Fall 12-30-2012

AN INVESTIGATION OF SECURITY CHALLENGES IN COGNITIVE RADIO NETWORKS

Deepraj S. Vernekar
University of Nebraska, dvernekarvernek@unomaha.edu

AN INVESTIGATION OF SECURITY CHALLENGES IN COGNITIVE RADIO NETWORKS

by

Deepraj Vernekar

A THESIS

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Master of Science

Major: Telecommunications Engineering

Under the Supervision of Professor Yaoqing Yang

Lincoln, Nebraska

December, 2012.

AN INVESTIGATION OF SECURITY CHALLENGES IN COGNITIVE RADIO NETWORKS

Deepraj Vernekar, M.S.

University of Nebraska, 2012

Adviser: Yaoqing Yang

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 spectrum demand for new wireless applications. The large portion of the allocated spectrum is sporadically used leading to underutilization of significant 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 attentions recently since the inherent properties of CR networks would pose new challenges to wireless communications. In this MS thesis, general concepts of security threats to the cognitive radio networks are briefly reviewed. Performances for primary user emulation attacks are studied from Neyman-Pearson criterion point of view. A novel system model with different configurations of the primary users has been proposed and studied. Our experimental results demonstrate the statistical characteristics of the probability of false alarm and miss detection in the proposed system. I will make performance comparison with others' research in the future.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my adviser Dr. Yaoqing Yang, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis and enabled me to develop an understanding of the subject.

Besides my advisor, I would like to thank the rest of my thesis committee: Dr. Hamid Sharif, Dr. Yi Qian, for their encouragement, insightful comments, and hard questions.

My sincere thanks also go to my colleagues, Ms. Omi Sunuwar, Mr. Qilin Qi and Mr. Andrew Minturn for their help and encouragement during my study at UNL.

Last but not the least; I would like to thank my family: my parents Surendra Vernekar and Sampada Vernekar, for giving birth to me at the first place and supporting me spiritually throughout my life.

Deepraj Vernekar

Table of Contents

Table of Figures

Nomenclature

CR	Cognitive Radio
PUE	Primary User Emulation
FCC	Federal Communication commission
PU	Primary User
SU	Secondary User
OSS	Opportunistic Spectrum Sharing
PER	Primary Exclusive Region
QOS	Quality of Service
NTIA	National Telecommunications and Information Administration
AM	Amplitude Modulation
MAC	medium access control
SNR	Signal to Noise Ratio
DOS	Denial of Service
AODV	Ad hoc On Demand Distance Vector
SSL	Secure Sockets Layer
TLS	Transport Layer Security

WEP	Wired Equivalent Privacy
TKIP	Temporal Key Integrity Protocol
RSS	Received Signal Strength
RTT	Round-Trip Time
PDF	Probability Density Function
RF	Radio Frequency

Chapter 1. Introduction

1.1 Background

The recent development in wireless communication has led to the problem of growing spectrum scarcity. Due to increasing spectrum demand for new wireless applications the available radio frequency spectrum has become scarcer. A significant amount of allocated radio frequency spectrum is used sporadically, causing underutilization of spectrum. Cognitive radio technology provides a promising solution for the spectrum scarcity issues in wireless networks. It allows the efficient use of the finite usable radio frequency spectrum. In cognitive radio terminology, Licensed users/Primary users are defined as users who have right to use the spectrum band whereas unlicensed users/Secondary users are defined as users who can use the spectrum which is temporarily not used by licensed users, without causing interference to them. At the same time, the security concerns of cognitive radio have received more attentions as the inherent properties of CR networks would pose new challenges to wireless communications. In cognitive radio network, an attack can be defined as an activity that can cause interference to the primary users or licensed users [2]. In this dissertation we also provide a brief explanation of most of the attacks that make use of one of the inherent properties of cognitive radio.

1.2 Benefits of Cognitive Radio Network

Why cognitive radio?

Spectrum is the lifeblood of communication systems. Without spectrum there is no electromagnetic communication. The radio frequency spectrum is the medium between the transmitters and receivers in wireless communication. The US spectrum is managed either by the FCC for non-governmental applications or by the NTIA for governmental applications [32]. As shown in Fig. 1.1 the radio frequency spectrum is characterized into different frequency bands. The frequency spectrum ranging from 300 kHz to 535 kHz is used for aeronautical and maritime communications and the frequency spectrum from 535 kHz and 1605 kHz is used for AM radio. The radio spectrum is becoming scarce due to the increasing growth of the wireless communication technology and the high requirement of capacity and date rates for various applications. We know that the amount of useable spectrum is limited. Due to vast improvement in wireless technology, radio spectrum will no longer be available for allocation for new services. Following Fig. 1.1 shows the radio frequency spectrum allocation in United States.

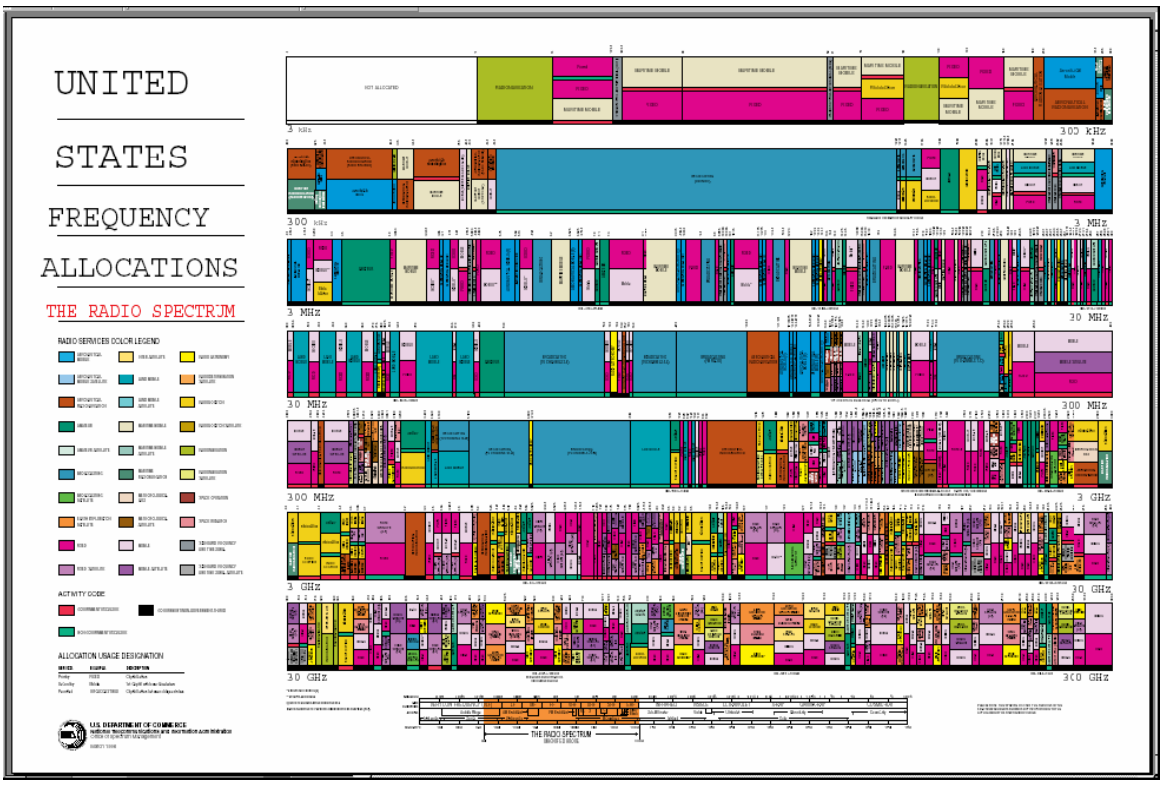

Figure 1.1 Radio frequency spectrum allocations in United States [21].

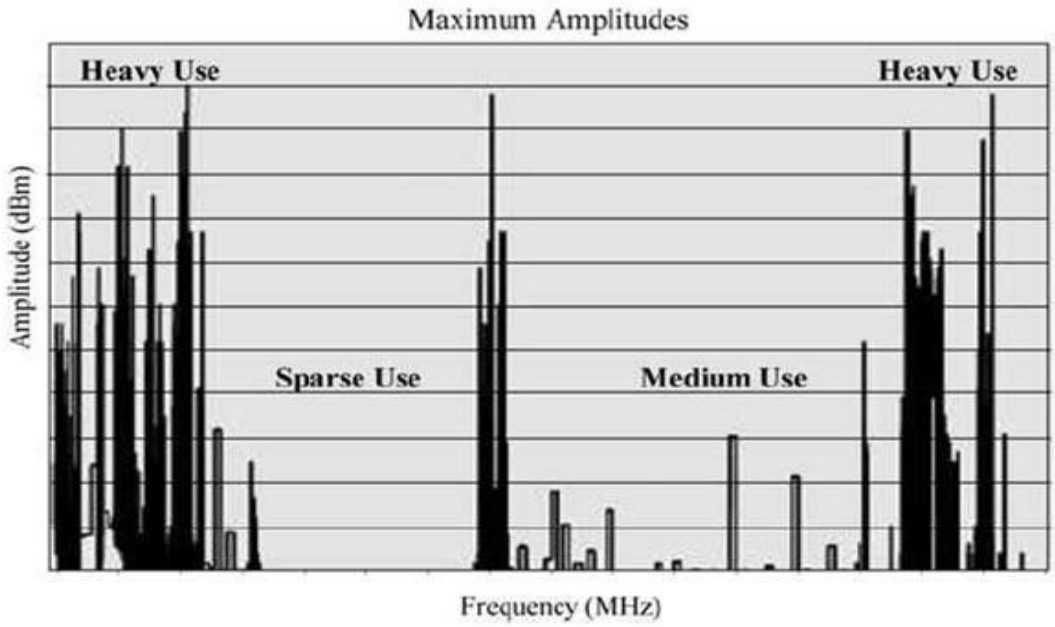

Figure 1.2 Spectrum Utilization [5].

From Fig. 1.2 we can conclude that significant portion of allotted spectrum is unused. There are portions of assigned spectrum that are concentrated in certain geographical areas. Certain portion of the wireless spectrum is unutilized. Studies reveal that a straightforward reuse of this unused radio frequency spectrum can provide an improvement in available capacity. Now the issue is not that spectrum is scarce – the issue is that we do not have the technology to effectively access the unused or wasted spectrum. This unused frequency spectrum can be used and accessed in an opportunistic manner by the secondary user. This gave a rise to new technology called "cognitive radio".

What is cognitive radio?

"A radio frequency transceiver designed to intelligently detect whether a particular segment of radio spectrum is in use and to jump into and out of temporarily unused spectrum very rapidly without interfering with the transmission of other authorized users. Cognitive radio enables secondary user to sense which portion of spectrum are available, select best available channel, coordinate spectrum access with other users and vacate the channel when a primary user reclaims the spectrum usage rights"[31].

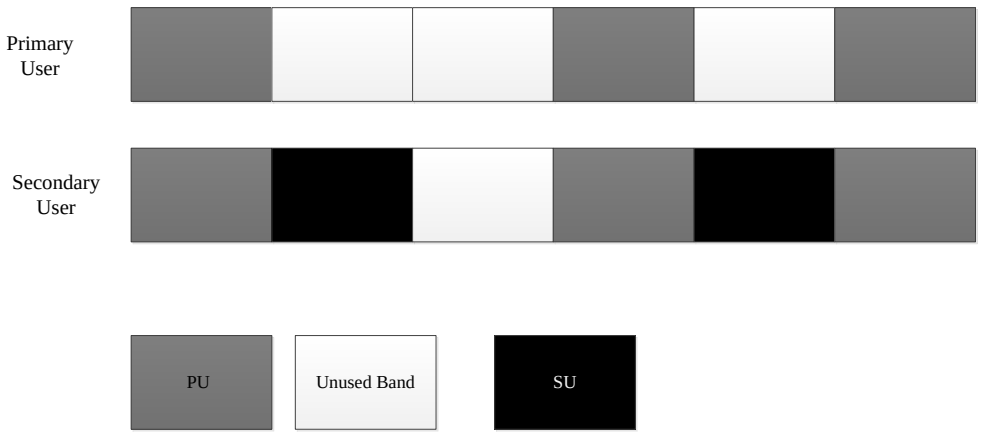

Figure 1.3. Cognitive radio Scenario [35]

Spectrum Sensing is a key step used in cognitive radio network. Basic requirement of cognitive radio is to scan the radio frequency spectrum and determine fallow bands which can be used in an opportunistic manner to increase spectrum efficiency [2]. The most efficient way to identify white space is to detect primary users. Primary user network & secondary user network are physically separate from each other. Secondary users do not get direct feedback from the primary users about their transmission. So in order to detect primary user transmission the secondary users have to depend on their sensing ability to [2]. Spectrum sensing is one of the most challenging issues in cognitive radio systems and has gained new aspects with cognitive radio and spectrum access concepts. Following are the features of cognitive radio [33],

- Frequency agility: It is the ability of a radio to change its operating frequency.
- Dynamic frequency selection: It is the ability of a radio to sense signals from nearby transmitters in order to choose best operating conditions.
- Location awareness: Determine its location, determine permission to transmit,

select parameters such as power, frequency allowed etc.

- Adaptive Modulation: Ability to modify transmission characteristics.
- Transmit power control: constrains the transmitter to a lower level to allow greater sharing of spectrum.

- **Cognitive radio Cycle**

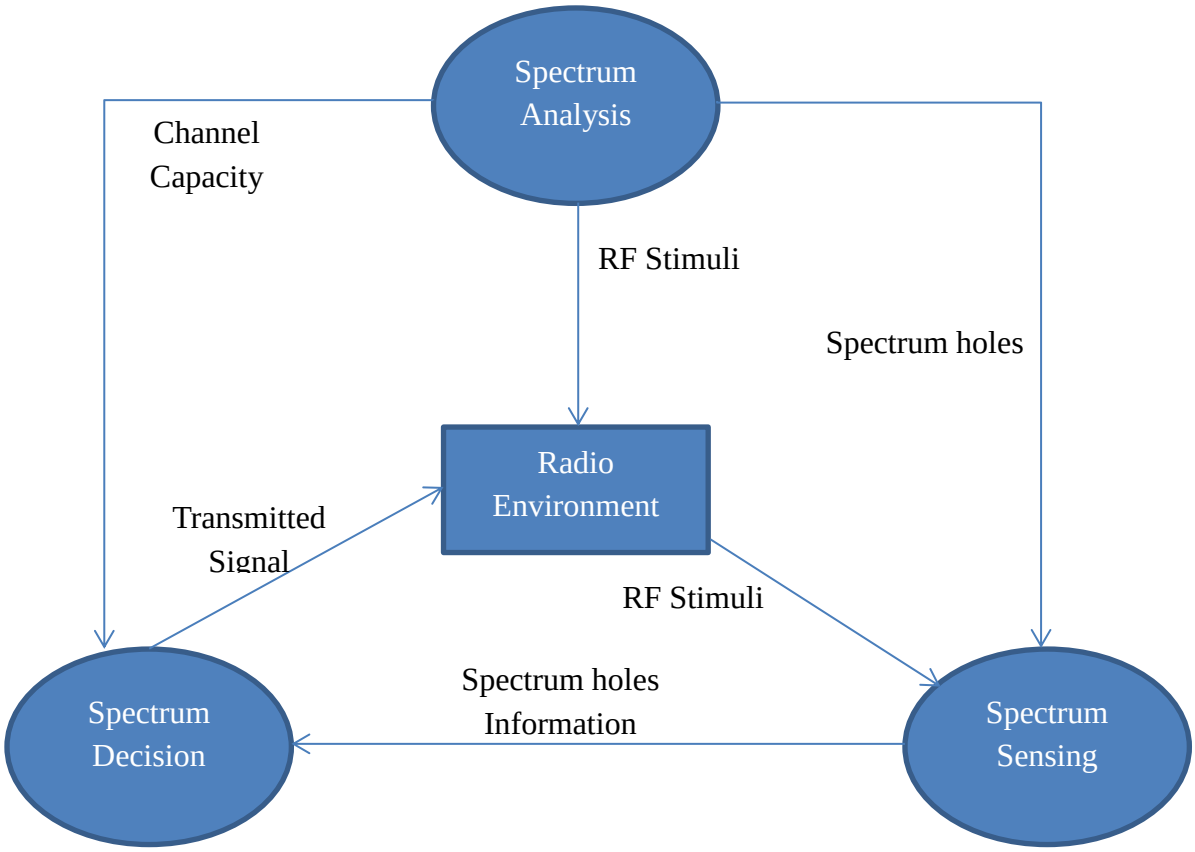

Figure 1.4. Cognitive radio cycle [34]

In cognitive radio cycle a cognitive radio scans the radio frequency spectrum, gathers information, and then identifies the vacant channels. Through spectrum sensing the properties of the vacant channels are evaluated. Then, the appropriate spectrum band is

chosen according to the spectrum characteristics and user requirements. The communication can be carried out after determining the operating frequency band. The four main functions of cognitive radio are as follows,

- Spectrum sensing: Spectrum sensing allows the CR users to adapt to the environment by detecting spectrum holes without causing interference to the primary network. One of the primary requirements of a cognitive radio is that, it should scan the radio frequency spectrum and identify “white spaces” [1].

- Spectrum decision: After sensing the frequency spectrum and identifying the “white spaces” Cognitive radio user should decide which frequency spectrum is the best among the available bands according to the Qos requirements for the applications. [1].

- Spectrum sharing : “Since there may be multiple cognitive radio users trying to access the spectrum, network access should be coordinated to prevent multiple users colliding in overlapping portions of the spectrum” [1]. Spectrum sharing can be classified as centralized or decentralized spectrum sharing, Cooperative or non-cooperative, overlay or underlay.

- Spectrum mobility: One of the primary requirements of cognitive radio is that, it should vacate the licensed band when the primary transmitter reappears and should search for another vacant frequency band in order to carry out its transmission. Thus spectrum mobility is defined as the ability of CR user to

switch between spectrum bands when the channel condition becomes worse or the primary user reappears.

- **Cognitive Radio Network Architecture**

This section provides a detailed description of the CR network architecture.

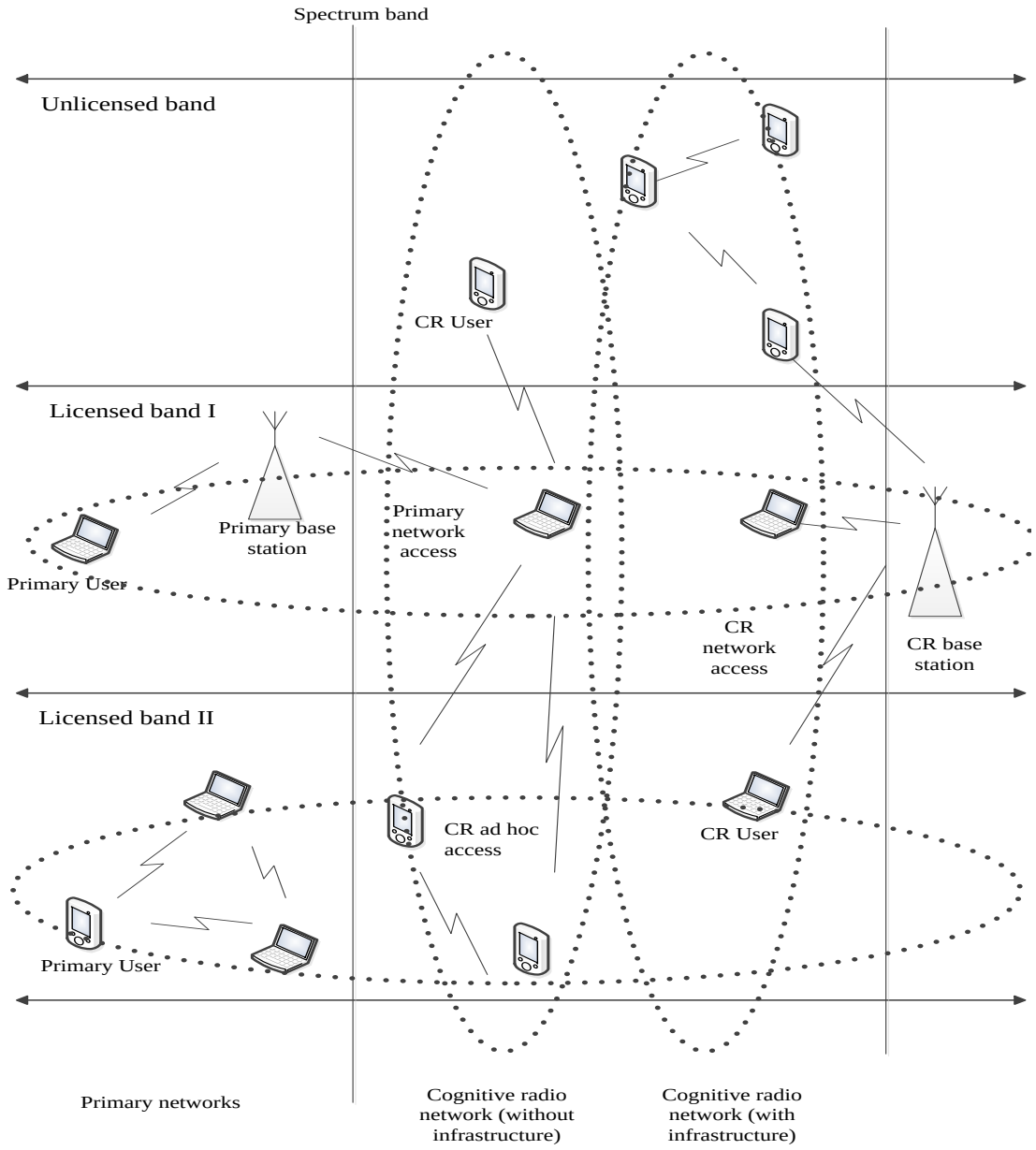

Figure 1.5. Cognitive radio network architecture [1].

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. According to Access type, cognitive radio network can be classified as CR network access, CR ad-hoc access, and primary network access.

- **Centralized cognitive network**: As shown in Fig. 1.5, the network is infrastructure oriented. A base station is used to manage each CR user in the network. The base station communicates directly with each user and controls the medium access and the secondary users in the network.

- **Distributed cognitive network**: As shown in Fig. 1.5, 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.

- **Licensed band operation**: This band is dedicated for the primary users in the network. It can be used by the unlicensed user if not occupied by the primary user. CR user must vacate the licensed band if the primary user reappears then and move to another vacant spectrum band.

- **Unlicensed band operation**: The unlicensed users have the same right to use the unlicensed band. There is no need to vacate the spectrum for the licensed users.

- **Cognitive radio network access**: As shown in Fig. 1.5, the cognitive users can share information with their base station on the licensed as well as the unlicensed spectrum band.

- **Cognitive radio ad-hoc access**: As shown in Fig. 1.5, the cognitive users in the network can share information with each other in ad-hoc manner on both the licensed and unlicensed spectrum band.

- **Primary network access**: As shown in Fig. 1.5, the CR users can also communicate with the primary base station on the licensed spectrum band with an adaptive medium access control protocol.

1.3 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 weaknesses and vulnerable aspects, introduced by the nature of cognitive radio [3]. 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 wireless media is open air, it is more vulnerable to attacks as compared to that of wired network.

The data in the wireless media may be eavesdropped or altered without notice and the channel might be jammed or overused by the adversaries. The cognitive radio technology opens more chances to attackers due to its intrinsic nature [3].

Inherent reliability Issues

Certain inherent reliability issues of cognitive radio networks are discussed [2].

- **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 detections.

- **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.

1.4 Summary

In this chapter we have given a brief description about how cognitive radio technology provides a promising solution for the spectrum scarcity issues in wireless networks. We have outlined the benefits of cognitive radio, the cognitive radio cycle, cognitive radio architecture. We have also discussed about the security issues in CR networks.

Chapter 2. Overview of security Threats in Cognitive Radio Networks

2.1 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 [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 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.

2.2 Security at different layers

In this section we will briefly describe the attacks associated with the five layers in the protocol stack i.e., the physical layer, link layer, network layer, transport layer and application layer [2][3].

- **Physical layer**

Physical layer is the lowest layer and it provides an interface to the transmission medium. Cognitive radio network doesn't operate on a fixed frequency that is signals can be transmitted and received at various frequencies across wide frequency spectrum band. The frequency spectrum is used dynamically. Thus, this makes the operation of physical layer in cognitive radio more complicated. Spectrum sensing is a key part cognitive radio, since it deals with identifying vacant bands or spectrum holes. Following are the possible attacks associated with physical layer.

- **Intentional jamming attack**

The malicious secondary user intentionally transmits signal 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 [3].

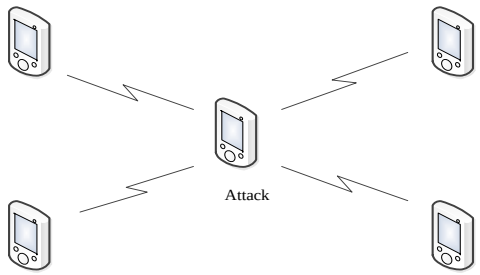

Figure 2.1. Intentional jamming attack [3].

- **Primary receiver jamming attack**

Since the secondary user does 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 requests transmission from the secondary users towards it. This will in turn cause interference to the primary receiver [3].

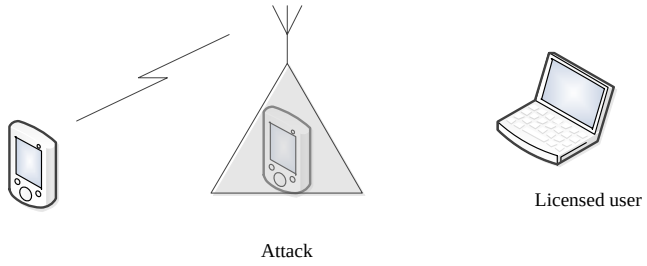

Figure 2.2. Primary receiver jamming attack [3].

- **Primary User Emulation Attack (PUE or PUEA)**

A malicious user can imitate the primary user, other secondary user in the network believes that the primary user reappears and they terminate their communication and release the frequency band. This prevents the secondary users from accessing that band [3].

- **Overlapping secondary user attack**

In cognitive radio networks, multiple secondary networks may exist at the same time over the same region. The transmissions from malicious entities in one network can cause 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 [2].

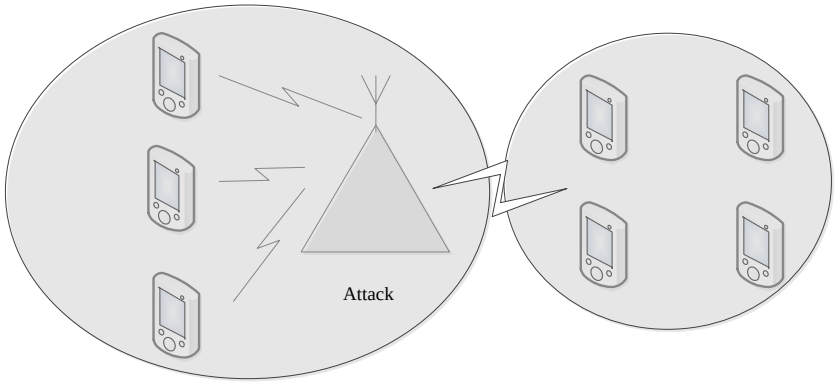

Figure 2.3. Overlapping secondary user attack [3].

- **Link layer**

Link layer sits just above physical layer in the protocol layer stack. This layer is responsible for transfer of data from one node to other in single hop. It ensures that initial 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. One of the important parameters to decide the fairness of a channel allocation scheme in traditional wireless environments is SNR. On the contrary, in cognitive 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 in cognitive radio networks [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 cognitive 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 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 attack is called as false feedback attack [2] [3].

- **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.

- **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 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 prevent route discovery where the source and the destination are more than two hops away. Protocols like Ariadne or secure AODV prevents such types of [2] [3].

- **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.

- **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 [2] [3].

- **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 [2] [3].

- **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 affect on the application layer [2] [3].

2.3 Security mechanisms

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

- **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) [3].

- **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 [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 [3].

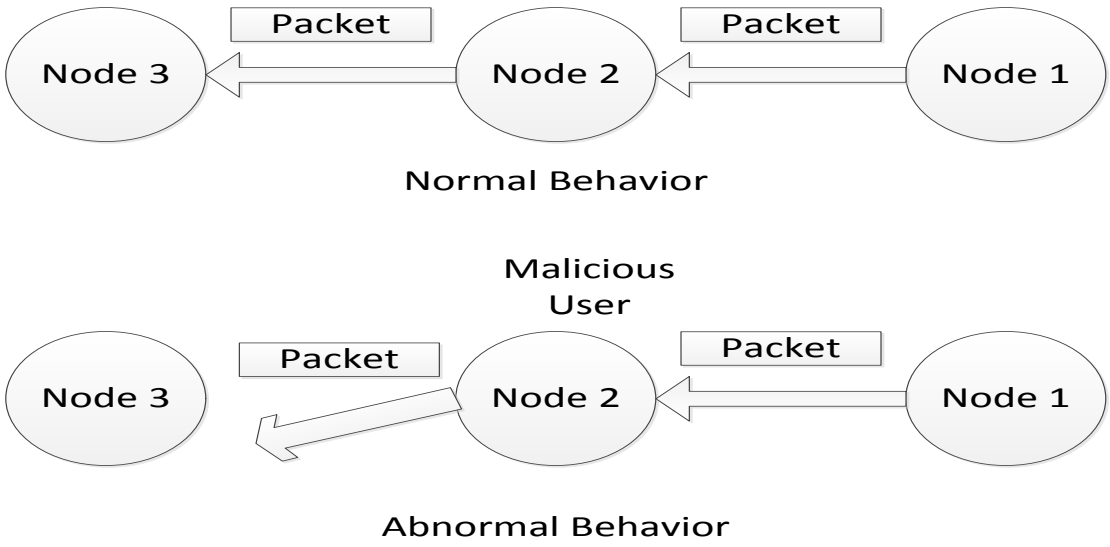

Figure 2.4. Intrusion detection at network layer [3].

For example, Fig. 2.4 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 [3].

- **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 [3].

- **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 [3].

2.4 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 3. Performance Study for Primary User Emulation Attack in Spectrum Sensing Networks

3.1 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 [4].

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 [4].

- **Selfish PUE attacks**: The main objective is to maximize attacker's bandwidth. For an instance, when malicious node identifies vacant band, it will prevent other secondary users from using that band by transmitting signals that resembles the incumbent signals [4].

- **Malicious PUE attack**: The main objective is to obstruct the secondary users from identifying and using vacant spectrum bands. Malicious attacker does not necessarily use vacant bands for its own communication purposes. It is important to note that in PUE attacks, malicious nodes only transmit in vacant bands [4].

3.2 Primary Exclusive Region

One of the deployment schemes in current related research is the primary exclusive region (PER). It sets a safeguard for primary receivers. The secondary network must be deployed outside PER. 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 [36]. Within this region 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 [36]. The secondary users are randomly and uniformly distributed within a network radius from the primary transmitter, outside the PER .

3.3 System Model of CRN

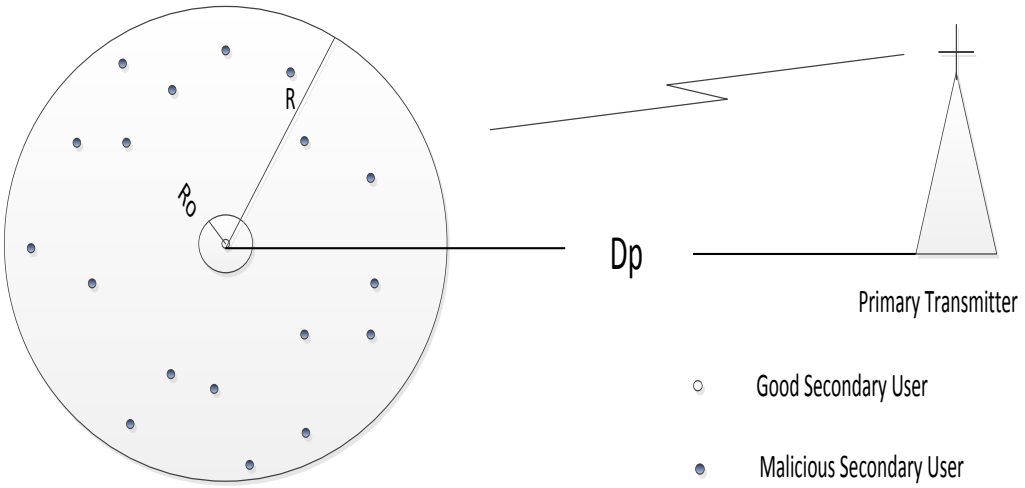

Figure 3.1 System model of CRN [10] [14]

Following assumptions are made for this system model [10] [14].There are M malicious users in the system and they transmits at power 'P_m'. 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 statistically 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_o, called as the exclusive radius from secondary user. There is no co-operation between the secondary users.

3.4 Analytical model

The PDF of the received signal at the secondary user due to transmission by the primary and the malicious user is calculated.

Consider M malicious users at (r_j,θ_j) $1 \leq j \leq$ M. The PDF of r_i is given as [14],

$$p(r_j) = \frac{2r_j}{R^2 - R_o^2} \qquad R_o \leq r \leq R \tag{3.9}$$

θ_j is uniformly distributed in $(-\pi, \pi)$. The received power at the secondary user from the primary transmitter is given by,

$$p_r^{(p)} = P_t d_p^{-2} {G_p}^2 \tag{3.10}$$

Where ${G_p}^2 = 10^{\frac{\varepsilon_p}{10}}$, $\varepsilon_p \sim N(0, \sigma_p^2)$. Since P_t and d_p are fixed the PDF of $p_r^{(p)}$ follows a log normal distribution and can be written as

$$p^{(Pr)}(\gamma) = \frac{1}{\gamma A \sigma_p \sqrt{2\pi}} \exp\{-\frac{\left(10\log_{10}\gamma - \mu_p\right)^2}{2\sigma_p^2}\} \tag{3.11}$$

Where A = $\frac{\ln 10}{10}$ and

$$\mu_p = 10log_{10}\, P_t \; - \; 20log_{10}\, d_p \tag{3.12}$$

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

$$p_r^{(m)} = \sum_{j=1}^{M} P_m \, D_j^{-4} G_j^2 \tag{3.13}$$

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.

$G_j^2 = 10^{\frac{\varepsilon_j}{10}}$ where $\varepsilon_j \sim N(0, \sigma_m^2)$. Each term in the right hand side of the Equ. (3.13) is log normally distributed random variable of the form $10^{\frac{\omega_j}{10}}$ where $\omega_j \sim N(\mu_j, \sigma_m^2)$, where μ_j is given by ,

$$\mu_j = 10log_{10}\, P_m \; - \; 40log_{10}\, d_j \tag{3.14}$$

The PDF of p_r^m conditioned on the positions of all malicious user can be written as,

$$p_{x|r}^{(m)} \; = \; \frac{1}{xA\sigma_M\sqrt{2\Pi}} \exp\{-\frac{(10\log_{10} x - \mu_M)^2}{2\sigma_M^2}\} \tag{3.15}$$

r is the vector with elements $r_1, r_2, \ldots, r_M$. And σ_M^2 and μ_M are given as,

$$\sigma_M^2 = \frac{1}{A^2} \ln \; [1 + \frac{\left(e^{A^2\sigma_m^2} - 1\right) \sum_{j=1}^{M} e^{2A\,\mu_j}}{\left(\sum_{j=1}^{M} e^{A\;\mu_j}\right)^2}] \tag{3.16}$$

$$\mu_M = \frac{1}{A}\ln \; (\sum_{j=1}^{M} e^{A\mu_j}) - \frac{A}{2}(\sigma_M^2 - \sigma_m^2) \tag{3.17}$$

The PDF of the received power from all the malicious users, $p^m(x)$, can be obtained by averaging Equ.(3.15) over $r_1, r_2, \ldots, r_M$ and is given by,

$$p^m(x) = \int_{R_o}^{R} \prod_{j=1}^{M} \; p_{x|r}^{(m)}(x|r) \; p(r_j)\, dr_j \tag{3.18}$$

Evaluating Equ.(3.18) is very complex so it is approximated to be a log normally distributed random variable with parameters μ_x and σ_x of the form,

$$p^m(x) = \; \frac{1}{xA\sigma_x\sqrt{2\pi}} \exp\{-\frac{(10\log_{10}\; x - \mu_x)^2}{2\sigma_x^2}\} \tag{3.19}$$

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

$$\sigma_x^2 = \frac{1}{A^2}\left(\ln E[(p_r^{(m)})^2] - 2\ln E[p_r^{(m)}]\right) \quad (3.20)$$

$$\mu_x = \frac{1}{A}\left(2\ln E[p_r^{(m)}] - \frac{1}{2}\ln E\left[\left(p_r^{(m)}\right)^2\right]\right) \quad (3.21)$$

From Equ.(3.15) The average probability of $p_r^{(m)}$, $E[p_r^{(m)}|r]$ can be written as,

$$\mathrm{E}\left[p_r^{(m)}\middle|r\right] = e^{A\mu_M + \frac{1}{2}A^2\sigma_M^2} = e^{A(\mu_j - \frac{A}{2}\sigma_M^2 + \frac{A}{2}\sigma_m^2 + \frac{1}{A}\ln M) + \frac{1}{2}A^2\sigma_M^2}$$

$$= e^{A\mu_j - \frac{A^2}{2}\sigma_M^2 + \frac{A^2}{2}\sigma_m^2 + \ln M + \frac{A^2}{2}\sigma_M^2} = e^{A\mu_j + \frac{A^2}{2}\sigma_m^2 + \ln M}$$

$$\mathrm{E}\left[p_r^{(m)}\middle|r\right] = Me^{A\mu_j} * e^{\frac{A^2\sigma_m^2}{2}}$$

Where,

$$\mu_j = 10log_{10}\,P_m - 40log_{10}\,D_j = 10\log_{10}(P_m * D_j^{-4})$$

$$e^{A\mu_j} = e^{A10\log_{10}(P_m * D_j^{-4})} = 10^{10\log_{10}(P_m * D_j^{-4})/10} = P_m * D_j^{-4}$$

$$\mathrm{E}\left[p_r^{(m)}\middle|r\right] = \mathrm{M}\,P_m * D_j^{-4} * e^{\frac{A^2\sigma_m^2}{2}}$$

Integrating above equation over $r_1, r_2, \ldots, r_M$,

$$E\left[p_r^{(m)}\right] = \int_{R_o}^{R} \mathrm{M}\,p(r_j)\,P_m\,D_j^{-4}\,e^{\frac{A^2\sigma_m^2}{2}}\,dr_j$$

$$= MP_m e^{\frac{A^2\sigma_m^2}{2}} \int_{R_o}^{R} \frac{2r_j}{\mathrm{R}^2 - R_o^2} * D_j^{-4}\,dr_j$$

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

$$E\left[p_r^{(m)}\right] = MP_m e^{\frac{A^2\sigma_m^2}{2}} \int_{R_o}^{R} \frac{2r_j}{R^2 - R_o^2} * \frac{1}{r_j^4}\,dr_j$$

$$= \frac{MP_m e^{\frac{A^2\sigma_m^2}{2}}}{R^2 - R_o^2}(2)\int_{R_o}^{R} \frac{1}{r_j^2}\, dr_j$$

$$= \frac{MP_m e^{\frac{A^2\sigma_m^2}{2}}}{R^2 - R_o^2}(2)\left[\frac{1}{2}\left[\frac{1}{R^2} - \frac{1}{R_o^2}\right]\right]$$

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

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

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

3.5 Neyman-Pearson Criterion for Detecting PUEA

The two hypothesis in Neyman-Pearson decision criterion are given as follows,

M_1 : Primary Transmission in progress

M_2 : Emulation attack in progress

There are two types of errors that secondary user can make in this hypothesis test.

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

Miss Detection: The secondary makes a decision that the 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 ratio of Λ,

$$\Lambda = \frac{p^{(m)}(x)}{p^{(P_r)}(x)}$$

Where $p^{(m)}(x)$ is defined in Equation (3.19) and $p^{(P_r)}(x)$ is defined in Equation (3.11). Λ is then compared with predefined threshold and the secondary decides the following

$\Lambda \leq \lambda$ D_1 : Primary transmission

$\Lambda \geq \lambda$ D_2 : PUEA in progress

First, secondary user may decide D_2 when M_1 is true, and second secondary user may decide that D_1 when M_2 is true. Each of these errors has a probability associated with it which depends on the decision rule and condition densities.

Miss Probability: $P\{D_2|M_1\}$ = Probability of making decision D_2 when M_1 is true.

False Alarm Probability: $P\{D_1|M_2\}$ = Probability of making decision D_1 when M_2 is true.

In terms of conditional densities these probabilities can be expressed as

$$P\{D_2|M_1\} = \int_{\Lambda \geq \lambda} p^{(P_r)}(x)dx = \alpha$$

$$P\{D_1|M_2\} = \int_{\Lambda \leq \lambda} p^{(m)}(x)dx$$

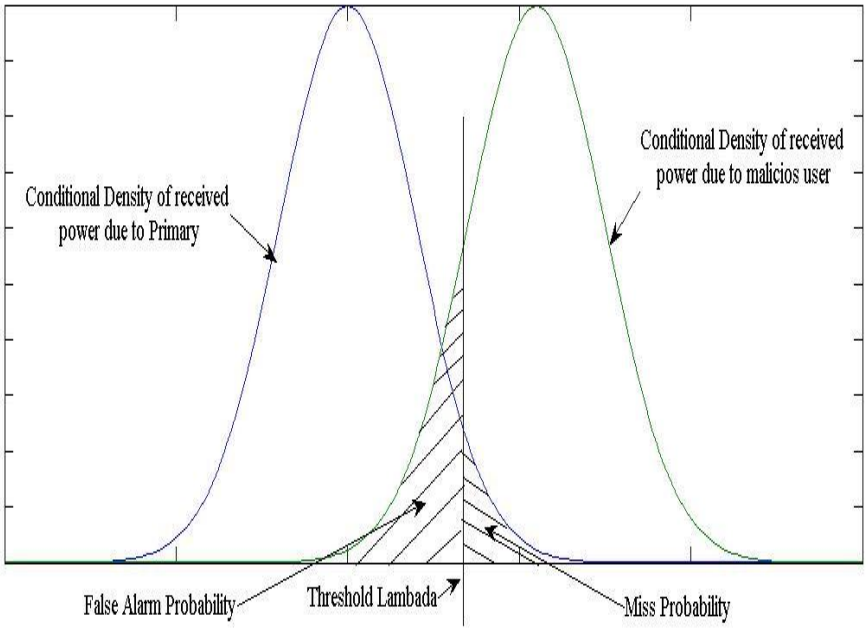

Figure 3.2 Decision Rule

Fig. 3.2 is a plot for Decision Rule showing Miss Probability and Probability of false alarm under Gaussian distribution. As shown in the figure, we can see the two conditional densities of the power received by the good secondary user from primary and malicious transmitters. The decision rule is then compared with the threshold value; Lambda (λ) and the two probabilities viz. miss probability and probability of false alarm are calculated accordingly.

3.6 Computed simulation Results and observations

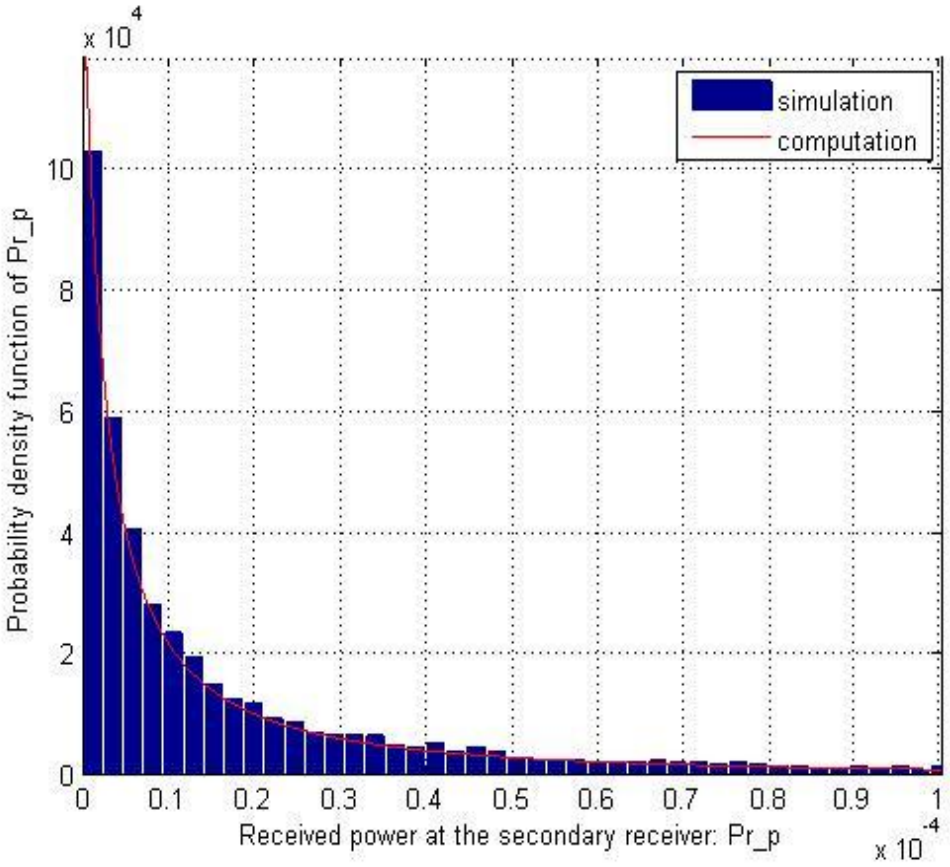

Figure 3.3 PDF of received power at the secondary receiver: Pr_p

Fig. 3.3 shows the Probability Density Function (pdf) of the received power at the secondary user when the primary transmitter is at distance 100Km, Primary transmitter power P_t=100Kw, σ_m= 5.5dB, σ_p= 8dB, R_0= 30m, R= 1000m, P_m= 4W. Probability Density Function of Received power is calculated for 10000 times. Both simulated and computed PDF are plotted in the same figure for easy comparision. Matlab simulation code can be found in Appendix A.

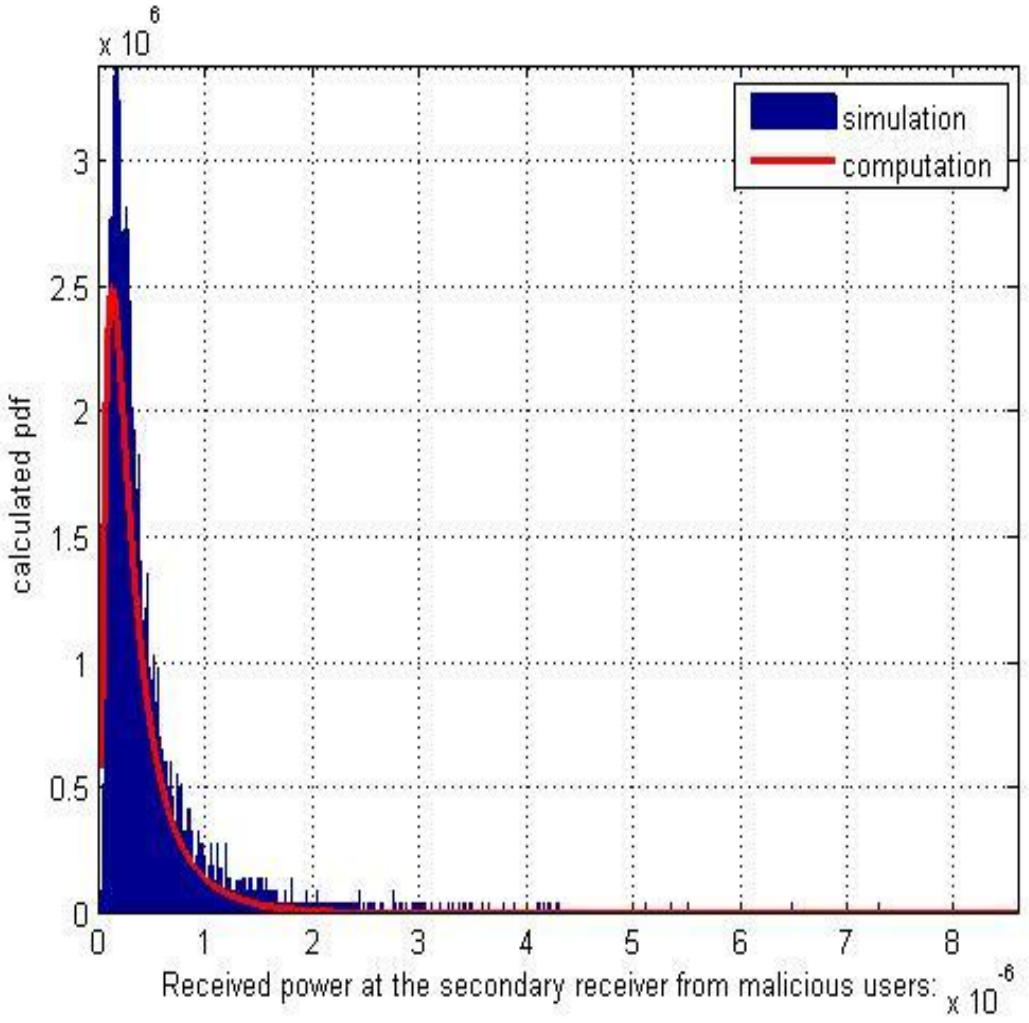

Figure 3.4 PDF of received power at the secondary receiver: Pr_m

Fig. 3.4 shows the Probability Density Function of the received power at the secondary user due to malicious users with Primary transmitter power P_t=100Kw, σ_m=5.5dB, σ_p=8dB, R_0= 30m, R= 200m, P_m= 4W. Probability Density Function of Received power is calculated for 10000 numbers of simulations. Numbers of malicious users chosen are 10 and are randomly distributed in the outer radius. Matlab simulation code can be found in Appendix B.

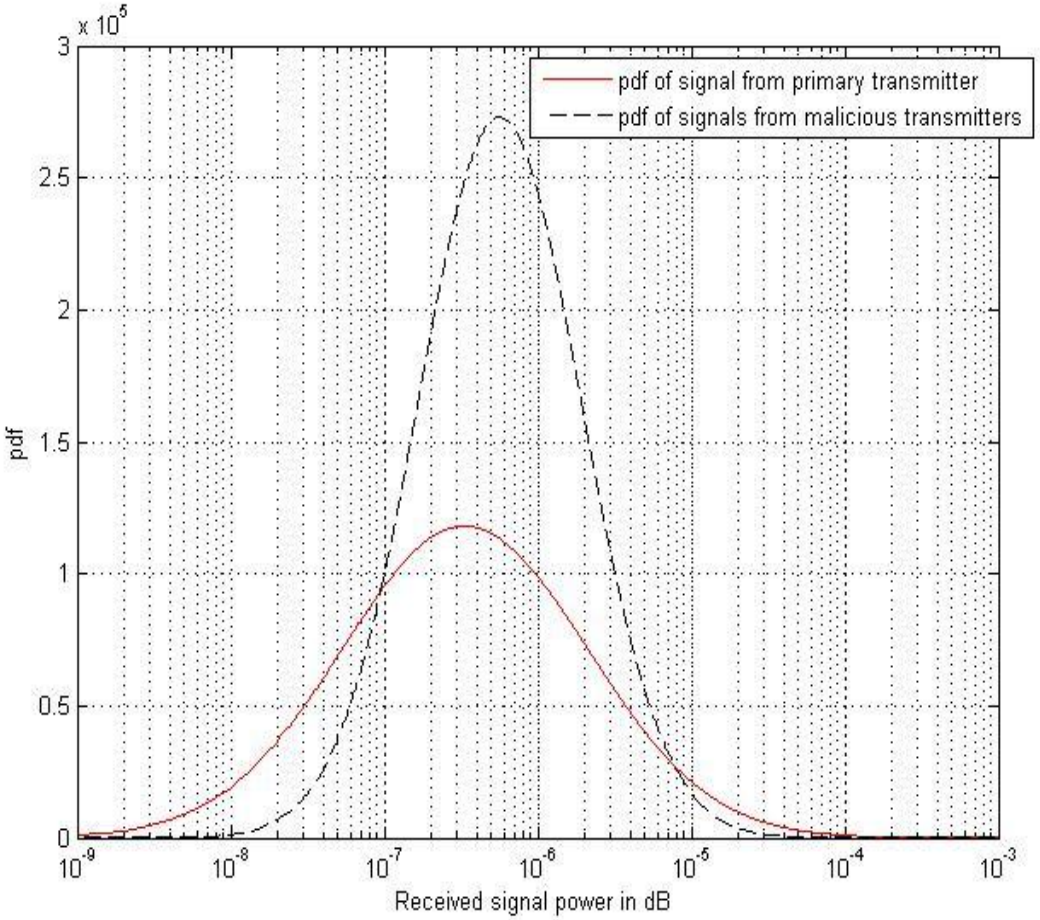

Figure 3.5 PDF of received signal power in dB at the secondary receiver due to primary transmitter and malicious user.

Fig. 3.5 shows the probability density plot of received signal power in dB at the secondary user due to primary transmitter and malicious user for M=5, R=400m, R_0=30m, P_t=100Kw, P_m=4w, σ_m= 5.5dB, σ_p= 8dB. To get the statistics we run the simulation over 10000 times. Matlab simulation code can be found in Appendix C.

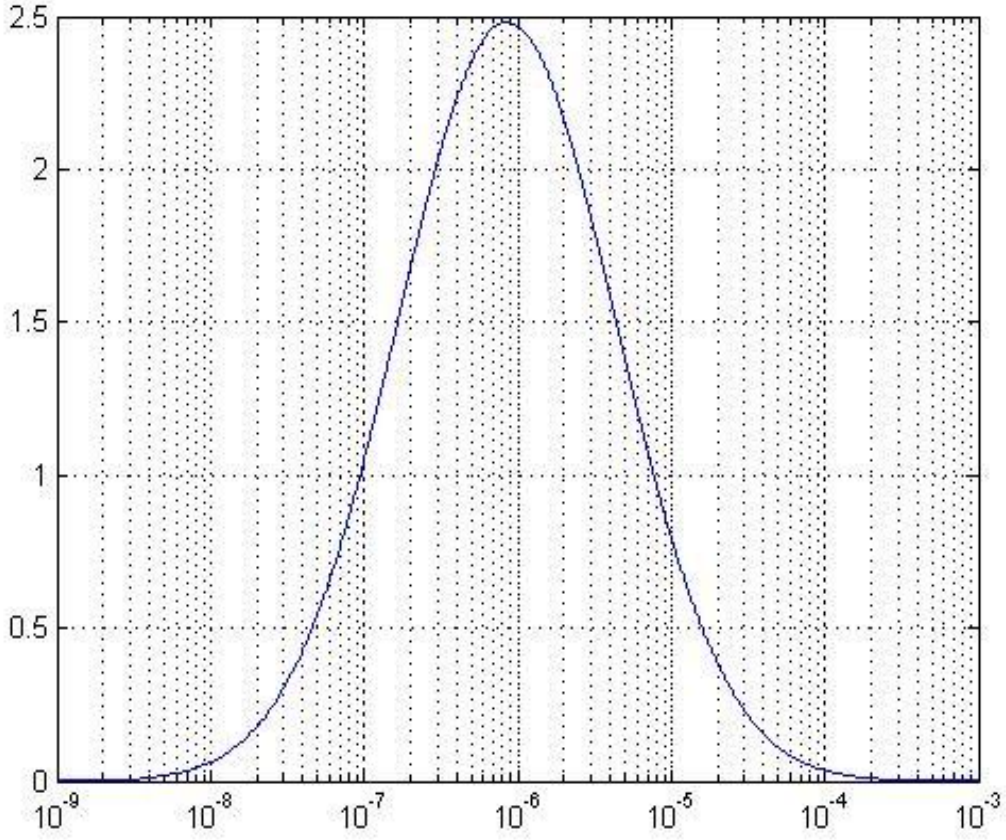

Figure 3.6 Ratio of received power due to malicious user over received power due to Primary transmitter

Fig. 3.6 shows the plot for Ratio of Received power in dB due to malicious users over Received power due to Primary transmitter, The radius of outer region is R=400m, 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. We run the simulation for 10000 times. The number of malicious users in this case is M=5. Matlab simulation code can be found in Appendix C.

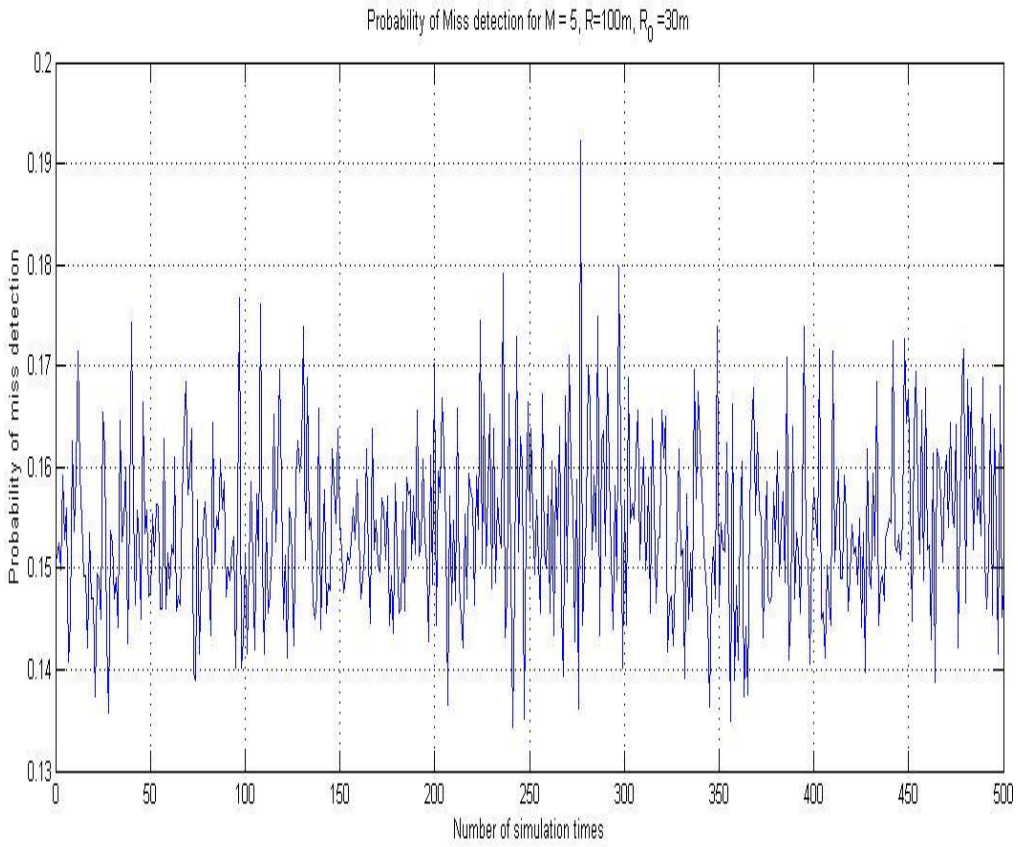

Figure 3.7 Probability of miss detection

Fig. 3.7 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=100m, Radius of primary exclusive region R_0 =30m, primary transmitter power P_t =100Kw, Malicious transmitter power P_m =4w, σ_m =5.5dB, σ_p = 8dB. Probability of miss detection is calculated for 500 times of simulations. The threshold value chosen for above simulation is set to 2, i.e. λ=2. Matlab simulation code can be found in Appendix C.

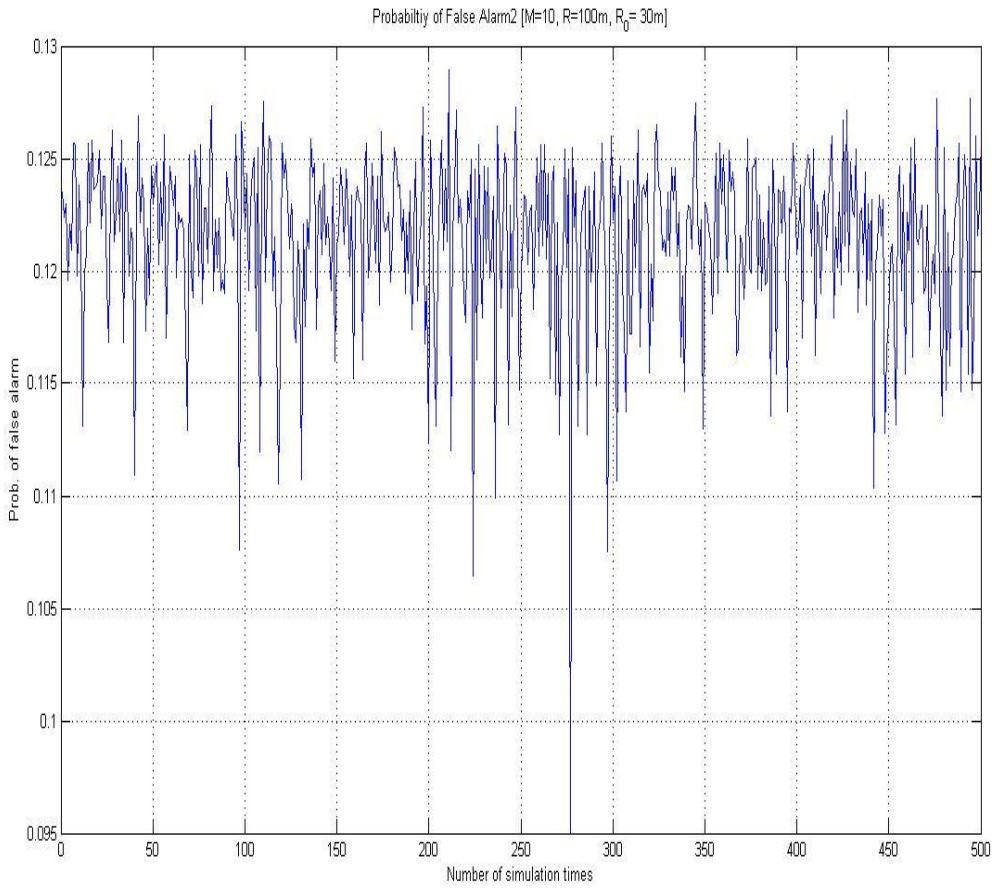

Figure 3.8 Probability of false alarm

Fig. 3.8 shows the plot for probability of False Alarm. The number of malicious users in this case is M=10, The radius of outer region R=100m, Radius of primary exclusive region R_0=30m, primary transmitter power P_t=100Kw, Malicious transmitter power P_m=4w, σ_m=5.5dB, σ_p= 8dB. Probability of False Alarm is calculated for 500 numbers of simulations. The threshold value chosen for above simulation is set to 2 i.e. λ=2. Matlab simulation code can be found in Appendix C.

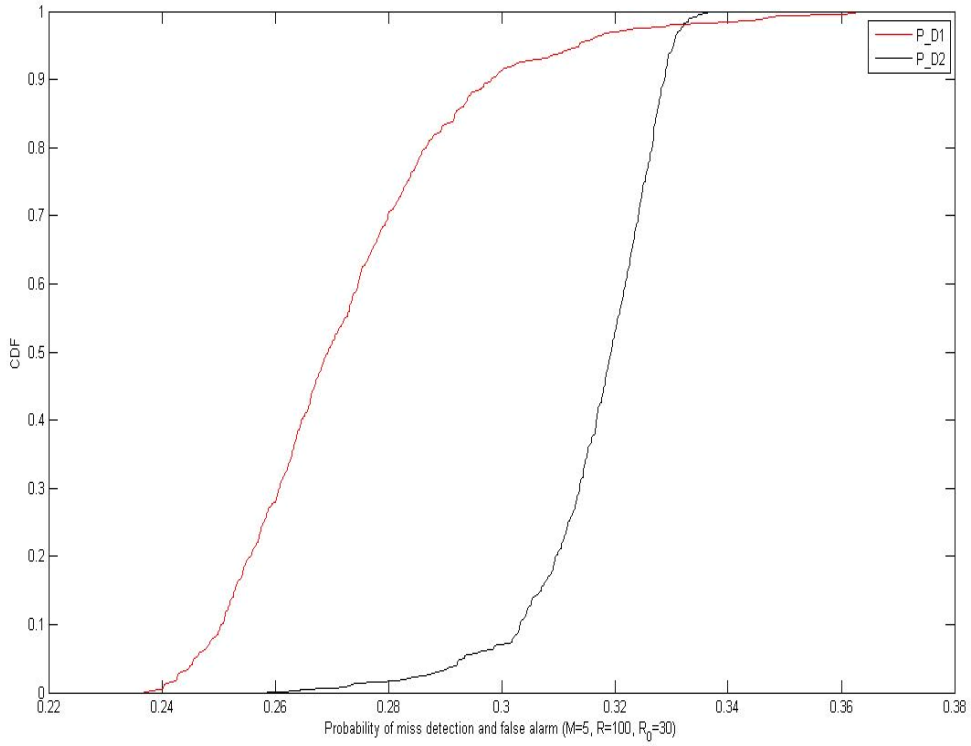

Figure 3.9 Probability of miss detection and false alarm

Fig. 3.9 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. Matlab simulation code can be found in Appendix C.

Case Study : Lambda(λ)= 2

The following table shows the probabilities of false alarm and miss detection of primary receiver with different range of R.

Number Of malicious users, M = 5							
Threshold Value, Lambda(λ)= 2							
R(meters)	100	200	300	400	500	600	700
P_D1_H2	0.2728	0.0765	0.0486	0.3172	0.026	0.0015	5.71E-04
P_D2_H1	0.317	0.0713	0.0373	0.1858	0.0203	0.0016	6.60E-04
Number Of malicious users, M = 10							
Threshold Value, Lambda(λ)= 2							
R(meters)	100	200	300	400	500	600	700
P_D1_H2	0.4054	0.4631	0.1458	0.0291	0.0288	0.0013	0.001
P_D2_H1	0.3681	0.3338	0.1041	0.0264	0.0223	0.0017	0.0011
M = 15							
Lambda = 2							
R(meters)	100	200	300	400	500	600	700
P_D1_H2	0.1498	0.1997	0.2661	0.0948	0.0062	0.0869	0.0204
P_D2_H1	0.7825	0.1558	0.1761	0.0698	0.0075	0.072	0.0177

3.7 Summary

In this chapter we have studied the analytical model for the primary user emulation attack in cognitive radio network. We have done a detailed analysis and simulation of the network for PUE attack. Simulations were carried out to determine the performance of the network for PUE attack in terms of probabilities of miss detection and false alarm. We discussed various results for our simulations and provided our Matlab codes for the simulations in the attached Appendices.

Chapter 4. Proposed PUE Attack Model with Maximum Likelihood Criterion

4.1 Introduction

Chapter 3 deals with the performance study of the analytical model for PUEA in cognitive radio. In this chapter we propose a new model for PUEA in CR network. Following assumptions are made for the new system model.

1. There are M malicious users in the network and are randomly and uniformly distributed in the circular region.

2. There are two primary transmitters P_{t1} & P_{t2}, separated by a fixed distance and their transmission are independent.

3. The distance between secondary user and P_{t1} is D_{p1}, The distance between secondary user and P_{t2} is D_{p2}.

4. No malicious user is present between within the exclusive region for the secondary user.

5. All the users in the network know about the location of primary transmitters.

6. The RF signals from primary and malicious transmitters undergo path loss and log normal shadowing.

7. The position of the good secondary user changes, it moves away from primary transmiiter1 towards primary transmitter 2.

4.2 Proposed System Model

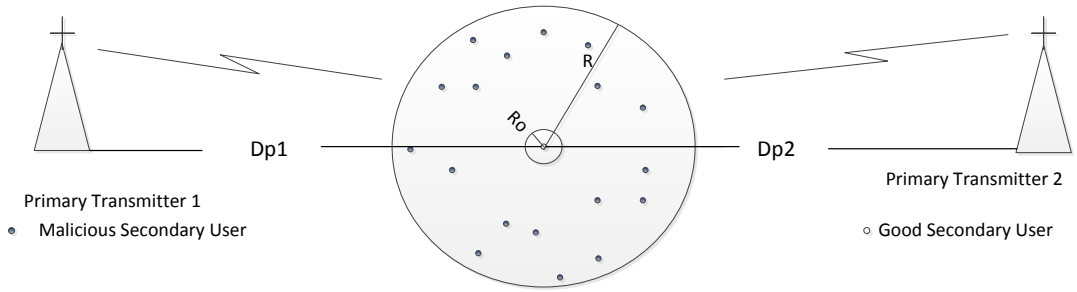

Figure 4.1 Proposed system model

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. Position of primary transmitter is known to all the users and is fixed at (r_p,θ_p). The RF signals from primary transmitter and malicious users undergo path loss and log normal shadowing. The path loss exponent for transmission from primary transmitter is 2 and that from malicious user is 4. For any secondary user fixed at co-ordinates(r,θ) no malicious users are present within a circle of radius R_o which is called the exclusive radius from secondary user. There is no co-operation between the secondary users.

The received power at the secondary user from the primary transmitter1 is given by,

$p_r^{(p1)} = P_{t1} d_{p1}^{-2} G_{p1}{}^2$

The received power at the secondary user from the primary transmitter1 is given by,

$p_r^{(p2)} = P_{t2} d_{p2}^{-2} G_{p2}{}^2$

The total power at receivers is then given by, $p_r^{(p)} = p_r^{(p1)} + p_r^{(p2)}$ due to their independence.

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

$p_r^{(m)} = \sum_{j=1}^{M} P_m \, D_j^{-4} G_j^2$

PDF of $p_r^{(p)}$ follows a log normal distribution and can be written as

$p^{(Pr)}(\gamma) = \frac{1}{\gamma A \sigma_p \sqrt{2\pi}} \exp\{-\frac{(10\log_{10}\gamma - \mu_p)^2}{2\sigma_p^2}\}$

PDF of $p_r^{(m)}$ follows a log normal distribution and can be written as

$p^m(x) = \frac{1}{xA\sigma_x\sqrt{2\pi}} \exp\{-\frac{(10\log_{10} x - \mu_x)^2}{2\sigma_x^2}\}$

4.3 Computed simulation results and observations

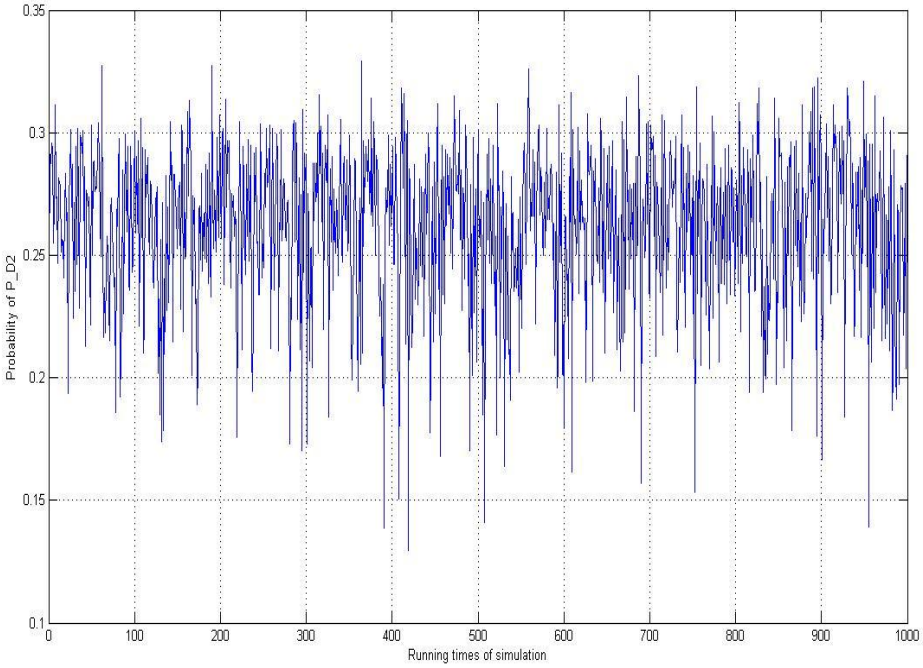

Figure 4.2 Probability for miss detection

Fig. 4.2 shows a sample plot of probability for miss detection. The number of malicious users in this case is M=10, The radius of outer region R=200m, Radius of primary exclusive region R_0 =30m, primary transmitter power $P_{t1} = 100Kw$, primary transmitter power $P_{t2} = 50Kw$, Malicious transmitter power P_m=4w, $\sigma_{m1} = 8dB$, $\sigma_{m2} = 10dB$. Probability of miss detection is calculated for 1000 numbers of simulations. It is observed that the probability of miss detection shows randomness between the range of 0.1 and 0.36. Matlab simulation code can be found in Appendix D.

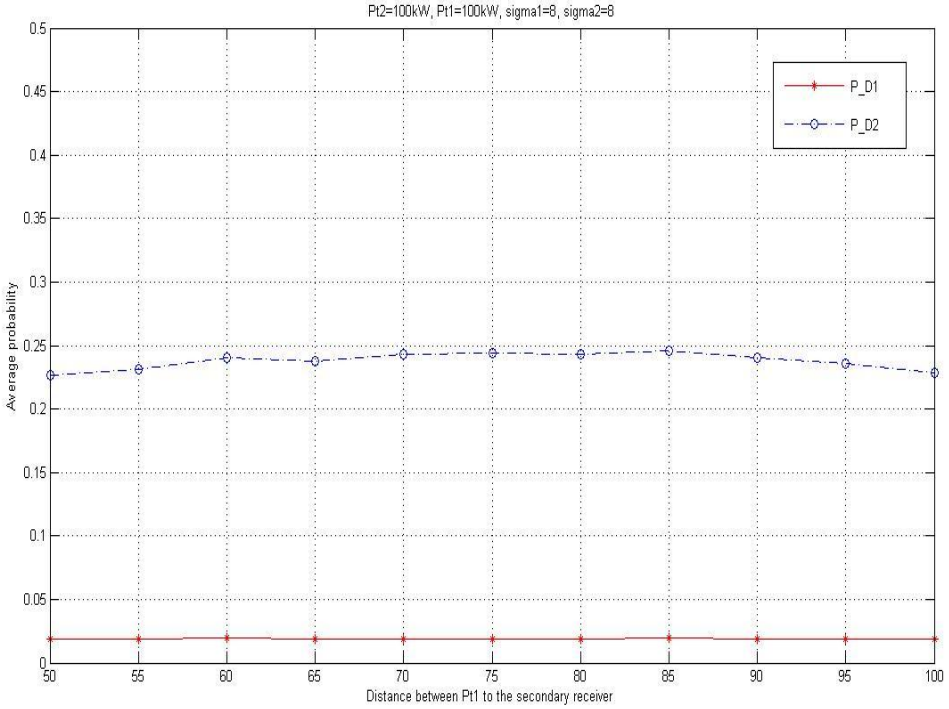

Figure 4.3 Average probability for miss detection and false alarm

Fig. 4.3 is the plot for average probability for miss detection and false alarm. The number of malicious users in this case is M=10, The radius of outer region R=200m, Radius of primary exclusive region R_0 =30m, primary transmitter power $P_{t1} = 100Kw$, primary transmitter power $P_{t2} = 100Kw$, Malicious transmitter power P_m =4w, $\sigma_{m1} = 8dB$, $\sigma_{m2} = 8dB$. It is noted that the probability curves show symmetric around 75Km, because we set up two transmitters equally. Matlab simulation code can be found in Appendix D.

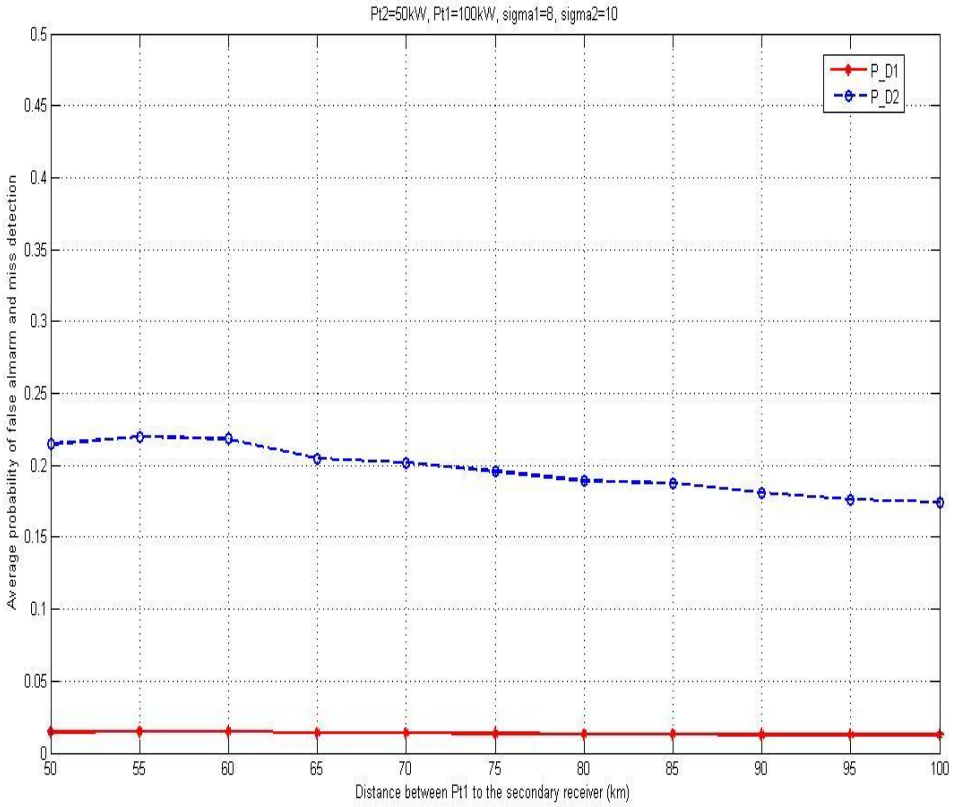

Figure 4.4 Average probability for miss detection and false alarm

Fig. 4.4 shows the plot for average probability for miss detection and false alarm. The number of malicious users in this case is M=10, The radius of outer region R=200m, Radius of primary exclusive region R_0 =30m, primary transmitter power $P_{t1} = 100Kw$, primary transmitter power $P_{t2} = 50Kw$, Malicious transmitter power P_m=4w, $\sigma_{m1} = 8dB$, $\sigma_{m2} = 10dB$. It is observed that the probability of false alarm does not change too much over the distance 50Km to 100Km. But the probability of miss detection decrease with the distance. Matlab simulation code can be found in Appendix D.

4.4 Summary

In this chapter we have discussed about the proposed network for the primary user emulation attack in cognitive radio network. We have done a detailed analysis and simulation of the network for PUE attack. Simulations were carried out to determine the performance of the proposed system model for PUEA attack in terms of probabilities of miss detection and false alarm. We showed various simulation results under different configuration of primary transmitters. Matlab codes for the simulations are attached in Appendices.

Chapter 5. Conclusion

In this MS thesis research, I have first investigated the general concepts of security threats to the cognitive radio networks. Then, I studied the performances for primary user emulation attacks from Neyman-Pearson criterion point of view. After that , I proposed a novel system model with different configurations of the primary users and conduct research on maximum likelihood criterion. Our experimental results demonstrate the statistical characteristics of the probability of false alarm and miss detection in the proposed system. I plan to make comprehensive performance comparison with existing research results in the future work.

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 = 100Km
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);
mu_p_2 = (10^(mu_p/10))^2;

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')
```

Appendix D

% Matlab code for Chapter 4 %

```
clear all;
close all;
clc;
MeanP_D1=[];
MeanP_D2=[];
num_run = 5000;   %testing times
N=100; %N loop numbers
M = 10; %%%%   number of malicious users
R =200;   %radius of outer circle, changeable 30:30:1500 meter
R0 = 30;%radius of inner circle
sigma_p1 = 8;   %fixed dB
sigma_p2 = 10;   %fixed dB
sigma_m = 5.5;   %fixed value dB
sigma_p1_2= (10^(sigma_p1/10))^2;
sigma_p2_2= (10^(sigma_p2/10))^2;

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 j^th malicious user and secondary
user %%%%%%%
for i= 1 : M % number of malicious users
    d(i)=sqrt((xCoordinates(i))^2 + (yCoordinates(i))^2);
end
sigma_m_2= (10^(sigma_m/10))^2;
Pt1 = 100e3; %%%%%%% Primary transmitting power = 100 Kw
Pt2 = 50e3; %%%%%%% Primary transmitting power = 100 Kw
```

```
A = log(10)/10;
x0 = 1e-9:1e-9:1e-3; %all x axis variables
Pm = 4;     %malicious user transmitting power 40watts
for dp1 = 1e3*(50:5:100); %%%%% distance between primary transmitter and
secondary user
P_D1_H2=[]; %initialize at a new location of d1
P_D2_H1=[];
dp2=150e3 - dp1
for J=1:1:N
%%%%% Received power at secondary user from primary transmitter %%%%%%
E_p1 =   sigma_p1*randn(1,num_run); %E_p dB in lognormal distribution
Gp1 = 10.^(E_p1/10);
Pr_p_tmp1 = Pt1*Gp1*dp1^(-2); %r. v. received power (watts) r.v.
E_p2 =   sigma_p2*randn(1,num_run); %E_p dB in lognormal distribution
Gp2 = 10.^(E_p2/10);
Pr_p_tmp2 = Pt2*Gp2*dp2^(-2); %r. v. received power (watts) r.v.
Pr_p_tmp=Pr_p_tmp1+Pr_p_tmp2;
Pr_p = sort(Pr_p_tmp);
mean_Pr_p=mean(10*log10((Pr_p))); %mean power in dB
mu_p1 = 10*log10(Pt1) - 20*log10(dp1); %calculation=mean(Pr_p) in db
=mean_Pr_p
mu_p2 = 10*log10(Pt2) - 20*log10(dp2); %calculation=mean(Pr_p) in db
=mean_Pr_p
mu_p= mu_p1+mu_p2;
mu_p_2 = (10^(mu_p/10))^2;
sigma_p12 = (1/A^2)*(log(mean(Pr_p.^2)) - 2*log(mean(Pr_p)));
P_gama =
(1./(A*x0*sigma_p12*sqrt(2*pi))).*exp(-((10*log10(x0)-mu_p)/(sqrt(2)*sigma_p12)
).^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 = 10*log10(Pm) - mean(40*log10(d)); %this mean is not correct.
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;
semilogx(x0,z); grid on;
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];
end;
MeanP_D1= [MeanP_D1; mean(P_D1_H2)]
MeanP_D2= [MeanP_D2; mean(P_D2_H1)]
end
plot(50:5:100, MeanP_D1,'r'); hold on; plot(50:5:100, MeanP_D2, '--'); grid on;
xlabel('Distance between Pt1 to the secondary receiver (km) ')
ylabel('Probability of false almarm and miss detection')
axis([50 100 0 0.5]);
legend('P\_D1', 'P\_D2')
```

References

[1] I. F. Akyildiz, W. Lee, M. C. Vuran, S. Mohanty, "A survey on spectrum Management in Cognitive Radio Networks," *IEEE Communications Magazine*, April 2008.

[2] Chetan N. Mathur, K.P. Subhalakshami, "Security issues in cognitive radio netwroks," Cognitive network: Towards Self-Aware Networks, 2007.

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

[4] R. Chen and J. Park "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," *Proc., IEEE workshop on Networking Technol. For Software Defined Radio Networks (SDR) 2006,* pp. 110-119, Sep. 2006.

[5] I. F Akyildiz , W-Y Lee, M. C. Vuran, S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Elsevier Jl. On Computer Networks*, vol. 50, pp. 2127-2158, May 2006.

[6] S. Anand, Z. Jin, K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," *To appear in Proc., IEEE symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN)* , Oct.2008.

[7] M. Vu, N. Devroye, V. Tarokh "The Primary Exclusive Region in Cognitive Networks," *Proc., IEEE Consumer Communications and Networking Conference (CCNC'2008)*, Jan. 2008.

[8] T. Yucek, H. Arslan, " A Survey Of Spectrum Sensing Algorithms for Cognitive Radio Applications" *IEEE Communications Surveys & Tutorials*, vol. 11, no.1, 2009.

[9] M. Vu, N. Devroye, M. Sharif, V. Tarokh, "Scaling Laws of Cognitive Networks," *Submitted to IEEE Journal on Selected Topics in Signal Processing*.

[10] Z. Jin, S. Anand, K. P. Subbalakshmi, "Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing," *Mobile Computing and Communications Review*, vol. 13, no. 2, 2009.

[11] S. Anand, R. Chandramouli "On the Secrecy Capacity of Fading Cognitive Wireless Networks" *Proc., IEEE Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM'2008)*, May 2008.

[12] L. F. Fenton, "The sum of log-normal probability distributions in scatter transmission systems," *IRE Trans. on Commun. Systems*, vol. 8, no.1, pp. 57- 67, March 1960.

[13] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications: Special Issue on Cognitive Radio Theory and Applications*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[14] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," *Proceedings, IEEE Internationall. Conference on Communications (ICC'2009)*, Jun. 2009.

[15] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of TV transmission in support of dynamic spectrum sharing," *Proceedings, IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN' 2005)*, pp. 338–345, Nov. 2005.

[16] Z. Chen, N. Guo, R. C. Qiu, " Demonstration of real time spectrum sensing for cognitive radio", *IEEE Communications Letters*, vol. 14, no. 10, oct. 2010.

[17] M. Vu, N. Devroye, V. Tarokh, "On the Primary Exclusive Region of Cognitive Networks", *IEEE Transactions On Wireless Communications*, vol. 8, no. 7, July 2009.

[18] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*. Boston, Academic Press, Inc., 1980.

[19] F. Digham, M. Alouini, M. Simo "On the Energy Detection of Unknown Signals over Fading Channels," *in Proc., IEEE International Conference Communications*, Anchorage, AK, vol. 5, pp. 3575-3579, May 2003.

[20] Y. Wu, B. Wang, K. J. Ray Liu. "Optimal Defense against Jamming Attacks in Cognitive Radio Networks using the Markov Decision Process Approach". IEEE Globecom 2010 proceedings.

[21] [Online].: http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf.

[22] J. L. Melsa and D. L. Cohn, *Decision and Estimation Theory*. McGraw-Hill Inc,.1978.

[23] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall Inc., New Jersey, 1996.

[24] J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Commun.*, vol. 6, pp. 13-18. Aug. 1999.

[25] S. Ross, Probability Models. Academic Press, 2003.

[26] Z. Jin, S. Anand, and K. P. Subbalakshmi, "NEAT: A Neighbor Assisted Spectrum Decision Protocol for Resilience against Primary User Emulation Attacks," Technical Report, Dec. 2009. Available: http://www.stevens.edu/suba.

[27] P. Kolodzy, "Spectrum policy task force: findings and recommendations," proceedings," *International symposium on Advanced Radio Technologies (ISART'2003)*, Mar. 2003.

[28] Z. Chen, T. Cooklev, C. Chen and C. Pomalaza-R´aez "Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks" *IEEE 28th International Performance Computing and Communications Conference (IPCCC)*, 2009.

[29] A. Goldsmith, Wireless Communications. Cambridge University Press, 2005.

[30] S. M. Ross, Introduction to Probability Models, Ninth Edition. Academic Press, 2007.

[31] B. Fette, "Three obstacles to cognitive radio," EE Times, Aug. 2004, quoting Joseph Mitola.

[32] http://en.wikipedia.org/wiki/Spectrum_management.

[33] http://www.wael-guibene.com/CEA_LETI.pdf.

[34] I. F. Akyildiz, W.-Y. Lee, K. R. Chowdhury: "CRAHNs: Cognitive Radio Ad Hoc Networks", Ad Hoc Networks, Elsevier, vol. 7, no. 5, pp. 810-836, July 2009.

[35] A. S. Kamil, I. Khider, "Open Research issues in Cognitive Radio," *16 Telecommunication Forum (TELFOR'2008)*, November 25-27, 2008.

[36] E. Hossain, L. Le, N. Devroye and M. Vu, "Cognitive Radio: From Theory to Practical Network Engineering," Available online: http://www.ece.uic.edu/~devroye/research/ch4.pdf.