THE UNIVERSITY OF HULL

Detection Performance and Mitigation Techniques in CR Networks

Being a Thesis submitted for the Degree of

Doctor of Philosophy

In the University of Hull

By

Mahmod Ammar, MSc

September 2017

Acknowledgements

First and foremost, I would like to thank my principal supervisor Dr. Nick Riley for his great guidance, advices and encouragement over the years. My sincere gratitude to all academics and colleagues within the research group.

I am also so grateful to all those people who have supported me and had contributions in making this thesis possible, my upmost thanks to the engineering department staff, graduate school and my second supervisor Dr. Kevin Paulson for the valuable suggestions and support.

Finally, I wholeheartedly thank my great parents, my wife and my lovely family for their understanding, encouragement and support.

Dedication

I would like to dedicate this work

To my wife, parents, and lovely family

Also

To LIBYA as a country of unlimited support

To Al-zawya university as a university of inspiration

Contents

List of Figures

List of Tables

Acronyms and Abbreviations

BS	Base Station
CCC	Common Control Channel
CDF	Cumulative Distribution Function
CH	Cluster Head
CR	Cognitive Radio
CSMA	Carrier Sensing Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSS	Cooperative Spectrum Sensing
CU	Cognitive User
DDT	Distance Difference Test
DoS	Denial of Service
DRT	Distance Ratio Test
DSA	Dynamic Spectrum Access
FC	Fusion Centre
FCC	Federal Communications Commission (of United States)
FDOA	Frequency Difference of Arrival
GPS	Global Position System
I.I.D	Independent and Identically Distributed
LV	Location Verifier
MAC	Media Access Control
NPCHT	Neyman-Pearson Composite Hypothesis Test
OFCOM	Office of Communications (of United Kingdom)
PDF	Probability Density Function
PDR	Packet Delivery Ratio
PU	Primary User
PUEA	Primary Users Emulation Attack

QoS ..... Quality of Service

RF ..... Radio Frequency

RX ..... Receiver

SNR ..... Signal to Noise Ratio

SSDF ..... Spectrum Sensing Data Falsification

SU ..... Secondary User

TDOA ..... Time Difference of Arrival

TX ..... Transmitter

UWB ..... Ultra Wide Band

WRAN ..... Wireless Regional Area Network

WSPRT ..... Wald's Sequential Probability Ratio Test

List of Symbols

L_i	Binary Local Decision i
(r_p, θ_p)	Cartesian Coordinates of Users
k	Constant Path-Loss Factor
Λ	Decision Variable of Neyman-Pearson Test
W_n	Decision Variable of Wald's Sequential Probability Test
T_D	Direct Trustworthiness of a User
d_p	Distance Between PT and SU
d	Distance Between Transmitter and Receiver
R_0	Exclusive Distance from the SU
Y	Final Decision
x(f)	Fourier Transform of Signal X(T)
f	Frequency
h_r	Heights of Receive Antennas
h_t	Heights of Transmit Antennas
T_H	Historical Trust Value
$\bar{x}$	Impact Weight of Direct Trust
$\bar{y}$	Impact Weight of Historical Trust
L_{gf}	Local Decision of Good User f
L_{gi}	Local Decision of Good User i
L_{mi}	Local Decision of Malicious User i
L_{mk}	Local Decision of Malicious User k
L_{di}	Local Decision of User i
PL	Log Normal Shadowing-Path Loss
n	Log Normal Shadowing-Path Loss Exponent
P_m	Malicious Users Power
μ	Mean of Distribution

R	Network Radius
H_0	No Primary Signals
n (t)	Noise Signal
G	Number of Good SUs
K	Number of Malicious Users
γ	Path Loss Exponent
$P^{P_r}(X_i)$	PDF of Received Power at a Secondary due to the Primary Transmission
$P^m(X_i)$	PDF of Total Received Power from all Malicious Nodes
λ	Predefined Threshold in Neyman-Pearson Test
s(t)	Primary Signal
H_1	Primary Signals Exist
Tx	Primary Transmitter Signal
P_t	Primary Transmitting Power
PF	Probability of False Alarm
PM	Probability of Missed Detection
P	Punishment Factor
ε_p	Random Shadowing Effect
G_r	Receive Antenna Gains
P_r	Received Power
$P^{(mi)}$	Received Power from Malicious User i
$Pr^{(p)}$	Received Power from the PU
y (t)	Received Signal
d_0	Reference Point in Free Space Model
c	Speed of Light
σ	Standard Deviation
L	System Loss in Propagation Models
Á	Threshold of Trustworthiness

M	.....	Total Number of Users
T_T	.....	Total Value of Indirect Trust
G_t	.....	Transmit Antenna Gains
P_t	.....	Transmitted Power
$x(t)$	.....	Transmitted Signal
T_g	.....	Trust of Good User
T_{gf}	.....	Trust of Good User f
T_{gi}	.....	Trust of Good User i
T_m	.....	Trust of Malicious User
T_{mi}	.....	Trust of Malicious User i
T_{mk}	.....	Trust of Malicious User k
T_i	.....	Trust of User i
σ	.....	Variance of Distribution
λ^*	.....	Wavelength
χ	.....	Zero-Mean Gaussian Distributed Random Variable in Log Normal Shadowing

Abstract

Pervasive wireless communications rely enormously on spectrum utilization; the increase in demand for new wireless services and their application has led to spectrum scarcity. Spectrum limitations can be resolved by cognitive radio (CR) which is a technology that allows secondary users (SUs) to use the spectrum when it is not occupied by primary users (PUs). In this thesis, the security issues that decrease CR performance are discussed; there are two major threats i.e. primary user emulation attack (PUEA) and spectrum sensing data falsification attack (SSDF).

Firstly, the CR network (CRN) is simulated whereby PUs and SUs are presented in the system with the presence of multiple malicious users that are randomly located within a circle of radius (R). The simulation results, based on an analytical model, show that the false alarm probability is significantly affected by the network radius R and malicious users' number, and it is proved that there is a range of R over which the PUEAs are most successful. Secondly, a transmitter verification scheme (direct scheme) and indirect trust scheme that considers the users' history are presented; the results proved that if the signal to noise ratio (SNR) is raised, correspondingly the trustworthiness of the PU is considerably increased. Based on these two schemes, the trustworthiness of the PU is much higher than that of the malicious user and because the indirect scheme considers the historical behaviour of the user, it improves the user's trustworthiness.

Finally, cooperative spectrum sensing (CSS) approaches are proposed, namely, a trust based approach, a punishment based approach and a dedicated punishment based approach. It is proved that these proposed CSS approaches outperform the traditional majority scheme despite a high number of malicious users. In addition, the dedicated punishment approaches which punish only the malicious users outperform the other approaches.

1 Introduction

Cognitive radio (CR) is the key technology that allows users to access dynamically the available spectral opportunities without any interference. The fundamental objective of CR is to enable an efficient utilisation of the wireless spectrum through a highly reliable approach. Through this approach, spectrum holes will be identified and therefore the available spectrum and the appropriate transmitting parameters can be selected.

Primary users (PUs) can be defined as wireless devices that have a prior access to operate in a specific spectrum band. However, their communication should not be interrupted or interfered with by any other users. Therefore, CR users must be able to sense the spectrum and utilise the unused bands in an opportunistic manner [1] [2]. In the literature, CR users are also referred to as secondary users (SUs).

Thus spectrum sensing is the key technology that enables the efficient operation of both the PU and the CR users. Recently, the security issues of CR networks (CRNs) have drawn more and more research attention. Due to the intrinsic properties of the CR paradigm, which produce new threats and challenges to wireless communications, the potential security vulnerabilities and mitigation techniques are discussed in this thesis, and also the background, motivation and advances of CR technology are introduced.

Some techniques to improve the detection performance and mitigate threats in CRN are proposed. Signal detection is achieved based on an analytical model and also using a

transmitter location verification scheme. Moreover, a cooperative spectrum sensing (CSS) technique based on trust management is proposed.

1.1 Motivation

The main aim of CR is to improve spectrum utilisation by opportunistically accessing the licensed spectrum without causing interference to the licensed users. The spectrum can be sensed based on many approaches, e.g. energy detection methods [3], matched-filtered detection methods [4] and cyclostationary detection methods [5].

The design of CRNs has led to new threats because there are some malicious users that aim to emulate the characteristics of the PU to gain a priority access to a channel used by another SU. Such attacks by malicious users are called primary user emulation attacks (PUEAs). There is another scenario that occurs in CR because of a shadowing or fading between the users, which causes uncertainty as to whether there is a signal from the PU or whether it is a white space [6]. This uncertainty problem can be mitigated by CSS to make a final decision about the spectrum availability [7] [8].

Mitigating these issues presents the main motivation of this thesis and, therefore, approaches to improve the security of CRNs and to increase detection performance are proposed for robust and secure access.

1.2 Objectives and Contributions

1.2.1 Objectives

This thesis aims to study the detection performance of CR and to improve spectrum utilisation and the efficiency of spectrum usage, focusing on security aspects in terms

of mitigating vulnerability and threats. More specifically, the study has the following objectives:

- ✓ Considering security problems arising from a PUEA in CRNs, investigate the impact of this attack on CRNs and develop a detection approach based on an analytical model.
- ✓ Improving trustworthiness among nodes in CRNs by generating users' trust values and considering the historical behaviour of users in the system.
- ✓ Developing an efficient CSS scheme based on users' trust and punishment approaches imposed on the users in a CRN.

1.2.2 Key Contributions

In this thesis, several security aspects of CR systems are investigated. The performance of detection schemes have been improved, not only on the detection performance aspects but also in terms of the impact of threats on CRN.

The main contributions of this thesis are summarised as follows:-

- ❖ **PUEA Remedy based on an Analytical Model:**

  The Neyman-Pearson composite hypothesis test (NPCHT) is used in this work to overcome the security threats and detect the PUEA by examination of the probability density function (PDF) of the received signals. Based on these PDFs, the probability of a successful PUEA (False Alarm) and the probability of a missed detection are obtained.

- **Trust Management Mechanism for the Detection of PUEA based on the Localization of Signal Source:**

  To ensure the trustworthiness among nodes in CRN, a mitigation technique for a PUEA is proposed. This technique depends on the Localization of the signal source. Also, this approach uses a trust mechanism for the detection of a PUEA. The security algorithm presented for improving the user's trustworthiness introduces direct and indirect trust models.

- **Trust and Punishment based Approaches for Secure Spectrum Access in CSS.**

  To improve spectrum utilisation, detection performance and the efficiency of spectrum usage, a CSS scheme based on trust and punishment approaches is investigated. The users make local decisions on the presence or absence of the PU signal, and then the fusion centre (FC) makes the final decision about the spectrum status. Based on these approaches, the mechanism can improve the security of the CRN and increase the sensing performance.

1.3 Thesis Outline

The remainder of this thesis is organised as follows:

Chapter 2:

Chapter 2 introduces the basic concepts of CRN, including their design and operational challenges. It presents a review of the technical challenges, such as spectrum sharing and access methods, and how these relate to dynamic spectrum access (DSA).

Chapter 3:

Chapter 3 summarises the security challenges in CRNs and the current methods used in spectrum sensing for the detection and mitigation of threats.

Chapter 4:

This chapter focuses on the security problems arising from a PUEA in CRNs. The impact of this type of attack on CRNs is studied, and detection approaches are also investigated. The NPCHT is used to detect the PUEAs.

Chapter 5:

This chapter is concerned with ensuring the trustworthiness among nodes in CRN. Two trust management schemes are proposed, namely, direct and indirect trust schemes. The direct scheme obtains trust values based only on the Localization of the signal source; it takes advantage of the fact that it is not possible for the malicious user to mimic both the coordinates and the power level of a PU. While the indirect trust model combines the direct trusts and the historical trust values.

Chapter 6:

To improve the spectrum utilisation, the detection performance and the efficiency of spectrum usage, a CSS scheme is proposed based on trust and punishment approaches. The users make local decisions on the presence or absence of a PU signal, and then the FC makes the final decision about the spectrum status. Based on these approaches, the mechanism can improve the security of the CRN and increase the sensing performance.

Chapter 7:

The conclusion, work limitations, bibliography and appendices are presented in this chapter.

1.4 List of Publications

The work presented in this thesis has led to a list of publications including papers published in international journals, conferences, meetings and workshops. These are:

Journal Publications

- Mehdawi, M., **Ammar, M.**, Riley, N., Paulson, K., Fanan, A, (2013). Spectrum occupancy survey in Hull-UK for CR applications: measurement & analysis. International Journal of Scientific & Technology Research, 2(4), 231-236.

Conference Publications

- **Ammar, M.**, Riley, N., Mehdawi, M, A. F., & Zolfaghari, M. Physical Layer Security in CR Networks. International Conference on Artificial Intelligence, Energy and Manufacturing Engineering (ICAEME'2015) Jan. 7-8, 2015 Dubai (UAE).
- **Ammar, M,** Nick Riley, Meftah Mehdawi, Anwar Fanan, Mahsa Zolfaghari. Detection Threats and Mitigation Techniques in CR based on Localization of Signal Source and Trustworthiness. 4th International Conference on Advances in Engineering Science (ICAESAM'2015).

- **Ammar, M.**, Riley, N., Mehdawi, M, A. F., & Zolfaghari, M. Security Aspects in CR Networks Detection and Mitigation of PU Emulation Attacks, In the Fifth International Conference on Advances in CR COCORA 2015.
- **Ammar, M.**, Mehdawi, M., Riley, N., Fanan, A., Paulson, K., & Zolfaghari, M. "A Spectrum Sensing Test Bed based on Matlab and USRP2".(2013). Int'l Conference Image Processing, Computers and Industrial Engineering (ICICIE'2014) Jan. 15-16, 2014 Kuala Lumpur (Malaysia).
- Mehdawi, M., Riley, N., **Ammar, M.**, & Zolfaghari, M. (2012, November). Comparing historical and current spectrum occupancy measurements in the context of cognitive radio. In *Telecommunications Forum (TELFOR), 201220th*(pp. 623-626). IEEE.
- Mehdawi, M. A., Riley, N. G., **Ammar, M.**, Fanan, A., & Zolfaghari, M. (2013, November). Cooperative wideband spectrum sensing with multi-bit hard decision in cognitive radio. In Telecommunications Forum (TELFOR), 2013 21st (pp. 220-223). IEEE.
- Mehdawi, M., Riley, N. G., **Ammar, M.**,Fanan, A., & Zolfaghari, M. (2014, November). Experimental detection using cyclostationary feature detectors for Cognitive Radios. In Telecommunications Forum Telfor (TELFOR), 2014 22nd (pp. 272-275). IEEE.
- Mehdawi, M., A. Buhafa, N. Riley, K. Paulson, **Ammar, M**: Evaluation of Interference between Antennas using Cosite Analysis Model. In international conference on Advances in Communication and Information

Technology (ACEEE 2012), September 2012.

- M. Mehdawi, N. G. Riley, **M. Ammar**, A. Fanan, M. Zolfaghari: Spectrum Occupancy Measurements and Lessons Learned in the Context of Cognitive Radio. In Telecommunications Forum (TELFOR), November 2015.
- A. Fanan, N. Riley, M. Mehdawi, **M. Ammar**, M. Zolfaghari: Comparison of Spectrum Occupancy Measurements using Software Defined Radio RTL-SDR with a Conventional Spectrum Analyzer approach. In Telecommunications Forum (TELFOR), November 2015
- M. Zolfaghari, N. G. Riley, M. Mehdawi, A. Fanan, **M. Ammar**, F. Meng: Quality Measurements of an UWB Reduced-size CPW-fed Aperture Antenna. In Telecommunications Forum (TELFOR), November 2015.

2 Cognitive Radio

2.1 Background

CR was conceived in 1998 by Mitola [1]. CR can be defined as a radio system that considers its surrounding environment via the functions of sensing and learning, and it has the capability of changing its parameters dynamically and independently [2] [9]. The main objective of CR is to improve spectrum usage using the idea of sharing the spectrum with the PU without any interference. Thus, the SU must vacate the channel whenever the PU needs to transmit again.

CR has two distinctive characteristics, namely cognitive capability and configurability, which allow the CR to interact in real time and find the communication criterion according to the quality of service (QoS) [10]. The capability is defined as the ability to sense the surrounding radio environment, analyse the acquired information and accordingly identify the best available spectrum bands for operation. The configurability can be defined as the SU's ability to adopt its operational parameters such as the transmit-power, carrier frequency, bandwidth and modulation strategy, based on the data collected from the surrounding environment and subsequently the SU can operate optimally in the candidate spectrum bands.

2.2 Why is Cognitive Radio?

If the scarcity of spectrum availability is artificial, as many researchers believe, then this misconception is strengthened by the FCC frequency chart [11] and Ofcom [12],

which show multiple allocations over all of the frequency bands. On the other hand, a large portion of the assigned spectrum is only used sporadically.

Also, some measurements of the spectrum occupancy are obtained in the Hull area, which shows the usage of the spectrum. The measurement equipment employed in this study is illustrated in Figure 2.1. A bilog antenna CBL 6143, with a frequency range of 30 to 3000 MHz, fed the received signal to an agilent E4407B spectrum analyser. The spectrum analyser converted the received signal into power versus frequency traces using an internal mixer, sampler, and a computational fast-fourier transform (FFT) engine. The traces collected from the spectrum analyser were transferred to a desktop computer by a general-purpose interface bus (GPIB), where the raw data was stored [13].

Figure 2.1 Equipment for spectrum occupancy measurement [13]

Figure 2.2 shows the measured received power versus frequency plot for the whole frequency range of the measurement (180 MHz to 2700 MHz). It is clear that the spectrum usage is concentrated on certain portions of the spectrum, while a significant amount of the spectrum remains unutilized. This appears to be a contradiction to the concern of spectrum shortage, since in fact there is an abundant amount of spectrum,

and the spectrum shortage is partially an artifact of the regulatory and licensing process.

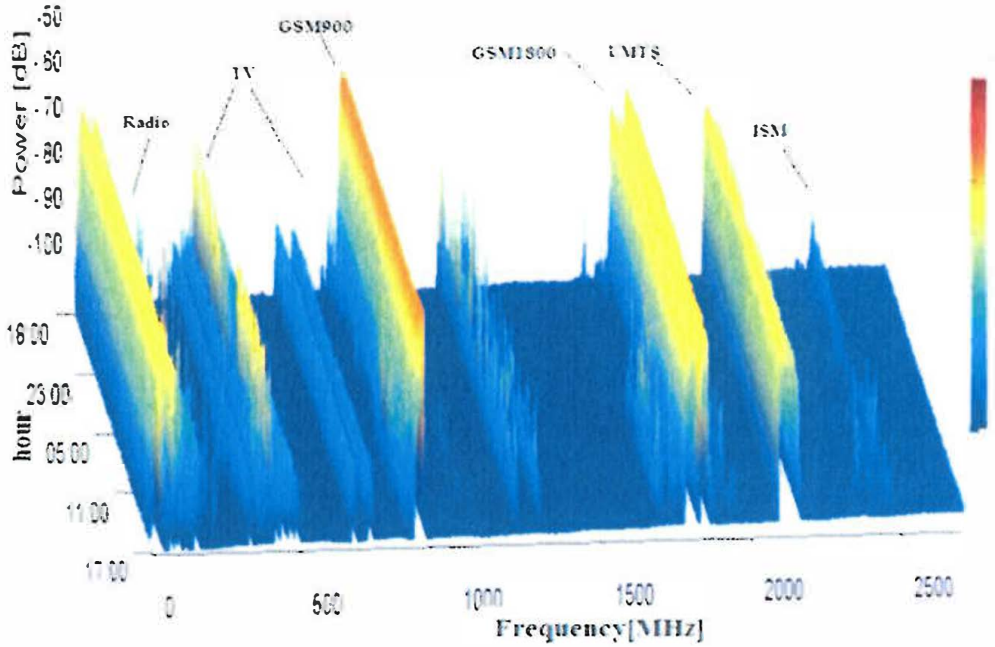

Figure 2.2 Received power versus frequency band (80MHz-2700MHz)

Therefore, the spectral efficiency can benefit from the dynamic reuse of the available spectrum. Such improved usage could break the current spectrum availability bottleneck.

2.3 CR Functions

The cognitive cycle in Figure 2.3 below illustrates how the basic functions of CR work.

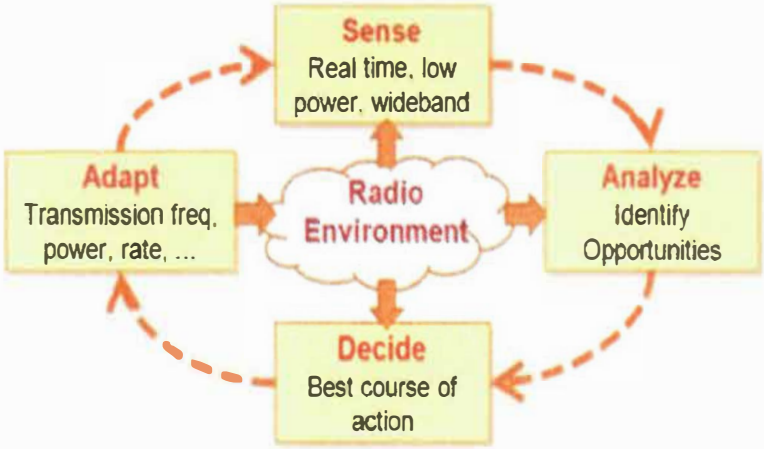

Figure 2.3 Functional architecture of a CR cycle

The duty cycle above contains the following major steps:

A. Spectrum sensing

Spectrum sensing can be defined as the ability of the CR to sense the amount of electromagnetic field in different spectrum bands and calculate some parameters such as the power level. In this step, the radio environment is constantly monitored, and spectrum holes are detected by a CR. In order to improve the usage of the spectrum, CR must monitor the whole of the bands rather than finding only the spectrum holes.

Spectrum sensing can be performed on a non-cooperative basis using energy detection [3], cyclostationary feature detection [5] and Matched Filter [14]. Recently, CSS has been used heavily because of its high performance in terms of detection accuracy [15].

B. Spectrum analysis

The spectrum is analysed in order to estimate the spectrum holes (spectral opportunities) that can be used without harm to the PUs. Spectrum analysis aims to determine if the QoS parameters (e.g., mean delay, packet loss probability) are provided for CR users. The data on the spectrum holes is analysed in order to estimate the interference level and the channel capacity which is then forwarded to the spectrum decision stage [16].

C. Spectrum access decision

After the spectrum is sensed and analysed, the next step is to take a decision about the availability of the spectrum i.e. finding the spectrum band to use. Some parameters need to be known in order to transmit without interference; these parameters include the transmission start time, the transmission power and the modulation rate [16].

2.4 Static Spectrum Access vs. Dynamic Spectrum Access

One of the reasons behind the spectrum shortage is using the radio resource based on a fixed allocation which is known as static spectrum access. In order to solve this issue, dynamic spectrum access (DSA) is used because it deals with the limited spectrum by allowing the SUs to access the PUs bands opportunistically [17].

Figure 2.4 illustrates the concept of spectrum holes in DSA. Spectral holes are also known as white spaces, which can be defined as the bands that can be used without any interference.

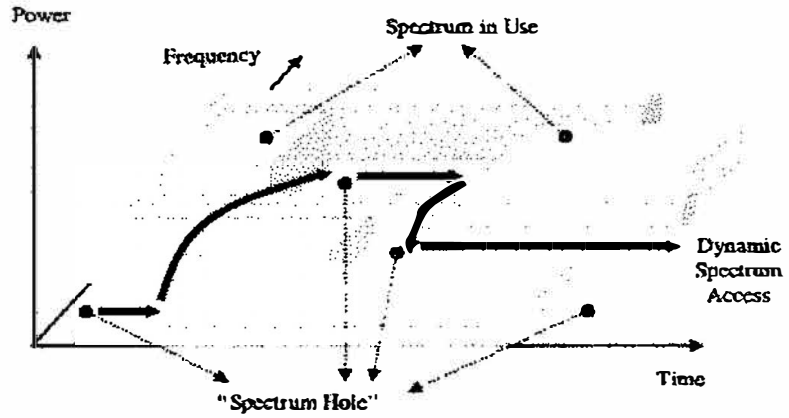

Figure 2.4 Concept of a spectrum hole [18]

❖ DSA Scenario

An example of DSA is explained in Figure 2.5, where there are SUs present along with the primary transmitters PT1 and PT2 in the network. Because the coverage of the PUs PT1 and PT2 is accessible by CR1 and CR2, both users CR1 and CR2 can access the band if the PUs PT1 and PT2 are not using it. The CRs always check to verify if the channel is still unused by the PUs, otherwise they must stop the transmission and look for another channel to use.

Two interference categories can be mitigated by DSA, namely harmful interference from malfunctioning devices and harmful interference from malicious nodes [19].

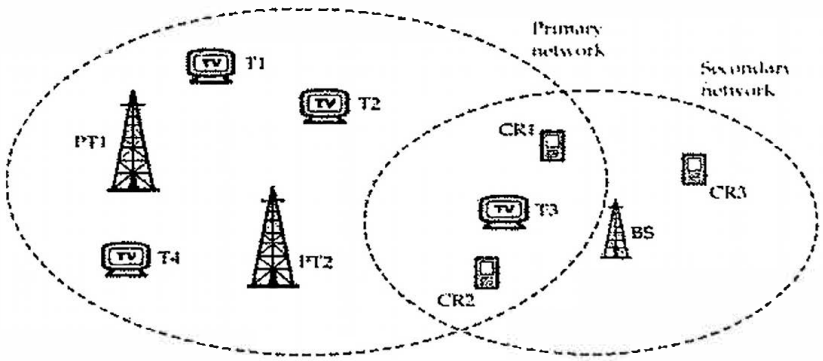

Figure 2.5 Coexistence of multiple primary and SU networks [20]

2.5 Approaches to Spectrum Sensing

Because spectrum sensing is a vital function in CR, it must be very accurate to avoid causing interference. There are two approaches to achieve this function. Firstly, there is transmitter detection, which is classed as a non-cooperation approach. In this approach, there are three widely used methods, i.e. matched filter, energy detection and cyclostationary detection. The second approach is called cooperative detection, and uses either a decision fusion method or a data fusion method [21]. These methods are explained in detail in the following sections. Spectrum sensing algorithms can be classified as shown in Figure 2.6.

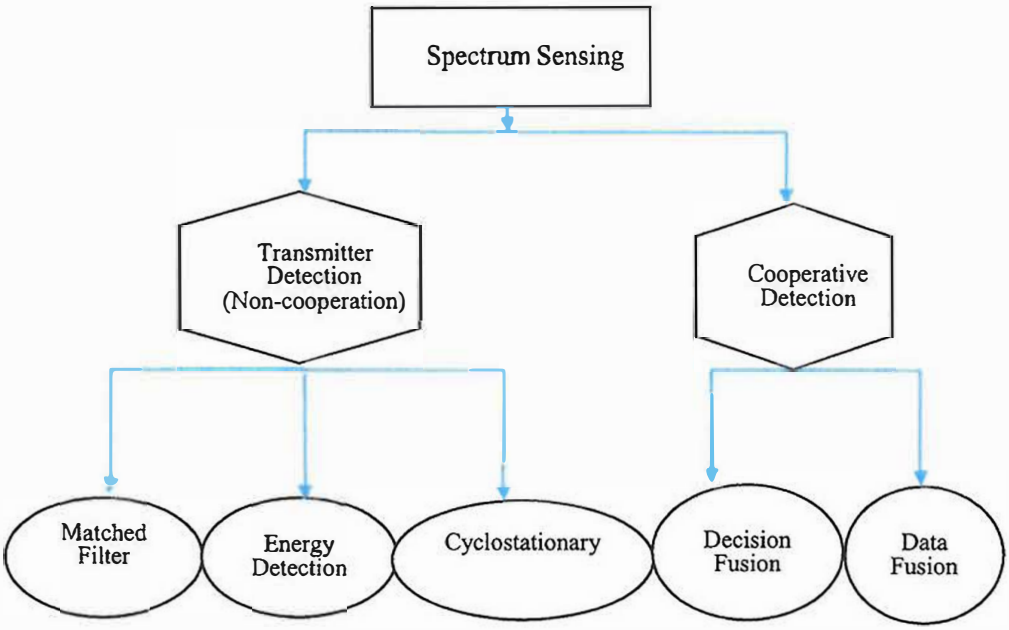

Figure 2.6 Spectrum sensing algorithms

2.5.1 Aspects and Methods of Non-CSS techniques

A. Spectrum Sensing using Matched Filter Detection

Matched filter detection needs prior information about the PU, for example the SU must know the type of modulation, packet format, and the pulse shape. If this information is inaccurate, the sensing result and the performance of this scheme will be poor. A block diagram for the matched filter approach is shown in Figure 2.7(a). The main advantage of this scheme is that it produces a good sensing result in a short sensing time [14].

B. Spectrum Sensing using Energy Detection

The energy detection approach does not require prior knowledge about the PUs, which was the main requirement in the matched filter approach. The main advantage of this method is that it has a relatively low implementation and computational cost [22]. On the other hand, the drawbacks of energy detection are its low detection performance when the signal to noise ratio (SNR) is low, so it cannot distinguish between the PU's signals and interference from other CUs [23]. Figure 2.7(b) illustrates the block diagram of the energy detection approach.

C. Spectrum Sensing using Cyclostationary Detection

In this kind of detection, the cyclostationary feature of the received signal statistics is considered for spectrum sensing. Transmitted signals are generally modulated signals with certain carriers, pulse trains, repeating spreading, hopping sequences or cyclic prefixes, with inherent periodicities. This method can be used to differentiate between the PU signals and the noise signal because the statistics of the PU signal possess cyclostationary features while the noise signal is a stationary process with no

such feature [10]. The block diagram of cyclostationary detection is shown in Figure 2.7(c). This method of detection is considered robust to noise uncertainty, so its performance is good even in very low SNR regimes. There are some disadvantages in feature detection, for example, it needs the knowledge of the PU's cyclic frequency, and this is not realistic for many applications of CR.

In comparison with energy detection, cyclostationary detection performs the transformation from the time domain (TD) into the frequency domain (FD) in order to produce the hypothesis in the new domain. Because of these calculations, the computational cost of this approach is high.

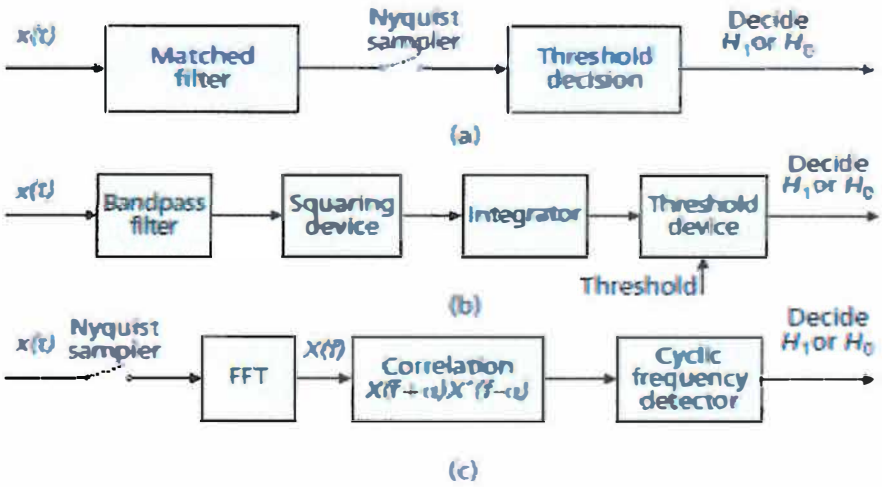

Figure 2.7 (a) matched filter, (b) energy detection, and (c) cyclostationary detection block diagrams

A summary of the advantages and disadvantages of spectrum sensing algorithms is given in Table 2.1.

Table 2.1 Summary of the advantages and disadvantages of spectrum sensing algorithms

Spectrum sensing algorithm	Advantages	Disadvantages
Matched filter	Optimal performance - Low computational cost	Requires prior information of the PU
Energy detection	Does not require prior information – Low computational cos	Poor performance for low SNR - Cannot differentiate users
Cyclostationary feature	Valid in low SNR region - Robust against interference	Requires partial prior information - High computational cost

2.6 Traditional Spectrum Sensing Challenges

Detection performance greatly depends on many factors. The most frequently found problems are multipath fading, shadowing, and the receiver uncertainty problem. Detection performance is evaluated based on the probabilities of false alarms and missed detections. A false alarm occurs when an SU concludes that a PU uses the spectrum but actually the spectrum is not in use by a PU. On the other hand, a missed detection occurs when the SU declares that the PU is absent but actually the spectrum is occupied by the PU. Both missed detection and false alarms reduce the spectrum efficiency.

Hidden PU issue: As shown in Figure 2.8, this problem occurs when a CR user causes interference to the PU (receiver) and this is because the signal of the primary transmitter (Tx) could not be detected because of the locations of the devices.

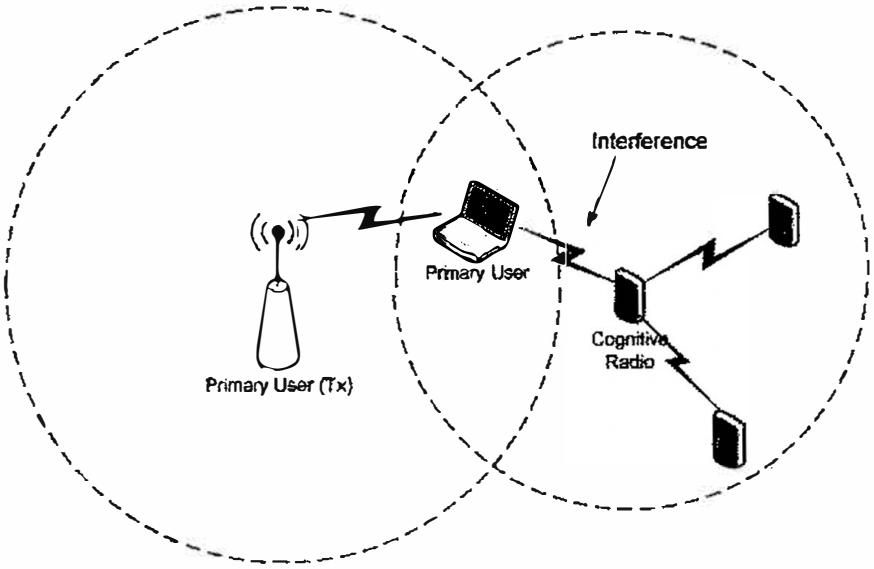

Figure 2.8 Hidden PU issue in spectrum sensing

Multipath and Shadowing Issue: The multipath issue occurs if multiple attenuated copies of the PU signal are presented, so the PU's signal cannot be correctly detected. The shadowing issue always happens when an object like a building blocks the PU signal.

2.6.1 Radio Wave Propagation

One of the fundamental limitations of the wireless radio channel is the propagation that affects the performance of wireless communications systems. The transmitted signals incur path loss as electromagnetic waves propagate from source to destination. The major categories of radio propagation can be given as follows:

- **Free Space Propagation**

Because both the transmitter and receiver have a clear line of sight path between them in the free space model as shown in Figure 2.9, so only the distance between them affects the way in which the field strength reduces. This model is used for simple path

loss estimations because of its simple form and limited number of required parameters [24][25].

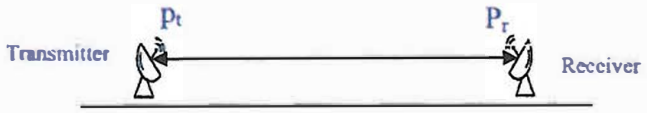

Figure 2.9 Free space model

The Friis transmission equation, which calculates the received signal power according to the signal loss in free space, is given as:

$$P_r(d)=(P_t G_t G_r \lambda^{*2})/(4 \Pi d)^2 \qquad 2.1$$

P_t is the transmitted power, P_r is the received power, G_t and G_r are the transmit and receive antenna gains, λ^* is the wavelength λ^* = c/f, c = speed of light, and f = frequency, d is the distance between the transmitter and receiver, P_t and P_r are in the same units, and G_t and G_r are dimensionless quantities.

It is common to select $G_t=G_r=1$ in simulation. The free space propagation can also be estimated in relation to a reference point d_0 as shown in Figure 2.10; a typical value for d_0 is 1m to 1km [26].

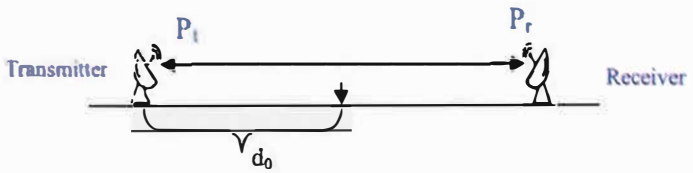

Figure 2.10 Free space model with a reference point

$$P_r(d) = P_t K (d_0/d)^2 \quad d \geq d_0 \qquad 2.2$$

K: Constant path-loss factor, d_0: a reference point

- **Ground Wave Propagation**

The two-ray model is one of the ray tracing models that predicts signal variation resulting from ground reflection. The two-ray model is used when a single ground reflection dominates the multipath effect. Both the direct path and the ground reflection path are considered in the two-ray ground reflection model. This model gives a more accurate prediction at a long distance than the free space model [27]. If d is the distance between the transmitter and the receiver, the received power at distance d is:

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \qquad 2.3$$

where h_t and h_r are the heights of the transmit and receive antennas respectively, and L is the system loss.

Generally, the following simplified model for path loss as a function of distance is commonly used for a system design:

$$P_r = P_t K (d_0/d)^{\gamma} \qquad 2.4$$

γ is the path loss exponent, which depends on the propagation environment; for example, propagation that approximately follows a free-space or two-ray model is set to 2 or 4 respectively. K is the Constant path-loss factor, and d_0 is a reference point. Table 2.2 shows the typical path loss exponent for different environments.

Table 2.2: Typical path loss exponents

Environment	Path loss exponent , γ
Free space	2
Urban area	2.7 to 3.5
Suburban area	3 to 5
Indoor (line-of-sight)	1.6 to 1.8

- **Shadow Fading**

In wireless communication, fading is the variation of the signal strength with respect to time/distance. Fading in the wireless environment is caused by multipath propagation and the mobility of objects. It is not only the path loss that affects the received signals, but also a signal will typically experience random variation due to blockage from objects in the signal's path. So a model that considers the random attenuation due to these effects is also needed. Because the location and size of the blocking objects, as well as the changes in reflecting surfaces and scattering objects that cause the random attenuation are generally unknown, statistical models are widely used to characterise this attenuation. The log-normal shadowing model is the most frequently used model for this additional attenuation; [28] [29] confirm that the log-normal shadowing is an accurate model in both outdoor and indoor radio propagation environments.

The log-normal shadowing model is a statistical model for variations in the received signal amplitude due to blockage [30]. It is used in the far field region of the transmitter, if $PL(d_0)$ is the path loss measured in dB at a distance d_0 from the transmitter, then the path loss (the loss in signal power measured in dB when moving from distance d_0 to d) at an arbitrary distance $d > d_0$ is given by:

$$PL_{d_o \to d}(dB) = PL(d_0) + 10n\log_{10}(d/d_0) + x \qquad 2.5$$

PL (d_0) = Path loss in dB at a distance d_0

PL ($d > d_0$) = Path loss in dB at an arbitrary distance d

n = Path loss exponent

χ = A zero-mean Gaussian distributed random variable (in dB) with standard deviation σ. If there is no shadowing effect, then χ is zero.

2.7 Cooperation and Local Spectrum Sensing

CSS is important approach in CR networks because multiple users are incorporated for PU detection [31]. By this approach, the accuracy and reliability of PU detection is increased. Furthermore the fading, shadowing and model uncertainties issues can be solved and, consequently, it reduces the required sensing time [32][33].

Centralised CSS

In this method, the FC is used to collect sensing information from the CUs and identify the spectrum availability, and then control the CR traffic [34] [35]. Figure 2.11(a) shows an example of a centralised CSS where five users, CR1, CR2, CR3, CR4 and CR5, forward their local spectrum sensing information to the FC in order to take a decision about the PU activity.

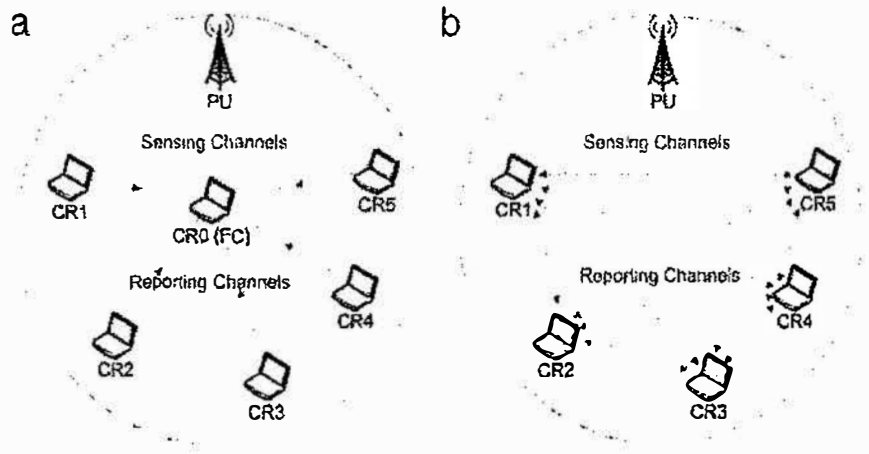

Figure 2.11 Cooperative sensing: (a) centralized, (b) distributed [36]

Decentralised CSS

The main idea in decentralised CSS is that CUs perform their local sensing and share the local sensing outcome with others [37] [38]. As in Figure 2.11 (b), each CR user sends its own sensing data to other users, combines its data with the received sensing data from other users, and decides whether or not the PU is present by using a local criterion.

Great improvements in system performance can be achieved using the CSS because:

a) The hidden node problem is reduced significantly compared to traditional spectrum sensing.

b) More accurate signal detection is achieved and false alarms are decreased.

Although the CSS has good performance, there are some disadvantages in CSS approaches such as:

a) Channels that are dedicated to control information transmission can face the problems of uncertainty and other issues, thus the performance of CSS will be greatly decreased (in some circumstances).

b) The CUs send their sensing data to each other or to the BS, and this leads to a cooperative overhead.

c) The global decision reliability decreases if the set of local decisions includes some of low reliability and are combined to make a global decision at the FC.

Generally, CSS algorithms can be categorised into data fusion and decision fusion, depending upon which type of sensing data is transmitted to the FC [38] [39].

2.8 Fusion Rules in Cooperative Spectrum Sensing

2.8.1 Decision Fusion

This approach uses the decisions of each user rather than the whole data. Each user in the network transfers its one-bit final decision to the FC. The FC then deploys a specific fusion rule to make the final decision [40]. These rules use 1 for signal present and 0 for signal absent. There is no other information available for the FC.

The section below describes the decision fusion rules commonly used for taking decision in spectrum sensing.

❖ **Logic OR Rule**

In the OR rule, the final decision of the FC is a logical one (1) when any local decision sent to the FC is a logical one (1) [41]. The probabilities of false alarm and detection can be given by:

$$p_f = 1 - \prod_{i=1}^{v} (1 - P_f^i) \quad 2.6$$

$$p_d = 1 - \prod_{i=1}^{v} (1 - P_d^i) \quad 2.7$$

where P_f^i and P_d^i denote the probabilities of false alarm and detection in the CR node i, respectively.

❖ **Logic AND Rule**

The final decision of the FC is a logical one (1) when all local decisions sent to the FC are a logical one (1) [42]. The probabilities of false alarm and detection can be given by:

$$p_f = \prod_{i=1}^{v} (P_f^i) \quad 2.8$$

$$p_d = 1 - \prod_{i=1}^{v} (P_d^i) \quad 2.9$$

❖ **C-out-of-V Logic Rule**

The final decision is the logic "1" only if c or more than c CRs decide "1", where c ∈ [1, v]. If the decisions from the v CRs are independent [43], so the probabilities of false alarm and detection can be given as:

$$p_f = \sum_{i=0}^{v-c} \binom{v}{c+i} (1 - P_f^i)^{v-c-i} (P_f^i)^{c+i} \quad 2.10$$

$$p_d = \sum_{i=0}^{v-c} \binom{v}{c+i} (1 - P_d^i)^{v-c-i} (P_d^i)^{c+i} \quad 2.11$$

Obviously, this fusion rule includes the logical OR rule (C = 1), and the logical AND rule (C = v) as special cases. Also the majority rule is a special case of the voting rule for V = C/2.

2.8.2 Data Fusion

In this fusion method, the CUs send all local sensing samples or their test statistics to the BS, so advanced signal processing methods can be applied. The shared information can be combined using different techniques such as selection combining SC [44], maximum ratio combining MRC [44] and square law combining SLC [45]. The disadvantage of data fusion methods is that they incur a bandwidth overhead due to the control channel and they need more computational resources in both the CRs and the FS.

2.9 Why we Need to Measure and Evaluate the Trustworthiness of CU_s?

Trust and reliability management is having an increasing influence on CR networks; therefore, efforts have been made to establish trust management in CSS.

The performance of CSS is highly dependent on the process of data fusion and user's trustworthiness. That is, when the trust value of SUs is evaluated, a higher detection probability should be guaranteed in the process of sensing data [46].

The user's trustworthiness is important for the following reasons:

- It represents how reliable the information is from corresponding CUs, which is called the authenticity of the user information.

- The trustworthiness helps the assessment of how reliable the CUs are, and so it can be taken into account while deciding punitive or rewarding policies for CUs.
- In CR communication, the trust values of users are usually calculated based on the relevant sensing information in order to classify the SU behaviour.

3 Security Challenges in CR Networks

In CRN, the major function of the physical layer is in detecting the available spectrum correctly and quickly for data transmission. This is a prerequisite for robust spectrum sensing and must be performed without causing any interference. Therefore, the operational and security aspects of CR have gained a great deal of attention.

The reasons that cause the CR to be vulnerable to new kinds of security threats are:

- The open and dynamic features of CRNs make CR systems more vulnerable to various malicious attacks. These attacks can be jamming, PUEA and spectrum sensing data falsification (SSDF) [47] [48].
- Because CRNs share some features with conventional wireless networks, it is necessary to deal with the conventional wireless security risks in addition to the threats targeted at the CR features. Conventional risks include MAC spoofing and Denial of Service [49].

Based on these vulnerabilities, counter-measures are needed to make CRNs robust and secure against any kind of threat.

3.1 Security Awareness in CRNs

Each spectrum function in CR has its specific threats that can affect CR performance. Therefore, attacks can be classed according to the functional objective [50], for example:

1. For the spectrum sensing function, the attacker can change the parameters of the spectrum (e.g., transmit power, carrier frequency, and modulation strategy).
2. For the spectrum access decision function, the attacker aims to manipulate the parameters of the objective function.
3. Providing false information in the case of the learning function; this incorrect information, for example about the PU's current and past behaviours, causes incorrect decisions to be made.
4. Exploiting spectrum mobility. The hand-off process makes the user vacate the current spectrum band and move to a new available spectrum band; during this process, the security threats are severe [51].

3.2 Mitigating Threats in Cognitive Radio

For any CRN, there are important and general steps to protect the CUs from attacks, these steps can be summarised as follows:

- The local observation about the surrounding environment must be authenticated by the SU.
- The SU must be able to co-operate with the other cognitive nodes.
- Considering the trustworthiness of the SU to degrade the effects of malicious users.

In CRNs, the attacker aims to achieve one or more of the following objectives:

- **Private data access**: The attacker node attempts to access data with no authorisation; this problem can be solved by cryptographic methods.

- **Interference to the PU**: The attacker aims to use the communication channel that is used by the PU, so denial of service occurs.
- **Data modification**: The data exchanged between some users is changed; in this case, the data integrity is affected.
- **Missed detection**: the SUs are prevented from using the available channels.
- **Data falsification**: In the CSS, some malicious users send wrong data to the cooperating nodes, so the CUs will follow the guidance of the attacker; this case needs an information authentication process.

3.3 Literature Review on CR Security

In the literature, many developers have performed work on PU attack remedies. Chen [52] studied advanced PUEA and produced an outstanding approach to tackle this type of attack when both the malicious user and the defender are intelligent enough to obtain the surrounding information of the environment. The work is based on learning strategy and estimation procedures. Also the authors Li and Hi [53] conducted studies on the effect of the PUEA on multiple channels CR, and they presented a mitigation approach known as the passive anti-jamming technique. In this approach, the SU selects a channel randomly in order to transit at each time; such an approach can face the PUEA statically. This is named the dogfight approach because of the computation between the malicious user and the defender. Also, the authors developed their work using multiple defenders and undefined channel statistics [54].

Several methods have been developed in the literature based on co-operative spectrum sensing. In [55], a method called the clustering-soften hard combination is presented to perform a great trade off between the overhead saving and the performance increase.

The cluster CSS has some disadvantages that occur when the SUs that have good location correlation are grouped into the same cluster in order to decrease the consumption of the energy for transitioning data to the cluster head (CH).

Moreover, efforts have been made to establish trust management in CSS. In [56] the author presented a trustworthiness system, where the user's trusts were achieved according to the suspicion level.

In [57], the authors propose a novel trust-aware hybrid spectrum sensing scheme, in which the Beta Reputation System is applied to construct the trust management model, and can detect misbehaving SUs and filter out their reported spectrum sensing results from the decision making process. Zeng et al. proposed a reputation based CSS scheme in [47]. This scheme introduces a reputation-based mechanism to identify misbehaviours and mitigate their harmful effect on sensing performance. It is based on the fact that such a secure CSS is sensitive to the correctness of reputations, thus the reputation-based CSS with trusted nodes assistance starts with reliable CRs. The sensing information from other CRs is incorporated into co-operative sensing only when their reputation is verified, which increases the robustness of cooperative sensing.

3.4 Threat Categorisation According to the Layers of Cognitive Networks

The cognitive communication layout contains many layers, namely the physical layer, the link layer, the network layer and the transport layer. The function and objective of each layer explained in [58][59]. Figure 3.1 shows the cognitive communications

layout. The attacks on CR networks can be categorised according to the layers that they target.

The names of the attacks in CR are assigned according to the layer; for example, the attacks that occur in the physical layer are called physical layer attacks, and the attacks that rely on the link layer are known as link layer attacks. By this classification of attacks, detection and defence approaches are taken.

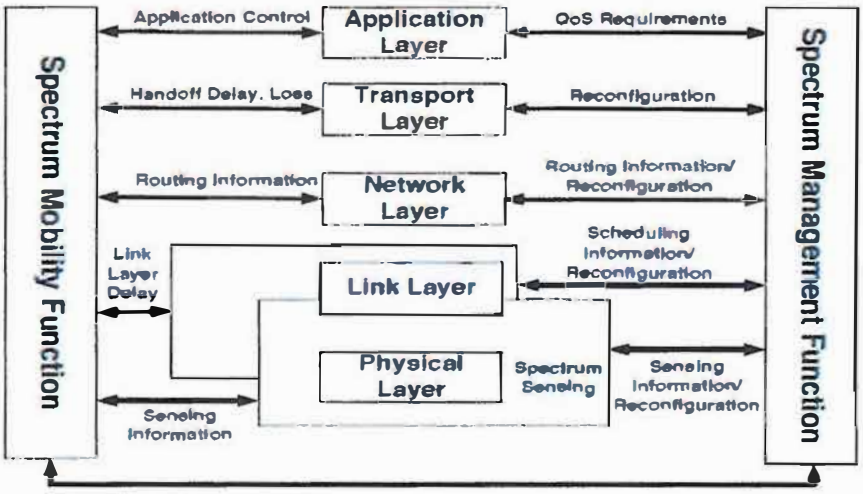

Figure 3.1 Cognitive communications layout [47]

3.4.1 Physical Layer Security

In the protocol stack, the physical layer is the interface to the medium of transmission. In CRNs, the physical layer is responsible for the following functions:

Spectrum sensing: to sense the available channel to be used for transmission and to avoid interference with the PU.

Channel estimation: in this stage, the channels are estimated via some parameters, for example, the bit rate and the transmission power.

Data transmission: the transmission of the data must be guaranteed without interference with the coexisting users.

The security of the higher layers can be achieved via authentication and encryption approaches while the physical layer can be secured by different approaches such as use of location information [60]. In the following section, some threats and attacks that are associated with the physical layer are discussed.

A. Primary User Emulation

To improve the performance of CR, all the users in the CR network must be evaluated to ensure that they are not adversary users aiming to use the resources of the specific channel and not to co-operate with other users in the cognitive network. Figure 3.2 shows the principle of the PUEA, where the PU emulator mimics the spectral characteristics of the PU.

PUEA motivation can be classified into two categories. Firstly, there is malicious PUEA, where the attacker aims to prevent the good SUs from using the available channel in the spectrum. Secondly, there is selfish PUEA, where the main objective of this attack is to increase the share of the spectrum resources. Many malicious users can co-operate to conduct this attack and use a link between them to communicate.

If the PUEA has some knowledge about the CRN, then a complicated attack can occur [61]. For example, the PUEA can use the quiet period in order to start an attack because at this time all the SUs stop transmitting in order to facilitate the spectrum sensing process, and during this time if any user receives signal strength beyond a specific threshold, this user is considered as a PU.

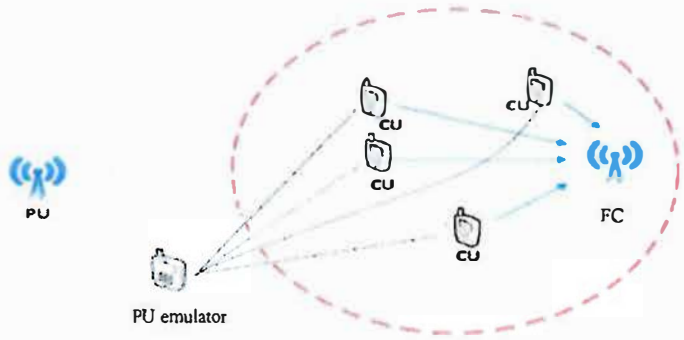

Figure 3.2 Concept of PUEA

- ***Mitigations Against a PUEA***

There are some approaches that have been presented to identify and defend against this kind of attack; the transmission source needs to be identified, i.e. whether the signal source is from a malicious user or a good PU. One of these approaches to identify the user is to use a cryptographic authentication strategy, such as digital signatures [62].

The location of the user can also be used to identify the signal source [63]. If the PU location is known and matches the location of the signal source, then the source of the signal is a good PU, but if the locations do not match, then it is considered a PUEA.

To identify the location of the signal source, certain techniques can be used. For example, the distance difference test (DDT) uses a signal phase difference, but this approach has a disadvantage in that it needs a synchronisation process in all the location verifiers (LVs) which are difficult to implement in terms of cost.

There is also another technique for localization that uses the time difference of arrival (TDOA) method and the frequency difference of arrival (FDOA). TDOA is implemented first to give some inputs to the FDOA, so the accurate location of the signal source is determined.

Also, the fingerprint procedure can be used to determine the transmitter source. RF fingerprinting (RFF) is a technology that allows the unique identification of transmitters. RFF is based on the transient phase of a transmitted signal and allows device identification at the physical level [64].

B. SSDF Attacks

In CSS, the performance of the network may be affected by a false observation from some malicious users. For example, as in Figure 3.3, all the users send their local observation about the spectrum to the FC in order to make a global decision about the presence of the PT. This kind of attack is also called the Byzantine attack [65].

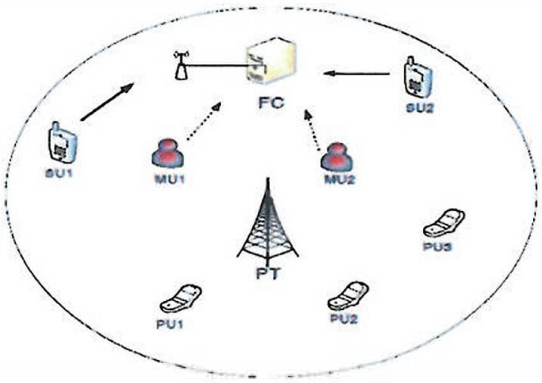

Figure 3.3 SSDF attack

The false observations can be sent to the FC by one malicious or a set of malicious users [66]. The malicious users that send false observations are classified as follows:

Malicious users: these users send false observations to confuse other users or the BS. Their objective is to cause the FC to make the wrong decision about the PU status. The legitimate SUs will either evacuate the specific band or they will cause interference for the PU.

Greedy users: as the name implies, they continuously confirm that a specific spectrum band is used by incumbent signals. The aim of these users is to occupy a specific band by forcing all other users to evacuate it.

Unintentionally misbehaving users: they send false observations of the spectrum status not because they are malicious users or greedy users, but because part of the software or hardware is malfunctioning. The cause for this attack can be a random fault [67].

- ***Defending Against SSDF***

There are some approaches that are used to tackle the SSDF problem; the work in [68] explains how the decision fusion method works to mitigate the SSDF issue. The main idea behind this method is that the local spectrum results are collected and summed, then compared with a threshold value to decide if the spectrum is occupied by a PU or not.

This approach depends on the threshold value to keep the interference as low as possible; the drawback of this procedure is that if the threshold value is increased, then the missed detection is increased.

Another data fusion approach presented in [66], known as the weighted sequential ratio test (WSRT), is used to protect the cognitive network from the SSDF. WSRT depends on two procedures; firstly, a reputation setup, where each user is assigned a reputation value and, secondly, there is a hypothesis test setup where a sequential probability ratio test is used.

C. *Jamming Attack*

There are two types of jamming in CR networks. There is single-channel jamming when a malicious user transmits high-power signals continuously on a specific channel, so the transmission via this channel is jammed. The second kind of jamming is applied to multiple channels simultaneously; the attacker transmits interfering signals using all of the channels. Jamming attacks aim to use a high percentage of bandwidth and create a denial of service (DoS) situation. A more risky situation when a jammer affects the dedicated channel that is being used to exchange sensing information between CRs [69]. Thus, jamming is an attack that is known in both physical and MAC layers.

- ***Defending Against Jamming***

DoS is most common at the physical layer and can also occur at the MAC layer. In the MAC layer, nodes can use medium access control protocols such as carrier sensing multiple access (CSMA) as a remedy against DoS.

While in the physical layer, legitimate users have the capability to distinguish between the level of noise by collecting data about the noise levels in the system, and then setting a model that depends on statistics that can be used for comparison if a DoS attack is carried out. Also, to defend against jamming, the relationship between two parameters is considered; these parameters are the signal strength (SS) and the packet delivery ratio (PDR) as explained in [70].

D. *Objective Function Attack*

CRs are adaptive to the environment; some radio parameters are available for manipulation in the effort to adapt the radio to the environment. Objective function

attacks can target any learning algorithms that utilise objective functions. Parameters that might be manipulated include bandwidth, power, modulation, coding rate, frequency, frame size, encryption type, and channel access protocol [58].

- ***Objective Function Attack Remedies***

One of the effective methods of mitigating objective function attacks uses predefined thresholds for each of the adjustable parameters. Communication would be prevented when one or more of the parameters did not fulfil its predefined threshold [62].

3.4.2 Threats Related to Other Different Layers

The open systems interconnection (OSI) model contains layers that can be attacked separately, but because the physical layer is the interface, it is more vulnerable than the others as the spectrum sensing process is achieved via this layer. This section explains the threats that can affect the other layers.

The common control channel (CCC) is one of the major attacks associated with the MAC layer. The CCC is vital in cognitive systems because it is responsible for exchanging control information. For example, the CCC is used to send and receive a great amount of control information, such as the co-operation sensing data and the spectrum hand-off information. Thus, the CCC is vulnerable to many attacks, for example:

- **MAC spoofing:** in this case, the attackers want to disrupt the CR network by using spurious messages. Multi-hop CR networks, which do not need a central unit for the authentication process between the users, are the most likely to be affected.

• **Congestion attack**: this attack occurs when the CCC receives a large amount of information from an attacker aiming to perform an extended DoS attack.

• **Jamming attacks:** the adversary user in this case causes DoS by increasing the interference level.

There is another concept related to layer attacks, which is known as a cross layer attack. This means that the attack can be started at multiple layers at the same time [29]. The co-ordination of this attack makes it very difficult to detect. This attack reduces the utilisation of the channel at both the physical layer and the MAC layer.

A summary of some attacks that can occur at each layer, and their remedies, is presented in Table 3.1.

Table 3.1 Summary of some attacks in different layers [72]

Attack type	Network Layer	Reason	Countermeasures
PU and SU jamming	physical	unknown location and unclear SU access	locations verification signal strength and noise contrast
SSDF (Byzantine attack)	physical	due to the openness of low-layer protocol stacks	robust co-operative spectrum sensing schemes users trust determination remove unreliable users from the co-operation
primary signal sensing	physical	low level of primary signal	co-operative spectrum sensing
overlapping SUs	physical	location unknown	game models nash equilibrium techniques
gain of SUs unauthorized	MAC	false data in order to gain signal	trust management for the SUs
increase interference by malicious node	network	compromising with malicious node	control for the local sensing

4 Mitigating Attacks in CR based on an Analytical Model

4.1 Introduction

The CR's ability to distinguish between PU signals and SU signals is important, but it becomes difficult when the CRs are operating in hostile environments. In a hostile environment, the attacker user may be able to modify the air interface of a CR to mimic a PU signal's characteristics, thereby causing legitimate SUs to erroneously identify the attacker as a PU.

When energy detection, for example, is used as a spectrum sensing method, it is noted that this technique has some disadvantages, for example, poor performance under low SNR values , and failure to separate between interference from PUs and noise that may restrain the performance of this methodology [3] [73].

The other conventional techniques for spectrum sensing, such as matched filter and cyclostationary feature detection, are able to recognise the intrinsic characteristics of PU signals, thus enabling them to distinguish these signals from those of SUs. However, such detection techniques are still not robust enough to counter PUEAs.

Because of the above limitations in conventional spectrum sensing approaches, this chapter focuses on one of the major threats in the CRN which is the PUEA. Using an analytical approach, the security against PUEAs in CR networks is proposed and the impact of this attack on the performance of the cognitive network is investigated. The NPCHT test is used to detect the PUEA.

4.2 Adversarial Attackers Classification

The classification of attacks depends on the objectives of the attacker in CR networks, and can be given as follows:

- Selfish attacks: this is where the attacker aims to acquire a channel for its use only and prevent the other good SUs from acquiring this channel [73].
- Malicious attacks: in many cases, the attacker does not aim to increase its own benefits but to prevent other users from using a spectrum [74].

4.3 Conventional Networks Vs CR Networks

Because the CR automatically senses and detects the available spectrum and is able to change the communication parameters in order to allow more communications to start concurrently, this makes the security in CR more challengeable and it requires more effort to tackle any attack [75][76].

Because the vulnerability in CR comes from its unique feature, i.e. dynamic spectrum access, the conventional security procedures cannot be implemented in a CR system.

Problems of Inherent Reliability

In CR, some issues of inherent reliability can exist; this section focuses on the inherent issues, and these are:

- **PU Unrecognized Location**

  In CRNs all the positions of the primary receivers must be identified by all the SUs. The goal of making the locations known is to reduce the interference to the primary node. Also, unknown locations cause the hidden users problem.

- **PU Signal Strength**

  Localization techniques that depend on received signal strength (RSS) provide low-cost implementation and low complexity. However, the RSS-based localization approaches could have a high localization error because they use an inexact path loss exponent (PLE). Thus, using RSS-based localization approaches for the PU localization might cause a high interference to the PU [76].

4.4 Primary Exclusive Area

In CR, where PUs and SUs are presented in the network, it is required that the SU must not be presented at a certain distance from the PU so that the interference to the PU is minimised. This area is called the primary exclusive area where the CUs are not permitted to transmit [77].

4.5 Examination of PDF of Received Signals

The PDF of the received powers from different users can be used in many approaches for the security of wireless systems, for example:

1. The PDF is used to obtain the trust in the networks as in the Bayer risk [78].

2. In mobile networks, the PDF is used to recognise the good nodes using the signature approach that utilises the likelihood ratio test.

3. It is widely used to determine the level of the interference in wireless networks [79].

4. In the cellular system, the PDF is used to estimate the received powers in the hand-off process and power control and also in many algorithms in order to improve the system's capacity [80].

5. Finding the error probability and correct sense probability in a network.

There are two widely used mechanisms to test the PDF of received signals. The two tests are as follows:

- **Wald's Sequential Probability Ratio Test (WSPRT):**

  WSPRT is a multi-stage iterative process where a set of observations is necessary to make a decision [32]. Because it needs many observations, it takes a long time for the decision processing. The test computes a ratio of the two probability distribution functions at each iterative step. The product of the ratios for n iterations gives the WSPRT decision variable denoted by W_n as:

$$W_n = \prod_{i=1}^{n} \frac{P^m(X_i)}{P^{P_r}(X_i)} \tag{4.1}$$

  where $P^m(X_i)$ is the PDF of the total received power from all the malicious nodes at the i^{th} iteration, $P^{P_r}(X_i)$ is the PDF of the received power at a secondary due to the primary transmission, and x_i is the measured power at the i^{th} iteration. The decision variable W_n is compared with two predefined thresholds in comparison to the Neyman Pearson test that uses only one predefined threshold. The two thresholds are functions of tolerable levels of false alarm and missed detection probabilities. If T1 and T2 are the two thresholds, a legitimate primary transmission is assumed when W_n is less than T1, and if W_n is greater than T2, then a PUEA is detected. For any other case, it is necessary to take more observations [32].

- **Neyman Pearson Composite Hypothesis Test (NPCHT):**

The PDFs of the received power at the secondary nodes due to the primary transmitter and due to the malicious users are used in the NPCHT. The NPCHT mitigates the PUEA by comparing the ratio of the two PDFs with a predefined threshold. Based on whether the ratio is above or below the threshold, primary transmission and emulation attacks can be distinguished.

4.6 CR Performance Metrics

In order to identify the unoccupied licensed spectrum, spectrum sensing needs to detect the frequency locations of the primary signals; a hypothesis test can be used to distinguish between some possible states. For example, the M-array hypothesis tests where there is an observation (possibly a vector or function) upon which there is a need to decide among M possible statistical situations describing the observations [79]. According to this criterion, a binary hypothesis testing is achieved by the spectrum sensing in order to decide whether or not there are primary signals in a particular channel. The two basic hypotheses are:

H_0: no primary signals, H_1: primary signals exist

H_0 is known as the null hypothesis because the received signals are only the noise in the RF environment and there is no primary signal presented. H_1 is the alternative hypothesis when the received signals are the noise and the primary signal. The two hypotheses can be expressed as:

H_0: $y[t] = n[t]$

H_1: $y[t] = s[t] + n[t]$

y[t] is the received signal, n[t] is the noise in the RF environment, and s[t] is the primary signal. Different decision rules and spectral detectors are used for spectrum sensing, but each detector is vulnerable to sensing errors due to additive noise, limited observations, and the inherent randomness of the observed data [80].

If actually there is no primary signal in the channel, but the detector detects an occupied channel, this is called a false alarm. Also, if actually there is a primary signal in the channel but the detector detects an empty channel then this error is known as the missed detection [79][5]. These two parameters (probability of false alarm and the probability of missed detection) are mostly used to measure the performance of a signal detector.

4.6.1 Signal Sources Determination

There are some possible states that can exist in a CR environment; for example, according to the work in [81] that denotes the transmitted signal by x(t). It assumes that if it is the authentic PU signal then x(t)=s(t) and if it is the PUE signal then x(t)=s′(t). Based on the energy of the signal and because the PUE signal is very similar to the PU signal, the author assumes both s(t) and s′(t) are independently and identically distributed (IID) random processes with mean zero and variance σ^2_s. Also, because the SUs have a significantly lower transmitted power than the PUs, it assumes x(t) = 0 when the SU is transmitting. So some possible states according to [81] can be expressed as:

$$y(t)=\begin{cases} n(t) & SU \\ h*S(t)+n(t) & PU \\ h*S'(t)+n(t) & PUEA \end{cases}$$

where y(t) is the received signal at the PUE detector, n(t) is the additive white Gaussian noise (AWGN) with mean zero and variance σ^2_n, and h is a constant gain. So the PUE detector can distinguish between the SU, PU and PUEA signals.

Other researchers consider that more signals can exist; for example, the work in [82] assumes that there are some possible states which can be expressed as:

S_0: Only Noise

S_1: PU + Noise

S_2: PUEA + Noise

S_3: PU + PUEA + Noise

S_0 occurs when the CR users receive only noise. Moreover, the channel is neither occupied by PU nor by PUEA. If the PU transmits over the channel while the PUEA is absent, then S_1 exists.

When the PUEA uses the channel and the PU is absent, then CR users receive only the PUEA signal plus noise as expressed in S_2. S_3 states the presence of PU, PUEA and noise signals.

Another work presented in [83] uses a two-phase algorithm to identify the hypothesis testing between PUs and non-PUs. Detection in this algorithm can be finished if the detection results of the first phase reveal that a PU is present, otherwise, it executes a second phase detection (energy detection) to further distinguish the PUEAs from the noise.

In this chapter, NPCHT is considered to investigate the impact of PUEAs. This test is able to distinguish between two hypotheses:

H_1: the signal is from a PU

H_2: the signal is PUEA

4.7 System Model

Mitigations of the PUEA can be categorised into two approaches. Firstly, there is the location aware approach that requires a significant infrastructure, such as a dedicated sensors network, in order to determine the locations of the transmitters. Secondly, there is the location unaware approach, which basically depends on signal analysis.

In this chapter, a technique that depends on PDF is used to detect the PUEA. The proposed technique depends on the analysis of received signals. The main objectives of the simulated model are:

A. Estimating the PDFs of received signals when the distance between the PU and all other users is relatively large.

B. Obtaining the probability of a successful PUEA for various thresholds which are used in the decision rule of the NPCHT.

4.7.1 Simulation Setup

The simulated model is shown in Figure 4.1 where the SU aims to identify the signal source, whether it is from a primary transmitter (PT) or malicious users.

Considering the scenario, the SU and malicious users are located in a circular area with radius R.

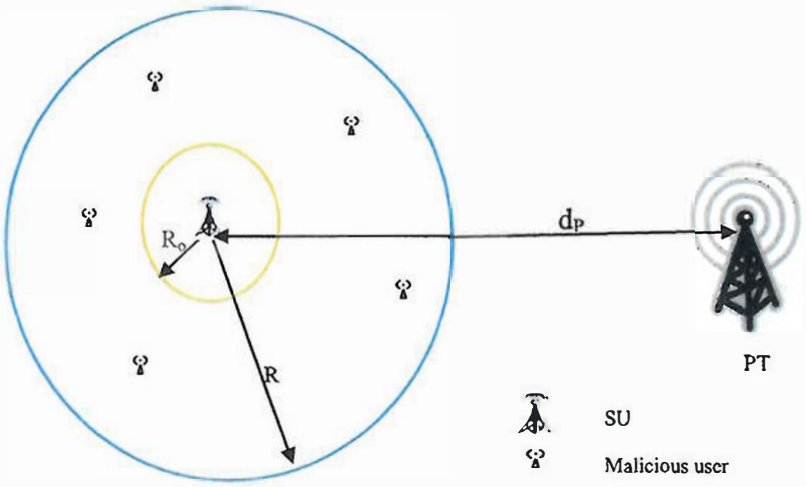

Figure 4.1 CR System Model

The SU measures the received powers from the surrounding users to determine the PDFs. The criterion for making a decision about PU presence is based on the NPCHT.

4.7.2 Simulation Model Assumptions

The following assumptions are considered in the simulated CR model:

- The PT is at a distance d_p from the SU, R is the network radius, R_o is the exclusive distance from the SU where no malicious users have presented within the circle of radius R_o [77] [84].
- In order to investigate the effect of the malicious users in the system, the coordinates of these malicious users are randomly chosen and distributed around the good user in the area between R and R_0. In this model, the primary transmitter is located at a distance of d_p = 120 km to the SU, R = 500 m and R_0 = 40 m, the primary transmitting power P_t = 120 kw, while the malicious nodes power P_m = 5 w (such approximations for analysis in CR networks were also made in [85] [86]).

The simulation model in Figure 4.2 shows how the malicious nodes are located randomly around the good SU (when the total of malicious nodes M=30).

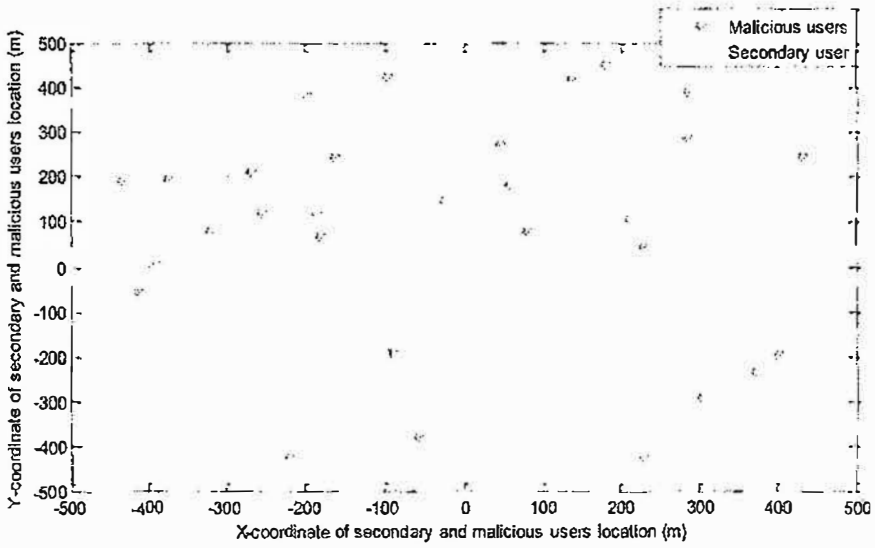

Figure 4.2 Simulation model of malicious users distributed randomly around the SU located at coordinate (0, 0)

- The coordinates of the PT are set at (r_p, θ_p) and this is known by all other users.
- The SU co-ordinates (r, θ), the co-ordinates of the users are transformed such that the SU lies at the origin (i.e. at (0, 0)). Therefore, the malicious users are uniformly distributed in the annular region (R_0, R) and the primary is at (d_p, θ_p).
- A path loss is assumed in the primary transmission, in addition to shadowing (zero mean, and variance σ_p^2). Path loss also occurs in the malicious transmission in addition to shadowing (zero mean, and variance σ_{mi}^2) with σ_p = 8 and σ_m = 5.5. These values are assumed because the primary and malicious transmissions are as those occurring in urban and suburban environments [27].

4.7.3 Model Analysis and PDFs of the Received Signals:

The density functions for the PU transmission and also for the transmission from malicious users are used with the NPCHT to determine the hypothesis test of the spectrum statues.

PDF of the Received Signals

Because the density function of the received power is an important factor in the NPCHT, this section explains mathematically how it is used to measure the performance metrics of the network and also to investigate how the PUEA affects the network.

In order to calculate the PDFs of the received signals, the received power is determined from the primary transmitter which is located at distance d_p and transmits at power P_t. Generally, the relationship between the received power P_r and the distance d is:

$$P_r \propto d^{\gamma} \qquad 4.2$$

where γ is the path loss. γ is set equal to 2 for the PT and 4 for the malicious nodes because a free space propagation model is used for the signal from the PT and a two-ray ground model is used for the signal from the malicious users, as explained in section 2.6.1.

In the free space model, the received power from the PU (denoted by $P_r^{(p)}$) at the SU can be expressed as:

$$P_r^{(p)} = P_t d_p^{-2} k \qquad 4.3$$

where k is the path loss factor given by $K = 10^{\varepsilon p/10}$, and ε_p is the random shadowing effect as assumed in section 4.7.2 $\varepsilon_p \cong N(0, \sigma_p^2)$.

After estimating the received power $P_r^{(p)}$ from the PU, the PDF of the received power from the PU, which is denoted by $P^{\Pr(x)}$, can be mathematically calculated. $P^{\Pr(x)}$ follows the PDF formula of a log-normal distribution, therefore, $P^{\Pr(x)}$ can be expressed as:

$$P^{\Pr(x)} = \frac{1}{A\sigma_p \sqrt{2\pi x}} \exp\left(-\frac{(10\log_{10} x - \mu_p)^2}{2\sigma_p^2} \right) \qquad 4.4$$

where μ_p, σ_p are the mean and variance of the distribution $\mu_p = 10\log_{10} P_t - 20\log_{10} d_p$

Next, the received power $P^{(mi)}$ from each malicious user *i* (*i*=1 to M) at the SU is calculated according to equation 4.5, which represents a two-ray ground model for the signal from the malicious users.

$$P^{(mi)} = (P_T)_{mi} \; d_i^{-4} K \qquad 4.5$$

The overall received power from the whole set of malicious users is the sum of $P^{(mi)}$ when *i*=1 to M , d_i is the distance between the malicious node *i* and the SU, K is the shadowing between the malicious node *i* and the SU, $(P_T)_{mi}$ is the power transmitted from the malicious node *i*.

4.8 Neyman-Pearson Performance Metrics

The performance of the NPCHT can be characterised by two parameters, i.e. the probability of a false alarm and the probability of a missed detection.

Probability of a False Alarm PF:

The SU concludes that the transmission is due to a PU, but actually the malicious user is transmitting. This is also known as the probability of a successful PUEA.

Probability of a Missed Detection PM:

The SU concludes that the transmission is due to a PUEA, but actually the PU is transmitting.

Using the PDF of the received power, a decision variable (Λ) can be calculated in NPCHT as:

$$\Lambda = P^{m}(\chi) / P^{\Pr}(\chi) \qquad 4.6$$

where x is the measured power of the received signal, and $P^{\Pr}(\chi)$ and $P^{m}(\chi)$ are the PDFs of the received power from the primary and from the malicious users, respectively.

NPCHT Threshold

The NPCHT criterion compares the decision variable Λ with a predefined threshold λ. Based on this threshold, the SU decides one of the following possibilities according to the NPCHT:

$$\text{Decision} = \begin{cases} \Lambda \leq \lambda & H_1 \\ \Lambda > \lambda & H_2 \end{cases}$$

where H_1 indicates a good primary transmission and H_2 is a PUEA.

Decision Rule of NPCHT: Figure 4.3 shows the decision rule of NPCHT. It shows the two conditional densities of the received power by the good SU from the primary and malicious users. The PM and PF are:

$$PM = \int_{\Lambda>\lambda} p^{Pr}(x)dx$$

$$PF = \int_{\Lambda<\lambda} p^{m}(x)dx$$

The performance metrics which are of interest in this thesis are the PF and the PM since they are mostly used to estimate the CR network's performance.

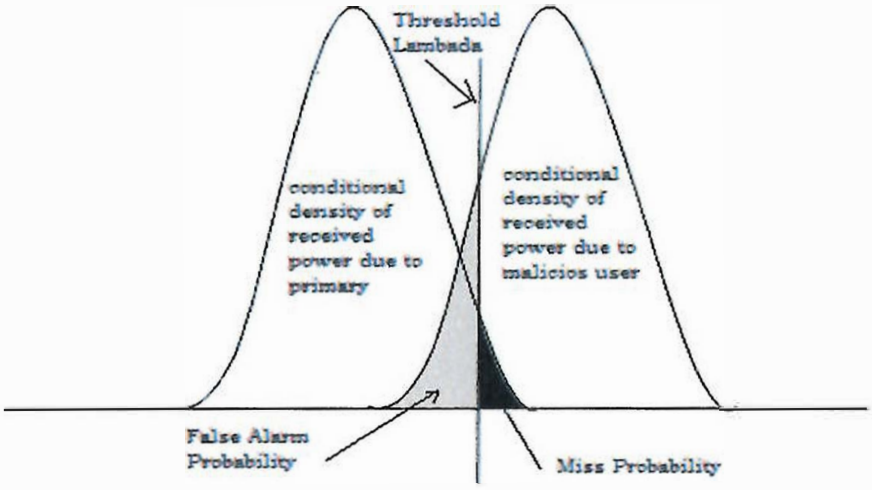

Figure 4.3 NPCHT decision rule

It can be seen from the decision rule that the missed detection probability and the false alarm probability can be changed (decreased or increased) by adjusting the detection threshold (λ).

4.9 Simulation Results and Analysis

In this section, the performance of the network in terms of the probability of a missed detection and a false alarm is investigated, also the relationship between the false alarm probability and the network radius R is studied. (The Matlab simulation code is attached to Appendix A).

Figure 4.4 and Figure 4.5 show the PDFs of the received power due to the primary transmitter and due to malicious users, respectively.

In these Figures, it is noted that the results of the PDFs gained using the simulations are considerably well matched with the ones derived mathematically.

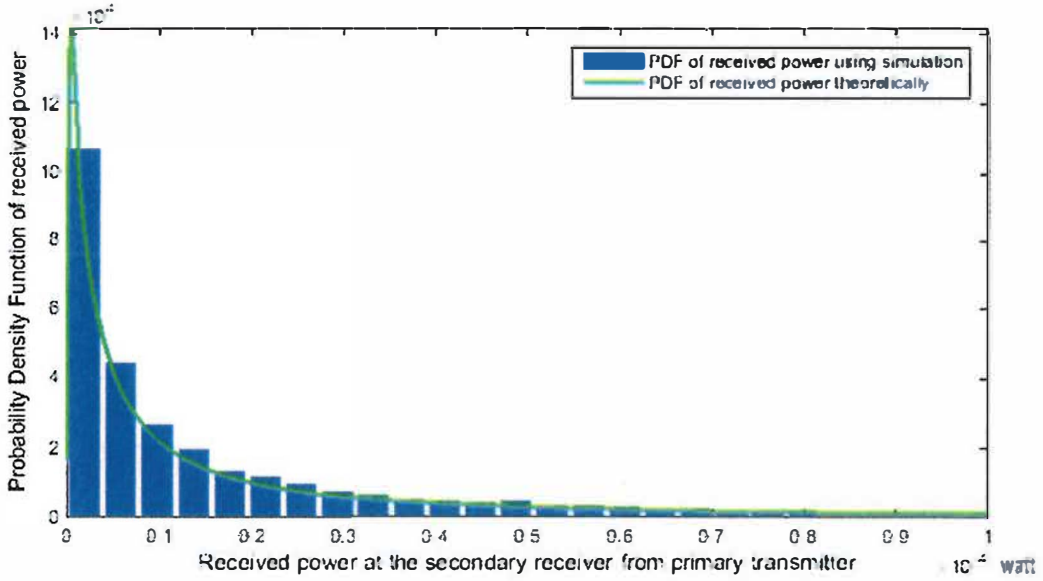

Figure 4.4 PDF of the received power due to the primary transmitter

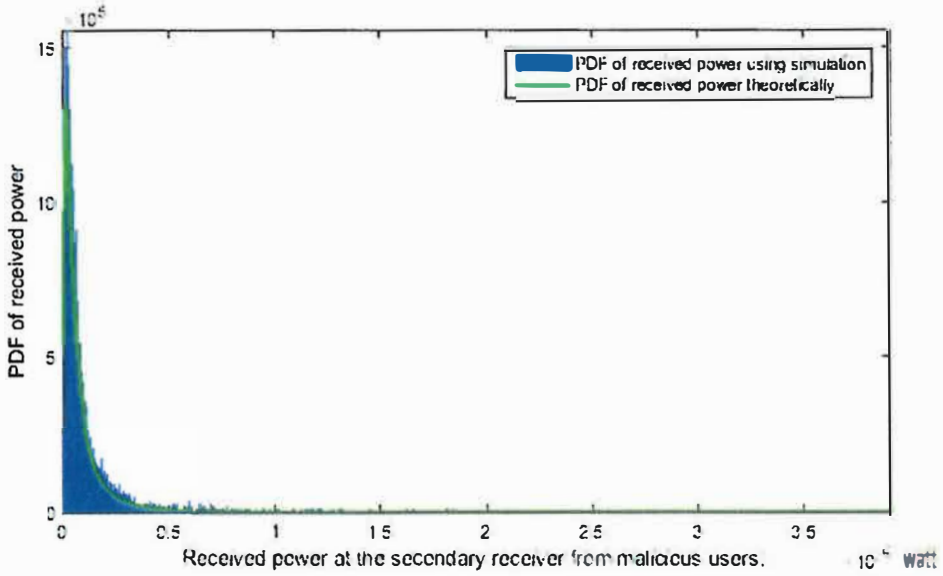

Figure 4.5 PDF of the received power due to the malicious users

Based on the PDFs of received signals and the NPCHT approach, the performance metrics (false alarm and missed detection probabilities) are obtained.

To verify the variety of the results over multiple simulation runs, both the probability of missed detection and false alarms are calculated for 40 simulations. The threshold value of NPCHT is set to 1.5, i.e. λ=1.5; the choice of λ and the optimal values of λ are studied in [87] that shows how to maximise the probability of detection and satisfy the false alarm probability. The number of malicious users is set to 5 (M=5), the rest of simulation parameters are as mentioned in section 4.7.2.

Figure 4.6 illustrates how the probability of a false alarm (successful PUEA) is converged for all simulation runs; it is averaged at 0.026 (within ±0.04) and this is because of the low number of malicious nodes M=5. On the other hand, Figure 4.7 depicts the missed detection probability, which is shown to be a bit higher and is averaged at 0.037; it is clear that the missed detection probability is quite similar for all of the simulation runs.

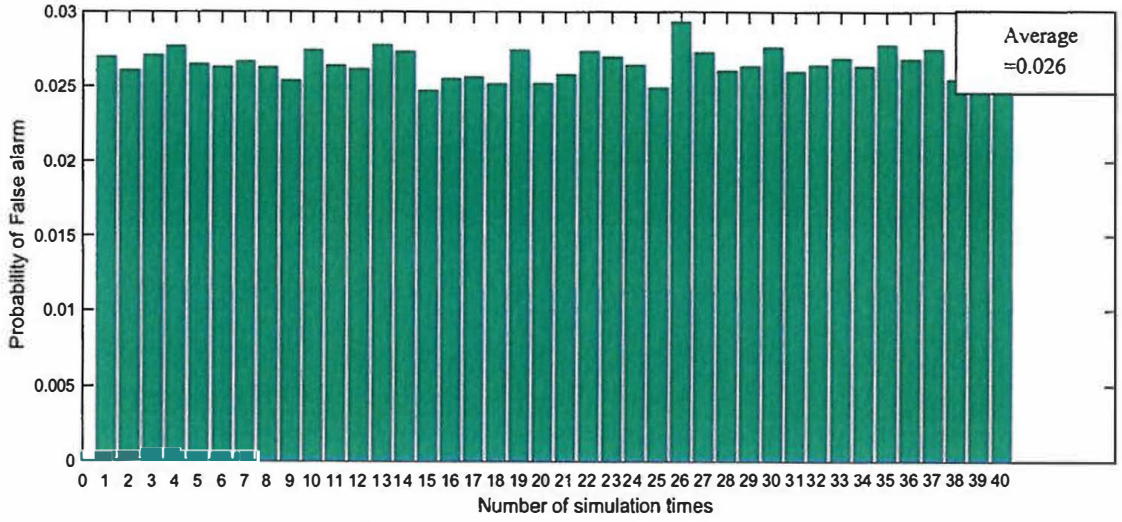

Figure 4.6 Probability of a successful PUEA (false alarm)

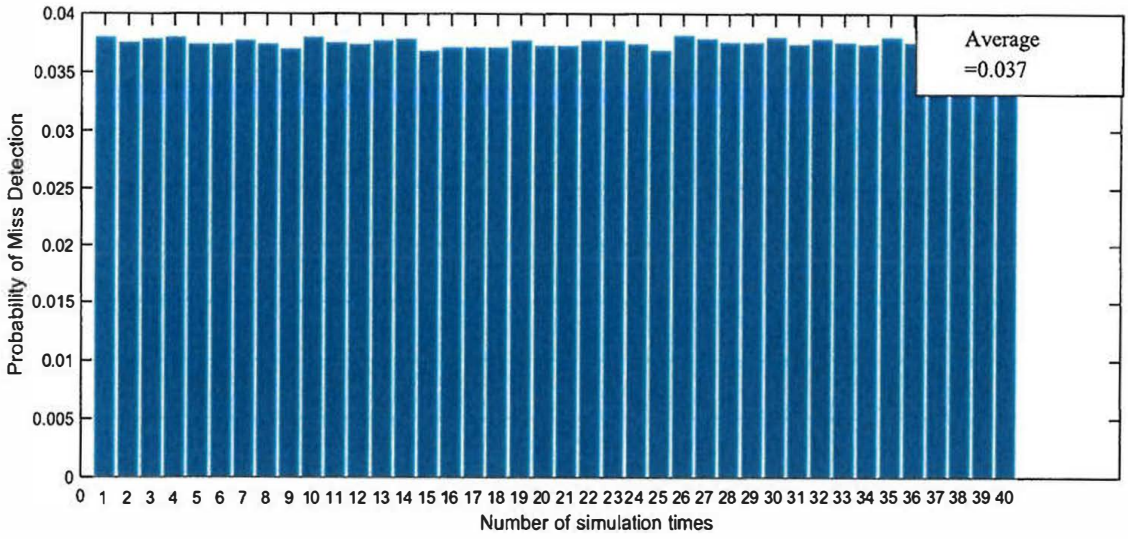

Figure 4.7 Probability of missed detection

To analyse the influence of the area R on the probability of a false alarm, Figure 4.8 shows the relationship between the false alarm probability and the network radius R.

The result in Figure 4.8 is obtained when λ=2 in order to maintain the false alarm probabilities below a certain level (the objective is to keep the false alarm probabilities lower than 0.5 and simultaneously minimizing the missed detection probabilities for all

values of R). A higher value of λ leads to a higher false alarm probability and lower missed detection probability because there is a positive correlation between λ and the false alarm as explained in Table 4.1. It is noted that in this network model when R is 200 m then the false alarm probability is at a maximum, i.e. the peak location is 200 m. The reason for this peak location is that the probability of a false alarm depends on the power received by the SU, and thus the false alarm probability rises to reach the peak location and then falls down with increasing value of R for the following reasons:

Case 1- When R is small, the malicious users are closer to the SU and the total received power from all the malicious users is likely to be larger than that received from the primary transmitter, thus decreasing the probability of a successful PUEA.

Case 2- For a larger R, the cumulative received power at the secondary from the malicious users may not be sufficient to successfully launch a PUEA.

Therefore, the network area R has a great impact on the network performance in terms of the false alarm probability, and also for any CR network there is a value of R that has a maximum false alarm probability.

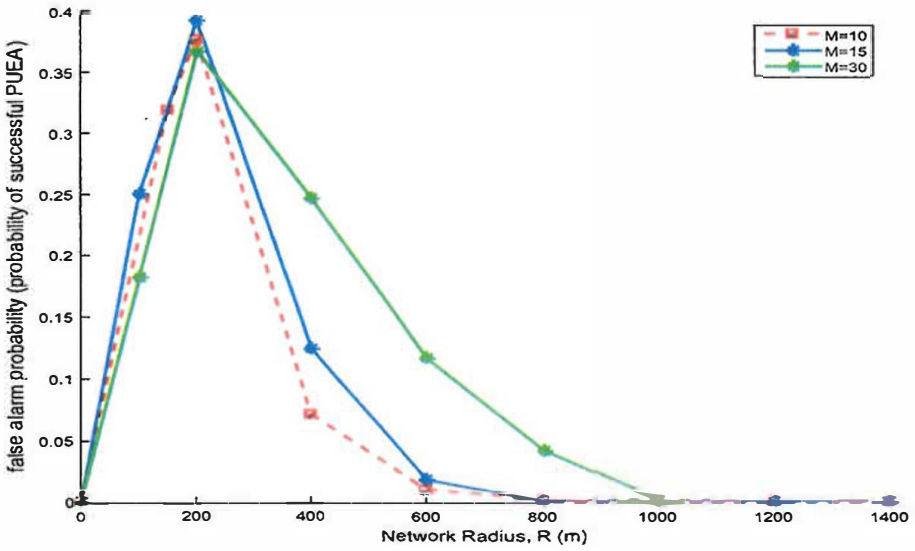

Figure 4.8 False alarm probability Vs network radius R

Also, Figure 4.8 shows the impact of the number of malicious users on the false alarm probability. The results show that a high number of malicious users in the system has a negative impact on the network causing the SUs to suffer from degradation in the quality of their communication due to the transmission from the malicious users.

Because the analytical model performance depends on the threshold value λ, which is used for comparison with the ratio Λ, the performance metrics evaluated under different values of λ as can be seen in Table 4.1. It is clear that there is an inverse correlation between λ and a missed detection, whilst there is a positive correlation between λ and the false alarm, i.e. as λ decreases, the probability of a false alarm decreases and a missed detection increases.

Table 4.1 False alarm and missed detection for different values of λ when M=35

Parameter	False alarm probability average	Missed detection probability average
λ =2	0.326	0.187
λ =1	0.043	0.4182
λ =0.5	0.041	0.43

Finally, the cumulative distribution function (CDF) is used to display both the false alarms and the missed detection probabilities on the same graph as shown in Figure 4.9.

It is clear that the CDF plot is a non-decreasing function and this indicates that the parameters and assumptions that were considered in the simulation are well-chosen.

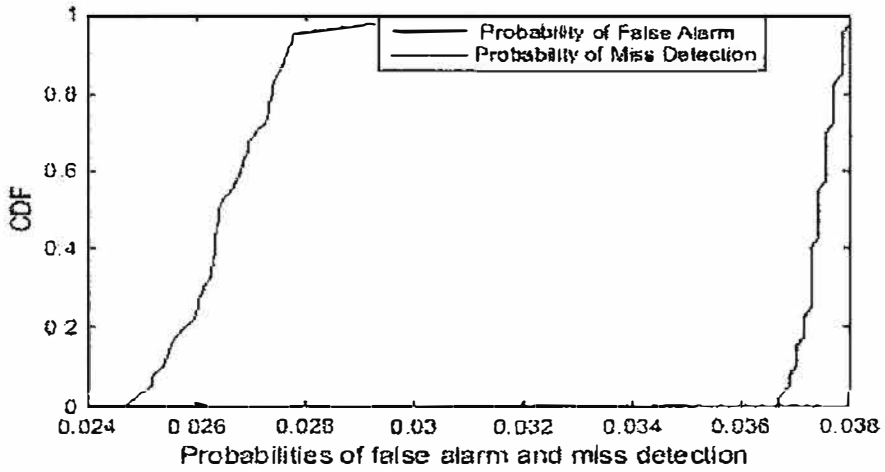

Figure 4.9 CDF of false alarm and missed detection probabilities when M=5, R=500m and R_0=40m

The X-axis shows the false alarms and the missed detection probabilities obtained from Figures 4.6 and 4.7 respectively.

4.10 Chapter Summary

In this chapter, the analytical model has been presented to obtain the PDF_s of the received powers at the SUs from the malicious nodes and also from the primary transmitter in the CRN.

Next, the PDFs obtained were used in the NPCHT to measure the performance metrics (the probability of false alarm and missed detection in the network). The results proved that the number of malicious nodes in the system has a great impact on the network and this has led to a reduction in the QoS due to the transmission from a high number of malicious users. These metrics are greatly influenced by the network area, where the SU is presented and surrounded by malicious nodes that aim to emulate the PU.

In this chapter, the investigation of the PUEA's impact on the CR is conducted using only the analytical approach. In the next chapter, the location and history of the signal source are used for the detection of a PUEA.

5 Trust Management Mechanism for the Detection of a PUEA based on the Localization and History of the Signal Source

5.1 Introduction

The new approach of spectrum management, which considers opportunistic spectrum usage, has forced CR developers to focus on some security features to improve the CRN's performance and protect the network from any adversary users (attackers) that aim to disturb the communication.

The trustworthiness of CR systems is important in order to improve spectrum utilisation and to ensure the smooth operation of the CR system. Trust in CR forms the foundation of the security platform of CRNs. However, trust for CRNs is quite different from that of other wireless scenarios and of other areas of computing trust. Trust is critical in CRN operation since it is considered as the main security solution [9].

The CR user's trust value represents its behaviour in the CR system. Therefore, obtaining a high trust value depends on some factors, such as vacating the PU's spectrum band on its arrival, normal joining to the CRN or leaving the CRN, and having enough residual power and bandwidth [88].

This chapter focuses on ensuring trustworthiness among nodes in CRNs. Trust determination mechanisms for the detection of a PUEA are proposed. These mechanisms use a localization technique and users' history to identify malicious users

in the system and to create a trustworthy network in order to build a strong relationship amongst nodes in CRNs.

5.2 Security and Users' Trustworthiness

In order to increase the CRN's QoS, the CR users change their parameters in order to be adapted to the environment. Therefore, the conventional security rules are not enough in the DSA. For instance, the conventional scheme for the security in ad-hoc networks, which is known as the public key infrastructure (PKI) mechanism and uses a routine procedure, cannot guarantee certain security requirements in the CR, e.g. location privacy. In order for the SU to ensure that it is communicating with a good PU, it is important that the user's trust value is evaluated to prevent malicious users and to improve spectrum utilisation [89]. Generally, in the CR system, which depends on users' trustworthiness, there is a trust value for each node, which can be established individually or by set of users in the system. The system can use this trust value to identify the signal source, i.e. whether it is from a trustworthy or untrustworthy user.

5.3 Detection of a PUEA based on Localization Schemes

To mitigate against a PUEA, different security techniques can generally be implemented in the spectrum sensing process. This section explains some techniques that depend on the user's location verification process.

5.3.1. Transmitter Signal Location Verification

Location verifiers (LVs) are needed to perform the verification procedure. LVs can be either dedicated devices or special second nodes.

Distance Ratio Test:

The distance ratio test (DRT) procedure depends on the relation between the signal strength and the distance between the transmitter and receiver [90]. At least two or more location verifiers can be used to verify the location of the transmitters.

If the ratios with respect to the transmitter and signal strength are matched, then this means that the user is a legitimate user, otherwise it is an adversary user.

Distance Difference Test:

The distance difference test (DDT) is considered to be more valuable than the DRT in terms of its performance. This technique depends on the differences of the relative phase of the received signal at two location verifiers. The first step in this approach is to calculate the differences of the time between two received signals at the location verifiers, after that the time differences are converted into distance differences. The distances are compared, and if they are close then the signal source is a legitimate user. This approach has some obstacles; the synchronisation process between the LVs needs to be accurate, and also the distances between the LVs must not be too large so that the DDT process is possible [90].

5.4 Proposed Approach for Users Trust Management based on Current and Historical Trusts.

The trustworthiness of users can be exploited to increase the performance of a CRN. Therefore, trust determination models are proposed based on the current and historical trust values of users to identify the PU.

5.4.1 Trust Determination Models

Trust values are classified into two categories, direct trust values and indirect trust values. Indirect trust values are a combination of historical and direct trust values.

A. Direct Trust Model

This trust is calculated according to current observation only. Malicious users and misbehaving nodes can act as good PUs aiming to disturb the SU's decision about the spectrum occupancy reports and this causes maximum interference and minimum spectrum utilisation. So it is therefore crucial to estimate the trustworthiness of users in order to identify the malicious users.

The direct trust values are achieved based on the transmitter verification scheme. The main idea of this scheme is that because it is not possible for the malicious user to mimic both the coordinates and the power level of the PU, so verifying the transmitter and producing its trust values are based on the distance measured on the basis of coordinates denoted by d_1 and distance measured based on received power level d_2. The methods for obtaining the values of d_1 and d_2 are explained in sections 5.4.1.1 and 5.4.1.2 respectively.

The CR user then uses d_1 and d_2 to calculate the direct trustworthiness T_D of a user as follows:

$$T_D = \min\left(\frac{d_1}{d_2}, \frac{d_2}{d_1}\right) \qquad 5.1$$

where the min function returns the minimum value of the equation's elements.

The distance that is calculated based on the received power d_2 is not accurate; however, the two distances d_1 and d_2 are close in the case of a good PU. Therefore, the T_D of the good PU is always close to 1.

5.4.1.1 *Distance Calculated based on the Location Coordinates d_1*

Let (x, y) be the coordinates of the SU and (x_1, y_1) the coordinates of the PU. The distance between the SU and the PU based on the coordinates can be calculated as follows:

$$d_1 = \sqrt{\{(x - x_1)^2 + (y - y_1)^2\}} \quad 5.2$$

In the simulation assumptions, each user broadcasts its location coordinates, so the distance between the users is calculated.

5.4.1.2 *Distance Measured according to the Received Power Level d_2*

As explained in section 2.6.1, the received power P_r with a given transmitted power P_t in the two-ray model is generally given by:

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \quad 5.3$$

where h_t is the height of the transmitter, h_r is the height of the receiver, G_t is the transmitter's antenna gain, G_r is the receiver's antenna gain, L is the system loss factor, and d is the distance between the transmitter and receiver.

Consider that h_t, h_r, G_t, G_r and L are equal to 1, then the received power is:

$$P_r = \frac{P_t}{d^4} \quad 5.4$$

Therefore, the distance d_2 can be calculated by:

$$d_2 = \sqrt[4]{\frac{P_t}{P_r}} \quad 5.5$$

The distance calculated using the received power may not be 100% accurate due to the noise level and the impact of the channel impediments and some other uncertainties caused by the signal propagation environment.

The ideal received power P_r is given by:

$$P_r\,(ideal) = \frac{P_t}{d_2^4} \tag{5.6}$$

The actual received signal power can be calculated as follows:

$$P_r\,(Actual) = \frac{P_t + \text{noise\_power}}{d_2^4} \tag{5.7}$$

where P_t is the transmitted power, d_2 is the distance between the transmitter and the receiver, and noise_power is the noise signal power.

B. Indirect Trust Model

In order to highlight the historical behaviour of a user in the role of trustworthiness evaluation, this model considers a historical trust value denoted by T_H that describes the behaviour of a user in the history of interaction.

This indirect trust value is a combination of direct trust T_D and historical trust T_H. This mechanism adds the function of querying the historical trust values. Therefore, the total value of indirect trust T_T is:

$$T_T = \bar{x}\,T_D + \bar{y}\,T_H \tag{5.8}$$

where $\bar{x}, \bar{y} >= 0$ and $\bar{x} + \bar{y} = 1$. $\bar{x}$ is the impact weight of direct trust T_D, and $\bar{y}$ is the impact weight of historical trust T_H.

$\bar{x}$, $\bar{y} \in [0,1]$. $\bar{x}$ = close to 1 indicates that the direct trust T_D plays a major role in the total trust calculation, and $\bar{x}$ = close to 0 means that the historical trust T_H plays a major role in the total trust calculation. The proposed approach gives higher weight to the direct trust, rather than the historical trust.

In the simulation of the proposed approach, $\bar{x}$ is set close to 1 to award the T_D a higher contribution to the T_T. So T_H value has less contribution to the T_T.

The flowchart in Figure 5.1 summarises the major steps of the trust-management mechanism.

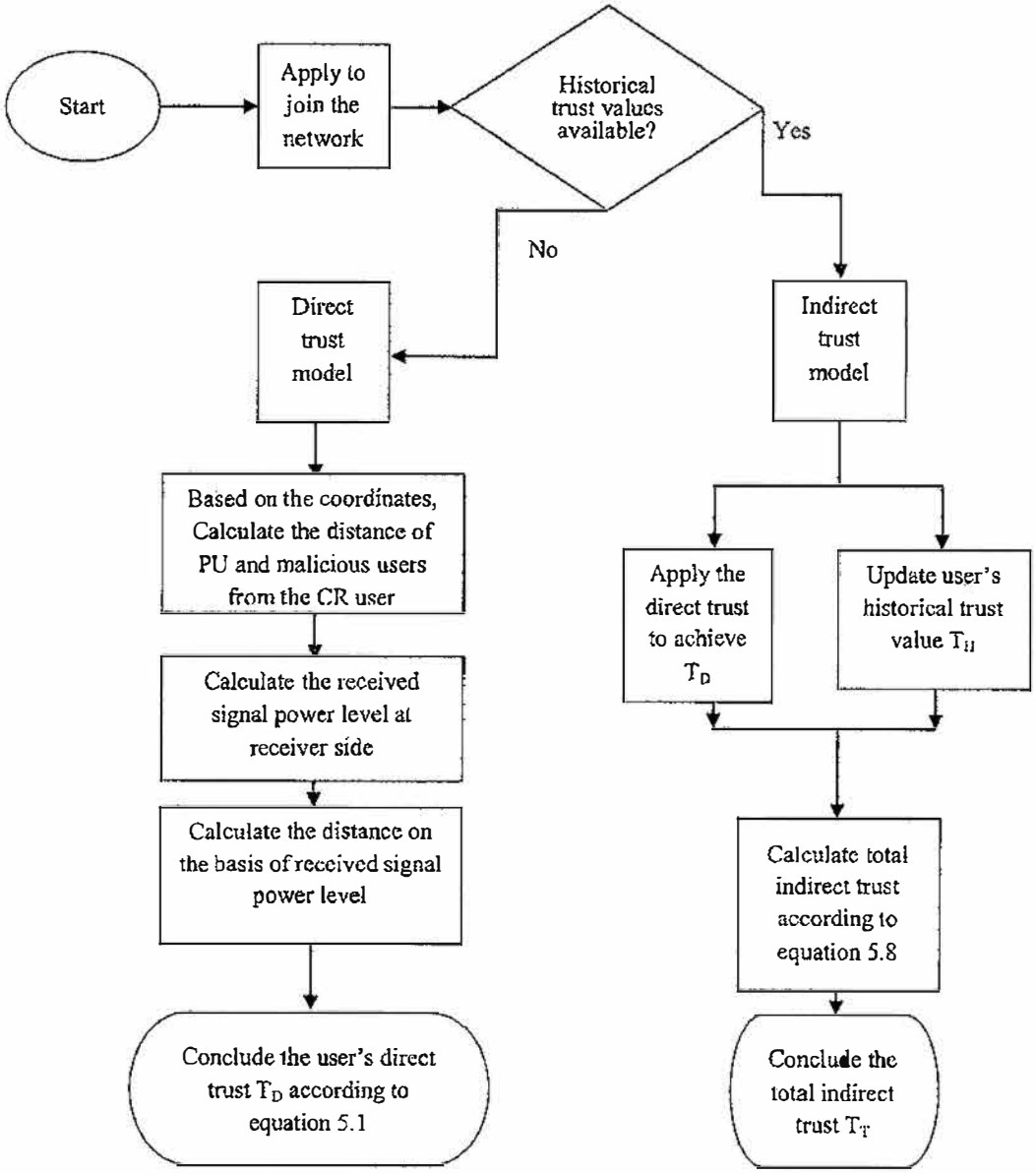

Figure 5.1 Trust management mechanism

5.5 Simulation System Model

A CRN is considered where there are a PU, SU and malicious users randomly distributed in an area of 15x15 Km^2 as shown in Figure 5.2 (This area range in general is consistent with various works in literature e.g. [85][100]).

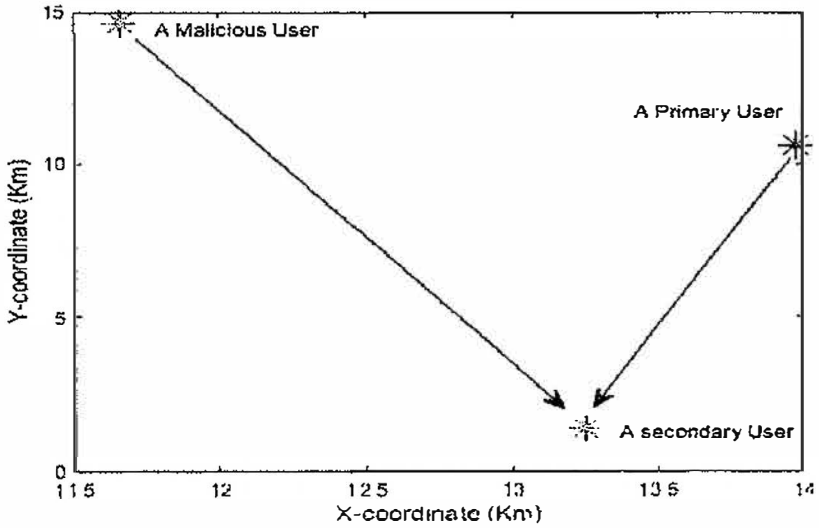

*Figure 5.2 Random location of primary, secondary and malicious users in an area of 15Km*15Km*

5.5.1 System Assumptions

In order to simulate the schemes, the following assumptions have been adopted:

- Because all the users in the system broadcast location coordinates, thus the primary user position is identified by the SU.
- The level of the transmitted power for each user is predefined and identified by all the users in the system.
- The CR user estimates d_1 and d_2. If these distances are matched, it means that the user is a legitimate user; otherwise it is an adversary user (malicious). A ground reflection (two-ray) model is considered for calculating the power level of a received signal over a distance.

To determine the location of all the users in the network, it is assumed that there are 60 instances of random coordinates for 50,000 samples. The distance is calculated based on the received power levels and also based on the coordinates. Also, it is assumed that

a Gaussian noise is added for various SNR levels. Table 5.1 below shows the simulation parameters:

Table 5.1 Simulation Parameters

Parameter	Value
SNR	-5,0,5,10,15,20,25
number of samples	50,000
N Number of instances random coordinates	60
Service Area	15km by 15km area

5.6 Simulation Results and Analysis

To evaluate the performance of the trust-management mechanisms, simulations are carried out via Matlab software (Appendix B). The simulation results for both models (Direct and Indirect trusts) are discussed in this section. Also, the fairness of the results is discussed.

Figure 5.3 shows the distance measured based on the coordinates and the distance measured based on the received power level of the PU from the SU. It is noted that both distances match considerably, indicating that the SU is actually communicating with a trustworthy user.

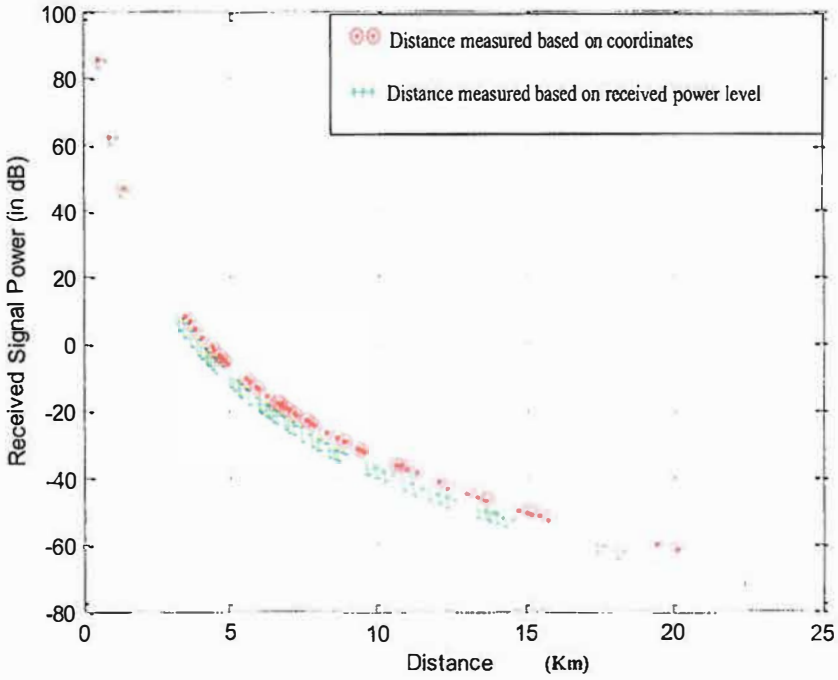

Figure 5.3 The distance measured based on the coordinates and the distance measured based on the received power level of the PU from the SU

5.6.1 Trustworthiness of the PU

To verify the performance of the direct trust approach and the indirect trust approach, the trust values are plotted in the same figure. The PU trusts are measured for different values of the historical trust which is denoted by T_H.

Figure 5.4 shows the trustworthiness of the PU with respect to the SNR values. It is noticeable that if the SNR value is raised, so correspondingly the trustworthiness of the PU increases. It is clear that the trustworthiness of the PU is always high (> 0.65) and reaches nearly 1 because it is a legitimate PU.

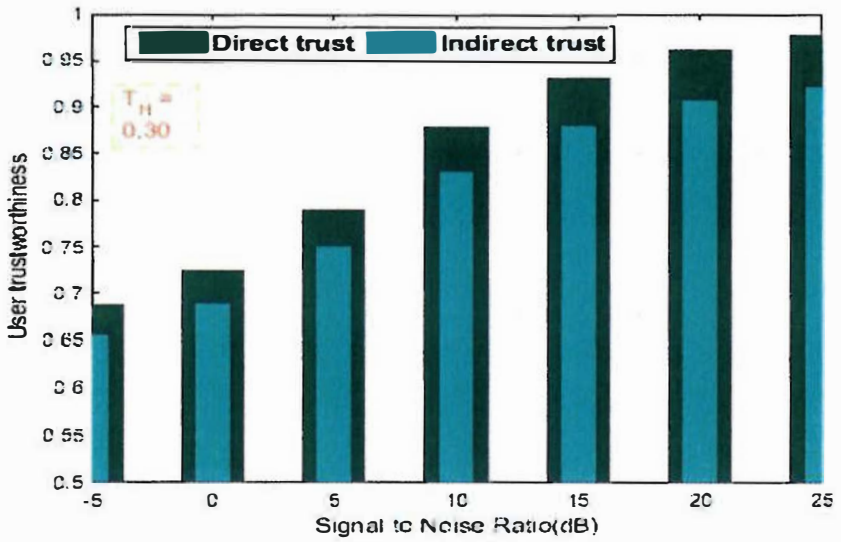

Figure 5.4 PU trusts vs. SNR when T_H =0.3

To evaluate the impact of the user's history on the total trust value, results are obtained for various T_H.

When T_H = 0.3 , as can be seen from Figure 5.4, the direct trust values are higher than the indirect trust values because the direct trust model does not take into account the historical trust behaviour of a user, whilst the indirect trust model considers the history of the user. For example, when SNR =-5 it is noted that the direct trust value is about 0.69, while the indirect trust value is about 0.65. These values of trust are slightly low because the SNR is also low. But if the SNR=15, then the direct trust increases dramatically to reach 0.93, and the indirect trust value is about 0.88, which is affected by the history of the user. However, all trusts are high because it is a good PU.

Figure 5.5 illustrates the trust values when a user has a higher T_H (T_H =0.5). It is clear that when SNR=-5, the direct trust is still at about 0.69, while the indirect trust value has slightly increased to reach 0.67 (it was 0.65 when T_H was 0.3). All the indirect trust

values are still below the direct trusts because the history of the user is still considered as low.

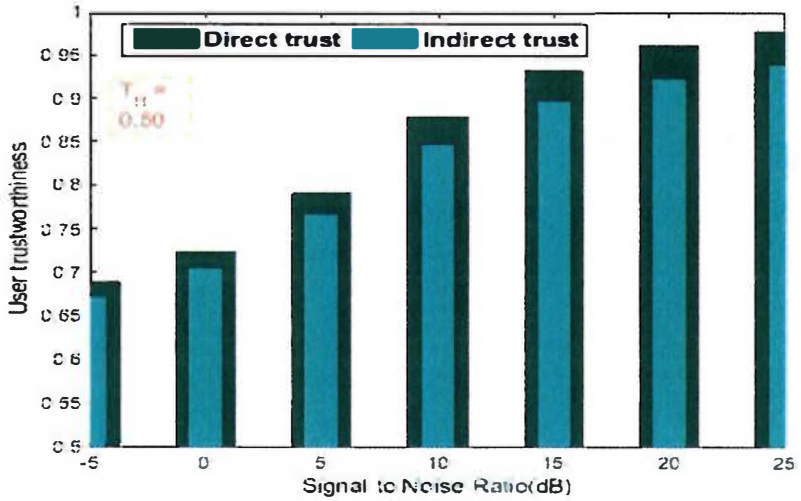

Figure 5.5 PU trusts vs. SNR when T_H =0.5

When T_H reaches 0.8, as in Figure 5.6, this will have a positive effect on the trustworthiness; for instance, when SNR =-5, the indirect trust increases from 0.67 to about 0.7. This shows the importance of the good history of a user.

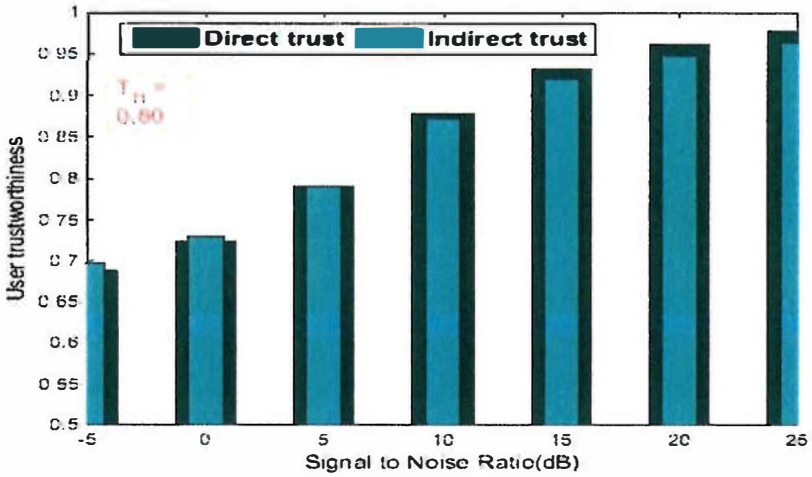

Figure 5.6 PU trusts vs. SNR when T_H =0.8

In the case where the user has a very good history, i.e. T_H =0.98 as in Figure 5.7, it is noticeable that the indirect trust reaches 0.72 when SNR=-5 and about 0.93 when SNR=15. In this case, it is clear that all the indirect trusts overcome the direct trusts and this is because the users have a great historical trust value.

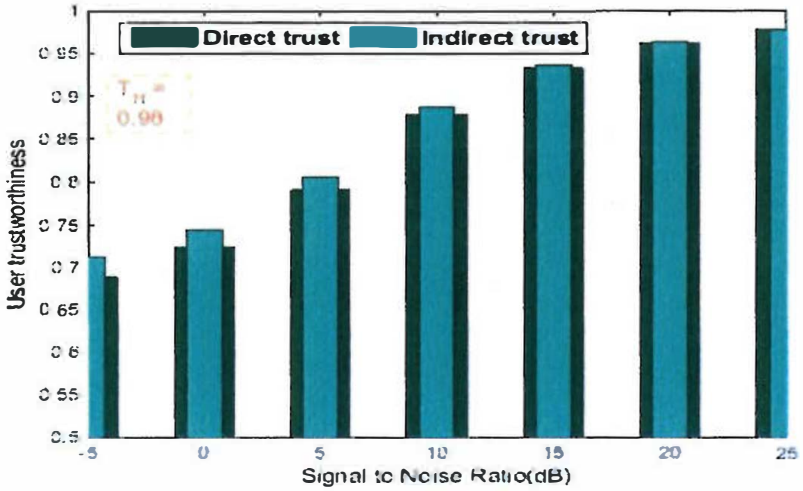

Figure 5.7 PU Trusts vs. SNR when T_H =0.98

5.6.2 Trustworthiness of the Malicious User .

The trustworthiness of the malicious users with respect to the SNR values is plotted in Figure 5.8; when T_H =0.2 this indicates that the history of the user is very low. It is noticeable that the direct trusts and the indirect trusts for the malicious user are always very low (< 0.64) even though the SNR has increased.

So the malicious user has lower trust values (direct and indirect) compared to the PU trusts, which nearly reach 1 as explained in section 5.6.1. It is noticeable that because the T_H is very low in this case, the indirect trusts for all SNRs are less than the direct trusts.

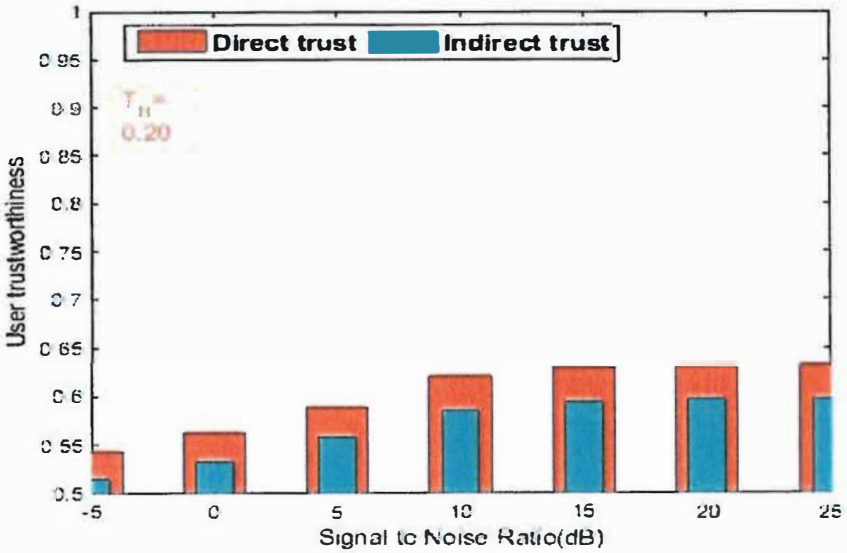

Figure 5.8 malicious user trusts vs. SNR when T_H =0.2

Once the T_H is raised, as in Figure 5.9 when T_H =0.4, the indirect trust values increase but are still below the direct trust as the history value is still low. For example, when SNR =-5, the indirect trust increases from 0.51 (when T_H =0.2) to 0.53, and this is because the user has a higher historical trust value.

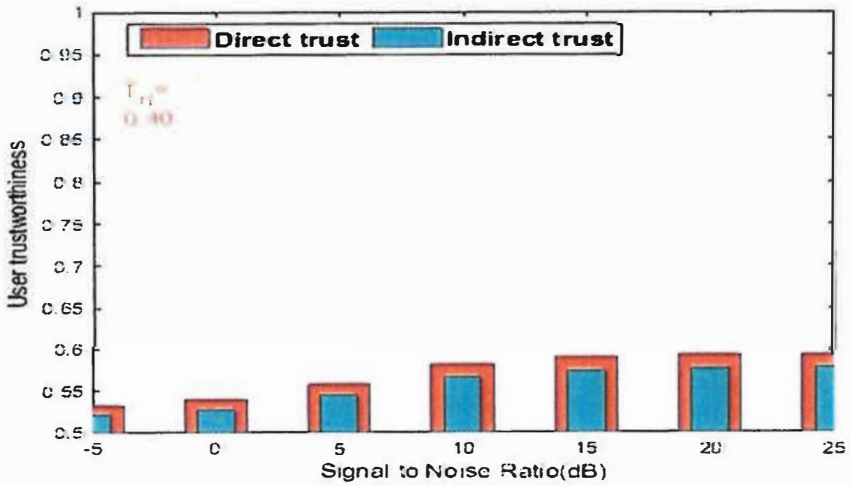

Figure 5.9 malicious user trusts vs. SNR when T_H =0.4

On the other hand, when the user has a high historical trust value T_H =0.8, as illustrated in Figure 5.10, the indirect trusts increase considering the good history of the user to overcome the direct trusts. For example, when SNR =5, the indirect trusts rise from 0.56 when T_H =0.4 to 0.59 when T_H =0.8. However, all the trust values of the malicious user (direct and indirect) are maintained at a low level even though the T_H of the user is high because the direct trust value plays the main role in the total trust calculation.

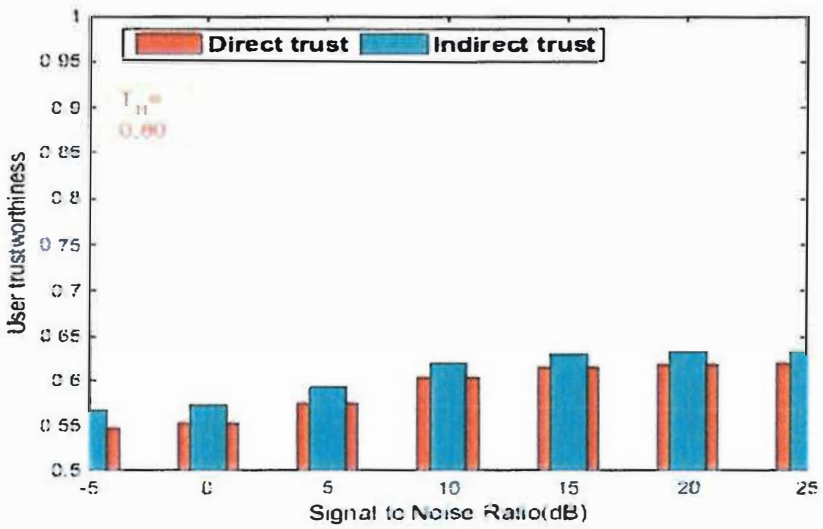

Figure 5.10 malicious user trusts vs. SNR when T_H =0.8

Fairness of the Proposed Scheme Compared to other Works

To evaluate the proposed approach, the trust-based spectrum allocation scheme presented in [91] is investigated. This shows that the trust-based model is capable of identifying the behaviour of each type of SU, and the system detected the malicious nodes and allocated them low trust values (which are about 0.2). Also, the good nodes are allocated with higher trust values of around 0.9. These results, in general, agreed

with the results of the proposed scheme, indicating that the trust values of the users represent a good assessment for securing a CRN.

5.7 Chapter Summary

In this chapter, a trust management mechanism has been studied because the user's trustworthiness is a crucial factor in a CR detection system. CRN has unique security problems, which are not faced by conventional wireless networks. The main objective of any preventive security mechanism is to eliminate or reduce the impact of malicious operations performed by an adversary.

Two trust-management schemes are presented in this chapter. Firstly, there is the direct trust scheme, which obtains user trust values based on the localization of the signal source. This scheme takes advantage of the fact that it is not possible for the malicious user to mimic both the coordinates and the power level of the PU, and thus the trustworthiness of the user is obtained by the distances measured using the coordinates and received signal power level. On the other hand, the indirect trust scheme combines the direct trust and the historical trust to obtain the trustworthiness of the users.

Simulation results have shown that the trustworthiness of the PU is much higher than that of the malicious user. Moreover, the indirect scheme improves the user's trustworthiness as it considers the historical behaviour of the user.

This chapter has studied detection schemes based on the localization technique and no punishment is imposed on the CR system. The next chapter investigates detection schemes using a CSS technique based on trust and punishment approaches to improve the performance of the CR network.

6 Trust and Punishment based Approaches for Secure Cooperative Spectrum Sensing

6.1 Introduction

The CSS process involves users that sense the spectrum and send local reports to the FC to process and manipulate these reports in order to make a final decision about the presence of a PU. During this cooperation, some adversary users can falsify the results of the spectrum sensing and the good SUs must be able to maximise the CRN's utility.

CR can be considered, for example, as wireless sensor network that needs many sensors deployed in the area of interest. Increasing the number of SUs also leads to an increased communication overhead. Various techniques can be used to perform a great trade off between the overhead saving and the performance increase; one of these techniques uses a method known as the clustering-soften hard combination [55]. The disadvantage of this cluster CSS method is noted when the SUs with good location correlation are grouped into the same cluster in order to decrease the consumption of the energy for transitioning data to the cluster head (CH). Therefore, it is highly probable that many of the SUs within a cluster can be affected by shadowing or attacker distribution, and thus the CH may make an incorrect group decision about the PU.

The spectrum sensing results that are collected from multiple users without any trust consideration could decrease the system performance significantly [92]. Therefore, designing a robust and secure CSS approach is a major challenge in terms of security management

The issues mentioned concerning the CSS can be resolved by considering a trust value for each user in the network and implementing effective punishment schemes. Therefore, to increase the performance of the CRN, trust and punishment based approaches in CSS are proposed in this chapter to improve spectrum utilisation and detection performance. In these approaches, the SUs locally decide about the presence or absence of the PU's signal and then the FC collects these decisions and uses one of the approaches to make a final decision about the spectrum status. Using these mechanisms will improve the security of the CRN and increase the sensing performance.

6.2 Tackling the Drawbacks of CSS

Combining the detection results of many users - that might have different sensing times and different sensing results - requires a powerful sharing algorithm to increase the detection performance. Therefore, trust management is essential for SUs to assess the trustworthiness of others and to selectively interact with more trustworthy users. Trust has been widely used with computing and web computing, ad hoc networks. However, the trust in CRNs is needed because the security in CSS usually needs a communication overhead in advance [93]. Trust can be defined in terms of degrees of belief that a network user can perform a job as expected; trust can be varied greatly from one CR user to another.

The FC in the cooperation system can obtain a trust value that represents the trustworthiness of a CR user based on some factors such as the local sensing difference, the sensing location factor and the control channel condition. These trust

values help to reduce the impact on the final decision of SUs that have low trust values, while improving the impact of SUs with high trust values.

Generally in the CSS, the malicious users can be classified as follows:

- Smart Malicious: This type of attacker senses the channel in each of the time slots and if the channel is occupied "1" they send "0" and vice versa.
- "Always Yes" Malicious: These malicious users always send "1" to FC and they are not as smart as the first type. They do not sense the channel and without any attention to the state of the channel, they always send "1". The purpose of these malicious users is a DoS attack.
- "Always No" Malicious: They are like 'always yes' nodes but always send "0" to FC. The purpose of this type of attacker is to cause interference with the PU in occupied bands.

6.3 Proposed Trust and Punishment based Approaches for CSS Model

A model that relies on user trust values and implements different punishment approaches is developed to improve the robustness of the data fusion techniques in order to make a global decision about spectrum availability.

This model assigns high weights to trusted users and lower weights for the users that are less trusted. Therefore, the proposed mechanism evaluates the trust values and can punish either the whole system or impose punishment only on users with low trust values.

It is assumed that the FC is mainly responsible for the trust value store/update, punishment policy procedure. SUs in the network report the local decision values to the FC, and if the trust value of the SUs is evaluated as low, based on the proposed

approaches, the less they contribute to the global decision. So a higher correct detection probability should be guaranteed.

Related Work

A trust-based secure spectrum situation fusion in distributed CRNs is proposed in [94] to counter attacks. The neighbouring nodes of SUs obtain the corresponding dynamic trust value according to their behaviour, which restricts the impact of the malicious behaviour based on the premise of ensuring the information interaction of normal nodes. They showed that the consensus fusion scheme based on trustworthiness has a better performance than the existing algorithm which eliminates the neighbouring node with the biggest deviation value from the mean value.

Also [95] studies the impact of high numbers of malicious users being present in a CRN; the study is based on trust accumulation to combat the adverse effects of misbehaved CRs. Considering the fact that the performance of this trust-based scheme is sensitive to the correctness of the global decision, the simulation results in this study verify the effectiveness of the proposed scheme even when there is a large number of misbehaviours.

To investigate the influence of the number of malicious users on the detection performance, the work in [96] studied the performance analysis of a cascaded energy and matched filter (CEM) detector in the presence of malicious users. The detection performance of the CEM detector is analysed with the incorrect sensing information of the malicious users. To reduce the effect of malicious users on the sensing performance, an authentication code is used which is validated by the FC for the overall decision making process. The work explained the achievable spectrum sensing

efficiency with different numbers of malicious users for the CEM detector. As the number of malicious users increases, the achievable spectrum sensing efficiency of the detector decreases. Higher numbers of malicious users greatly affect the spectrum sensing efficiency of the CEM detector.

6.3.1 Cognitive Scenario of the Proposed Mechanism

In this section, the scenario of CSS in CRNs is described in order to investigate the impact of the user's weights and punishment procedure on the CRN's performance.

6.3.1.1 Application Scenario

A centralised CRN scenario is presented as in Figure 6.1; it is assumed that there are some honest 'Good' SUs and some malicious users in the network. All users send their reports to the FC node.

FC: each user sends its report to the FC, which is responsible for using these reports to decide on the presence or absence of a PU. It calculates and stores the trust values of all the SUs in a CRN, implementing punishment on the users according to the punishment model, and then updating the SU trust values.

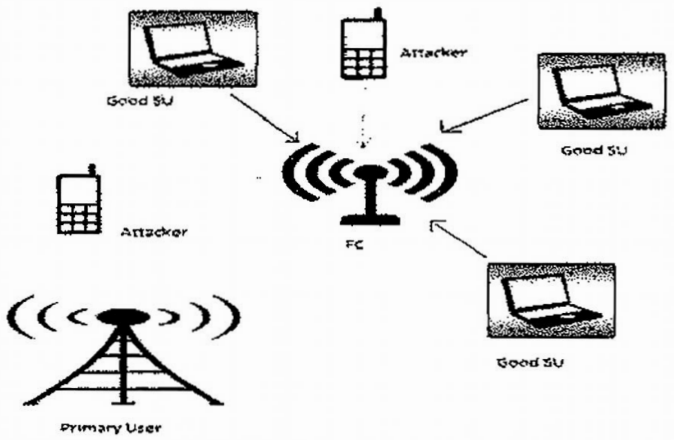

Figure 6.1 Central FC structure

6.3.1.2 Hypothesis of the Simulated FC

The mechanism of the FC is as follows:

1- Consider a CRN, with M SUs to sense the spectrum in order to detect the existence of a PU.

   The whole set of SUs M is divided into two sets, malicious and good SUs. The number of good SUs is denoted by G where the number of malicious users is denoted by K, So M=G+K.

2- It is considered that each CR user i performs local spectrum sensing independently, considering the i^{th} CR user. The local spectrum sensing problem is to decide between the following two hypotheses: if a PU is present (H_1) or not (H_0):

$$x_i(t) = \begin{cases} n_i(t): & H_0 \\ s(t) + n_i(t): & H_1 \end{cases} \qquad 6.1$$

   Here: s(t) is the transmitted signal from the PU

   $x_i(t)$: is the observed signal at the i^{th} CR,

   $n_i(t)$ is the additive white Gaussian noise (AWGN)

3- The CR users make the one bit decision and send it to the FC to process all the received reports and use one of the proposed approaches: the trust based

CSS approach, the general punishment based CSS approach or the dedicated punishment based CSS approach.

6.4 The Mechanism Flowchart of Trust and Punishment Approaches

This section explains the CSS flowchart based on trust and punishment approaches. As shown in Figure 6.2, the CSS scheme is carried out in various steps, i.e. combining reports from different SUs, trust evaluation, punishment procedure, and then the global decision is made. Each step accomplishes its own task as explained in the following sections.

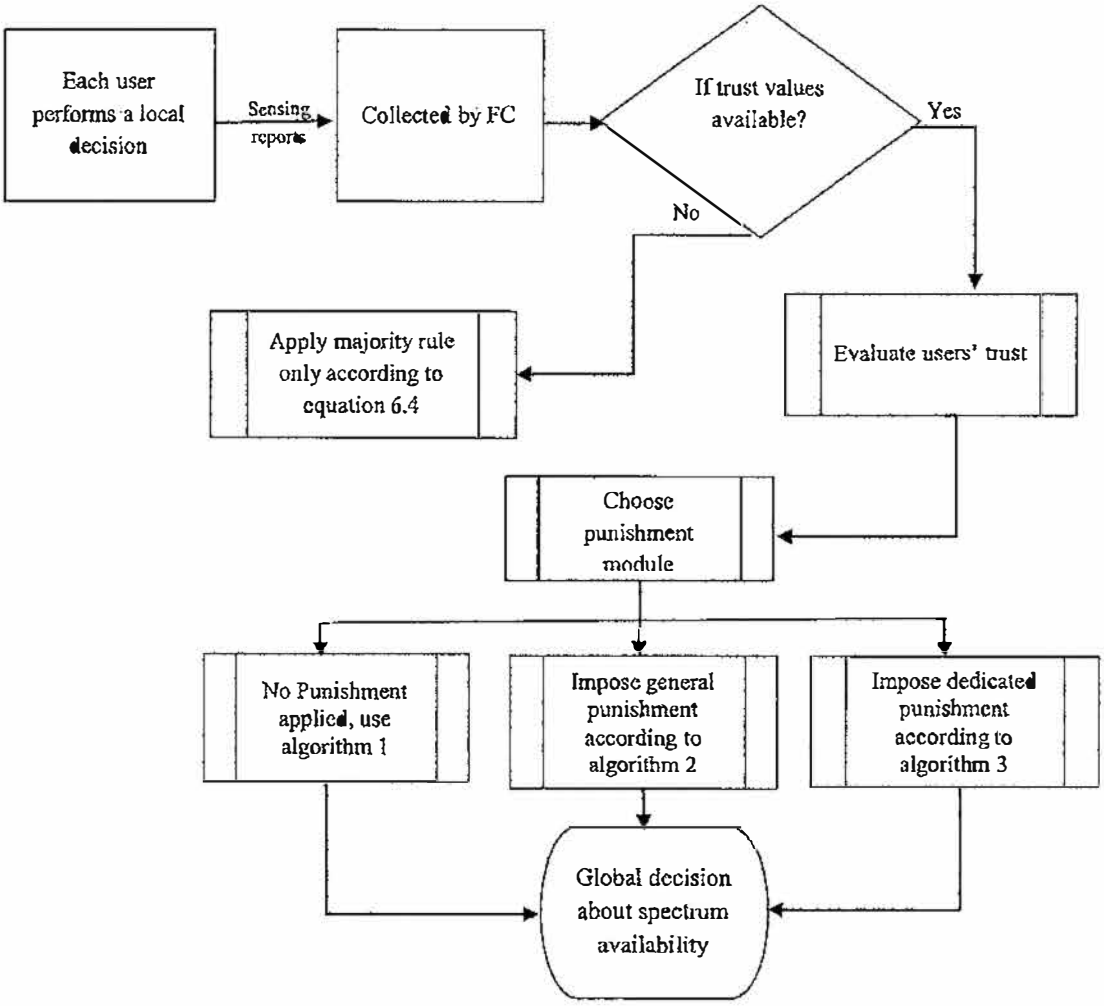

Figure 6.2 Flowchart of trust and punishment based scheme

6.4.1 Trust Evaluation

The trustworthiness of SUs needs to be evaluated by the FC, and updated continuously based on new observations. Trust values are usually employed to represent the trustworthiness of SUs.

The FC evaluates and maintains the trust values of SUs according to their sensing results in CSS, i.e. whether they match the actual sensing result or not. For instance, each SU_i has a trust value T_i which is a real number ranging from 0 (complete distrust) to 1 (complete trust). A higher trust value makes the SU contribution greater for making a correct decision and vice versa.

In this work, a user is considered as a 'low trust' user if its trust value is less than a predefined trustworthiness threshold (Á). Consequently, this user will have a lower contribution to the global decision.

6.5 Proposed Approaches

Because malicious users significantly reduce the detection accuracy and have an adverse impact on the global decision, it is therefore crucial to alleviate their impact on the network's performance. In this section, the proposed approaches are explained and the impact of the number of honest and malicious users on the system is studied.

These approaches are namely: the trust based approach, the general punishment based approach, and the dedicated punishment based approach.

6.5.1 Conventional Majority based Approach for CSS

In the majority scheme based CSS, the FC declares that the channel is occupied when half or more than the half of the SUs declare that the channel is occupied [97]. The whole set of SUs is divided into two groups as mentioned in section 6.3, i.e. good users

and malicious users. The number of malicious users is denoted by K, the total number of all users is M, and so the number of good SUs in the system is G:

$$G = M - K \tag{6.2}$$

As the name of this model implies, majority-based CSS is used without trusted nodes assistance (no trust value is assigned to be used), and it depends only on the number of users. So the correct decision is achievable only if the number of good SUs is greater than or equal to the number of malicious users.

Mathematically, the majority rule makes the global decision as follows:

Depending on the sensing result, each SU decides on one of the two hypotheses: either H_0 which implies that the channel is unused, or H_1 which implies that the channel is used. Then it reports its binary local decision L_i (0="un*used*", 1="*used*") to the FC in order to take a final decision Y based on the following equation:

$$\text{Final decision } Y = \begin{cases} 0 & , \text{ if } \sum_{i=1}^{M} \text{Li} < M/2 \\ 1 & , \text{ if } \sum_{i=1}^{M} \text{Li} \geq M/2 \end{cases} \tag{6.3}$$

When Y=0, the spectrum is not used, and when Y=1, the spectrum is used.

The majority only based approach is not ideal in the environment where the likelihood of the number of malicious users existing in the system is higher than the good users. This limitation has motivated the design of trust and punishment approaches which depend on the weights of the users.

6.5.2 Trust based Approach for CSS

In order to ensure the robustness of CSS, this section presents a trust based mechanism which relies on the trust values and number of the users rather than the number of users only.

The main idea is that the users with a high trust value should have a higher contribution to the final decision. Taking into account the shortcomings of the majority approach explained earlier, which does not take into account the trustworthiness of the users, this approach presents a flexible trust CSS model against malicious users via the utilisation of trust values.

Algorithm 1 below shows how this approach operates, the key contribution of this scheme is that it effectively distinguishes malicious users from good users by their trust values. SUs whose trust values are over a predefined threshold (Á=0.5) are considered as trustworthy users. Therefore, this increases the contribution of the 'high trust' SUs in the global decision.

Algorithm 1: trust based algorithm for CSS

Input: T_i, Trust values of users i ,i=1: to M

Á =0.5 , Threshold of trustworthiness

Assume Spectrum is occupied (H_1)

For all SUs i=1: to M do

If $T_i \geq$ Á then L_{di} =1

Otherwise L_{di} =-1

End for

Take the final decision according to equation below

$$\text{Final\_Decision } Y = \begin{cases} H_1 ; \sum_{i=1}^{M} L_{di} T_i \geq 0 \\ H_0 \quad otherwise \end{cases}$$

If $Y=H_1$ then a correct decision is made. Otherwise, a wrong decision is made

L_{di} = Local decision of user i [1 spectrum occupied, -1 spectrum unoccupied], and M= Total number of users.

Mathematical Analysis

During the reporting phase, all the local decisions L_{di} are sent to the FC. The FC applies one of the presented approaches to obtain a global decision.

In order to investigate how the user's trust influences the detection performance with incorrect sensing information from the malicious users, it is assumed that the spectrum is actually occupied H_1 and the local decisions L_{di} =1 for the good user and -1 for the malicious user because it is considered that the malicious users convert the actual spectrum status.

Numerical Example for Trust based Approach

To explain how the trust based approach works mathematically, the case when M=20 is discussed in this section. Algorithm 1 determines how many good users G out of M are needed to make a correct sensing decision by declaring that the spectrum is busy H_1. K is varied (in ascending order) to find out when an incorrect decision is made. In this case, when M=20 and for the instant when K=12, this implies that there are 8 good SUs. Also, each SU is assigned with a trust value T_i; for example, when T_i=0.7 for the good users and 0.3 for the malicious users, the final decision Y according to algorithm 1 is H_1, which indicates that the final decision matches the actual decision so a correct decision is taken. But if K=16, for example, the final decision Y is H_0 and this is an incorrect decision.

6.5.3 General Punishment based Approach for CSS

Obtaining the trust values of all users in order to evaluate their contributions to the global decision represents an important step in alleviating their effects on network performance. However, further action should be taken against less trustworthy users in the cognitive system in order to reduce their contribution, which might affect the whole

of the cognitive system's utility. In this section, a punishment based mechanism is proposed; algorithm 2 explains the mechanism of this approach.

If malicious users exit in the system, a penalty would thus be imposed on the system. It is assumed that if all the SUs follow the controller's spectrum-access policy and a collision occurs, then all of them are responsible and share the punishment enforcement. Otherwise, the penalty is imposed on the particular SU that has a low trust value as explained in algorithm 3.

The shortcoming of this approach is that when the punishment factor is set very high, it causes a resistance cost that reduces the honest user contribution even if it has a high trust value.

Algorithm 2: General punishment based algorithm for CSS

Input: T_i, trust values of users i, i=1: to M

Á =0.5, Threshold of trustworthiness

Assume Spectrum is occupied (H_1)

For all SUs i=1: to M do

If $T_i \geq$ Á then L_{di} =1

Otherwise L_{di} =-1

End for

Do steps below to start a general punishment process

Choose a punishment factor P

Take a final decision according to equation below

$$\text{Final\_Decision} \quad Y = \begin{cases} H_1 : \sum_{i=1}^{M} L_{d_i} T_i^P \geq 0 \\ H_0 \quad otherwise \end{cases}$$

If Y=H_1 then a correct decision is made

Otherwise, a wrong decision is made

L_{di} = Local decision of user i [1 spectrum occupied, -1 spectrum unoccupied] , M= Total number of users.

Numerical Example for General Punishment based Approach

This approach aims to investigate the impact of imposing a punishment on the users; thus the number of users is varied and a punishment is imposed to find out when a wrong decision is made due to increasing the number of malicious users. As an example, if M=23, algorithm 2 can find out the maximum number of malicious users a system can tolerate to make a correct decision. Referring to final decision Y in algorithm 2, let T_i=0.7 for the good users and 0.3 for the malicious users and p=1.5. When K =12 (which means 11 good users out of 23) then the final decision Y will be H_1, which matches the actual decision, so a correct decision is taken. But if k= 20 (which means 3 good users out of 23) then an incorrect decision is made.

6.5.4 Dedicated Punishment based Approach for CSS

Imposing the punishment on all users in the cognitive system (as in algorithm 2) could affect the good users by causing them to have a lower contribution to the global decision.

Because there is a need to maximise the expected utility of all the good SUs in the global decision, this approach is designed to impose the punishment only on the particular SU who violates the FC (users with low trust values). The FC in this model acts on behalf of all the SUs in the cognitive network and imposes punishment on unreliable users only. According to the above analysis, algorithm 3 illustrates the mechanism of dedicated punishment approach.

Algorithm 3: Dedicated punishment based algorithm for CSS

Input: T_i, trust values of users i ,i=1: to M

Á =0.5; Threshold of trustworthiness

F=0; Good users counter

K=0; Malicious users counter

Assume Spectrum is occupied (H_1)

For all SUs i=1: to M do

If $T_i \geq$ Á then

{ User i is good SU ,F=F+1, L_{gf}=1 and T_{gf}=T_i }

Otherwise {User i is malicious user, k=k+1, L_{mk}= -1 and T_{mk}=T_i }

End for

Do steps below to start dedicated punishment process

Choose a punishment factor P

Take a final decision according to equation blew

$$\text{Final\_Decision } Y = \begin{cases} H_1 : \sum_{i=1}^{F} L_{gf} T_{gi} + \sum_{i=1}^{k} L_{mi} T_{mi}^{p} \geq 0 \\ H_0 \quad otherwise \end{cases}$$

If $Y=H_1$, a correct decision is made

Otherwise, a wrong decision is made

When L_{gf}= Local decision of good user f, L_{gi} = Local decision of good user i, T_{gf}= Trust of good user f, T_{gi}= Trust of good user i, L_{mk} = Local decision of malicious user k, L_{mi} = Local decision of malicious user i, T_{mk}= Trust of malicious user k, T_{mi}= Trust of malicious user i, [1 spectrum occupied, -1 spectrum unoccupied].

Numerical Example for Dedicated Punishment based Approach

Imposing a punishment on malicious users only, rather than punishing all the users, is examined in this approach by varying the number of users. For example, if M=16, algorithm 3 can determine the maximum number of malicious users that a system can tolerate to make a correct decision. Let T_i=0.7 for the good users and 0.3 for the malicious users and p=1.5, when K=14 (which means only 2 good users out of 16), then the final decision Y in algorithm 3 will be H_0.This does not match the actual

decision, so an incorrect decision is taken. But if k=10 (which means 6 good users out of 16) then a correct decision is made.

6.6 Simulation Results and Analysis

To evaluate the performance of the proposed CSS approaches and to discuss their effectiveness on the detection probability, MATLAB software is used to simulate the algorithms 1, 2 and 3 (Matlab simulation codes are attached to appendix C). In the simulation, the total number of users M and the number of malicious users K are varied to find out when a wrong decision is made.

It is considered that the fusion rule explained in section 6.3.1 is used. In order to verify the schemes, the malicious users in the attack scenario are assumed to be smart malicious users and always send the opposite result to the FC to reduce the spectrum sensing accuracy.

6.6.1 Result of the Conventional Majority based Approach

For comparison, the conventional majority scheme and the proposed trust weighted schemes are simulated with different numbers of good and malicious users. Here, the majority conventional scheme is the conventional CSS scheme without trust values assigned as explained in equation 6.3.

Because conventional majority scheme is used when there are no trust factors available, so it depends only on the number of users. The relationship between the correct sensing range and the number of SUs is analysed when the number of malicious users is varied.

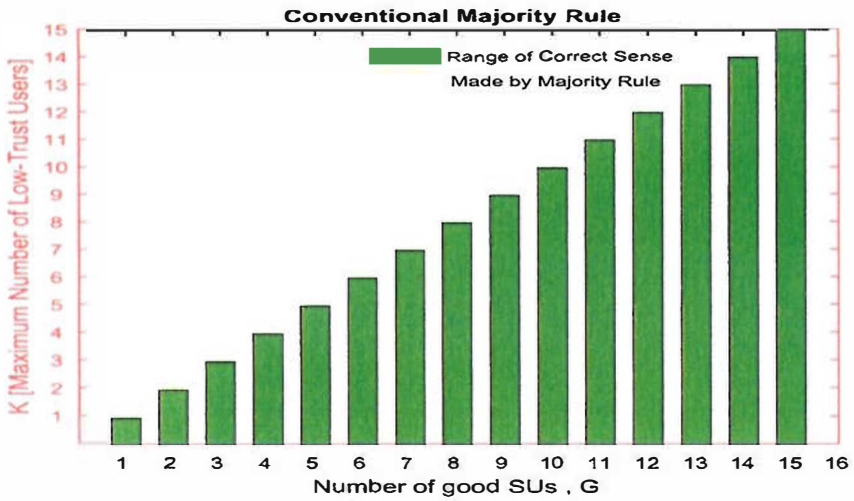

Figure 6.3 Range of correct sense for different G and K

As shown in Figure 6.3, based on the conventional majority rule only, the correct sense about the spectrum availability is achieved only when the number of good SUs is equal or greater than the number of malicious users. For example, when G is equal to 8, so the correct decision is achievable only if K is 8 or less, i.e. the ratio of good SUs needed in the system to make a correct decision must be at least 50%.

Notice that this approach is not ideal in an environment where there are more malicious users in existence in the system than there are good SUs; this has led to the proposed methods that overcome the disadvantages of this approach.

6.6.2 Result of Trust based CSS Approach

This model takes advantage of the fact that the FC combines the local decisions with other information to compute the final sensing result. So the FC can make the correct decision even though the number of malicious users is greater than the good SUs.

Figure 6.4 shows the correct sensing range when varying the number of malicious users in the network.

The trust value of good SUs is denoted by T_g and the malicious users' trust is denoted by T_m, and the result is obtained with different values of T_g and T_m. First, take the case when T_g =0.7 and T_m=0.3.

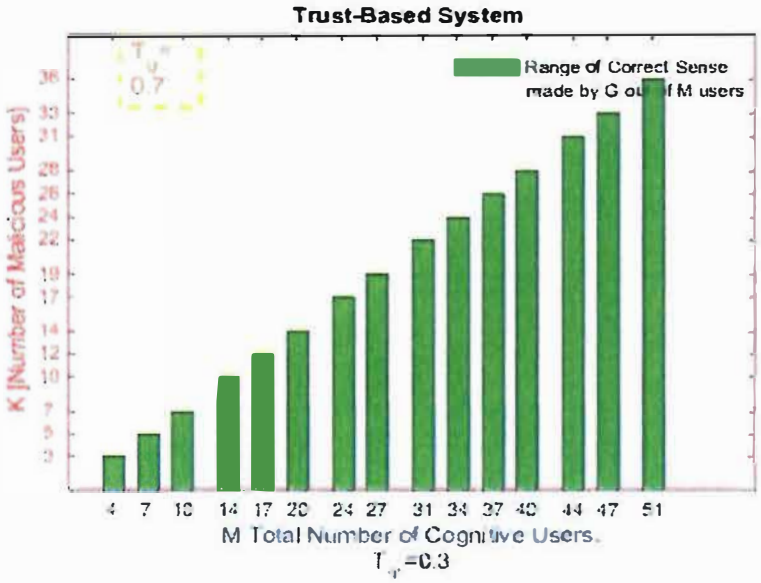

Figure 6.4 Range of correct sense for different M and K

To explain the result in Figure 6.4, let us investigate the case when M=34. In this case, if K is above 24 then an incorrect decision is made and a correct decision is taken if K is less or equal to 24. In another example, when M=37, then K must be less than or equal to 26 for a correct decision.

In another case, the good users trust is increased to 0.8 (T_g =0.8) while the malicious users still have the same trust value (T_m=0.3) as in Figure 6.5. Let us consider the case when M=34 and M=37 in order to compare with the previous example; the result shows that the correct decision when M=34 is achievable with the condition that K<=25. And when M=37, K must be <=27 for a correct sense. i.e.

if T_g =0.7 , M=34: K <=24 for a correct sensing.

if T_g =0.8 , M=34: K <=25 for a correct sensing.

if T_g =0.7 , M=37: K <=26 for a correct sensing.

if T_g =0.8 , M=37: K <=27 for a correct sensing.

This indicates that the system can tolerate more malicious users K to make a correct decision when the good user trust T_g is increased.

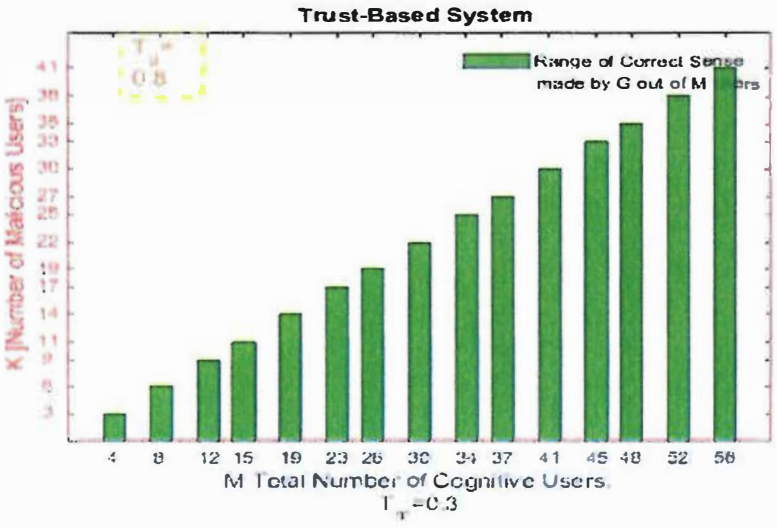

Figure 6.5 Range of correct sensing for different M and K

If T_m is increased to 0.4 while T_g is 0.7, so more good SUs are needed to cooperate to make a correct decision. As shown in Figure 6.6, for example when M=20, then 14 or more malicious users can make a wrong decision. In contrast, when T_m was 0.3 and T_g=0.7, 14 malicious users were not able to make an incorrect sensing decision.

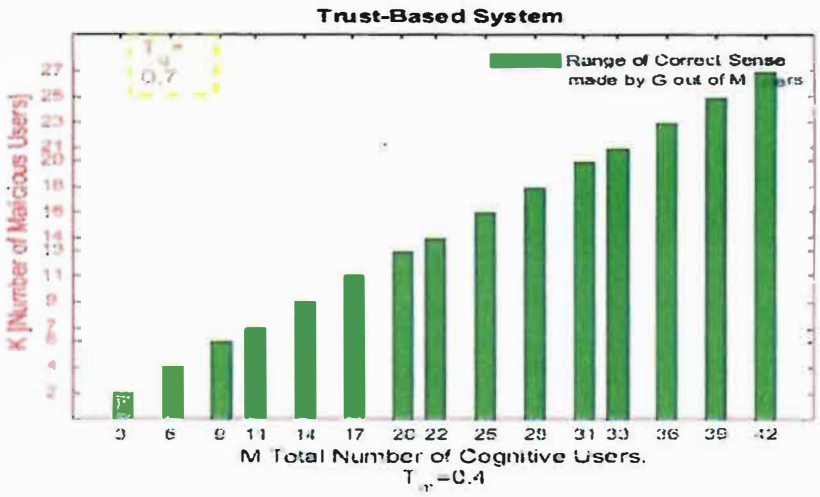

Figure 6.6 Range of correct sensing for different M and K

Simulation Assumptions Influence on the Result Relationship

From these result, it is noticeable that when all malicious users have the same trust value and the good users have the same constant trust value T_g, there is a positive correlation between the total number of users and the maximum number of malicious users that a system can tolerate to make a correct decision. The maximum number of malicious users increased, when the total number of users and the number of good users increased.

The aim of the simulation is to investigate the influence of the number of users on the final decision about the spectrum status, and to find out the maximum number of malicious users that the system can tolerate to make correct spectrum sensing decisions. Therefore, it is assumed that the good users have the same constant trust value T_g and the range of correct sense is obtained when all malicious users have the same trust value T_m with varying only the users number. Because in each example T_g and T_m are not varied, only the numbers of good and malicious users are varied in the

system, thus the final decision equation formulates a linear relationship in all the results.

To investigate the influence of assigning different trust value (T_g and T_m) for each user on the relationship of these results, a numerical example is discussed in section 6.6.4.

6.6.3 Result of the General Punishment based CSS Approach

In this section, the impact of the general punishment approach is discussed whereby the punishment is imposed on all the users as the system believes all the users must be punished.

To investigate the effect of the number of attackers that exist in the network and the punishment effectiveness on the system, different punishment factors are applied on the system. The existing trust models consider different values of the punishment factor; for example, [92] considered the punishment factor =1.25. The penalty factor in [98] is set to 5. In [99], the punishment could be set as a large enough fixed value because the malicious users are detected correctly, such that the punishment does not cause any resistance cost.

In the proposed approaches, the punishment factor P is varied between 1.5 and 2 in order to investigate its effectiveness on detection performance.

The range of correct sensing using the general punishment mechanism is shown in Figure 6.7, while varying the number of users. First, the result is shown when T_g=0.7, T_m=0.3 and P=1.5. For example when M=37, in this case the number of malicious users can be up to 29 for a correct sensing, while there were only up to 26 malicious users in the trust approach. This indicates that the punishment approach can tolerate more malicious users than the trust approach to make a correct sensing.

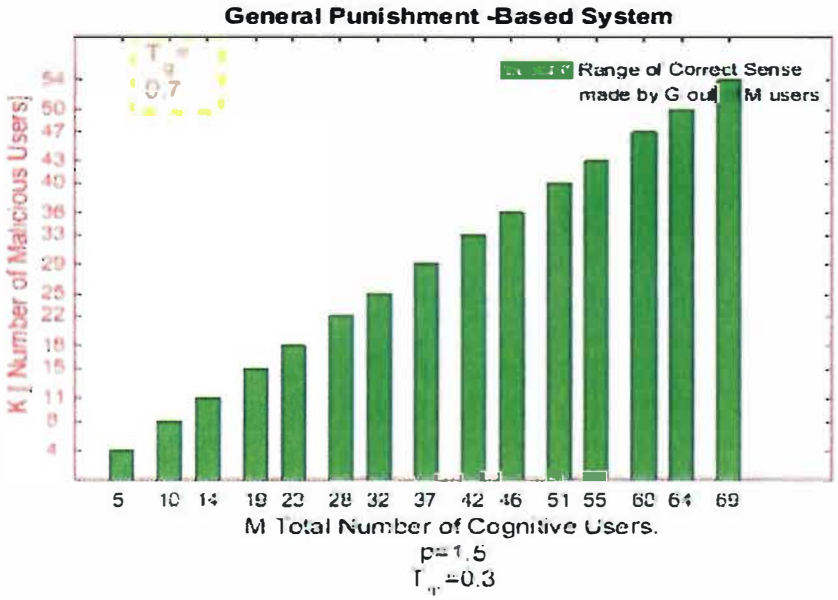

Figure 6.7 Range of correct sensing for different M and K

Now the throughput is investigated when increasing P to 1.7 as shown in Figure 6.8, when M=37 for example, then only more than 30 malicious users are able to make the FC conclude with the wrong decision while when P was 1.5 more than 29 malicious users were able to make the FC conclude with the wrong decision. This explains that a higher punishment factor makes the system more tolerate of malicious users.

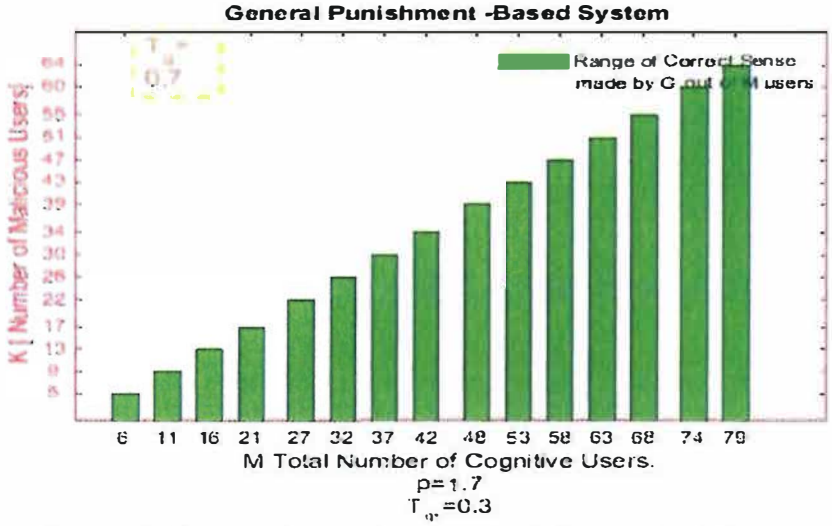

Figure 6.8 Range of correct sensing for different M and K

6.6.4 Impact of Trust Variation on the Linear Relationship

This section explains the impact of varying the users' trust values on the form of the relationship between the total number of cognitive users and the number of the malicious users. Therefore, in the following numerical example it is assumed that each user has a different trust value, whereas, each previous example used constant trust values T_g and T_m that led to form a linear relationship between M and K.

Based on algorithm 2, Figure 6.9 shows some wrong decision points (red dashes) for different M and K with various users' trust values. Users' numbers are sorted in an ascending order.

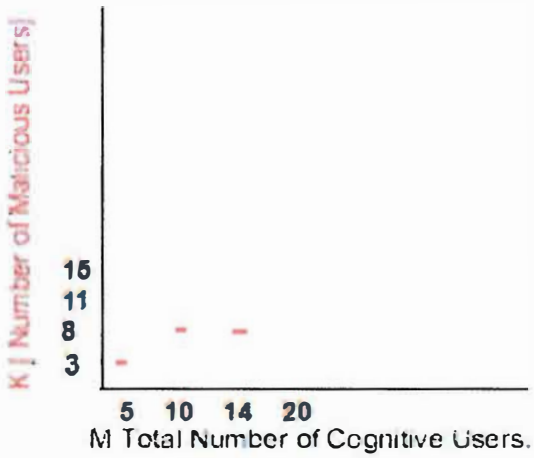

Figure 6.9 Wrong decision points for different M and K when varying users' trust values

To discuss the result in Figure 6.9, let T_{gi} denotes the trust value of good user number i, and T_{mi} denotes the trust value of malicious user number i. For analysis, M and K values in this example are chosen as follow:

Case 1: If the total number of users is 5 (m=5) and there are 3 malicious users (k=3), then this means there are 2 good users. For the purpose of analysis, it is assumed that

all the users have different trust values as follows (according to algorithm 2, the trust value is lower than 0.5 for the malicious users and 0.5 or greater for the good cognitive users).

For the two good users assume T_{g1}=0.60 and T_{g2} =0.55

For the three malicious users assume T_{m1}=0.48, T_{m2} = 0.49 and T_{m3} =0.45

Using these different trust values, and according to the final decision equation in algorithm 2 with P=1.5, the FC will make a wrong decision. However, this wrong decision point can be changed if the trust values of the users are changed, which can lead to a different form of result relationship.

Case 2: For this example M=10, and K=8, which means there are only 2 good users out of a total 10 users. If each user has a different trust value as follows:

T_{m1}=0.48, T_{m2}=0.34, T_{m3}=0.45, T_{m4}=0.47, T_{m5}=0.33, T_{m6} =0.44, T_{m7}=0.46, T_{m8} =0.32 and assume T_{g1}=0.60 and T_{g2}=0.55 in this case and according to algorithm 2, an incorrect decision is taken. This incorrect decision point can be changed if the trust values of the users are changed.

Case 3: For this analysis M=14, and K=8, meaning there are 6 good users. If different trust values for each user are assumed as follows:

T_{m1}=0.49, T_{m2}=0.40, T_{m3}=0.48, T_{m4}=0.47, T_{m5}=0.33, T_{m6} =0.44, T_{m7}=0.46, T_{m8} =0.42

T_{g1}=0.52, T_{g2}=0.55, T_{g3}=0.50, T_{g4}=0.51, T_{g5}=0.54, T_{g6}=0.50 then these trust values make incorrect decisions. Changing these trust values will change the decision point.

This example illustrates that when assigning different trust values for each user, the decision point does not depend only on the number of users, but also on the trust value

of each user. A different trust value for each user forms a non-linear relationship between the malicious users' number and the total number of cognitive users.

6.6.5 Dedicated Punishment based CSS Approach Result

In this section, the impact of imposing a punishment on malicious users only is investigated. The performance of the dedicated punishment approach is investigated first when T_g =0.7, T_m =0.3 and P=1.5. From the result in Figure 6.10, focusing on the case when M=32. The result shows that the system in this case can tolerate up to 26 malicious users to make a correct sensing, but if K is greater than 26 then an incorrect decision is made. For comparison, the general punishment approach was able to tolerate only up to 25 malicious users when M=32 as shown in Figure 6.7. This means that the dedicated punishment approach out-performs the general punishment approach because it can tolerate more malicious users.

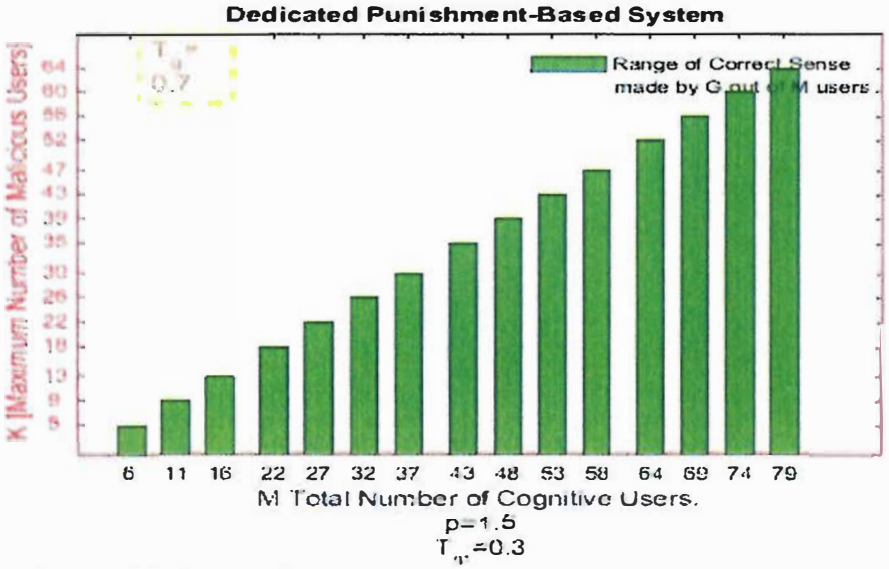

Figure 6.10 Range of correct sensing for different M and K

To investigate the influence of the punishment factor on the dedicated punishment approach, P is increased (P=1.7) keeping the same trust values (T_g =0.7, T_m=0.3), and K is varied to examine the range of correct sensing as shown in Figure 6.11. For the

case when M=58, it is noticeable that the decision is correct when K is up to 49, which means that 9 good users out of 58 users are able to identify the spectrum appropriately, while when P was 1.5 (Figure 6.10), at least 11 good users were required out of 58 users for correct sensing.

This means that increasing the punishment factor in a hostile environment where many malicious users can exist can reduce the effect of the high number of malicious users.

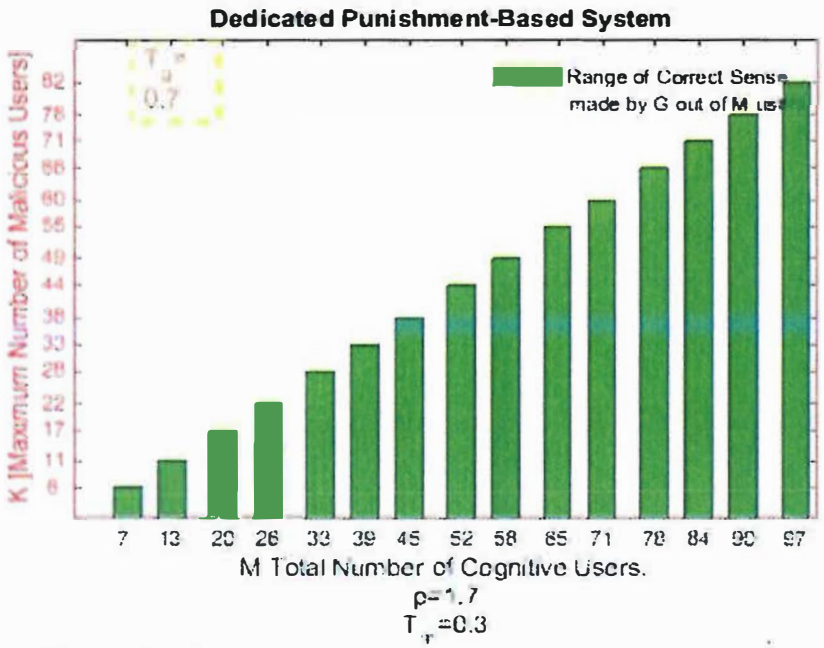

Figure 6.11 Range of correct sensing for different M and K

This result indicates that the dedicated punishment approach increases the detection performance even though there is a great number of malicious users in the CRN. The choice of the value of P in the proposed approaches is ideal from 1.5. Because if P is less than that, the range of correct sensing can be degraded even though a small number of malicious users exists.

6.7 Chapter Summary

In this chapter, the issue of improving the performance of CSS has been discussed. Trust and punishment approaches for secure spectrum access in CRNs have been addressed. The main idea in these approaches is that each SU performs local sensing and then forwards the sensing results to the main FC, so the FC makes the final decision about the presence of the PU based on the local sensing and the trust values of the users. The punishment approach does not depend only on the trust values but it also punishes the users in order to substantially reduce the effect of SUs with a low trust value, while improving the impact of SUs with a high trust value on the final decision.

Simulation results show that the proposed approaches can improve the sensing performance under the impact of different numbers malicious users in the CRN. The results show that the proposed approaches outperform the conventional majority scheme despite a high number of malicious users. Also, the dedicated punishment approach, which punishes only the malicious users, outperforms the other approaches as it can tolerate more malicious users to make a correct decision.

7 Conclusions and Work Limitations

7.1 Conclusions

CR allows the users to utilise the available spectrum by opportunistic access to the licensed spectrum bands with no interference with the other users. The fundamental objective of CR is to provide an efficient utilisation of the wireless spectrum.

The unique characteristics of CR communication have led to new threats that need to be faced. This thesis has studied some of the threats in CR, such as the PUEA and the SSDF.

In order to successfully deploy a CRN and realise its benefits, some of the counter-measures were proposed and analysed.

The main contributions of the thesis are summarised as follows:

- ✓ **Mitigation of a PUEA based on the Analytical Model:**

The PUEA is one of the major security threats to spectrum sensing because it degrades the performance of the CRN. In this thesis, a CRN model consisting of a PU, an SU and some malicious users is discussed. The impact of a PUEA on a CRN is investigated using an analytical model that detects the PUEA without using any location information and without any dedicated sensors in the network.

This analytical model uses the Neyman-Pearson test to detect the PUEAs in CRNs. The main idea in this approach is based on obtaining the PDFs of the received signals and then these PDFs are compared with a predefined threshold to measure some performance metrics such as the probability of a successful PUEA (False Alarm) and

the probability of missed detection. The results show that these performance metrics are greatly influenced by the network area where the SU is surrounded by malicious users and there is a range of network radius in which the PUEAs are most successful. Also, increasing the number of malicious nodes in the system has a negative impact on the network performance because it increases the false alarm probability.

✓ Trust Management Mechanism for the Detection of PUEAs based on the Localization and History of the Signal Source

In order to detect the PUEA, the location of the signal source can be examined, i.e. whether the sensed received signal is coming from a known legitimate PU or whether it is from a PU emulator. Two trust-management mechanisms are proposed. Firstly, there is the mechanism that takes advantage of the fact that it is unlikely for the malicious user to mimic both the coordinates and the power level of the PU; this mechanism is called the direct trust mechanism because it obtains the users trust values based on the Localization of the signal source only. Thus the trustworthiness of the user in this case is obtained by the distances measured using the coordinates and the received signal power level.

On the other hand, the indirect trust mechanism combines the direct trust and the historical trust to obtain the trustworthiness of the users. Simulation results have shown that, based on both techniques, the trustworthiness of the PU is also much higher than the malicious user. Moreover, the indirect scheme improves the users' trustworthiness as it considers the historical behaviour of the user.

✓ Trust and Punishment based Approaches for Secure CSS:

To improve spectrum utilisation, detection performance and the efficiency of spectrum usage, a CSS scheme is proposed based on trust and punishment approaches for secure access in the CRN.

The FC in the presented trust approach makes the final decision about the presence of the PU based on the local sensing result and the trust values of the users, while the punishment approach does not depend on the trust values only but uses a punishment procedure to reduce the effect of the SUs with a low trust value on the final decision.

These approaches are verified via simulation under different numbers of malicious users in the CRN. The results proved that the proposed schemes outperform the traditional majority scheme despite a high number of malicious users. Also the dedicated punishment approaches that punish only the malicious users outperform the other approaches because it can make a correct decision with more tolerance to malicious users.

7.2 Work Limitations

- In Chapter 4, considering in the scenario where all the users (SUs and malicious users) are presented in a circular area, this assumption enables us to calculate the area where the users are distributed, but in practical terms the users can be presented randomly in any form rather than a circular form.

- There are some possible states that can exist in a CR environment, e.g. SU, PU, PUEA, PU + Noise, PUEA + Noise or PU + PUEA + Noise ....etc. In reality, any combination of the states can exist together but because in this thesis the NPCHT is used to investigate the impact of a PUEA, this test is only able to

distinguish between two hypotheses, i.e. H_1: the signal is from the PU, or H_2: the signal is from the attacker.

- In Chapter 5, it is assumed that each user sends its location coordinates so the distance between the users can be calculated. But actually some users cannot broadcast their location coordinates, for example for privacy reasons.

- Another limitation of this work is that the proposed methods in Chapter 6 assume that all the malicious users have the same trust value and all the good SUs have the same trust value as well. This assumption enables us to determine how the trust value affects the final decision and to clearly compare SUs trust with malicious users trust. However, in practice, the users can have different trust values.

- In order to investigate how the users trusts influence the detection performance with incorrect sensing information from the malicious users, it is assumed that the spectrum is occupied and that the malicious users declare that it is not occupied. But actually the spectrum can be occupied or unoccupied.

Bibliography

1 J. Mitola III, "Cognitive radio," Licentiate thesis, Royal Institute of Technology, Stockholm, Sweden, 1999.

2 FCC, "Facilitating opportunities for flexible, efficient, and reliable spectrum use employing CR technologies," Comments of the National Telecommunications and information Administration on FCC ET Docket No. 03-108, Feb.2005.

3 R. Qingchun and L. Qilian, "Performance analysis of energy detection for cognitive radio wireless networks," in Proc. the 2nd International Conference on Wireless Algorithms, Systems and Applications (WASA '07), pp. 139-146,Chicago, Ill, USA, Aug. 2007.

4 A. Sahai, R. Tandra, S. M. Mishra, and N. Hoven, "Fundamental design tradeoffs in CR systems, " in Proceedings of the first international workshop on Technology and policy for accessing spectrum. ACM, 2006, p. 2.

5 S. Haykin, D. Thomson, and J. Reed, "Spectrum sensing for cognitive radio," Proc. IEEE, vol. 97, no. 5, pp. 849-877, May 2009.

6 Z. Quan, S. Cui, H. Poor, and A. Sayed, "Collaborative Wideband Sensing for Cognitive Radios,'' IEEE Signal Process. Mag., vol. 25,no. 6, pp. 60-73, Nov. 2008.

7 S. Mishra, A. Sahai, and R. Brodersen, "Cooperative Sensing among Cognitive Radios, " in Proc. IEEE ICC, vol. 4, pp. 1658-1663, 2006.

8 P. Kaligineedi, M. Khabbazian, and V. Bhargava, ''Secure Cooperative Sensing Techniques for CR Systems, " in Proc. IEEE ICC, pp. 3406-3410, 2008.

9 S. Haykin, "Cognitive radio: brain-empowered wireless communications," IEEEJ. Selected Areas Commun., vol. 23, no. 2, pp. 201–220, Feb. 2005.

10 B. Wang and K. Liu, "Advances in CR networks: a survey," IEEE Journal of Selected Topics in Signal Processing, vol. 5, pp. 5 –23,Feb. 2011.

11 Federal Communications Commission (FCC), "Spectrum Inventory Table 137 MHz to 100 GHz."

12 Ofcom,"Statement on Cognitive Access to Interleaved Spectrum", July 2009.

13 M. Mehdawi, M. Ammar, N. Riley, K. Paulson, and A. Fanan, "Spectrum Occupancy Survey In Hull-UK For Cognitive Radio Applications: Measurement & Analysis," International Journal of Scientific & Technology Research, Volume 2, Issue 4, April 2013, issn 2277-8616 231 www.ijstr.org

14 D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in 38th Asilomar Conference on Signals, Systems and Computers, vol. 1, pp. 772 –776, Nov. 2004.

15 G. Taricco, "Optimization of linear CSS for cognitive radio networks," IEEE J. Sel. Topics Signal Process., vol. 5, no. 1, pp. 77–86,Feb. 2011.

16 I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty,"A survey on spectrum management in CR networks," Communications Magazine, IEEE, vol. 46, no. 4, pp. 40-48, 2008.

17 S. Chaudhari, "Spectrum Sensing for Cognitive Radios: Algorithms, Performance, and Limitations," Aalto University publication series, Doctoral Dissertations, ISBN 978-952-60-4831-4, 135/2012.

18 E. Arun, V. Reena, and Harisree, "Relay Based Cooperation for CR Networks", International Journal of Signal System Control and Engineering Application, 2011, Volume: 4, Issue: 1, Page No. 1-9.

19 P. Yadav, S. Chatterjee, and P. Bhattacharya, "A survey on Dynamic Spectrum Access Technique in CR," International Journal of Next-Generation Networks (IJNGN) Vol.4, No.4, Dec. 2012.

20 R. Adriano, A. Souza, D. Guimarães,"Simulation Platform for Performance Analysis of Cooperative Spectrum Sensing with a Realistic Receiver Model Under Impulsive Noise", DOI: 10.5772/55432 2013.

21 T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for CR applications," IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, 116-130, First Quarter 2009.

22 D. Cabric, A. Tkachenko, and R. Brodersen, "Experimental study of spectrum sensing based on energy detection and network cooperation," in ACM 1st International Workshop on Technology and Policy for Accessing Spectrum (TAPAS), Aug. 2006.

23 F. Digham, M. Alouini, and M. Simon, "On the energy detection of unknown signals over fading channels," in IEEE International Conference on Communications (ICC), pp. 3575–3579, May 2003.

24 I. Gruber, O. Knauf and H. Li, "Performance of Ad Hoc Routing Protocols in Urban Environments", In Proceedings of European Wireless 2004 (EW'2004, Barcelona, Spain, February 24 - 27, 2004.

25 A. Schmitz, and M. Wenig, "The Effect of the Radio Wave Propagation Model in Mobile Ad Hoc Networks," Torremolinos, Malaga, Spain, MSWiM'06, October 2-6, 2006

26 M. Torlak, "Path Loss," EE4367 Telecom, Switching & Transmission.

27 T. Rappaport, "Wireless Communications: Principle and Practice," Prentice Hall Inc., New Jersey, 1996.

28 K. Letaief, and W. Zhang, "Cooperative communications for cognitive radio networks," Proceedings of the IEEE, 97 (5) (2009) 878–893.

29 A. Toleda, and X. Wang, "Robust detection of Selfish misbehaviour in Wireless networks, "IEEE Journal on Selected Areas in Communication, vol.25, pp.1124-1134, August 2007.

30 J. Seybold, "introduction to RF propagation," John Wiley & Sons, 2005.

31 D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios, " in: Proc. of Asilomar Conf. on Signals, Systems, and Computers, vol. 1, pp. 772–776, 2004.

32 S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in: Proc. of IEEE ICC, vol. 4,pp. 1658–1663, 2006.

33 C. Guo, T. Zhang, Z. Zeng, and C. Feng, "Investigation on spectrum sharing technology based on cognitive radio," in: Proc. IEEE Int. Conf. on Communications and Networking in China, Beijing, China, pp. 1–5, Oct. 2006.

34 E. Visotsky, S. Kuffner, and R. Peterson, "collaborative detection of TV transmissions in support of dynamic spectrum sharing," in: Proc. of IEEE DySPAN 2005, pp. 338–345, 2005.

35 Z. Li, F. Yu, and M. Huang, "A CSS consensus scheme in cognitive radios," in: Proc. of IEEE Infocom 2009, 2009, pp. 2546–2550.

36 G. Padmavathi and S. Shanmugavel, "Performance Analysis of Centralized CSS Technique for CR Networks," Asian Journal of Scientific Research, 7: 536-545.

37 G. Ganesan, Y. Li, "CSS in cognitive radio - part I: two user networks," IEEE Transactions on Wireless Communications 6 (6) (2007) 2204–2213.

38 W. Zhang and K. B. Letaief, "Cooperative communications for CR networks," Proceedings of the IEEE, vol. 97, pp. 878–893, May 2009.

39 H. Ekram and B. K, "Cognitive Wireless Communications Networks," Springer Publication, 2007.

40 A. Ghasemi and E. Sousa, "Opportunistic spectrum access in fading channels through collaborative sensing," Journal of Communications, vol. 2, no. 2, p. 71,2007

41 A. Ghasemi and E. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments," DySPANn 2005, pages 131– 136, Nov. 2005.

42 E. Peh, and Y. Liang, "Optimization for Cooperative Sensing in Cognitive Radio Networks," WCNC 11-15, Pages: 27-32, March 2007.

43 W. Zhang, R. K. Mallik, and K. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks", IEEE Trans. on Wireless Comm., vol. 8, no. 8, pp. 5761-5766, December 2009.

44 M. Simon and M. Alouini, "Digital communication over fading channels," John Wiley & Sons, Inc., 2 ed., Dec. 2004.

45 F. Digham, M. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," in Proceedings of IEEE International Conference on Communications (ICC 2003), pp. 3575–3579, May 2003.

46 K. Zeng, P. Pezak, and D. Cabri, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," IEEE Communications Letters, vol.14, no.3, pp.26-228, 2010.

47 G. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," IEEE Communications Surveys and Tutorials, Vol. 15, No. 1, 2013, pp. 428-445.

48 "Radio Networks," in Proc. 45th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, 2011, pp. 1-6.

49 W. Wang, S. Bhattacharjee, M. Chatterjee, and K. Kwiat, "Collaborative jamming and collaborative defence in cognitive radio networks," Pervasive and Mobile Computing, 2012.

50 G. Mao, and L. Zhu, "An investigation on security of cognitive radio networks," in Proc. International Conference on Management and Service Science (MASS), Wuhan, 2011, pp. 1-4.

51 G. A. Safdar, and M. O'Neill, "Common Control Channel Security Framework for CR Networks," in Proc. IEEE 69th Conference on Vehicular Technology, Barcelona, 2009, pp. 1-5.

52 Z. Chen, T. Cooklev, C. Chen, and C. Raez, "Modelling primary user emulation attacks and defences in CR networks," in IEEE International Performance Computing and Communications Conference (IPCCC), Dec. 2009, pp. 208–215.

53 H. Li and H. Zhu, "Dogfight in spectrum: Jamming and anti-jamming in multi channel CR systems," in IEEE Global Telecommunications Conference (GLOBECOM), Dec. 2009, pp. 1–6.

54 "Blind dogfight in spectrum: combating PU emulation attacks in cognitive radio systems with unknown channel statistics," in IEEE International Conference on Communications (ICC), May. 2010, pp. 1–6.

55 J. Ma, G. Zhao, and Y. Li, "Soft combination and detection for CSS in CR networks," IEEE Trans. on Wireless Communications, vol. 7, no. 11, pp. 4502-4507, 2008.

56 W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks," Department of Electrical, Computer and Biomedical Engineering communications database (2009).

57 T. Qin, H. Yu, C. Leung, "Towards a trust-aware cognitive radio architecture," ACM SIGMOBILE Mobile Computing and Communications Review," vol.13, no.2, PP.86-95, 2009.

58 H. Zimmermann, "OSI reference model - the ISO model of architecture for Open Systems Interconnection," IEEE Transactions on Communications, 28(4):425–432, 1980.

59 G. Vinton, and E. Cain, "The DoD Internet Architecture Model," Computer Networks, 7 (1983), North-Holland, pp. 307-318.

60 H. Wang, L. Lightfoot, and Li T, "PHY-layer security of cognitive radio: collaborative sensing under malicious attacks, "44th Annual Conference on Information Sciences and Systems (CISS); 2010 Mar 217–19; Princeton, NJ. IEEE. p. 66–73.

61 O. León, J. Hernández-Serrano and M. Soriano, "Securing CR Networks, "International Journal of Communication Systems, Vol.23, No.5, 2010, pp.633-652.

62 C. Mathur and P. Subbalakshmi, "Digital signatures for centralized DSA networks," in Proc. 1st IEEE Workshop on Cognitive Radio Networks, 2007, pp. 1037–1041

63 L.Huang, L. Xie, H. Yu, W. Wang, and Y. Yao, "Anti-PUE Attack Based on Joint Position Verification in CR Networks," International Conference on Communications and Mobile Computing (CMC), Vol.2, Shenzhen, China, April, 2010, pp.169-173.

64 C. Zhao, W. Wang, L. Huang and Y. Yao, "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio," 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'09), Beijing, China, September, 2009, pp.1-5.

65 P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious User Detection in a CR Cooperative Sensing System," IEEE Transactions on Wireless Communications, Vol. 9, No. 8, August 2010.

66 T. Aysal, S. Kandeepan, and R. Piesewicz, "Cooperative Spectrum Sensing with Noisy Hard Decision Transmissions," in Proc. ICC, 2009, pp. 1–5.

67 J. Fitton, "Security considerations for software defined radios," in Proc.SDR '02 Technical Conference and Product Exposition, 2002, pp. 1–7.

68 A. Pandharipande, "IEEE P802.22 Wireless RANs," Technology Proposal Package for IEEE 802.22, IEEE 802.22 WG on WRANs, November, 2005.

69 Y. Zhang, G. Xa and X. Creng, "Security threats in CR Networks, In 10th IEEE International Conference on High Performance Computing and Processing," (HPCC 2008) Dalian, China, Sept. 2008, pp.1036-1041.

70 W. Xu, W. Trappe, Y. Zhang and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proceedings of ACM MobiHoc, Urbana, IL, May, 2005, pp.46-57.

71 Q. Yan, M. Li, T. Jiang, W. Lou, and Y. Hou, "Vulnerability and protection for distributed consensus based spectrum sensing in CR networks," 2012 Proceedings IEEE INFOCOM, 2012, pp. 900–908 (IEEE).

72 Y. Reddy, "Security Issues and Threats in Cognitive Radio Networks", The Ninth Advanced International Conference on Telecommunications , AICT 2013.

73 C. Mathur, and K. Subbalakshmi, "Security issues in CR networks," Chapter: Cognitive Networks: Towards Self-Aware Networks, John Wiley & Sons, Ltd, pp. 271–291, October 2007.

74 G. Jakimoski and K. P. Subbalakshmi, "Denial-of-service attacks on DSA networks," IEEE CogNets Workshop, IEEE International Conference on Communications (ICC) 2008, pp. 125-132, May 2008.

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

76 D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in Proceedings of the Thirty-eight Asilomar Conference on Signals, Systems, and Computers, November 2004.

77 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. networks," Cognitive network: Towards Self-Aware Networks, 2007.

78 E. Eskin, "Anomaly detection over noisy data using learned probability distributions," in Proc. Seventeenth International Conference on Machine Learning, pp. 255–262, July 2000.

79 C. Palamidessi, "Inference of probability distributions for trust and security applications." Available: http://www.ecs.soton.ac.uk/people/vs/publications, Oct 2008.

80 R. Narasimhan and C. Cox, "Estimation of mobile speed and average received power in wireless systems using best basis methods," IEEE Trans. Commun., pp. 2172–2183, Dec 2001.

81 D. Pu, A. Wyglinski, K. Pahlavan, and W. Wang , "Primary User Emulation Detection in Cognitive Radio Networks," PhD thesis, Department of Electrical & Computer Engineering, Worcester Polytechnic Institute, Worcester, Massachusetts, USA , April 2013

82 A. Sharifi, and J. Niya, " Robust Cooperative Spectrum Sensing under Primary User Emulation Attack in Cognitive Radio Networks," Journal of Computing and Security, Volume 2, Number 2, pp. 109{117), April 2015, ISSN: 2322-4460 http://www.jcomsec.org

83 M. Dang, Z. Zhao and H. Zhang, "Optimal Cooperative Detection of Primary User Emulation Attacks in Distributed Cognitive Radio Network," 2013 8th International Conference on Communications and Networking in China (CHINACOM), 978-1-4799-1406-7 © 2013 IEEE

84 M. Vu, N. Devroye, M. Sharif, and V. Tarokh, "Scaling laws of cognitive networks," Submitted to IEEE Journal on Selected Topics in Signal Processing.

85 W. Ghanem, M. Shokair, and M. Dessouky, "Defense Against Selfish PUEA in Cognitive Radio Networks Based on Hash Message Authentication Code," International Journal of Electronics and Information Engineering, Vol.4, No.1, pp. 12-21, Mar. 2016

86 W. Ghanem, M. Shokair and M. Dessouky, "Investigation of PUEA in Cognitive Radio Networks Using Energy Detection in Different Channel Model," Circuits and Systems: An International Journal (CSIJ), Vol.2, No.2/3/4, October 2015.

87 K. Mergu, B. Alebachew, and A. Metaferia, "An Improved Spectrum Sensing Technique using Matched Filter Detection with a NP Observer" , IJECT, Vol. 7, Issue 2, ISSN : 2230-7109, April - June 2016.

88 S. Parvin, S. Han, B. Tian, F. Hussain, "Trust-Based Authentication for Secure Communication in Cognitive Radio Networks," 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.

89 K. Chen, N. Prasad, Y. Liang, and S. Sun, "Cognitive radio network architecture: part II- trusted network layer structure," in Conference On Ubiquitous Information Management And Communication 2008, ACM: Suwon, Korea p. 120-124.

90 Y. Yu, L. Hu, H. Li, Y. Zhang, F. Wu, and J. Chu, "The Security of Physical Layer in Cognitive Radio Networks", Journal of Communications Vol. 9, No. 12, December 2014.

91 S. Wenguil, and L. Yang, "A Jury-Based Trust Management Mechanism in Distributed Cognitive Radio Networks," China Communications, Security Schemes And Solutions, July 2015.

92 W. Zhendong, W. Huiqiang and Z. Qiang, "A Trust Game Model and Algorithm for Cooperative Spectrum Sensing in Cognitive Radio Networks," International Journal of Future Generation Communication and Networking Vol. 8, No. 3 (2015), pp. 1-14 http://dx.doi.org/10.14257/ijfgcn.2015.8.3.01.

93 S. Jana, K. Zeng and P. Mohapatra, "Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks ", IEEE Transactions on Information Forensics and Security (Volume: 8, Issue: 9, Sept. 2013).

94 L. Fangwei, L. Fan, Z. Jiang, and N. Yifang, "Reputation based secure spectrum situation fusion in distributed cognitive radio networks," The Journal of China Universities of Posts and Telecommunications, vol. 22, no. 3, pp. 110–117, 2015.

95 K. Zeng, P. Pawełczak, and D. Cabric, "Reputation-Based Cooperative Spectrum Sensing with Trusted Nodes Assistance," IEEE Communications Letters, Vol. 14, No. 3, March 2010.

96 A. Rauniyar, D. Jeong, G. Chand, S. Shin, "Performance Analysis of Cascaded Energy and Matched Filter Detector With Malicious Users in CR Networks", 2015 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS) November 9-12, 2015.

97 S. Kyperountas, N. Correal, and Q Shi, "A Comparison of Fusion Rules for Cooperative Spectrum Sensing in Fading Channels," EMS Research, Motorola.

98 W. Wang, L. Chen, K. Shin and L. Duan, "Secure Cooperative Spectrum Sensing and Access Against Intelligent Malicious Behaviors," IEEE infocom 2014, 978-1-4799-3360-0/14.

99 L. Duan, A. Min, J. Huang, and K.G. Shin, "Attack Prevention for Collaborative Spectrum Sensing in CR Networks," IEEE J. Sel. Areas Commun., vol. 30, no. 9, pp. 1658–1665, Oct. 2012.

100 D. Pang, G.Hu and M. Xu, "Trust Model-based Secure Cooperative Sensing Techniques for Cognitive Radio Networks," The Tenth International Conference on Networks, ICN 2011.

Appendices

Appendix A – Matlab code for Mitigating Attacks in CR based on an Analytical Model

1 PDF of the received power due to the primary transmitter

```
% calculation the recieved power in order to calculate the PDFs , from
% Primary
 clc;    clear all;  close all;
 power_t = 120e3; % the Primary  power
power_m = 5;    % the power of malicious users
 distance_p = 120e3; % the distance between primary transmitter and
secondary user
format long;
rad1 =500;   %out circle radii
rad2 = 40;%  inside circle radii
sigma_p = 8;  % segma P
sigma_m = 5.5;  %  Segma M
mal = 15; %%%%  number of malicious users
A = log(10)/10;
smaples  = 100000;
E_p =  sigma_p*randn(1,smaples );
Gp = 10.^(E_p/10);
 Rec_power = power_t*Gp*distance_p^(-2); %r. v. received power
sort_power = sort(Rec_power);
 mu_p = 10*log10(power_t) - 20*log10(distance_p);
mu_p_2 = (10^(mu_p/10))^2;

pdf =(1./(A*sort_power*sigma_p*sqrt(2*pi))).*exp(-((10 *log10
(sort_power)-mu_p)/(sqrt(2)*sigma_p)).^2);  % pdf from primary

[reg1,reg2] = hist(Rec_power,4000);
bar(reg2,reg1/trapz(reg2,reg1));
axis([0 1e-4 0 max(pdf) ]);
grid on, hold on;
xlabel('Received power at the secondary receiver from primary
transmitter')
ylabel('PDF of received power')
plot(sort_power,pdf,...
     'linewidth',2,...
    'color','g')
axis([0 1e-4 0 max(pdf)])
legend('PDF of received power using simulation', 'PDF of received
power theoretically' )
```

2 PDF of the received power due to the malicious users

```
% calculation the recieved power in order to calculate the PDFs , from
% malicious users
```

```
clear all;
close all;
clc;
samples  = 100000;
%grid minor
power_t = 120e3; % the Primary  power
power_m = 5;    % the power of malicious users
distance_p = 120e3; % the distance between primary transmitter and
secondary user
Mal = 15; %%%% number of malicious users
A = log(10)/10;
%%%% calculation of the random Points within circle with radius rad1 &
radius rad2
xCoordinates = [];
yCoordinates = [];
n = Mal;
format long;
rad1 =500;  %out circle radii
rad2 = 40;%  inside circle radii
sigma_p = 8;  % segma P
sigma_m = 5.5;  %  Segma Mal
 %internal circle
      while n > 0
          x = unifrnd(-rad1,rad1,1,1);
        y = unifrnd(-rad1,rad1,1,1);
          no = sqrt((x.^2) + (y.^2));
        level= find((rad2 <= no) & (no <= rad1));
          xCoordinates = [xCoordinates; x(level)];
        yCoordinates = [yCoordinates; y(level)];
                  n = Mal - numel(xCoordinates);
    end

% calculation of the distance between jth malicious user and secondary
user %%%%%%%
for i= 1 : Mal % number of malicious users
        d(i)=sqrt((xCoordinates(i))^2 + (yCoordinates(i))^2);
end
 %  ther received power at secondary user from malicious users %
 for kk = 1:samples
E_j= sigma_m*randn(Mal,1);
G = 10.^(E_j/10);
for j = 1:Mal
    P(j) = power_m*(d(j)^(-4))*G(j);
end
   sort_power2(kk)= sum(P);
end
  rec_power2 = sort(sort_power2);
[reg1,reg2] = hist(sort_power2,4000);
figure(2)
bar(reg2,reg1/trapz(reg2,reg1));
axis([0 max(reg2) 0 max(reg1/trapz(reg2,reg1))])
grid on; hold on;
 sigma_x_2 = (1/A^2)*(log(mean(rec_power2.^2)) -
2*log(mean(rec_power2)));
mu_x = (1/A)*(2*log(mean(rec_power2)) - 0.5*log(mean(rec_power2.^2)));
 pdf2 = (1./(A*rec_power2*sqrt(sigma_x_2)*sqrt(2*pi))).*exp(-
((10*log10(rec_power2)-mu_x)).^2/(2*sigma_x_2)); % pdf from malicious
 plot(rec_power2, pdf2,...
```

```
    'linewidth',2,...
    'color','g')
     xlabel('Received power at the secondary receiver from malicious
users: ')
ylabel('PDF of received power')% axis([0 max(Pr_m) 0 max(P_m_gama)])
legend('PDF of received power using simulation', 'PDF of received
power theoretically' )
```

3 Probability of a successful PUEA (false alarm) , Probability of missed detection and CDF

```
% probability of miss detection , false alarm and CDF

clc ; clear all;  close all;

samples= 100000;   % samples  = 100000;

mal = 5; %%%% number of malicious users
rad1 =500;  %out circle radii
rad2 = 40;%  inside circle radii
sigma_p = 8;   % segma P
sigma_m = 5.5;   %  Segma Mal
power_t = 120e3; % the Primary  power
power_m = 5;    % the power of malicious users
distance_p  =  120e3;  %%%%% distance  between  primary  transmitter  and
secondary user
A = log(10)/10;
x0 = 1e-9:1e-9:1e-3; %all x axis variables
sigma_p_2= (10^(sigma_p/10))^2;
sigma_m_2= (10^(sigma_m/10))^2;

%%%% Random Points within circle with radius rad1 & radius rad2
false_alarm=[];
Miss_detection=[];
  xCoordinates = [];
yCoordinates = [];
n = mal;
    while n > 0
          x = unifrnd(-rad1,rad1,1,1);
        y = unifrnd(-rad1,rad1,1,1);

        no = sqrt((x.^2) + (y.^2));
        level = find((rad2 <= no) & (no <= rad1));

        xCoordinates = [xCoordinates; x(level)];
        yCoordinates = [yCoordinates; y(level)];

          n = mal - numel(xCoordinates);
    end
% finding The distance between  malicious user j and secondary user %
for i= 1 : mal % number of malicious users
    d(i)=sqrt((xCoordinates(i))^2 + (yCoordinates(i))^2);
end

NumberofRuns=40;
for J=1:1:NumberofRuns
```

```
    E_p =  sigma_p*randn(1,samples); %E_p dB in lognormal distribution
Gp = 10.^(E_p/10);
Pr_p_tmp = power_t*Gp*distance_p^(-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(power_t) - 20*log10(distance_p);
%calculation=mean(Pr_p) in db =mean_Pr_p
mu_p_2 = (10^(mu_p/10))^2;
Pdf = (1./(A*x0*sigma_p*sqrt(2*pi))).*exp(-((10*log10(x0)-
mu_p)/(sqrt(2)*sigma_p)).^2);
for kk = 1:samples
E_j= sigma_m*randn(mal,1);
G = 10.^(E_j/10);
    P = power_m*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./Pdf;
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,Pdf(1:index));
Miss_detection=[Miss_detection;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)));

false_alarm =[false_alarm; P_D1_H2_tmp];

 % close all
end;
  % plot of prbabilities
false_alarm1=(false_alarm);
miss_detection2=(Miss_detection);

N=40;
bar(miss_detection2,'FaceColor',[0 .2 .4],'EdgeColor',[0 .2 .2],
'LineWidth',.1);set(gca,'XTick', [0:N]);
grid;
xlabel('Number of simulation times ') ;
ylabel('Probability of Miss detection ') ;

hold , figure ,
bar(false_alarm1,'FaceColor',[0 .8 .6],'EdgeColor',[0 .5.5],
'LineWidth',1);set(gca,'XTick', [0:N]);
grid;
xlabel('Number of simulation times ') ;
```

```
ylabel('Probability of False alarm') ;
%cc=mean(false_alarm1)
ccc=sort(false_alarm1) ; vvv=sort(miss_detection2) ;
 figure ;
plot(ccc, (0:1/N:1-1/N), 'r', vvv, (0:1/N:1-1/N),'k');

grid
xlabel('Probabilities of false alarm and miss detection')
ylabel('CDF')
legend('Probability of False Alarm','Probability of Miss Detection');
```

4 Plot of simulation model for malicious users distributed randomly around the SU located at coordinate (0, 0)

```
plot(xCoordinates,yCoordinates,'*'); hold on ; ;grid ,plot(0,0,'^ r')
x=0;y=0;r=40;
hold on
th = 0:pi/50:2*pi;
xunit = r * cos(th) + x;
yunit = r * sin(th) + y;
legend('Malicious users' ,'Secondary user');
h = plot(xunit, yunit);
hold off
x=0;y=0;r=500;
hold on
th = 0:pi/50:2*pi;
xunit = r * cos(th) + x;
yunit = r * sin(th) + y;
h = plot(xunit, yunit);
xlabel('X-coordinate of secondary and malicious users location (m)')
ylabel('Y-coordinate of secondary and malicious users location (m)')
hold off
```

Appendix B – Matlab code for Trust Management Mechanisms for the Detection of a PUEA

1 Trustworthiness of the PU

```
close all; clear all
history=[0.5]; % assumed history of the user %
RC=60; % number of random coordinates
% Area of the cognitive network a , b
a = 0;
b = 15;
%   coordinates of the cognitve user
 x_cognitive= (b-a).*rand(RC,1) + a ;
 y_cognitive= (b-a).*rand(RC,1) + a ;
%   coordinates of the Primary user user
 x_primary= (b-a).*rand(RC,1) + a ;
 y_primary= (b-a).*rand(RC,1) + a ;
%   coordinates of the malicious user user
 x_malicious= (b-a).*rand(RC,1) + a ;
 y_malicious= (b-a).*rand(RC,1) + a ;
```

```
  trustworthiness2prim=[];
  checkhistory2=[];
    checkhistory2bad={};
    powerSamples=10000 ;
  allSNR=-5:5:25; % SNR in decibel
trustworthiness2=[];

for repetition = 1:RC
    % repetition
    x = x_cognitive(repetition);
    y = y_cognitive(repetition );
    x1 = x_primary(repetition);
    y1 = y_primary(repetition);
    x2 = x_malicious(repetition);
    y2 = y_malicious(repetition);

      % cognitive radio distance  from the primary user
     coo_distance=sqrt((x-x1).^2+(y-y1).^2);
      dco(repetition)=coo_distance;

    % cognitive radio distance  from the malicious user
     actual_distance=sqrt((x-x2).^2+(y-y2).^2) ;
     dact(repetition)=actual_distance;
    trust_calculation = zeros(1,length(allSNR));

    for ii=1:length(allSNR)
                  power_transmitted=500;     % transmitted power
without noise
        SNR_dB=allSNR(ii); % SNR in dB
        SNR = 10.^(SNR_dB/10);   % real value of SNR
noise_power = power_transmitted/(SNR);
noise_signal=sqrt(noise_power) * randn(1,powerSamples);    % Gaussian
Noise assumed


        tx_signal = sqrt(power_transmitted) ;    % transmitted signal
        rx_signal =  tx_signal + noise_signal;   % received signal
    prim_rx_signal_power= ((rx_signal).^2)/(coo_distance^4);
 % calculation of actual received signal power over actual distance dl
    d_power_prim=(power_transmitted./prim_rx_signal_power).^(1/4);
 % the calculated distance based on received signal power
    trust_repetitionprim = min(coo_distance./d_power_prim,
d_power_prim./coo_distance);    % calculation of trustworthness

 fff(ii)=mean(d_power_prim);
     ppp(ii)=mean(prim_rx_signal_power);
    ppp_db(ii)=10*log(ppp(ii));
       ggg(repetition)=mean(fff);
       zzz(repetition)=mean(ppp_db);
    trustworthinessprim(ii)=mean(trust_repetitionprim);

    checkhistory(ii)=trustworthinessprim(ii);

checkhistory(ii)=.92*trustworthinessprim(ii)+.08*mean(history);
    end
   trustworthiness2prim=[trustworthiness2prim; trustworthinessprim];
```

```
   checkhistory2bad=[checkhistory2bad;checkhistory];
end


%  primary trust plots
nnn=bar(allSNR,mean(trustworthiness2prim),.5,'FaceColor',[0 0.2 0.1])
;
hold on
mmm=bar(allSNR,mean(checkhistory2bad),.3,'FaceColor',[0 0.7 0.7]) ;
 grid minor
l = cell(1,1);
l{1}='Direct trust'; l{2}='Indirect trust';
yh=legend([nnn mmm], l,'Location', [0.35 0.85 0.15
0.05],'Orientation','horizontal','FontWeight','bold');
set(yh, 'FontSize',12);

annotation('textbox',...
    [0.15 0.65 0.3 0.15],...
    'String',{'T_H=',num2str(history,'%.2f')},...
     'FitBoxToText','On',...
     'FontSize',11,...
    'FontName','Arial',...
    'LineStyle','--',...
    'EdgeColor',[1 1 0],...
    'LineWidth',1,...
    'BackgroundColor',[0.9  0.9 0.9],...
    'Color',[0.84 0.16 0])
xlabel ('Signal to Noise Ratio(dB)');
ylabel ('User trustworthiness');
axis([min(allSNR) max(allSNR) 0.5 1]);
```

2 Trustworthiness of the malicious users

```
close all;  clear all ;
malhistory=[0.8]; % assumed history of the malicious users
RC=60;  % number of random coordinates
% Area of the cognitive network a , b
a = 0;
b = 15;
%   coordinates of the cognitve user
 x_cognitive= (b-a).*rand(RC,1) + a ;
 y_cognitive= (b-a).*rand(RC,1) + a ;

  %   coordinates of the Primary user user
 x_primary= (b-a).*rand(RC,1) + a ;
 y_primary= (b-a).*rand(RC,1) + a ;

  %   coordinates of the malicious user user
 x_malicious= (b-a).*rand(RC,1) + a ;
 y_malicious= (b-a).*rand(RC,1) + a ;
  powerSamples=100000 ;
  mal_trustworthiness=[];
trustworthiness2malhis=[];
trustworthiness2mal=[];
  allSNR=-5:5:25;  % SNR in decibel
```

```
for  repetition = 1:RC      %
    x = x_cognitive(repetition);
    y = y_cognitive(repetition );
    x1 = x_primary(repetition);
    y1 = y_primary(repetition);
    x2 = x_malicious(repetition);
    y2 = y_malicious(repetition);
      % distance of the cognitive radio from the primary user
     coo_distance=sqrt((x-x1).^2+(y-y1).^2);
      dco(repetition)=coo_distance;

    % distance of the cognitive radio from the malicious user
     actual_distance=sqrt((x-x2).^2+(y-y2).^2) ;
     dact(repetition)=actual_distance;
    trustworthiness = zeros(1,length(allSNR));

    for ii=1:length(allSNR)
         SNR_dB=allSNR(ii); % SNR in dB
        power_transmitted=500;     %  transmit power without noise
        SNR = 10.^(SNR_dB/10);  % SNR in real value
       %  power_transmitted_prim=8;
        noise_power = power_transmitted/(SNR);
% noise_power_prim = power_transmitted_prim/(SNR);
        noise_signal=sqrt(noise_power) * randn(1, powerSamples);
% assume Gaussian Noise
        tx_signal = sqrt(power_transmitted) ;    % transmitted signal
        rx_signal =  tx_signal + noise_signal;  % received signal

        rx_signal_power= ((rx_signal).^2)/(actual_distance^4);
% actual received signal power over actual distance d1

        d_power_mal=(power_transmitted./rx_signal_power).^(1/4);
 % calculated distance based on received signal power

        trust_repetition = min(coo_distance./d_power_mal,
d_power_mal./coo_distance);    % trustworthness based on power
        mal_trustworthiness(ii)=mean(trust_repetition);
      ff(ii)=mean(d_power_mal);
    pp(ii)=mean(rx_signal_power);
     pp_db(ii)=10*log10(pp(ii));
    gg(repetition)=mean(ff);
maliciushis(ii)=.92*mal_trustworthiness(ii)+.08*mean(malhistory);

    end
       trustworthiness2mal=[trustworthiness2mal; mal_trustworthiness];
      trustworthiness2malhis=[trustworthiness2malhis; maliciushis];
      zz(repetition)=mean(pp_db);
      gg(repetition)=mean(ff);
end

xx=bar(allSNR,mean(trustworthiness2mal),.5,'FaceColor',[1 0.3 0.1]) ;
hold on

ss=bar(allSNR,mean(trustworthiness2malhis),.3,'FaceColor',[0 1 1]) ;
l = cell(1,1);
```

```
l{1}='Direct trust'; l{2}='Indirect trust';
yh=legend([xx ss], l,'Location', [0.35 0.85 0.15
0.05],'Orientation','horizontal','FontWeight','bold');
set(yh, 'FontSize',12);
grid minor
annotation('textbox',...
    [0.15 0.65 0.3 0.15],...
    'String',{'T_H=',num2str(malhistory,'%.2f')},...
     'FitBoxToText','on',...
     'FontSize',11,...
    'FontName','Arial',...
    'LineStyle','--',...
    'EdgeColor',[1 1 0],...
    'LineWidth',1,...
    'BackgroundColor',[0.9  0.9 0.9],...
    'Color',[0.84 0.16 0])
xlabel ('Signal to Noise Ratio(dB)');
ylabel ('User trustworthiness');
axis([min(allSNR) max(allSNR) 0.5 1]);
```

3 Distances plot of the PU from the SU measured based on the coordinates and received power level

```
clc
iteration=RC ;
grid minor
for kk=1:iteration
     hold on
     plot(dco(kk),zzz(kk),'or')

   plot(ggg(kk),zzz(kk),'+g')

xlabel ('Distance');
ylabel ('Received Signal Power (in dB)');
legend('Distance measured based on coordenates', 'Distance measured
based on received power level');

end
```

4 Plot of random location of primary, secondary and malicious users in an area of 15Km*15Km

```
width = 3;      % Width in inches
height = 3;     % Height in inches
alw = 0.75;     % AxesLineWidth
fsz = 11;       % Fontsize
lw = 1.5;       % LineWidth
msz = 15;        % MarkerSize
plot(x_cognitive(10),y_cognitive(10),'*r','LineWidth',lw,'MarkerSize',
msz);
hold on
plot(x_primary(10),y_primary(10),'g*','LineWidth',lw,'MarkerSize',msz)
hold on
grid minor
```

```
plot(x_malicious(l0),y_malicious(l0),'b*','LineWidth',lw,'MarkerSize',
msz);
hold on
xlabel('X-coordinate (Km)')
ylabel('Y-coordinate (Km)')
hold off
```

Appendix C – Matlab code for Trust and Punishment based Approaches for Secure Cooperative Spectrum Sensing

1 Trust based CSS Approach

```
clc;
clear all;
close all;
% u , Assumed Users trusts
% The values of u and the number of values inside u (size of u) are
changeable as desired
% the number of users ( size of u) can be changed as we desire for the
simulation
 u=[.3  .3  .3  .8 .8 .8 .8 .3 .8 .3 .8 .3 .8 .3 .8 .3 .8 .3 .3 .3 .8
.3 .3 .3 .8 .3 .3 .3 .8 .3 .8 .3  .3  .3  .3  .8 .8 .8 .8 .8 .3 .3
.3  .3  .3  .3 .3]
% Users count
trust=0;
  untrust=0;
  for  zzz=1 : length(u)
      if u(zzz)>=.5
          trust=trust+1;
          Trustworthy= u(zzz);
      else
          untrust=untrust+1;
          Untrustworthy = u(zzz);
      end

  end
occupied = 1;
not_occupied = -1;
  N= trust;
N2= untrust;
n=1
    Trust_users = 1:N;
Malicious_users = 1:N2;
detection=[] ;
detection2=[];
tipping_point2=[];
for jj=1:N2
     tipping_point=[];
    for ii=1:1:N ;
          detection= (Trustworthy.^n)*Trust_users(ii) * occupied
+(Untrustworthy.^n).*Malicious_users * not_occupied;
       % end
          false_decision = find([detection<0]);
        tipping_point = [tipping_point false_decision(1)];
```

```
        detection2=[detection2; detection];
    end
   tipping_point2=[tipping_point2; tipping_point];
    N  ; N2;
   end
 totalusers=0;
  for yyy=1:N
     totalusers(yyy)=yyy+tipping_point2(1,yyy);
  end
figure(1);
h=bar(totalusers,tipping_point2(1,:),.6,'g');
l{1}='Range of Correct Sense'; l{2}='made by G out of M
users';l{3}='OKOKOK';
lgnd =
legend(h,l,'Orientation','vertical','edgecolor','none','FontSize',9);
set(lgnd,'color','none');
set(gca,'XTick',totalusers); % Change x-axis ticks
set(gca,'XTickLabel',totalusers); % Change x-axis ticks labels to
desired values
%yyyyyyyy

dim = [.635 .555 .3 .3];
str = l{2};
annotation('textbox',dim,'String',str,'FitBoxToText','on','edgecolor',
'none','FontSize',9)
set(gca,'YTick',tipping_point2(1,:)); % Change x-axis ticks
set(gca,'YTickLabel',tipping_point2(1,:)); % Change x-axis ticks
labels to desired values
ay = gca;
ay.YColor = 'red';
%axis([0 100 0 200])
annotation('textbox',...
    [.19 .62 0.3 0.3],...
        'String',{'T_g=', Trustworthy(1)},...
    'FitBoxToText','on',...
    'VerticalAlignment','top',...
    'FontSize',12,...
    'FontName','Arial',...
    'LineStyle','--',...
    'EdgeColor',[1 1 0],...
    'LineWidth',2,...
    'BackgroundColor','none',...
    'Color',[0.84 0.16 0])
xa = [.25 .32];
ya = [.865 .865];
grid on;
xlabel({['M Total Number of Cognitive Users.'];['T_m='
num2str(Untrustworthy(1))]});
ylabel ('K [Number of malicious users]','FontSize',12);
titletext=['Trust-Based System '];
title(titletext);
```

2 General Punishment based CSS Approach

```
clc;
clear all;
```

```
close all;
% u , Assumed Users trusts
% The values of u and the number of values inside u (size of u) are
changeable as desired
% the number of users ( size of u) can be changed as we desire for the
simulation
 u=[.7 .7 .3  .7 .7 .7 .7 .7 .7 .3  .3  .7  .3  .7 .7 .7 .7 .7 .3 .7
.3 .7 .3 .7 .3 .3 .3 .7 .3 .3 .3 .7 .3 .3 .3 .7 .3 .3 .3 .7 .3 .7 .3  .3  .3  .3
.3  .7 .7 .7 .7 .7 .3 .3]
% Users count
trust=0;
  untrust=0;
  for  zzz=1 : length(u)
      if u(zzz)>=.5
          trust=trust+1;
          Trustworthy= u(zzz);
      else
          untrust=untrust+1;
          Untrustworthy = u(zzz);
      end
  end
occupied = 1;
not_occupied = -1;
  N= trust;
N2= untrust;

p= 1.7% Penalty Factor
    Trust_users = 1:N;
Malicious_users = 1:N2;
detection=[] ;
detection2=[];
tipping_point2=[];
for jj=1:N2
    tipping_point=[];
    for ii=1:1:N ;
 detection= (Trustworthy.^p)*Trust_users(ii) * occupied
+(Untrustworthy.^p).*Malicious_users * not_occupied;
false_decision = find([detection<0]);

 tipping_point = [tipping_point false_decision(1)];
       detection2=[detection2; detection];
    end
   tipping_point2=[tipping_point2; tipping_point];
    N  ; N2;
end
 totalusers=0;
  for yyy=1:N
      totalusers(yyy)=yyy+tipping_point2(1,yyy);
  end
figure(1);
h=bar(totalusers,tipping_point2(1,:),.6,'g');
l{1}='Range of Correct Sense'; l{2}='made by G out of M
users';l{3}='OKOKOK';
lgnd =
legend(h,l,'Orientation','vertical','edgecolor','none','FontSize',9);
set(lgnd,'color','none');

set(gca,'XTick',totalusers); % Change x-axis ticks
```

```
set(gca,'XTickLabel',totalusers); % Change x-axis ticks labels to
desired values
%yyyyyyyy
dim = [.635 .555 .3 .3];
str = 1{2};
annotation('textbox',dim,'String',str,'FitBoxToText','on','edgecolor',
'none','FontSize',9)
set(gca,'YTick',tipping_point2(1,:)); % Change x-axis ticks
set(gca,'YTickLabel',tipping_point2(1,:)); % Change x-axis ticks
labels to desired values
ay = gca;
ay.YColor = 'red';
%axis([0 100 0 200])
 annotation('textbox',...
    [.19 .62 0.3 0.3],...
        'String',{'T_g=', Trustworthy(1)},...
    'FitBoxToText','on',...
    'FontSize',12,...
    'FontName','Arial',...
    'LineStyle','--',...
    'EdgeColor',[1 1 0],...
    'LineWidth',2,...
    'BackgroundColor','none',...
    'Color',[0.84 0.16 0])
xa = [.25 .32];
ya = [.865 .865];
grid on;
xlabel({['M Total Number of Cognitive Users.'];['p='
num2str(p)];['T_m=' num2str(Untrustworthy(1))]});

ylabel ('K [ Number of malicious users]','FontSize',12);
titletext=['General Punishment -Based System '];
title(titletext);
```

3 Dedicated Punishment based CSS Approach

```
clc;
clear all;
close all;
% u , Assumed Users trusts
% The values of u and the number of values inside u (size of u) are
changeable as desired
% the number of users ( size of u) can be changed as we desire for the
simulation
 u=[.7 .7 .7 .7 .3  .3  .3  .3  .7 .7 .7 .7 .7 .3 .7 .3 .7 .3 .7 .3 .3
.3 .7 .3 .3 .3 .7 .3 .3 .3 .7 .3 .7 .3  .3  .3  .3  .3  .7 .7 .7 .7 .7
.3 .3  .3  .3  .3  .3 .3]
% Users count
trust=0;
  untrust=0;
  for  zzz=1 : length(u)
      if u(zzz)>=.5
          trust=trust+1;
          Trustworthy= u(zzz);
      else
          untrust=untrust+1;
          Untrustworthy = u(zzz);
```

```
      end
  end
occupied = 1;
not_occupied = -1;
  N= trust;
N2= untrust;

p=1.7 % Penalty Factor
    Trust_users = 1:N;
Malicious_users = 1:N2;
detection=[] ;
detection2=[];
tipping_point2=[];
for jj=1:N2
    tipping_point=[];
    for ii=1:1:N ;
           detection= (Trustworthy.^1)*Trust_users(ii) * occupied
+(Untrustworthy.^p).*Malicious_users * not_occupied;
       % end
           false_decision = find([detection<0]);
        tipping_point = [tipping_point false_decision(1)];
        detection2=[detection2; detection];
    end
   tipping_point2=[tipping_point2; tipping_point];
    N  ; N2;
end
  for yyy=1:N
     totalusers(yyy)=yyy+tipping_point2(1,yyy);
  end
figure(1);
h=bar(totalusers,tipping_point2(1,:),.6,'g');
l{1}='Range of Correct Sense'; l{2}='made by G out of M
users';l{3}='OKOKOK';
lgnd =
legend(h,l,'Orientation','vertical','edgecolor','none','FontSize',9);
set(lgnd,'color','none');
set(gca,'XTick',totalusers); % Change x-axis ticks
set(gca,'XTickLabel',totalusers); % Change x-axis ticks labels to
desired values
%yyyyyyyy
dim = [.635 .555 .3 .3];
str = l{2};
annotation('textbox',dim,'String',str,'FitBoxToText','on','edgecolor',
'none','FontSize',9)
set(gca,'YTick',tipping_point2(1,:)); % Change x-axis ticks
set(gca,'YTickLabel',tipping_point2(1,:)); % Change x-axis ticks
labels to desired values
ay = gca;
ay.YColor = 'red';
annotation('textbox',...
    [.19 .62 0.3 0.3],...
        'String',{'T_g=', Trustworthy(1)},...
    'FitBoxToText','on',...
    'FontSize',12,...
    'FontName','Arial',...
    'LineStyle','--',...
    'EdgeColor',[1 1 0],...
    'LineWidth',2,...
```

```
    'BackgroundColor','none',...
    'Color',[0.84 0.16 0])
xa = [.25 .32];
ya = [.865 .865];
grid on;
xlabel({['M Total Number of Cognitive Users.'];['p='
num2str(p)];['T_m=' num2str(Untrustworthy(1))]});
ylabel ('K [Maximum Number of malicious users]','FontSize',12);
titletext=['Dedicated Punishment-Based System '];
title(titletext);
```

4 Conventional Majority based Approach

```
clc;
clear all;
close all;
occupied = 1;
not_occupied = -1;
  N=15; % number of good users is varied from 1 to 15
N2=20;  % number of malicious users is varied from 1 up to 20
% N and N2 are changeable as we desire
Trust_users = 1:N;
Malicious_users = 1:N2;
detection =[];
detection2=[];
  tipping_point2=[];
for jj=1:13
    tipping_point=[];
for ii=1:1:N ;
detection = Trust_users(ii) * occupied + Malicious_users *
not_occupied;
        false_decision = find([detection<=0]);
        tipping_point = [tipping_point false_decision(1)];
        detection2=[detection2; detection];
    end
   tipping_point2=[tipping_point2; tipping_point];
    N  ; N2;
   end
 totalusers=0;
  for yyy=1:N
           totalusers(yyy)=yyy+tipping_point2(1,yyy);
  end
  totalusers2=0;
  for yyyy=1:N
      totalusers2(yyyy)=yyyy+tipping_point2(1,yyyy);
  end
figure(1);
h=bar(Trust_users,tipping_point2(1,:),.6,'g');
l{1}='Range of Correct Sense'; l{2}='Made by Majority Rule';
lgnd =
legend(h,l,'Orientation','vertical','edgecolor','none','FontSize',9);
set(lgnd,'color','none');
kk=1:50;
%yyyyyyyy
set(gca,'XTick',kk); % Change x-axis ticks
```

```
set(gca,'XTickLabel',kk); % Change x-axis ticks labels to desired
values
dim = [.5 .555 .3 .3];
str = l{2};
annotation('textbox',dim,'String',str,'FitBoxToText','on','edgecolor',
'none','FontSize',9)
set(gca,'YTick',tipping_point2(1,:)); % Change x-axis ticks
set(gca,'YTickLabel',tipping_point2(1,:)); % Change x-axis ticks
labels to desired values
ay = gca;
ay.YColor = 'red';

grid on;
xlabel({['Number of good SUs , G']});%['n=' num2str(n)];['B='
num2str(Untrustworthy(1))]);
%h = xlabel(tt);
ylabel ('K [Number of malicious users]','FontSize',12);
titletext=['Conventional Majority Rule '];
title(titletext);
```