Security Analysis in Cognitive Radio Network

Supervisor: Dr. Amitabha Chakrabarty
Co- Supervisor: Moin Mostakim

Fahia Nasnin 13101138
Mst. Najia Islam 13101142

Department of Computer Science and Engineering

Submitted on: 18th April, 2017

Declaration of Authorship

We, hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This Thesis, neither in whole or in part, has been previously submitted for any degree.

Signature of Supervisor

Dr. Amitabha Chakrabarty

Signature of Author

Fahia Nasnin

Signature of Author

Mst. Najia Islam

We would like to dedicate this thesis to our loving parents .....

Abstract

In wireless communication system Cognitive Radio(CR) is a structure that can gives an intelligent privileges to communicate over internet. Cognitive Radio(CR) intelligently allows user to use free spectrum. It is dynamically configured and it allows more user in wireless network. IEEE 802.22 standard cognitive radio (CR) was developed first. Due to spectrum sensing, sharing, mobility there is a issue in security. Ensuring security and using spectrum efficiently is challenging. In this paper, the security threats of cognitive radio network are briefly discussed. After explaining some of possible attack, we have emphasized on Primary user emulation attack(PUEA). With the existing system model the probability of false alarm and miss detection has been studied. MATLAB R2010a tool has been used to analyze the model. This pa- per we have shown Neyman-Pearson Criterion to detect PUEA and a for different malicious users status to create false alarm and miss detection

Acknowledgements

First of all, we would like to express our deepest sense of gratitude yo almighty Allah. We write this acknowledgement with great honor, pride and pleasure to pay our respects to all who enabled us either directly or indirectly in completing this thesis. We would like to show our gratification to our Supervisor Amitabha Chakrabarty for being constant source of inspiration, valuable guidance and constant encouragement to us especially for solving the problems that we have encountered while working on this thesis. We also like to thank our Co-Supervisor Mr. Moin Mostakim for his valuable guidance.

Contents

Declaration of Authorship iii

Abstract vii

Acknowledgements ix

1 **Introduction 1**

1.1 Introduction to Cognitive Radio Network. 1

1.2 Problem Definitions. 2

1.3 Motivation. 3

1.4 Thesis Outline. 3

2 Literature Review 5

2.1 Cognitive Radio. 5

2.2 Functionality of Cognitive Radio Network. 6

2.2.1 Spectrum Sensing. 6

2.2.2 Spectrum Decision. 6

2.2.3 Spectrum Sharing. 6

2.2.4 Spectrum Mobility. 7

2.3 Cognitive Radio Network Architecture. 7

2.3.1 Centralized cognitive network. 8

2.3.2 Distributed cognitive network. 8

2.3.3 Licensed band operation. 9

2.3.4 Unlicensed band operation. 9

2.3.5 Cognitive radio network access. 9

2.3.6 Cognitive radio ad-hoc access. 9
2.3.7 Primary network access. 9
2.4 Security issues in cognitive radio. 10

3 **Overview of security Threats in Cognitive Radio Networks** **11**
3.1 Security and its requirements. 11
Primary User Emulation Attack (PUE or PUEA). 11
Overlapping secondary user attack. 13
3.1.1 Link Layer. 13
Biased Utility Attack. 14
False feedback attack. 14
Dos Attack. 14
3.1.2 Network Layer. 14
Hole Attack. 15
Ripple effect attack. 15
3.1.3 Transport Layer. 15
Key Depletion Attack. 16
3.1.4 Application Layer. 16
3.2 Security Mechanism. 16
3.2.1 Physical Layer. 17
Range based localization. 17
Range free Localization. 17
3.2.2 Link Layer. 17
3.2.3 Network Layer. 18
3.2.4 Transport Layer. 18
3.2.5 Application Layer. 19
3.3 Summary. 19

4 **Methodology & Design** **21**
4.1 Introduction. 21

4.1.1 Selfish PUE attacks. 21

4.1.2 Malicious PUE attack. 22

4.2 Primary Exclusive Region. 22

4.3 System Model of CRN. 22

4.4 Analytical Model. 23

4.5 Neyman-Pearson Criterion for Detecting PUEA. 24

4.5.1 Probability of False Alarm. 25

4.5.2 Probability of Miss Detection. 25

4.6 Work Flow. 26

5 Observations & Result Analysis 27

5.1 Simulation Results & Observations. 27

5.1.1 Received Power. 27

5.1.2 Miss Detection. 30

5.1.3 False Alarm. 31

5.1.4 Average of miss detection & false alarm. 33

5.2 Our Proposed Model. 34

5.2.1 Observations from our system. 35

6 Conclusion 37

List of Figures

2.1 Cognitive Cycle. 6

2.2 Basic Architecture of Cognitive Radio Network (Khare and Saxena, 2013). 8

3.1 Primary User Jamming Attack. 12

3.2 Primary User Emulation Attack. 12

3.3 Overlapping Secondary user attack. 13

3.4 Intrusion Detection at network layer. 18

4.1 System Model. 23

4.2 Our work flow. 26

5.1 PDF of received power at the secondary receiver. 27

5.2 PDF of received power at the secondary receiver from malicious user 28

5.3 Probability of Miss Detection. 30

5.4 Probability of False Alarm. 31

5.5 Probability of Miss Detection & False Alarm. 33

5.6 Proposed System Model. 34

5.7 Average probability for miss detection and false alarm. 35

List of Abbreviations

CR	***C**ognitive **R**adio*
PUE	***P**rimary **U**ser **E**mulation*
PU	***P**rimary **U**ser*
SU	***S**econdary **U**ser*
PER	***P**rimary **E**xclusive **R**egion*
QoS	***Q**uality **o**f **S**ervice*
DoS	***D**enial **o**f **S**ervice*
PDF	***P**robability **D**ensity **F**unction*
SSL	***S**ecure **S**ockets **L**ayer*
RF	***R**adio **F**requency*

Chapter 1

Introduction

1.1 Introduction to Cognitive Radio Network

For communication and networking it’s important to focus on utilizing the bandwidth and free channel. But tradition networking system is failing to fulfill this need to utilize empty channel and use bandwidth. Therefore it’s a challenge to fix this

. IEEE 802.22 was established first to develop the concepts of Cognitive radio network (Mitola and Maguire, 1999). Cognitive radio is software defined intelligence system that can perform and settle users demand according to free spectrum status. This is a dynamic spectrum access model to sense the free spectrum to assign the free spectrum of unlicensed user if licensed users are not present. Traditional regulatory structures have been built for an analog model and are not optimized for cognitive radio. The location of primary users remain in database of licensed users so that CR can identify available channels. Spectrum sensing observes the spectrum and identifies occupied channels. Cognitive radio chooses different free spectrum at different time. As spectrum availability changes, the network adapts to prevent interference with licensed transmissions. In traditional networking system there is spectrum short- age problem. Therefore, Cognitive Radio (CR) is introduced to allow the unlicensed users along with licensed users to maximize the spectrum utilization. In that case, ensuring security is one major challenge and security issues are classified in different types of attack. Primary user Emulation attack (PUEA) is one of them. Our research work is about security analysis of CR network and its performance when malicious user (MU) mitigate primary user’s signal. However, our main objective is to focus on how PUEA affects the bandwidth utilization of CR network.

1.2 Problem Definitions

In cognitive radio networking security analysis is one major activities. Hence, there is dynamic frequency selection to access free spectrum therefore there is more security threats in CR models. There are so many attacks can be occurred in cognitive net- working and QoS (Quality of service) can be affected by CR models weakness aspects.

Some attacks are DOS attacks, key depletion attacks, Hole attacks, Ripple effect attack, False feedback attack, PUEA attack and also is attack can be happened in physical layer and link layer. Among all attacks we are considering PUEA as one of the most security threat. If SU cannot access the spectrum then the whole purpose to implement CR network will fail to reach its goal. Malicious users and its false alarm rate, miss detection mitigation can be a solution to overcome PUEA.

1.3 Motivation

The wireless communications evolution followed in recent years has an intrinsic problem: the growing scarcity of spectrum. With the Cognitive Radio (CR) definition, it is attempted to solve this problem by using the spectrum dynamically.

CR allows efficient use of available spectrum by defining of two types of users in wireless networks: licensed and unlicensed users. An unlicensed user (also called Secondary User (SU)) can use the spectrum if it is not being used at that time by licensed users (also called Primary User (PU)). When the licensed user appears to use the spectrum, unlicensed user must find another spectrum to use. Despite cognitive radio is an active field of research, security aspects have not yet been fully explored even though security will likely play a key role in the long-term commercial viability of the technology. The security paradigms are often inherited from classic networking and do not fit with the specifications of cognitive radio networks.

Although there is not lot of literature about this topic, lately, researchers has seen that cognitive radio has special characteristics that makes its own security an interesting research field, since more chances are given to attackers by cognitive radio technology compared to general wireless network. At this present time, no such secure system exists for cognitive radio networks.

1.4 Thesis Outline

Chapter1 gives a brief overview of cognitive radio network, our motivation and on what problem we have done our research. Chapter2 discusses the literature review and background study of our project. Here the functionalities and the basic architecture of cognitive radio have been discussed. Chapter3 discusses security threats in cognitive radio network. We have discussed about layer based security threats. Chapter4 discusses the methodology and design based on what we have progressed our research. There is brief about Neyman-Pearson Criterion for detecting PUEA and our system work flow. Chapter5 focuses on observation & simulation results. We have also discussed about our proposed model and observation from it. Chapter6 ends our paper with conclusion and proposed future works for the system.

Chapter 2

Literature Review

2.1 Cognitive Radio

In 1999 the term cognitive radio was officially used by Mitola and Maguire (Mitola and Maguire,1999). It is an intelligent network that builds its communication through spectrum. Spectrum scarcity is recently a vital problem in wireless communication. In cognitive radio network, the radio frequency is the media to make connection between transmitter and licensed secondary user [SU]. Spectrum mobility allow them to change the spectrum and spectrum sharing allow unlicensed user to use spectrum if Primary user [PU] is not present in channel. Moreover spectrum sensing gives a signal to Secondary user about the presence of Primary user. Without disturbing the Primary user when secondary user get information that one channel is empty then they are allowed to access the channel. In this case there are many security issues. When unlicensed secondary user got access in spectrum then they may behave malicious user [MU] that is not acceptable. Malicious user can behave like primary user to occupy the full spectrum and send false alarm to other secondary user. After getting the false alarm Secondary user cannot detect that this signal has sent by malicious user. Therefore SU can't utilize spectrum. It is a big challenge to mitigate malicious user attack.

2.2 Functionality of Cognitive Radio Network

The four main functions of cognitive radio are as follows:

2.2.1 Spectrum Sensing

Spectrum sensing allows the CR users to adapt to the environment by detecting spectrum holes (white spaces) without causing interference to the primary network. Spectrum sensing is done by secondary user.

2.2.2 Spectrum Decision

*A*fter sensing the frequency spectrum and identifying the "white spaces" cognitive radio user should decide which frequency spectrum is the best to use (Alahmadi et al., 2014).

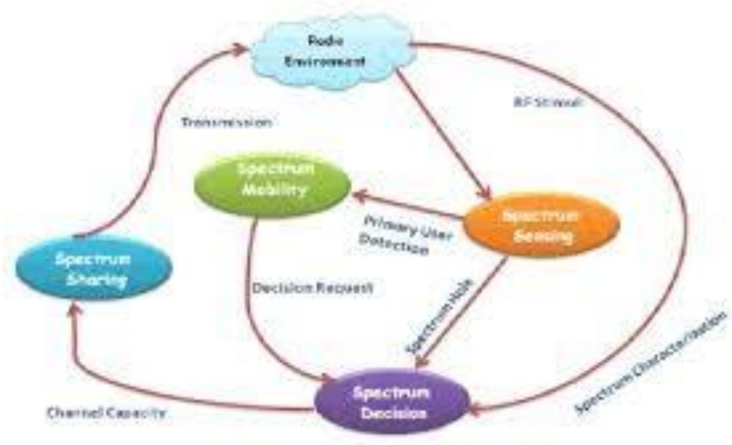

Figure 2 Cognitive Cycle.

FIGURE 2.1: Cognitive Cycle

2.2.3 Spectrum Sharing

Spectrum sharing cognitive radio networks allow cognitive radio users to share the spectrum bands of the licensed-band users. However, the cognitive radio users have to restrict their transmit power so that the interference caused to the licensed-band users is kept below a certain threshold.

2.2.4 Spectrum Mobility

Process by which a cognitive-radio user changes its frequency of operation. Cognitive- radio networks aim to use the spectrum in a dynamic manner by allowing radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during transitions to better spectrum (Liu, Ning, and Dai, 2010).

Hence, the opportunity of spectrum sensing, sharing and mobility pave the way to CR users, it is also difficult to detect malicious user who wants to use the whole spectrum. When unlicensed secondary user got accessed in available spectrum then they may behave malicious user [MU] that is not acceptable in CR network. Malicious user can mitigate primary user's signal to occupy the full spectrum and send false alarm to other secondary user. After getting the false alarm Secondary user cannot detect that this signal has sent by malicious user. Therefore SU can't utilize spectrum. It is a big challenge to mitigate malicious user attack. In this paper, we have also discussed about some attacks model. We can categorize the security threats upon cognitive radio network in two ways: threats to the cognitive user and threats to primary user. We can categorize the security threats upon cognitive radio network in two ways: threats to the cognitive user and threats to primary user.

2.3 Cognitive Radio Network Architecture

This section provides a detailed description of the CR network architecture. According to the architecture, cognitive radio networks can be classified as Centralized or Distributed networks. According to operations point of view, cognitive radio networks can be classified as licensed band operation and unlicensed band operation. Cognitive radio network can be categorized as CR network access, CR ad-hoc access, and primary network access.

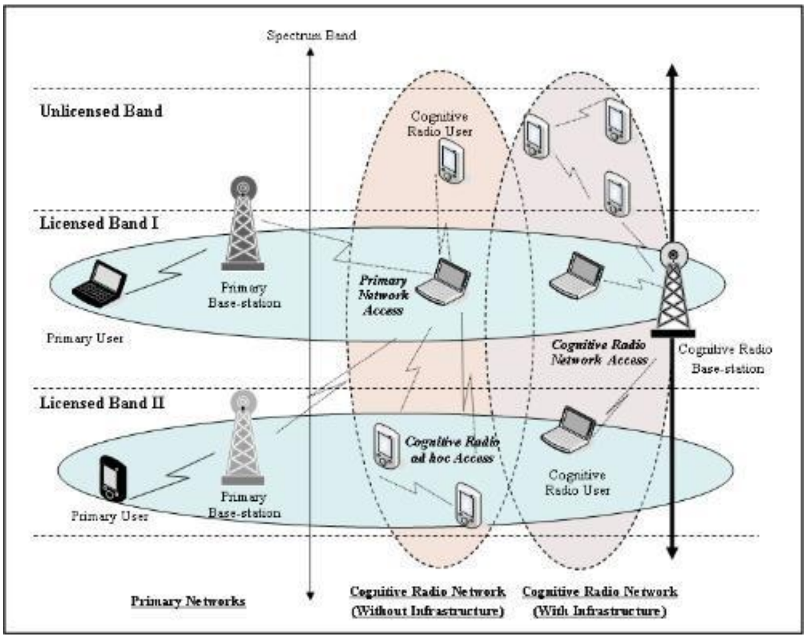

FIGURE 2.2: Basic Architecture of Cognitive Radio Network (Khare and Saxena,2013)

2.3.1 Centralized cognitive network

As shown in Fig. 2.2, the network is infrastructure oriented. A base station is used to manage each CR user in the network. Each user are directly accessed by the base station and the station controls the medium access and the secondary users in the network.

2.3.2 Distributed cognitive network

As shown in Fig. 2.2, the CR users communicate with each other in an ad-hoc manner. Information is shared directly between the secondary users who fall within the communication range; otherwise information is shared over multiple hops.

2.3.3 Licensed band operation

The spectrum channel is allocated for the primary users in the network. Unlicensed user can use the channel if the primary user doesn’t occupy it already. CR user must vacate the licensed band if the primary user reappears then and move to another vacant spectrum band. Although there is not lot of literature about this topic, lately, researchers has seen that cognitive radio has special characteristics that makes its own security an interesting research field, since more chances are given to attackers by cognitive radio technology compared to general wireless network.

2.3.4 Unlicensed band operation

The unlicensed users have the same right to use the unlicensed band. They don’t have to free the spectrum for the primary users.

2.3.5 Cognitive radio network access

As shown in Fig. 2.2, the cognitive users can share information with their base station on the licensed as well as the unlicensed spectrum band.

2.3.6 Cognitive radio ad-hoc access

As shown in Fig. 2.2, the cognitive users in the network can share information with each other in ad-hoc manner on both the licensed and unlicensed spectrum band.

2.3.7 Primary network access

As shown in Fig. 2.2, the CR users can also communicate with the primary base station on the licensed spectrum band with an adaptive medium access control protocol.

2.4 Security issues in cognitive radio

In comparison with traditional wireless networks, there are more chances open to attackers in cognitive radio technology. As a result, security in cognitive radio networks has become a challenging task. Quality of service (QoS) provisioning and security requirement for the entire network may be adversely affected by these weak- nesses and vulnerable aspects, introduced by the nature of cognitive radio (Zhang and Li,2010). Many general schemes proposed in the past cannot satisfy such special network requirements, since the spectrum is used dynamically in cognitive radio. Cognitive radio network is similar to wireless network. Since the nature of the wire- less media is open air, it is more vulnerable to attacks as compared to that of wired network.

Chapter 3

Overview of security Threats in Cognitive Radio Networks

3.1 Security and its requirements

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 networks because of the open air nature of wireless media (Haykin,2005). 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 cognitive radio deals with the use of unused spectrum in an opportunistic manner with the unscheduled appearance of the primary users. In the following section we consider each protocol layer and the attacks associated with it (Zhang and Li,2010).

Primary User Emulation Attack (PUE or PUEA)

A malicious user can imitate the primary user then secondary user in the network believes that the primary user present in the network. Therefore they terminate their

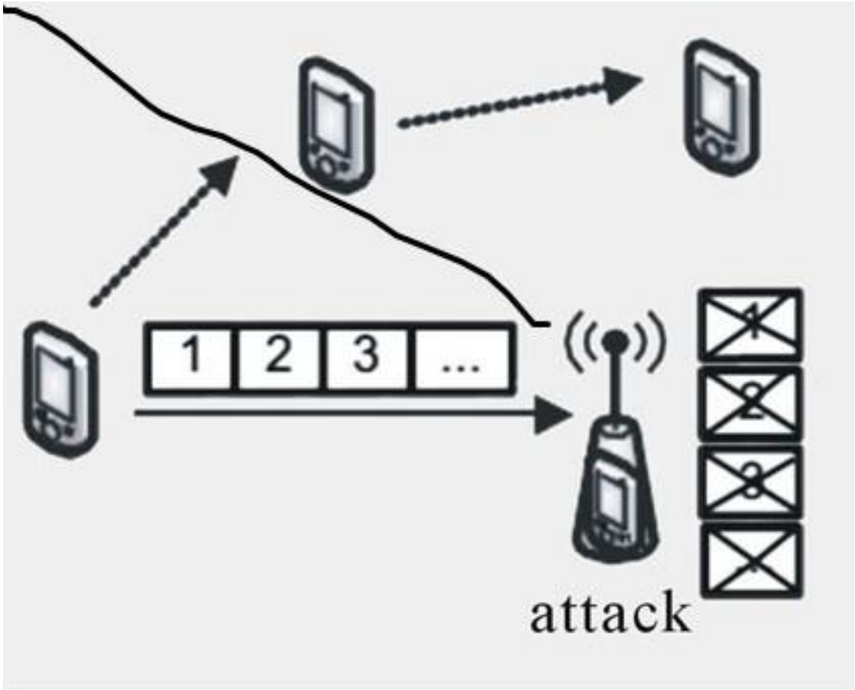

FIGURE 3.1: Primary User Jamming Attack

communication and release the spectrum. This imitation of primary user can terminate the using of secondary user (Zhang and Li,2010).

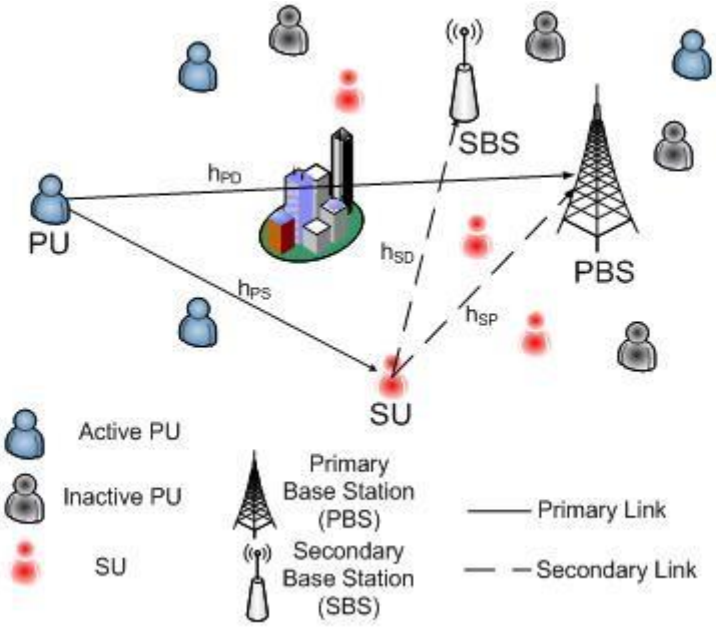

FIGURE 3.2: Primary User Emulation Attack

Overlapping secondary user attack

In a same PER there could be multiple users who needs bandwidth .The transmissions from malicious entities in one network can occur interference to the primary and secondary users of the other network. Since the malicious users or attackers may not be under the direct supervision of the secondary base station of the victim network, this type of attack is very difficult to prevent (Mathur and Subbalakshmi, 2007).

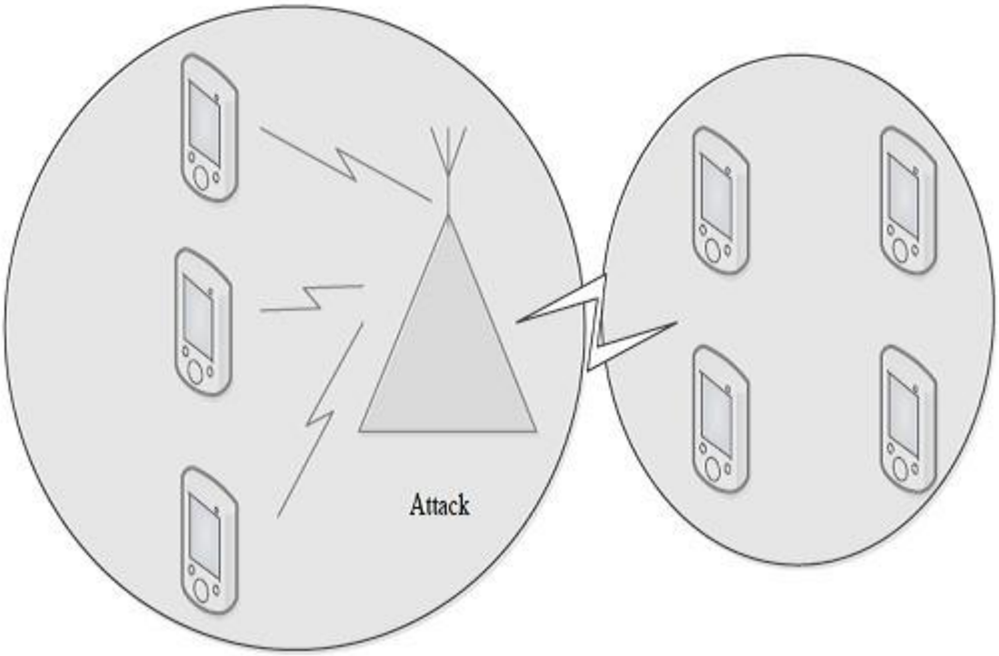

FIGURE 3.3: Overlapping Secondary user attack

3.1.1 Link Layer

Link layer is the second layer of networking model. This layer is responsible for transfering of data from one node to other in single node. It confirms that onitial connection has been set up, divides output data into 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.

Biased Utility Attack

A malicious secondary node may try to change the parameters of utility function so that malicious user can increase its own bandwidth and use the spectrum for a long time. As a result of this the good secondary user is deprived of available bandwidth and cannot utilize the channel.

False feedback attack

In a decentralized cognitive network, secondary user may make wrong decision due to false feedback from one malicious secondary user. This can cause severe interference to the licensed user. For an example, a malicious node in the network may not tell the other secondary users in the network about the reappearance of the licensed user, who cannot sense the information due to fading or long distance. Such an at- tack is called as false feedback attack (Mathur and Subbalakshmi,2007; Zhang and Li,2010).

Dos Attack

The main objective of malicious node is to prevent good secondary nodes from accessing the vacant radio frequency band. An attacker may try to jam a network and thus reduce a legitimate user's bandwidth, prevent access to a service, or disrupt service to a specific system or a user (Weifang,2010).

3.1.2 Network Layer

The main objective of network layer is end-to-end packet delivery. Functions of the network layer are routing, flow control, ensures 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 in the spectrum is called a hole. There are various types of hole attacks such as Black hole attack, Gray hole attack, Worm hole attack. Black hole attack is defined as attack in which the malicious node attracts/request packets 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 hole attack is defined as the attack in which the malicious user uses two pairs of nodes and there exist a private connection between the two pairs. The worm hole attack is a considered as dangerous attack amongst all. It can pre- vent route discovery where the source and the destination are more than two hops away. Protocols like Ariadne or secure AODV prevents such types of (Mathur and Subbalakshmi, 2007; Zhang and Li,2010).

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 (Le, Chin, and Lin,2016). This can disrupt the traffic for long time.

3.1.3 Transport Layer

The transport layer is responsible for transfer of data between two end hosts. It is responsible for flow control, congestion control and end-to-end error recovery. Some attacks occur during session setup, while others happen during the period of sessions. Following are the attacks associated with this layer (Mathur and Subbalakshmi,2007; Zhang and Li,2010).

Key Depletion Attack

Sessions in cognitive networks last only for a short period of 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 cognitive networks are large, large numbers of keys are established, thereby increasing the probability of using the same key twice. Key repetitions can be exploited to break the underlying cipher system. The WEP and TKIP protocols used in IEEE 802.11 are more prone to key repetition attacks (Mathur and Subbalakshmi,2007; Zhang and Li,2010).

3.1.4 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 layers. As a result, any attack on physical, link, network or transport layers may have an adverse effect on the application layer.

3.2 Security Mechanism

In this section we describe the security mechanisms and the architecture at different protocol layers.

3.2.1 Physical Layer

The security concerns mainly lies in the process of spectrum sensing. Factors such as, location of the transmitter, received signal strength can be used to identify attackers at this layer. In order to decide the location of the CR users in the network, Localization techniques can be used. There are various localization techniques which are listed as follows.

Range based localization

The travel time of the signal from source to destination is used to calculate the position.

Range free Localization

First we calculate the total number of hops in the network and then we convert it into physical distance.

In order to locate the transmitter Received signal strength can also be used. In practice location information and the received signal strength are used together to detect the intruder. Two schemes based on RSS are used to detect the intruder: Distance ratio Test (DRT), Distance Difference Test (DDT) (Zhang and Li,2010).

3.2.2 Link Layer

MAC address is examined at this layer. Each channel has its own schedule for transmission. Unusual activity results when an adversary does not follow its schedule. Also the average packet rate is monitored. If the packet rate is higher and last for long period, then there is a possibility of some unusual activity (Zhang and Li, 2010).

3.2.3 Network Layer

Routing information can be encrypted using cryptographic protocols and authentication can be used to confirm the integrity of routing table and identity of the nodes. The scheme of watch dog can be implemented to monitor the data packets passing through the network (Zhang and Li,2010). For example, Fig. 3.5 shows the normal and abnormal behavior at the network layer. In case of normal behavior, the packets are passed from node1 to node2 and then to node3. In abnormal behavior node2 acts as a malicious node, that is it will either change the contents of the packets or just drop the packet after receiving from node1. As a result node 3 will get the altered packet or will never get the packet. The concept of watch dog is used to buffer the packet at node1. Node3 after receiving the packet will compare it with the buffered one. If there is any difference, it is regarded as abnormal activity and a log is created for further processing (Mathur and Subbalakshmi,2007).

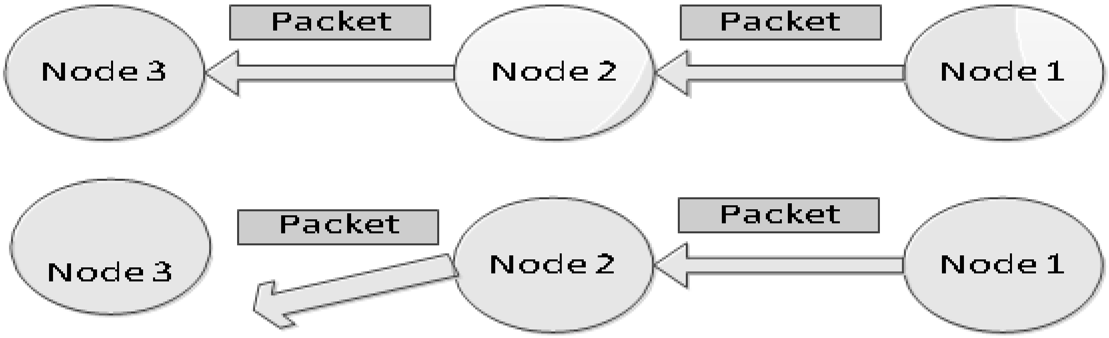

FIGURE 3.4: Intrusion Detection at network layer

3.2.4 Transport Layer

The round trip time and the number of frequent retransmissions are monitored. If the retransmissions are occurring very frequently or the round trip time is longer than the average value, then we can say that there is some unusual activity in the network. An intrusion detection scheme based on RSS and RTT detection can be used to detect attacks at this layer (Zhang and Li, 2010).

3.2.5 Application Layer

Since the activity of other protocol layers may affect each other, so at this layer the multiple protocol layers can be monitored or data can be analyzed. For example if an application creates many connections without any real operations, such abnormal activity can be easily detected at application layer (Zhang and Li, 2010).

3.3 Summary

In this chapter we discuss about the security and its requirement in CR networks. This chapter relates to the characteristics of different protocol layers. We have also discussed the security mechanisms for different protocol layers.

Chapter 4

Methodology & Design

4.1 Introduction

Security issues in cognitive radio networks are drawing more attention in recent years. Major issue associated with spectrum sensing is, how accurately it can differentiate incumbent signals from secondary user signals an attacker can easily exploit the spectrum sensing process. For example, an attacker may imitate as an incumbent transmitter by transmitting unrecognizable signals in one of the licensed bands, thus preventing other secondary users from accessing that band (Chen and Park, 2006).

Primary user emulation (PUE) attack is considered to be one of the severe threats to cognitive radio systems. It poses a great threat to spectrum sensing. In this attack, a malicious node transmits signals whose characteristics emulate those of incumbent signals. There are two types of behavior associated with the primary user emulation attack, which are discussed as follows (Chen and Park, 2006).

4.1.1 Selfish PUE attacks

When attacker wants to maximize its using bandwidth and malicious node identifies vacant band, it will prevent other secondary users from using that band by transmit- ting signals that resembles the incumbent signals (Chen and Park, 2006).

4.1.2 Malicious PUE attack

The main objective is to create obstacle to the secondary users from accessing and using vacant spectrum bands. Malicious attacker does not necessarily use vacant bands for its own communication purposes. It is essential to identify that in PUE attacks, malicious nodes only transmit in vacant bands (Chen and Park, 2006).

4.2 Primary Exclusive Region

Primary exclusive region (PER) is one of the research area to mitigate attacks. It makes a safe zone for primary receivers. The secondary network must be accessed outside network. The exclusive zone is also called as keep-out region. It gives primary receiver a protection area. It is a way of imposing a certain distance on cognitive users from the primary user thereby reducing interference to the primary receiver. Within this PER cognitive users are not allowed to transmit. This type of deployment scheme is suitable to a broadcast network. For an instance, network in which there is one primary transmitter communicating with multiple primary receivers. TV network or the downlinks in the cellular network are the good examples of a broadcast network. In such type of networks, primary receivers may be passive devices. Such a primary-exclusive region has been proposed for the upcoming spectrum sharing of the TV band. The secondary users are randomly and uniformly distributed within a network radius from the primary transmitter, outside the PER.

4.3 System Model of CRN

Following assumptions are made for this system model (Jin, Anand, and Subbalakshmi, 2009a). There are M malicious users in the system and they transmits at power P_a. The distance between primary transmitter & all the users is D_p and transmits at power P_t. The position of secondary user is at the center of the exclusive region. Malicious users are uniformly distributed in circular region of radius R and are sta-

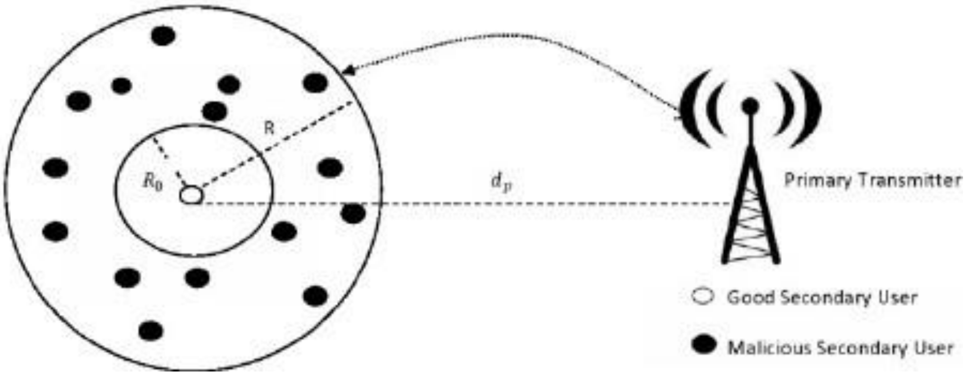

FIGURE 4.1: System Model

tistically independent of each other. Co-ordinates of primary transmitter are known to all the users and are fixed at (r_pt, θ_pt). The transmission from primary transmitter and malicious users undergo path loss and log normal shadowing. The path loss exponent chosen for transmission from primary transmitter is 2 and from malicious user are 4. No malicious users are present within a circle of radius R_0, called as the exclusive radius from secondary user. There is no co-operation between the secondary users (Jin, Anand, and Subbalakshmi,2009a).

4.4 Analytical Model

The calculation of the received signal at the secondary user due to transmission by the primary and the malicious user is done to find out probability density function. We consider, M malicious users at ($\mathbf{r_j}$,θ_j). $1\leq \mathbf{j} \leq$M. The PDF of $\mathbf{r_i}$ is given as (Jin, Anand, and Subbalakshmi, 2009a),

$$p(r_j) = \frac{2r_j}{R^2 - R_0^2}$$

θ_j is uniformly distributed in (π, π)(Jin, Anand, and Subbalakshmi, 2009a). The power that the secondary users receive from primary transmitter is,

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

where

$$G_p{}^2 = 10^{\frac{s_p}{10}}$$

Since P_t and d_p are fixed the probability density function(Jin, Anand and Subbalakshmi, 2009a) of p^p_r is

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

where $A = \frac{\ln 10}{10}$ *and*

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

The total received power at the secondary user from all the malicious users is given by,

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

D_j is the distance between the jth malicious user and the secondary user. G_j^2 is the shadowing between the jth malicious user and the secondary user.

4.5 Neyman-Pearson Criterion for Detecting PUEA

Based on the measured values of received signal strength, we have considered two hypotheses: M1- that the identified signal belongs to primary user and M2-that the identified signal belongs to malicious user or the attack is in progress. Based upon the observations there may be two types of threats experienced by the secondary user in this hypothesis (Jin, Anand, and Subbalakshmi, 2009b):

4.5.1 Probability of False Alarm

When the secondary user cannot recognize the transmission of the malicious user and thinks that primary user is transmitting.

4.5.2 Probability of Miss Detection

When the secondary user cannot recognize the transmission of the primary user and thinks that malicious user is transmitting.

4.6 Work Flow

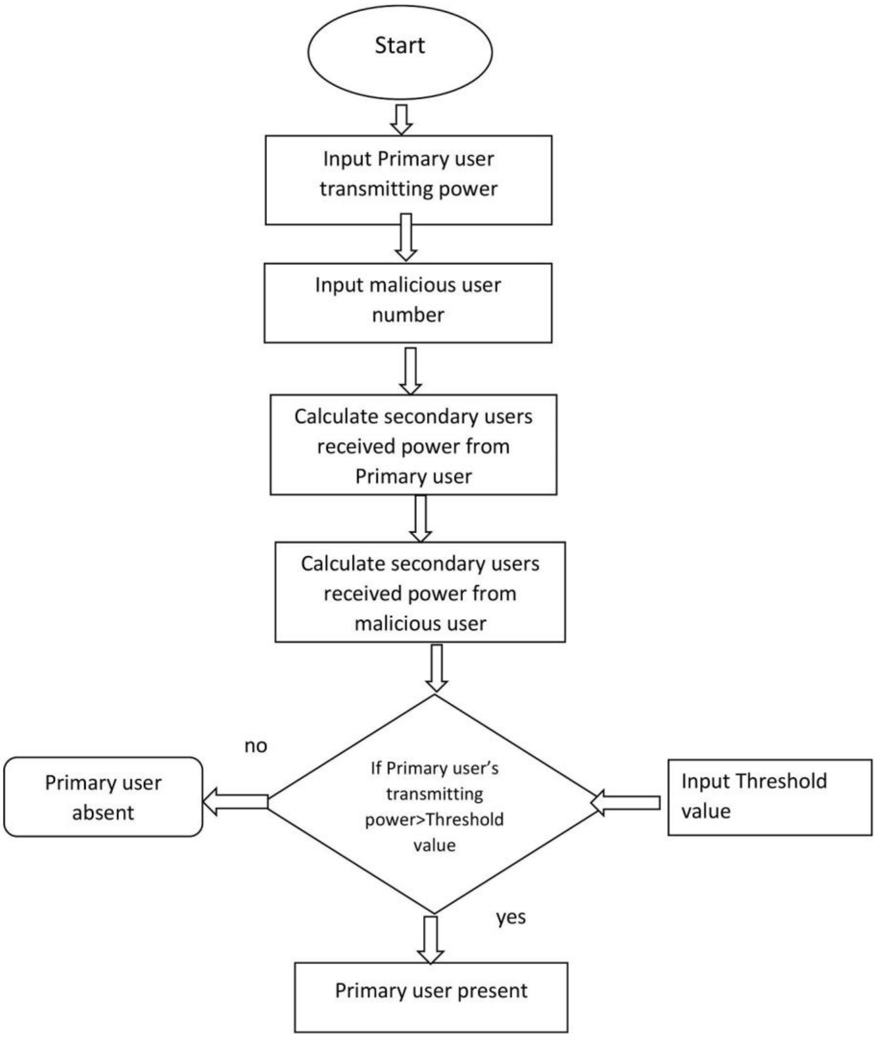
Start
Input Primary user transmitting power
Input malicious user number
Calculate secondary users received power from Primary user
Calculate secondary users received power from malicious user
no
Primary user absent
If Primary user's transmitting power>Threshold value
Input Threshold value
yes
Primary user present

FIGURE 4.2: Our work flow

Chapter 5

Observations & Result Analysis

5.1 Simulation Results & Observations

5.1.1 Received Power

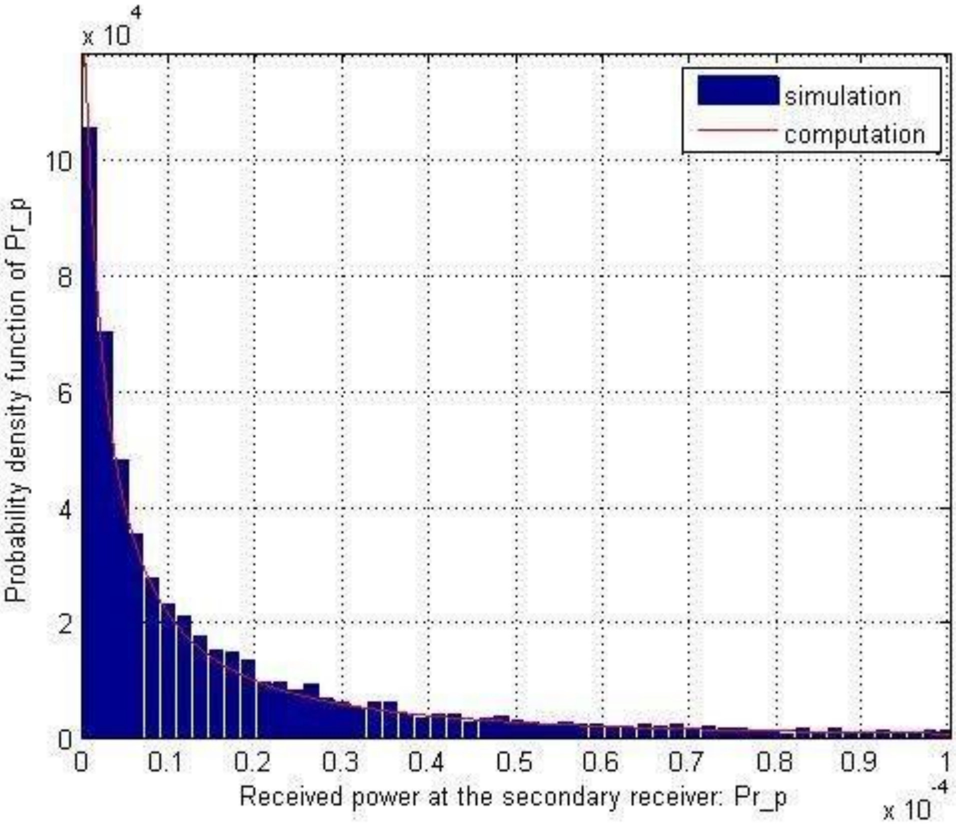

FIGURE 5.1: PDF of received power at the secondary receiver

Fig. 5.1 shows the probability density function (PDF) of received power at the unlicensed user. This graph is plotted for the value when there is one primary transmitter in channel. and the primary transmitter is at 150 km away from outer circle . The primary transmitter is at distance 100Km, Primary transmitter power P_t =500Kw, σ_m = 4.5dB, σ_p= 8dB, R_0= 30m, R= 1000m, P_m= 4W. Here PDF is calculated for 1000 simulation times and it is plotted in a graph both simulated and

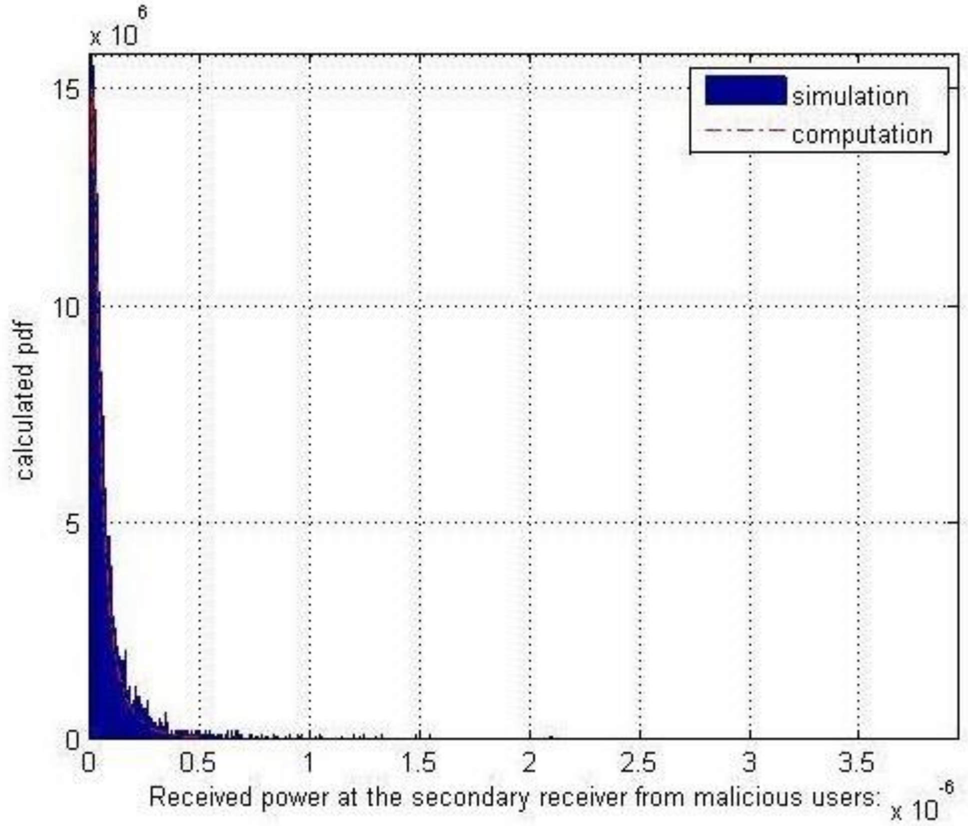

FIGURE 5.2: PDF of received power at the secondary receiver from malicious user

Fig. 5.2 shows the Probability Density Function of the received power at the secondary user due to malicious users with Primary transmitter power =100Kw, σ_m=5.5dB,σ_p=8dB, R_0= 30m, R= 200m, P_m= 4W.Here 10 malicious users are chosen random and distributed in the outer PER to calculated the PDF over 1000 times simulated .Numbers of malicious users are chosen 10 and its randomly distributed in the outer radius and received power in calculated 10000 number of simulations. It is very clear that the PDF of the received power at the secondary user from the primary *transmitter in CR network is differ from the received power at the secondary user from the malicious user.*

5.1.2 Miss Detection

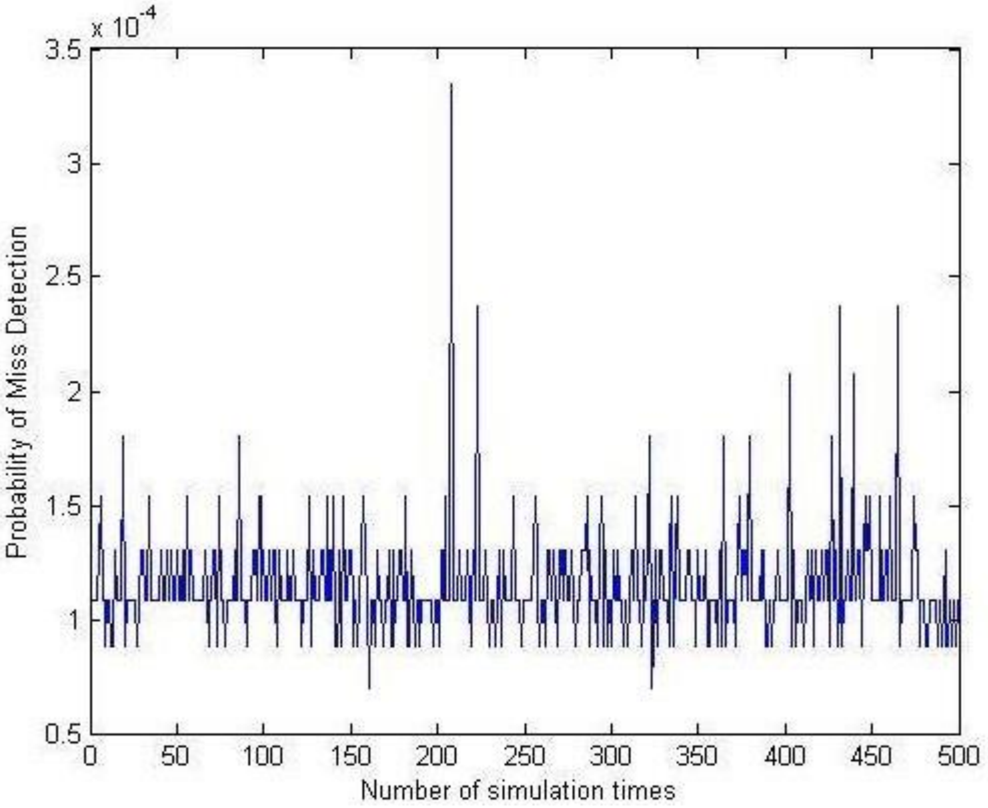

FIGURE 5.3: Probability of Miss Detection

Fig. 5.3 is the plot for the probability of miss detection. The number of malicious users in this case is set to be M=5, the radius of outer region R=1000m, Radius of primary exclusive region R_0 =20m, primary transmitter power P_t =1000Kw, Malicious transmitter power P_m =4w, σ_m=3.5dB, σ_p = 4dB. Probability of miss detection is calculated for 500 times of simulations. The threshold value chosen for detecting miss detection is 2.5, i.e. λ=2. In graph it is clear that in presence of malicious users there will remain the probability of miss detection.

5.1.3 False Alarm

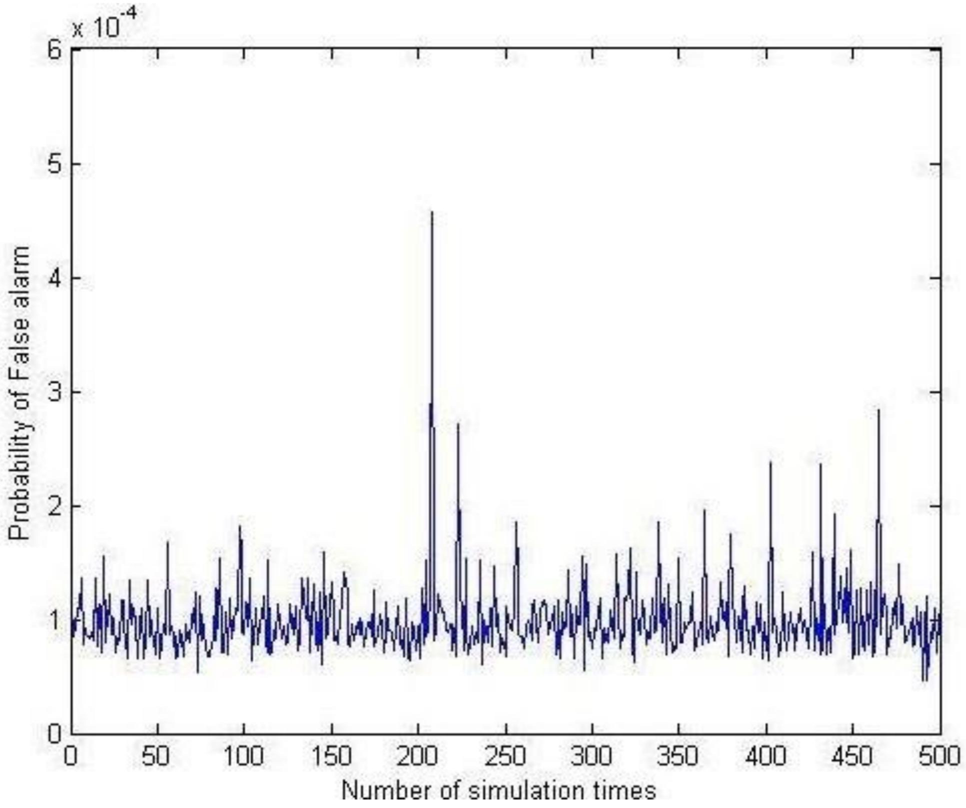

FIGURE 5.4: Probability of False Alarm

*Fig. 5.*4 shows the plot for probability of False Alarm. The number of malicious users in this case is M=5, the radius of outer circle R=1000m, Radius of primary exclusive region R_0=20m, primary transmitter power P_t=1000Kw, Malicious transmitter power *P_m=5w, σ_m=3.5dB, σ_p= 4dB.* Probability of False Alarm is calculated for 500 numbers of simulations. The threshold value chosen for simulating graph is *2.5 i.e.* λ=2.

Fig. 5.3 and Fig. 5.4 are the plots for the probability of miss detection vs. the number of simulation times and False alarm vs. the number of simulation times respectively, Probability of miss detection and false alarms are calculated for 500 times of simulations. The threshold value for this simulation is set to 2*, i.e.λ=2. .* In both cases the probability of false alarm and miss detection is always close to 1 to

1.5, if we increase the Malicious user number then the false alarm probability will increase.

5.1.4 Average of miss detection & false alarm

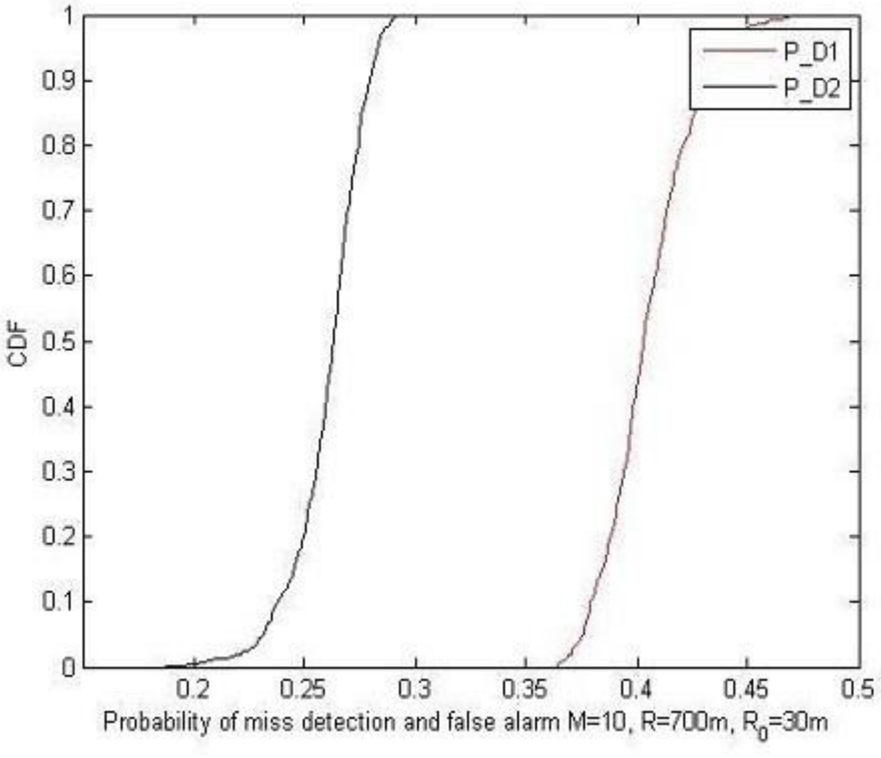

FIGURE 5.5: Probability of Miss Detection & False Alarm

Fig. 5.5 shows the plot for probability of miss detection and false alarm for, The radius of outer region is R=100m, Radius of primary exclusive region R_0*=30m, primary transmitter power* P_t*=100Kw, Malicious transmitter power is* P_m*=4w,* σ_m*=5.5dB,* σ_p*= 8dB. Probability of miss detection and false alarm are calculated for 500 numbers of simulations. The threshold value chosen for above simulation is set to 2 i.e.* λ*=2. The number of malicious users in this case is M=5.*

5.2 Our Proposed Model

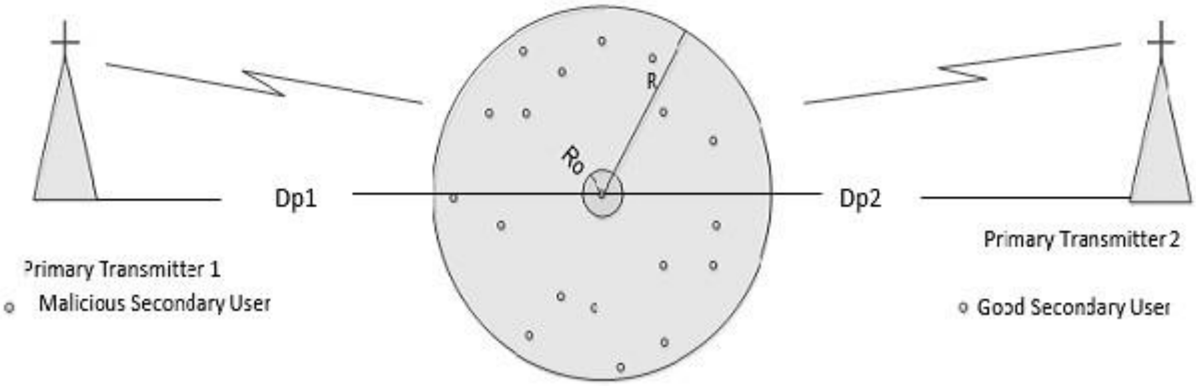

FIGURE 5.6: Proposed System Model

There are M malicious users in the system which transmits at power P_m. The primary transmitter P_t1 is at distance D_p1 and the primary transmitter P_t2 is at distance D_p2 from all the users and transmits at power P_t. The positions of secondary and malicious users are uniformly distributed in circular region of radius R and are statistically independent of each other. The path loss exponent for transmission from primary transmitter is 2 and that from malicious user is 4.

5.2.1 Observations from our system

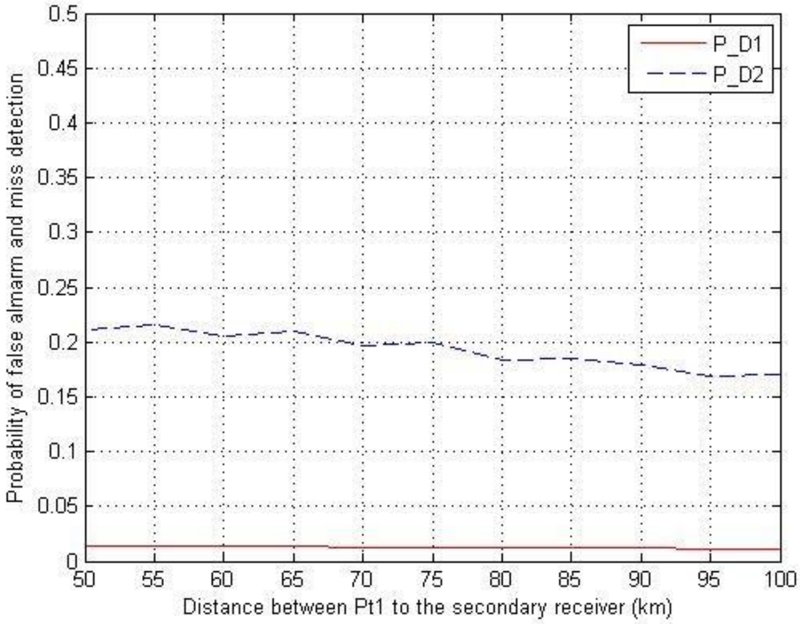

FIGURE 5.7: Average probability for miss detection and false alarm

Fig. 5.7 shows that number of miss detection is decreased with the distance from transmitter to outer region. The graph is plotted probability of miss detection and false alarm. The number of malicious users in this case is M=15, the radius of outer region R=1000m, Radius of primary exclusive region R0 =50m, primary transmitter power Pt1=100 Kw, primary transmitter power Pt2 = 50 Kw. In this case we have shown an experimental result by using two primary transmitter. We have observed that the change in false alarm probability is not too much. But we have noticed that miss detection probability has decreased with the decrement of the distance.

Chapter 6

Conclusion

In this thesis research, we have first investigated the general concepts of security threats to the cognitive radio networks. Then, we studied the performances for primary user emulation attacks from Neyman-Pearson criterion point of view. We have also shown the analytical experimental simulations to plot PDF ‘s of received power of two different cases, one is for received power from primary transmitter and second is for received power when malicious users attack in CR network . The PDF is calculated based on Neyman-Pearson composite Hypothesis. This PDF shows the number of malicious user has a great role to affect the CR network of sending false alarm and creating miss detection.

Our future work will be to secure CR network by implementing an efficient algorithms to verify secondary user using encryption techniques. Encrypted key will be generated by Primary user and to occupy the channel by good secondary user, they must have to match the key first.

Bibliography

Alahmadi, A. et al. (2014). “Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard”. In: *IEEE Transactions on Information Forensics and Security* 9.5, pp. 772–781. ISSN: 1556-6013. DOI: 10.1109/TIFS.2014.2310355.

Chen, R. and J. M. Park (2006). “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks”. In: *2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, pp. 110–119. DOI: 10.1109/SDR.2006.4286333.

Haykin, S. (2005). “Cognitive radio: brain-empowered wireless communications”. In: *IEEE Journal on Selected Areas in Communications* 23.2, pp. 201–220. ISSN: 0733-8716. DOI: 10.1109/JSAC.2004.839380.

Jin, Z., S. Anand, and K. P. Subbalakshmi (2009a). “Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks”. In: *2009 IEEE International Conference on Communications*, pp. 1–5. DOI: 10.1109/ICC.2009.5198911.

— (2009b). “Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks Using Hypothesis Testing”. In: *SIGMOBILE Mob. Comput. Commun. Rev.* 13.2, pp. 74–85. ISSN: 1559-1662. DOI: 10.1145/1621076.1621084. URL:http://doi.acm.org/10.1145/1621076.1621084.

Khare, Dr. Anubhuti and Manish Saxena (2013). “Attacks and Preventions of Cognitive Radio Network-A-Survey”. In: *International Journal of Avanced*

Reasearch in Computer Engineering and Technology(IJARCET) 2. ISSN: 2278-1323.

Le, T. N., W. L. Chin, and Y. H. Lin (2016). "Non-cooperative and cooperative PUEA detection using physical layer in mobile OFDM-based cognitive radio networks". In: *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1–5. DOI: 10.1109/ICCNC.2016.7440583.

Liu, Y., P. Ning, and H. Dai (2010). "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures". In: *2010 IEEE Symposium on Security and Privacy*, pp. 286–301. DOI: 10.1109/SP.2010.24.

Mathur, Chetan N. and K. P. Subbalakshmi (2007). "Security Issues in Cognitive Radio Networks". In: *Cognitive Networks*. John Wiley & Sons, Ltd, pp. 271–291. ISBN: 9780470515143. DOI: 10.1002/9780470515143.ch11. URL: http://dx.doi.org/10.1002/9780470515143.ch11.

Mitola, J. and G. Q. Maguire (1999). "Cognitive radio: making software radios more personal". In: *IEEE Personal Communications* 6.4, pp. 13–18. ISSN: 1070-9916. DOI: 10.1109/98.788210.

Weifang, Wang (2010). "Denial of service attacks in cognitive radio networks". In: *2010 The 2nd Conference on Environmental Science and Information Application Technology*. Vol. 2, pp. 530–533. DOI: 10.1109/ESIAT.2010.5567385.

Zhang, Xueying and Cheng Li (2010). "Constructing secured cognitive wireless networks: experiences and challenges". In: *Wireless Communications and Mobile Computing* 10.1, pp. 50–69. ISSN: 1530-8677. DOI: 10.1002/wcm.878. URL: http://dx.doi.org/10.1002/wcm.878.