MALICIOUS USER DETECTION IN INFRA-STRUCTRE BASED COGNITIVE RADIO NETWORS (CRNs)

By

FARHEEN KOUSAR

A thesis submitted to the faculty of Electrical Engineering Department Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Electrical Engineering

February 2018

ABSTRACT

The ultimate purpose of Cognitive Radios is to achieve best available channel using its special features re-configurability and cognitive capability. The most challenging task is to share spectrum along with licensed user devoid of causing harmful obstruction as per rules & regulations of FCC. Cognitive radio overcomes the shortage of spectrum by usage of unused or underutilized spectrum band which is termed as white space or spectrum hole. Cognitive Radios have become popular in recent few years due to its unique properties.

But on the other hand security of CRNs also matters a lot. Many latest technologies has been invented in wireless network environment but the issue of security is still there because of open mode of communication. CRNs suffers all conventional security threats besides these some new security issues are also there due special characteristics (re-configurability and cognitive capability) of CRs.

In this research work we have focused to propose a technique based on fuzzy logic for secure communication of CRNs. There are many existing security algorithms but proposed algorithms is more robust having less computational complexity. Main objective of our research is to propose an algorithm for detection of security attack in infra-structure based CRN, to identify the malicious node which is attacking and to improve overall performance of network by suppressing the malicious user.

DEDICATION

With the blessing of Almighty ALLAH I am able to complete this thesis and I would like to dedicate this work to my

FAMILY, TEACHERS and FRIENDS

For their remarkable support during the whole duration of this Masters.

ACKNOWLEDGEMENT

All commendation because of Almighty Allah who showered his blessing and able me to complete such exploration work.

I would like to take this opportunity to special thanks for an amazing support that my supervisor Dr. Muhammad Imran have been, throughout the course of my thesis. He helped me a lot to able me in completing my MS Degree, he was all time readily available for my guidance and to help me throughout my Research work.

With sincere gratitude and bundle of prayers for Him!

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

Acronym Name: Complete Name

FCC: Federal Communications Commission

SDR: Software Defined Radio

CR: Cognitive Radio

PSD: Power Spectral Density

DSA: Dynamic Spectrum Access

ISM: Industrial Scientific and Medical Band

PU: Primary User

CRN: Cognitive Radio Network

FC: Fusion Centre

CSS: Collaborative Spectrum Sensing

UNII: Unlicensed National Information Infrastructure

PUEA: Primary User emulation Attack

SSDF: Spectrum Sensing Data Falsification Attack

P_{fa}: Probability of False Alarm

P_{md}: Probability of Miss-Detection

CIA: Confidentiality Integrity Authenticity Model

SBW: Back Off Window

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

QoS: Quality of service

Chapter 1

INTRODUCTION

1.1 Introduction of Cognitive Radios

The Federal Communications Commission (FCC) is in charge for guideline of interstate telecommunication, management and licensing of electromagnetic spectrum within the United States and it enforces necessities on inter station interference in all radio frequency bands. They provide license to precise users in specific geographical domains. Some unlicensed bands were gone free for someone to use under some power rules and regulations. But due to growth of wireless communication these unlicensed bands have become over congested.

To overcome this congestion new ways of managing RF resources have been investigated by FCC. The concept behind its implementation is that uses are permitted to use the licensed band if they ensure the minimal obstruction is caused to primary licensed users .Practically implementation of this concept is on skyline due to advances in software and cognitive radios. In this era new communication mode is software defined radio (SDR). Fixed transmission parameters adjusted by the operator were used in early radios but, the attractive feature of SDR is that its parameters (frequency variation, modulation type or maximum radiated or conducted output power) are not fixed. These operating parameters can be changed by simply changing the software while the hardware is intact. A reliable and cheap solution is provided to the user using SDR as hardware requirement is minimized but, spectrum availability is not addressed. Cognitive Radio (CR) is advance form

of SDR, including all features of SDR and also take into consideration spectrum accessibility. Cognitive radio is best solution to this spectrum insufficiency dilemma because it adjusts unlicensed users along with primary licensed users. Cognitive Radio (CR) is a smart radio having capability to check its surroundings, adjust and operate consequently providing upper limit of spectrum efficiency. CR's are completely programmable wireless devices that can vigorously settle in their transmission waveform, channel access schemes, spectrum utilization & networking protocols same as desirable for high-quality network, working environment and application performance.

In recent survey of FCC 70% of licensed spectrum remain under-utilized according to geographical area and time of usage [36]. For example in New York city the frequency band 30 MHz to 3 GHz has maximum occupancy of 13.1% [1, 2]. A similar report was examined for rushy area of Washington, D.C, for below 3 GHz Frequency band and results conclude that spectrum occupancy is less than 30%. The Power Spectral Density (PSD) of 6GHz received signal has been calculated and shown in figure given below [3]. Figure shows that from 3-6 GHz spectrum band is underutilized.

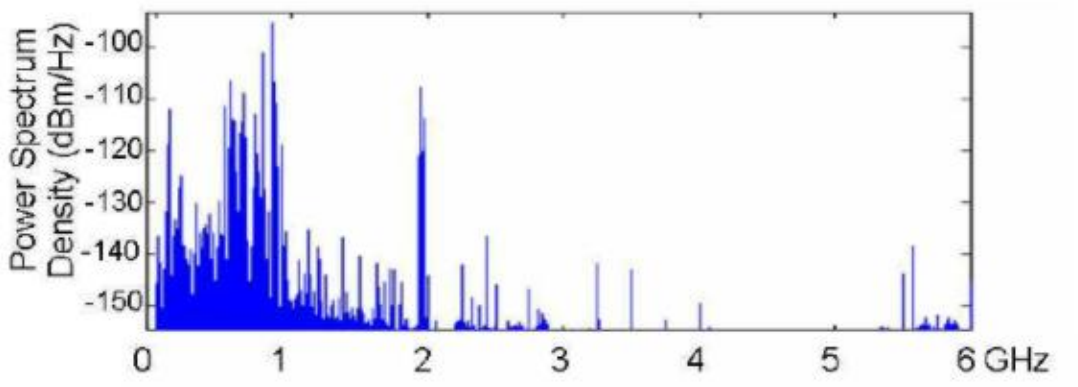
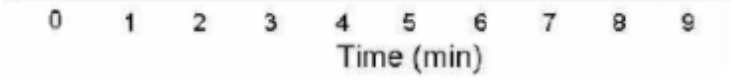


Figure 1: Measurement of 0-6 GHz spectrum utilization at BWRC [3]

Freq (GHz)	0~1	1~2	2~3	3~4	4~5	5~6
Utilization(%)	54.4	35.1	7.6	0.25	0.128	4.6



Dynamic Spectrum access (DSA) plays a vital role in using spectrum efficiently. CR can work in best available frequency band using Dynamic spectrum Access .More generically we can say that using CR, user has ability to detect available spectrum band (sensing the spectrum), choose the finest spectrum channel (Management of spectrum), communicate with all other users (sharing of spectrum) & also evacuate the channel on demand of licensed user demands bank (mobility of spectrum). A specific spectrum is selected in spectrum decision according to the parameters like transmission mode, data rate etc.

1.2 Features of Cognitive Radio (CR)

The concept of DSA is implemented using CR due to its special features. CR was developed by Joseph Mitola at DAPRA as a new version of SDR. In CR spectrum band is chosen dynamically and parameters are adjusted accordingly. The core characteristics of cognitive radios is Cognitive Capabilities along with Re-configurability.

1.2.1 Cognitive Capability

Cognitive Capability tells about CR's capability to judge the environment and having interaction on real time. Mainly three characteristics explain the cognitive capability; sensing the spectrum, Analysis of spectrum and Decision of spectrum. Sensing of Spectrum is to find out and monitor the spectrum holes. The specifications for spectrum holes are examined with spectrum

analysis.

1.2.2 Re-configurability

Capability of radio which permits CR to change their parameters like working frequency, transmission power, modulation in any time exclusive of changing the hardware. In simple words SDR is re-configurability of CR. Changing's can be done in all communication layers depending on the spectrum availability while the hardware remains the same as shown in figure 2.

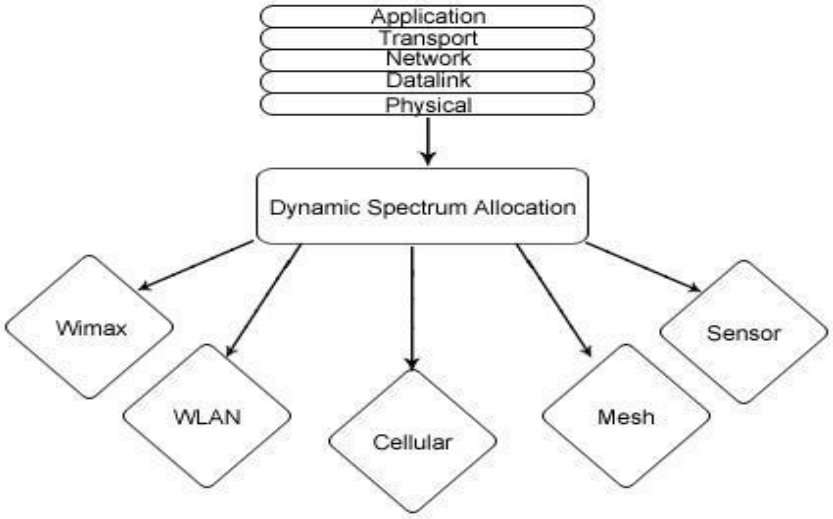


Figure 2: Dynamic changes in all Layers

According to FCC, CR is a system that scrutinize its operating environment and has ability to adjust freely and forcibly its working parameters to alter system operation, like to increase throughput, moderate obstruction, enable interoperability [4]. Unlicensed spectrum is considered as a "Wall of Interference" in ordinary radios while in case of CR unlicensed spectrum is "window of opportunity". CR technology provide an efficient solution to underutilized spectrum band by allowing unlicensed user to occupy spectrum devoid of causing obstruction to primary licensed users. Such type of

spectrum sharing is named as DSA. A CR independently exploits a spectrum hole to create another way of spectrum access. Following functions are performed by a CR.

- Make each user to sense outside environment by sensing continuous time basis;
- Acclimatize the working of every transceiver to numerical changing of the incoming radio frequency stimuli by learning the environment;
- To provide a way of communication among multipath users by cooperating in a self-organized method;
- To manage communication between users through allocating accessible resources properly;
- To produce familiarity of objective and self-consciousness.

Beside all these functions two primary objectives of CR are:

1. To endow with a trustworthy communication between users

2. A fair minded way exploitation of radio spectrum

1.3 Cognitive Radio Cycle

A CR senses the channel, gathers information and then finds the spectrum holes. Properties of vacant channels are assessed from spectrum sensing. According to the features of spectrum and user's requirement a specific spectrum band is chosen. The users can start communication after selecting operating frequency. A cognitive cycle is described in figure 3.

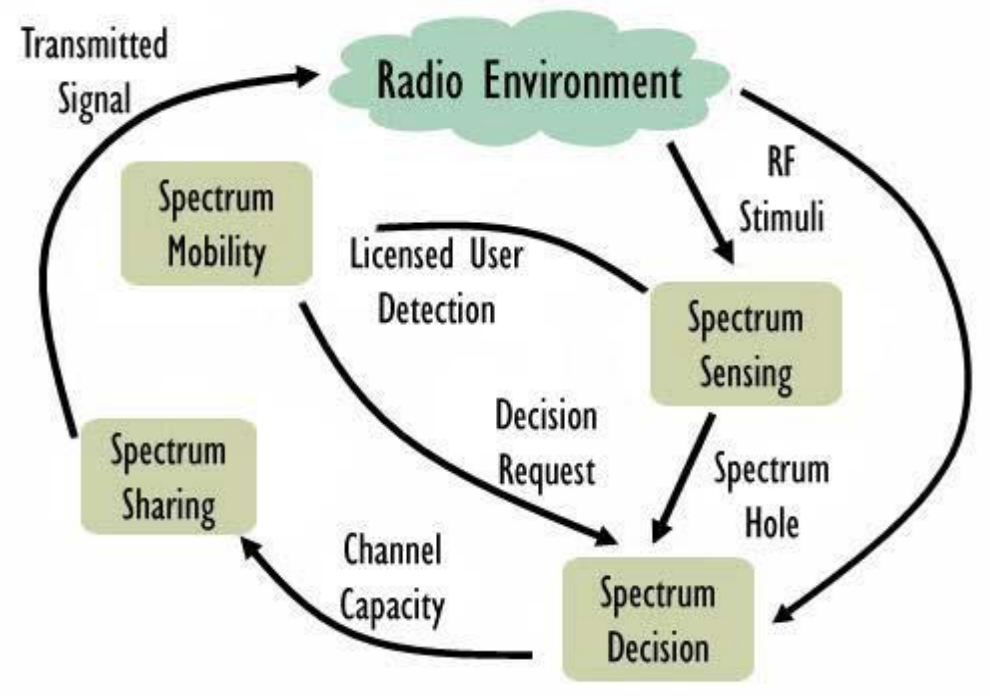


Figure 3: Cognitive cycle for the cognitive radio network

Four basic functions of CR are as follows:

1.3.1 Spectrum sensing (SS)

The ultimate purpose of CR is to achieve best available channel using its special features re-configurability and cognitive capability as discussed above. The most challenging task is to share spectrum along with licensed user devoid of causing harmful obstruction as per rules & regulations of FCC. CR overcomes the shortage of spectrum by using unused or underutilized spectrum band which is termed as white space or spectrum hole as shown in figure 3. If the occupied band by unlicensed user is demanded back by licensed user then CR will vacate the channel within two seconds or remains in the same band by changing its parameters like modulation scheme or power level in-order to reinforce interference. Spectrum sensing is a vital characteristic of CR to use the spectrum holes more effectively. Spectrum sensing can be done using different methods but it is very crucial to choose

best sensing technique under fading, AWGN environment etc. Basic role of CR in SS is to find the white space and communicate. It seems to be an easy task but not in actual because of channel impairments and other intruders. Sometimes channel is vacant but CR is not able to detect and vice versa. CRs share the information about the vacant spaces to the other users by constantly sensing the spectrum which is called out of band sensing. Secondary Users (SU) after adjusting its parameters in accordance with vacant band starts communicating. While communication, a SU continuously performs in band sensing (sensing about the arrival of PU). If a PU comes and wants to occupy the channel, SU left the channel and start hunting for another channel.

There are a number of sensing techniques used named as Energy Detection, Multiple Antenna, Eigenvalue, Covariance, Multi-taper ,Wavelet Packet Transform, Matched Filter Detection, Cyclo-stationary Feature Detection method etc. Each technique having its own advantages and disadvantages because there always exists a tradeoff b/w accuracy and complexity.

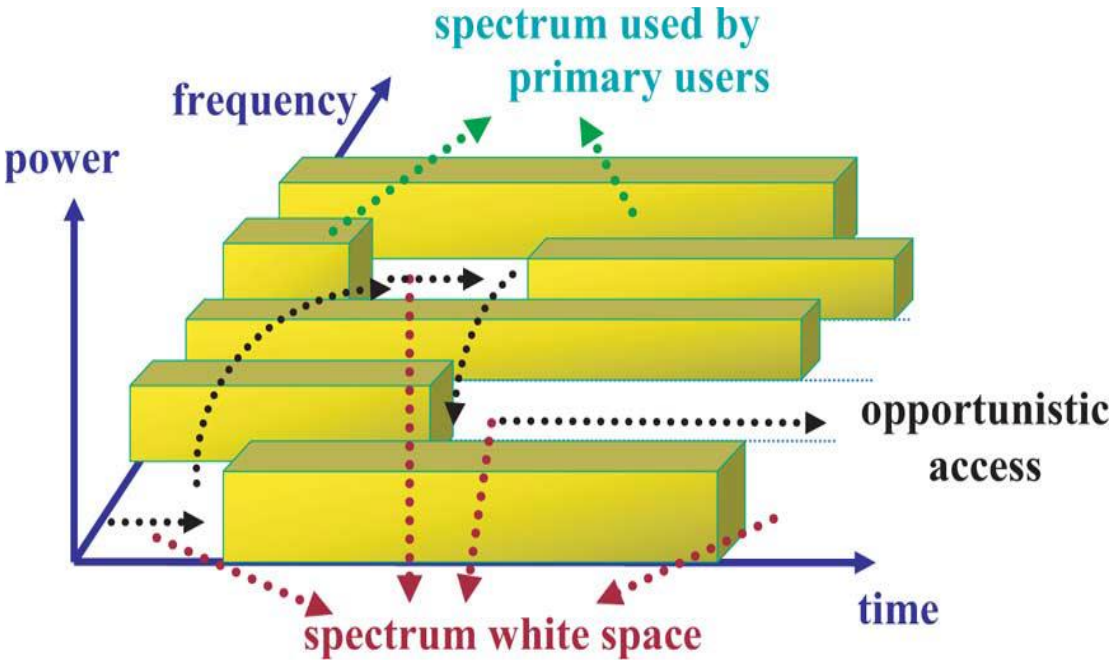


Figure 4: Spectrum hole or white space concept

These SS methods generally fall under three categories; cooperative, non-cooperative & interference based technique.

1.3.2 Spectrum decision

In spectrum decision, a CR decides a best channel for communication from the channels sensed in spectrum sensing stage. Channel is selected according to the quality of service (QoS), Communication cost and spectrum availability. First CR finds its own parameters like transmission bandwidth, transmission mode and data rate. Then select a spectrum band and can perform communication over that vacant spectrum hole. Since, the radio environment varies with time, therefore CR should also modify itself according to those changing.

1.3.3 Spectrum sharing

There should be coordination among CRs about spectrum access to avoid the collision because at the same there may be many CRs trying to find the white space. There are two ways of SU's spectrum sharing with PU [6] .In first way when SU is utilizing the spectrum and in the meantime PU appears and wants back the channel. SU left the channel and start looking for another free channel. Such type of sharing is named as opportunistic spectrum access. In second way, on arrival of PU, the SU stops its communication but does not leaves that channel, it stay silently in same channel to get it free again. This type is named as spectrum sharing.

1.3.4 Spectrum mobility

If CR is communicating on a spectrum hole and meanwhile PU appears then CR should move to another vacant band in order to avoid interruption in

communication. In such situation a seemless transmission is provided by spectrum mobility. During the transmission of CR if environment changes (primary user activation, change in traffic or user mobility) then this adjustment activates. Different spectrum mobility techniques are used as shown in the figure 5 given below.

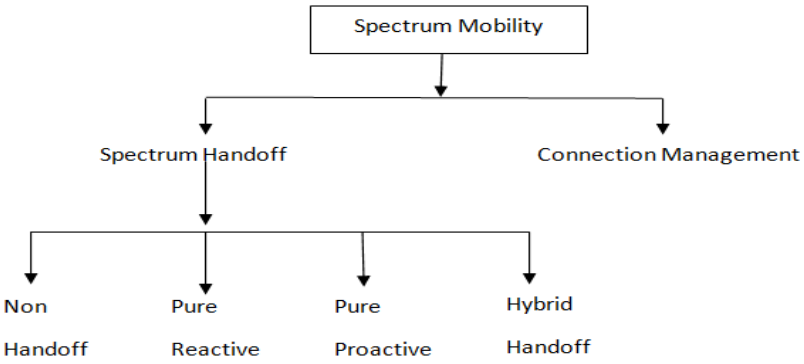


Figure 5: Classification of spectrum mobility techniques [6]

1.4 Cognitive Radio Architecture

Current architecture of wireless network inflicts heterogeneity for communication technologies and spectrum policies. Whole radio spectrum can be separated into two bands: licensed and unlicensed band (called industrial scientific and medical (ISM) band). FCC controls the spectrum usage in the United States. Devices operating on WiFi lies in ISM band. As radio spectrum being crowded day by day cause to increase in congestion spectral crisis. Major portion of the licensed band remains idle for 90 percent of the time. In order to apply communication protocols to CRN a description of its architecture is necessary.

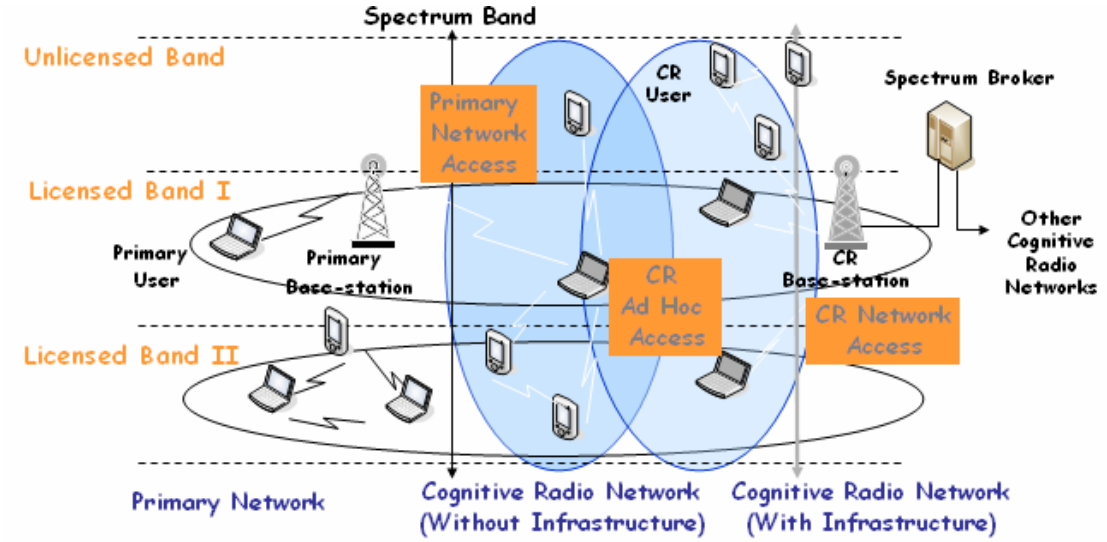


Figure 6: Cognitive Radio Network Architecture [7]

We can classify CRN on a number of parameters like their architecture, access behavior and access methods. Regarding architecture of CRN, it is decentralized or centralized. For centralized CRN, a secondary base station or Fusion Centre (FC) handles spectrum management. But in decentralized case all SUs share sensing reports among each other and work independently. Access behavior splits CR in two types, non-cooperative and cooperative. For cooperative method, FC is responsible for taking final decision after gathering sensing reports from all SUs, on the other hand non-cooperative case refers to distributed network. CRN can be licensed band or unlicensed band networks on the basis of operational point of view. On the basis of access type CRN may be Ad-hoc access or primary access. Special characteristics of CRs distinguishes them from ordinary radios, some of them are summarized in figure 7.

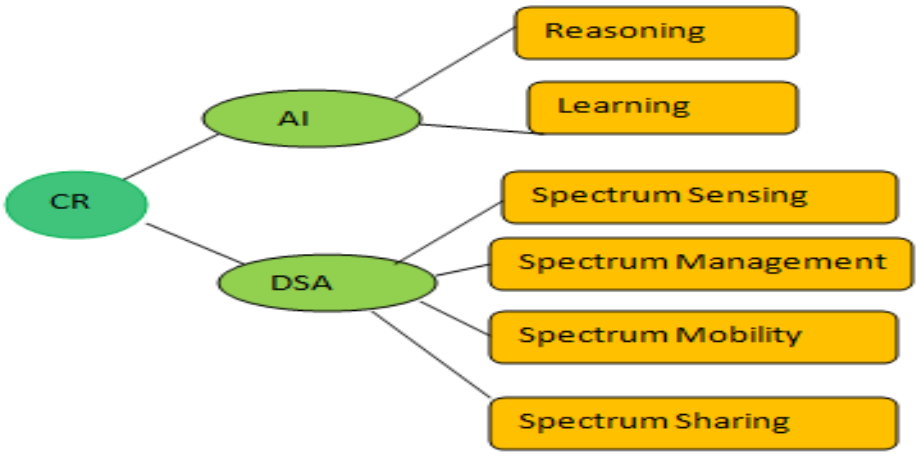


Figure 7: Special features of CRs based on artificial intelligence (AI) Dynamic spectrum access (DSA)

As shown in the figure Cognitive Radio Network (CRN) can be classified in two parts named as Primary network and Cognitive network. PUs are licensed users having direct access to the spectrum. While SUs have no direct access to the network are called unlicensed users.

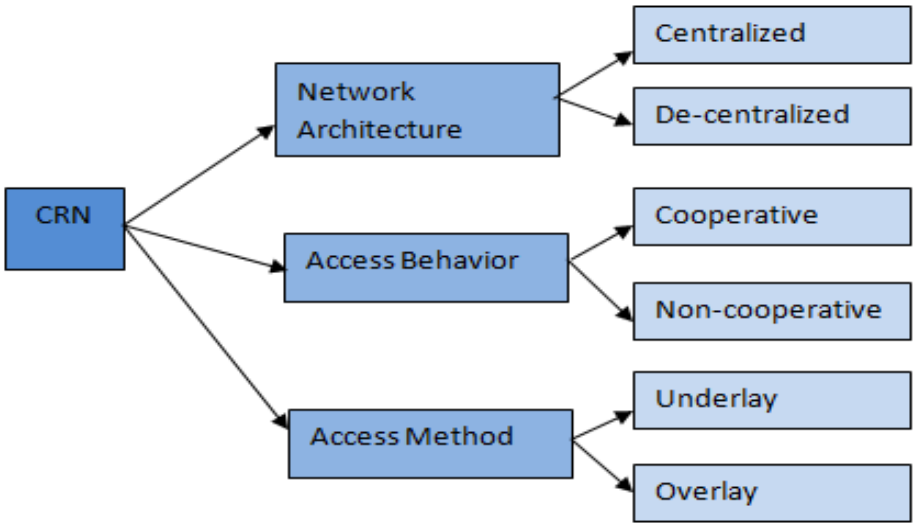


Figure 8: Classification of CRN based on Network Architecture, Access Behavior and Access Method

1.4.1 Primary network

Network having license is called primary network. Primary network include cellular network, CDMA, TV broadcast networks and Wi MAX. Following components are included in primary network.

1.4.1.1 Primary base-station

A network having a fixed infrastructure element specified to a particular technology having licensed band, termed as Primary base-station. For example BTS in Wi MAX and BTS of a cellular system are examples of Primary base-station. It cannot exists along with CRN therefore, some changing are required. Primary base-station require both licensed and un-licensed protocols in order to have access to unlicensed users.

1.4.1.2 Primary user

A user having license to work in a specific band is called PU. Via base- station a PU accesses the network. Base-station controls all its operations and services. Hence, user of any other network or unlicensed user has no effect on PU. Therefore, PU can co-exist with CR base-station and CR user without any changing.

1.4.2 Cognitive Radio network

CRN is such a special network in which spectrum is accessed only in opportunistic way and do not have license to direct access the required band. Both type of networks infrastructure based or Ad-hoc can be implemented in CRN. Working flow of CRN in 4 steps in shown in figure 9. Major elements of CRN are described below.

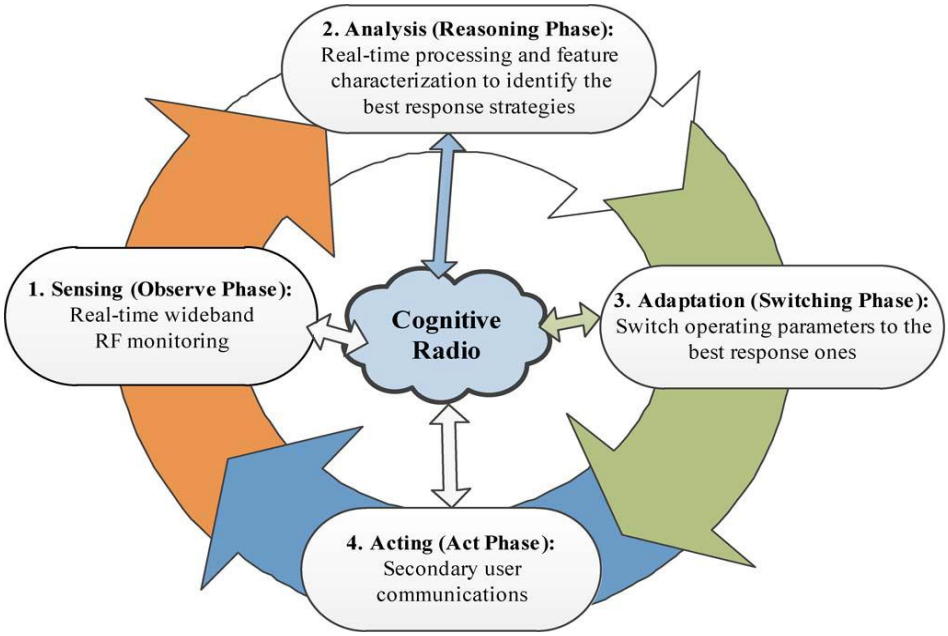


Figure 9: Working flow of CRN [8]

1.4.2.1 Cognitive Radio User or Secondary User

A CR User or SU is not a licensed user means it uses DSA for communication. A SU can receive its data only when PU is inactive because PU has priority over SU. SU uses the spectrum in such a way that it causes no interference with PU.

1.4.2.2 Cognitive Radio base-station

Secondary Base-station otherwise CR base-station is basically infrastructure based element of CRN that connects one hope to the CR User or SU without using a license of spectrum. A SU can communicate to other networks due to this base-station.

1.4.2.3 Spectrum broker or Fusion Centre (FC)

In case of infrastructure based CRNs Fusion Centre (FC) or spectrum broker is a central component that manages all sharing of resources among CRs.

Just like star network topology, FC is connected to CRN performing all functions of a central server. FC knows all about availability of network resources and helps all CR users to utilize the spectrum. FC gathers all sensing reports from SUs and apply the some fusion rule (discussed later) to find the final assessment about existence or absence of PU. After that FC communicate this decision to all SUs in its sensing group. In this way sensing accuracy is increased because sensing of a single SU about PU's signal may be false due to multiple factors. So, FC helps SUs in spectrum sensing. For a final decision, FC takes reports of all SUs and apply some fusion rule on that data. Fusion rules are of two categories namely soft decision and hard decision. Hard decision includes three type of decisions AND, OR and majority rule. For soft decision FC takes the sensing reports from SUs in the form of energy. Hard decisions are easy to implement as compared to soft decision which requires greater communication overhead and complexity. For that reason we mostly use hard decision in the form of binary 1 and 0. Basic functionality of FC is shown in the figure 10.

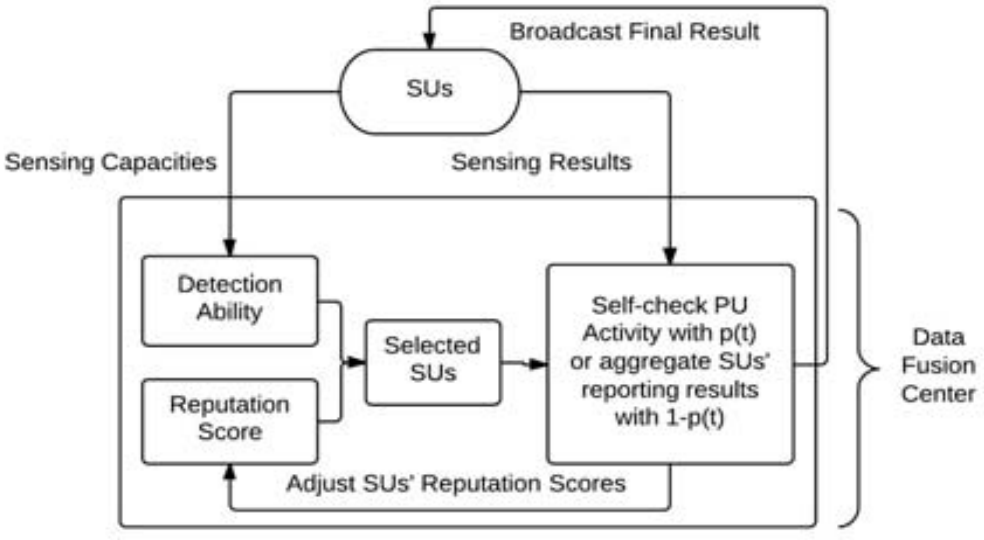


Fig 10: Function of fusion Centre

1.5 Metric of Performance of CRN

Performance of CRN can be measured using two parameters namely Probability of False Alarms (P_{fa}) and Probability of miss detection (P_{md}). Basic task of SUs is to detect the signal of PU that will conclude either the spectrum is free or not. If a SU performs sensing and it results that PU is present but in reality PU is not there, this error is called false alarm. While in case of miss detection SU senses that PU is not present but in actual scenario it is present. These two errors can occur due to different reasons such as channel impairments or malfunctioning of devices. This can also be due to misbehaving SU who has malicious intentions to use the spectrum in unfair manners.

1.6 Cooperative Spectrum Sensing or Collaborative spectrum Sensing (CSS)

In the past few years, CS is used to increase the sensing exactness. In cooperative or collaborative spectrum sensing results of a group of SUs are combined to take a final decision. In this way PU detection will be improved. Cooperative sensing concept can be implemented in both Ad-hoc and centralized (for example standard IEEE 802.22) CRNs. The sensing result of a SUs mainly degraded due to multiple factors like channel effects, multipath effects, shadowing and equipment malfunctioning. CSS is best and effective strategy to mitigate these all factors and introduces lower sensitivity and better detection. But on the other hand, CSS also faces extra overheads (like extra sensing time, energy, delay).These overheads can be minimized using

binary sensing reports. CSS can be beneficial to the overall network in many aspects. For example using CSS we can achieve high spectral density, high throughput, low interference and compatibility to the network conditions. Although CSS has advantages but on down side it is also possible that some SUs in the sensing can also send wrong sensing decision to FC with the aim of to reduce spectrum efficiency. Therefore, to compete with the malicious users a robust sensing technique is needed or FC should use some method to remove malicious users from the group. The basic concept of CSS is shown in the figure 11.

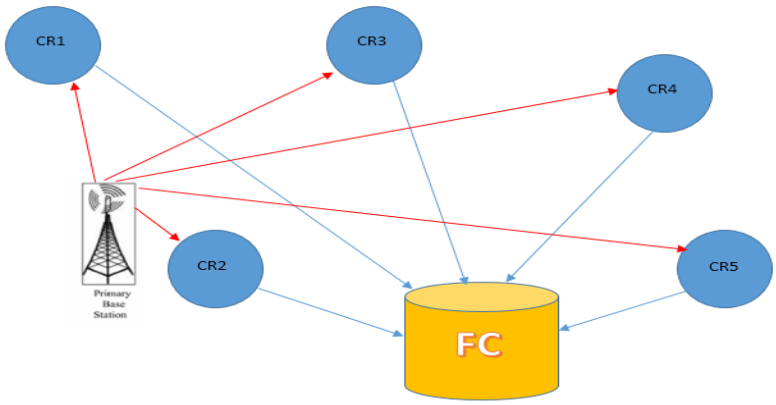


Figure 11: Cooperative Spectrum Sensing (CSS)

1.7 Fusion rules at FC

In case of CSS, FC takes decisions from all SUs and apply some fusion rule to add them. A very critical issue with sensing is that it faces problem in detecting a very weak signal, a signal below threshold level, shadowed and faded signals. These problems cannot be overcome with a single SU's sensing report. CSS introduces diversity gain against channel impairments [9]. Some fusion rules are briefly explained below.

1.7.1 Majority Rule

In majority rule also known K-out of-N rule, final decision is taken on the behalf of majority of SUs. That is, if half or more than half SUs say yes about presence of PU then final decision will be yes. In fusion case, where K-out of-N CRs are taking part in sensing to take the final decision about presence of PU, can be easily represented by Binomial distribution which is based on Bernoulli trials. Decision process of each CR is represented by a trial. Generic equation used for calculating overall detection probability Q_d is as follows:

$$Q_d = \sum_{l=k}^{N} \binom{N}{l} P_d^l (1 - P_d)^{N-l} \quad \ldots (1.1)$$

While in case of majority rule, we take $k = N/2$, where N is total number of CRs. P_d is probability of presence and $(1 - p_d)$ is about absence. $Q_{d,Maj}$ Can be calculated by setting $k = \lfloor N/2 \rfloor$ in (1.1)

1.7.2 AND Rule

And rule is also called N out of N rule. Detection probability can be estimated by setting $k = N$ in equation (1.1).

$$Q_{d,AND} = \sum_{l=N}^{N} \binom{N}{l} P_d^l (1 - P_d)^{N-l} = (P_d)^N \quad \ldots (1.2)$$

All sensing reports in the form of binary 1 or 0 is received at FC and finally combined using AND rule.

1.7.3 OR Rule

OR rule is also called 1 out of N rule. Using OR rule at the FC, the value of

$k = 1$ in equation 1.1 is used in following way to compute the probability.

$$Q_{d,OR} = \sum_{l=1}^{N} \binom{N}{l} P_d^l (1-P_d)^{N-l} = 1 - \binom{N}{l} P_d^l (1-P_d)^{N-l} \Big|_{l=0} = 1 - (1-P_d)^N$$

… (1.3)

Where N are total number of CRs or SUs, P_d is presence probability and $(1 - P_d)$ is about absence of PU.

1.8 Applications of Cognitive Radios

CRs have become popular in recent few years due to their unique properties. Some important and critical applications of CRN are as follows [10, 11].

1.8.1 Military network

CRN is an innovative technology having enough potential to be used in military network where security is an essential parameter [12]. Interference and jamming are mainly problems faced by military networks. DAPRA has worked on many research projects to use the CRN in military defense applications. In war environment, military radio can select any random spectrum band, coding and modulation scheme. So in this way CRN can be used in military defense networks.

1.8.2 Emergency network

In case of any disaster condition like earthquake, CRN can be deployed instead of infrastructure based wireless networks. Opportunistic spectrum access nature of CRN makes it enables to be used as an emergency network in disaster condition for safety of public.

1.8.3 Leased network

A licensed network is to facilitate leased network in a way by permitting CR users to use its spectrum without causing any harmful interference with the communication of basic licensed or primary user.

1.8.4 Use of TV white spaces

FCC has allowed CR users to sense and utilize free TV spectrum band. Power transmission limit has been set by FCC for CR users to operate in unlicensed band these power band limitations for Unlicensed National Information Infrastructure (UNII) and ISM band are given below in tabular form.

Band	Frequency range (MHz)	Bandwidth (MHz)	Max Power (Watts)
ISM-900	902-928	26	1W
ISM-2400	2400-2483.5	83.50	1W
ISM-5800	5725-5850	125	1 W
UNII-1	5150-5250	100	50mw
UNII-2	5250-5350	100	250mw
UNII-2e	5470-5725	255	250mw
UNII-3	5725-5825	100	1W

Table 1: FCC APPROVED RF POWER LIMITS IN ISM AND UNII BANDS (UN-LICENSED BANDS)

1.8.5 Cognitive mesh network

Mesh networks in wireless communication are considered as cost-efficient technology. But, if mesh network in used in some of applications that require high throughput in such cases, high capacity will be needed. Such requirement of high capacity of mesh network can be fulfilled using a CRN that dynamically access huge spectrum amount. In this way CRN is used in mesh wireless networks.

1.8.6 Use in future Cellular and wireless Networks

CRN can be used in cellular networks & wireless communication networks. In LTE-Advanced (LTE-A) and IEEE 802.16m, the concept of Femto cells has been used as an application of CRN. CRNs has been assigned definite licensed & unlicensed bands for their working. Communication networks and their operation bands are shown in table 2.

Category	Wireless Networks / Standard	Operating Freq band
PAN	802.15.1- Bluetooth 802.15.3a – UWB 802.15.5 – Zigbee	2.4GHz 3.1 – 10.6GHz 868/900 MHz/2.4GHz
LAN	802.11 a/b/g/n – WLAN	2.4 GHz, 5 GHz
MAN	802.16 d/e -Wi-Max	2-11/10-66 GHz
WAN	802.20-GSM,GPRS, CDMA, 2.5G, 3G, 4G	850/900/1900/ 2100 MHz
RAN	802.22- Cognitive Radio	54-862 MHz

Table 2: WIRELESS NETWORKS AND THEIR OPERATINGFREQUENCYBANDS (LICENSED / UN-LICENSED

1.9 Security of Cognitive Radio Network (CRN)

Many latest technologies have been invented in wireless network environment but the issue of security is still there because of open mode of communication. CRNs suffers all conventional security threats, besides these some new security issues are also there due to special characteristics (re-configurability and cognitive capability) of CRs. Attacks due to cognitive capability are PU emulation Attack (PUEA), spectrum Sensing Data Falsification attack (SSDF) and jamming of channels during acting & sensing phase for PUs and SUs. While re-configurability may be exploited by installing some malware or malicious code on the SU devised during adaptation or analysis phase of CR cycle. Therefore, successful implementation of CRN

requires more strict security arrangements than conventional radios. A layered structure of CRN in reference with OSI model showing security in CRN span has been described in figure 12.

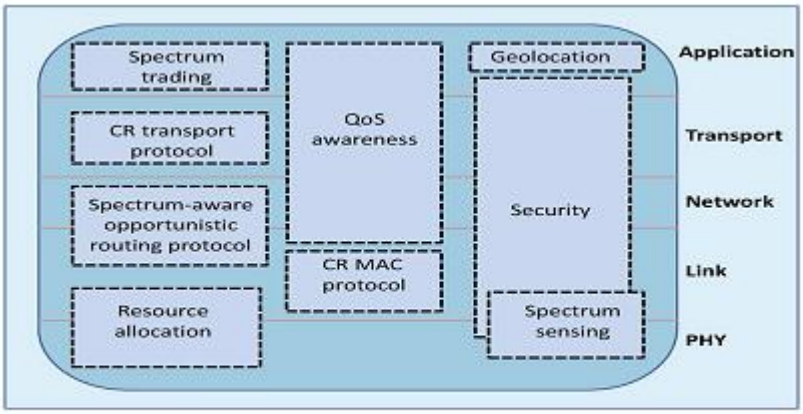


Figure 12: Architecture of CR in the layered model [8].

1.9.1 Security Attacks in Cognitive Radio Network

As already discussed CRN is not only prone to all previous security attacks but also to some new attacks due to their special characteristics. We will discuss only attacks specific to CRN. Here we will only list all the security attacks their details will be discussed in later chapter. Figure 13 shows the summary of all attacks to CRNs. Security attacks can be categorized according to different parameters such as malicious nodes, external attackers and greedy SUs. But attacks may be divided mainly in two scenarios namely Active and passive. In case of passive attack attacker only listen the useful information of honest users without having any active interaction with system. But in active attack, attacker has connection with communication system. Most of the attacks in CRN are active in nature.

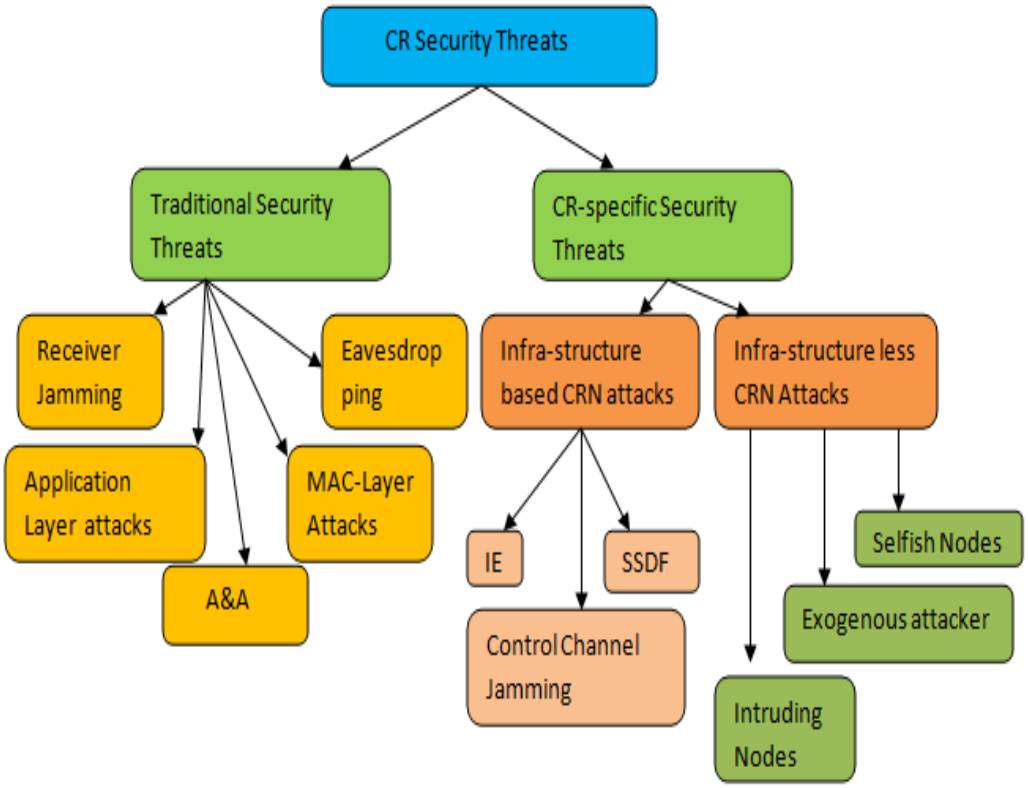


Figure 13: A summary of attacks related to CRN Environment

1.9.2 Malicious User (MU)

Dishonest users not performing correct sensing are known as malicious users. FC may take wrong decision due false sensing reports. These reports may be false due to SU's receive malfunctioned reports or due to malicious intent of SU who want to use the spectrum by unfair means or reduce the performance of overall system. There exist, many kinds of malicious users (MU) but we will discuss only three of them here: always yes malicious user always no malicious user and smart malicious user.

1.9.2.1 Always YES

We collect the sensing report in form of binary 1's or 0's at the FC.1 represents existence of PU while 0 for nonexistence of PU. Always yes MU

sends always 1 to the fusion Centre regardless of presence or absence of PU. Such malicious users reduce the spectrum utilization efficiency. Because if PU is not present and channel is free this user is telling that channel is occupied not free. Hence, it prevents the honest users from utilizing the spectrum or causing denial of service problem for legitimate users.

1.9.2.2 Always NO

This MU sends always binary 0 to the FC showing that always PU is absents. This MU causes interference with PU. Because, it always reports absence of PU and if SU start communicating it will interfere with already existing PU.

1.9.2.3 Smart Malicious User

Smart MU sends report opposite to the actual sensing. If sensing result is 1 and PU is occupying the channel this user report to FC 0. And if it senses 0 means that PU is inactive channel is free this smart MU sends binary1 to the FC to misguide it. This MU cause interference and reduces spectrum utilization efficiency as well. In some scenarios, MU behave maliciously to certain probability or for some period of time it performs correct sensing and for some other duration it start behaving maliciously with some probability.

1.10 Problem Statement

Wireless network is very prone and challenging to security threats, reason behind is that wireless channel is not able to distinguish among malicious and legitimate user that (anyone can listen and receive the signal). Due to diverse nature of attacks, there is need to work on countermeasures therefore, security of CRN is also critical. By using intelligent jamming devices an attacker can jam the CRN transmission or DoS attack for the secondary

Users/primary users. Therefore it really an emerging and important research area to analyze CRN's performance in such threat environment. Identification of attacks and malicious nodes in CRN and applying surveillance against these attacks and malicious nodes improves the overall performance of the wireless communication. Therefore, the core objective of this research is to identify the malicious node that destroys the overall performance of CRN and to exclude that user from the sensing group for a secure CRN communication.

1.11 Objectives

Following are the objectives of this research.

- To purpose an algorithm for detection of security attack in infra-structure based CRN.
- To identify the malicious node which is attacking.
- To improve overall performance of network by suppressing the MU.

CRN is urbanized for resourceful exploitation of unused spectrum with the help of sensing the environment, hence the spectrum scarcity issue is resolved. By securing the CRN from MU or attacks, we ensure that the resources are not wasted and being properly utilized that result in the improved performance of the communication system.

1.12 Proposed Solutions

To identify such malicious nodes in infra-structure based CRN a novel strategy has been adopted. Fuzzy logic is applied to suppress and identify malicious nodes in CRN. These three type of MUs has been taken into account using MATLAB simulations. Performance has been measured using probability of false alarm and probability of miss-detection. Performance of

purposed solution is also compared with already existing algorithms.

1.13 Thesis Organization

Thesis organization is as follows:

- Chapter 1: In this chapter Introduction to CRs has been given along with its architecture and needs for its Security and areas of its applications has been described.
- Chapter 2: Different types of attacks and their counter measures are discussed. Attacks are also explained according to different layers of CRN and OSI model as well. In this chapter existing techniques have been briefly explained.
- Chapter 3: This chapter descries the proposed methodology along with its algorithms in detail.
- Chapter 4: In this chapter results of simulations are compiled and proposed algorithm has been compared with other algorithms.
- Chapter 5: This is final chapter that concludes all the work done and its future perspectives to extend this work.

1.14 Summary

This chapter covers the main aspects of research topic. A detailed overview has been given on the architecture of CRN. It explains the need for security for CRN and basic objective & motivation for selecting this topic as a Master's thesis research work. The scope of this project has been highlighted with the help of problem statement. In the end of this chapter thesis organization is described.

Chapter 2

LITERATURE REVIEW

In this chapter we will discuss the different attacks and their counter measures as well. Attackers aim is to degrade the overall network performance in aspects of regarding access control, confidentiality, integrity and availability. Besides of these traditional attacks CRN introduces a new class of security attacks due to its dynamic access nature. So to make a secure communication of SU by allowing it to access the licensed band in honest manner is more challenging. Due to these additional security threats to the intelligent CRN most of its applications in military and commerce are being blocked to some extent. Traditional attacks includes spoofing, eavesdropping, Denial of service (DoS) attack and tampering. While attacks due to cognitive nature of CRN comprises of spectrum manager attacks, PU emulation attack (PUEA) and jamming. Breakdown of CRN can occur due to all these threats. Therefore, a very strong planning and its implementation is needed for a secure communication of CRN [13].

Most of the attacks are due to cooperative sensing in infrastructure networks. In this thesis, we will find the malicious user in sensing phase during cooperative sensing. Cooperative sensing is very helpful to improve the sensing reliability but it opens a new window for attackers to compute false sensing. Although we will discuss all attacks and their already existing strategies but major focus will be on physical layer attacks. Because these attacks are very critical. The attack to mitigate in this research is SSDF attack to find the malicious users that performs wrong sensing. There may be

obstacles in avoiding the attacks due to cooperative spectrum sensing. One challenging task is to separate the trusted user from un-trusted when they sends the sensing reports to the fusion Centre. The process of CSS depends mainly on three parameters: SU's behavior, PU's activities and wireless environment. There may be error in the sensing of a trusted user due to noise, multipath effect and fading. In other case a SU is not honest it intentionally sends false report to misguide the FC for its greedy purposes. These two behaviors effects the working of CSS. In the working of CRN, information of PU is confidential and not revealed to SUs because of privacy of licensed user having priority. That's why CSS depends on unreliable sensing reports of SUs. Unreliability means that these reports may be fake due to certain reasons. Before discussing the defense schemes first we need to understand the attacks in detail. A figure showing factors for unpredictability of CSS is shown in figure 14 given below [13].

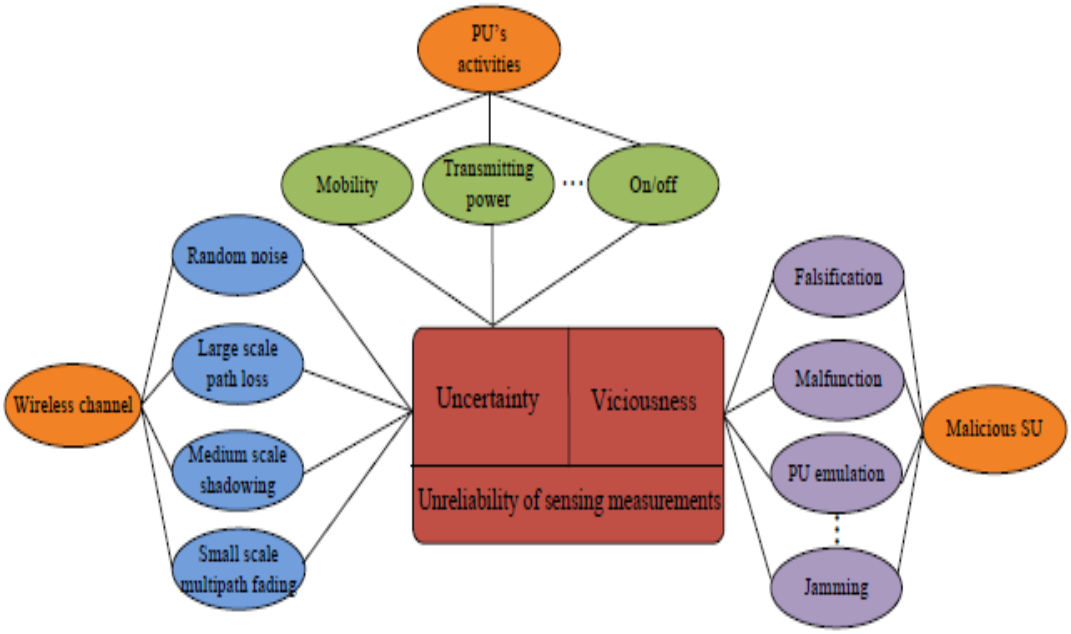


Fig 14: Unpredictability of CSS

2.1 Attacks in Cognitive Radio networks

CRN is best technology to resourcefully use the spectrum. Spectrum sensing considered as key parameter in working of CRN and its performance depends on the sensing. Malicious user may perform wrong sensing to mislead the FC. Most of the attacks in CRNs are in sensing phase like SSDF attack, PUEA attack are critical one. Sensing is performed on the physical layer of CRNs and if this layer is compromised then working of all other layers depends on this. In this way the whole working of the CRN will be disturbed. Although all layers should be secured but securing physical layer is very important [14] .The impact and duration of different attacks to infra-structured based CRNs and probability of attack is summarized in table 3.

Attack type	*Impact*	*Time Horizon of Impact*	*Probability*
Receiver Jamming	Moderate to High	Short and Long Term	High
Eavesdropping	Low to Moderate	Long Term	Low
Mac-Layer Attacks	High	Short Term	High
App-Layer Attack	High	Long Term	Low
A&A	Moderate to High	Long Term	Low
IE	High	Short and Long Term	Low
SSDF	Moderate	Short and Long Term	Moderate
Control Channel Jamming	High	Short Term	Low

Table 3: Impact and Probability of CRN Attacks [14]

There are a number of security attacks at different layers of CRNs. We will explain attacks specific to CRN at four layers. These attacks violates the

security requirements and damage the network. Table 4 shows different attacks with respect to contravention of CIA & attack type [15].

Layer	Attack name	CIA	Network member	Specification	Attack Active/Passive
Physical Layer	PUEA	A	External	Malicious user pretends to be PU	Active
	Jamming	A	External	Create hurdle in fair spectrum usage by sending jamming packets	Active
	SU overlapping	A	Both	Two SUs network overlaps and MU in one network also effects the other network	Active
	Objective Function	A	Internal	Transmission rate parameters are changed according to Attacker	Active
Data Link Layer	SSDF	A	Internal	Malicious SUs sends false Sensing results to FC to reduce spectrum efficiency	Active
	CC Jamming	A	Both	Control channel is jammed resulting difficulty in radio cooperation	Active
	CC Saturation	A	Internal	Control channel is saturated and is unable to send data.	Passive
Network Layer	Wormhole	C,I,A	Internal	Two MUs make tunnel to pass messages b/w them	Active
	Sinkhole	C,I,A	Internal	Captures the data before it reaches to destination	Active
	HELLO Flood	A	Internal	Attacker send hello message with high power showing best route.	Active
	Sybil	A	Internal	Similar to SSDF attack change the sensing decision	Active
	Ripple	A	External	MU shares incorrect channel information with others causing confusion in routing process	Active
Transport Layer	Depletion of Key	C,I	Internal	Large number of session keys is generated causing vulnerability to security system.	Active
Application Layer	Policy attacks	A	External	Attacker change CRN policy according to its demands	Passive
	CR Virus	A	Both	CRN is vulnerable to virus causing malfunctioning	Passive
Cross-Layer	Routing Information Jamming	A	Internal	Without changing information of routing legitimate user is forced to start handoff	
	Jellyfish	A	Internal	Similar to lion attack but throughput is compromised	Active
	Small Back-off window	A	Internal	MU gain unfair access to the channel at MAC layer	Active
	Lion	A	External	PUEA is used to disturb working of TCP protocol	Active

Table 4: Attacks are Different Layers of CRN [15]

2.2 Physical Layer Attacks

The physical laye is below among all CRN layers facilitating communication between networks devices (fibers or cards). Due to dynamic access nature of CRN, physical layer is more complicated as compared to physical layer of conventional wireless network. Our main emphasis is on physical layer because it effects the perormance of overall system. If security measurements

and precautions are done at the initail level, ultimately it is fruitful in avoiding the attacks for upper layers and also better cross layer optimization. Sensing is very challenging task to be performed on physical layer which makes vulnerable the CRN to many attacks. Major attacks due to sensing on the phusical layer are jamming, PUEA, secondary users oneralapping and Objective Function attack. Here we will discuss some imporatnt attacks and their defence techniques for mitigation of their effect.

2.2.1 Primary User Emulation Attack (PUEA) and counter-measures

In PUEA, an attacker produce a signal like PU's signal to make sure and confuse the legitimate SU that PU is present. The honest SU receives that fake primary signal and vacate the channel as per FCC rules for CR users to use the licensed band. Such type of attack degrades the spectrum usage efficiency by keeping honest users away from using the channel. PUEA can be of two types:

- Malicious PUEA: In malicious PUEA the intention of attacker is to prevent the legitimate users from finding the white spaces for communication. It is a DoS attack to certain extent.
- Selfish PUEA: Reasons behind selfish PUEA is to gain unfair access to the spectrum. Attacker tells other SUs that PU is present by sending a fake signal like PU's signal for enhancing its own spectrum shares. Two attackers cooperate together to launch this attack by creating a dedicated path among two malicious PUEA. A typical PUEA is shown in figure 15.

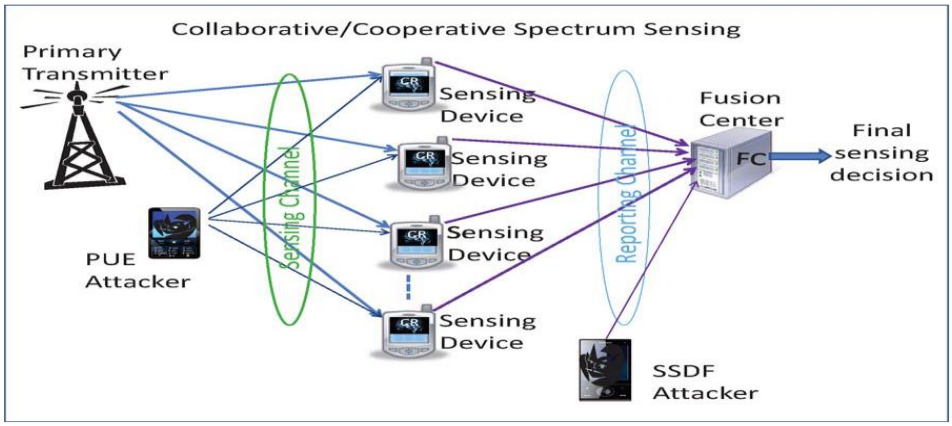


Figure 15: PUEA in CSS environment

2.2.1.1 Countermeasures against PUEA

PUEA can severely affect the overall performance of the system therefore its mitigation is important. A number of techniques have been purposed against this attack [17]. We will review some of them.

a) Transmitter verification Scheme or Localization based defence (Loc-Def) scheme

In the transmitter verification scheme PUEA can be handled if we know the exact location of the primary user. This method is also known as Localization based defence (LocDef) scheme. The authors in [16, 19, and 22] used this scheme by assuming that all the CR users know the location of primary user and exact distance between them. On the basis of coordinates which are known to the CRs the distance b/w primary user & CRs is designed .If a user sends a fake PU's signal its distance is also designed on the basis of received signal strength. The both results are compared to find the malicious user. Working process of transmitter verification scheme is shown in the form of flow chart in figure 16. Similar technique has been used in [18] where PU s verified using the fingerprint of the signal and location.

Belief Propagation technique have been used in [17]. Location function, a function of compatibility is calculated by all SUs continuously computed messages are shared with neighbours and belief function is computed till the convergence is achieved. The attacker will be detected at the stage where convergence is obtained and a message is broadcasted to all SUs containing all characteristics of fake primary signal. In this way all SUs are protected from malicious users. Received signal strength of transmitted signal in location function is used to find the malicious intent.

In this scheme, honest users are unaware of the attackers' location and signal strength. The malicious user is identified on the basis of measured distance of signal strength by large number of users. For one user to find the location of attacker there should be minimum three number of neighbours. After calculating the compatibility function and location, let's say the sum of belief manipulation sum is higher than a defined threshold then received PU signal is trusted PU not an attacker.

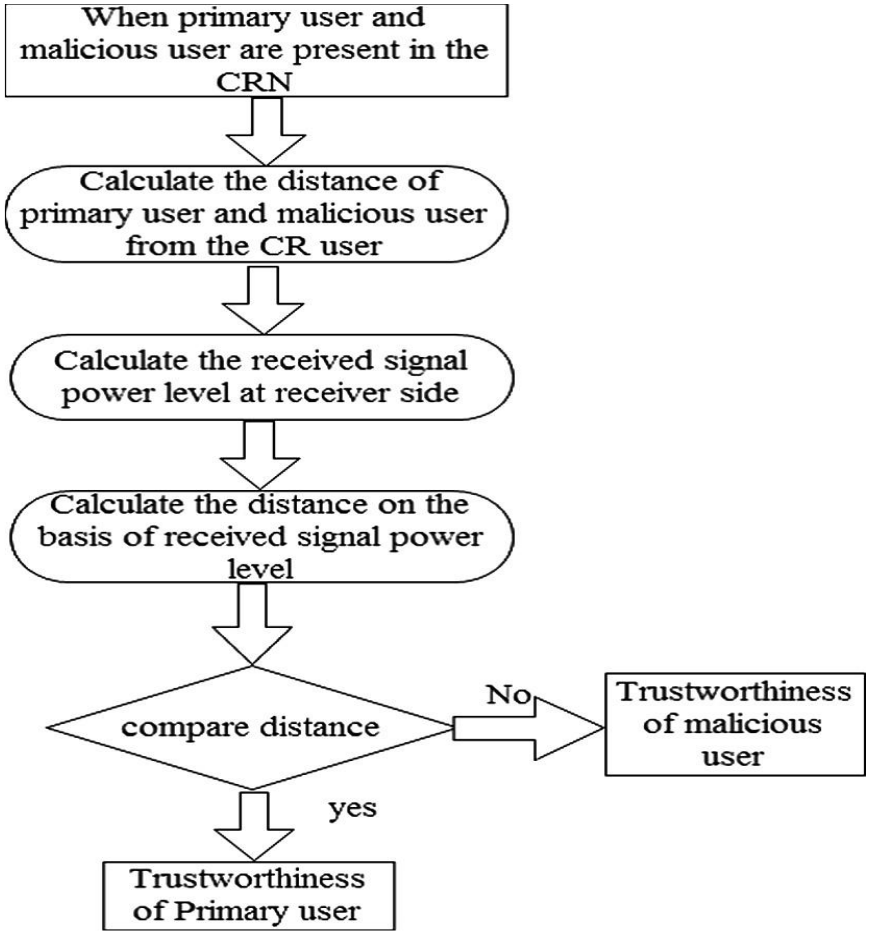


Figure 16: Proposed transmitter verification scheme

b) Finger print verification method

Based on the ANN scheme, phase noise is calculated from signal received. Wavelet transform is used in ANN to detect the PU. Fingerprint is a special parameter that is used to obtain the rate of false alarm hypothesis based on this, channel can be applied. This PUEA defense technique is used in OFDM. In this technique SNR has a direct relationship with the probability of detecting PU emulating signal [20, 23].

c) PU Authentication Method

Additional helping nodes are there to provide authentication about the presence of PU by having link signature and broadcast the information about

spectrum vacancy to all SUs. Public key infrastructure and certificate assigned by a third authenticated party is used to validate the helping node [21]. For mobile users algorithm used is helper resolution (HR) and has been analyzed for a number of attacks. This method is a very successful defense against PUEA to save more number of SUs. No repeated training is required to achieve this.

d) Water Marking Method of Authentication

In this method to avoid the PUEA, a water mark signal is added with every PU's signal. This authentication method can be used in digital television signals. This method does not affect the bit error rate of the primary signal. But this technique has a drawback that it is a sub-optimal method of authentication [24]. We can see the performance of any technique used for PUEA on the basis of certain parameters such as either it is localization based or not. The purposed scheme is cooperative or not. What are advantages and disadvantages of the purposed scheme, either the purposed solution follows the FCC rules and regulations as no changing's are required in the PU's signal. The technique's performance can also be judged on the basis of simulations that it performs or its real time implementation. Some more contributions to mitigate the PUEA attacks are summarized in table 5 on the basis of these parameters.

e) Intense Explore Algorithm

A proactive approach to remove the PUEA is Intense Explore Algorithm [25]. In this algorithm two sets of SUs (for example A_t, B_t) are taken into account. The alleged MUs are detected by FC on the basis of reports calculated from

A_t. The SUs in set A_t sends the report about neighbor in group B. If any two users sends the same report to the FC about a particularly neighbor, and that node has an energy level higher than required threshold then the node considered as malicious. The energy level of the neighbor node is calculated by using the energy detection method.

This method proactively detects the alleged MU's. Robustness of this algorithm is proved with the help of simulations. The detection latency and throughput loss has been reduced to 65%. The future work by extending this algorithm is to find the malicious users by taking into account the signals activity.

2.2.2 Overlapping secondary users Attack [15]

A geographical region may surround contemporaneous, overlapping more than one secondary networks. In situation both the networks experiences security vulnerabilities due to dynamic spectrum access. If a dishonest user is present in one network it may be dangerous for PU and SUs of both networks. Dishonest user sends wrong sensing data, hence depressingly heartwarming the objective function of the network (one or both). On the other hand malicious user can imitate as PU signal occasionally resulting to vacate the channel by honest SUs of one or both networks. It may also happen in a special condition that a node sends the report of presence of PU to one network and same report to other network causing harm to its objective function. Attack scenario is shown with the help of figure17.

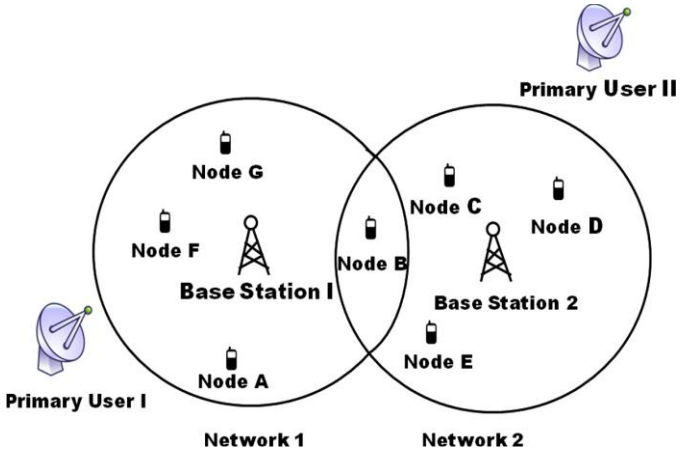


Figure 17: Overlapping secondary attack

It is not easy to avoid this attack because the secondary base station or the sufferer network has no direct control on it. Fundamentally this attack can affect the spectrum sharing and sensing for both Ad-hoc and infra-structure based networks resulting in denial of service attack. Three mitigation way out can be used to avoid the SU overlapping attack. These techniques can also be implemented to the any other DoS attacks.

1. Modification in Modulation Scheme:

Denial of service attack can be avoided using SS techniques (Frequency Hopping (FH), Direct Sequence (DS)). It will make more difficult to commence DoS attack. The quality of service still degraded due to these attacks.

2. Recognition and preclusion of attacks:

Same method is used as discussed earlier in prevention of PUEA. By noticing the PU's signal characteristics and its location attack can be avoided.

3. Using trust models and validation

In this method, mistrust level, reliability value and trust value is used to detect and remove a MU. And if the channel report of any user is different from others then it declared as malicious. Over the time period trust value is calculated and stability shows a stable trust value. A node having low trust

value will be finally acknowledged and a miss behaving user is excluded from the network.

2.2.3 Objective function attack (OFA)

Transmission rate parameters are manipulated at the attacker, therefore calculated results for the function are to be partial towards attacker's benefit. This attack exploits the availability of security aspects. It's a type of internal attacker, or active attack. This attack also known as Belief Manipulation Attack. Most of radio parameters are adopted according to environment inferred to maximize the objective function. Learning algorithms that learn from objective function are porn to this attack. Parameters that can be manipulated may include protocol of channel access, frame size, modulation, frequency, bandwidth, power and coding rate but these parameters are not limitation.

For example objective function can be defined in the following equation.

$$f = W_1P + W_2R + W_3S \quad \ldots. (2.1)$$

Where f is the objective function, S, R, P and W_i are security, rate, power and weights respectively. If the attacker want to compromise the security of the CR it will observe the channel and send jamming signal when CR will sends its data with high security. Due to jamming by attacker the CR will experience difficulty in sending the data. Either it will send the data with less security or it will not be able to send the data. One method to avoid OFA is to set a threshold for all parameters and CR will not communicate if certain parameter's value drops below a defined threshold level. The following two solutions are discussed in case of Ad-hoc network.

a) Outlier Detection Scheme

In [26] authors purposed a solution to defend a type of OFA in which attacker has ability to adjust and learn its attack tactics according to the wireless surroundings. The attacker endeavors to surreptitiously influence the sensing outcome for an Ad-hoc network to attack the final decision and objective function of CRN. A robust outlier detection technique for distributed network is purposed to tackle this hidden attack. A neighborhood voting method is used instead of alarms and threshold value as in older methods. All nodes find a mean based on algorithm and accomplish special correlation assessment after collecting all the sensing results from the direct neighbors. After that all nodes vote for their neighboring nodes about their authenticity. If for a specific node more than half of its neighbors declared as disbelieving then the node is not true user.

Authors in [27] presented a method to detect the nodes sharing false information about the channel to the neighboring nodes. This attack is same as OFA because target of the attacker is same to change the algorithms of decision construction for the CRN. Algorithms based on spatial correlation are used to authenticate the channel information of any node. These algorithms detect the malicious nodes with high detection accuracy with less false alarms. Simulations results show the accuracy for malicious node detection.

2.2.4. Jamming

In a communication system interference can be of two types: system inherent interference and hostile jamming. Interference because of source in the network is called system inherent interference (SII). Hostile jamming is introduced by the attacker due to its malicious intents. SII may be mitigated by efficient system model strategies and protocol for multiuser. But jamming is

performed by saturating the link between transmitter and receiver with jamming signals. These jamming signals are random and capricious and not following the rules of communication protocols. Conventional defense techniques are not effective to hostile jamming which cause the denial of service (DoS) attack. Before going towards the defense techniques first we know the jamming signal. Mainly jamming signals can be of three type's partial time jamming, tone jamming and band jamming. After analyzing the different jamming techniques following types of jammers have been proven effective. Reactive jammers jams the channel when PU sending the data. These jammers jam the communication system and uses low power. Deceptive jammers send continuous jamming packets to the communication channel. Channel will always be busy for legitimate users as showing the presence of PU. As this jammer send jamming signals constantly therefore it is easy to detect and its life time is short. Constant jammer is like deceptive jammer but it sends bits continuously instead of packets. It also causes DoS attack. Random jammer sends jamming signals for a period of time and remains silent for some period. Random, deceptive and constant jammers affect the transmitter to stop the sender from communication.

Minimum SNR is needed in CRNs to decode the signal at receiver. Jamming is a main type of attack in CRNs damaging the SNR of the signal. In jamming attacks attacker sends signal with high power and can be detected by using techniques based on energy and triangulation. If attacker is moving then it is difficult to detect. It is initial step to find the presence of jammer before mitigating it. Because if the performance of the network receiver is poor then it may be due to the some other factors rather than jamming. CRNs in both

scenarios cooperative or non-cooperative are prone to jamming attack. In non-cooperative CRN, nodes are distributed and not using a common channel for their information sharing therefore it is more defiant against jamming attacks. In jamming attacks the attacker may be detain the information of the channel and start sending the data on same frequency, or slows down the data rate as a consequence of jammed common channel. In case of non-cooperative attacks anti-jamming defense strategies are more robust in case of attacks but not efficient as cooperative case. For the non-cooperative networks in normal conditions (no jamming attack) throughput is less. Reason behind the lower throughput is that every node has to invest its energy to find the channel for transmission or reception. Here we will review some jamming mitigation techniques in case of cooperative networks.

2.2.5 Mitigation Techniques in case of Cooperative Networks

In [28] a scenario consists of a SU, PU and a jammer has been discussed. The authors calculate the amalgamations of number of data channels and control channels by launching a jamming attack to increase the transmission time of honest user during jamming attack. The fortitude of control and data channel was precise to the particular nature of application requiring certain throughput and service quality. If greater than 1 channel are allocated to the common control then simulation results shows that a tradeoff exists between probability of transmission and efficiency. It was also shown that results are not always obeying the rules that were expectation. If we take five control channels and data channels are three then this is a less efficient and conservative strategy than using four data and control channels. This example is for application of electronic mail in case of jamming attack.

2.2.5.1 Collaborative Defense Technique

A collaborative defense technique has been purposed in [29] for case of collaborative jamming attack. This collaborative defense technique is based on a multi-tier proxy .which is cooperative defense approach which utilize the spatial and temporal diversity obtainable to the honest users in infra-structure based CRN. Followers and proxies are two parts of the network. Base-station and followers are connected by proxies using as relays. This create problem for jammers by introducing a new layer of communication. The jamming attackers need to jam both proxies and followers in order to have a successful attack. Therefore this collaborative strategy gives tough time to the jamming attackers. It is understood fact that in case of cooperation, availability of spectrum is increased. But on the other hand, the communication latency is high due an increasing the layer in communication chain of command.

2.2.5.2 Particle Swarm Optimization (PSO) Technique

In [30] Particle Swarm optimization technique is used against jamming attack. A game theoretic point of view is used to resolve the most advantageous security strategy. Optimization problem can be easily solved numerically by applying swarm optimization algorithm (PSO). PSO resembles to a number of natural phenomena and every member in a group finds the best optimum solution for its own and relating to its neighbors.

2.2.5.3 A Stochastic Game Theory Approach

In this approach, the main concept is that PU's signal & jamming signal can be discernible and attacker is not able to jam the legitimate transmission. There is a conflict between malicious and honest user's intention: malicious user's aim is to reduce the utilization of spectrum by jamming while honest

user on opposite side want to increase the spectrum efficiency by designing schedules of channel switching. By taking the advantage of this concept that the honest user and attacker having opposite objectives, this problem can be solved by game theory (zero sum game) [31]. In this game theory model the honest user acclimatize its technique on the basis of switching among data and control channel in accordance to the availability of spectrum, quality of channel and proceedings of attacker. The simulation results shows that this optimal policy obtain better results (as throughput) by taking account cognitive capability of attacker, dynamics of environment and defense policy randomly. While on the other hand learning policy just increases the payoff at every step not considering all the factors disused above.

2.3 Data Link Layer Attacks

Data link layer liable for node to node communication within a single hope. Open nature of wireless channel opens a new window for the attackers. Major attack on data link layer is Spectrum Sensing Data Falsification Attack (SSDF). We use CSS for improving the reliability for sensing but it has also some disadvantages. Sources causing unreliability in CSS are shown in figure 14.

2.3.1 Byzantine Attacks or Spectrum Sensing Data Falsification attacks

In SSDF attack SU tells incorrect sensing report to FC to make the final decision wrong. Basic two purposes of MU launching SSDF attack includes vandalism and misuse objective.

Vandalism objective

Such type of MU is also called always NO MU because it always report absence of PU either it is present or not. This will results in interference with

legitimate PU. Due to wrong sensing reports probability of miss detection increases at the FC and severe interference with the PU. In this way SU does not satisfies the criteria defined by FCC and PU avoid by sharing their spectrum with SUs.

Misuse objective

Such MUs are a type of always YES MU because it always sends PU presence report to FC either the channel is occupied or free. This results to the wrong global decision declared by the FC the channel is busy and SU have to wait or to move for another free channel. The MU may use that free channel to increase its spectrum utilization by unfair means.

It is not necessary that an attacker can launch attack for only one of these two objectives. A MU can also launch attack for both above two objectives to increase attack probability.

Before discussing countermeasures against SSDF attack, there must be sound understanding of existing challenges and obstacles. One basic and major challenge is to correctly distinguish among honest and MU in CSS. Sources of unreliability to CSS are elaborated in figure 17 which tells that CSS depends on activities of PU, behavior of SU and channel impairments. Uncertainty shows that sensing report of an honest SU may be false due to limitation of sensing capabilities. Viciousness shows that a user is intentionally malicious and sends false values. These two factors degrade the performance of CSS. As SUs have no information about PU's behavior and it depends on the CSS. Viciousness and uncertainty have same effect on the sensing reports. Uncertainty is helpful in hiding MUs from detection as report of an honest user may be erroneous and different from other honest users. Mainly

viciousness and uncertainty of measurement are two major problems for consideration and most of the researchers have done work on them [13]. Undeniably, uncertainty is an important characteristic of sensing phase and is considered as unreliability source in measurement. A similar type of uncertainty is induced by MU by injecting false data to the sensing repots. Therefore, whenever MU is present in the network, sensing measurements has unreliability due viciousness and uncertainty. That is, these two issues should be tackled together [13].

Before describing the countermeasures against SSDF attack first I will explain some parameters about SSDF attack and some attack models. A very simple attack model is shown in figure 18.

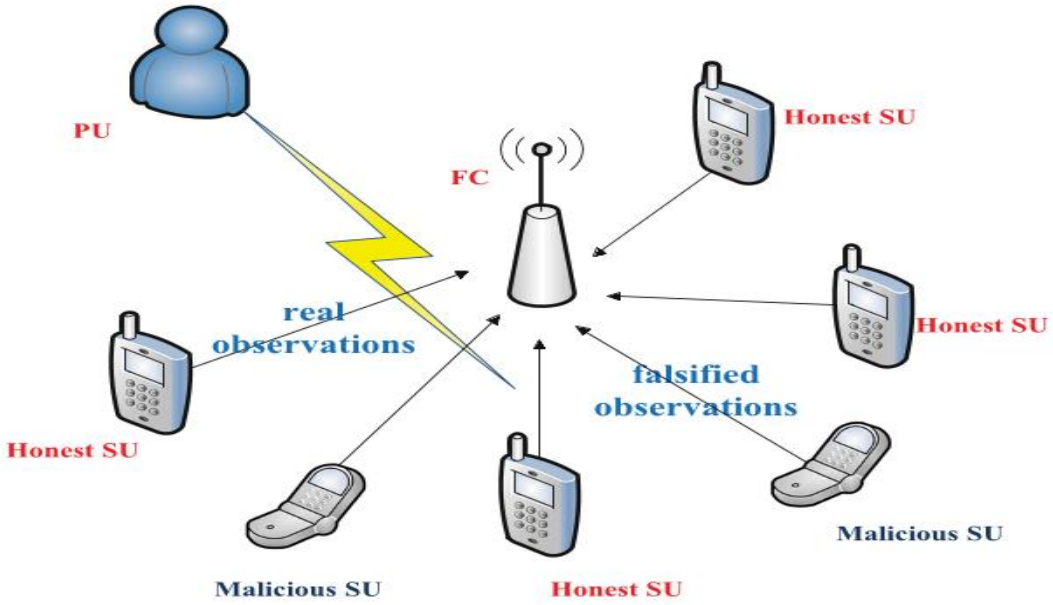


Figure 18: SSDF Attack Model [13]

2.3.1.1 Attack parameters and attack models

Diversity and flexibility are two critical features of SSDF attack that makes its detection more challenging. Basically four parameters can be used to describe this attack namely attack opportunity, attack basis, attack population, and attack scenario, which tells when, how, who and where to commence the SSDF attack, respectively. Taxonomy of all these parameters is shown in figure 19.

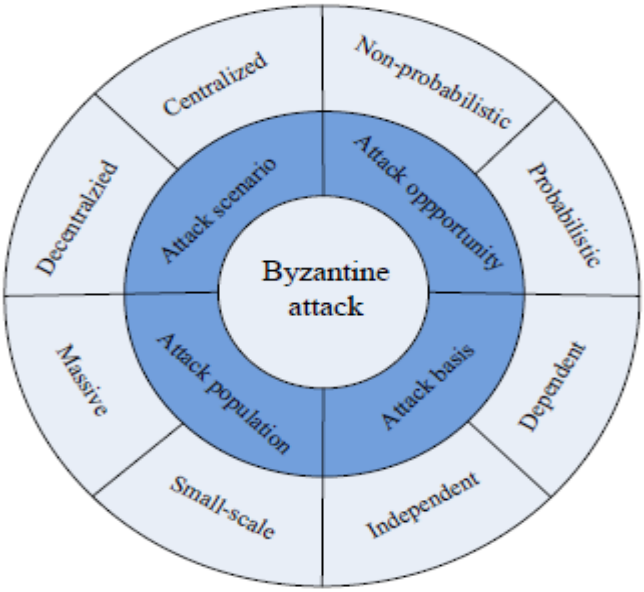


Figure 19: Different Attack Parameters of SSDF Attack

Attack scenario tells that where to attack according to the environment of the network. CSS can broadly classify as centralized or de-centralized based on the presence of FC in the network. The way of attack is affected by the behavior of interaction among SUs that is determined by CSS. Attack basis tells information on which attacker's attack strategy is based. Basic information is sensing report and a MU may gain some extra information such as sensing report of other SUs, fusion rule, defense strategy, and so on. Strong attack basis helps attacker to design an effective attack methodology.

Attack opportunity tells either the attack is probabilistic or non-probabilistic. Different type of attack behaviors and flexibility is revealed by attack opportunity [32]. Attack population tells who is attacking and MU's percentage in all SUs. It shows the degree of attack severity to the whole network. Logically, with an increase in attack population more sensing reports at FC are affected by SSDF attack. Different attacks models are designed based on these four parameters. Different attack models are shown in table 5. Attack model is represented by combining first letter of attack parameter. The tick sign shows that work has been done on such attack model while asterisk shows that any may be chosen and no contribution is done.

Parameters / Attack model	Attack scenario		Attack basis		Attack opportunity		Attack population	
	Centralized	Decentralized	Independent	Dependent	Probabilistic	Non-probabilistic	Small-Scale	Massive
CIPS	√		√		√		√	
DIPS		√	√		√		√	
CDPS	√			√	√		√	
DDPS		√		√	√		√	
CDNS	√			√		√	√	
CIPM	√		√		√			√
Others	*	*	*	*	*	*	*	*

Table 5: Current work on SSDF attack, where attack modes re denoted with combination of initial letters of their attack parameters, the check character indicates that the corresponding attribute is related, the asterisk character means may chose

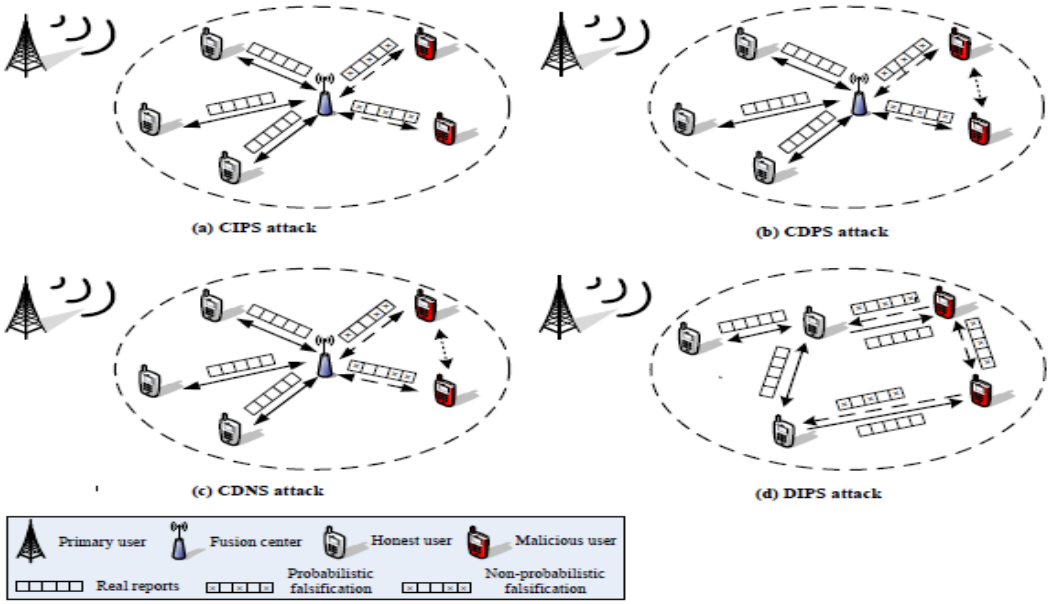


Figure 20: Attack models

These attacks models are defined based on SSDF attack parameters. There should be 16 attacks models by combination of all attacks parameters. But in reality only a few of them have been studied in literature. Mainly contributions have been done to these four attack models, (CIPS), (CDPS), (CDNS) and (DIPS). A detailed summary of different attack models is shown in figure 21.

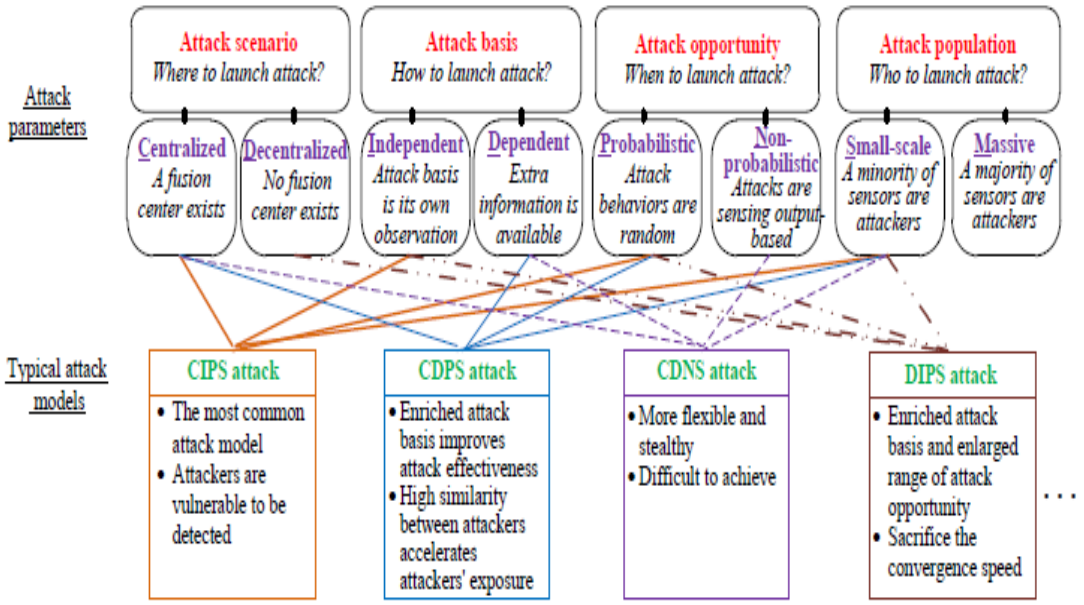


Figure 21: A summary of attack models and attack parameters

2.3.2 Defense of SSDF Attack

We know that SSDF attack badly degrades performance of CSS by sending false report, while purpose of its defense is to eradicate depressing effects of attacker, for efficient utilization of idle spectrum band. Best attack strategies for attackers and best defending techniques that maximize the objectives, are two fundamental issues for investigating SSDF attack defense. Although defense and attack are opposite but there are many tradeoffs between SSDF defense and attack. Figure 22 illustrates their relation.

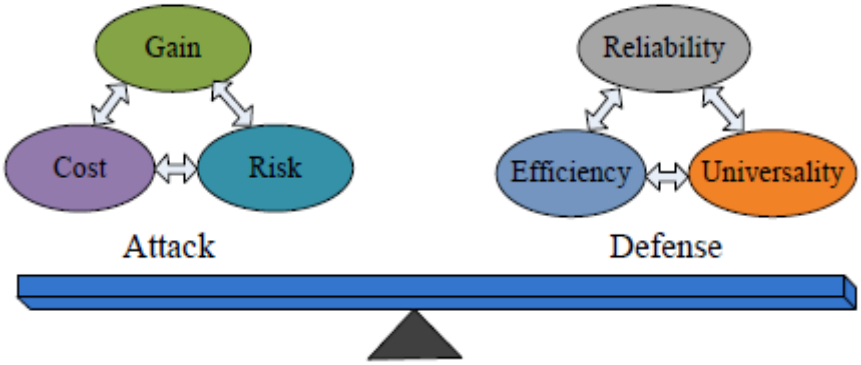


Figure 22: Game among SSDF attack and defense

While launching the SSDF attack, the attacker has taken into account: attack risk, attack gain and attack cost.

Attack risk is the product of probability of punishment and being identified. Attack gain tells about vandalism gain achieved by data falsification. Attack cost is about expenses to launch the attack. Attacker's gain perseverance is directly affected by attack danger i.e., attacker has to take extra attack risk for achieving more attack gains [33]. While a small attack risk and more gain can be obtained by increasing attack cost. For example, if attackers communicate with each other to launch attack their decision dominance probability may be

increased but on the other hand cost of attack is increased. Similarly, for defense there parameters are under consideration. Reliability is related to the attack situation and performance of spectrum sensing. Defense efficiency describes about convergence rate [34] and computational complexity. Convergence rate is important performance metric and a small convergence rate means that transmitting time is shorter [35]. Universality defines the defense algorithm's universality. In most of the defense schemes defense universality and efficiency are generally ignored and main focus is on defense reliability. From this discussion it can be concluded that SSDF attack and its defense are reserved to each other. Attackers need to develop the strategy effecting the final decision and not detected by defenders, while defenders need to investigate the attack behavior and implement defense rules accordingly. Mostly defense techniques are based on reputation and trust metrics trust and reputation schemes are similar in case of CRNs.

The authors in [39] purposed Pinokio method for detection of SSDF attack. Pinokio is based on a Misbehavior Detection System that keeps the normal performance profile on the basis of training data. Misbehavior is detected by observing bit rate. Some users may mark as malicious due to path-loss or other channel impairments. To avoid such behavior location reliability and malicious intention (LRMI) based scheme is purposed in [40]. The purposed LRMI scheme consists of two parts:

1. Path-loss attributes of wireless environment is reflected by Location Reliability.
2. True intentions of each SU are captured by malicious intention.

Basically two evidences are used to evaluate the reports at the FC, the location from the report comes and report generated by which SU. On the basis of these two parameters trust value is assigned to each user. The combination of these two parameters provides more accuracy in trust evaluation.

Zhang and et al. have comprehensively discussed SSDF attacks in [13]. According to Zhang, Defense algorithms can be separated into two broad classes namely Homogeneous Scenario & Heterogeneous Scenario. A summary is given in figure 23.

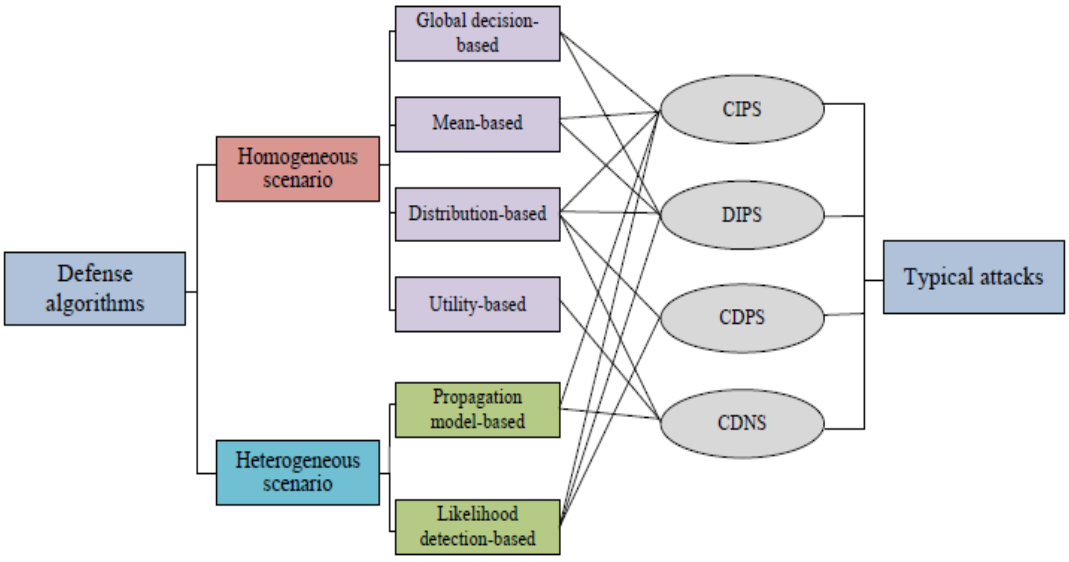


Figure 23: Existing defense algorithms against SSDF attack

2.3.2.1 Homogeneous Scenario

In homogeneous scenario all sensors are probable to work in same way that result to make them work on a universal standard to evaluate the other sensors and detects outliers. The universal standard can be of different type

such as global decision, mean, utility and distribution based. In global decision FC takes a global decision by merging sensing reports of all users and then compares that global decision with that of local sensing report of each user. If the report is not consistent with global decision then user declared as malicious. In [41]-[43] global decision is used to detect the malicious users. A sequential probability ratio test is introduced in [42] which is reputation based mechanism. This method is simple to analyze and perform but on the other hand its effectiveness and robustness is low in case of dependent attacks.

Similarly, in mean based method variance and mean of reports is calculated and find the deviation of each local sensing report from the mean value. This method having high robustness has been used in [44]-[46]. But this is also not suitable for dependent attacks. In homogeneous case all SUs are expected to follow the same distribution regarding their observation. But because of SSDF attack, MUs do not obey the distribution, which helps to distinguish outliers from honest users. This method is used in distribution based defense scheme. One approach is to make a comparison among the SUs' reports and find similarity between SUs [47]-[52]. Another way is to evaluate some metrics from reports showing the distribution [53]-[55]. This technique has advantage that it can handle dependent attack but having high detection delay and computational complexity. Intelligent MUs can calculate their utilities and have capability to maximize them. In reality attackers are afraid of penalties and sensitive to the incentives system. Therefore, utility based scheme is proposed to lead the malicious nodes to behave honestly by adjusting incentives and penalty avoiding the direct detection of attackers. A same technique has been applied in [56]-[58].

2.3.2.2 Heterogeneous Scenario

Heterogeneous scenario is different from homogeneous; performance of discrepant detection is shared among SUs because of path-loss, multipath shadowing and shadowing. Heterogeneity if scenario may also be increased due to different signal detection techniques of SUs. There are basically two types of defense strategies in heterogeneous scenario namely propagation based and likelihood detection based. Propagation model defense technique is based on the concept that observations of SUs are closely linked with channel propagation while the relation is deteriorates in case of SSDF attack. So on the basis of propagation model, the rationality of sensing reports of SUs is calculated and SU that are irrational are declared as malicious. Fast probe algorithm based on this technique has been explained below. Same method has been adopted in [36] [59]-[63]. This scheme has disadvantage that location privacy of SU is at risk.

Maximum likelihood detection technique evaluates the relation among SUs' sensing reports and detection performance to detect MUs from true users. There is a critical factor whether probabilities of false alarm and detection are earlier known or not. In ideal scenario, probabilities of false alarm and detection are known as same work in [65]-[67]. This method can handle more number of wrong cases but having more computational complexity. It is effective for preventing CIPS attack but if MUs cooperate to falsify the reports then it is no more effective.

2.3.2.3 Fast Probe Algorithm [36]

Fast probe algorithm is based on active transmission for detecting MU. It proactively detects the MUs therefore avoid the wrong sensing decision by the

FC. Accuracy of sensing is increased as well as interference with PU is reduced. This is the first algorithm that also detects the SU not performing in-band sensing. It has been compared with previous algorithms and simulations shows that throughput loss has been reduced to 65% and enhanced detection accuracy [36]. But on downside its performance is not good if no of MUs are increased more than 20%. Basic working of Fast probe algorithm is shown in below figure 24.

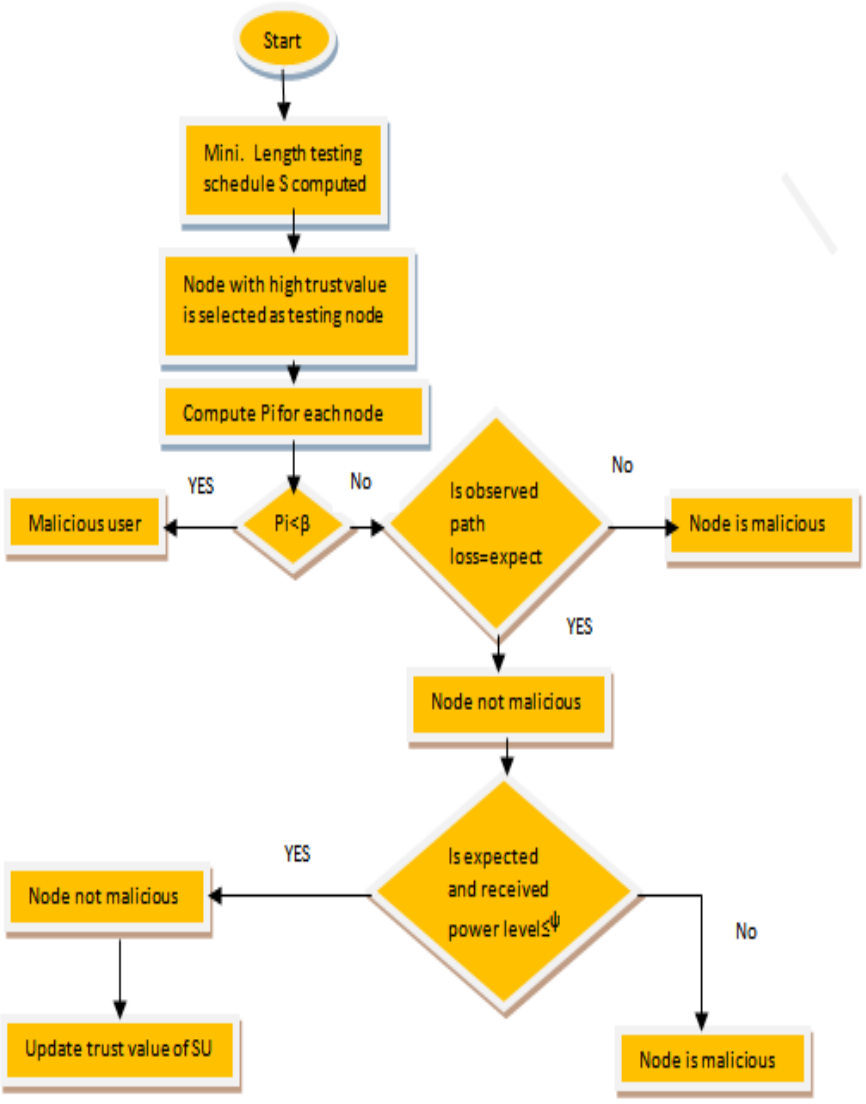


Figure 24: Fast probe Algorithm working flow chart

2.3.2.4 k-Mediods Clustering Using Pam-2 Algorithm

This algorithm is not based on conventional technique which requires a pre-defined threshold. Finding the threshold is a very challenging task. Moreover, it also difficult to vigorously vary threshold value in accordance with the scenario. This scheme is based on k-medoids clustering which is data mining technique for detecting SSDF attack. It does not require any threshold value and beyond detecting the SSDF attackers it also isolate them on fly [37]. It handles both dependent and independent attacks and attacker strategy is not known a priori. Its disadvantage is that it tackles only limited attack scenarios means attack can be launched by adding only 1's and 0's in the sensing report. Inputs to this algorithm are only sensing reports and global decision of FC. This algorithm is applied at the FC as this data is available at FC. Always yes, Always no, smart MUs, independent attacks and colluding attacks are tackled using this algorithm. Majority decision rule has been used at the FC to take a final global decision. Simulation results show the false detection rate & detection rate. Flowchart of k-mediods algorithm is given below in figure 25.

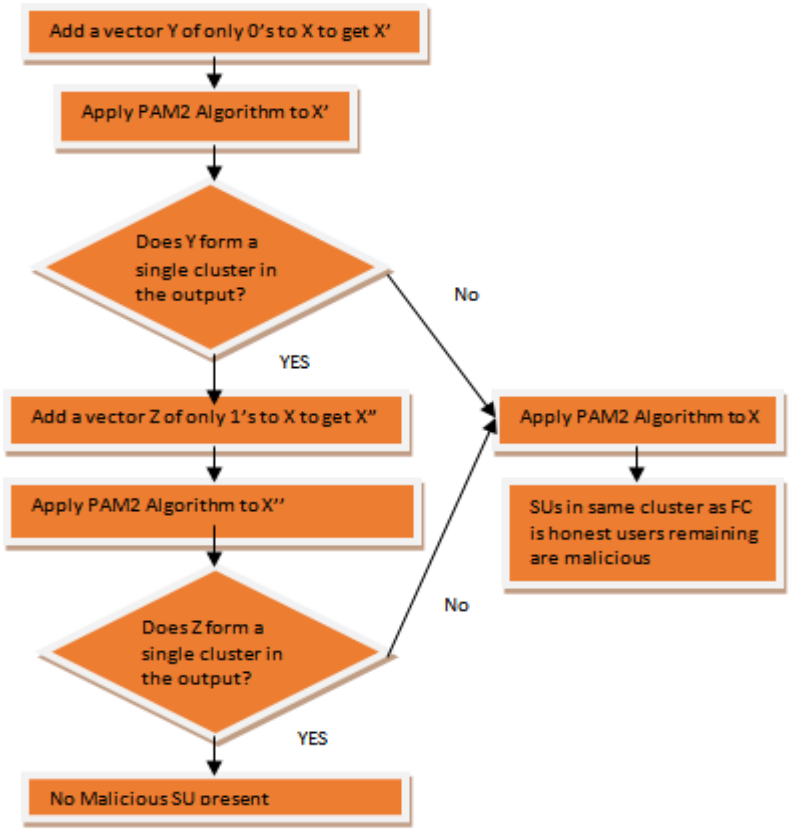


Figure 25: Detection using k-Mediods clustering

2.3.2.5 Credibility based defense algorithm

This is also a proactive approach for detection of MUs, using continuous type of reporting and q out of N rule at the FC [38]. This defense scheme comprises of three steps: calculate the credit value of each SU, eliminate the MUs, and take final decision by only trusted SUs. The credit value of every SU is maintained by comparing its sensing report with that of final decision. Accordingly its credit value is updated. After that fusion rule used to take a global decision, then SUs are judged by making a comparison with its credit value to that of threshold. If the credit value of any certain SU satisfies the threshold criteria then it is assumed to be trusted user and allowed to

participate in next spectrum sensing round. If the credit value is lower than that threshold, the node is confirmed as malicious and not allowed to take part in next phase of spectrum sensing. Working of algorithm is shown in figure 26.

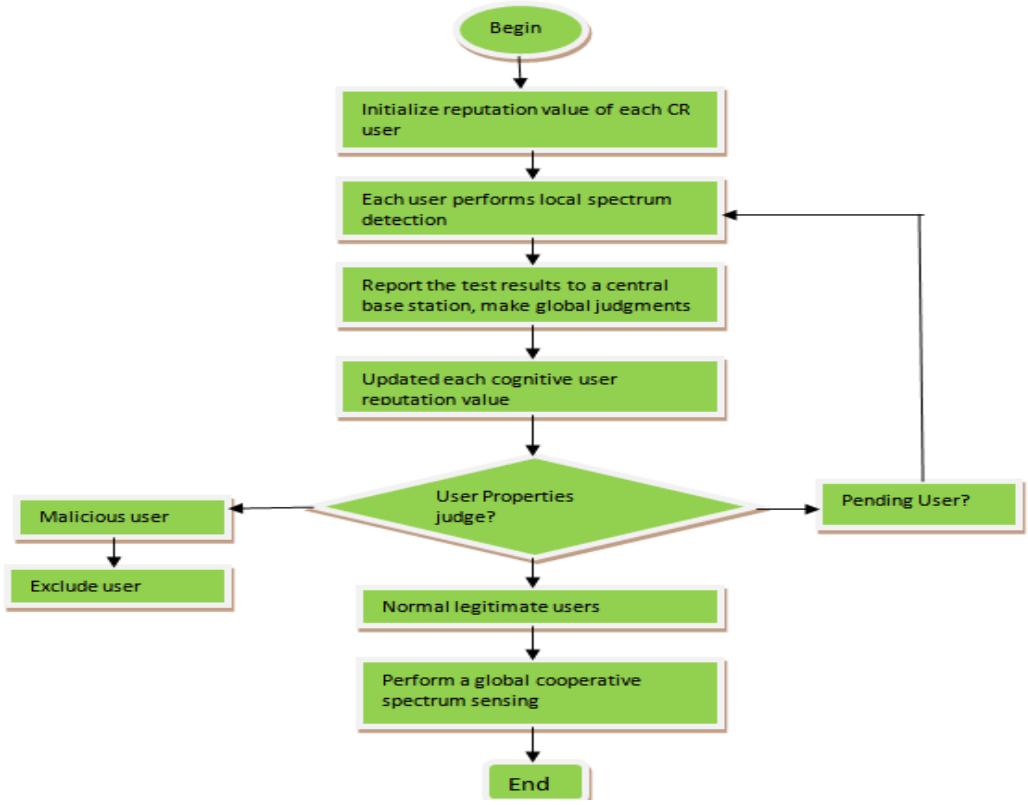


Figure 26: Credibility based defense scheme and malicious user removal

By seeing the flowchart of the algorithm it is evident that it has low complexity because MUs are eliminated as their credit value drops below threshold. It also upgrades the CSS accuracy because only trusted users having high trust value takes part in CSS. But this algorithm has disadvantage that only limited attack types are tackled.

2.4 Network layer Attacks

Network layer is in charge for delivery of data from a node of a network to another network node with quality of service maintenance. Every node has a routing table maintaining information of its neighbor nodes. Before sending

the data every node checks best path towards the destination by seeing its routing table. A malicious node may share wrong information with its neighbors or route the packets to undesired destination. The CRNs' security issues are shared with wireless networks because of shared architecture if infrastructure, mesh and ad-hoc network. As in CRN a SU has to vacate the channel as PU is sensed present, this makes routing more complicated. Therefore, due to some architectural requirements CRN is inherited to security vulnerabilities. Attacks related to network layer are briefly discussed as follows.

2.4.1 Sinkhole Attack

Multi-hop routing is often used by CRN. Multi-hop routing has been exploited by sinkhole attacker by showing itself best route towards the destination. Definitely the neighbor nodes will chose the best path for forwarding their packets. Infrastructure based and mesh networks are more prone to sinkhole attack because all the traffic from network must pass through base station. Outside sinkhole attacker can be avoided by encryption and authentication of data link layer. An outsider will not be able to enter in the network by using authentication. In CRN only members are allowed for routing, outside attacker will not be able to show itself as finest route [15]. A continuous update of trust can be used for countermeasure of inside sinkhole attacker. A separate entity may be used to report the FC for changed and dropped packets. After investigation the FC inform all the members about recent issues. In this way the malicious node is dropped from community. Security aware ad-hoc routing may also be used for keeping away from inside attacker [68].

2.4.2 HELLO flood Attack

In such type of attack, the MU broadcasts a HELLO message having high power showing than other nodes as their neighbor. If they send their packets through this node, packets will be lost because it is not neighbor node rather it the far and malicious node. The attacker may not capable of reading the data packets but only captured overhead packets are rebroadcasted with high power to all nodes. Attack can be avoided by authenticating bi-directional links for the received message on the same link before using the link. Bi-directional verification can be achieved by session key provided by a third party or FC. An alarm is generated if a node claims that it is neighbor of excessive nodes [15].

2.4.3 Wormhole Attack

The wormhole and sinkhole attack are related to each other. Attacker tunnels the message from one network part over low latency of the network. Another part of network is used to replay these messages. A simple example is that a node between two other nodes is used to communicate among two other nodes. Basically two malicious nodes administer the wormhole attack that minimizes the distance among them, by relaying data packets towards an out-of-bound path that is un-reachable for other users. Attack is shown in figure 27.

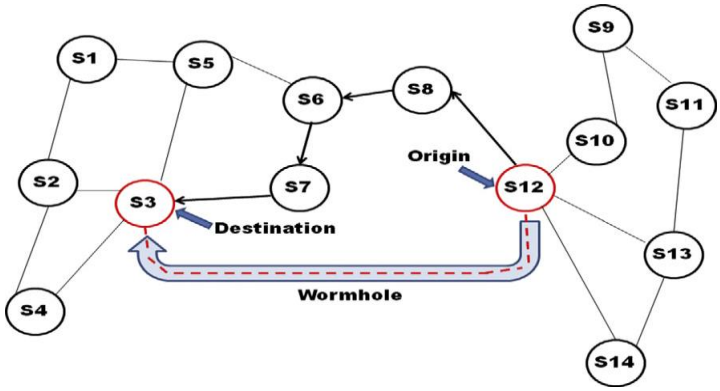


Figure 27: Wormhole Attack Model

2.4.4 Ripple effect

During communication changing the channel makes CRs vulnerable to a new type of attack named ripple attack. This channel changing nature of CRN makes them able to avoid interference with PU and take benefit from best channel according to their requirements. Ripple attack resembles to PUEA or SSDF attack because it convince the other users to change their channel by sending them incorrect channel information. The aim of ripple attacker is to put the system in a confusion state by passing incorrect information from one hope to another hope. The attack is possible only when attacker's signal power is high the reason behind it is that:

1. PU's activity is greater that SU, therefore arrival of PU may severe affect the communication of SU.
2. For changing the channel SU has to append time and energy for finding some other vacate channel.
3. Ripple effect may be caused due channel changing of one SU, or cascaded changing of more secondary users [68].

Defense for ripple effect is same as for SSDF or PUE attack. It is significant to validate and distinguished presence of PU.

It is also necessary to validate the information passed by neighbor about the presence of PU. This will results the switching of channel only when required by validating that a licensed cannel is vacated.

2.4.5 Sybil Attack

This attack exploits the availability parameter of the network. In this attack, the attacker sends packets to different identities causing down the system trust value. It has a large effect on the overall system performance. Sybil attack can be avoided by validating each node.

2.5 Transport Layer Attacks

Transport layer performs error recovery, congestion control and flow control. This layer is also prone to several security threats.

Key depletion is the major attack on this layer. In CRNs duration of transport layer session is very small because of large round trip time and commonly retransmission of data. This thing impels to generate more sessions. In most of the protocol of transport layer, transport layer security, secure socket layer create cryptographic keys for each session at the beginning. If session key is generated for every session then it is most probable that keys may be repeated and can cause exploitation of system security. Protocols such as WEP and TKIP are prone to this type of attacks. CCMP protocol has been designed to reduce this key repetition. This system reduces the vulnerability to these repetition attacks.

2.6 Application Layer Attacks

Closest layer to end user is application layer. The application layer and user

both have to interact with application software. Finding the resources availability, detecting devices for communication and communication synchronization are major responsibilities of application layer. CRs need more capacity, memory and processing power than those conventional smart phones. This is due to more tasks performed by CR, such as learning and sensing. Therefore, CRs are vulnerable to software malware and viruses. Quality of service is also degraded because of spectrum handoffs, attacks of network layer and delays introduced by recurrent key changes. Quality of service is main concern of application layer.

2.7 Cross-layer Attacks

Cross layer attacks affect to multiple layers of CRN. Such type of attacks can degrades the whole network performance, spectrum sensing, spectrum decision and spectrum analysis. All attacks described above can be cumulatively used to launch cross-layer attacks. For cross layer attacks, adversary launches the attack at one layer while it badly affects the other layer. Performance of data link layer often affected by cross-layer attacks at physical layer. All cross layer attacks exploit the availability parameter of security standards. Jamming of routing information is also this kind of attack which takes the advantage of spectrum handoff delays. These delays can jam the information of routing between neighbors. The consequence is wrong routing of data packets and stale routs. Another cross-layer attack is small back off window (SBW). This is possible for CRNs at data link layer with protocol Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The attacker’s aim is to gain unjust admittance to the channel for which parameters of contention protocol are manipulated. A very small contention

window has been chosen by MU to achieve more access to channel [15]. Lion attack is also cross-layer attack occurs at data link or physical layer and affecting transport layer. In reality, the attacker launches PUE attack to disturb the TCP connection. This attack may be active or passive. Due to PUEA handoffs occur and affect the performance of TCP, TCP in not aware of handoff and switchover and continue to create connections and send packets without receiving acknowledgment. This results in reduction of congestion window and retransmission of packets. The consequence is reduced throughput, packet loss and delays. One more attack similar to lion attack is jellyfish attack. Both these attacks affect TCP but the only difference is that lion attack affects the TCP due to recurrent handoffs. While in case of jellyfish attack, dropped, out of order and belated packets cause the degradation of TCP.

SYSTEM MODEL AND PROPOSED SOLUTION

3.1 System Model

The basic network of CR comprises of a number of SUs, Pus and FC. For simulations and simplicity a typical network consisting of a few SUs, one PU and one FC has been taken into consideration. By using a collaborative SS data fusion rule, and all the secondary nodes send sensing data in the form of binary one or zero to the centralized FC. Then at FC Fuzzy Logic (further discussed in detail) is used to take the final conclusion regarding the presence of PU. Collaborative SS in typical CRN is shown in figure 28.

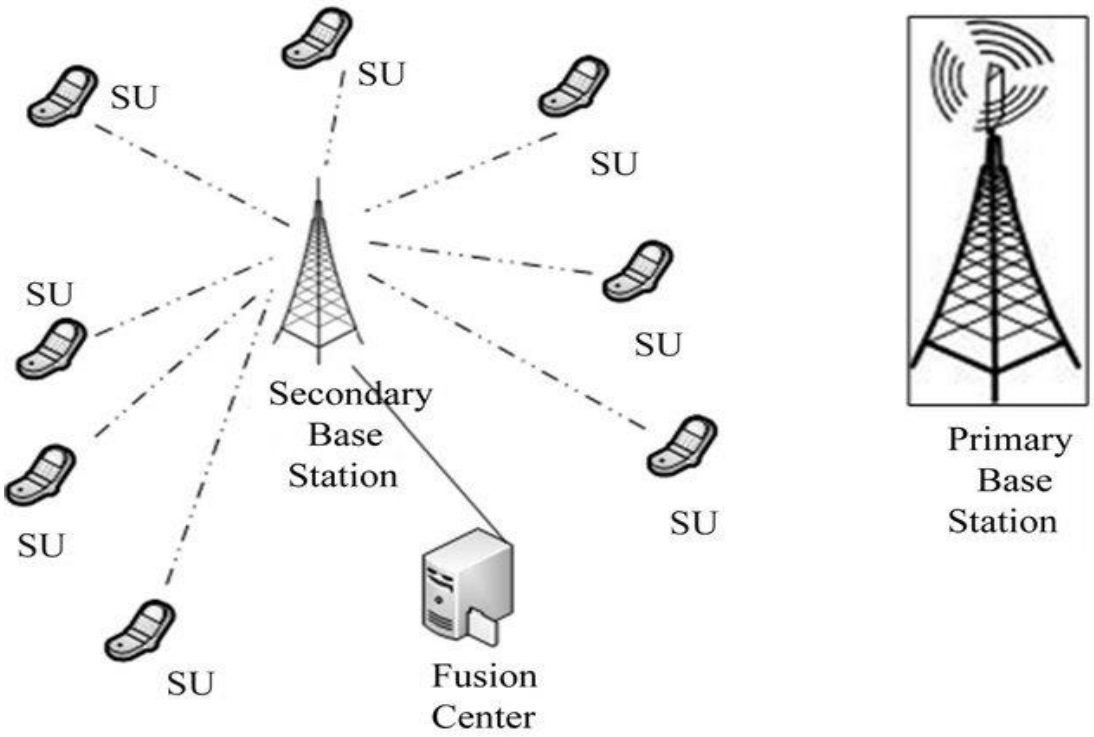


Figure 28: A Typical CRN with Collaborative SS

Suppose the signal transmitted by PU is T_P, which is completely considered as random signal consisting sequence of binary samples. So we can present the random signal as given below

$$T(1, K) = \text{Rand}(1, K) \quad \ldots (3.1)$$

Where T (1, K) is the symbol for random sequence having length K. The signal T_P (1, K) to be transmitted can be articulated as

$$T_P(1, K) = T(1, K) > \mu \quad \ldots (3.2)$$

Where μ is threshold. The signal T (1, K) would be transmitted on the basis of this threshold. If the threshold is less than T (1, K) transmitted signal would be 1 else 0. In our system model all SUs detect the presences of PUs in a way that they scan the signal by PU, calculating the signal energy level and make a comparison with pre-defined threshold. If calculated energy is greater than threshold μ, SU reports the FC that PU is existing and in other case if energy is less than μ zero would be reported to the FC showing absence of PU. Suppose that the energy calculated at the K_{th} time instance, by nth SU is E (n, K). And at any time instance K, R_x (n, K) be the received signal by nth SU. Random noise along with variance would be added in every received signal. Hence the received signal can be formulated as

$$R_x(n, K) = T_P(n, K) + \text{Noise Variance} \quad \ldots (3.3)$$

And the energy calculation for the received signals can be as following

$$E(n, K) = |T_P(n, K) + \text{Noise Variance}|^2 \quad \ldots (3.4)$$

$$E(n, K) = |R_x(n, K)|^2 \quad \ldots (3.5)$$

Let the decision reported to the FC by nth SU based on the received signal is

presented by r (n, K). It will be consisting of a binary sequence, which each SU reports. We have taken a group of five SU's under following categories:

- Smart MU
- Always NO
- Always YES
- Honest Users

The users reporting the correct decision are named as honest users. For the sake of simplicity and more clarity the secondary users can be defined in this way:

$$r(1,K) = 1 - T_P(1,K) \quad ...(3.6)$$

$$r(2,K) = 0 \quad ...(3.7)$$

$$r(3,K) = 1 \quad ...(3.8)$$

$$r(4,K) = T_P(1,K) \quad ...(3.9)$$

$$r(5,K) = T_P(1,K) \quad ...(3.10)$$

We can write the signal transmitted by PU and decision reports by SU in the matrix form as given below:

T_p= [1 1 0 0 0 1] PU's signal

$$r(n,K)=\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

The number of row are showing the SUs and columns showing the time slots of sensing.

Where, r (1, K) is smart MU, r (2, K) & r (3, K) are Always NO and always YES respectively and r (4, K) & r (5, K) are honest users.

3.2 Proposed solutions and motivation towards Fuzzy Logic Based solution

3.2.1 Least Mean Square (LMS) Algorithm

Least mean square algorithm is the most famous algorithm that is being used for the adaptive filtering. It works on the same principle as steepest descent method and statics are assessed continuously. Our main goal is to tackle with such problems in which information is not known. Since in LMS algorithms the statics are assessed continuously, the changes in signal statics are adapted accordingly. In this way LMS algorithms is used in place of adaptive filter. It parodists as required filter by calculating filter coefficients to generate the lease mean square error for the signal (difference among required and actual signal is squared). This algorithm was introduced by Professor Bernard Widrow from Stanford University and Ted Hoff one of his PHD student in 1960 [71].

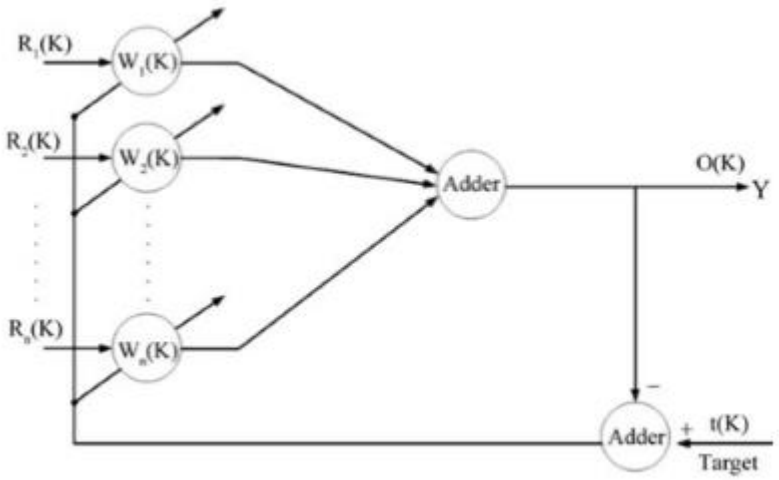


Figure 29: LMS Algorithm

$$e(i,k) = T(i,k) - Y(i,k) \quad \text{… (3.11)}$$

$$Y(i,k) = W(i,k) * Y(i,k) \quad \text{… (3.12)}$$

$$W_{(i,k+1)} = W(i,k) + \mu * e(i,k) * R(i,k) \quad \text{… (3.13)}$$

μ is leaning rate and its value is between 0 and 1. After Training of the network the plot is given in figure 30.

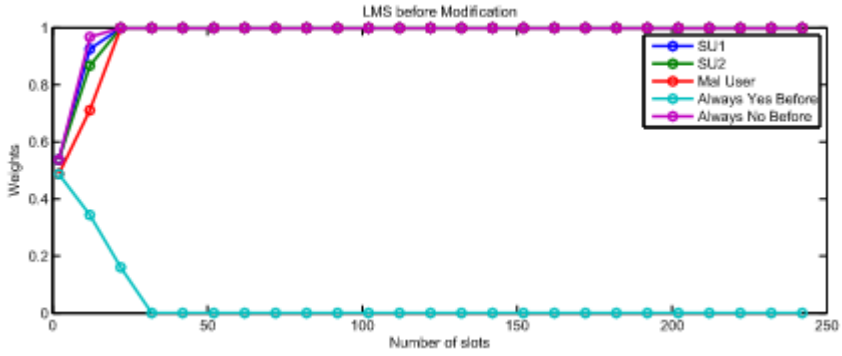


Figure 30: LMS Malicious Node Detection

Output against every secondary users are mapped as R (i,k) where 0 mapped

against -1 and 1 mapped against 1.

$$R(i,k) = 2r(i,k) - 1 \quad \text{… (3.14)}$$

This is obvious from above graph that LMS algorithm in its original form can identify only always yes malicious user accurately. Always No and smart malicious user is not being identified by this algorithm. If we modify the weight update equation then Always No and smart malicious user can also be identified. Modified LMS algorithm can identify all three malicious users that needs to be detect in our proposed model.

3.2.2 Modified Least Mean Square Algorithm

We have seen that LMS algorithm in standard form is able to detect only Always Yes malicious user. The weight update equation for LMS is given below:

$$W_{(i,k+1)} = W(i,k) + \mu e(i,k) R(i,k) \quad \text{… (3.15)}$$

If we introduce slighter modification in this equation then it can be used to detect all type of malicious users (Always Yes, Always No and Smart Malicious Users).

The weight update equations are modified as following:

For honest users

$$W_{(i,k+1)} = W(i,k) + |\mu e(i,k) R(i,k)| \quad \text{… (3.16)}$$

For Malicious users

$$W_{(i,k+1)} = W(i,k) - |\mu e(i,k) R(i,k)| \quad \ldots (3.17)$$

after these modification in weight update equations, it has been observed all three malicious users are correctly identified as shown in below figure 31.

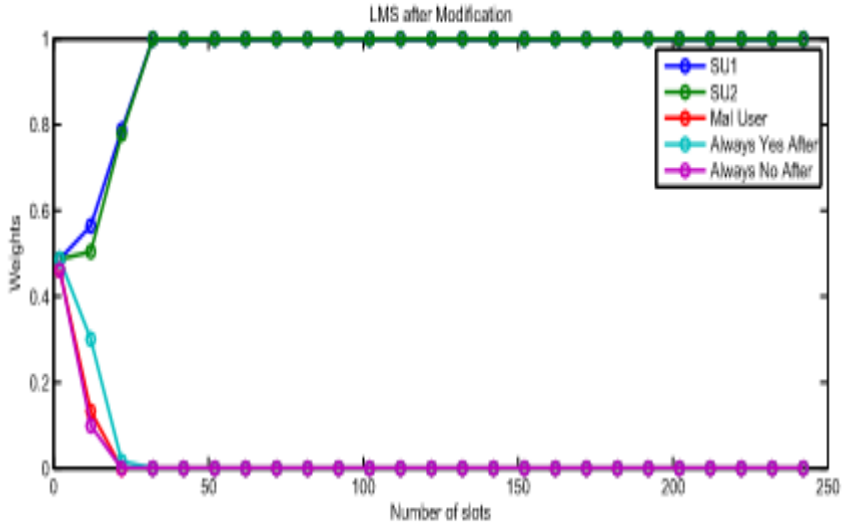


Figure 31: Detection with Modified LMS Algorithm

LMS algorithm has simplicity in implementation, stable and vigorous against different conditions of signal. But it has a disadvantage that is, having very slow convergence.

3.2.3 Feed forward Neural Networks

Feed forward Neural Network is used for solving problems on a large scale. They have been extensively used in financial prediction, protein structure prediction, medical diagnose, image processing and speech recognition. Minimum three number of layers are used in feed forward neural networks, An Input, Output and hidden layer as shown in figure given below. The number of hidden layers depends on the nature of problem we are going to solve. Steepest Descent or gradient descent method is being used for training of the

SUs.

Suppose $R1$, $R2$, $R3$, $R4$ and $R5$ are mapped decisions (0 mapped with -1 and 1 mapped with 1) for the binary reports that SUs send to FC after sensing. u1, u2, u3, u4 and u5 are supposed to be weighted inputs to neuron 6,7,8,9 and 10.

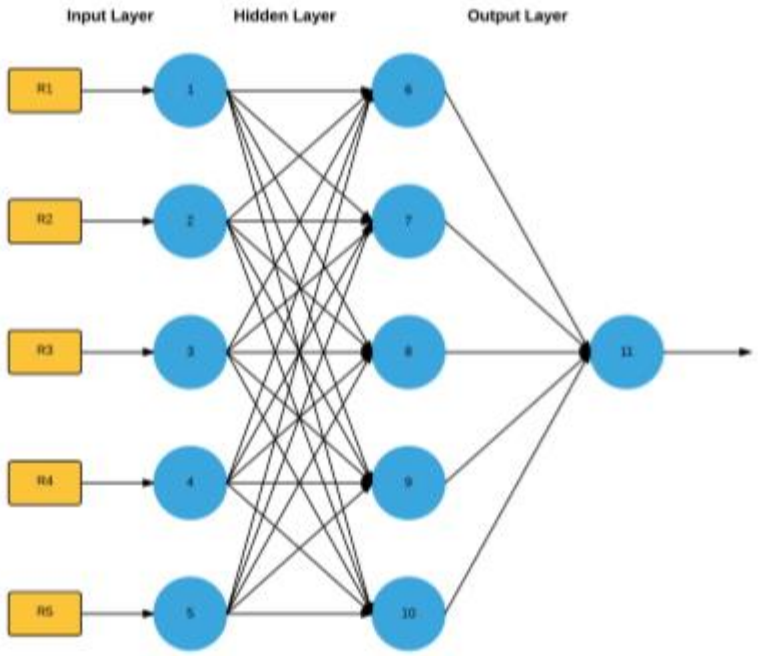


Figure 32: Feed forward Neural Network

These inputs are calculated by using equations as follows:

$$u_1 = R_1 W_{(1,6)} + R_2 W_{(2,6)} + R_3 W_{(3,6)} + R_4 W_{(4,6)} + R_5 W_{(5,6)} \quad \ldots (3.18)$$

$$u_2 = R_1 W_{(1,7)} + R_2 W_{(2,7)} + R_3 W_{(3,7)} + R_4 W_{(4,7)} + R_5 W_{(5,7)} \quad \ldots (3.19)$$

$$u_3 = R_1 W_{(1,8)} + R_2 W_{(2,8)} + R_3 W_{(3,8)} + R_4 W_{(4,8)} + R_5 W_{(5,8)} \quad \ldots (3.20)$$

$$u_4 = R_1W_{(1,9)} + R_2W_{(2,9)} + R_3W_{(3,9)} + R_4W_{(4,9)} + R_5W_{(5,9)} \quad \text{… (3.21)}$$

$$u_5 = R_1W_{(1,10)} + R_2W_{(2,10)} + R_3W_{(3,10)} + R_4W_{(4,10)} + R_5W_{(5,10)} \quad \text{… (3.22)}$$

The compact form of u_i can be written as

$$u_i = Ri'W \quad \text{… (3.23)}$$

The output against each neuron would be like this

$$O_6 = \frac{1}{1+e^{-u_1}} \quad \text{… (3.24)}$$

$$O_7 = \frac{1}{1+e^{-u_2}} \quad \text{… (3.25)}$$

$$O_8 = \frac{1}{1+e^{-u_3}} \quad \text{… (3.26)}$$

$$O_9 = \frac{1}{1+e^{-u_4}} \quad \text{… (3.27)}$$

$$O_{10} = \frac{1}{1+e^{-u_5}} \quad \text{… (3.28)}$$

Input for neuron 11 can be formulated as

$$u_{11} = W_{(6,11)}O_6 + W_{(7,11)}O_7 + W_{(8,11)}O_8 + W_{(9,11)}O_9 + W_{(10,11)}O_{10} \quad \text{… (3.29)}$$

At neuron 11 final output would be

$$O_{11} = \frac{1}{1 + e^{-u_{11}}}$$

… (3.30)

This method for detecting the MUs in CRN is based on AI. The system is based on 5 users and a hidden layer as shown in below figure 33.

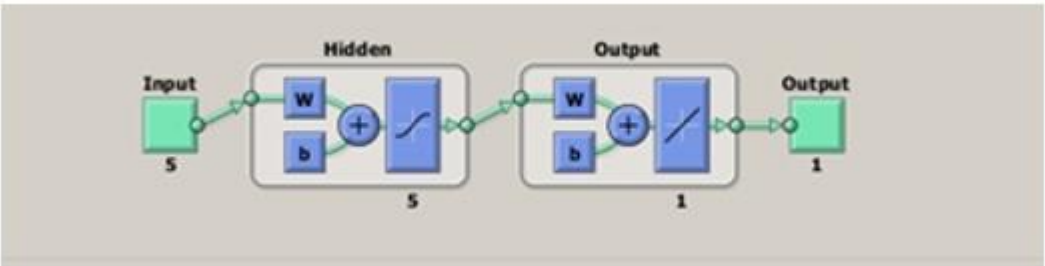


Figure 33: Neural Network having 5 inputs and 1 output

Neural Network is very good candidate for this problem where it is hard to present the problem in any mathematical form and the system behavior is also not deterministic. All types of malicious users aimed to detect in our problem are detected by using this algorithm. Neural network is good solution as compared to LMS and modified LMS in a way that it is more robust having fast learning of binary data but it has more complexity. And there are multiple learning algorithm that we can use any one of them based on the problem nature. But still there are some back holes like simplicity in implementation, more robustness, fast convergence and less complexity. We need all these things together, which gives us motivation to find another solution.

3.3 Motivation towards Fuzzy Logic Based Solution

For many reasons, Fuzzy Logic is a very suitable algorithm for securing the spectrum sensing. In CRNs there is no distinct boundary among honest and MU's. By using fuzziness nature of fuzzy logic, it will help to smooth the rapid

severance of abnormality and normality. Another motive for using fuzzy logic is diminution in probabilities of miss detection & false alarm. Below points are the major reason for selecting the Fuzzy logic for MU detection:

- Easy to implement by defining the rules according to the system environment
- Less complexity as compared to the other algorithms such as Neural networks
- More Robust as compared to the existed methods

3.4 Fuzzy Logic for Secure Spectrum Sensing and malicious user Detection

Dr. Lotfi Zadeh of Berkeley introduced Fuzzy logic in 1960's as mean for modeling of uncertainty for natural language [70]. Fuzzy logic is widely used for deploying efficient control systems. Fuzzy logic is a method to get precise and definite results and solutions based on an imprecise, unclear, missing or ambiguous input data. A fuzzy logic controller is shown in the below figure 33. Fuzzy Logic can be described in short in these steps: 1) Input values based on the system parameters needs to be analyzed. 2) Defining IF-THEN rules for the input values. 3) Results from all rules are combined to get a single value. 4) De-fuzzification the output to get a crisp value. In developing the Fuzzy Logic controller, Fuzzy rules and defining the Membership functions (MFs) for each Input/output is very important. Membership function shows the magnitude of every participating input in the graphical form. Based on these Input MF values Fuzzy Logic IF-THEN rules determine the output sets [70].

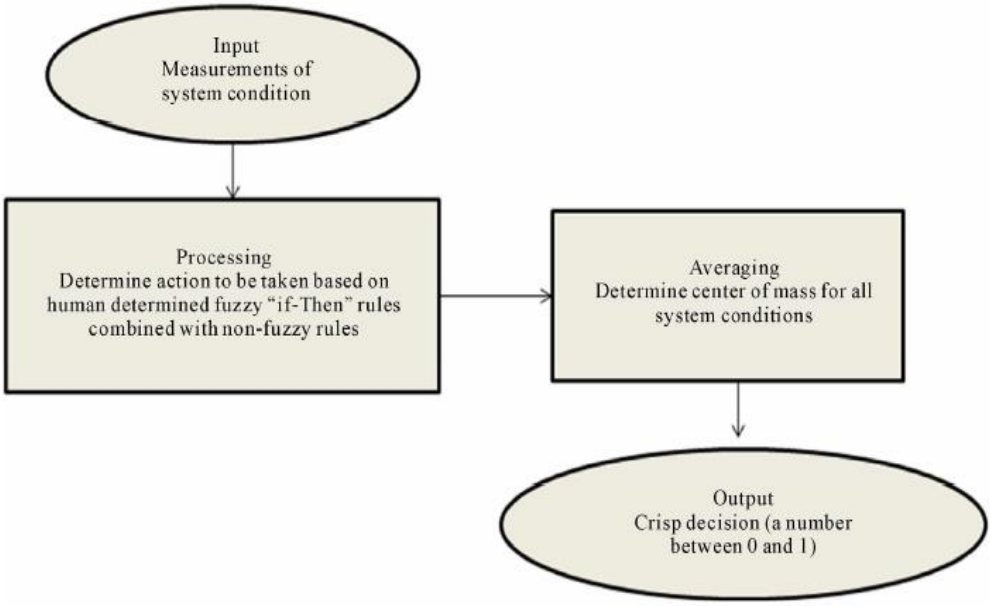


Figure 34: Fuzzy Logic controller Components

We are using the fuzzy controller at FC for the detection of MU's. In our system there will be two Input values for the fuzzy controller, one is average reputation value taken from training data and other is X-OR of real time sensing decision of a SU & decision known to FC. The scenario is shown in the figure 35.

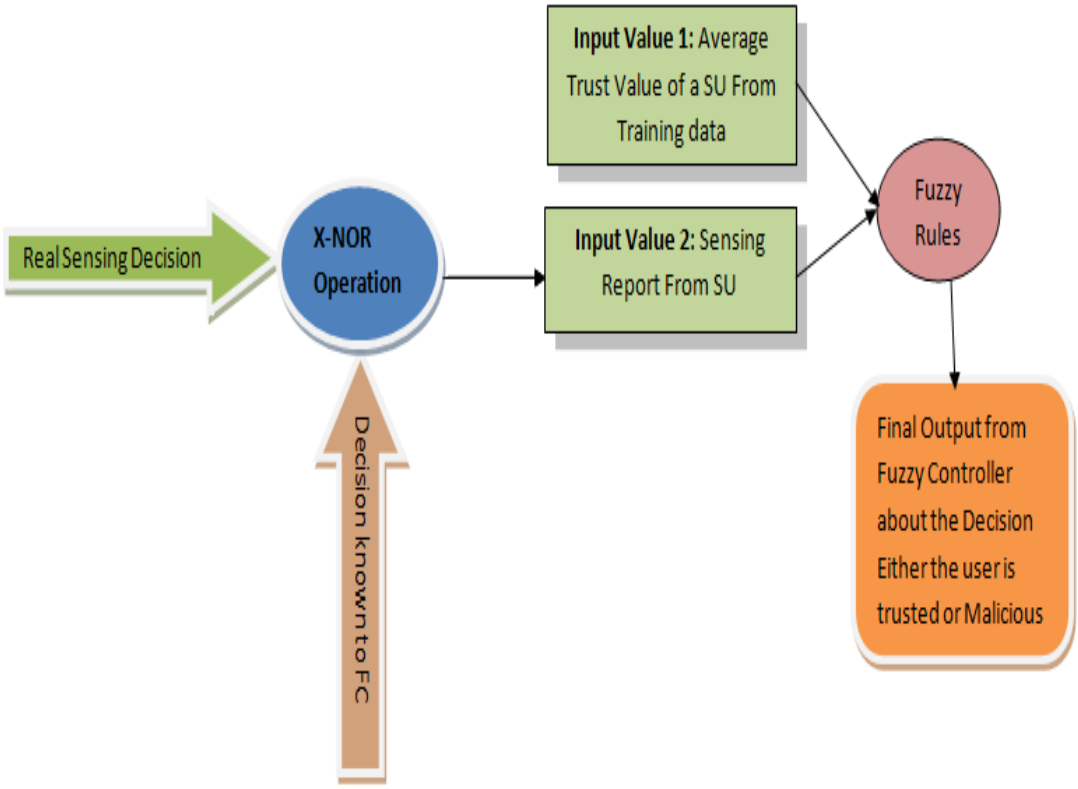


Figure 35: Proposed Solution using Fuzzy Logic for Malicious user detection

The working and implementation of proposed solution can be explained with the help of algorithm.

Algorithm:

There will be two inputs one is average trust value of each SU obtained from training data and second input will be real time sensing report. The final output is the decision about each SU either it is malicious or trusted user.

1. Computation of average Trust Value (ATV) for All Secondary users (Input 1)

Take inputs from Secondary users

Compare these inputs with FC data

Where i=0

While (i <= No of sensing trials)

IF (Decision of a secondary user==correct)

Trust Value (i+1)=Trust Value (i)+ Normalized Factor

IF (Decision==Incorrect)

Trust Value (i+1)=Trust Value (i) - 3.5 Normalized Factor*

i=i+1;

end While

Final Average trust value has been assigned to each user

2. Users' Decision from Real time sensing (Input 2)

Take real time input from users

Apply logical X-NOR operation on FC already known decision and real time user input.

Sensing Decision from Secondary user is computed

3. Inputs to the fuzzy Controller and fuzzy rules

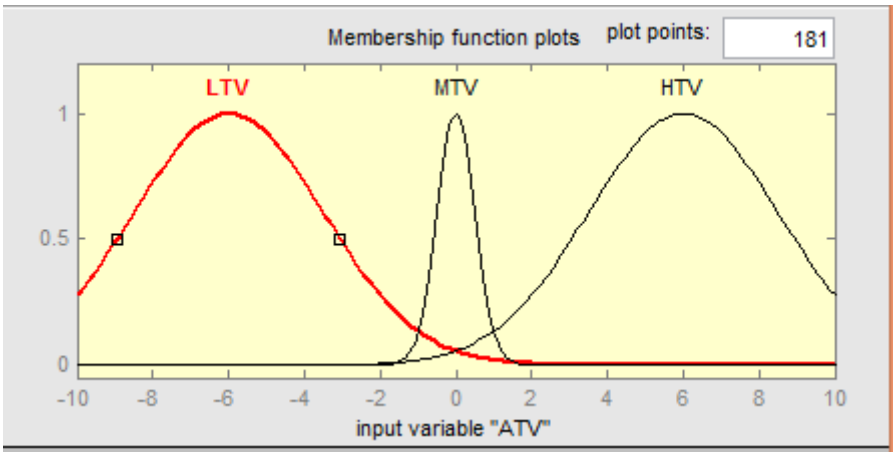
The above two Inputs are required to compute the fuzzy logic decision

i. *ATV*
ii. *SU's Sensing Decision*

Membership functions are defined for these inputs as shown in the below graphs.

Total four "IF and THEN" fuzzy rule are applied by fuzzy controller on these two inputs.

- 1. If (ATV is LTV) then (OD is ODO)
- 2. If (DFC is DFI) and (ATV is MTV) then (OD is ODI)
- 3. If (DFC is DFO) and (ATV is MTV) then (OD is ODO)
- 4. If (ATV is HTV) then (OD is ODI)



a) Membership function for Input 1 (Average Trust Value ATV)

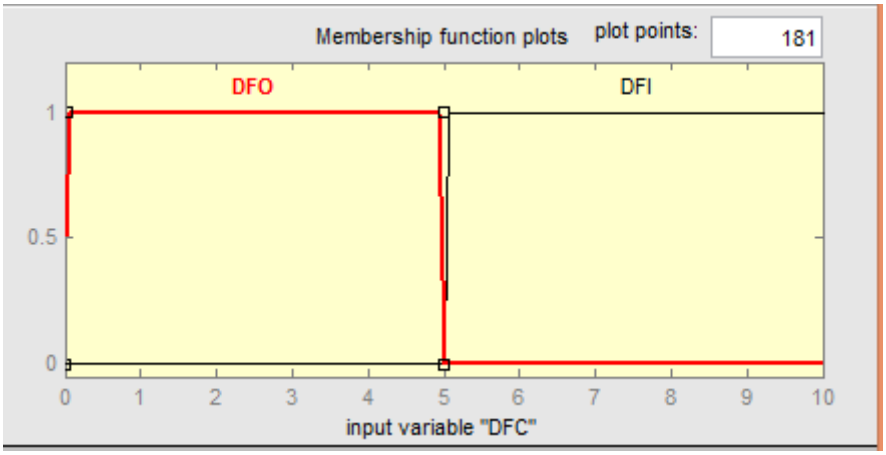


Figure 36: b) Membership function for Input 2 (SU's Sensing Report from real time sensing)

Final Decision is computed and every user is assigned a title trusted or malicious.

Three levels for ATV are given in below table 6 along with the fuzzy rule base table.

ATV	Value Range
High	0.7~1
Medium	0.4~0.7
Low	0~0.4

Table 6: Average Reputation Level Range

Average Reputation or Trust Value from Training data	Decision from Real time sensing	User status / Honest Or Malicious
High	1	Honest
High	0	Honest
Medium	1	Honest
Medium	0	Malicious
Low	1	Malicious
Low	0	Malicious

Table 7: Fuzzy Rules Base Table

The final output of the fuzzy controller is the decision about the SU, either it is honest or malicious. Fuzzy controller is ideal option for the given scenario, because of non-deterministic behavior and difficulty in presenting to mathematical form. MATLAB built-in GUI has been used for simulations.

Chapter 4

DISCUSSION AND RESULTS

In this chapter, results have been described using fuzzy logic and their short comings. A comparison has been made with neural networks, modified least mean square algorithms [71]. These three techniques have already been used for the same scenario as in our problem. It has been deduced from results that the proposed Fuzzy logic not only detects the MU but also reduce the false reporting effect. Our proposed method is robust, it detects the MU's even after introducing 20% false detection.

4.1 Malicious Node detection with LMS and Modified LMS algorithm

As we discussed earlier that, LMS algorithm in its pure form cannot detect all the MU's. Modified LMS can identify the behavior of all users, honest users have increasing trend of weights and malicious have decaying trend showing that Modified LMS algorithm can be used for malicious node detection as shown in graph, in figure 37. But it has disadvantage that, its convergence is very slow and it does not work well in case of false alarm and miss detection.

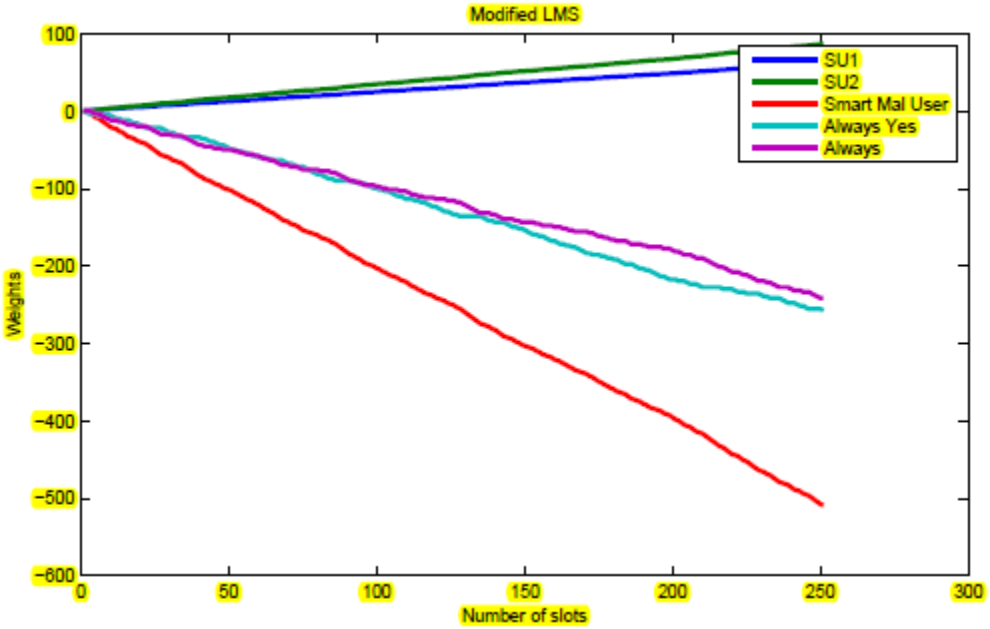


Figure 37: Final Weights using Modified LMS algorithm (1, 2 Honest Users) [71]

4.2 Malicious Node Detection using Feed- forward Neural Networks

This is already proposed algorithm used for secure spectrum sensing for the same scenario as discussed in our problem statement. Total five users, are taken for simulations 2 honest and three MU's. A sample Feed-forward Neural Network comprises of 5 inputs, 1 hidden layer having five neurons and 1 output layer is taken for simulations and below are assumptions and simulations parameters used.

No of Users (Neurons) = 5

No of Hidden Layers = 1

No of decisions = 250

Training function = Gradient descent

Learning rate μ= 0.025 (any value between 0 and 1 can be taken)

Simulations results have been taken using different cases and varying the number of malicious users. Total 250 decisions have been taken before taking final output [71]. The below graphs in figure 37 a & b shows, when the user 1 and 2 are trusted.

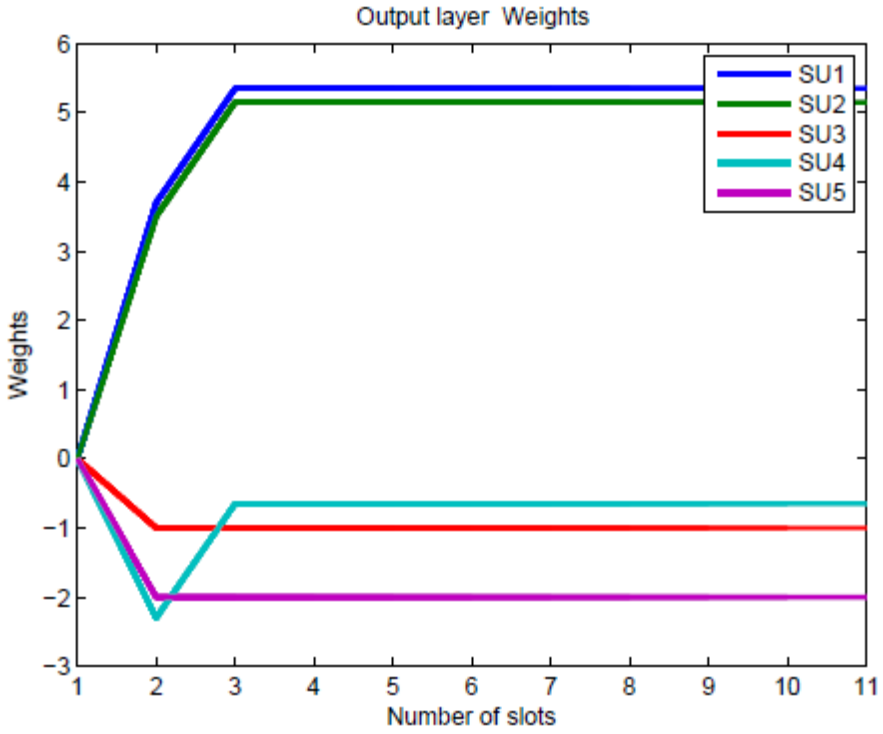


Figure 38 a): Output layer Weights (SU1, SU2 are trusted)

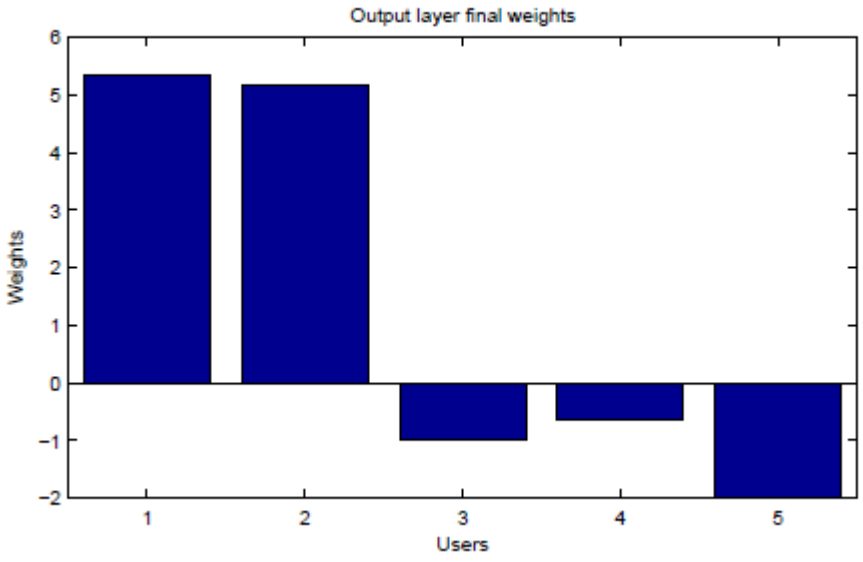


Figure 38 b): Final Weights of Trusted users

It is obvious Neural networks are better option as compared to Modified LMS algorithm. It even works very well if 10% Probability of false alarm and miss detection has been introduces. But on the other hand it is very complex regarding computations.

4.3 Results for fuzzy controller using Fixed Number of Honest Users

We have discussed the results for existing algorithms for LMS, modified LMS and Neural network. Now different cases using fuzzy logic will be discussed below.

Assumptions and Parameters for Simulations

Number of sensing time slots for training data= 20

Number of users= 5

Case 1: When SU1 and SU2 are Honest

In this case SU1 and SU2 are trusted and remaining three are malicious. Graphs in below figure 39 shows that, trusted users have increasing trend for average trust value and malicious have decaying trend. And based on these trust values fuzzy controller takes final decision about the behavior of each user and labels trusted or malicious. Percentage of error is zero in this case.

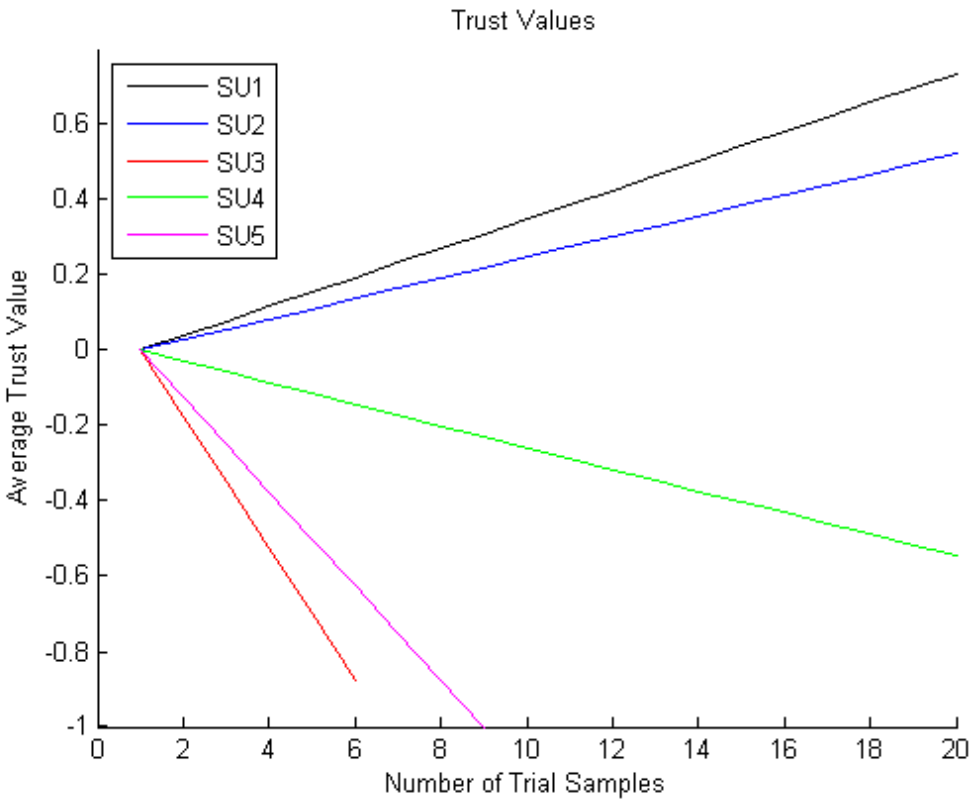


Figure 39 a): weights of the users from Training Data

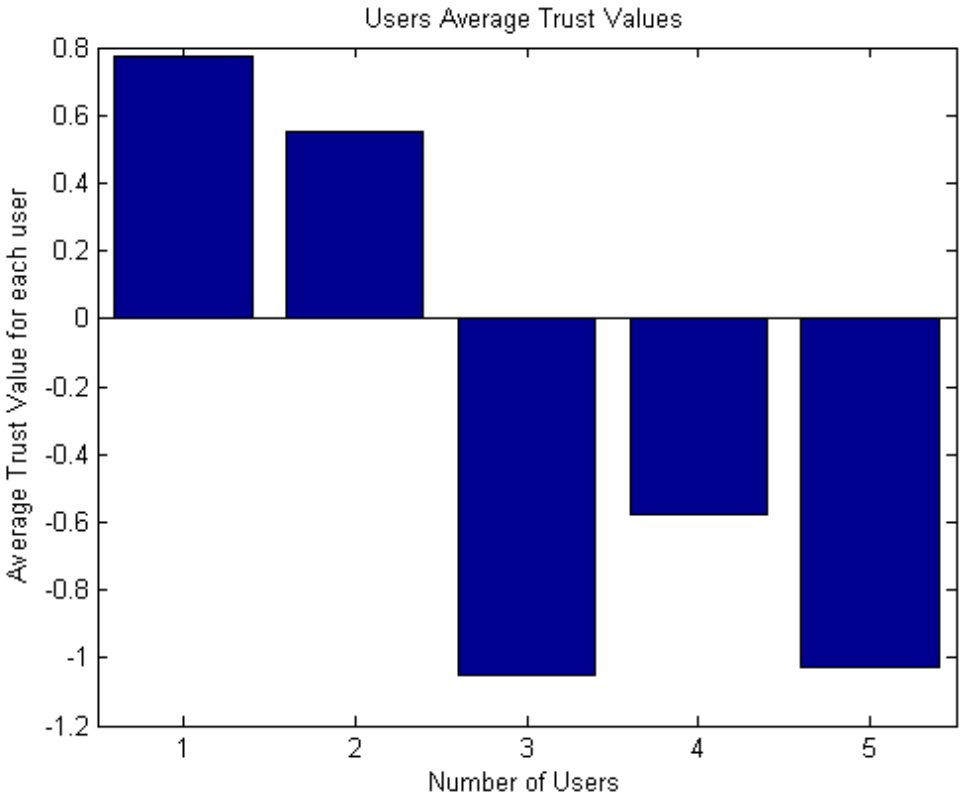


Figure 39 b): Average Trust Value Computation of Each User

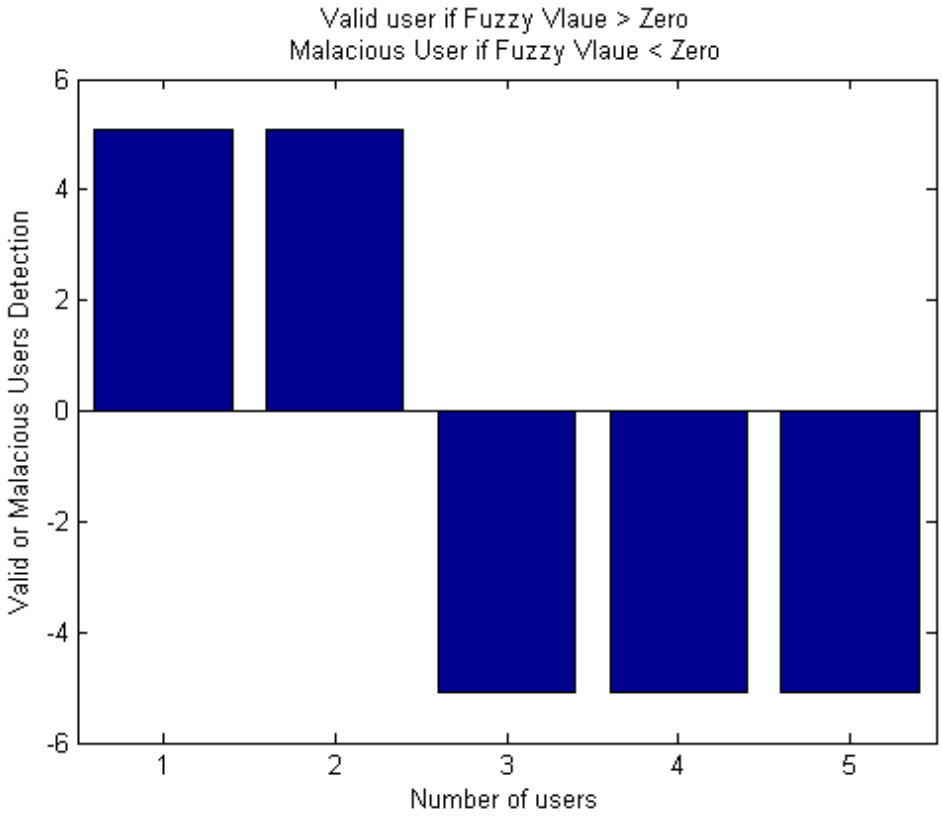


Figure 39 c): Final Decision of Fuzzy controller

Case 2: When SU3 and SU4 are Honest

In this case SU3 and SU4 are trusted, SU1, SU2, SU5 are malicious. There are three graphs in figure 40, first is showing the trust value of each user after their training. Second graph shows the results after average trust value computation. And third graph is showing the final decision about each user after applying fuzzy logic. It is obvious from the graphs that, fuzzy controller marked correctly each user according to its behavior. Percentage error is zero, probabilities of false alarm and miss detection are not introduced.

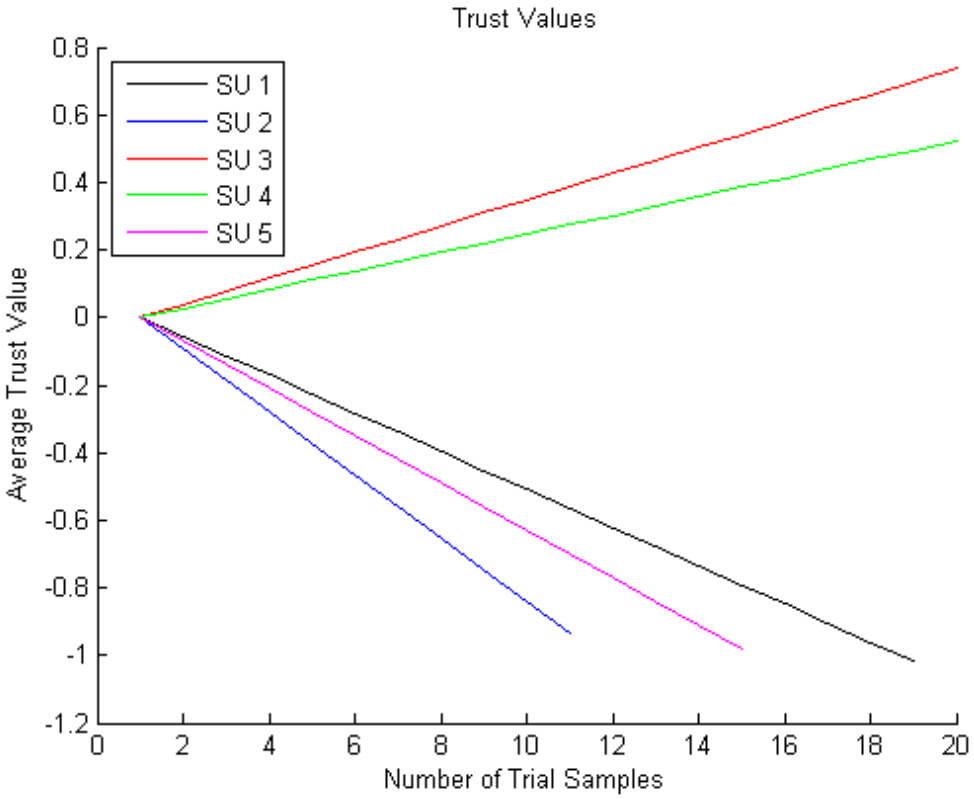


Figure 40 a): weights of the users from Training Data

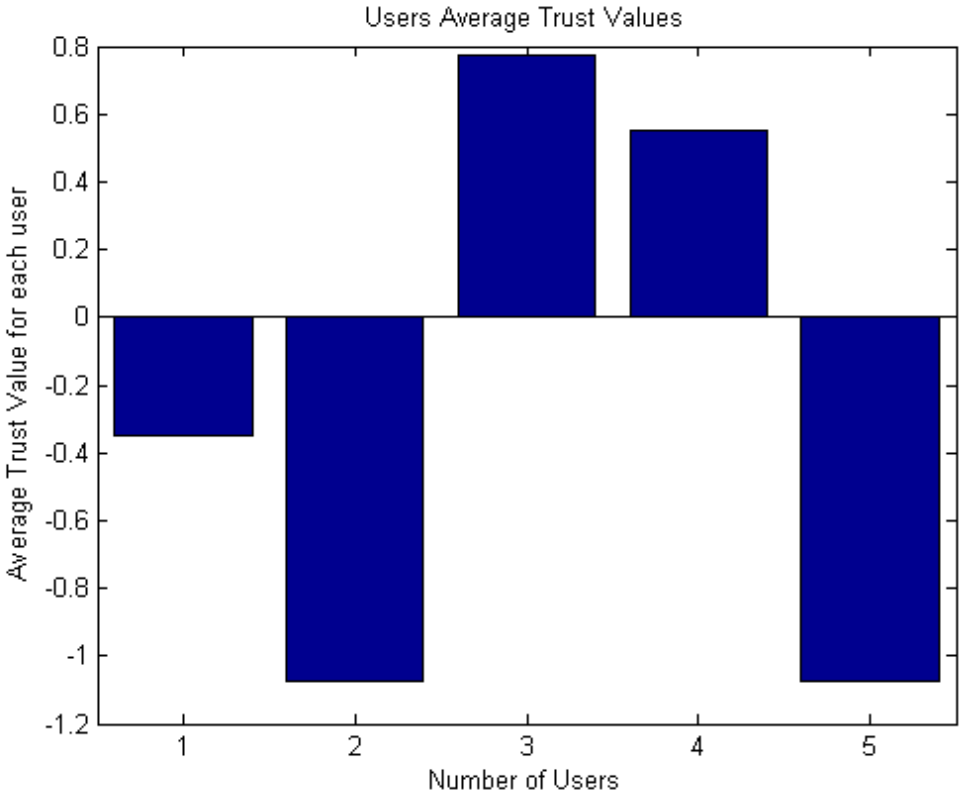


Figure 40 b): Average Trust Value Computation of Each User

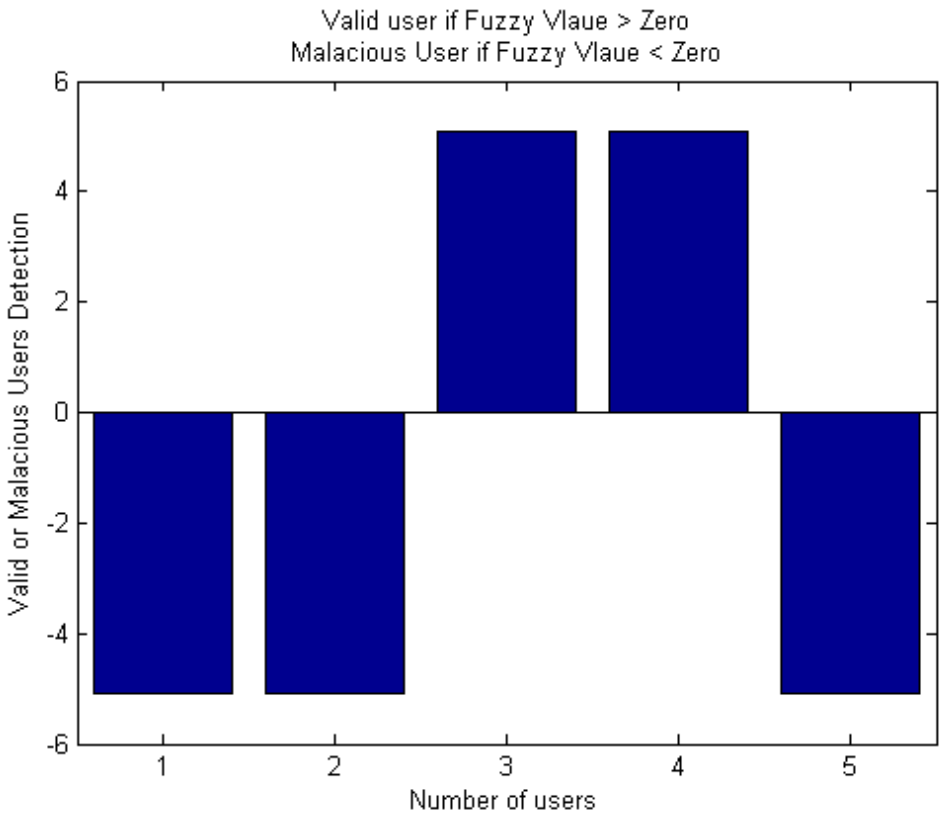


Figure 40 c): Final Decision of Fuzzy controller

Case 3: When SU1 and SU5 are Honest

For this case SU1 and SU5 are taken as trusted users and SU2, SU3 and SU4 are malicious. The graphs in figure 41 shows that trusted users have positive trends for weights, while malicious have decreasing trend. Fuzzy controller detects the malicious nodes and also weaken their effect.

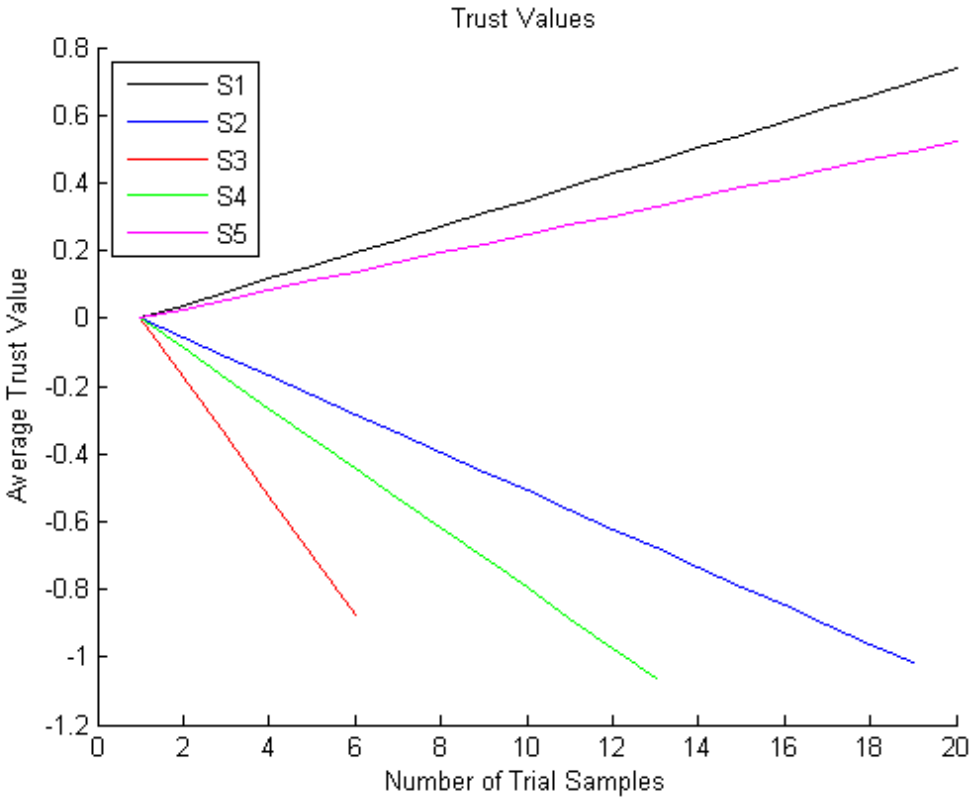


Figure 41 a): weights of the users from Training Data

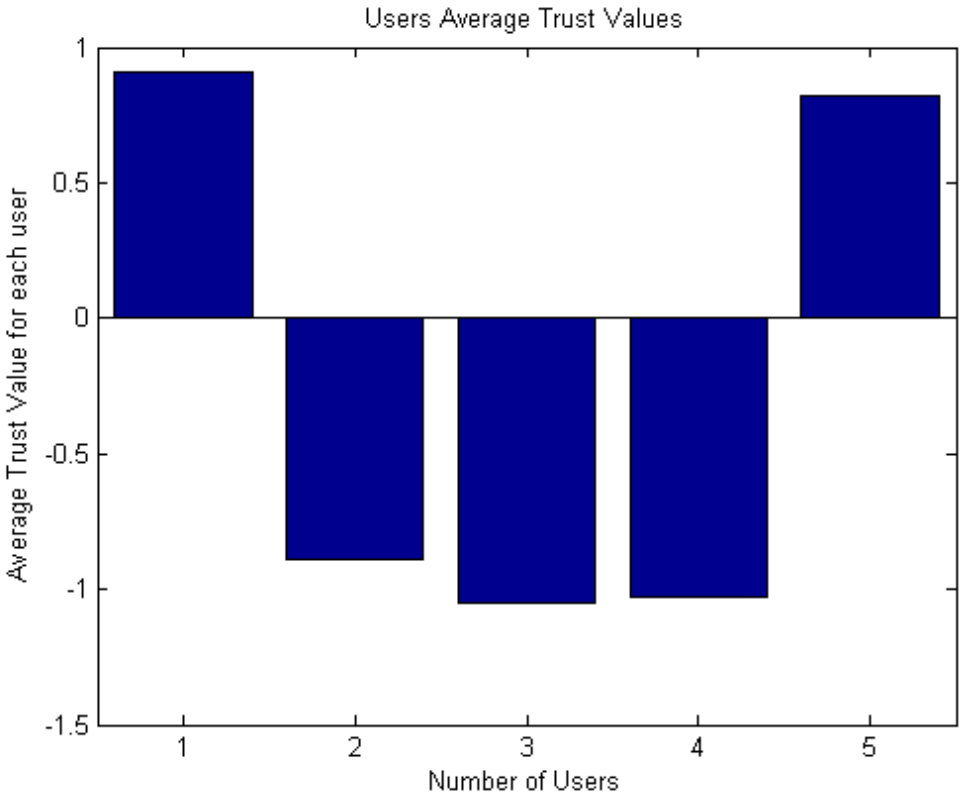


Figure 41 b): Average Trust Value Computation of Each User

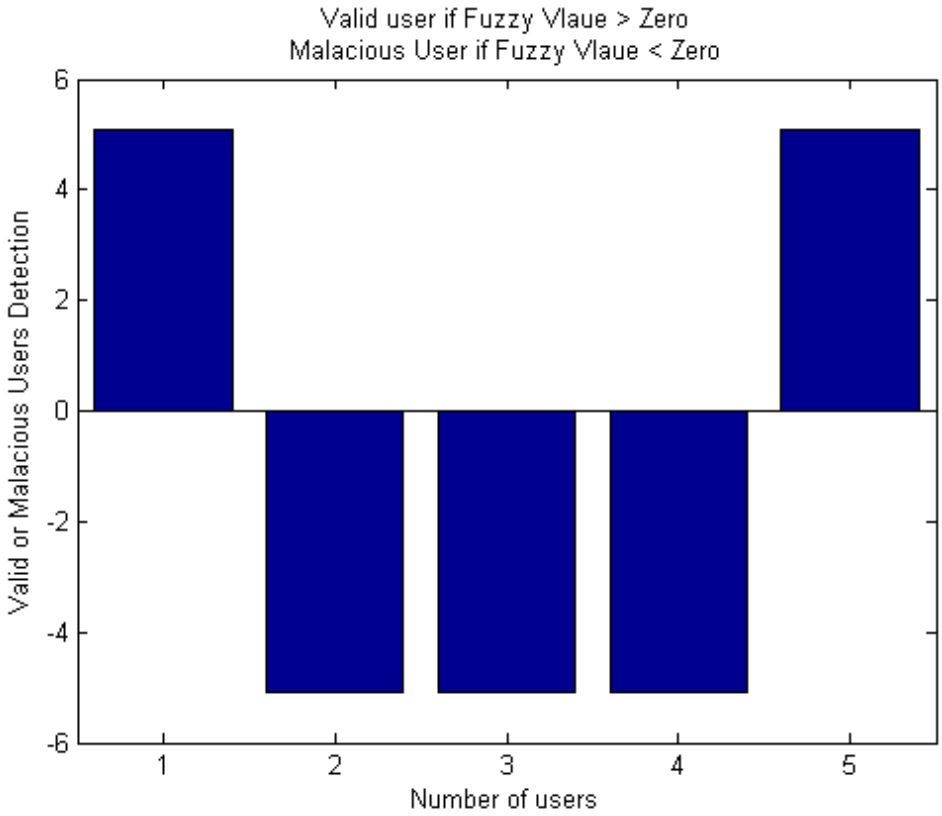


Figure 41 c): Final Decision of Fuzzy controller

Case 4: When SU4 and SU5 are Honest

For this case, same results have been obtained but SU4 and SU5 are honest and SU1, SU2 and SU3 are malicious. The percentage error is also zero same as for above three cases. The graphs in figure 42 shows that honest users have positive trend for weight update and on the other hand, malicious having negative trend. Graphs shows that fuzzy controller correctly detects all the users based on their behavior.

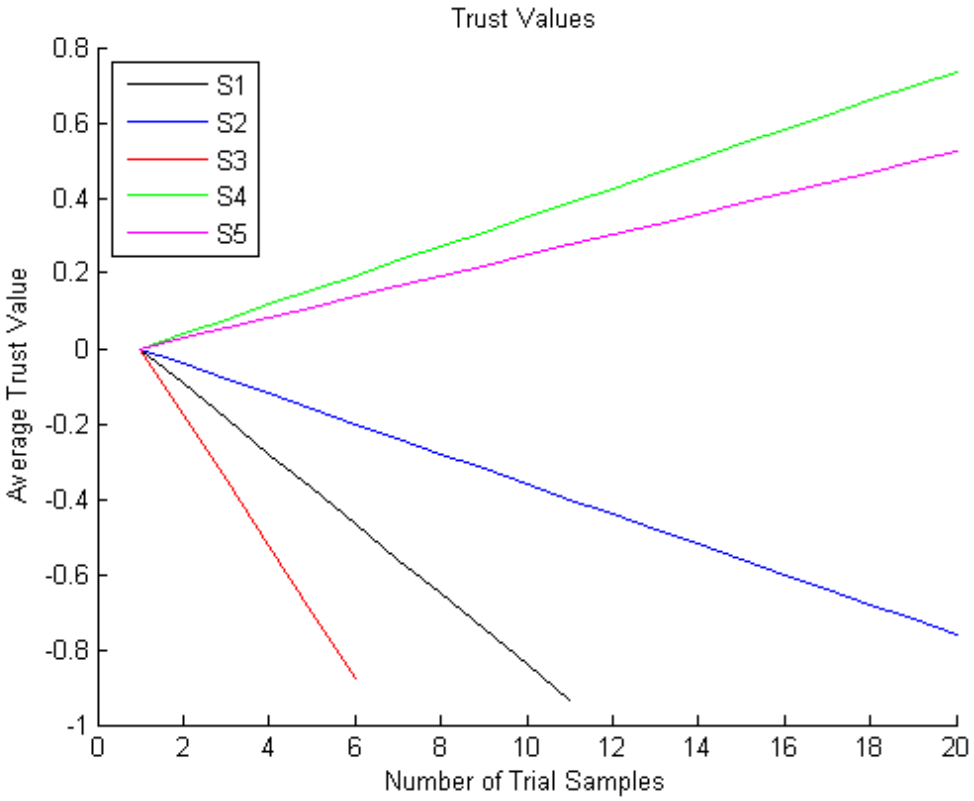


Figure 42 a): weights of the users from Training Data

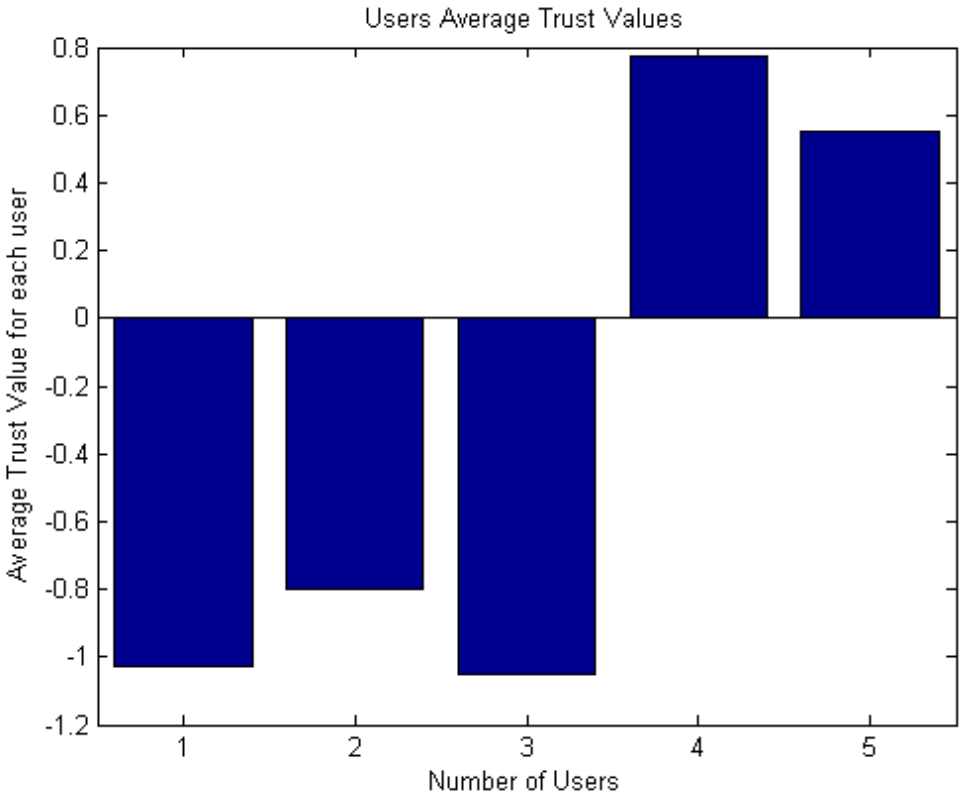


Figure 42 b): Average Trust Value Computation of Each User

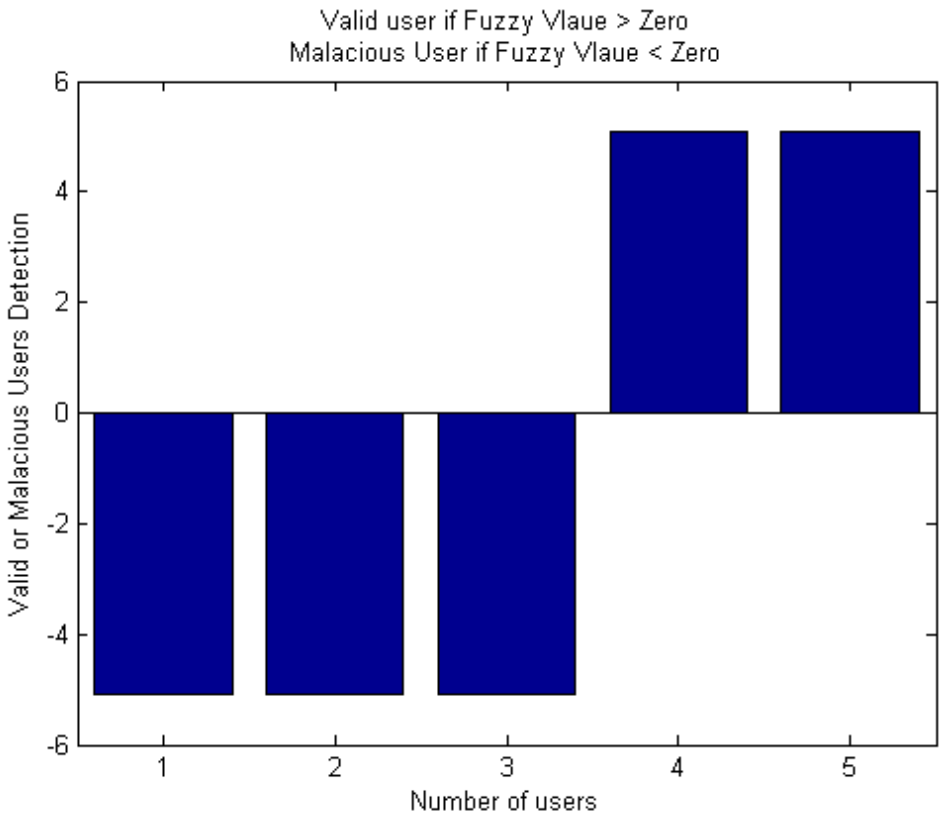


Figure 42 c): Final Decision of Fuzzy controller

Case 5: All SUs are Honest

In this scenario all the SUs are taken as honest and none of the user is malicious. The graphs in figure 43 shows that all users have positive trend for weight updates and average trust value. Percentage error is zero in this case, and fuzzy controller also marked all the users trust as shown in figure 43 c.

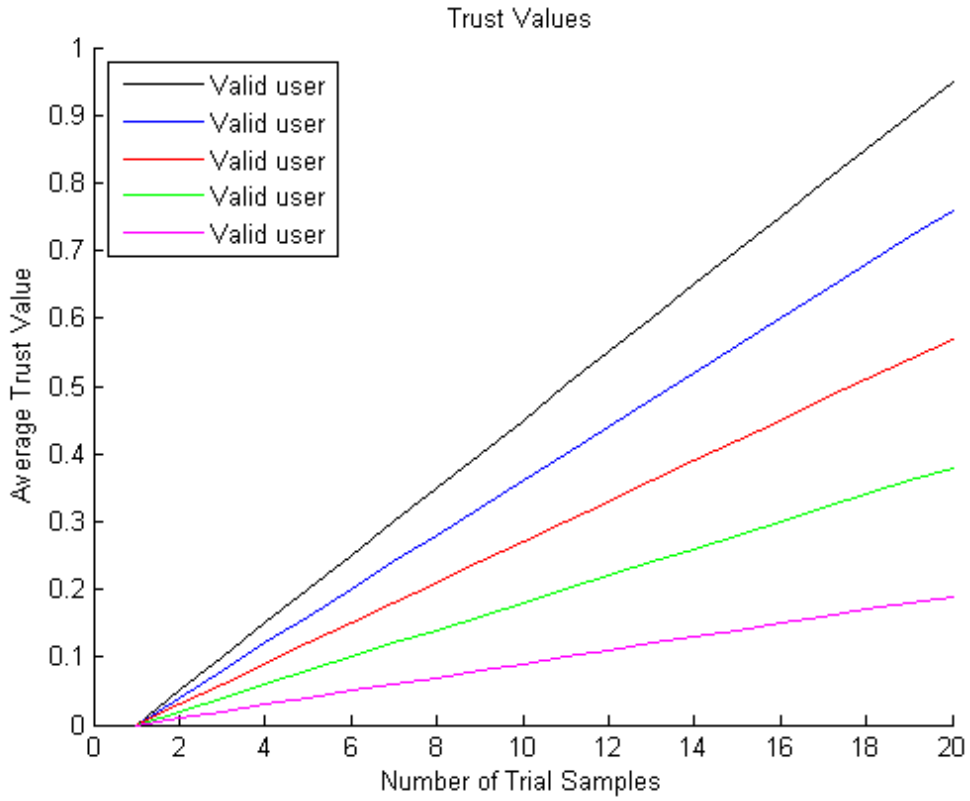


Figure 43 a): weights of the users from Training Data

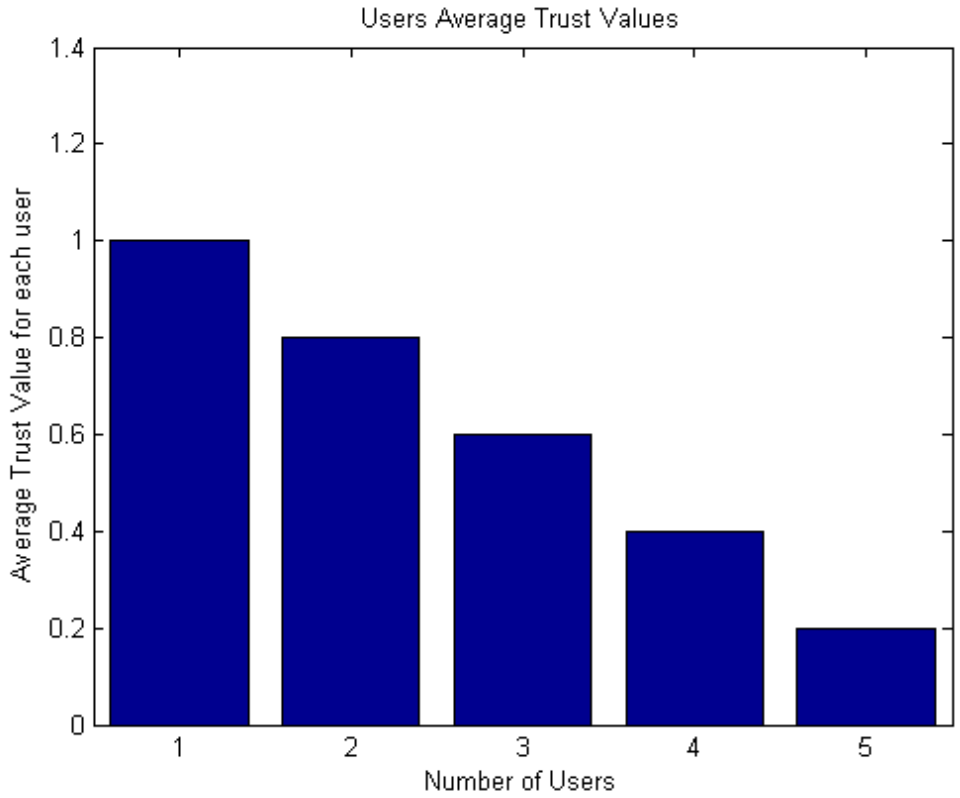


Figure 43 b): Average Trust Value Computation of Each User

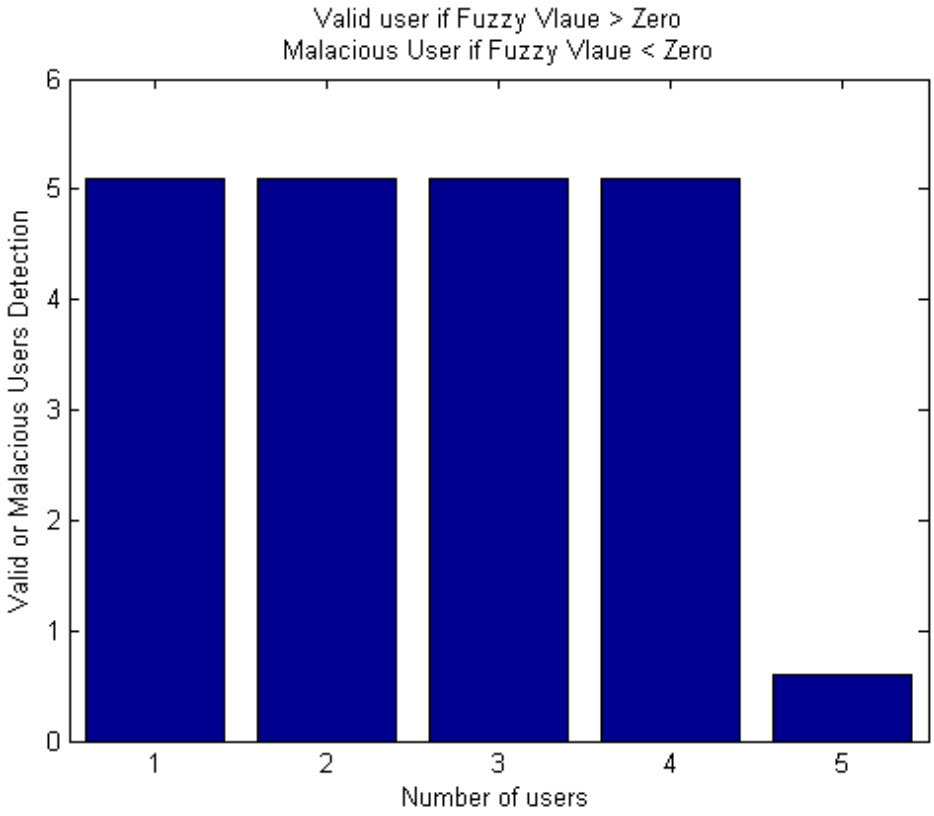


Figure 43 c): Final Decision of Fuzzy controller

4.4 Imperfect Sensing / Results after Introducing Probability of False Detection

5, 10, 15 and 20% probability of false detection has been introduced to honest user's data to check the robustness of the system. Below graphs shows that even after introducing the error our system is correctly detecting the honest and MU's correctly. Three cases have been taken under discussion with varying the probability of false detection for different honest SUs. Fixed 20 sensing slots are taken in each scenario.

Case 1: **5%** error for SU1 and **10%** error for SU2

In this case, SU1 and SU2 are trusted having **5%** and **10%** probability of false detection respectively. The graphs in figure 44 shows that even after

introducing probability of false detection, trusted users have increasing trend for their trust value. Finally fuzzy controller marked them as trusted users which shows proposed algorithm is robust against false alarm and miss detection.

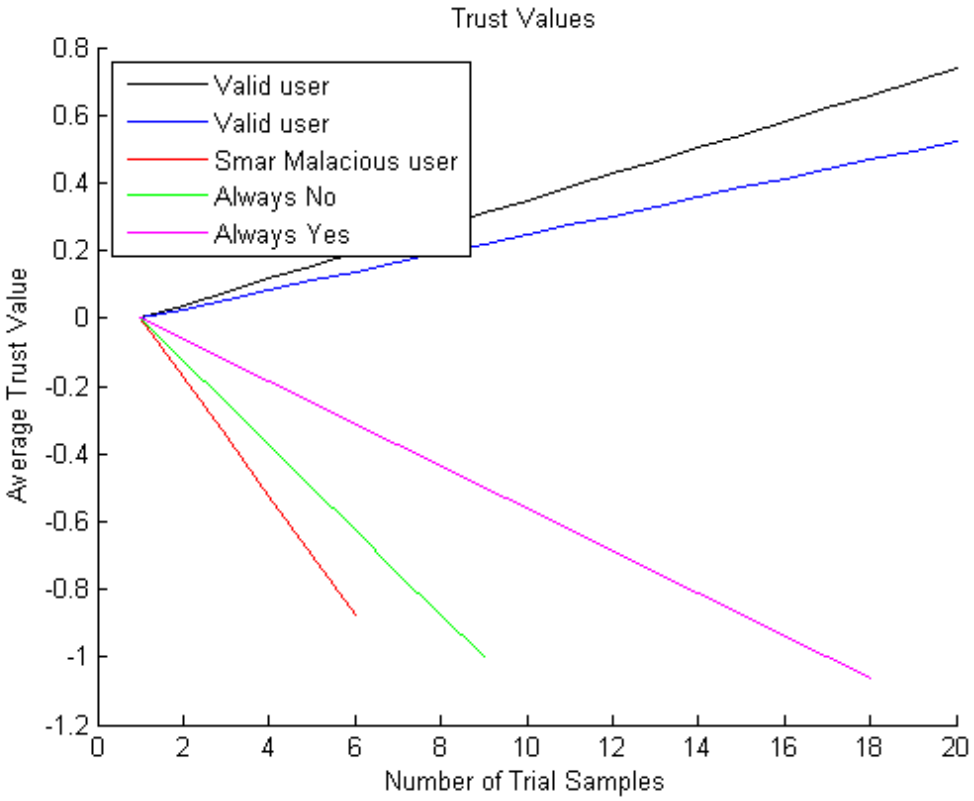


Figure 44 a) : weights of the users from Training Data

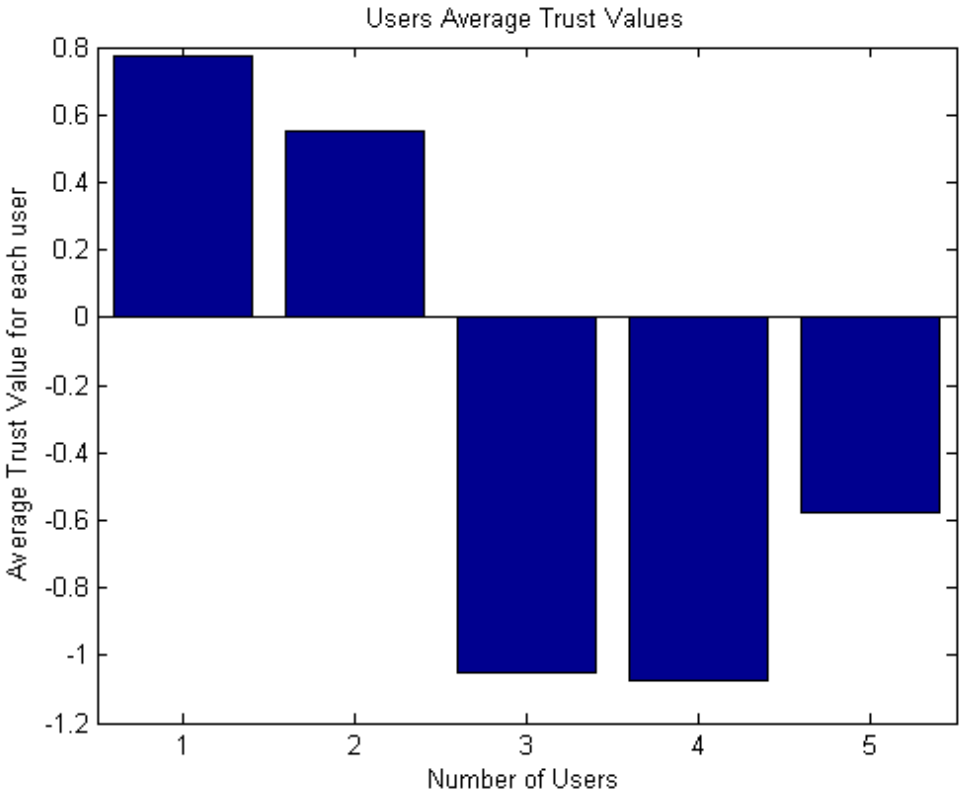


Figure 44 b) : Average Trust Value Computation of Each User

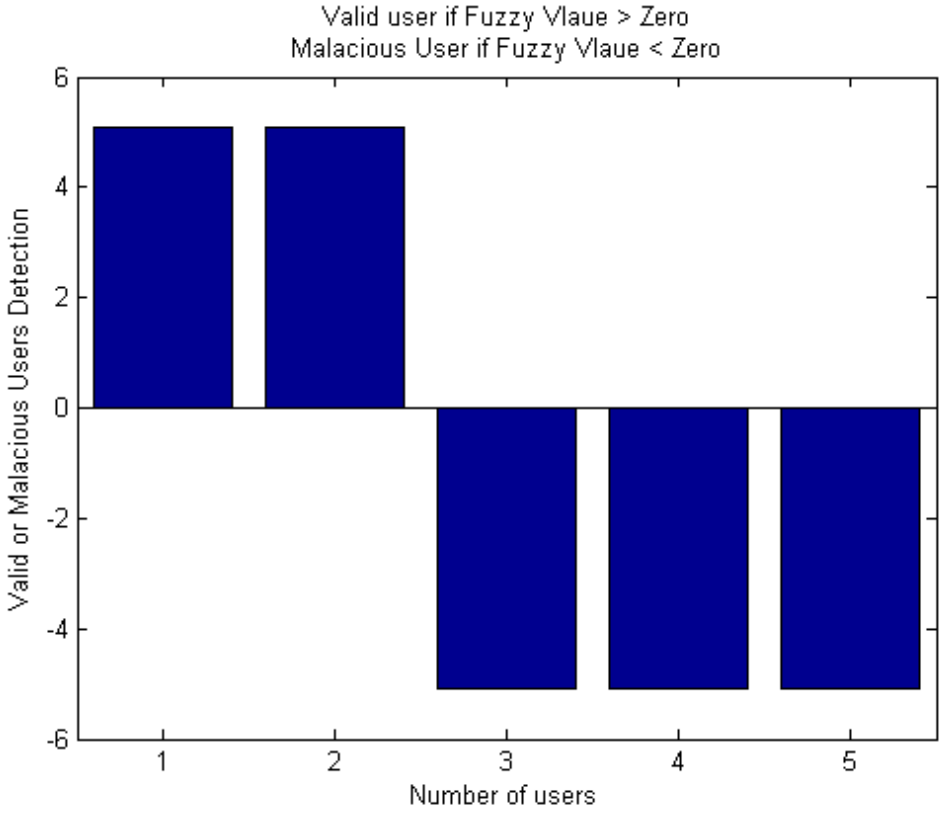


Figure 44 c): Final Decision of Fuzzy controller

Case 2: **10%** error for SU1 and **15%** error for SU2

In this scenario, probabilities of false detection for trusted users SU1 and SU2 are **10%** and **15 %** respectively. The graphs in figure 45 shows that proposed algorithm work efficiently even after introducing error in sensing. Trusted user still remains trusted not marked as malicious. Only MUs are labeled as malicious.

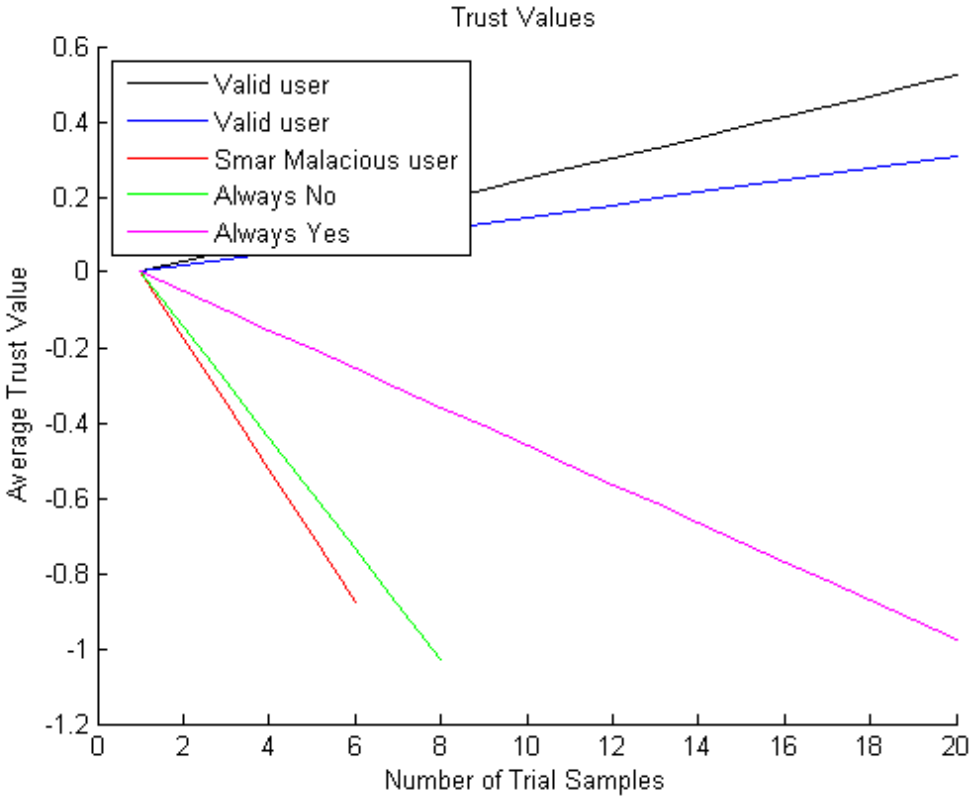


Figure 45 a): Weights of the users from Training Data

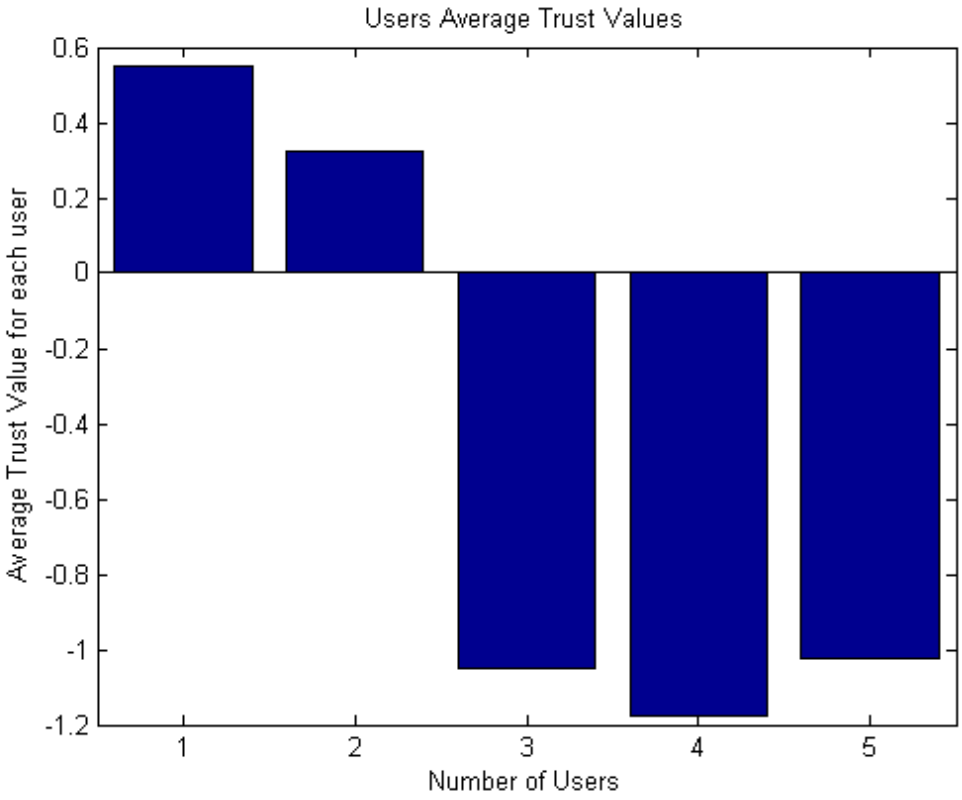


Figure 45 b): Average Trust Value Computation of Each User

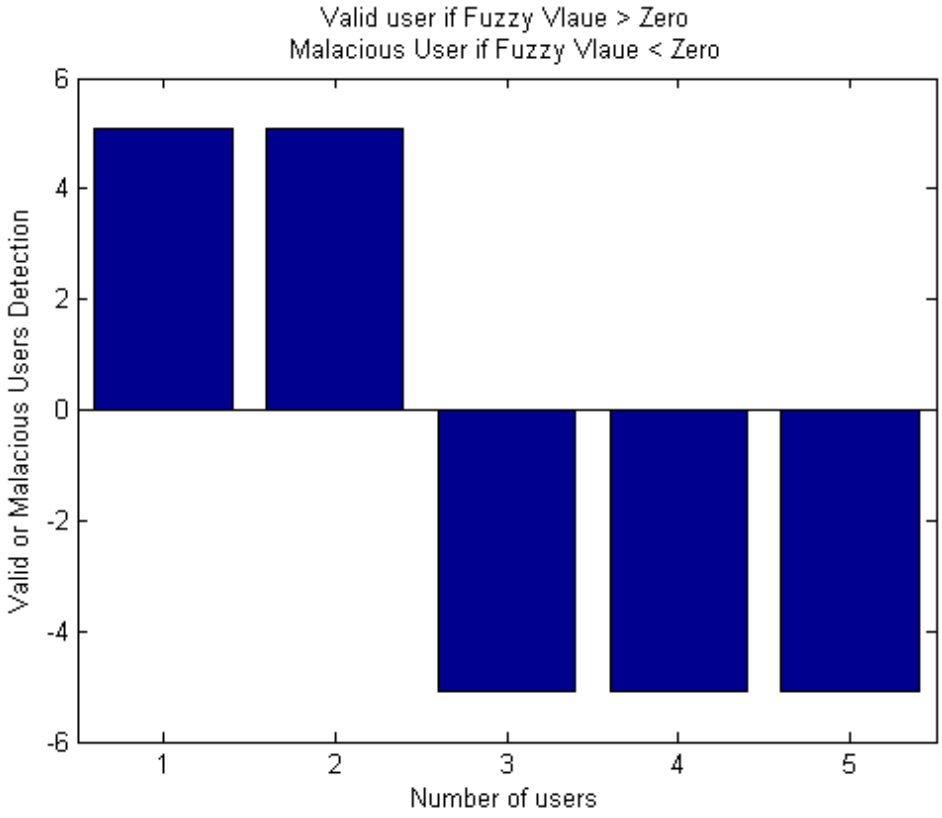


Figure 45 c): Final Decision of Fuzzy controller

Case 3: **15%** error for SU1 and **20%** error for SU2

In this case up to 20% error has been introduced for SU2 and 15% error for SU1. The graphs in figure 46 shows that, fuzzy controller detects the MUs correctly, and reduce their effect on overall performance of the system. For neural network algorithm, it works well only for 10% probability of false detection as shown in figure 46 d. More than 10% error effects neural network's performance. Therefore it is obvious that, fuzzy logic based algorithm is more robust than existing algorithms LMS, modified LMS and neural networks. Fuzzy controller has less computational complexity as compared to neural network and fast convergence than LMS algorithm. This is the reason, fuzzy logic is best options for the said problem statement in this research. Fuzzy logic based algorithm is best in a way, having less computational complexity, easy to implement, fast convergence and more robustness as compared to existing algorithms as discussed earlier in chapter 3.

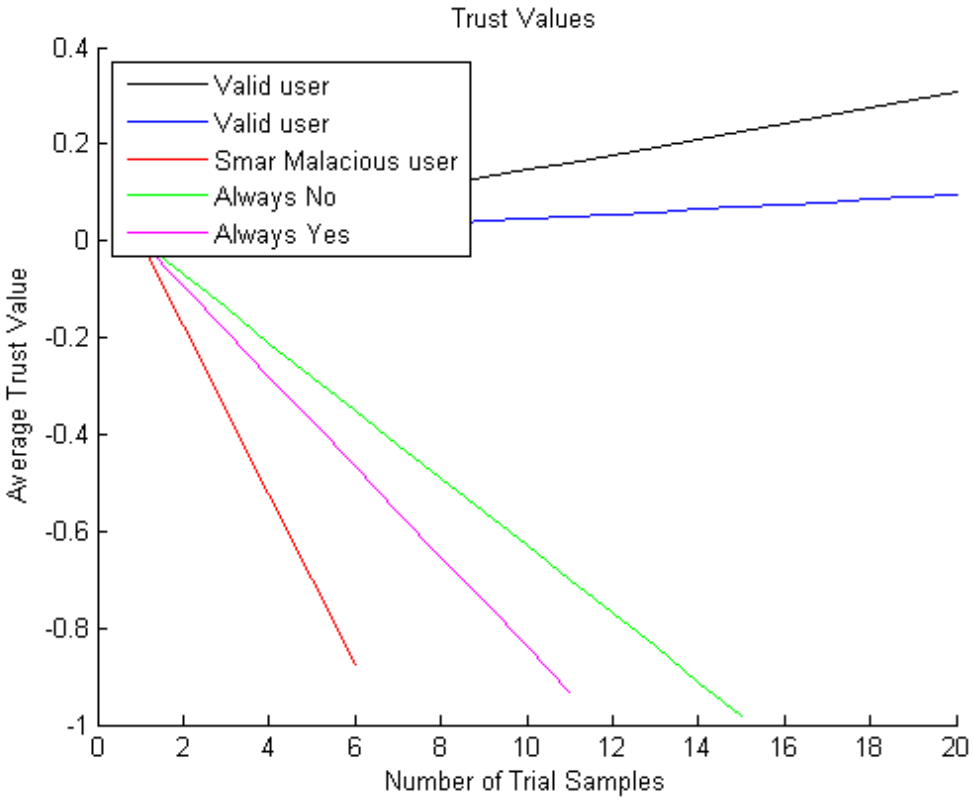


Figure 46 a): weights of the users from Training Data

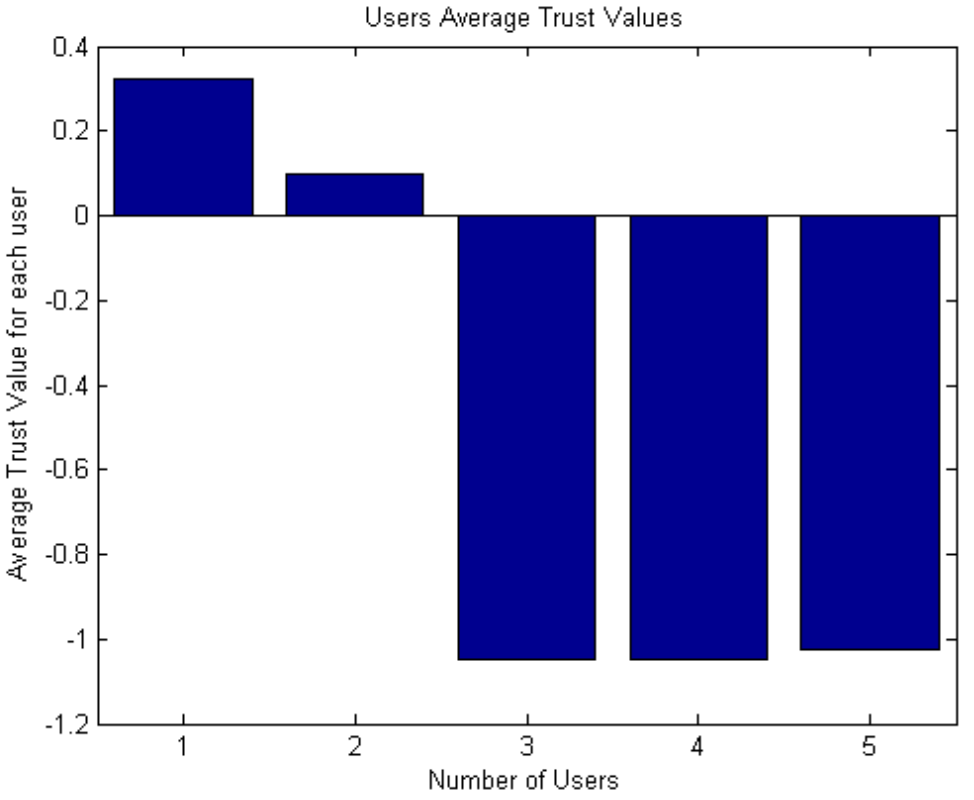


Figure 46 b): Average Trust Value Computation of Each User

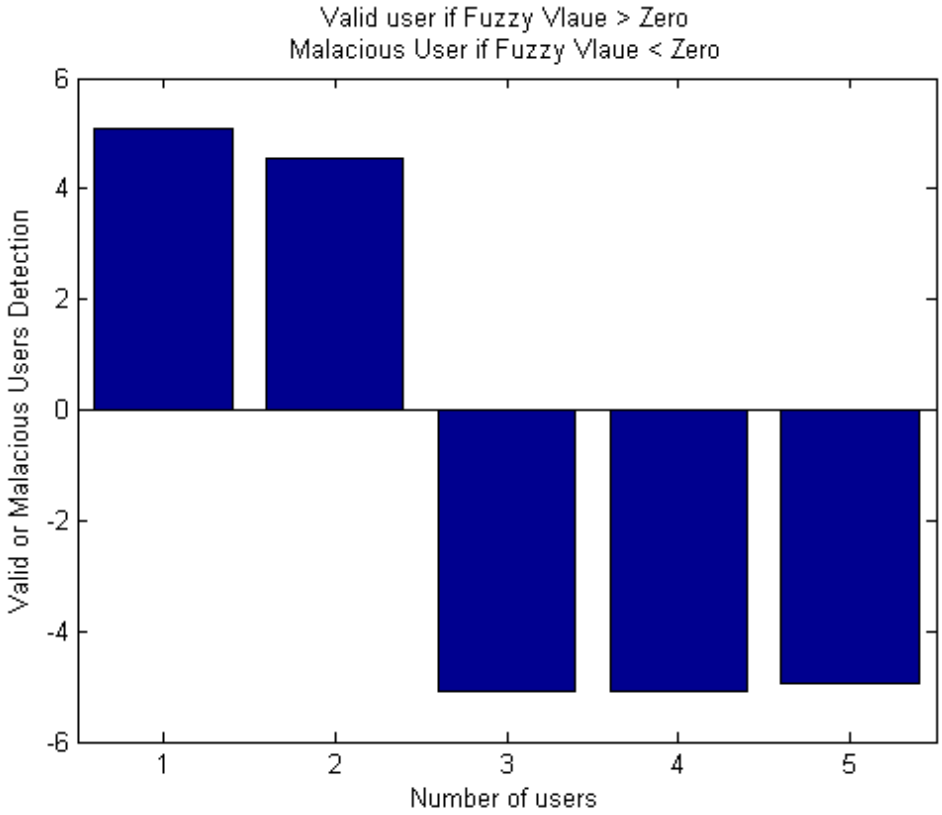


Figure 46 c): Final Decision of Fuzzy controller

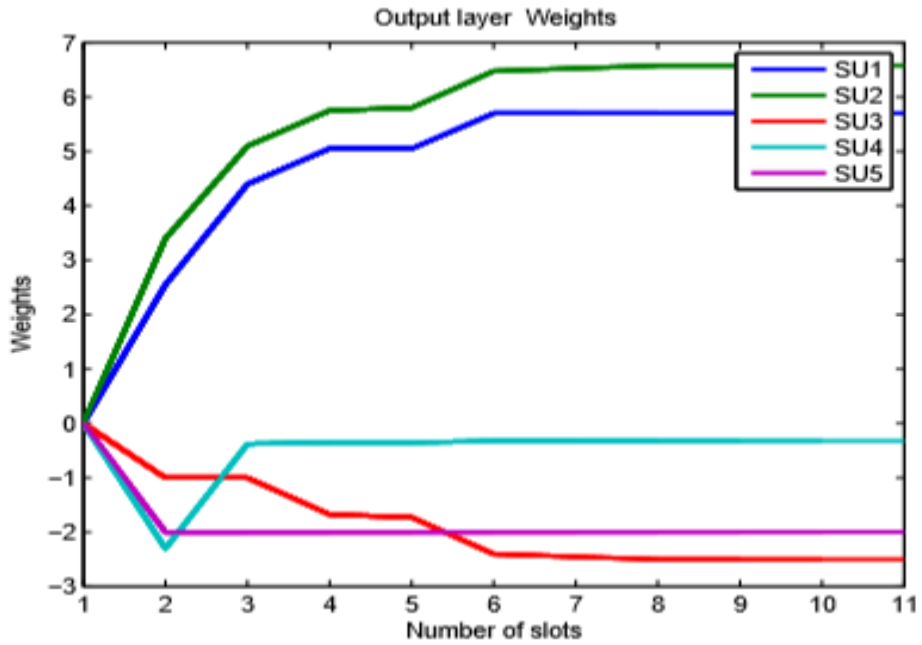


Figure 46 d): Output layer Weights (SU1, SU2 are trusted) 10% probability of False detection

4.5 With Varying Number of Users

In this scenario, the number of users have been increased from 5 to 10. Total 10 users are taken in consideration, seven are trusted and three are malicious. The SU3, SU4, SU5 are malicious and SU1, SU2, SU6 SU7, SU8, SU9, SU10 are honest users. Percentage of error is zero in this case, probabilities of false alarm and miss detection are not introduced. The graphs in below figure 47 shows that even increasing the number of users, proposed algorithm is working with good performance, properly evaluating the honest and MU's.

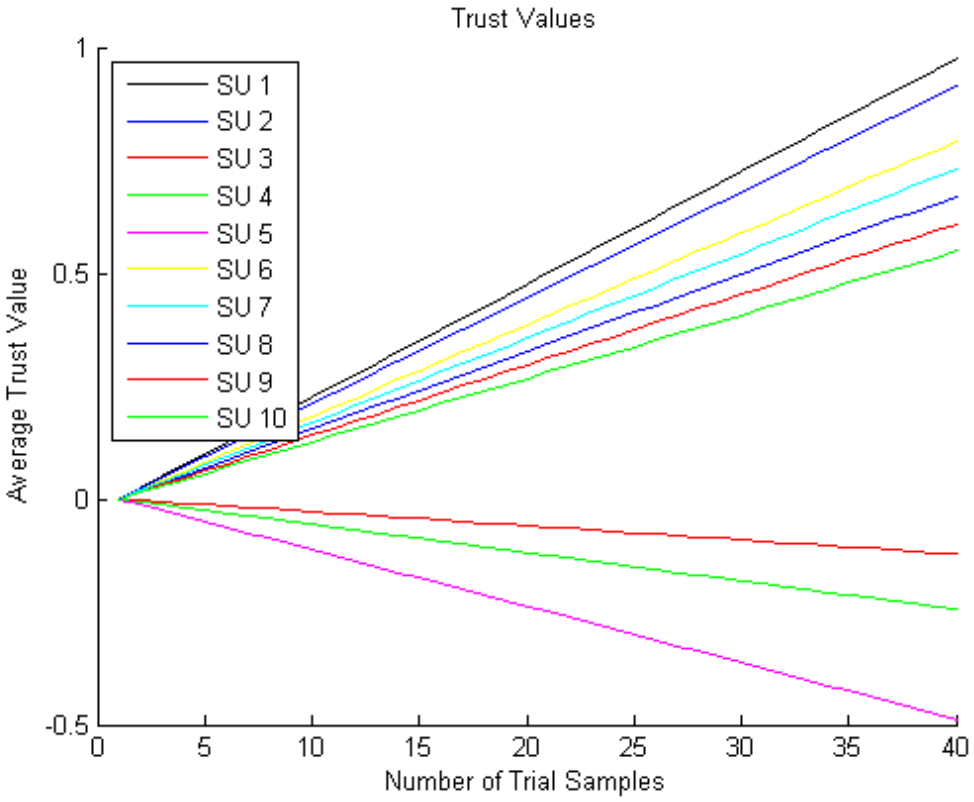


Figure 47 a): weights of the users from Training Data

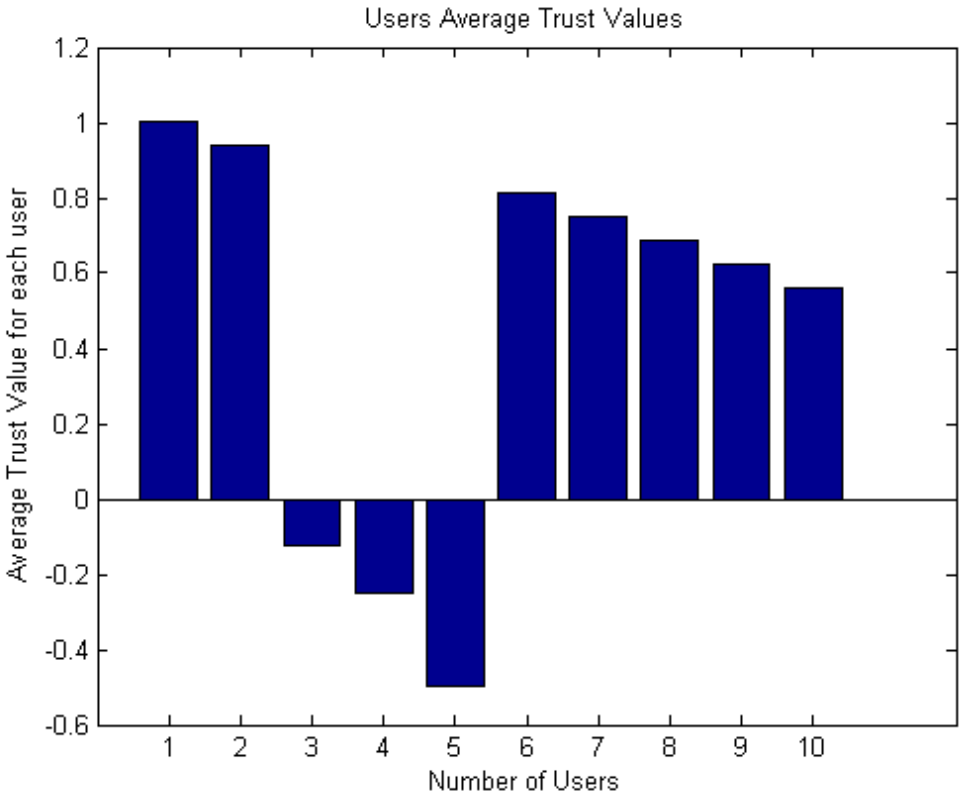


Figure 47 b): Average Trust Value Computation of Each User

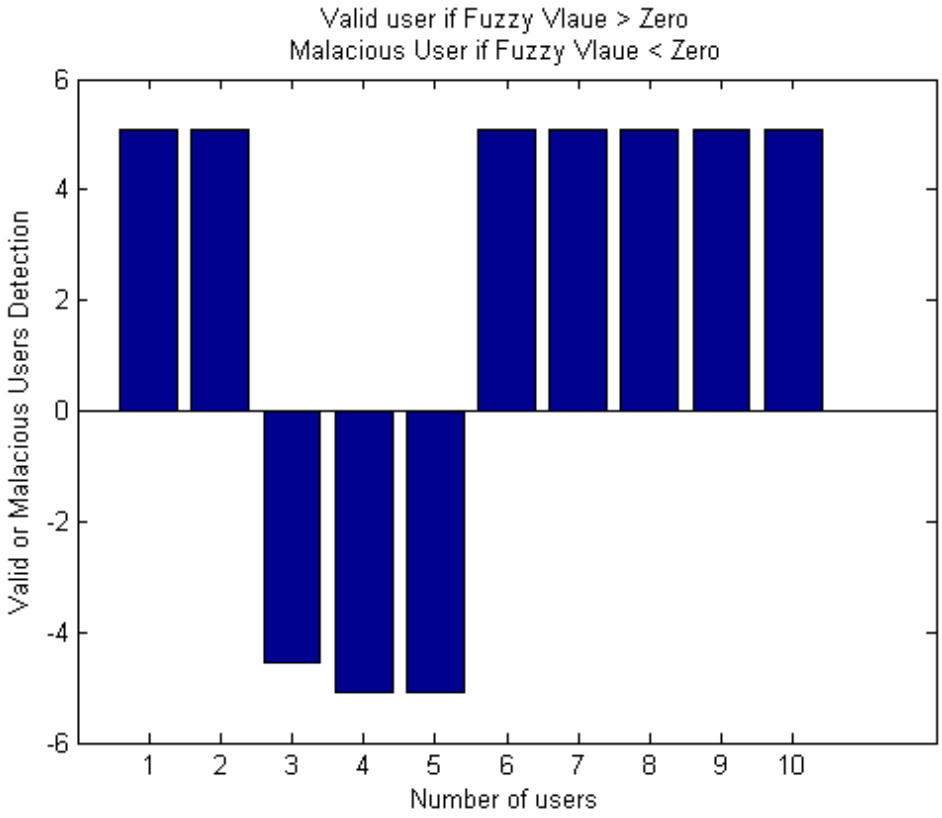


Figure 47 c): Final Decision of Fuzzy controller

We have taken different scenarios for simulations and results as shown in above graphs. It is obvious from results that, fuzzy logic based algorithm is more robust than existing algorithms LMS, modified LMS and neural networks. Fuzzy controller has less computational complexity as compared to neural network and fast convergence than LMS algorithm. This is the reason, fuzzy logic is best options for the said problem statement in this research. For many reasons, Fuzzy Logic is a very suitable algorithm for securing the spectrum sensing. In CRNs there is no distinct boundary among honest and MU's. By using fuzziness nature of fuzzy logic, it will help to smooth the rapid severance of abnormality and normality. Fuzzy logic based algorithm is best in a way, having less computational complexity, easy to implement, fast convergence and more robustness as compared to existing algorithms as discussed earlier in chapter 3. Another motive for using fuzzy logic is

diminution in probabilities of miss detection & false alarm and it works well even with imperfect sensing environment as shown in above graphs.

Chapter 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

As in chapter 4 we have discussed previously proposed algorithms namely LMS, modified LMS and feed-forward Neural Networks and our proposed algorithm based on Fuzzy Logic controller. It has been demonstrated from graphs that these techniques can be used for MU detection but there are some drawbacks, like slow convergence and more computational complexity. But fuzzy logic is better than others in a way that, it has less computational complexity as compared to neural networks and fast convergence than LMS and modified LMS algorithms. Our Technique is also more robust even after introducing up to 20% probability of false alarm and miss detection, MUs are identified correctly and honest users are labeled as trusted.

5.2 Future Work

This research work provides the basis for researchers to investigate in more details about the attacks in CRNs. Other Artificial intelligence techniques like Principle Component Architecture, Particle Swam Optimization, Neural Gas and genetic Algorithm can also be used for this problem.

BIBLIOGRAPHY

[1] Mc.Henry, A. Mark, *"*NSF spectrum occupancy measurements project sum-mary shared spectrum company report*",* 2005*.*

[2] M. Livsics, E. Nguyen, T. Majumdar and Nivedita,"Dynamic spectrum access eld test results, topics in radio communications", *IEEE Communications Magazine,* vol. 45, no. 6, pp. 51-57, 2007.

[3] B. Saklar*, "*Digital Communications: Fundamentals and Applications (2nd Edition) (Prentice Hall Communications Engineering and Emerging Technologies Series)"*,* 2001.

[4] J. O. Neel*, "*Analysis and design of cognitive radio networks and distributed radio resource management algorithms*", Ph.D. dissertation, Virginia Polytechnic Institute and State University,* 2006.

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

[7] I.F Akyildiz, W. Lee, M.C. Vuran and S. Mohanty*, "*Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey*", Computer Networks,* pp. 2127-2159, 2006.

[8] R. K. Sharma, D. B. Rawat*, "*Advances on security threats and countermeasures for cognitive radio networks: A survey*" IEEE Communication surveys & tutorials,* vol. 17, no. 2, 2015.

[9] S. Kyperountas, N. Correal and Q. Shi, "A comparison of fusion rules for cooperative spectrum sensing in fading channels*," EMS Research, Motorola,* 2008*.*

[10] P. Steenkiste, D. Sicker, G. Minden, and D. Raychaudhuri, "NSF workshop report, future directions in cognitive radio network research*",* 2009.

[11] L. Lu, X. Zhou, U. Onunkwo and G. Y. Li, "Ten years of research in spectrum sensing and sharing in cognitive radio*", EURASIP Journal on Wireless Communication and Networking,* 2012*.*

[12] D. B. Fette, D. Sto, and V.A. Arlington, "Fourteen years of Cognitive Radio Development"*, IEEE military communications conference,* 2013.

[13] L. Zhang, G. Ding, Q. Wu, and J. Wang and Y. Zou *"*Byzantine Attack and Defense in Cognitive Radio Networks: A Survey*"*, 2015*.*

[14] A. Attar, V. C. M. Leung, H. Tang, A. V. Vasilakos and F. R. Yu, *"*A survey of security challenges in cognitive radio networks: solutions and future research directions*", Proceedings of the IEEE,* vol. 100, no.12, 2012.

[15] D. Hlavacek, J.M. Chang, *"*A layered approach to cognitive radio network security: A survey*", Computer Network,* 2014.

[16] Z. Yuan, D. Niyato, H. Li, J. B. Song and Z. Han, *"*Defeating primary user emulation attacks using belief propagation in cognitive radio networks*", IEEE Journal for selected Areas in Communication,* vol. 30, no. 10, pp. 1850–1860, 2012.

[17] R. Dubey, S. Sharma, L. Chouhan, *"*Secure and trusted algorithm for cognitive radio network*", IEEE ninth international conference on wireless and optical communications networks (WOCN),* pp. 1–7, 2012.

[18] C. Chen, H. Cheng, Y. D. Yao, *"*Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack*" , IEEE Transaction in wireless communications*, pp. 2135–2141, 2011.

[19] R. Chen, J. M. Park, and J. H. Reed, *"*Defense against primary user emulation attacks in cognitive radio networks*", IEEE Journal for selected Areas in Communication,* vol. 26, pp. 25–37, 2008.

[20] Y. Tan, K. Hong, S. Sengupta and K. P. Subbalakshmi, *"*Using sybil identities for primary user emulation and byzantine attacks in DSA networks*" ,IEEE Global Telecommunications Conference GLOBECOM,* vol. 1, no. 5, pp. 5-9, 2011.

[21] Z. Xiao, X. Yang, L. Yuanyuan, *"*Encryption and displacement based scheme of defense against primary user emulation attack*", Fourth IET International Conference on Wireless Mobile & Multimedia Networks ICWMMN,* vol. 44, no. 49, pp. 27-30 , 2011.

[22] C. Zhao, L. Xie, X. Jiang, L. Huang and Y. Yao, *"*A PHY-layer authentication approach for transmitter identification in cognitive radio networks*", International Conference on Communications and Mobile Computing CMC ,* vol. 2, no. 154, pp. 158, 2010.

[23] H. Wen, S. Li, X. Zhu and L. Zhou, *"*A framework of the PHY layer approach to defense against security threats in cognitive radio networks*",* *IEEE Network,* vol. 27, no.3, pp. 34-39, 2013.

[24] N. Goergen, T. C. Clancy, and T. R. Newman, *"*Physical layer authentication watermarks through synthetic channel emulation*", New Frontiers in Dynamic Spectrum in Proceeding IEEE International Symposium,* vol. 1, no. 7, pp. 6-9, 2010.

[25] A. C. Sumathi, Dr. R .Vidhyapriya and C. Kiruthika, *"*A proactive elimination of primary user emulation attack in cognitive radio networks using intense explore algorithm*", International Conference on Computer Communication and Informatics* ICCCI, 2015.

[26] C. Chen, M. Song, C. Xin, M. Alam, *"*A robust malicious user detection scheme in cooperative spectrum sensing*", IEEE Global Communications Conference GLOBECOM,* pp. 4856–4861, 2012.

[27] Y. Song and J. Xie, *"*Finding out the liars: fighting against false channel information exchange attacks in cognitive radio ad hoc Networks*", IEEE*

Global Communications Conference GLOBECOM, pp. 2095–2100, 2012.

[28] M. Camilo, D. Moura, J. Galdin and R. M. Salles, *"*Anti jamming defense mechanism in cognitive radios networks", *Military Communications Conference MILCOM,* pp. 1–6, 2012.

[29] W. Wang, S. Bhattacharjee, M. Chatterjee and K. Kwiat*, "*Collaborative jamming and collaborative defense in cognitive radio networks*", Pervasive and Mobile Computing,* vol. 9, no. 4, pp. 573-587, 2012.

[30] H. Zhang, Z. Liu and Q. Hui*, "*Optimal defense synthesis for jamming attacks in cognitive radio networks via swarm optimization", *IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA),* pp. 1–8, 2012.

[31] B. Wang, Y. Wu, K. J. Ray and T. C. Clancy*, "*An anti-jamming stochastic game for cognitive radio networks*", IEEE Journal on Selected Areas in Communications,* vol. 29, no. 4, pp. 877–889, 2011.

[32] H. Li and Z. Han, *"*Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks*", IEEE Transactions in Wireless Communication,* vol. 9, no. 11, pp. 3554-3565, 2010.

[33] L. Zhang, Q. Wu, G. Ding, S. Feng, and J. Wang*, "*Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing" , *EURASIP Journal on Advances in Signal Processing,* vol. 67, no. 1, pp. 1-12, 2014.

[34] E. S. Mohammadi and M. Naraghi-Pour*, "*Fast detection of malicious behavior in cooperative spectrum sensing*", IEEE Journal in Selected Areas of Communication,* vol. 32, no. 3, pp. 377-386, 2014.

[35] Q. Yan, M. Li, T. Jiang T, W. J. Lou, and Y. T. Hou, *"*Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks*," Proceedings of INFOCOM,* pp. 900-908, 2012.

[36] T. Bansal, B. Chen, and P. Sinha*, "*Fast Probe: Malicious user detection in cognitive radio networks through active transmissions*," In Proceedings IEEE INFOCOM, Toronto, Canada,* pp. 2517-2525, 2014.

[37] S. Nath, N. Marchang and A. Taggu*, "*Mitigating SSDF attack using K-medoids clustering in cognitive radio networks*", International Workshop on Selected Topics in Mobile and Wireless Computing,* 2015.

[38] H. Du, S. Fu, H. Chu, *"*A credibility based defense SSDF attacks scheme for the expulsion of malicious users in cognitive radio*", International Journal of Hybrid Information Technology,* vol. 8, no. 9, 2015.

[39] K. Tan, S. Jana, P. H. Pathak and P. Mohapatra*, "*On insider misbehavior detection in cognitive radio networks", IEEE Networks, 2013.

[40] S. Jana, K. Zeng, P. Mohapatra*, "*Trusted collaborative spectrum sensing

for mobile cognitive radio networks", *Proceedings IEEE INFOCOM,* pp. 2621–2625, 2012.

[41] Y. E. Sagduyu, "Securing cognitive radio networks with dynamic trust against spectrum sensing data falsification", *Military Communications Conference MILCOM,* pp. 235-241, 2014.

[42] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks", *Computer Communications INFOCOM,* pp. 13-18, 2008.

[43] A. S. Rawat, P. Anand, H. Chen and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing,* vol. 59, no. 2, pp. 774-786, 2011.

[44] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications,* vol. 9, no. 8, pp. 2488-2497, 2010.

[45] T. Zhang, R. S. Naini, and Z. Li, "ReDiSen: Reputation-based secure cooperative sensing in distributed cognitive radio networks", *International conference on Communications ICC, Budapest, Hungary,* vol. 9, no. 13, pp. 2601-2605, 2013.

[46] H. Li, X. Cheng, K. Li, and C. Hu, "Robust collaborative spectrum sensing schemes for cognitive radio networks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2190-2200, 2014.

[47] H. Li and Z. Han, "Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks", *IEEE Transactions on Wireless Communications,* vol. 9, no. 11, pp. 3554-3565, 2010.

[48] S. Li, H. Zhu, B. Yang, C. Chen, and X. Guan, "Believe yourself: a user-centric misbehavior detection scheme for secure collaborative Spectrum sensing", *IEEE International Conference on Communications ICC, Kyoto, Japan,* pp. 5-9, 2011.

[49] J. Wang, J. Yao, and Q. Wu, "Stealthy-attacker detection with a multidimensional feature vector for collaborative spectrum sensing", *IEEE Transactions on Vehicular Technology,* vol. 62, no. 8, pp. 3996-4009, 2013.

[50] M. Wang, B. Liu, and C. Zhang, "Detection of collaborative SSDF attacks using abnormality detection algorithm in cognitive radio Networks", *IEEE International Conference on Communications ICC, Budapest, Hungary,* pp. 342-346, 2013.

[51] S. S. Kalamkar, P. K. Singh, and A. Banerjee, "Block outlier methods for malicious user detection in cooperative spectrum sensing", *Proceeding in IEEE Vehicular Technology Conference,* 2014.

[52] Y. Han, Q. Chen, and J. X. Wang, *"*An enhanced DS theory cooperative spectrum sensing algorithm against SSDF attack*", IEEE 75th Vehicular Technology Conference, Yokohama, Japan,* pp. 6-9, 2012.

[53] A. Vempaty, K. Agrawal, P. Varshney, and H. Chen, *"*Adaptive learning of Byzantines' behavior in cooperative spectrum sensing*", Wireless Communication Network Conference WCNC, Cancun, Mexico,* vol. 28, no. 31, pp. 1310-1315, 2011.

[54] X. He, H. Dai, and P. Ning, *"*HMM-based malicious user detection for robust collaborative spectrum sensing*", IEEE Journal for Selected Areas in Communications.* vol. 31, no. 11, pp. 2196-2208, 2013.

[55] X. F. He, H. Y. Dai, and P. Ning, *"*A byzantine attack defender in cognitive radio networks: the conditional frequency check*", IEEE Transactions on Wireless Communications,* vol. 12, no. 5, pp. 2512-2523, 2013.

[56] L. Duan, A. W. Min, J. Huang, and K. G. Shin, *"*Attack prevention for collaborative spectrum sensing in cognitive radio networks*", IEEE Journal for Selected Areas in Communications,* vol. 30, no. 9, pp. 1658-1665, 2012.

[57] S. Sodagari, A. Attar, V. C. M. Leung, and S. G. Bilen, *"*Denial of service attacks in cognitive radio networks through channel eviction triggering*", GLOBECOM,* Miami, pp. 6-10, 2010.

[58] W. Wang, L. Chen, K. G. Shin, and L. Duan, *"*Secure cooperative spectrum sensing and access against intelligent malicious behaviors*", IEEE Proceedings INFOCOM, Toronto, Canada,* 2014.

[59] A. W. Min, K. G. Shin, and X. Hu, *"*Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation*", IEEE Transactions on Mobile Computing,* vol. 10, no. 10, pp. 1434-1447, 2011.

[60] S. Jana, k. Zeng, and P. Mohapatra, *"*Trusted collaborative spectrum sensing for mobile cognitive radio networks*", IEEE Transactions on Information Forensics and Security,* vol. 8, no. 9, pp. 1497-1507, 2013.

[61] Z. Qin, Q. Li, and G. Hsieh, *"*Defending against cooperative attacks in cooperative spectrum sensing", IEEE Transactions on Wireless communications, vol. 12, no. 6, pp. 2680-2687, 2013.

[62] M. F. Amjad, B. Aslam, and C. C. Zou, *"*Reputation aware collaborative spectrum sensing for mobile cognitive radio networks*", Military Communications Conference MILCOM, San Diego,* pp. 951-956, 2013.

[63] C. Chen, M. Song, C. Xin and M. Alam, *"*A robust malicious user detection scheme in cooperative spectrum sensing*", GLOBECOM,* pp. 4856-4861, 2012.

[64] E. S. Hammadi and M. N. Pour, "Fast detection of malicious behavior in cooperative spectrum sensing", *IEEE Journal for Selected Areas in Communication,* vol. 32, no. 3, pp. 377-386, 2014.

[65] W. Wang, H. Li, Y. L. Sun, and Z. Han, "Catch It: detect malicious nodes in collaborative spectrum sensing", *IEEE Global Telecommunications Conference GLOBECOM, Honolulu,* 2009.

[66] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Joint spectrum sensing and detection of malicious nodes via belief propagation", *IEEE Global Telecommunications Conference GLOBECOM, Houston, 2011.*

[67] W. Wang, Y. Sun, H. Li, and Z. Han, "Cross-layer attack and defense in cognitive radio networks", *IEEE Global Telecommunications Conference GLOBECOM,* pp. 6-10, 2010.

[68] S. Yi, P. Naldurg and R. Kravets, "Security aware ad hoc routing for wireless networks", *Proceedings of the 2nd ACM International Symposium on Mobile ad hoc Networking for Computing,* pp. 299–302, 2001.

[69] J. Zhao and G. Cao, "Robust topology control in multi-hop cognitive radio networks", *IEEE Proceedings in INFOCOM,* pp. 2032–2040, 2012.

[70] E.M. Taghavi, B. Abolhassani, "Two step secure spectrum sensing algorithm using fuzzy logic for cognitive radio networks", *International Journal in Communication Networks and system science, pp. 507-513, 2011.*

[71] A.H. Hashmi, "Malicious users detection in cognitive radio networks", *Masters Dissertation*, *Mohammad Ali Jinnah University, Islamabad*, 2015.