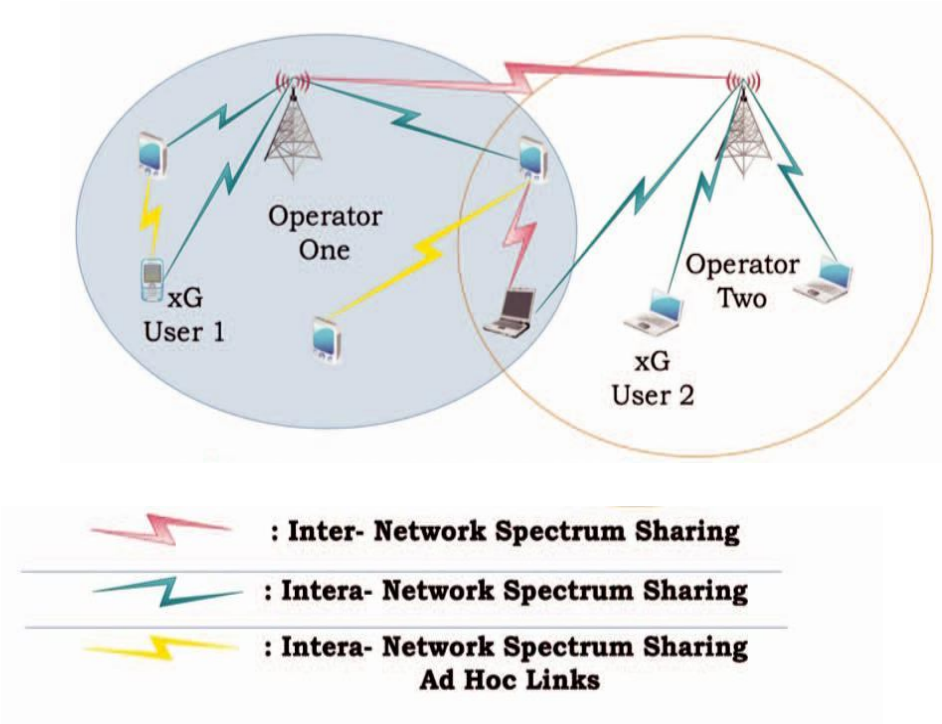


Figure 2. 7 Inter-network Spectrum Sharing

- Spectrum Sharing Challenges Some of the spectrum sharing challenges are:
  1) Common control channel (CCC).
  2) Dynamic radio range.
  3) Spectrum unit.

2.3 TV White Space

The spectrum holes localized within the TV spectrum are known as TVASs. TV broadcast band have special interest since new approaches for TV-band spectrum holes for enabling wide-area Internet services are being considered . In fact, FCC in the US has approved the dynamic access of unlicensed users in TVWSs and the Institute of Electrical and Electronics Engineers (IEEE) is developing the 802.22 and 802.11 standards.

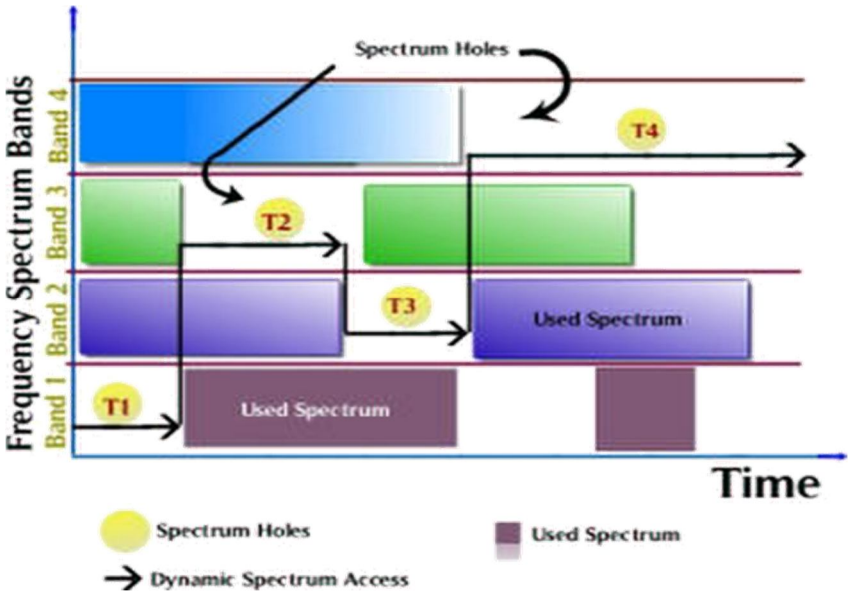


Figure 2. 8 White Spaces in the Spectrum

2.4 Security Issues in Cognitive Radio

Attack always accompany with the security system , since security and attack interacts with each other . The main objective of the security system is to protect the communication from the malicious users. The cognitive radio network has the same security requirements as that of the general wireless media [3].

The major difference between the cognitive radio network and the traditional wireless network is that it doesn't operate on a fixed frequency spectrum (i.e. the

frequency spectrum is being used dynamically). While implementing security scheme in CR network various factors need to be taken into consideration because CR deals with the use of unused spectrum in an opportunistic manner with the unscheduled appearance of the primary users.

However, as with many new technologies, initial research has not focused on security aspects of cognitive radio. Typically security is always bolted on after the fact by adding some sort of link authentication and encryption. This typically works well for data traversing a wireless network, but not necessarily for things fundamental to the operation of the wireless link itself [13].

2.4.1 Artificial Intelligence Behavior Threats

- Policy Threats In order to communicate more effectively in an intelligence way, a CR needs policies for reasoning different environment or from different conditions. Policy threats come from two aspects: lack of policy and failure when using policy.
- Learning Threats Some CRs are designed with the capability of learning. These CRs can learn from the past experiences or current situ-ations to predict future environment and select optimal operations, and they are vulnerable be-cause of the learning capability.
- Parameters Threats A CR control a large number of radio parameters. Both in policies and learning process, CR use parameters to control operations and estimate its performance. The functionalities of these parameters are variety. For example, some of these parameters are used to weigh and estimate the performance of CR; some of them are the conditions or the switching bases of policies. Altering these parameters can cause sub-optimal or wrong operations for a CR.

2.4.2 Dynamic Spectrum Access (DSA) Threats

- Spectrum Sensing Threats In DSA environment, primary users have the license to use the certain frequency band whenever they want. When the primary uses do not use their spectrum, the spectrum is idle, and secondary users could use the available spectrum opportunistically. Such secondary users need sensing algorithms to detect spectrum holes for communication, and CRs have the capability of detecting the spectrum holes. In addition, a CR has to vacate the channel when the primary user uses it.
- Spectrum Management Threats The threats here come from the possibility of false or fake spectrum characteristic parameters. The false or fake parameters impact the results of spectrum analysis, and then impact the results of spectrum decision. So a CR may select the wrong band or the sub-optimal band, and the performance of communication may be impaired. For example, in spectrum analysis, spectrum characterization is focused on the capacity estimation recently.
- Spectrum Mobility Threats During spectrum handoff, the security threats are seriously. Because a failed handoff may need a long time to resume the communication. An attacker can induce a failed spectrum handoff through ways of: compelling the CR vacating the current band by masking primary user; jamming to slower the process of selecting for a new available band or to cause a communication failure. Comparing the centralized and distributed architectures and the cooperation and non-cooperation connecting approaches, obviously, the centralized architecture and cooperation approach are more vulnerable to at-tacks. The most severe attack to these two solutions is Denial of Service (DoS) attack. In centralized architecture network, if an attacker can manipulate the central entity or prevent the central entity from communication,

the whole network is under control of the attacker. In cooperation CRN, if an attacker controls one of the nodes, he can transmit fake information to other nodes, or terminate transmitting information to others. This kind of attack is valid the most in ad hoc network. Especially, common control channel is a target for DoS attacks since successful jamming of this one channel may prevent or hinder all communication [13].

2.4.3 Inherent Reliability Issues

- High Sensitivity to Primary User Signal The secondary users should identify the primary transmission in order to prevent interference to the primary users. One of the stringent requirements for cognitive network is to predict the temperature interference on nearby primary receiver and keep it below a threshold. As a result of this the sensitivity towards the primary user signal is usually set to high. In case of energy based detection this high sensitivity increases false detection.
- Unknown Primary Receiver Location The secondary user must know where exactly the primary receiver is located, so that the interference to primary user is minimized. Unknown primary receiver location may lead to hidden node problem. By exploiting the receiver power leakage, the location of primary receiver can be identified.

2.5 Security at Different Layer

In this section we will briefly describe the attacks associated with the five layers in the protocol stack.

2.5.1 Physical Layer

Physical layer is the lowest layer and it provides an interface to the transmission medium. CR network doesn't operate on a fixed frequency that is

signals can be transmitted and received of various frequencies across wide frequency spectrum band. The spectrum is used dynamically. Thus, this makes the operation of physical layer in CR more complicated. Spectrum sensing is a key part in CR, since it deals with identifying vacant bans or spectrum holes. Following are the possible attacks associated with physical layer:

- Intentional Jamming Attack The malicious secondary user intentionally transmits signals in a licensed band and jams primary and other secondary users . The problem would be worse when the malicious mobile node launches attack in one geographical area and moves to another area before being identified .
- Primary Receiver Jamming Attack Since the secondary user dose not know the location of the primary receiver, the attacker can take advantage of this to launch a primary receiver jamming attack. For an example , the attacker may move closer to the primary receiver and request transmission from the secondary users towards it , this will in turn cause interference to the primary receiver [3].
- Overlapping Secondary User Attacks In CR network multiple secondary network may exist at the same time over the sane region. The transmissions from malicious entities in one network can cause interference to the primary and secondary users of the other network.

2.5.2 Link Layer

Link layer sits just above physical layer in the protocol layer stack. This layer is responsible for transfer of data from one to other in single hop. It ensure that initial connection has been set up, divides output data frames, and handles the acknowledgements from a receiver that the data arrived successfully. The MAC layer which controls channel assignment, is one of the important sub layers of the link layer.

One of the important parameters to decide the fainess of a channel allocation to decide the fainess of a channel allocation scheme in traditional wireless environments is SNR . On the contrary, in CR network various parameters such as holding time, delay, path loss, interference and link error rate are as important as the SNR. Hence channel assignment is a more complex operation CR network [2] [3].

- Biased Utility Attack A malicious secondary node may try to change the parameters of utility function in order to increase its own bandwidth . As a result of this the good secondary user is deprived of available bandwidth.
- False Feedback Attack In a decentralized CR network , secondary user may make wrong decision due to false feedback from one malicious secondary user, this in turn will cause severe interference to the licensed user. For an example, a malicious node in the network may not tell other secondary users in the network about the reappearance of the licensed user .

2.5.3 Network Layer

The main objective of network layer is end-to-end packet delivery. Functions of the network layer are routing, flow control, ensure quality of service (QoS). Every node maintains routing information about its neighboring nodes in the network . Before establishing connection, every node identifies which of its neighbors should be the next link in the path towards the destination. An attacker in the path can drastically alter routing by either redirecting the packets in the wrong direction or by broadcasting incorrect routing information to its neighbors. Following are the possible attacks associated with the network layer.

- Hole Attack In the hole attack the node which pretends is called a hole .There are various types of hole attacks such as Black hole attack , Gray hole attack and Worm hole attack Black hole attack is defined as attack in which the malicious

node attracts (request) pockets from every other node and drops all the packets .The gray hole attack is defined as the attack in which the malicious node selectively drops the packets . The worm hold attack is defined as the attack in which the malicious user two pairs of nodes the two pairs. The worm hold attack is considered as the dangerous attack amongst all. It can prevent route discovery where the source and the destination are more than two hops away.

- Ripple Effect Attack The main objective of the malicious node is to provide wrong channel information so that the other nodes change their channel. This false information will transmit on hop by hop basis and in turn the entire network will come to a confusing state, this can disrupt the traffic for long time.

2.5.4 Transport Layer

The transport layer is responsible for transfer of data between two end hosts. It is responsible for control, congestion control and end-to-end error recovery. Some attacks occur during session setup, while others happen during the period of sessions.

- Key Depletion Attack Sessions in CR networks last only for a short period at time due to frequently occurring retransmissions. Therefore, large numbers of sessions are being initiated. Security protocols at the transport layer like SSL and TLS establish cryptographic keys at the beginning of every transport layer session. Since numbers of sessions in CR networks are large, large numbers of keys are establishes, there by increasing the probability of using the same key twice. Key repetitions can be exploited to break the underlying cipher system.

2.5.5 Application Layer

It is the top most layer of the protocol stack. It provides application services to the end users. Protocols that run at the application layer completely rely on the services provided by the underlying lower layer. As a result any attack on physical,

link, network or transport layers may have an adverse affect on the application layer [2] [3].

2.6 Primary User Emulation (PUE) Attack

PUE attacks are known as a new type of attacks unique to CR networks. In such an attack, the hostile user (attacker) takes the advantage of the inherent etiquette in CR networks that the legitimate SU has to evacuate the spectrum band upon the arrival of a PU. An attacker emulates the PU,s transmitting signal and the spectrum band .

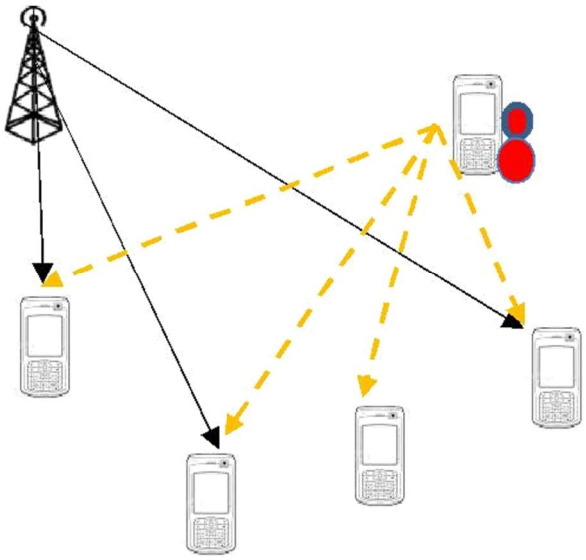


Figure 2.9 PUE Attack

From a security perspective, the PUE attack can be viewed as an authentication problem. However, the traditional authentication mechanisms based upon the cryptographic signatures cannot be directly applied since the FCC states very clear that “ no modification to the primary system should be required “ . Therefore, other schemes of authentication must be designed to defend against such attacks.

2.6.1 Classification of PUE Attackers

Since the security problem caused by PUE attacks was identified, different type of PUE attacks have been studied, such as:

- Selfish Attacker A selfish attacker aims at stealing bandwidth from legitimate SUs for its awn transmission. The attacker will monitor the spectrum. One an unoccupied spectrum band is discovered, it will compete with the legitimate SUs by emulating the primary signal. The purpose of a malicious attacker, however, is to disturb the dynamic spectrum access of legitimate SUs but not to exploit the spectrum for its own transmission.
- Malicious Attacker Malicious attacker may emulate a primary signal in both an unoccupied spectrum band and a band currently used by legitimate SUs. When an attacker attacks a band being used by a legitimate SU, there exists the possibility that the SU fails to discover the signal, and hence, an interference occurs between the attacker and the legitimate SU.

2.6.2 Essential Conditions for Successful PUE Attacks

In a CR networks, the successful realization of a PUE attack relies on several essential conditions, we summarize these essential conditions as follows:

No PU- SU Interaction: If the legitimate SUs are allowed to exchange information with the PUs, a PU verification procedure could be designed to easily detect a PUE attack.

- PU and SU Interaction If the legitimate SUs are allowed to exchange information with the PUs, a PU verification procedure could be designed to easily detect a PUE attack.
- PU and SU Signals Have Different Characteristics An SU receiver is designed only for the secondary signal but unable to demodulate and decode the primary

signal. The PUE attackers take advantage of this fundamental condition to emulate the primary signal that is unrecognizable for the legitimate SUs.

2.6.3 Impact of PUE Attacks on CR Network

The presence of PUE attacks cause a number of troubles problems for CR networks, such as:

- Bandwidth Waste PUE attackers may steal the spectrum " hole" from the SUs, leading to spectrum bandwidth waste.
- QoS Degradation The appearance of PUE attack may severely degrade the Quality-of- service (QoS) of the CR network by destroying the continuity of secondary services. Frequent spectrum handoff will induce unsatisfying delay and jitter for the secondary services.
- Communication Unreliability If a real time secondary service is attacked by a PUE attacker and finds no available channel when performing spectrum handoff, the service has to be dropped.
- Denial of Service Consider PUE attacks with high attacking frequency, then the attackers may occupy many of the spectrum opportunities. The SUs will have insufficient bandwidth for their transmissions, and hence, some of the SU services will be interrupted. In the worst case, the CR network may even find no channels to set up a common control channel for delivering the control messages. As a consequence, the CR network will be suspended and unable to serve any SU.

2.6.4 Detection Approaches for PUE Attacks

The existing detection approaches can be classified into energy detection, Received Signal Strength (RSS) based detection, feature detection, location verification and cooperative detection :

- Energy Detection Energy detection is a simple but widely used approach for spectrum sensing in CR networks. It is also one of the basic approaches for the detection of PUE attacks. By measuring the power level of the received signal at the SU receiver and comparing it with that from the true PUs, the CR network could judge whether the signal comes from an attacker or not. However, a pure energy detector is not robust enough to tackle an advanced PUE attack.
- RSS-based Detection Received Signal Strength (RSS) based detection approach does not need dedicated sensor networks. The PUE attackers are assumed to be distributed randomly around the SUs.
- Feature Detection The approach proposed in [9] uses energy detection to identify the existing users in the frequency band. The approach then employs a cyclostationary calculation to represent the features of the user signals, which are then fed into an artificial neural network for classification. As opposed to current techniques for detecting PUE attacks in CR networks, this approach does not require additional hardware or time synchronization algorithms in the wireless network.
- Location Verification Two location verification schemes are proposed in [2]. They are called Distance Ratio Test (DRT) and Distance Difference Test (DDT), respectively. In both schemes, dedicated cognitive nodes (SUs or a cognitive BS) with enhanced functionality are involved for location verification. DRT uses a Received Signal Strength (RSS) based method, where two dedicated cognitive nodes measure the RSS of the signal source and calculate the ratio of these two RSS to check whether it coincides with their distances to the true PU (e.g., a TV broadcast tower). Using DDT, the arrival time of the transmitted signal from the source is measured by the two dedicated cognitive

nodes. The product of the time difference and the light speed is then compared to the distance difference from the true PU to the two dedicated nodes in order to identify the source.

2.6.5 Defense Approaches Against PUE Attacks

The defense against PUE attacks is an important but seldom explored topic in CR networks. There are practical requirements for efficient PUE attack defense approaches. We illustrate this by two examples below. First, although a variety of PUE attack detection approaches have been proposed, none of the existing approaches is able to promise accurate detection of all attacks. There still is a chance that some attacks are not detected. This necessitates system level mechanisms to maintain the overall performance of a CR network under undetected PUE attacks. Second, when there are malicious attackers in the network, their purpose is to interrupt the communications of the cognitive users. Even if they have been discovered, malicious attackers may still transmit in order to interfere with the transmissions of the SUs. In this case, the signal processing units in the RF front-ends of the SU receivers should be applied to get rid of the interference signals, in order to try to recover the secondary signal.

2.6.6 Defense Approaches at Various Protocol Layers

To defend against PUE attacks, effective counter measures could be taken at different layers of the communications protocol stack:

- Physical-layer Approach Physical-layer techniques such as source separation, signal design, spread spectrum and directional antennas could be employed to deal with the intended interference from malicious PUE attackers. The key in the design of an efficient physical-layer counter- measure is to exploit the a priori knowledge about the characteristics of the primary signal and its dissimilarity with the interference signal.

- MAC-layer Approach Undetected PUE attacks will steal bandwidth from the CR network. To let the SUs maintain moderate QoS performance, Radio Resource Management (RRM) strategies such as admission control, spectrum handoff and spectrum scheduling should be studied.
- Network-layer Approach In cognitive ad hoc networks, once the location of the PUE attackers are estimated, a position-based cognitive routing strategy could be employed to deal with the PUE attacks. Those SUs that are located within the attacking range of the PUE attackers should be considered to be temporary unavailable. End- to-end routing paths should be established without crossing the unavailable SU nodes.
- Cross-layer Approach A cross-layer design framework may be set up to defend against PUE attacks. In the framework, the behavior of the detected PUE attacks is observed at the physical layer and reported to the upper layers, such as the RRM mechanism at the MAC layer or the routing mechanism at the network layer. We emphasize that, even the undetected PUE attacks could be estimated in the physical layer by considering the theoretically derived detection probability. The control parameters of the upper layer are jointly optimized considering the existence of PUE attacks.

2.7 Related Works

2.7.1 Related Works on Identification of Cognitive Radio Network Threats

This section presents a detailed discussion on the some of the existing works in the literature identifying various types of attacks on CR networks and the mechanisms of launching these attacks.

- Jamming Attack Sampath et al. present various ways in which jamming attacks can be launched on single channel and multi-channel 802.11 standard-compliant networks (Sampath et al., 2007). In the single channel jamming attack, the attacker continuously transmits high-power signals in the channel and causes interference to the communications from legitimate users in the network. In order to minimize energy consumption and to make the detection of the attack difficult, the attacker can also take a periodic jamming strategy in which the attacker transmits jamming packets at periodic intervals of time. In this strategy, the impact of jamming depends on the length of inter-jamming interval, the size of the jamming packets, and the size of the data packets sent to the victim node. It has been found that the impact of jamming degrades gracefully with the increase in inter-jamming interval, while the use of large packet size at the victim node increases the impact of jamming. In multi-channel jamming attacks, the attacker manipulates the CR to switch frequently across different channels and jam multiple channels simultaneously. Since, in addition to fast channel switching, the nodes in a CR have advanced channel sensing capabilities, the attacker can use a CR node to build up channel usage patterns of network users, and switch only among the channels are currently under use. These types of highly intelligent and efficient attacks are very difficult to detect in CR networks. Burbank et al. present a detailed description on how various types of jamming attacks can be targeted in a CR network and how adverse these attacks can be on the overall network performance (Burbank et al., 2008). Sethi and Brown discuss various ways in which DoS attacks can be launched on CR networks and present a framework to analyze those attacks (Sethi & Brown, 2008). The framework, known as the “Hammer Model Framework”, graphically presents the potential risks

sequences for DoS attacks, and investigates various types of vulnerabilities that may prevent CR communication is specific spectrum bands or completely deny a CR network to communicate or induce it to cause harmful interference to its existing legitimate users. In addition to jamming attacks, the authors have also considered attacks related to malicious alterations of cognitive messages and masquerading of a CR node by a malicious adversary. Zhang et al. propose a classification of various attacks on a CR network which can adversely affect its learning capability and its ability to gainfully utilize the benefits of dynamic spectrum access (Zhang et al., 2008). Arkoulis et al. have identified, analyzed and explained the security weaknesses and vulnerabilities of cooperative, dynamic and open spectrum access environments that can be targeted by a malicious adversary to disrupt the network operations or degrade its performance (Arkoulis et al., 2008). The authors have followed an approach for identifying threats based on the types of anomalous behavior of the nodes such as: misbehavior, selfishness, cheating, and malicious intention. Burbank presents some major security threats in CR networks in general, and identifies various challenges in defending against these threats (Burbank, 2008). In order to identify specific security challenges in CR networks the author has first pointed out two fundamental differences between a traditional wireless network and a CR network. In the CR networks the attacker has: (i) the potential far reach and long-lasting nature of an attack, and (ii) the ability to have a profound effect on network performance and behavior through simple spectral manipulation by generating false signals. In a CR network, the nodes exchange locally-collected information to construct a perceived environment that that determines the current and future behavior of the nodes. The author argues that in a CR network, a malicious adversary can propagate its behavior

through the network in the same way a malicious worm propagates in a network. The adversary can carry out spectral manipulation for influencing the behavior of a set of local CRs or a distant CR as well. The author has also identified various features of CR networks and the implications of these features on potential attacks on these networks. Brown and Sethi present a multidimensional analysis and assessment of various DoS attacks on all types of CR networks (Brown & Sethi, 2007). The authors have carried out vulnerability analysis of CR network against various DoS attacks using different parameters such as network architecture employed, the spectrum access technique used, and the spectrum awareness model. The attacks are categorized into two types: denial attacks and induce attacks. While the denial attacks are intended to prevent communications in the network, the induce class of vulnerabilities stimulate the CR node to communicate causing interference with a licensed transmitter. The adverse impact of these attacks is not reflected immediately. However, these attacks cause permission policies to be tightened or eliminated potentially denying network services over a long-term. In multi-dimensional analysis of DoS attacks, a number of metrics such as jamming gain, jamming efficiency, packet send ratio, and packet delivery radio, have been proposed.

- Primary User Emulation (PUE) Attack Chen et al. have identified a threat to spectrum sensing, named the primary user emulation (PUE) attack in which an adversary's CR transmits signals whose characteristics emulate those of incumbent signals (Chen et al., 2008c). This attack is particularly easy to launch in CR due to the highly flexible and software-based air interfaces of CR sensor nodes. The PUE attack can be catastrophic since it severely interferes with the spectrum sensing process and reduces the channel resources available to the legitimate unlicensed users in the network. In another work, Chen et al.

have discussed two different security threats on CR network which are known as incumbent emulation (IE) attack and spectrum sensing data falsification (SSDF) attack (Chen et al, 2008b). The IE attack is essentially same as the PUE attack since the primary users are also sometimes referred to as the incumbents. The SSDF attack is carried out by malicious secondary nodes that transmit false spectrum sensing data to other nodes. This attack is critical in a CR, since sending of false spectrum sensing information to a data collector in the network can cause the data collector to make a wrong spectrum sensing decision resulting in a catastrophic impact on the network performance. Wang et al. have argued that one of the major challenges in CR networks is to detect the presence of primary users' transmission, since malicious secondary users can send false spectrum sensing information and mislead the spectrum sensing data fusion process to cause collision, interference and inefficient spectrum usage (Wang et al., 2009c). Clancy and Khawar have highlighted the need of robust signal classification mechanisms for CR networks so that different types of transmitters can be differentiated in a particular frequency band in order to defend against the PUE attacks (Clancy & Khawar, 2009). Anand et al. present a novel analytical framework to analyze the feasibility of PUE attack in a CR network which can be applied to a CWSN as well (Anand et al., 2008).

- Masquerading Attack Masquerading attacks on a CR node and attacks involving malicious alteration of CR nodes for disrupting spectrum sensing functions have also been studied extensively. Wang et al. have shown the adverse effect of malicious and compromised secondary users in a CR network (Wang et al., 2009b). Chen et al. have considered the security issues related to malicious secondary users reporting false spectrum sensing information due to Byzantine failure in a distributed spectrum sensing environment

in a CR network (Chen et al., 2008a). The Byzantine failures, such as device malfunction or attacks severely affect the spectrum sensing functions in a CR network since these failures or attacks can enable an attacker to constantly report the spectrum in a band being in use causing severe under- utilization of the available spectrum. Hu et al. have also addressed the issue of Byzantine failures of secondary users in a CR network, and have proposed a security mechanism that is similar WSPRT, in which the binary local reports used in WSPRT are replaced with N-bit local reports to achieve an enhanced detection performance (Hu et al., 2009). Mody et al. have discussed various security threats in IEEE 802.22 standard-compliant devices which are deployed in CR networks (Mody et al., 2009).

- Attacks Involving Salse Spectrum Reports Sent Secondary Users The threats due to false spectrum reports sent by malicious secondary users are also critical. Securing the control channels ensures that CR messages communicated over these channels cannot be altered by a malicious adversary. This protection is critical in CR which are deployed for mission-critical applications. In this perspective, Safdar and O'Neill have identified the need of securing the cognitive control channels to perform channel negotiations before data communication among the nodes in a CR network (Safdar & O'Neill, 2009). The authors propose a novel framework for providing common control channel security for cooperatively communicating CR nodes so that a pair of CR nodes can authenticate each other. Li and Han have discussed a critical security issue in collaborative spectrum sensing in which malicious secondary user(s) sends false spectrum report to thwart the spectrum data fusion process (Li & Han, 2010).

- Attacks on Cognitive Control Channels Securing cognitive control channels is an extremely important security issue in CR networks. Prasad have argued that design of a CR network poses many new technical challenges in protocol design, power efficiency, spectrum management, spectrum detection, environment awareness, novel distributed algorithms design for decision making, distributed spectrum measurements, quality of service (QoS) guarantees, and security (Prasad, 2008). The author have identified various research challenges for security in CR networks and have presented the security and privacy requirements, threat analysis and an integrated framework for security using fast authentication and authorization architecture. The particular focus of the proposed security framework is to defend against jamming attacks and attacks on the cognitive control channels (CCCs) in CR networks.
- Attacks on The MAC Layer Zhu and Zhou have provided a security analysis of the MAC protocols used in CR networks by investigating the impact of DoS attacks on these protocols (Zhu & Zhou, 2008). In order to make a security analysis of the MAC protocols, the authors have distinguished two types of attacks and then discussed how DoS attacks can be successfully launched on the MAC protocols. The authors have also presented a detailed discussion on MAC layer greedy behaviors in CR networks and the factors that determines the efficiency of the DoS attacks.
- Attacks on The Cognitive Engines Clancy and Goergen identify three classes of attacks on the cognitive engine of CR networks (Clancy & Goergen, 2008). All these types of attacks manipulate the behavior of the CR system such that the radio acts either sub-optimally or even sometimes maliciously. Three classes of attacks are identified: (i) sensory manipulation attacks against policy radios,

(ii) belief manipulation attacks against the learning radios, and (iii) self-propagating behavior leading to cognitive radio viruses. In a policy radio, the main vulnerability lies in the fact that an attacker can spoof faulty sensor information that can cause the radio to select a sub-optimal configuration. Since the radio sensors take digitized RF and extract useful statistics from it, by manipulating the RF that is available to the radio, an attacker can cause faulty statistics to appear in the CR knowledge base. The learning radios are also vulnerable to the same threats as the policy radios. However, since a leaning radio uses all its past experiences in building its long-term behavior, attacks on it are much more detrimental. For example, an attacker can transmit a jamming signal whenever a policy radio attempts to switch to a faster modulation rate. This will always force the CR to operate at a lower modulation rate, resulting in lower links speeds and link degradation. The authors have called these attacks as belief manipulation attack since these attacks can potentially have long-term adverse impact of the learning radios. The self-propagating behavior of the radio can be utilized by a malicious attacker to launch the most powerful type of attack. In such an attack, the state on radio causes a behavior that can induce the same state on another radio. Once the target radio attains the state, it exhibits behavior that leads to a state change in another radio so that it attains the same state. Eventually, the same state propagates through all radios in a particular area in the CR network. The net effect is that of a cognitive radio virus that propagates through the network.

- Threats Related to the Hidden Node Problem The threats related to the hidden node problem in CR networks have also been studied extensively by the researchers. Biswas et al. propose a technique to handle both wideband and cooperative spectrum sensing tasks in a distributed spectrum sensing

environment (Biswas et al., 2009). Nuallain presents a fast and robust propagation method for addressing the hidden node problem in a CR network (Nuallain, 2008). Bliss have investigated the optimal spectral efficiency for a given message size that minimizes the probability of causing disruptive interference for a CR network (Bliss, 2010). The goal of the work is to have an optimization between longer transmit duration and wider bandwidth versus higher transmit power so as to tackle the hidden node problem. It may be noted that among all the threats in CR, jamming and masquerading of the primary users are most critical. Another interesting point to note is that some of the attacks can be correlated to launch a powerful two-phase attack. For example, an attacker may first eavesdrop on cognitive messages and then may replicate and modify the cognitive messages to transmit false information.

2.6.2 Related Works on Security Mechanisms to Defend Against Attacks in CRs

This section will identify the main security requirements in a CR networks and then discuss various security schemes for defending against various attacks. In a CR networks, the sensor nodes participate in collaborative spectrum sensing activities. Gao et al. have identified the following security requirements in CRs (Gao et al, 2012): (i) authentication mechanisms, (ii) incentive mechanisms, (iii) data and message confidentiality, (iv) privacy protection of the sensor data.

- Authentication Mechanisms A robust authentication mechanism is a prime requirement in collaborative spectrum sensing. The authentication scheme may have different perspectives to different categories of nodes in a CR networks. The authentication of the primary users is a critical issue since an attacker may transmit signals with high power that has close resemblance with the signals of a primary user and launch a primary user emulation (PUE) attack

(Chen et al., 2008c; Liu et al., 2010). To prevent such an attack, the secondary users should have a robust verification scheme for verifying the authenticity of the received signals. Similarly, when the secondary users receive the sensing reports from other users, they should be able to verify the authenticity of the other secondary users; otherwise, a potential adversary may be able to spoof the identity of a secondary user. The authentication of sensing reports distributed across the network is also a very important issue. Even if the authentications of the secondary users are done during the sensing report aggregation process, it is still possible for a malicious secondary user to send false sensing reports and launch spectrum sensing data falsification (SSDF) attack (Wang et al., 2009b). Hence, each sensing report in the aggregation process should be authenticated.

- Incentive Mechanisms Most of the current collaborative sensing schemes assume that the secondary nodes voluntarily participate in spectrum sensing. However, this assumption may not hold good for selfish secondary users who may not cooperate in order to conserve their own resources (Wang et al., 2010). Such selfish behavior may seriously degrade the performance of a CR networks. Incentive schemes are necessary for minimizing the probability of such selfish behavior.
- Data and Message Confidentiality The sensing reports need to be well protected so that these messages are not misused by unauthorized external users. Data and message confidentiality can be achieved by using end-to-end robust encryption algorithms which in turn needs mutual authentication and authorization among the collaborating nodes participating in spectrum sensing.

- Privacy Preservation of Sensor Data Privacy protection is primarily for preserving the anonymity of the sensing nodes and/or privacy of its location. Location privacy protection attempts to prevent a possible adversary form linking a sensing node's sensing report to the physical location of the sensing node. In order to satisfy the aforementioned security requirements and to defend against various possible attacks on the sensor nodes in a CRs, various defense mechanisms are proposed by the researchers. These security schemes can be broadly divided into the following categories: (i) mechanisms for enhancing the robustness in sensor inputs, (ii) schemes based on the reputation and trust of the nodes, (iii) mechanisms based on identification of masquerading attack by signal analysis, (iv) robust authentication schemes using appropriate cryptographic algorithms, (v) mechanisms for preventing unauthorized access to the spectrum, (vi) mechanisms for defending against attacks on the MAC layer and the cognitive engine of the network, (vii) schemes for increasing the robustness of the cognitive control channel against jamming and saturation attacks, and (viii) schemes using geo-location database of the primary users in the network. The following sections present a brief discussion on these various types of security mechanisms.
- Enhancing the Robustness in Sensor Inputs Many of the attacks on CR networks can be defended if the reliability of sensor inputs is enhanced. For example, if the cognitive radios can minutely identify the differences between interference and noise, they can distinguish natural and artificial RF events. Such sensors can feed specialized policy algorithms that specifically look for hostile signals that may be try to subvert a radio's belief. In a distributed computing scenario, a group of cognitive nodes can fuse sensor data to improve the performance of the overall network. For example, if multiple sensor nodes exchange time-

synchronized RF information, they can cross-correlate the exchanged information to arrive at a more precise identification of an attacker. The task becomes challenging, however, since the all sensory inputs are imprecise to a certain extent.

- Reputation and Trust-based Security Systems A significant number of schemes have been proposed by the researchers using reputation and trust of the CR nodes for defending various types of attacks. Using the concepts of reputation and trust, a CR node can be mapped to a particular level of reputation and trust on the basis of the spectrum sensing information the node shares with other CR nodes. If the information shared by the node is found to be not correct after a certain number of iterations, then the specific CR node is considered to be malicious and appropriate action is taken against the node based on pre-defined security policies. Zeng et al. have proposed a reputation-based cooperative spectrum sensing (CSS) framework using trusted nodes in a CR network for achieving correctness in the global decisions on spectrum sensing (Zeng et al., 2010). In the proposed scheme, at the beginning, sensing information from trusted nodes is only considered reliable and used in the decision making. Reputations of other CR nodes are put in the pending state, and they are accumulated through a consistency check between the global and local sensing decisions. The information received from the nodes which have their trust values greater than a pre- defined threshold is then considered reliable and their sensing results are incorporated in the CSS. The use of reputation system increases the robustness of cooperative sensing scheme. Duan et al. propose a spectrum sensing algorithm that is based on the reputation of the nodes (Duan et al., 2009). The algorithm is effective in mitigating the effects of shadowing and fading in wireless channels and in eliminating the problem

related to fail sensing in CR networks with double threshold detector. Li and Han have presented an anomaly detection algorithm for identifying attackers in a collaborative spectrum sensing environment (Li & Han, 2010). The proposed scheme does not assume any a priori information about the strategy used by the attackers in launching the attack, which makes scheme suitable for real-world deployment. Kaligineedi et al. propose an attack detection scheme to identify malicious users that send false spectrum sensing information in a CR network (Kaligineedi et al., 2008). The proposed scheme uses the average power obtained from the real-valued reports received from the CR nodes for making a global decision on spectrum sensing. Chen et al. present a security scheme based on weighted sequential probability ratio test (WSPRT) to address Byzantine failures on CR nodes in the data fusion process of collaborative spectrum sensing (Chen et al., 2008a). The mechanism involves an allocation of a reputation rating to each node based on the consistency of its local sensing report with the final decision in the spectrum sensing. Peng et al. discuss various security aspects in cross-layer design of CR networks and propose a novel architecture in which dynamic channel access is achieved by a cross-layer design between the PHY and the MAC layers of a CR network (Peng et al., 2009). The proposed architecture is able to handle Byzantine failure of nodes. Anand et al. have analyzed the performance limitations of collaborative spectrum sensing in a DSS environment under Byzantine attacks where malicious users send false spectrum sensing data to the fusion center leading to increased probability of incorrect sensing results and wrong global decisions being taken by the CR (Anand et al., 2010). It has been shown that if the percentage of Byzantine attackers in a CR network exceeds a certain threshold value, the data fusion scheme become completely incapable in carrying out

reliable data fusion and no reputation-based fusion system can achieve any performance gain in the data fusion operation. The authors have presented optimal attacking strategies for a given set of attacking resources and have also proposed possible counter measures at the data fusion center. Xu et al. propose a collaborative sensing algorithm that uses an energy detector with double thresholds and an extended data fusion rules to identify untrusted and possibly malicious CR nodes (Xu et al., 2009). Yu et al. have studied the security issues related to the SSDF attack in which attacker(s) sends false local spectrum sensing results in a DSS environment (Yu et al., 2009). A consensus-based cooperative spectrum sensing scheme is proposed that is inspired from the self-organizing behavior of animal groups.

- Detection of Masquerading Attacks by Signal Analysis Signal analysis is an important technique used in identification of malicious attacker(s) in CR networks. This method is very effective in addressing security threats which involve a malicious attacker masquerading as an incumbent transmitter by transmitting unrecognized signals in one of the licensed bands and thereby effectively preventing secondary users in the CR network from accessing the same spectrum band. Spectrum sensing can be done in a variety of ways. Some of the commonly used spectrum sensing methods are: energy detector based sensing (also known as radiometry or periodogram), waveform-based sensing, cyclostationarity-based sensing, radio identification-based sensing, matched filtering, multi-taper spectral estimation, wavelet transform-based estimation, Hough transform, and time- frequency analysis (Yucek & Arslan, 2009). However, each of these spectrum sensing techniques have vulnerabilities in a CR network since an adversary can masquerade a primary or a secondary user or by emulating its signal. Various security schemes have been proposed by

researchers to detect and defend against such attacks. Some of the mechanisms are briefly discussed in the following. Chen and Park propose a security mechanism for defending against masquerading of a primary user by a malicious adversary (Chen & Park, 2006). The proposed scheme is based on a transmitter verification procedure that employs a location verification scheme to distinguish incumbent signals (i.e., signals from a primary user) from unlicensed signals masquerading as incumbent signals. Location verification is achieved by using two techniques: (i) distance ratio test (DRT), which uses the received signal strength indicator (RSSI) of a signal source and (ii) distance difference test (DDT), which uses relative phase difference of the received signal as the signal is received at different receivers. It is assumed that the location information of some of the CR nodes in the network is always known a priori either because these nodes are fixed or they use trusted GPS information. These CR nodes perform DRT and DDT operations within their coverage areas and also serve as the location verifiers (LVs). The LVs exchange the location information of incumbent transmitters through a cognitive pilot channel. Zhao and Zhao propose a cooperative detection scheme that can suppress malicious users (Zhao & Zhao, 2009). In the proposed scheme, the secondary users collaborate by exchanging and using decision fusion on the local decision results instead of using the detected energy. A mechanism of weighted coefficients is used which updates the weights of the coefficients recursively according to the deviations between separate decision information and the combined final results. Zhao et al. propose an identification mechanism of the CR nodes using an analysis of the transmitted signals in which wavelet transform is used to magnify the fingerprints of the transmitter characteristics (Zhao et al., 2010). This PHY-layer authentication approach is intended to

prevent the PUE attack in CR networks. Afolabi et al. have describe a PHY layer attack model that exploits the adaptability and flexibility of the CR networks and propose a waveform pattern recognition scheme to identify emitters and detect camouflaging attackers by using electromagnetic signature (EMS) of the transceiver (Afolabi et al., 2009). The EMS of a device is computed based on the distinctive behavior in the waveform being emitted by the components of the transceiver including the frequency synthesis systems, modulator sub-systems, and the RF amplifiers. Clancy and Khawar present sophisticated signals processing algorithms like cyclostationary analysis, classification engines, or signal feature extraction for identifying false signals in CR networks (Clancy & Khawar, 2009). The authors propose the use of unsupervised learning in feature-based signal classification and provide recommendations to mitigate the impact of the attack on CR networks.

- Robust Authentication using Cryptographic Techniques Cryptographic techniques are widely used in designing robust and efficient authentication protocols in wireless networks. However, in CRs, authentication mechanism should be adaptable to all communication protocols with which the CR nodes have to interface. Hence, design and implementation of authentication protocols for CRs pose significant challenges. Kuroda et al. propose a radio-independent authentication framework for CR networks that can be integrated with the extensible authentication protocol (EAP) (Kuroda et al., 2007). The protocol is suitable for deployment in real-world networks since it allows fast switchover in CR network and does not need any communication with the authentication authorization and accounting (AAA) server for any re-authentication of the CR nodes. Jakimoski and Subbalakshmi have proposed an efficient and provably secure protocol that can be used to protect the spectrum

decision process against a malicious adversary (Jakimoski & Subbalakshmi, 2009). The proposed protocol is designed to provide secure spectrum decisions in a clustered infrastructure-based network where the spectrum decisions are made at periodic intervals and the decision in each cluster is taken independently of the decisions in other clusters. The CRs should ensure authorization of the cognitive sensor nodes for transmitting specific spectrum bands or for performing specific network functions. The authorization is often conditional to the nature of the spectrum environment, i.e., the presence of primary users in the area. The authorization is needed to define the roles of the CR nodes in performing the CR functions. For authentication and authorization purposes, the nodes exchange information through a common CCC. Safdar and O'Neill propose a security framework for protecting the information exchanged over the CCC (Safdar & O'Neill, 200).

- Security Mechanisms for Prevention of Unauthorized Spectrum Access A malicious node can access spectrum in a CR network in an unauthorized way either to use the spectrum selfishly or to launch a DoS attack on the primary users. Several propositions are made by researchers for defending against such attacks. In the following, we provide a brief discussion on some of these schemes. Xu et al. present a framework known as TRIESTE (Trusted Radio Infrastructure for Enforcing SpecTrum Etiquettes) for ensuring that radio devices are only allowed to access the spectrum according to their privileges (Xu et al., 2006). The framework is based on a trusted computing (TC) base in each CR node that enforces the policy rules for spectrum access and etiquettes defined in the XG Policy Language (XGPL). Atia et al. propose an enforcement structure for defending against malicious attacks (Atia et al., 2008). The goal of the work is to provide a framework so that the primary users can distinguish

between the wireless environmental losses and the presence of harmful interference of the secondary users. A popular approach for defending against unauthorized spectrum access is to deploy a spectrum monitoring system in the CR network. The spectrum monitoring system acts as a spectrum "watch guard" for detecting spectrum misuse and carries out the following functions: (i) monitoring of the spectrum usage in a specific spatial region and over a range of frequencies, (ii) identifying wireless services and the nodes providing such services. However, design of an effective spectrum monitoring system is a challenging task since natural or man-made obstacles can change the features of the radio signal, and identification of wireless services may be difficult if an attacker can successfully emulate a specific wireless service being provided in the network. To address these problems, spectrum monitoring systems can be distributed across the nodes. Information on the wireless services in an area can be transmitted to a central monitoring location, which can, then, correlate the various inputs and check the received information against other data like the known position of the wireless services in the area and their source.

- Defense Mechanisms against Attacks on the MAC and the Cognitive Engine Attacks on the MAC layer, network layer and on the cognitive engine of a CR network are usually defended by making a robust system design. IEEE 802.22 standard provides a robust authentication and encryption scheme to mitigate attacks on the MAC layer. As a defense mechanism for the cognitive engine, Perich and McHenry propose a policy-based spectrum access control system for the Defense Advanced Research Projects Agency (DARPA) NeXt Generation (XG) communications program for mitigating the harmful interference caused by a malfunctioning device or a malicious user for a cognitive software defined

radio (SDR) (Perich & McHenry, 2009). The authors propose two protection mechanisms for defending against attacks on the cognitive engine. In the first approach, the authors have argued that the likely effect of a threat on a CR network is to disrupt the state machine of the CR network and to bring the CR device to an incorrect (i.e. faulty) state. Formal state-space validation, as done with cryptographic network protocols, can be applied to the state machine to ensure that a "bad state" is never arrived at. In the second approach, the authors propose that the beliefs of the cognitive engine should be constantly re-evaluated and compared to a priori knowledge (e.g., local spectrum regulations) or rules (e.g., the relationship between transmit power, propagation, and frequency).

- Security Mechanisms for the Cognitive Control Channels The cognitive pilot channel (CPC) of a CR network is responsible for distributing the cognitive control messages. The CPC is vulnerable to numerous attacks including the DoS attacks and the saturation attacks on the control channels. A popular protection mechanism against the jamming attack in a specific spectrum band of a CR network is to use frequency hopping. The CPC could use more than one spectrum band and "hop" around the spectrum bands to avoid a possible jamming attack. The trade-off is an increased complexity of the CR network as the CR nodes should be notified about the change in the frequency band of the CPC. If an attacker effectively monitors the CPC, it could "chase" the CPC band for every change and eventually cause continual adaptation and outage of service to the CR network. Yue et al. present two coding schemes for recovering lost packets transmitted through parallel channels for designing an efficient anti-jamming coding technique (Yue & Wang, 2009). The two coding schemes, known as rateless coding and piecewise coding, can be adapted to CWSNs for

protecting the CPC and CCC. Meucci et al. present a lightweight mechanism for achieving security in the PHY layer in a CR network using orthogonal frequency division multiplexing (OFDM) (Meucci et al., 2009). In the proposed scheme, the user's data symbols are mapped over the physical sub-carriers using a permutation strategy. The security in the PHY layer is achieved using a random and dynamic sub-carrier permutation which is based on a single pre-shared information.

- Security Mechanisms using Geo-location Database of Primary Users In this approach, the CR network provider maintains a database of the positions and transmission characteristics (e.g., transmit power) of all the primary users in the network. The CR finds its own location information using a GPS and compares the data received from the spectrum sensing functionality with the known position of the primary users. Any anomaly in position information triggers an alert for a possible malicious attack. Borth et al. propose a protection technique wherein a primary user would transmit a beacon to alert secondary users to not transmit in specific spectrum bands (Borth et al., 2008). The drawback of this scheme is that the primary user devices are to be modified for beacon transmission.

CHPTER 3

SYSTEM MODEL

3.1 Model Description

In this model all secondary and malicious users are distributed in a circular grid of radius R as shown in Figure 3.1 below

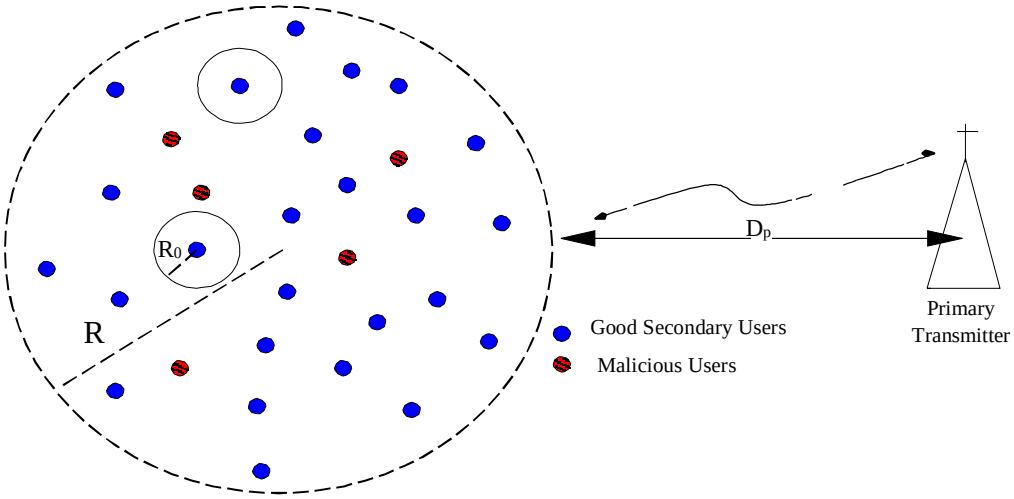


Figure 3.1 Cognitive Radio Network Model

A primary user (eg., a TV tower), is located at some distance from all the users , the secondary users are randomly and uniformly distributed within a network radius from the primary transmitter . In order to detect the white spaces or the return of the primary user, the secondary users measure the received power , if the received power is below a specified threshold to be vacant (white space) . It the received power is above the specified threshold T, then based on the measured power, a decision is made as to whether the received signal was transmitted by a primary transmitter or by a set of malicious users . (Energy detection involves the

application of a threshold T in the frequency domain, which is used to decide whether a transmission is present at a specific frequency. Any portion of the frequency band where the energy exceeds 100 dBm is considered to be occupied channel. Since different transmitters employ different signal power levels and transmission ranges, one of the major concerns of energy detection is the selection of an appropriate threshold) .

Then a statistical test must be used, here we use Neyman Pearsons,s Composite Hypothesis test (NPCHT) to obtain a criterion for making this decision. To perform the analysis, the assumptions below are taken:

- The distance between primary transmitter and all the users is d_p (The actual co-ordinates of the primary transmitter depends on the actual location of the secondary user and will not be exactly d_p for all the users. However, typically, $d_p \gg R$ and hence it is justified to approximate the co-ordination of the primary user to be (d_p,θ_p) irrespective of which secondary user we consider for the analysis) .
- There are M malicious users in the system.
- The locations of malicious users are uniformly distributed in the circular grid of radius R.
- The primary transmit at a power P_t while the malicious users transmitter co-ordinates are fixed at a point (rp, θp) and this position is known to all the users in the grid.
- The secondary user co-ordinates (r,θ), no malicious users are present within a circle of radius R_o known as " exclusive distance from the secondary user " centered at (r, θ) , in case of the condition is not met then the received power at the secondary due to transmission from any subset of malicious

users present within a distance R_o from the secondary becomes too large to create PUE attack .

- The transmission from primary transmitter and malicious users undergo path loss and log normal shadowing.
- The path loss exponent chosen for transmission for primary transmitter is 2 and from malicious user are 4.
- There is no communication or co-operation between the secondary users. The PUE attack on each secondary user can be analyzed independent of each other.

3.2 Model Analysis

First we have to obtain the probability Density Function (pdf) of the received power at the secondary user due to transmission by the primary and by the malicious users in order to obtain a hypothesis test using NPCHT, since there is no co-operation between the secondary users, the probability of successful PUE attack on any user is same as that on any other user. Hence, we analyze the pdf of received power at any one secondary user.

3.2.1 Probability Density Function of The Received Signal

One of the applications of the probability density function of the received power is using it in NPCHT or any other statistical test to identify attackers in CR network.

We consider M malicious users located at co-ordinates (r_j , $(-)$ j)$1 \leq j \leq$ M. Since the position of the j^{th} malicious user is uniformly distributed in the annular region between R_o and R , r_j and $(-)_j$ are statistically independent $\forall$ j.

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

$$P_r^{(m)} = \sum_{j=1}^{M} P_m \cdot d_j^{-4} \cdot G_j^2 \quad \text{(3.1)}$$

Where , d_j is the distance between the j^{th} malicious user and the secondary user .

G_j^2 is the shadowing between the j^{th} malicious user and the secondary user.

The pdf of $P_r^{(m)}$ conditioned on the positions of all malicious user can be written as:

$$P^m(X) = \frac{1}{x.A.\sigma_{x\sqrt{2\pi}}} \exp\left\{-\frac{(10\,log_{10}X-\mu_x)^2}{2\,\sigma_x^2}\right\} \quad \text{(3.2)}$$

The received power at a secondary user from the primary transmitter is given by :

$P_r^{(p)} = P_t \cdot d_p^{-2} \cdot G_p^2$ (3.3)

Where, $G^2_{p=10^{\varepsilon_{p/10}}}$ and $\varepsilon_p = N(o, \sigma_p^2)$

Since p_t and d_p are fixed

The Pdf of $P_r^{(p)}$ follows a log-normal distribution and can be written as :

$$P^{P_r}(Y) = \frac{1}{\gamma.A.\sigma_p\sqrt{2\pi}} \exp\left\{-\frac{(10\,log_{10}y-\mu_p)2}{2\ \ \sigma_p^2}\right\} \quad \text{(3.4)}$$

3.2.2 Detecting PUE Attack Using Neyman–Pearson Criterion

By applying the two hypothesis in NPCHT decision criterion which are given below,

H1: Primary Transmission in progress.

H2: Emulation Attack in progress.

In the hypothesis test there are two types of errors that secondary user can make:

- False Alarm The secondary makes a decision that transmission is due to primary but the malicious user is transmitting.

- Miss Detection The secondary makes a decision that transmission is due to malicious user but the primary is transmitting. The power of the received signal is measured in order to calculate the decision variable which is given by the ration of

$$V = \frac{P^{m}(X)}{P^{P_r}(X)} \text{ ——————————(3.5)}$$

Where. $P^{P_r}(X)$ and $P^{m}(X)$ is the pdf of received power from all malicious users respectively .

V is then compared with predefined threshold and the secondary decides the following.

$V \leq \lambda \rightarrow D1$: Primary transmission in progress.

$V > \lambda \rightarrow D2$ PUE attack in progress.

First, secondary user may decide D1 when H2 is true, and second secondary user may decide that D2 when H1 is true.

Each of these errors has a probability associated with it.

CHAPTER 4

RESULTS AND ANALYSIS

4.1 Introduction

This chapter present the results obtained using Matlab simulation and also the theoretical results for similar setup for the probability density function of the received power the secondary user due to the primary transmitter and the received power at the secondary user due to the malicious users. Also we determined the performance of the network for PUE attack in terms of probability of miss detection and false alarm. In addition to the relationshipbetween the false alarm probability (i.e., the probability of successful PUE attack) and the Radius R of the network. In the simulation I have used the parameters presented in Table 4.1.

4.2 System Parameters for Simulation

The parameters of the system is set as in table 4.1 these parameters are used in the both cases to establish a fairly compression .

Parameter	Value
D_p : Distance between primary transmitter and other users	120 Km
R : Radius of the circular grid	300 m
R_o: Radius of annular region	40m
M:Number of malicious users in the system	30/10
P_t: Primary transmission power	20Kw
P_m: Malicious transmission power	5 w
σ_p: Variance of Primary users	8 dB
σ_m: Variance of Malicious users	5.5 dB

Table 4.1 System Parameters

4.3 Probability Density Function Using Simulation and Mathematically

We can see from figure 4.1 and figure 4.2 that the result of the probability density function using simulation considerably match with the one derived mathematically.

There is a slight mismatch and the reason behind this is due that the theoretical derivation is for ideal setup and over an unlimited duration of time while the simulation testing times are limited in number and also have random effects as per the simulation settings.

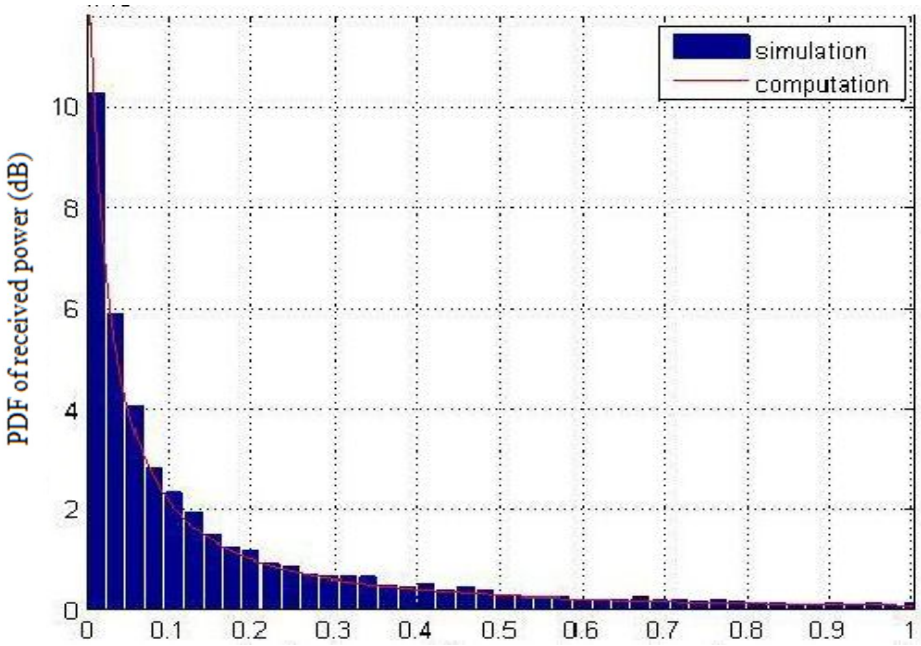


Figure 4.1 PDF of the received power vs. received power at the secondary receiver from primary transmitter (dB)

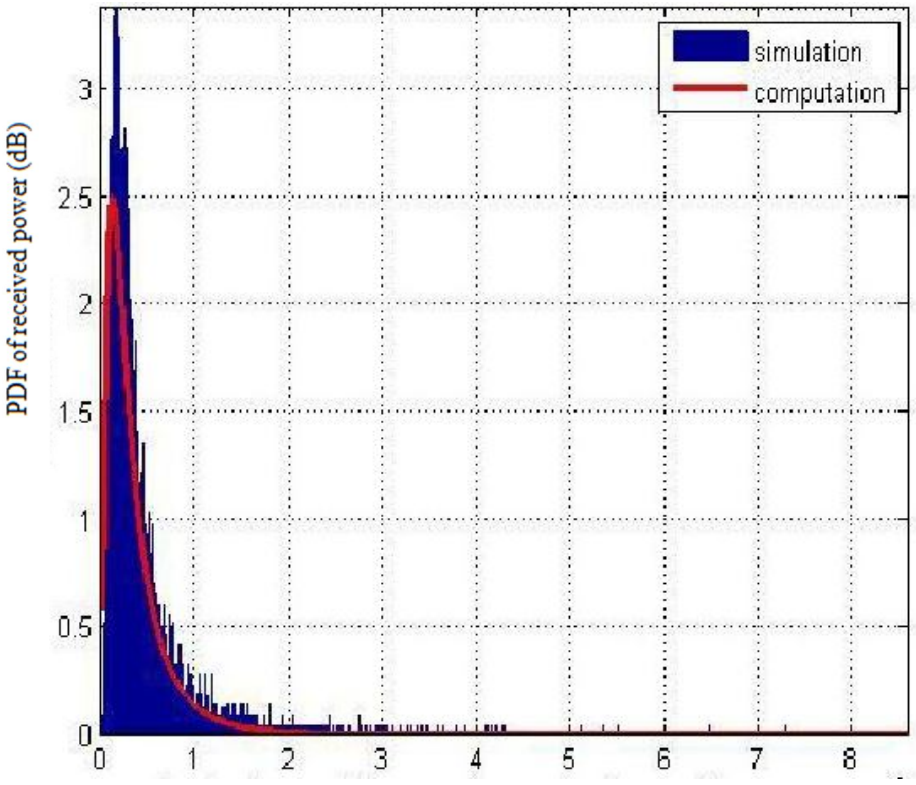


Figure 4.2 PDF of the received power vs. received power at the secondary receiver from malicious users (dB)

It's clear that the probability density functions of the received power at the secondary user from the primary transmitter is differ from the received power at the secondary user from the malicious user (Matlab code is in appendix A).

4.4 Case One

The first scenario will execute the model with a particular number of malicious users which is chosen to be M=30 (high) and different values of R in order to investigate the values of the probability of miss detection and the values of the probability of false alarm (successful PUEA) .

Figure 4.3 and Figure 4.4 are the plots for the probability of miss detection Vs. The number of simulation times and false alarm Vs. The number of simulation respectively.

The probabilities are calculated for 600 time of simulations. The threshold value is set to 2, i.e $\lambda = 2$, the radius of primary exclusive region $R_o = 40$ Radius of outer region in this case is R= 300, primary transmitter power $P_t = 20$ Kw, malicious transmitter power $P_m = 5$ w , σ_m= 5.5 dB , σ_p = 8dB.

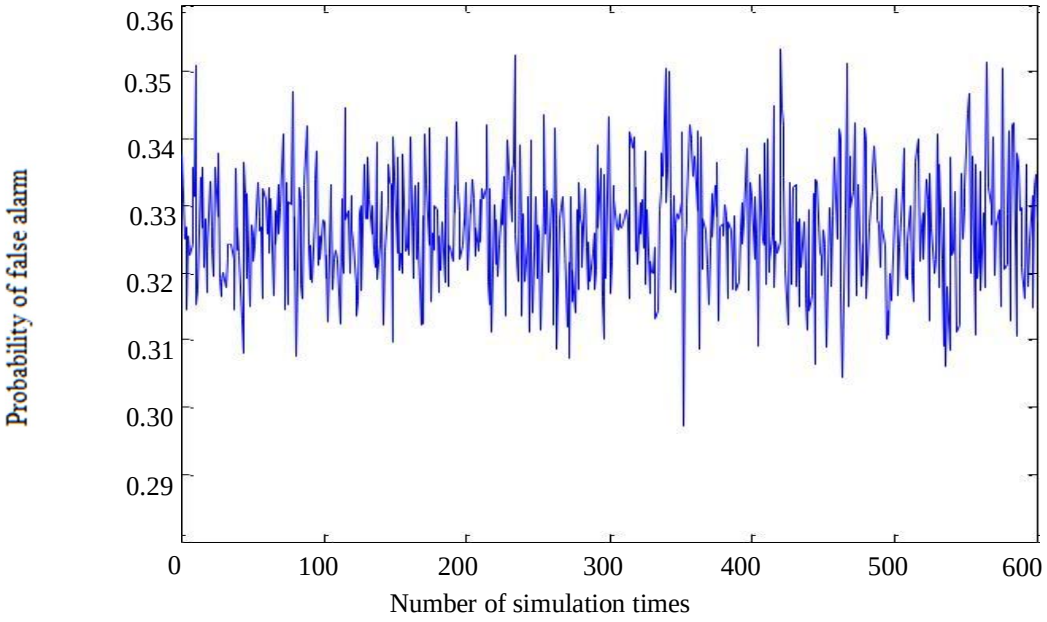


Figure 4.3 Probability of false alarm (successful PUE attack) vs. number of simulation times

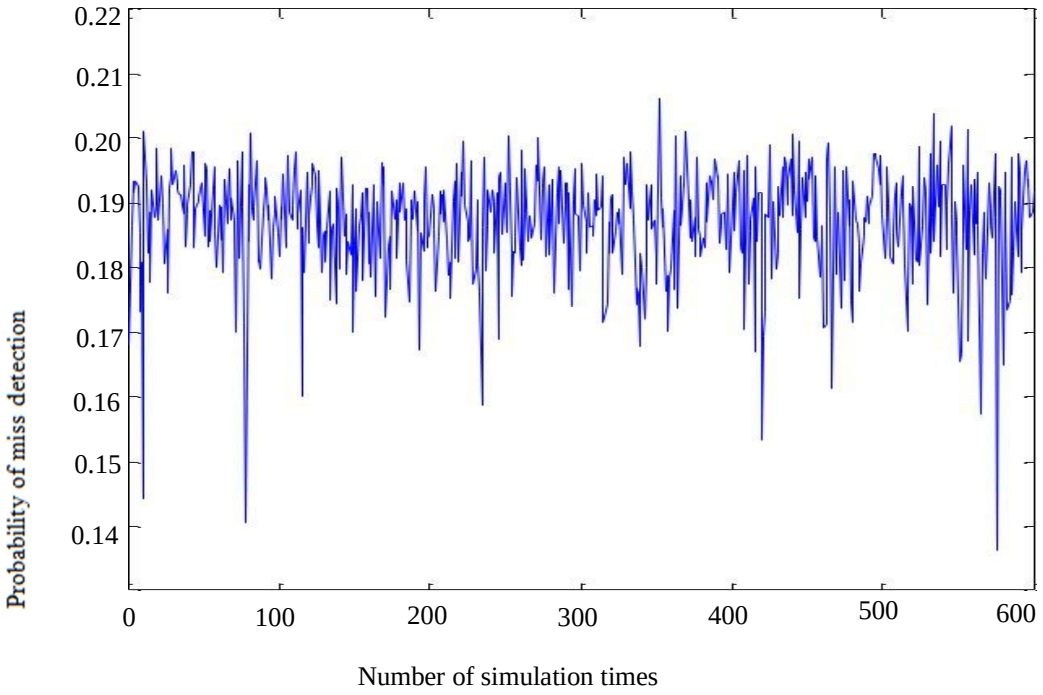


Figure 4.4 Probability of miss detection vs. number of simulation times

As we can see from the experimental probability of false alarm (successful PUE attack) is always close to 0.326 (within ± 0.04 of this value) for the all number of simulation runs and this is because the high number of malicious. The miss detection probability is averaged at 0.187 for the whole 600 runs.

I have done the simulation with different values of R as shown in Table 4.2. (Matlab code is in appendix B).

Number of malicious users , M= 30							
Threshold value , λ = 2							
R(meters)	100	200	300	400	500	600	700
P-D1-H2	0.258	0.380	0.326	0.250	0.170	0.122	0.07
P-D2-H1	0.7825	0.1558	0.187	0.069	0.0075	0.072	0.017

Table 4.2 Case one probabilities values

4.5 Case Two

The second scenario will execute the model with a number of malicious users which is chosen to be M= 10 (low) and different values of R.

Figure 4.5 and Figure 4.6 are the plots for the probability of miss detection vs. The number of simulation times and false alarm vs. The number of simulation respectively. The probability are calculated for 500 time of simulations. The rest of parameters are as in case number one.

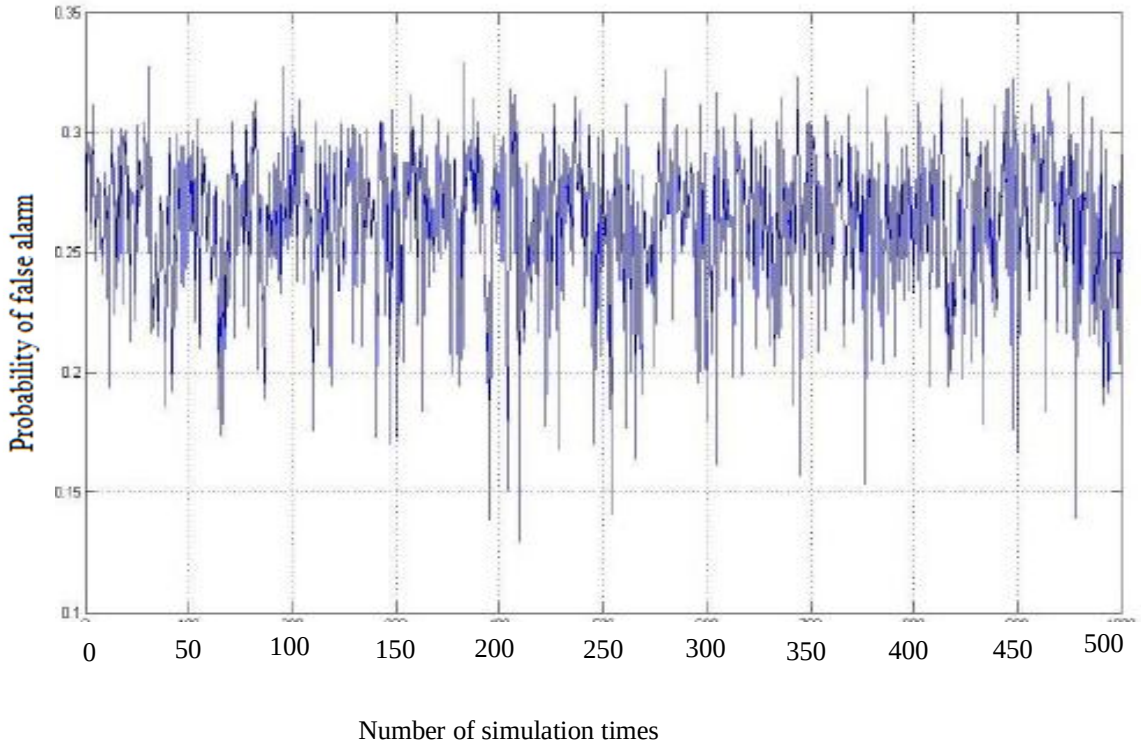


Figure 4.5 probability of false alarm (successful PUE attack) vs. number of simulation times

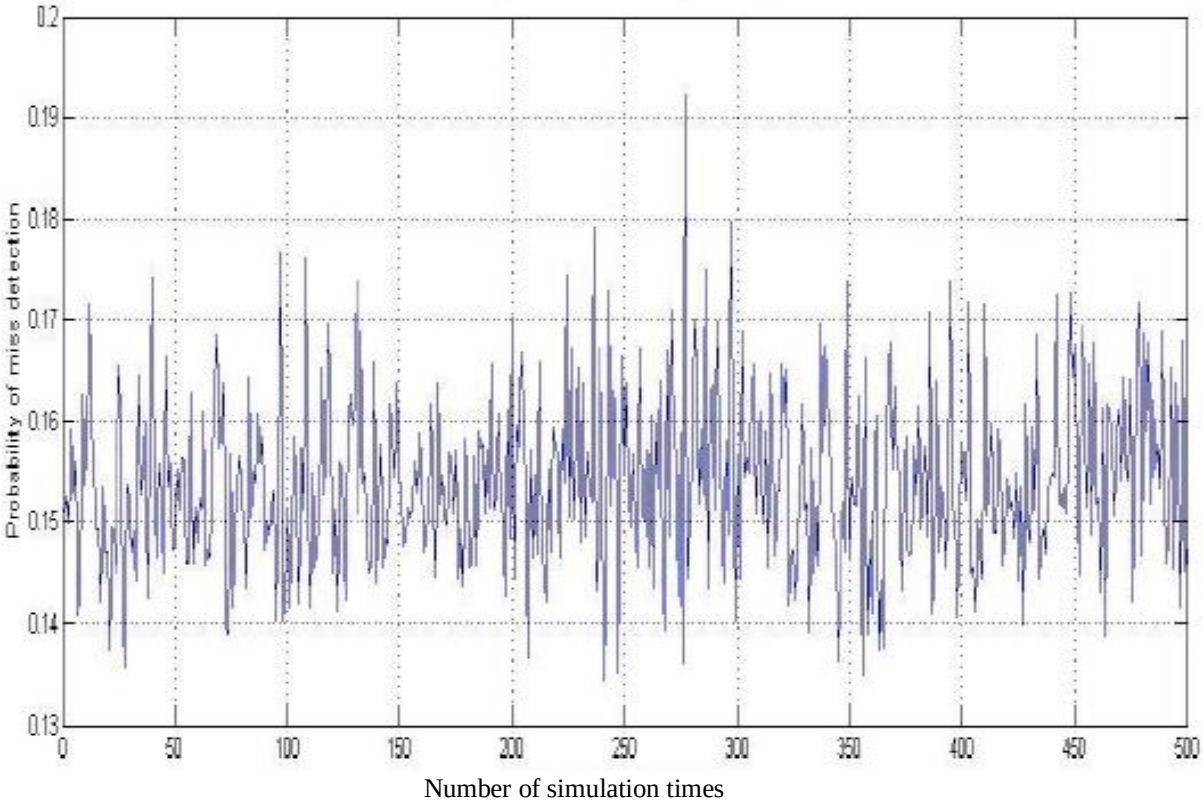


Figure 4.6 Probability of miss detection vs. number of simulation times

As we can see from the experimental probability of false alarm (successful PUE attack) is always close to 0.270 (within ± 0.04 of this value) for the all number of simulation runs and this is because the low number of malicious. The miss detection probability averaged at 0.155 for the whole 500 runs.

I have done the simulation with different values of R as shown in Table 4.3. (Matlab code is in appendix C).

Number of malicious users , M= 10							
Threshold value , λ = 2							
R(meters)	100	200	300	400	500	600	700
P-D1-H2	0.230	0.380	0.270	0.07	0.03	0.02	0.01
P-D2-H1	0.210	0.333	0.155	0.024	0.223	0.0017	0.0011

Table 4.3 Case two probabilities values

Based on the PDF which achieved in the simulation and Neyman Person's Composite Hypothesis test approach we have obtained the probability of successful PUE attack (False Alarm), it is observed that the probability of false alarm rises and then falls down with increasing value of R and also there is a value of R for which the probability of false alarm is maximum, this is expected because:

For a given Ro, if R is small, the malicious users are closer to the secondary user and total received power from all the malicious users is likely to be larger than the received from the primary transmitter ($V > \lambda$), thus decreasing the probability of successful PUE attack. But for larger R, the cumulative received power at the secondary from the malicious users may not be sufficient to successfully launch PUE attack.

Based on the result of the simulation in case one and case two , the results prove that when PDF is used with NPCHT, the number of malicious users in the system has a signification impact on the network causing the secondary users suffer from degradation in the quality of their communication due to the transmission from the malicious users , Figure 4.7 summaries the results.

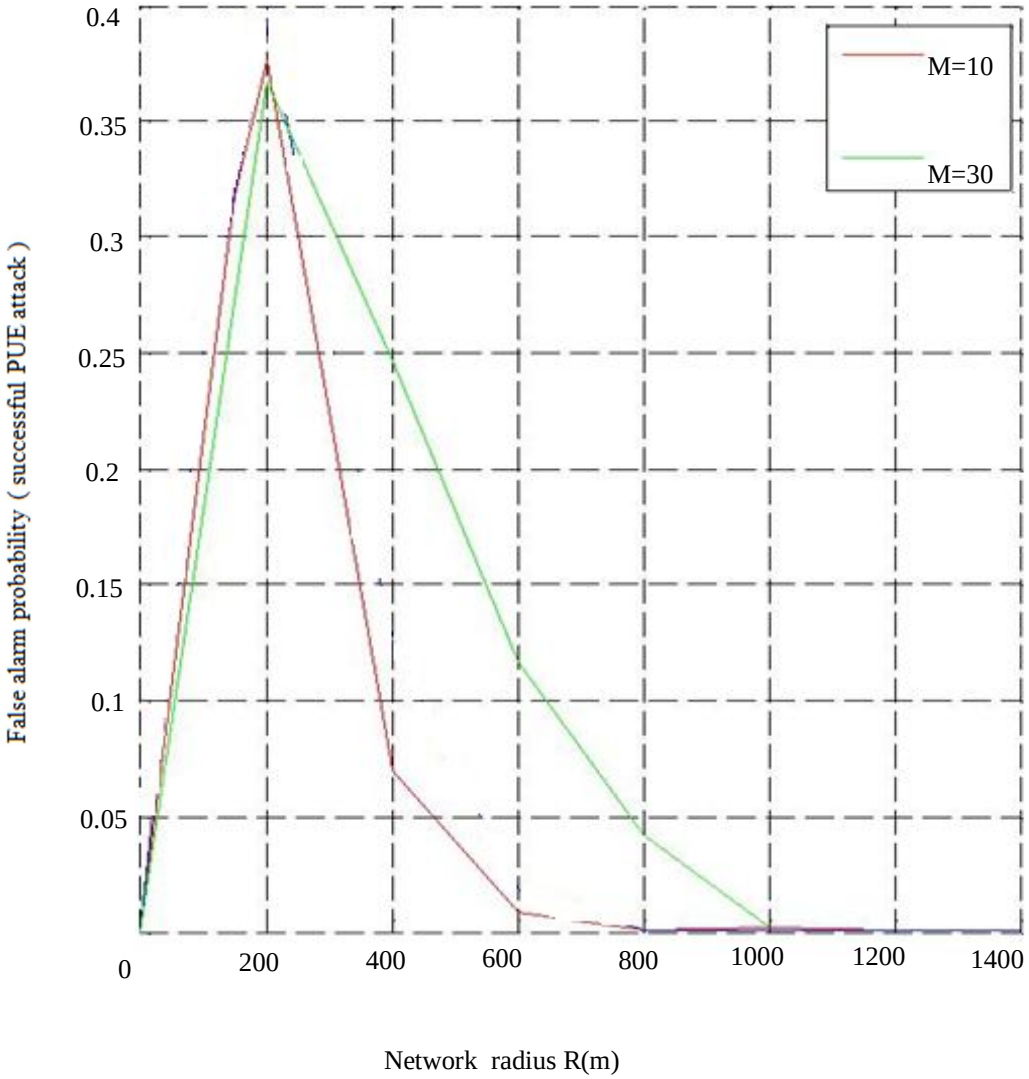
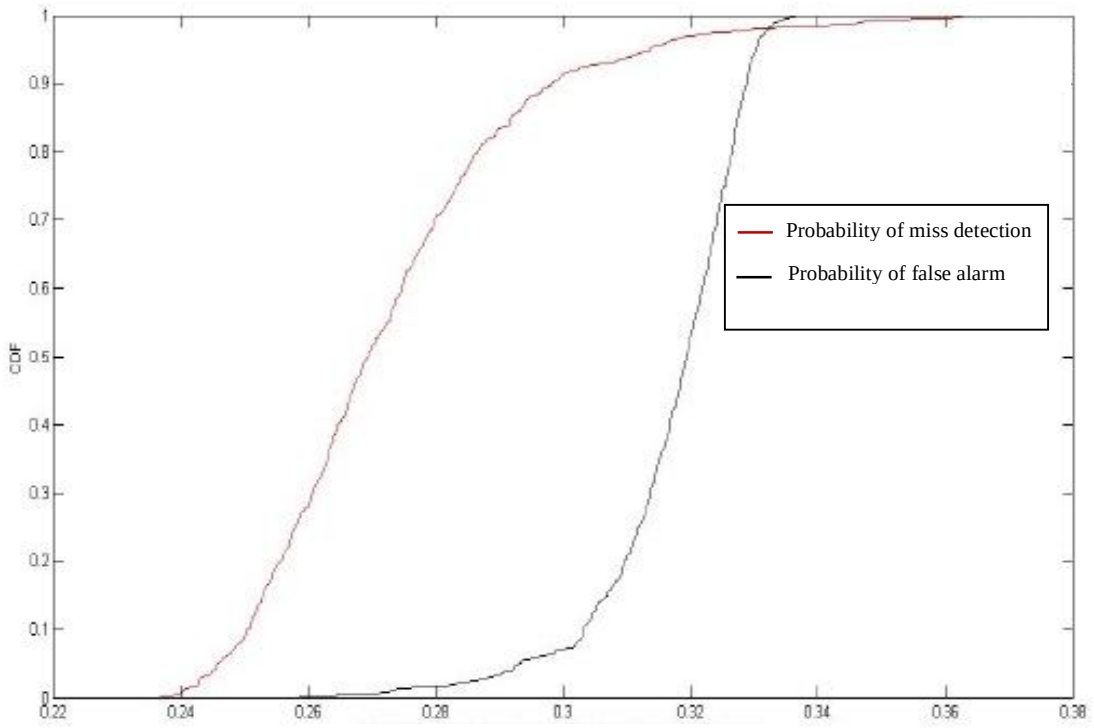


Figure 4.7 False alarm Probability vs. network radius R

Finally by using the cumulative distribution function (CDF) to describe and show how both the false alarms and miss detection probability appears on the same graph.

It is clear from Figure 4.8 below that the CDF plot is non-decreasing and right-continues function as must be meaning that the parameters and assumption are well-chosen and very close to the real-life values.



Probability of miss detection and false alarm

Figure 4.8 CDF vs . probability of miss detection and false alarm

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

This thesis presents an analytical and experimental approach to obtain the PDFs of received powers at the secondary users due to malicious users and also from the primary transmitter in a cognitive radio network.

The PDF obtained was used in Neyman– Person Composite Hypothesis Test to show the probability of false alarm in the network . The results show that the number of malicious users in the system has a great impact on the network causing the secondary user to suffer degradation in the quality of their communication due to the transmission from the malicious users (case one , M= 30, P-D1 – H2 = 0.326) . Also show that there is a range of network radii in which PUE attack are most successful (case one R= 300).

5.2 Future Work

The future work will be as a second stage of this work, in this stage it important to propose a security algorithm for transmitter verification scheme based on two parameters (distance and received signal power level) in order to identify the primary and malicious users.

5.3 References

[1]Wassim ElHajj; Haider Safa; Mohsen Guizani, “Survey of Security issues in Cognitive Radio Network,” journal of internet technology, volume 12 2011.

[2] Zhaoyu Gao; Haojin Zhu; Shuai Li; Suguo Du; Xu Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," Wireless Communications, IEEE , vol.19, no.6, pp.106,112, December 2012.

[3] Romero, E.; Mouradian, A.; Blesa, J.; Moya, J.M.; Araujo, A., "Simulation framework for security threats in cognitive radio networks," Communications, IET , vol.6, no.8, pp.984,990, May 22 2012.

[4] Jin, Z.; Anand, S.; Subbalakshmi, K. P., "Performance Analysis of Dynamic Spectrum Access Networks under Primary User Emulation Attacks," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE , vol., no., pp.1,5, 6-10 Dec. 2010.

[5] "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks," Communications, IEEE Transactions on, vol.60, no.9, pp.2635,2643, september 2012.

[6]Ruiliang Chen; Jung Min Park; Reed, J.H., "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," Selected Areas in Communicatios, IEEE Journal on , vol.26, no.1, pp.25,37, Jan.2008.

[7] Anand, S.; Jin, Z.; Subbalakshmi, K. P., "An Analytical Model for Primary Usr Emulation Attacks in Cognitive Radio Networks," New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on ,vol., no., pp.1,6, 14-17 Oct. 2008.

[8] Jin, Z.; Anand, S.; Subbalakshmi, K. P., "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Communications, 2009. ICC '09. IEEE International Conference on , vol., no., pp.1,5, 14-18 June 2009.

[9] Zesheng Chen; Cooklev, T.; Chao Chen; Pomalaza Raez, C., "Modeling primay user emulation attacks and defenses in cognitive radio networks," Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th Interational , vol., no., pp.208,215, 14-16 Dec.

[10] Caidan Zhao; Wumei Wang; Lianfen Huang; Yan Yao, "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio," Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on , vol., no., pp.1,5, 24-26 Sept. 2009.

[11] Wen-Long Chin; Chun-Lin Tseng; Chun-Shen Tsai; Wei-Che Kao; Chun-Wei Kao, "Channel-Based Detection of Primary User Emulation Attacks in Cognitive Radios," Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th , vol., no., pp.1,5, 6-9 May 2012.

[12] Caidan Zhao; Liang Xie; Xueyuan Jiang; Lianfen Huang; Yan Yao, "A PHY-layer Authentication Approach for Transmitter Identification in Cognitive Radio Networks," Communications and Mobile Computing (CMC), 2010 International Conference on , vol.2, no., pp.154,158, 12-14 April 2010.

[13] Olga León, Juan Hernández-Serrano, Miguel Soriano, Cooperative detection of primary user emulation attacks in CRNs, Computer Networks, Volume 56, Issue 14, 28 September 2012.

[14] Chandrashekar, S.; Lazos, L., "A Primary User authentication system for mobile cognitive radio networks," Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on , vol., no., pp.1,5, 7-10 Nov. 2010.

[15] Feijing Bao; Huifang Chen; Lei Xie, "Analysis of primary user emulation attack with motional secondary users in cognitive radio networks," Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on , vol., no., pp.956,961, 9-12 Sept. 2012.

[16]Min,A.W.;Kyu Han Kim; Shin, K.G., "Robust cooperative sensing via state estimation in cognitive radio networks," New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on , vol., no., pp.185,196, 3-6 May 2011.

[17] Zhou, Xiao; Xiao, Yang; Li, Yuanyuan, "Encryption and displacement based scheme of defense against Primary User Emulation Attack," Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on , vol., no., pp.44,49, 27-30 Nov. 2011.

[18] Yi Tan; Kai Hong; Sengupta, S.; Subbalakshmi, K. P., "Using Sybil Identities for Primary User Emulation and Byzantine Attacks in DSA Networks," Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , vol., no., pp.1,5, 5-9 Dec. 2011.

[19] Fayu Liu; Huifang Chen; Lei Xie; Kuang Wang, "Maximum-minimum eigenvalue detection-based method to mitigate the effect of the PUEA in cognitive radio networks," Wireless Communications and Signal Processing (WCSP), 2011 International Conference on , vol., no., pp.1,5, 9-11 Nov. 2011.

[20] Sorrells, C.; Potier, P.; Lijun Qian; Xiangfang Li, "Anomalous spectrum usage attack detection in cognitive radio wireless networks," Technologies for Homeland Security (HST), 2011 IEEE International Conference on , vol., no., pp.384,389, 15-17 Nov. 2011.

Appendix A

```
%Matlab code for Received power by secondary User due to primary transmitter %
% Primary Transmitter power = 100Kwatts
% Malicious Transmitter Power = 4watts
% Network Radius = 1000m
% Distance between Primary transmitter and good secondary user = 20Km
clear all;
close all;
clc;
num_run = 10000; %testing times
format long;
R =1000; %radius of outer circle, changable 30:30:1500 meter
R0 = 30;%radiu of inner circle
sigma_p = 8; %fixed value
sigma_m = 5.5; %fixed value
Pt = 100e3; %%%%%% Primary transmitting power = 100 Kw
Pm = 4; % malicious user transmitting power
dp = 100e3; %%%%% distance between primary transmitter and secondary user
M = 15; %%%% number of malicious users
A = log(10)/10;
E_p = sigma_p*randn(1,num_run);
Gp = 10.^(E_p/10);
Pr_p_tmp = Pt*Gp*dp^(-2); %r. v. received power
Pr_p = sort(Pr_p_tmp);
```

```
mu_p = 10*log10(Pt) - 20*log10(dp);
P_gama =
(1./(A*Pr_p*sigma_p*sqrt(2*pi))).*exp(-((10*log10(Pr_p)-mu_p)/(sqrt(2)*sigma_p)).^2);
figure(1)
[f2,x2] = hist(Pr_p_tmp,4000);
bar(x2,f2/trapz(x2,f2));
axis([0 1e-4 0 max(P_gama)]);
grid on, hold on;
xlabel('Received power at the secondary receiver: Pr\_p')
ylabel('Probability density function of Pr\_p')
plot(Pr_p, P_gama,'r');
axis([0 1e-4 0 max(P_gama)])
legend('simulation', 'computation' )
```

Appendix B

```
% Matlab code for Received power by secondary User due to Malicious Users %
clear all;
close all;
clc;
num_run = 10000; %testing times
format long;
R =1000; %radius of outer circle, changeable 30:30:1500 meter
R0 = 30;%radius of inner circle
sigma_p = 8; %fixed value
sigma_m = 5.5; %fixed value
Pt = 100e3; %%%%%% Primary transmitting power = 100 Kw
Pm = 4; %malicious user transmitting power
dp = 100e3; %%%%% distance between primary transmitter and secondary user
M = 10; %%%% number of malicious users
A = log(10)/10;
%%%% Random Points within circle with radius R & radius R0
xCoordinates = [];
yCoordinates = [];
n = M;
   while n > 0
x = unifrnd(-R,R,1,1);
y = unifrnd(-R,R,1,1);
norms = sqrt((x.^2) + (y.^2));
```

```
inBounds = find((R0 <= norms) & (norms <= R));
xCoordinates = [xCoordinates; x(inBounds)];
yCoordinates = [yCoordinates; y(inBounds)];
n = M - numel(xCoordinates);
end
%%%%%%%%% Distance between jth malicious user and secondary
user %%%%%%%
for i= 1 : M % number of malicious users
d(i)=sqrt((xCoordinates(i))^2 + (yCoordinates(i))^2);
end
%%%%% Received power at secondary user from malicious users %%%%%%
for kk = 1:num_run
E_j= sigma_m*randn(M,1);
G = 10.^(E_j/10);
for j = 1:M
    P(j) = Pm*(d(j)^(-4))*G(j);
end
  Pr_m_tmp(kk)= sum(P);
end
Pr_m = sort(Pr_m_tmp);
[f1,x1] = hist(Pr_m_tmp,4000);
figure(2)
bar(x1,f1/trapz(x1,f1));
axis([0 max(x1) 0 max(f1/trapz(x1,f1))])
```

```
grid on; hold on;
xlabel('Received power at the secondary receiver from malicious users: Pr\_m')
ylabel('simulated pdf. Probability density function of Pr\_m')
sigma_x_2 = (1/A^2)*(log(mean(Pr_m.^2)) - 2*log(mean(Pr_m)));
mu_x = (1/A)*(2*log(mean(Pr_m)) - 0.5*log(mean(Pr_m.^2)));
P_m_gama =
(1./(A*Pr_m*sqrt(sigma_x_2)*sqrt(2*pi))).*exp(-((10*log10(Pr_m)-mu_x)).^2/(2*si
gma_x_2)); %Equ (11)
plot(Pr_m, P_m_gama,'r-.');
xlabel('Received power at the secondary receiver from malicious users: ')
ylabel('calculated pdf')% axis([0 max(Pr_m) 0 max(P_m_gama)])
legend('simulation', 'computation' )
```

Appendix C

```
% Matlab code for Calculating Probabilities of false alarm and miss detection %
clear all;
close all;
clc;
P_D1_H2=[];
P_D2_H1=[];
num_run = 10000; %testing times
M = 15; %%%% number of malicious users
R =500; %radius of outer circle, changeable 30:30:1500 meter
R0 = 30;%radiu of inner circle
sigma_p = 8; %fixed dB
sigma_m = 5.5; %fixed value dB
sigma_p_2= (10^(sigma_p/10))^2;
sigma_m_2= (10^(sigma_m/10))^2;
Pt = 100e3; %%%%%% Primary transmitting power = 100 Kw
Pm = 4; %malicious user transmitting power 40watts
dp = 100e3; %%%%% distance between primary transmitter and secondary user
A = log(10)/10;
x0 = 1e-9:1e-9:1e-3; %all x axis variables
%%%% Random Points within circle with radius R & radius R0
xCoordinates = [];
yCoordinates = [];
n = M;
```

```
   while n > 0
         x = unifrnd(-R,R,1,1);
         y = unifrnd(-R,R,1,1);
         norms = sqrt((x.^2) + (y.^2));
         inBounds = find((R0 <= norms) & (norms <= R));
         xCoordinates = [xCoordinates; x(inBounds)];
         yCoordinates = [yCoordinates; y(inBounds)];
         n = M - numel(xCoordinates);
     end
%%%%%%%% Distance between jth malicious user and secondary
user %%%%%%%
for i= 1 : M % number of malicious users
    d(i)=sqrt((xCoordinates(i))^2 + (yCoordinates(i))^2);
end
N=500; %N loop numbers
for J=1:1:N
%%%%% Received power at secondary user from primary transmitter %%%%%%
E_p = sigma_p*randn(1,num_run); %E_p dB in lognormal distribution
Gp = 10.^(E_p/10);
Pr_p_tmp = Pt*Gp*dp^(-2); %r. v. received power (watts) r.v.
Pr_p = sort(Pr_p_tmp);
mean_Pr_p=mean(10*log10((Pr_p))); %mean power in dB
mu_p = 10*log10(Pt) - 20*log10(dp); %calculation=mean(Pr_p) in db =mean_Pr_p
mu_p_2 = (10^(mu_p/10))^2;
```

```
P_gama =
(1./(A*x0*sigma_p*sqrt(2*pi))).*exp(-((10*log10(x0)-mu_p)/(sqrt(2)*sigma_p)).^2);
%%%%% Received power at secondary user from Malicious users %%%%%%
for kk = 1:num_run
E_j= sigma_m*randn(M,1);
G = 10.^(E_j/10);
    P = Pm*d.^(-4).*G';
  Pr_m_tmp(kk)= sum(P);
end
Pr_m = sort(Pr_m_tmp);
sigma_x_2 = (1/A^2)*(log(mean(Pr_m.^2)) - 2*log(mean(Pr_m)));
mu_x = (1/A)*(2*log(mean(Pr_m)) - 0.5*log(mean(Pr_m.^2)));
P_m_gama =
(1./(A*x0*sqrt(sigma_x_2)*sqrt(2*pi))).*exp(-((10*log10(x0)-mu_x)).^2/(2*sigma_x
_2)); %Equ (11) same x0
z= P_m_gama./P_gama;
lambda=2;
index= max(find(z >= lambda));
x_threshold = x0(index);
t0=1e-9:1e-9:x_threshold; %t0 is from 0 to lamdba
P_D2_H1_tmp = trapz(t0,P_gama(1:index));
P_D2_H1=[P_D2_H1;P_D2_H1_tmp];
tt_size= round((1e-3-x0(index))/1e-9); %tt is index from lambda to right end value
tt = x0(index+(1:1:tt_size));
```

```
P_D1_H2_tmp = trapz(tt,P_m_gama(index+(1:1:tt_size)));
P_D1_H2 =[P_D1_H2; P_D1_H2_tmp];
% close all
end;
P_D1=sort(P_D1_H2);
P_D2=sort(P_D2_H1);
plot(P_D1, (0:1/N:1-1/N), 'r', P_D2, (0:1/N:1-1/N),'k');
xlabel('Probability of miss detection and false alarm M=10, R=700m, R_0=30m ')
ylabel('CDF')
legend('P\_D1', 'P\_D2' );
MeanP_D1=mean(P_D1_H2)
MeanP_D2=mean(P_D2_H1)
figure (2)
plot(P_D1_H2)
xlabel('Number of simulation times ')
ylabel('Probability of False alarm')
figure (3)
plot(P_D2_H1)
xlabel('Number of simulation times ')
ylabel('Probability of Miss Detection')
```