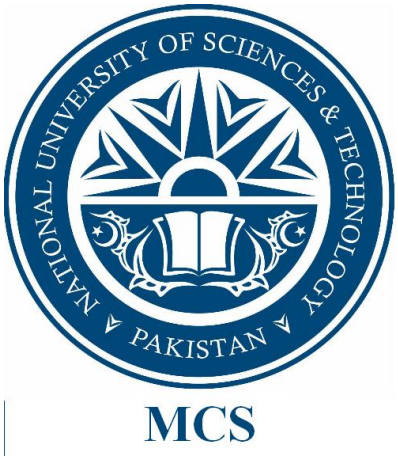
MITIGATION TECHNIQUE AGAINST PRIMARY USER EMULATION ATTACK IN COGNITIVE RADIO NETWORKS



by

Syed Bilal Haider Naqvi

MSIS-10

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

June 2014

Dedication

I dedicate my dissertation work to my family. A special thanks to my loving parents whose prayers, words of encouragement and push for tenacity ring in my ears and made me work even harder. My brother never left my side and is very special. His motivation and support during this degree was unmatched.

I also dedicate this dissertation to all my teachers who taught me right from nursery till masters and made me what I am.

Acknowledgement

I wish to thank my supervisor Dr. Baber Aslam, who was more than generous with his expertise and precious time. A special thanks to all my committee members for their support and guidance. I also thank my colleagues who helped me during my thesis.

I hereby acknowledge the support of my supervisor for his countless hours of reflecting, reading, and most of all patience throughout the entire process.

I thank all the staff of Department of Information Security for keeping updated about all the deadlines, departmental activities, etc.

Abstract

The increasing demand of usable spectrum range alarmed the world of serious shortage in the coming years. Cognitive Radio technology emerged to solve this problem by allowing unlicensed users to utilize the spectrum resources whenever the licensed users are not active. With the emergence of this technology many security issues arose, that if successful may hamper all the benefits this promising technology has to offer. Among many other security issues Primary User Emulation Attack (PUEA) is one. In this thesis focus is on the PUEA however other attacks to Cognitive Radio are also discussed. Existing work to counter PUEA is also discussed, along with its limitations.

The thesis basically describes the proposed approach based on randomized sensing to counter PUEA. It is proposed to have sensing randomized at different intervals other than the defined sensing intervals. This approach is advantageous over other approaches in a sense that it does not only identify a malicious PUEA but also provides countermeasure, as the unlicensed user (also known as Secondary User or SU) is able to utilize remaining slot for performing its transmission.

To check the impact of PUEA on the Cognitive Radio technology, an environment consisting of nodes (CRs) was setup. To generate effective results, environment close to the real world (in terms of behavioral aspects of the nodes in Cognitive Radio) was simulated. The behavior of nodes in attack free environment was evaluated first and then the effects of PUEA were evaluated through simulation results. In the end the results after incorporating the proposed approach were generated to see the impact of proposed approach on attack environment.

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Syed Bilal Haider Naqvi

Table of Contents

List of Figures

List of Tables

List of Abbreviations

CR	Cognitive Radio
CRN	Cognitive Radio Network
PU	Primary User
SU	Secondary User
SU_M	Malicious Secondary User
PUE	Primary User Emulation
PUEA	Primary User Emulation Attack
IEEE	Institute of Electrical and Electronic Engineers
UWB	Ultra wide band
DDT	Distance Difference Test
DRT	Distance Ratio Test
TDOA	Time Difference of arrival
FDOA	Frequency Difference of arrival
IDS	Intrusion Detection System
LIDS	Local Intrusion Detection System
LACE	Local Aggregation and Correlation
GACE	Global Aggregation and Correlation
ZBIDS	Zone Based Intrusion Detection System
NUMC	Network User Management Center
RSS	Received Signal Strength
VANET	Vehicular Ad-hoc Networks
MANET	Mobile Ad-hoc Networks
PDA	Personal Digital Assistant
RRA	Radio Regulation Authority

QoS	Quality of Service
OSI	Open Systems Interconnection
TCP	Transmission Control Protocol
IP	Internet Protocol
FCC	Federal Communications Commission
DoS	Denial of Service
CBR	Constant Bit Rate
NS-2	Network Simulator 2

CHAPTER 1

INTRODUCTION

1.1 Background of Cognitive Radio Technology

In the past few decades the world has seen many new inventions among which the wireless technology is one. It is history when there used to be one wired telephone serving hundreds of people in town, now through use of wireless technology everyone is having own wireless phone. Telephone is not the only advantage that this technology has brought instead sophisticated applications like Internet, vehicle to vehicle (V2V) communication, cloud computing etc. partly or solely involve the use of this technology.

Various numbers of applications involving the use of wireless technology led the researchers focus on acute shortage of wireless spectrum which is expected to increase in years to come. As a first step J. Mitola in 1998 proposed the concept called Cognitive Radio to overcome the spectrum shortage problem [18]. It solves the spectrum shortage problem by allowing unlicensed users to utilize the network resources when the licensed users are not using those network resources, thus allowing more number of users to utilize the same resources by adding intelligent usage phenomena to the communicating devices. In other words rather than the spectrum resource being wasted (due to absence of the licensed user), it is utilized by the unlicensed user.

The licensed users are also called the Primary Users (PU) and those who use the resources when spectrum allocated to PU is vacant are called the Secondary Users (SU) [21]. The SU can only use the resources till the time the PU is not using the allocated resources; however upon reappearance of the PU, the SU has to leave the channel for use by the PU. The Cognitive Radio, therefore, provides opportunistic access to the SU whenever the channel is vacant. However more details on Cognitive Radios will be covered in the coming chapters.

Due to the role of Cognitive Radio in solving spectrum shortage problem and its increasing use in many applications, it is susceptible to many attacks including the Primary User emulation (PUE) attack, hello flood attack, sinkhole attack, jamming attack, lion attack etc. which will also be covered in the coming chapters. However the focus of this is the Primary User Emulation attack [1].

Primary User Emulation Attack (PUEA) is defined as the attack done by a malicious SU during the sensing time masquerading as a PU to obtain the network resources, thus refraining other SUs from using the resources. More details on PUEA will be covered in the coming sections.

1.2 Current Status of development

It has been almost 15 years since this technology was first proposed and since then Cognitive Radio is receiving a lot of importance of the researchers as it is near deployment stage [18]. There is a dire need of better ideas to deploy it in perfect shape. As mentioned in the previous section the Cognitive Radio has a crucial role to play in enabling our wireless conversations of future. Due to many contributions on successful working of Cognitive Radio like the coexistence mechanisms, sensing algorithms have been proposed but the security issues received a little less attention.

As far as standardization efforts are concerned a great deal of effort is being made for developing standards related to CRs. Organizations like IEEE, International Telecommunications Union-Radio Sector (ITU-R) and Software-Defined Radio (SDR) Forum are among the prominent working in his regard [54]. The most commonly known is IEEE standard, which (relevant to the use of Cognitive Radio) is in the development stage, only draft version of the standard specific to use of Cognitive Radio in TV network (802.22) has

been published and the standard relative to use of CRN in CDMA, GSM/GPRS, Wi-Max, LTE and other networks is yet to get any standardization maturity level.

There is no practical application currently in use but as per FCC recommendation the CR technology will be deployed by 2020 in US [1], therefore companies are finalizing the deployment stages and testing their products to enable their usage [55].

1.3 Motivation behind selection of the topic

To protect Cognitive Radio networks against Primary User Emulation Attack, many schemes have been proposed but all other proposed schemes employ physical layer level detection of the attack and do not incorporate the case where location of PU is not static [1]. Also the proposed schemes like transmitter finger printing can be affected by noise and since noise varies in different networks therefore we need to define different threshold values for different networks [7]. Hence the proposed schemes are limited to the network they have been proposed for. The existing solutions are not enough as their application is limited to static environments and they focus only on identification of the attack.

For Cognitive Radio applications deployed in ad-hoc networks specifically Vehicular Networks there is need of a countermeasure to PUE attack that is flexible to incorporate changing network environment and should not be too much dependent on physical layer level attributes due to changing location. In a network environment where the location of PU/SU is not static and there is not much time to deploy techniques as transmitter fingerprinting that may result in high number of false positives/negatives as a countermeasure to PUE attack.

1.3.1 Problem Statement

A solution against PUE attack is required that incorporates the changing nature of the ad-hoc networks and also gives correct detection results and efficient protection in case

of a successful PUE attack. As discussed above all the proposed solutions focus on identification not its counter measure therefore main motivation was **"to propose a countermeasure for PUEA that is not reliant on the attributes like static location, received signal strength etc. and is not limited only to identification of the attack"**.

1.4 Aim and Objectives

The aim behind the work was to propose a mitigation technique against the Primary User Emulation Attack as most of the research conducted up till now focuses on the attack's identification not its mitigation/ counter measure. However the objectives of the thesis are as under:

a. Understanding of the Cognitive Radio principles and standards.
b. Understanding PUE attack and its effects
c. Proposing a solution to counter this attack
d. Evaluating effectiveness of the solution.
    I. In terms of protection it provides.
    II. Scenarios it is applicable in.
    III. Advantages that it has over other solutions.

1.5 Scope

The work in this thesis is applicable to any organization in military or private planning to deploy the Cognitive Radio technology for their communication purposes. Since security is an essential aspect of every new deployment and Cognitive Radio being a new technology as far as deployment is concerned, is facing tremendous challenges by attackers. Therefore this work refers to essential measures that need to be taken by the deploying organization to meet the one of the biggest challenges posed by attackers, i.e the Primary User Emulation Attack.

1.6 Thesis Organization

This thesis is organized in 6 chapters. Chapter 2 covers the Literature Review. Chapter 3 covers the details about Cognitive Radio Technology. Chapter 4 covers the Attacks to Cognitive Radio Technology. Chapter 5 covers the Solution and Results. Chapter 6 covers the Conclusion.

1.7 Summary

In this chapter the basics of Cognitive Radio were covered along with the current status of development. Different aspects of development like research, products, standardization were considered. The objectives behind the work were described. Some of the existing solutions were discussed along with their limitations. After necessary discussion on the CRs the problem statement was defined. After the problem statement was defined the area of application or the scope of the work was discussed. In the end the organization of the rest of the thesis was described.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter the solutions to PUEA, as proposed by other authors, will be presented and discussed. Based on findings after literature review the proposed solutions to counter PUE attack fall in three broad categories as depicted by the Figure 2.1.

In distributed/ individual node based schemes, the focus is on providing solution applicable to an individual user and guarding a particular user from the attack. While the centralized/ cooperation based schemes emphasize on cooperation among all communicating nodes in the network. All the nodes in centralized scheme send their impression of the current state of the environment to the central authority upon discovery of unusual activity.

The main difference among the two is that of decision authority. In distributed/ individual node based schemes the decision making authority rests with the individual user where as in centralized scheme the decision making rests with central authority.

Third category is the intrusion detection system based (IDS) schemes. These schemes as the name suggests focus on detecting intrusion in the network, and PUEA is one kind of intrusion to the network. Intrusion means imposition or disturbance and refers to an unwanted occurrence or break-in that is undesired. There are many kinds of intrusion and intrusion detection is a broad term. One kind of intrusion can be a PUEA, so IDS can detect PUEA as well.

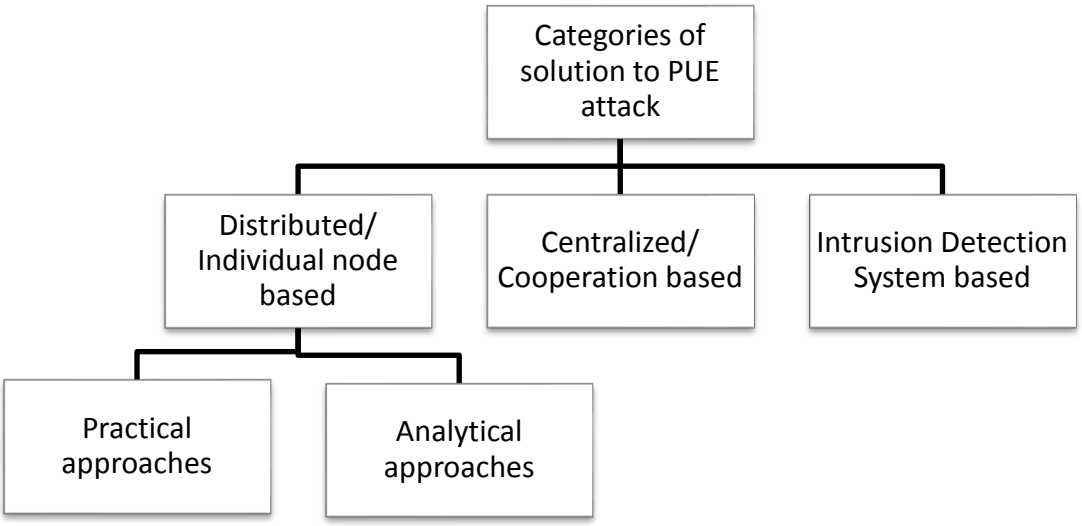


Figure 2.1: Taxonomy representing categories of solutions proposed for PUE attacks

2.2 Distributed/ Individual node based solutions

Distributed/ individual node based schemes accentuate applying the proposed procedure to individual user and guard that particular user from the attack. In this section the schemes that do not require cooperation among the nodes in the Cognitive Radio network will be discussed.

2.2.1 Practical approaches:

Chen et al., in [4] proposed the transmitter verification scheme called LocDef. This scheme uses the signatures of the transmitter and verifies whether the signal is generated by a legitimate PU or not. It performs the estimation based on the location and observing signal characteristics. The scheme employs a wireless sensor network to measure the received signal strength (RSS) value and based on this RSS value the RSS peaks are identified and transmitter location are estimated. It is worth mentioning here that this scheme applies to the case where the Primary User is the TV transmission tower fixed at static locations.

As an extension of the work in [4] Chen et al., proposed two tests for location verification of the transmitter namely the Distance Ratio Test (DRT) and Distance Difference Test (DDT). DRT focuses on RSS (received signal strength) value whereas the DDT relies on relative phase difference of the received signal. This scheme is particularly applicable in TV networks where signals are generated by powerful base station and such power is difficult to emulate by malicious SU. In addition to the Distance Ratio Test (DRT), this scheme takes advantage of the geographical location of a base station using distance difference test (DDT). Since the location of the base station is fixed, so whenever SU detects Primary User as active, it estimates the location from where the received signal was generated. If the location from where the received signal was generated matches that of the base station it is assumed to be a legitimate Primary User otherwise an attack is detected.

Khare et al., in [5] studied the threats to Cognitive Radio networks and suggested that the strategies in [4] are applicable in detecting PUE attacks. The authors suggested that distance difference test **(**DDT**)** and the distance ratio test (DRT), are applicable to detect the PUE attack. Both these techniques are used for location verification of the received signal. Employing the above techniques it can also be determined whether the received signal strength is equal to the strength generated by legitimate PU [4] or not. In addition the authors in [5] proposed a Network User Management Centre (NUMC) based Cognitive Radio architecture where the role of NUMC is the authorization of all the Secondary Users SUs.

Huang et al., in [6] proposed a strategy similar to [4], featuring localization, but due to some shortcoming in DDT and DRT, proposed an efficient positioning scheme based on Time Difference of arrival (TDOA) and Frequency Difference of arrival (FDOA). In the proposed technique TDOA will run first and will make computation such that the time difference of arrival of the received signal compared to what it should be in case of the

legitimate PU. FDOA uses result computed by TDOA to identify the exact location of the transmitter and hence it is again applicable in case where the location of the transmitting resource is static. However these techniques rely on a set of many assumptions making their use restricted and specific.

Zhao et al., in [7] proposed a scheme to counter PUE attacks that is based on transmitter fingerprinting. It makes use of the fact that phase noise for each transmitter is unique and random. After the signal is received high level statistical analysis is performed to generate the finger print of the transmitter. Or in other words the phase noise of the noisy career is extracted. The extracted sample is then applied to identify the transmitter. If the extracted sample matches that of the original transmitter then it is acceptable otherwise an attack is detected.

2.2.2 Analytical Approaches:

Jin et al., in [8] proposed an analytical approach to detect PUE attack based on Neyman-Pearson composite hypothesis test and Wald's sequential probability ratio test. In their approach firstly probability density function is generated for the received signal. Based on the probability density function result, Neyman-Pearson composite hypothesis test is conducted which under certain scenarios can have high probability of a false alarm. Therefore Wald's sequential probability ratio test is applied which gives improvement in results by allowing user to specify thresholds for false alarms and probability of a miss.

In another paper Jin et al., [9] proposed an analytical scheme independent of the location information and does not require any dedicated sensors. They present their analysis using Fenton's approximation and Wald's sequential probability ratio test. As discussed above using Wald's sequential probability ratio test allows user to set threshold values on probability of successful attack and probability of a miss thus giving improved

results. In their previous study the considered fading wireless environment and expression for probability of successful PUE attack is derived using Fenton's approximation. Markov's inequality is then applied to get the lower bound on probability. However in this paper Fenton's approximation is applied to obtain probability density function of the received signal from attacker which is used in the Wald's sequential probability ratio test. If the received power of the signal is above a specified threshold then Wald's sequential probability test criterion involving the Fenton's approximation is applied to decide whether it is being generated from legitimate transmitter or from malicious transmitter. The whole scheme is based on the assumption that the legitimate transmitter is the TV station transmitter.

Anand et al., in [10] proposed an analytical approach based on Fenton's approximation and Markov inequality. Both these techniques are used to obtain lower bound of probability of successful PUE attack. There is an assumption that there is set of cooperating malicious users in the fading wireless environment that they have considered. The proposed scheme uses received power at a SU and treats it as log-normally distributed random variable. Fenton's approximation is then applied to determine the mean and variance of power received at SU. The lower bound on probability of the case of successful attack is then determined using Markov inequality. The authors also show that the probability of successful attack increases as the distance between the primary transmitter and the set of malicious users increase.

Clancy et al., in [11], in their study of threats to Cognitive Radio networks studied threats relative different types of radios such as policy radio, learning radio. Policy radios have predefined list of rules that guide on adaptation in different scenarios. In other words the hard-coded rules in a policy radio drive the radio in adapting to different types of

situations. Learning radios on the other hand have a learning engine that keeps track of percept-action history, based on actions taken by the radio in response to different perceptions in the past. This history guides adaptation to get optimal results. The learning engine incorporates the techniques of artificial intelligence (AI). The difference lies in the fact that the learning radios are self-learning and update the knowledge base for future reference whereas the policy radio need to be configured and updated manually. The authors suggest that since artificial intelligence engine is incorporated in each wireless device so we need to be aware that these AI engines can be provided false input to do generate the necessary action that may be in the interest of an attacker. Therefore care needs to be taken in this regard too. In their study they also classified the malicious users in two kinds one being the on-path and other being the off-path. In the end to protect against the PUE attack they suggest that development of better sensing algorithms with low false positive rates can be helpful in mitigating PUE attack. A better developed sensing algorithm will be able to distinguish whether the signal generate by the legitimate or by the malicious user.

2.3 Centralized/Cooperation based solutions

In centralized schemes the emphasis is on cooperation and nodes communicate their findings to central authority upon discovery of strange activity. What separates the two is the decision authority, in distributed schemes the decision making authority rests with the individual user while in centralized scheme the decision making rest with central authority. The solutions to PUE attack that fall in this category are as follows.

Ramzi Saifan, in [12] proposed a cooperative scheme for in-band sensing that can be used to detect PUE attacks. The proposed scheme suggests that nodes in Cognitive Radio network have two discrete tasks that are sensing and transmission. Nodes whose task

is sensing perform in-band sensing and generate alerts/ warnings messages (about re-appearance of the PU) to the nodes performing transmission, whereas the nodes in transmission mode only do transmission and receive alerts/warning messages generated by the sensing nodes. As far as technique to counter PUE attack is concerned, the author proposed feature detection technique capable of identifying modulation type of a primary signal. Using this technique the system will be able to distinguish whether the received signal is generated by Primary User or is generated by the emulating Secondary User.

Kaligineedi et al., in their study to counter PUE attacks [13] proposed a scheme to detect a malicious user activity in Cognitive Radio network. The proposed scheme requires a set of cooperative nodes in the network. All the cooperating nodes send their sensing results to a central authority which makes the decision about presence or absence of the Primary User. In this scheme all the cooperating nodes use energy detectors and each user is assigned outlier factors. The assigned factors are used to identify and nullify the effect of a malicious user. Once the nodes send their data to a central authority (an access point), then it's up to the central entity to make the decision. The central entity uses data fusion and detection schemes to decide about presence of absence of the Primary User.

2.4 IDS Based Solutions

In addition to other two categories the authors also propose an Intrusion Detection System based scheme to identify malicious user in the network. Identifying malicious user is generic term and to be more specific one activity of malicious user can be PUE, so these schemes proposed for identification of malicious user can prove beneficial for detecting PUE attack. The proposed solutions employ both distributed and centralized schemes and have specific architectures specific to deployment in ad-hoc networks. Some architecture styles are as follows.

a. Stand-alone Intrusion Detection Systems

b. Hierarchal Intrusion Detection Systems

c. Distributed and Cooperative Intrusion Detection Systems

d. Mobile agent for Intrusion Detection Systems

Zhang et al., proposed an IDS based scheme consisting of six modules namely the local data collection module, local detection engine, local response module, global response module, cooperative detection engine and secure communication module [22]. The local data collection module collects data from the nodes in network. The collected data includes user activities in the network. This data is then examined by the local detection engine for detection of anomalies. If an abnormal behavior is detected with solid evidence and it is determined that the system is under attack, a response is generated through the local response module or global response module depending on level of certainty of the evidence and type of intrusion. However if local detection engine module detects an anomaly with weak evidence IDS agent request the neighboring nodes for cooperation through cooperative detection engine and all communication to neighbors is done using the secure communication module.

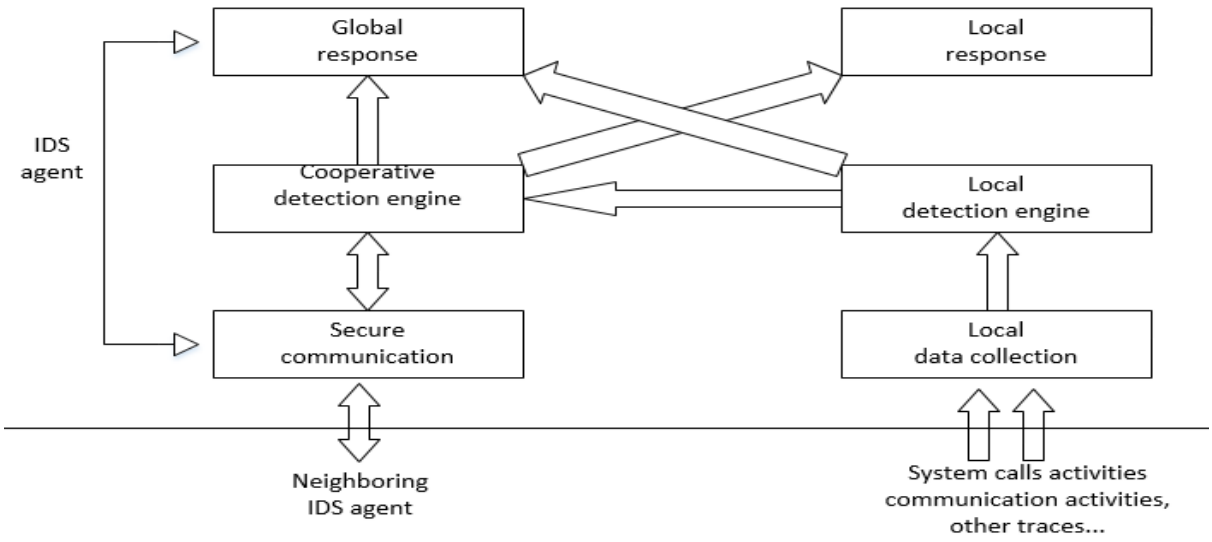


Figure 2.2: Model for IDS agent as suggested by Zhang et al., [22]

Albers et al., in [27] proposed a scheme named as local intrusion detection system (LIDS). This scheme needs to be implemented on every node in the network. The system can be extended for global coverage by forming a network of all LIDS. Data exchanged in LIDS constitutes security data and intrusion alerts.

To identify intrusion data is obtained from LIDS detection results and analysis is performed to judge whether the intrusion occurred or not. However in the architecture of LIDS the author has proposed local LIDS agent, local MIB agent, Mobile agent and mobile agents place [27]. All of these characteristics have specific contributions in successful functioning on LIDS.

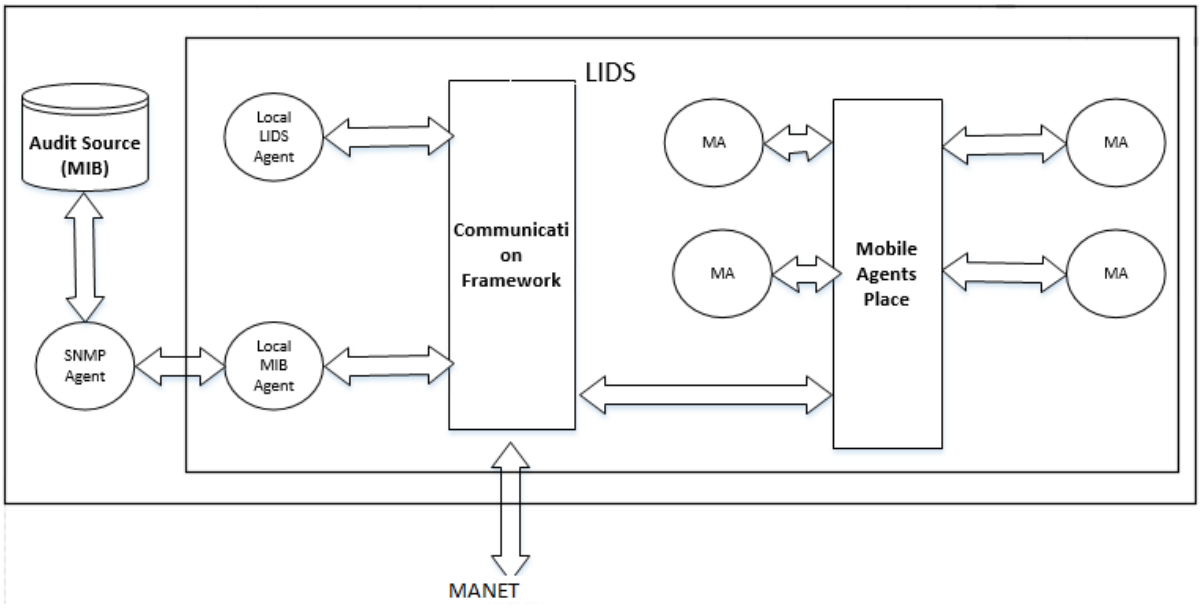


Figure 2.3: LIDS architecture as suggested by Albers et al., [27]

Kachirski and Guha in [23] proposed Distributed IDS using Multiple Sensors. They propose Monitoring Agent, Action Agent and Decision Agent for their scheme. Monitoring agent is responsible for two functions: network monitoring and host monitoring. Two set of monitors run in the scheme, one is host monitoring agent that is responsible for monitoring activity within the node by using sensors and other is the network monitoring agent that records the activity of some of the selected nodes with in its range. Each node also has one

action agent. The entire host based monitoring agents send their findings and report any unusual activity based on detection of an anomaly. When there is an evidence that anomaly has been detected the action agent take action such blocking the user from the network. Decision agent runs on only few nodes and its responsibility is to collet packet from all nodes running network monitoring agent and determine whether or not the network is under attack.

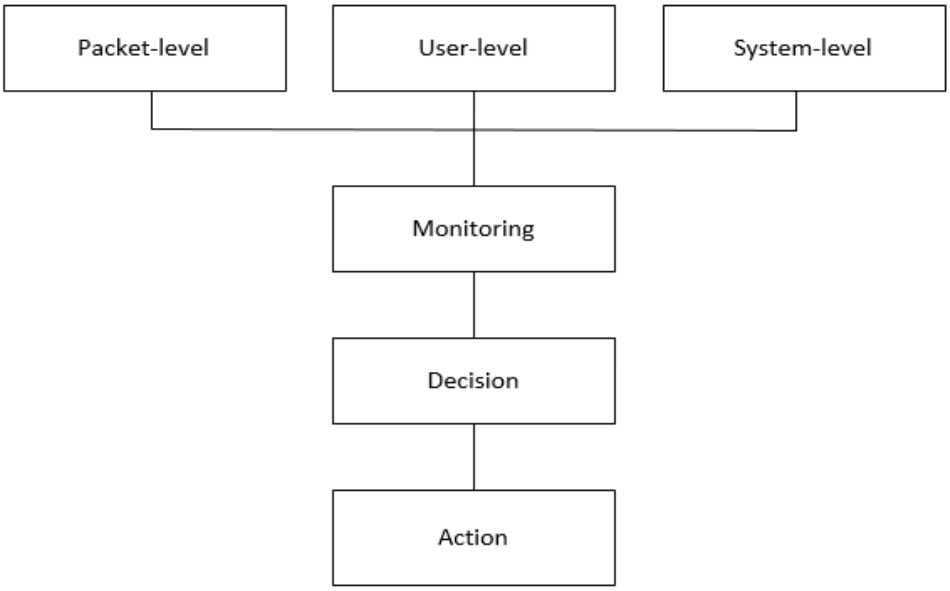


Figure 2.4: Layered Mobile Agent as suggested by Kachirski et al., [23]

Sterne et al., in [24] proposed dynamic hierarchal intrusion detection architecture. This technique has introduced a hierarchy among the nodes and nodes perform at different level such as nodes that are members of first level are called leaf nodes. Nodes have different tasks such as logging, analysis, generating alerts and reporting. After collecting data from various nodes data fusion, integration and data reduction is applied and then based on data fusion results different computations are performed before passing it to upper level. In the end the computation results are forwarded to top most level cluster to manage and detect and respond to result provided by the nodes in cluster below.

Sun et al., in [28] proposed Zone based intrusion detection scheme (ZBIDS). In this technique the network is distributed into non overlapping zones and nodes are also categorized in two categories Intra zone node and Inter zone node.

Each node runs an IDS agent that has data collection module and detection engine to collect the data. The collected data is forwarded to LACE (local aggregation and correlation) or GACE (global aggregation and correlation). These two cooperate to have more precise information to discover anomaly. In the end the intrusion response module handles alarms generated by GACE.

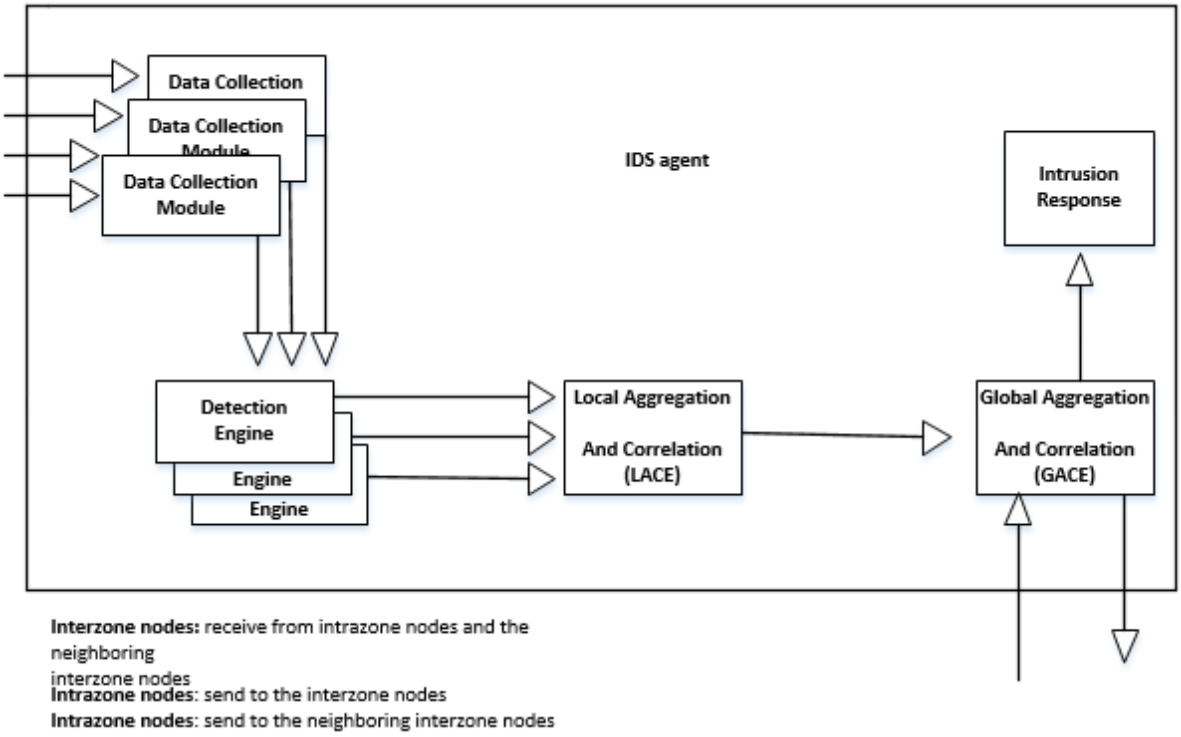


Figure 2.5: IDS agent in ZBIDS as suggested by Sun et al., [28]

The IDS based solutions have mostly been suggested for wireless ad-hoc networks and MANETs.

2.5 Critical Analysis of Proposed Solutions

All the solutions discussed in previous section employ either physical layer level detection mechanism or analytical solutions or are IDS based solutions. All the solutions

discussed in the previous section had one thing in common, that is they only provide detection mechanisms to PUE attacks rather than its mitigation.

In [4] and [5] the author proposed detection on the basis of static location and received signal strength, however this solution is infeasible in case of ad-hoc networks where the location of Primary User is not static, thus reducing the effectiveness of DDT. These solutions are limited to the case where the location is static and upon receiving a signal the SU can determine whether the signal is generated by legitimate PU or not. Also DDT has a major weakness that is it can be compromised by transmitting from vicinity/neighbourhood of a legitimate PU [1]. The technique proposed in [6] also focuses on detection and not on mitigation. In [7] finger printing scheme has been proposed to verify the transmitter of the legitimate PU but if signal is affected by more than expected noise such that it discards the signature portion of the transmitter, then the signal generated by legitimate transmitter may be considered as false.

In [8], cooperative scheme was proposed but what if the node in sensing mode leaves the network? There would not be any node to sense for the reappearance of the PU and to transmit warning to the nodes performing transmission and hence creating a chance of collision with the PU which is against the FCC recommendation which states that *"no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by Secondary Users"* [1].

All IDS based solutions require some central management authority to collect data from all nodes that are in transmission mode. Configuration of the rules against what is anomaly and what is not needs to be done to guard against specific attacks. Configuring such rules on the run time might not be possible is safety critical applications like VANETs.

2.6 Summary

Based on literature content being reviewed the existing solutions were grouped. To conclude, all discussed solutions along with their limitations are tabulated in table 2-1:

Table 2-1 Table of summary of all discussed solutions

Solution	Protection Mechanism Suggested	Evaluation
Loc Def	Detects PUE attack based on RSS (received signal strength) value	Applicable mostly in 802.22 networks not in ad-hoc networks
Network User Management Centre (NUMC) based Cognitive Radio architecture	Employs distance difference test **(**DDT**)** and the distance ratio test (DRT)	Applicable in the case where location of PU/ SU is static
Time Difference of arrival (TDOA) and Frequency Difference of arrival (FDOA)	Employs Time Difference of arrival (TDOA) and Frequency Difference of arrival (FDOA) for location verification	Applicable in the case where location of PU/ SU is static
Neyman-Pearson composite hypothesis test and Wald's sequential probability ratio test	An analytical approach employing Neyman-Pearson composite hypothesis test & Wald's sequential probability ratio test is applied which gives improvement in results by allowing user to specify thresholds for false alarms and probability of a miss	An Analytical approach. Neyman-Pearson composite hypothesis test has high probability of false alarm and adding Wald's sequential probability ratio test adds complexity to the solution
Fenton's approximation and Wald's sequential probability ratio test	An approach independent of sensor information and employs Fenton's approximation and Wald's sequential probability ratio test for detection of the attack	Analytical approach. Complexity high to make it practically applicable in especially ad-hoc networks
Fenton's approximation and Markov inequality	The proposed scheme uses received power at a SU and applies Fenton's approximation to determine the mean value. Both these values are used to determine lower bound on probability of successful PUE attack using Markov inequality	An Analytical approach and based on received power at the SU. Received power alone is not a perfect metric to make a decision regarding occurrence of an attack

Feature detection technique	Feature detection technique that is capable of identifying modulation type of a primary signal .Using this technique the system will be able to distinguish whether the signal is generated by Primary User or by malicious Secondary User	Identifies the PUE attack only does not provide any counter measure
Centralized/ access point based scheme	All the nodes send their sensing data to an access point which makes the decision about presence or absence of Primary User	Not applicable in rapidly changing networks like VANET
Transmitter fingerprinting	The phase noise of the noisy career is extracted and directly applied to identify the transmitter	Noise attenuation can seriously degrade its performance
IDS Based System	Zhang et al., proposed an IDS based scheme consisting of six modules namely the local data collection module, local detection engine, local response module, global response module, cooperative detection engine and secure communication module	Difficult to employ in ad-hoc networks
Local Intrusion Detection System (LIDS)	These scheme needs to be implemented on every node in the network. The system can be extended for global coverage by forming a network of all LIDS	Implementation on every node and configuration can add an overhead
Distributed IDS	They propose monitoring agent, action agent and decision agent. Monitoring agent is responsible for two functions i.e. network monitoring and host monitoring. Decision agent runs on only few nodes and its responsibility is to collet packet from all nodes running network monitoring agent and determine whether or not the network is under attack	Difficult to employ in ad-hoc networks specifically VANET as computational time is an overhead
Dynamic Hierarchal Intrusion Detection Architecture	This technique has introduced a hierarchy among the nodes and nodes perform at different level such as nodes that are members of first level are called leaf nodes. Nodes have different tasks such as logging, analysis, generating alerts and reporting	Difficult to employ in ad-hoc networks specifically VANET as computational time is an overhead
Zone Based Intrusion Detection Scheme	Each node runs an IDS agent that has data collection module and detection engine to collect the data. The collected data is forwarded to LACE	Difficult to employ in ad-hoc networks specifically VANET

(ZBIDS)	(local aggregation and correlation) or GACE (global aggregation and correlation). These two cooperate to have more accurate information to detect anomaly	

COGNITVE RADIO

3.1 Introduction

Wireless Communications are being increasingly used all around the world; studies suggest that every person is surrounded by the networks mostly wireless networks and each of those networks carrying multiple wireless communications. Provision of technology like the laptop, smart phones, PDA has made it more complex to provide bandwidth which of course is limited to each and every one who demands it. The usable spectrum is the same but the demand has increased by many folds.

Imagine the case of Internet around us, in the last 12-14 years, the percentage of people using the Internet has increased by 566.4% [2]. Internet is not the only technology that makes use of this spectrum bandwidth; other technologies incorporating use of wireless technology have similar usage trend as that of Internet. Consider GSM users, the number of users have increased in past years. GSM services shifting to more fast networks like 3G and 4G means the use of more wireless spectrum resources. What if this trend continues to increase in the coming years? Will there be any increase in the available spectrum range with the growing number of users? The answer to second question is NO, which means there is need of a technology that addresses this proliferation of the wireless technology around the world. The technology that addresses this problem is known as Cognitive Radio.

It is clear that we cannot generate new resources of spectrum all we can do is to use the available spectrum efficiently. Recent surveys performed in the United States show that almost 70% of the allocated spectral resources are idle at some time of the day [2]. Cognitive Radio solves the spectrum shortage problem by letting the Secondary Users SU (also known as unlicensed user) to consume the spectral resources when the Primary User PU (also known as licensed user) is not active. The users that use the resources when spectrum allocated to PU is vacant are called the Secondary Users (SU). The SU can only use

the resources till the time the PU is not using the allocated resources; however upon reappearance of the PU, the SU has to leave the channel for use by the PU. The Cognitive Radio, therefore, provides opportunistic access to the SU whenever the channel is vacant [18].

The SU has to perform sensing to detect presence of Primary User (PU) and only if the channel is vacant (i.e. the Primary User is not active), then the SU will be able to use the channel [3]. To ensure proper advantages of Cognitive Radio, i.e., to provide spectral resources to unlicensed users; two issues are of prime importance: (1) to find available slots (called whitespaces) in the bandwidth for use by the SU, (2) to have a mechanism that ensures no interference with the PU. To solve the first issue, out-band sensing is performed to find out white spaces in the network bandwidth. Based on the results of out-band sensing, the SU selects whitespace according to its Quality of Service (QoS) requirements. After selecting a white space the SU starts using it to communicate with desired SU. Once the transmission starts the SU enters into periodic transmission and sensing cycle. Each sensing interval is followed by a transmission interval the SU transmits data to communicate with other SU. During sensing interval referred to as in-band sensing the SU ensures that the PU, whose whitespace is currently being utilized, is not active. This also ensures non-interference with the PU, whose whitespace is being utilized. The SU has to vacate the channel within a certain amount of time after the re-emergence of the PU. The upcoming IEEE 802.22 standard, governing use of Cognitive Radio over the unused bandwidth of TV channels, states that the SU has to vacate the channel within two seconds of detection of PU via in-band sensing [3]. After performing in-band sensing the SU transmits for a short time then does in-band sensing again, this process continues till the time PU is active or when the transmission of SU is over and does not require resources any more.

3.2 The Vision of Cognitive Radio

Vision that led to development of this promising technology was to have a radio that detects and makes the use of the spectrum to enhance and make the spectrum usage more efficient. If the spectral resources are to be utilized as mentioned in the previous section then this will lead a user to find the available resource in spectrum which may add time as an overhead. By learning the environment Cognitive Radio can improve link reliability and help networks automatically improve capacity as well as coverage [30].

3.3 Advantages of CR

Use of Cognitive Radio as discussed in the previous sections will make the networks interoperable allowing them to communicate with different protocols. Interoperability will increase the coverage and data rate considerably making the global roaming easier. This technology would also allow us to overcome the drawbacks of the legacy analogue components.

To use any network there are two types of switching, packet switching and circuit switching. In packet switched networks the resources are shared among users however in circuit switching networks the resources are reserved and hence wasted. A lot of spectral resources can be saved using CR which involves packet switching preeminent [34].

3.4 Cognitive Cycle

The concept behind Cognitive Radio can be best understood by looking at cognitive process itself [32]. Generally the cognitive process basically consists of cycle of the under mentioned processes:

a. Sensing.

b. Analysis.

c. Reasoning.

d. Adaptation.

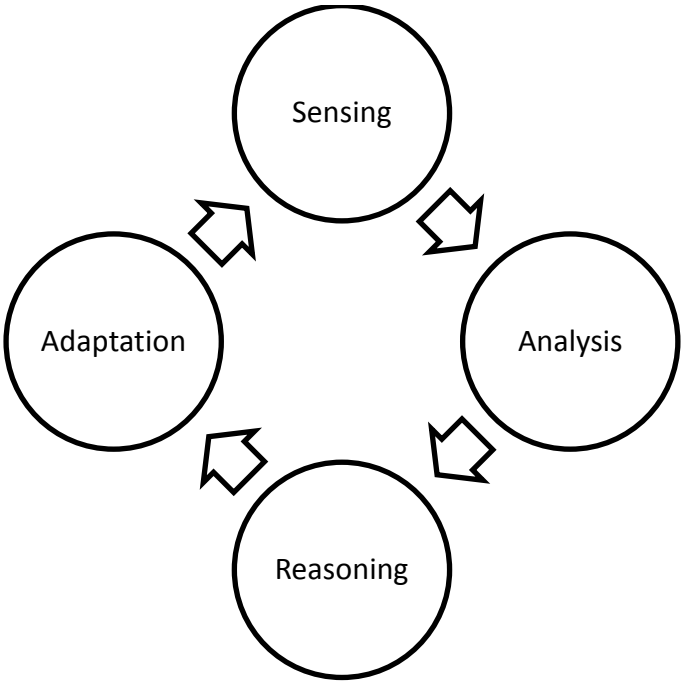


Figure 3.1: A basic Cognitive cycle

Figure 3.1 shows the four steps of cognitive cycle. Sensing is performed first and it is the most important step involved in this cycle. Based on the sensing results the radio performs analysis of the sensed data as per its QoS requirements or in other words the results are analysed and characterization of the environment is done as per the QoS requirements. When the analysis has been performed, reasoning is performed based on type of radio. In case of policy radio the reason to adapt to new parameters comes from the hard coded policies where as in learning radio it is the AI engine that helps gathering the reasoning to perform adaptation. All the succeeding actions performed in the cognitive cycle are based solely on the sensing results. In the end adaptation is performed to make a transition to the new operating parameters.

3.4.1 Tasks performed by the CR

Complying the cycle discussed in the previous section, the CR performs the following:

a. Radio analysis

b. Channel identification

c. Dynamic spectrum management.

Radio analysis is done to avoid any interference limit and to detect presence of white spaces. Channel identification is performed to achieve coherent detection and it will also enhance the spectrum utilization. Dynamic spectrum management is also performed at the transmitter to take decisions based on the results obtained from radio analysis and channel identification [31].

3.4.1.1 Radio Analysis

Radio Analysis includes both *active awareness* and *passive awareness*. In passive awareness, the information is gathered from the prevailing system. Passive awareness provides the ease to the PU and SU where they use the spectrum with mutual understanding. In other words the requisite information required by the SU to use the spectrum is provided by PU or in some cases there is a central dedicated entity to provide this information to the SU [31].

In another technique of passive awareness the SU senses the environment and adapts accordingly. This is mostly beneficial in a non-cooperative environment where the nodes work and make decisions independently. However in a cooperative environment all relevant observations of the SUs are collected and then decision is made regarding spectrum usage.

3.4.1.1.1 Passive Awareness

The passive awareness scheme incorporates different techniques some of which are discussed in the Figure 3.2.

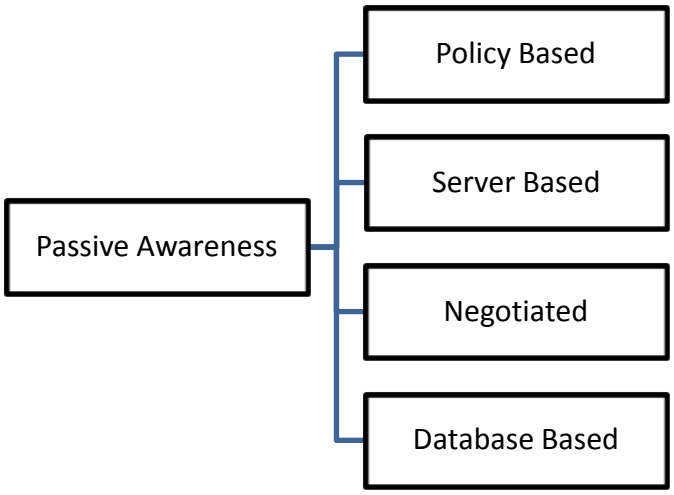


Figure 3.2: Kinds of techniques involved in passive awareness

3.4.1.1.1.1 ***Policy based system:*** In policy based scheme there is a central regulatory authority known as "Radio Regulation Authority" (RRA). The authority identifies the spectrum range for which usage is low. The RRA also has the authority to implement new rules regarding spectrum usage and will also have the authority to update the policy.

3.4.1.1.1.2 ***Server based system:*** This scheme employs a dedicated central server whose task is to gather relevant information about the neighboring nodes. This information can then be used to solve interference issues among the SUs and later develop a mechanism towards efficient usage of the spectral resources by all the SUs.

3.4.1.1.1.3 ***Negotiated:*** This scheme employs the basic functionality of the passive awareness scheme where PU and SU coordinate with each other. The PU informs the SU about the frequencies which are available in the spectrum range. This is mostly applicable in the case where the PU is the TV transmitter station. These negotiations can involve technical as well as financial aspects related to QoS.

3.4.1.1.1.4 ***Database approach:*** This technique is basically an extension of policy based approach described earlier. In addition to the policy based approach the RRA will also have to maintain a database. Besides the basic information about PU and SU it will include

information such as location, estimate of interference. The database will be updated by the RRA.

3.4.1.1.2 Active Awareness

The active awareness scheme incorporates different techniques some of which are discussed in the Figure 3.3.

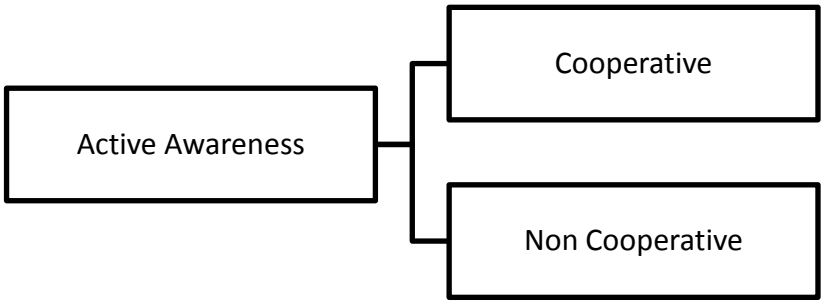


Figure 3.3: Kinds of techniques involved in active awareness

The Figure 3.3 shows that active awareness involves two techniques cooperative and non-cooperative. In active awareness the SU sense the environment and adapt according to the sensing results. This is mostly done in non-cooperative manner where all SUs sense their individual and adapt to what the environment demands. However in cooperative scheme the SUs send their sensed data to central entity for decision making. Cooperative sensing is preferable over non-cooperative scheme because of hidden terminal problem.

3.4.1.2 Channel Identification and Estimation

The channel state information is essential to ensure coherent reception. Coherent reception means that the phase of the desired signal is known to the receiver. Phase of desired signal is not enough to compute the channel capacity therefore channel state

information is also needed by the CR nodes. To compute channel state channel Identification algorithms are used that are classified as under:

3.4.1.2.1 ***Data aided***: In this type of channel estimation, it is presumed that the sent data is known and based on this presumption the channel is identified.

3.4.1.2.2 ***Non Data aided:*** In this type of channel estimation, it is presumed that the sent data is unknown.

3.4.1.2.3 ***Decision directed methods:*** This method uses approximation of the data by detecting data it as a reference for identifying the channel.

3.4.1.2.4 ***Acquisition mode training methods:*** One of the methods generally used for channel state estimation is to use the acquisition mode followed by the training mode. In the acquisition mode training sequence is used to get an initial channel estimate where pilot symbols are also used.

3.4.1.3 Dynamic Spectrum Management / Transmit Power Control

In the end when the available spectrum range has been known the CR will select the transmission parameters such as the spectrum holes and power levels to transmit. In this case managing the spectrum would make the following possible [34]:

a. SU utilizing the vacant spectrum has to coexist with the PU.

b. Interference must not surpass a certain set level.

Power/ bit rate control and spectrum management is all done at the transmitter end. Another important attribute here is the transmission technique, which mainly fall into the following categories:

3.4.1.3.1 ***Overlay:*** This transmission technique allows parallel transmission of the PUs and the SUs, this procedure is also known as the concurrent transmission. The SU uses part of its power to relay the PU data and some part of its power for its own transmission.

3.4.1.3.2 ***Underlay:*** This allows concurrent transmission or parallel transmission of the PU and the SU in the Ultra Wide Band. But due to power issues underlay scheme provides short range of communications. The difference between overlay and underlay is that underlay is limited to short range communications.

3.4.1.3.3 ***Interweave:*** Here the CR will monitor the spectrum from time to time and then communicates over the available vacant spectrum regions. It will communicate in such a way that whenever the PU will communicate and the SU in the same frequency band will remain silent.

If the SU is transmitting and at the same time PU starts to transmit with the same frequency then the SU has to vacate the channel in time T, where T is the maximum time a PU can withstand the interference. The draft standard for 802.22 networks suggests that the SU has to vacate the channel within 2 seconds after the reappearance of the PU [21]. The Cognitive Radio requires more effective and reconfigurable hardware to deal with various RF spectrum and basebands simultaneously.

3.5 Implementation Issues

The introduction of this promising technology poses many challenges like spectrum sensing, interference management, resource allocation, RF design and others. Following are the implementation issues that pose a challenge to deployment of CR [31] [32]:

a. Sensing.

b. Interference Management.

c. Resource allocation.

d. Architecture.

e. Physical Layer.

f. Protocols and Standardization.

g. Signaling.

h. Security.

3.5.1 Sensing

This is the most important characteristics of the CR. The CR must have to ability to sense the radio channel, or inother words the CR must have ability to know when the spectrum is available and at the same time sensing is important to ensure non-interference with te PU because it is sensing that lets the SU know that the PU has reappeared. Two types of sensing is performed by the SU. One is known as the out-band sensing which is basically performed to find out the white spaces or vacant holes in spectrum. Other is known as in-band sensing that the SU periodically performs once it starts to use any white space. The purpose of in-band sensing is to ensure non interfrence with PU.

Upon sensing there are three kinds of spaces that exist in the spectrum:

a. Black Spaces

b. Grey Spaces

c. White Spaces

Black spaces are the spaces occupied by devices with high power interference. Grey Spaces are employed by devices with little power interference. White Spaces are free to use.Black spaces are forbidden to be used by the SU for transmission because of the high power interference. So the concerning are white spaces and grey spaces. Spectrum sensing can also be termed as spectrum detection because sensing involves detection; many schemes were proposed to identify the white spaces in the spectrum, sensing techniques are mainly of two types [35]:

3.5.1.1 ***Energy Detection:*** Also known as the stationary detection. The performance is a concern in this technique as detection scheme is prone to varying noise levels and

interference. Also the energy detector cannot distinguish between modulated signals, noise, and interference and can only determine the presence of the signal. This scheme does not work when signal is a direct sequence or a frequency hopping signal.

3.5.1.2 ***Feature Detection:*** Also known as cyclo-stationary detection. Feature detection is preferable over Energy Detection as its main advantage it that it can sense signals with very low SNR.

The biggest challenge related to spectrum sensing is to develop a cost efficient sensing technique which can sense weak signal.

3.5.2 Interference management and resource allocation

The better utilization of the spectrum can be made in a case where the Secondary User uses the frequency band which is not utilized by the PU at that point in time. Most of the research concerning the use of Cognitive Radios suggests that the CR should sense the spectrum and then decides which portion of the spectrum vacant at that instance of time. Upon sensing results it will start utilizing that space of the spectrum. Some recent studies in this regard have enhanced the CR protocols to let the SU transmit concurrently with PU at an acceptable interference rate.

3.5.3 Architecture

While lot of research is underway on the protocols and sensing algorithms, a lot of effort is put in towards developing hardware and software architecture in order to support CR implementations.

In the case if the CR environment consists of a single CR node then this situation is quite similar to Software Defined Radio (SDR) and research work in this regard is applicable to CR. As far as environment suggests the need of cooperation among CR nodes, it demands

much more work. Questions like compliance, inter-operability with ISO/OSI or TCP/IP protocols need to be addressed as well.

It is worth mentioning here that an important part of implementing the hardware is to have ready equipment that builds base of the architecture. Work needs to be done in this regards as well. Thorough tests need to be conducted on readiness of the equipment and also to check whether or not it is compatible with existing network infrastructure, as SU has to sense the bandwidth already being used which is sometimes being wasted in the case of idle sate of the PU.

After these devices have gone through the tests they have to go through the certification process. To prove that a CR will remain within working limits will be more problematic task than the normal conventional radios. This is why the future hardware vendors must be well aware and up to the task so that CR can be implemented and is able to deliver the basic functionality that it has to offer with causing any overhead and interference.

3.5.4 Physical Layer

Every CR node must be able to detect which portion of the spectrum is vacant or in other words must possess sensing capability. Sensing mechanism should be such that it ensures non-interference mechanism and does not give false readings.

SU uses the spectrum whenever the PU is not active therefore we say that CR provides opportunistic access to the SU. One of the main things to consider for the opportunistic access is to identify whitespaces and then make it available to applications without affecting the Primary User because as per FCC recommendation *"no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by Secondary Users"*.

3.5.5 Protocols and Standardization

The CR has many features involved in its successful implementation like sensing, spectrum mobility etc. So to have these working we need protocols that govern these features, research is being carried out in this regard and we need protocols that govern implementation of CR in every field.

Work still needs to be done in the standardization of CR principles. Basically there are three kinds of standards:

a. Proposed standard

b. Draft standard

c. Internet standard

The description of these levels as proposed by Internet Engineering Task Force is as follows. A Proposed Standard is defined as *"The basic maturity level for the standards track is the Proposed Standard".* Draft Standard is defined as *"A requirement from which at least two independent and interoperable implementations from different code bases have been developed, and for which sufficient successful operational experience has been obtained, may be elevated to the Draft Standard level".* Internet Standard is defined as *"A specification for which significant implementation and successful operational experience has been obtained may be elevated to the Internet Standard level"* [33].

Internet standard is at the highest maturity level. It is applicable for wide spread use in the world. As far as CRs are concerned, only draft standard relevant to use of CR in TV networks is present and standardization effort is still to achieve any maturity level as far as use of CR in Wi-Fi, GSM etc. is concerned.

3.5.6 Signaling

Signaling is another area on which emphasis needs to be put on. A CR requires configuration of lower level parameters and the underlying infrastructure to provide services reconfiguration and reprogramming. These tasks pose two main challenges which are as under.

a. Due to the limitations in the layering principles efficient operations, the programmable radios/devices must provide cross layer interfaces. The idea behind the cross layer technique is to make use of the local information produced by other protocols, to allow optimization and provide improved network performance.

b. Due to limitations we have to incorporate the cross layered approach but introduction of this approach requires signaling architecture that supports cross layer solutions. Several signaling architectures are available, which are classified on the basis of their applicability in providing different interaction among protocols at different layers, or on whole the classification is on the basis of inter network or intra network signaling.

3.5.7 Security

More research carried out till now is focused towards other issues as discussed previously, but unfortunately the security issues gathered a little less attention as compared to other issues. Security is the most critical aspect involved in the implementation of CRN, because if an attack (due to an unaddressed security issue) occurs, then CR will be unable to deliver its basic functionality that is the opportunistic access.

Work needs to be done on developing secure protocols for the SU having mechanism such as authentication, authorization. CRN is based on the assumption that PU and SU are

to be differentiated in the network, authenticating PU and SU is specifically mandatory since both PU and SU deserve different level of authorization and different privileges to access the spectrum. Authentication can be easily implemented for centralized architectures by having a centralized authority; however it is difficult to implement such scheme in a distributed/ non-cooperative environment.

The CRN provides conditional authorization. Conditional authorization refer to the term where the SU can only transmit in licensed frequency bands till the time the Primary User for that licensed band does not require that band.

In the coming chapter security issues to CRN by describing possible attacks with the emphasis on PUE attack will be discussed in detail.

3.6 Summary:

In this chapter details about Cognitive Radio were discussed. Firstly the need that became the reason for invention of CR was discussed and then the importance of CR in solving the spectrum shortage problem was discussed. In the following section the Cognitive Cycle was introduced and described. Then discussion was made on tasks performed by the CR including analysis, channel identification and spectrum management. In the last section issues related to deployment of CR including the sensing, interference management, resource allocation, architecture, physical layer, protocols, standardization, signaling and security were also discussed in detail.

Attacks on Cognitive Radio Networks

4.1 Introduction

With the improvements in technology, security based threats also emerged that may hamper the benefits technology has to offer. Each node which is part of a network is susceptible to many security based threats. The threats are not only limited to nodes or existing technologies but these threats pose serious challenge to upcoming technologies like Cognitive Radio. As Cognitive Radio solves spectrum shortage problem and it has increasing use in many applications once it gets deployed, therefore it is vulnerable to many attacks like the Primary User emulation (PUE) attack, hello flood attack, sinkhole attack, jamming attack, lion attack etc. [1]. Attacks to CR are discussed in sufficient detail along with the solutions prescribed to counter those attacks in this section. Since Primary User Emulation Attack is the focus of this thesis, it will be discussed in the next section in more detail. The other attacks to Cognitive Radio are:

a. Objective function Attack
b. Jamming
c. Spectrum Sensing Data Falsification Attack
d. Control Channel Saturation DOS Attack
e. Selfish Channel Negotiation Attack
f. Sinkhole Attack
g. Hello Flood Attack
h. Lion Attack

4.1.1 Objective Function Attack

The Cognitive Radio is basically a smart radio that senses its environment and adapts accordingly. The cognitive engine is basically responsible for adapting according to the certain parameter such as bandwidth, power, modulation type, coding rate, channel

access protocol etc., in order to abide by the obligations such as low energy consumption, high data rate, and high security [36]. The cognitive engine which is the sole responsible for all this calculates these parameters by unravelling the objective functions.

The attack done by manipulating the radio parameters under control of the attacker, while the cognitive engine is running and resolving the objective functions so as to find the appropriate radio parameters in order to adjust according to the current environment is called Objective Function Attack. The intent or motivation behind this attack is that attacker can make the results tailored according to his interest.

4.1.1.1 Defending against Objective Function Attack

León et al., suggest in [37], to define threshold values for each updatable radio parameter. If the radio parameters do not satisfy the limits as defined by thresholds; the communication stops. The authors also suggest employing IDS based solution.

4.1.2 Jamming

Jamming in other words can be termed as a Denial of Service (DOS) attack. In this attack the attacker creates a situation where the legitimate SUs cannot send or receive data; consequently, creating a denial of service situation. Such situation can be created in different ways such as sending continuous data packets so that the legitimate SU never finds channel idle. In another technique the attacker my send continuous packets to receiver thus making it unavailable by occupying all the communication capacity that it has or in other words creating a ping to death.

In another technique the attacker may use the smart methodology of smart jamming. In smart jamming the attacker uses the information of the learning radio and instead of transmitting continuous packets it applies these techniques when the nodes are in sensing and whenever the nodes do sensing if the attacker applies any such technique as

explained above he may force the SUs in to jammed situation where they will be unable to perform any transmission.

This attack is different from PUEA in a sense that the attacker has to be use proper jamming devices or jamming techniques in order to refrain SU from using the network where as in PUEA, SU can be refrained by emulating or pretending to be the PU of the network.

To make things even more worst the attacker may disrupt communication that would result in the corruption of packets received by genuine SUs. A more hazardous attack may occur in cooperative schemes of CR where the attacker jams the channel dedicated for exchange of sensing information between CRs. Jamming attack can be done on the data link and physical layers. Basically there are four types of jammers [1]:

a. Constant Jammer
b. Deceptive Jammer
c. Random Jammer
d. Reactive Jammer

Constant jammer transmits data packets uninterruptedly without any concern to the data link layer protocols. The deceptive jammer works by deceiving the legitimate users and sends out packets continuously making the users switch into a receiving state in which they remain till the time they detect a continuous stream of incoming data packets. The random jammer inserts quite intervals between the jamming signals, however it adopts the behavior of a constant or deceptive jammer. The reason of inserting quite intervals may be to conserve energy in case the jammer doesn't have unlimited power supply. The reactive jammer employs continues to sense the channel all times and whenever it detects any communication, it starts transmitting the jamming signals. This jammer is solider to detect because it is not transmitting all the time.

To perform this attack at data link layer, the attacker sends attack packets to a particular radio channel, thus creating a situation where all nodes in the radio vicinity start assuming that the channel is engaged and defer their transmission of data [38].

To perform this attack at the physical layer, the attacker may use a specialized device such as programmable radios and waveform generators, capable of emanating energy at the same frequency as used by other nodes in the network. This creates interference among the transmissions.

Sampath et al., in [39] describe an attack scenario where a single Cognitive Radio sends jamming packets to multiple channels. It sends packet to one channel and switches through channels quickly after it has sent the desired number of packets. This process repeats and after sending the jamming packets to the last channel, the attacker returns to the previous channels and repeats the jamming cycle.

4.1.2.1 Defending against Jamming

Since DoS attack can be performed at both data Link and physical layer, therefore we need to have detection at these both layers. In data link layer detection, denial of service attack can be detected by sensing the channel the nodes want to use for their transmission. For this, employing carrier-sensing multiple-access (CSMA) may provide the desired result. In CSMA, node continually senses a channel until it finds it to be idle and upon finding a channel as idle the node waits for some time before starting transmission (propagation delay) so as to make sure that the channel is vacant.

In the physical layer detection, the legitimate devices should be able to distinguish between the normal and abnormal level of noise in a channel. This can be done by collecting data regarding the noise level in the CRN and then constructing a statistical model to use for comparison when a denial of service attack occurs [38].

In [40], the authors suggested Signal Strength Consistency Checks, a jamming detection technique that inspects the signal strength (SS) and packet delivery ratio. Packet delivery ratio (PDR) is the ratio of packets delivered to packets sent. If SS is high and PDR is low it is assumed that the channel is being jammed, unless one of the neighbours has high SS and PDR. Another technique called Location Consistency Checks is suggested. This is applicable in the case where the location of the neighbours is important. The location information is advertised by each node and can be acquired through GPS. A node is considered as jammed when its neighbours have low PDR.

4.1.3 Spectrum Sensing Data Falsification Attack

Spectrum Sensing Data Falsification, also known as the Byzantine Attack, is done by an attacker, by sending incorrect spectrum sensing results to its neighbours (in case of distributed schemes) or to the fusion centre (in case of cooperative schemes). This propagation of false sensing results to the neighbours causes a wrong spectrum-sensing decision at the victim [49] [50].

Both centralized and distributed CRN are susceptible to this attack. SSDF attack is more destructive in a distributed CRN, because the incorrect information spreads quickly and there is no mean to control its spread, however in the centralized CRN, the central entity can lessen the effect of false information by matching the data received from all nodes in CRN.

4.1.3.1 Defending against Spectrum Sensing Data Falsification Attack

The authors in [51] presented an analytical approach to counter SSDF attack. In the proposed scheme the performance limits are established in terms of the fraction of SSDF attackers, which shades the vision of the fusion centre.

In [52], a fusion technique is proposed that collects sensing results from all nodes in the CRN. Then all the gathered results are summed. If the sum is greater than a certain threshold, then the final sensing result denotes that the PU is active. Otherwise, the band is determined to be free, which means absence of PU.

In [53], the authors proposed Weighted Sequential Ratio Test (WSRT) to counter SSDF attacks. In the proposed technique each node that has to perform sensing collects local sensing reports from neighbouring nodes. This scheme also employs reputation based mechanism. Each node is initially given a reputation value equal to zero. Upon each correct sensing report the reputation value will be increased by 1.

The authors in [41] proposed a weight based fusion scheme incorporating a trust approach and pre-filtering techniques. The approach relies on pre-filtering the data to identify and nullify sometimes faulty and permanently faulty malicious users by assigning a trust factor to each user.

The authors in [42], proposed a detection scheme for SSDF attacks that works by counting mismatches between the local decisions and the global decisions at the fusion centre.

In [43], the authors proposed a Bayesian detection scheme that requires the knowledge of a priori conditional probabilities of the sensing results. Numerous cases occur based on the local and final sensing results, which are either correct or incorrect. A small cost is assigned to the correct cases and a large cost is assigned to the wrong cases. The overall cost is the sum of all the costs assigned previously weighted by the probabilities of the corresponding cases.

In [44], the Neyman-Pearson test was proposed; it requires the user to define two things. One is maximum acceptable probability of false alarm and the second is maximum

acceptable probability of miss. The Neyman-Pearson test pledges that the other probability is minimized, whereas the defined probability is accepted.

In [45] the authors proposed an algorithm that computes the mistrustful level of SUs based on their past behaviours. This algorithm calculates trust values as well as consistency values (used to eliminate the influence of malicious users on the PU detection results). For a node with fewer bad behaviours, the trust value recovers after a certain good behaviours, however the trust value is impossible to recover in case of regular bad behaviours.

4.1.4 Control Channel Saturation DoS attack

In a CRN with multiple nodes, the nodes perform channel negotiation in distributed manner, prior to their communication. During the channel negotiation several control frames are exchanged to reserve the channel. Since many nodes may want to communicate simultaneously, therefore the common channel used for exchanging control frames may become a bottleneck due to finite capacity of the control channel. An attacker intending control channel saturation DOS attack may generate fake control frames to occupy the control channel and thus degrading the network performance.

It is significant to mention here that this attack is applicable only to distributed CRNs because all control frames in centralized CRNS are passed after authentication by the central entity.

4.1.4.1 Defending against Control Channel Saturation DoS Attack

Control channel saturation attack can be mitigated by adapting a trusted architecture employing sequential probability ratio test. In the trusted architecture any suspicious node will be monitored and evaluated by its neighbours. Based on monitoring the neighbour can then perform a sequential analysis on observed data, and determine whether a node is acting maliciously or not. [46].

4.1.5 Selfish Channel Negotiation Attack

Energy and power are finite characteristics, as far as nodes in a CRN are concerned. Nodes for conserving energy may refuse to forward data in place of other nodes, so as to help them in their communication. By doing this a node may increase its throughput which resulted from selfishly concealing the channel [46]. Same objectives can be accomplished if the selfish host is able to alter the proper MAC behaviour of the nodes in the CRN. This attack can severely destroy throughput of the whole CRN.

4.1.5.1 Defending against Selfish Channel Negotiation Attack

Selfish channel negotiation attack can be mitigated by adapting a trusted architecture employing sequential probability ratio test as applicable in mitigating control channel saturation attack [46].

4.1.6 Sinkhole Attack

Sinkhole attack is done by an attacker who publicises itself as the best route to a particular destination, persuading the neighbours to use it for forwarding their packets [47]. As the attacker receives packets from all nodes, it can either read the conversation or drop the packets by not forwarding it to the destination it was meant for. A severe form of this attack is where attacker advertises itself as best path to the base station in case of centralized schemes.

4.1.6.1 Defending against Sinkhole Attack

Sinkhole attack is hardest to detect among other attacks to CRNs. However defence against this attack lies in development of geographic routing protocols. Geographic routing protocols construct an on demand topology using only local communications and information without instigation from the base station. Using this scheme all the traffic is

transmitted to the geographical location of the actual base station and it is hard to divert it to a malicious node for creation of a sinkhole [47].

4.1.7 Hello Flood Attack

An attack done where an attacker broadcasts a packet to all nodes in a CRN, with sufficient transmission power to persuade them that the attacker is their neighbour, is called HELLO flood attack [47]. An attacker may use this attack from far away to convince the victim that he is its neighbour. As a result of this victim switches to wrong route and does all its transmission through the malicious node (attacker). This will result in high number of lost packets. Since all of them will be using the same route, even if the victim realizes the attack, it will be left with no neighbours to forward its packets to.

4.1.7.1 Defending against HELLO Flood Attack

The authors in [47] proposed to employ symmetric key cryptography to counter Hello flood attack. Each node should share a symmetric key trusted central authority. The two parties will share a symmetric key, which will provide two benefits; one is the authentication among the nodes sharing the key and second is the nodes will be able to encrypt the transmission between them. The number of shared keys should be limited so as to prevent an attacker from creating a session key with every node on the network, the authors also proposed that if a node claims to be the neighbour of many nodes in the network, an alarm should be raised.

4.1.8 Lion Attack

The lion attack is a cross-layer attack performed at the physical layer and it exploits the instinctive capability of TCP at the transport layer. The PUEA forms a basis of the Lion attack. When a PUEA is performed all SUs have to vacate the channel for use by the PU (spectrum mobility). When this spectrum handoff occur, the TCP running at transport layer

of the SU, will be unaware of this handoff and will keep creating logical connections. Also the TCP at SU's transport layer continues to send packets to port number of the receiver without receiving any acknowledgments. When no acknowledgment is received TCP follows it's built in mechanisms like retransmission timer, fast retransmit etc. To make situation even worst, an attacker can create total network starvation, if he can predict the frequency band tested in a handoff, and claim it by performing PUEA [1],[48].

4.1.8.1 Defending against Lion Attack

To counter Lion attack, Hernandez-Serrano et al. in [48] suggested, employing data sharing among physical/data link and transport layers. By sharing data among layers, the nodes in CRN will be able to freeze TCP connection parameters during handoffs and acclimate according to the new network conditions after the handoff. A group key management (GKM) was proposed that can be used to allow nodes in CRN to achieve confidentiality and authentication.

4.2 Primary User Emulation Attack (PUEA)

PUE attack is done by a malicious SU during the sensing time masquerading as a PU to obtain the network resources, thus refraining other SUs from using the resources. The PUE attack that if successful forms a basis of other attacks like a Lion attack or in extreme form it can result into a Denial of Service (DoS) attack.

The Figure 4.1 is the basic diagram representing the PUEA scenario. It assumes the users are the mobile phone devices. The legitimate PU is in the idle state and a malicious SU is emulating itself as the PU of the network thus refraining the victim SU from using the resources. The attacker can launch malicious PUE attack with the motivation to prevent legitimate SUs from using the holes found in a spectrum.

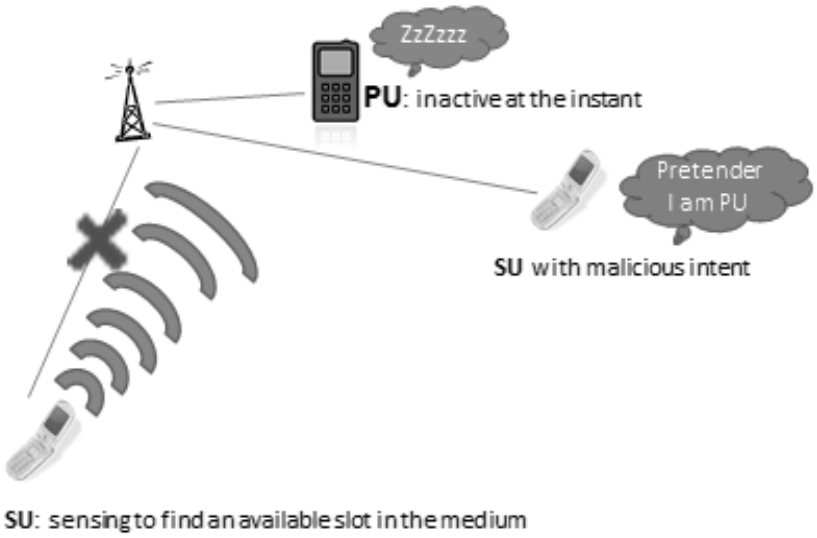


Figure 4.1: A basic diagram describing the PUEA scenario

Both types of Cognitive Radio Policy Radios and Learning Radios are susceptible to PUE attack. The effect of the attack from policy radio disappears as soon as the attacker vacates the channel, however in case of learning radios the situation gets even more critical. Since in learning radios information about behaviour of the PU can be gathered and idle times of PU can be predicted and on basis of this behaviour PUEA can be launched every time when the channel is not in use by the PU.

The effect of such attack would be more disastrous, as the behaviour will get predictable and legitimate SU would never be able to use such a spectrum slot ever again if the malicious SU launches the attack every time. PUE attacks are getting more and more sophisticated when the attacker is having some knowledge about the CRN.

4.2.1 Explanation of Attack through a scenario

In-band sensing was discussed in Chapter 3. An attacker can exploit this inbuilt capability of CRN, since sensing is periodic and after getting hold of a slot the SU enters into periodic sensing and transmission cycles as represented by the figure 4.2.

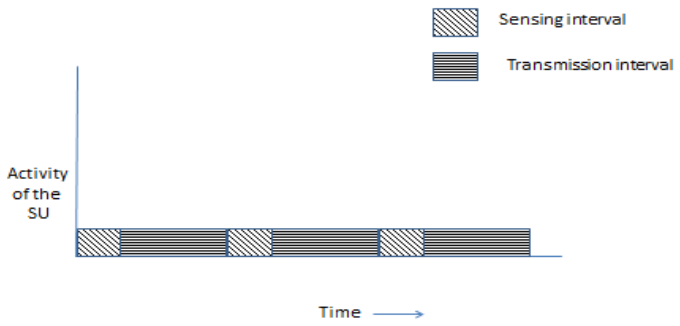


Figure 4.2: Representation of usual activity of SU depicting sensing and transmission slots.

In the Figure 4.3, it can be seen that there is one PU who is in inactive state initially and during most of time in the considered scenario. When the PU is inactive, SU_1 appears and performs sensing to check for availability of bandwidth. Upon sensing SU_1 finds network to be available and transmits. Once SU_1 is transmitting SU_2 appears and senses for availability of networks and finds network to be unavailable therefore enters a timed wait interval. In the meantime SU_1 finishes its transmission and leaves the network. SU_2 senses again and finds the network available and then enter transmission phase. Upon finishing its transmission SU_2 leaves. Then it can be seen that SU_3 appears and senses for network availability and it finds the network available it enter into transmission phase. Upon completion of first transmission slot SU_3 has some more data to send therefore it senses again to check for reappearance of the PU and based on sensing SU_3 finds PU to be active therefore SU_3 has to leave the network as the PU has high priority and SU can only use the spectral resources till the time PU is inactive.

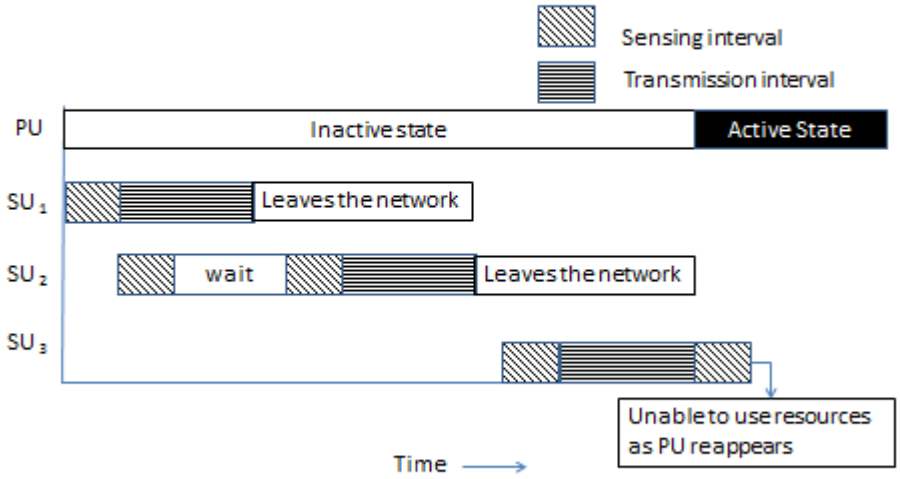


Figure 4.3: Representation of ideal case consisting of a PU and three SUs

Now consider an attack scenario where malicious SU represented as SU_M emulates itself as a PU and makes the network unavailable for others SUs. In the Figure 4.4, it can be seen that SU_1 appears and performs sensing. Based on the sensing results it transmits and then leaves the network. While SU_1 was transmitting, SU_2 appeared and performed sensing and entered into wait state. Once SU_1 leaves the network, a malicious SU emulates the characteristics of the PU and pretends to be PU. SU_2 senses again which is at point in time when SU_1 is no more using the network but a malicious SU is pretending to be PU thus making SU_2 to enter in other waiting interval. Ultimately SU_2 leaves the network without getting a chance to transmit because the network was made unavailable by phenomena that is called the Primary User Emulation Attack.

Similarly SU_3 appears and senses while emulation by malicious SU is under way. SU_3 senses for network availability but finds it to be unavailable because of emulation attack. The same is depicted by the Figure 4.4.

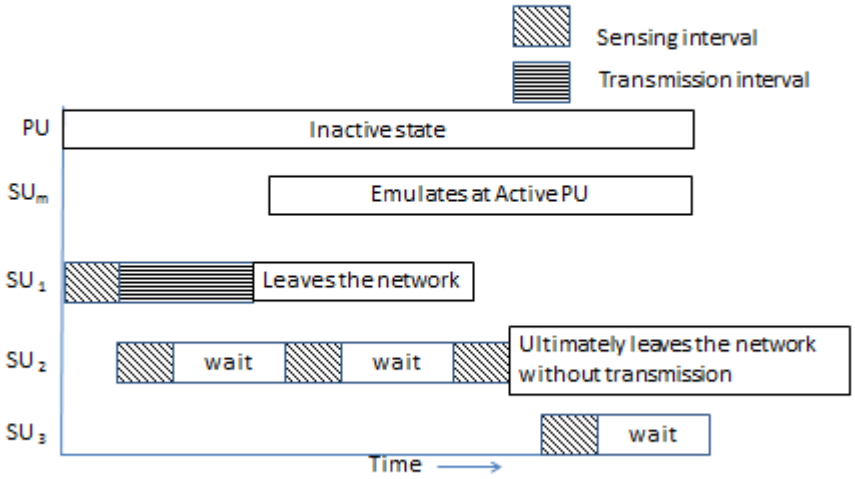


Figure 4.4 Representation of attack scenario by malicious SU making network resources unavailable.

If the PUE attack is successful then Cognitive Radio technology is unable to deliver the purpose it has been devised for i.e. providing access to unlicensed users whenever the spectrum is vacant. However situation can get more worst if malicious SU schedules PUE during each sensing interval ultimately causing a denial of service (DoS) attack.

To elaborate the attack in more detail a flow diagram is drawn in Figure 4.5. It can be seen in Figure 4.5 that a SU is sensing whether the PU is active or not. Initially the SU finds PU to be inactive and therefore starts transmission. After transmission cycle the SU checks whether or not the PU is active again, so the SU performs sensing and while sensing it finds PU active because of emulation by the malicious SU. The result is spectrum mobility i.e. the SU has to vacate the spectrum resource currently being utilized.

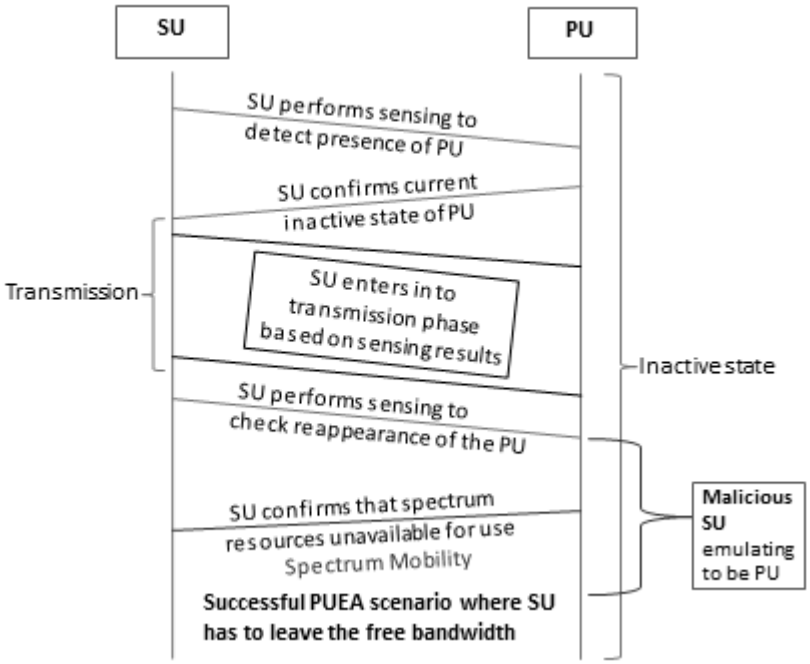


Figure 4.5: Flow Diagram depicting scenario of successful Primary User Emulation Attack

4.2.2 Types of Primary User Emulation Attack

There are two types of this attack.

Selfish PUE attack: It is the case in which the focus of the attacker is to increase its own share in the spectral resources [1].

Malicious PUE attack: It is the in which the attacker prevents legitimate SUs from using the resources [1], [20].

To elaborate these types of PUE attacks further consider a simple scenario consisting of a Primary User (PU), a legitimate Secondary User (SU_1) and a malicious Secondary User SU_M.

4.2.2.1 Selfish PUE attack

To explain the difference between the two kinds of PUEA, we have considered the PU to be inactive during the scenario. In the Figure 4.6 it can be seen that there is an inactive PU. SU_1 appears and senses for the spectrum slot and finds a slot available. Based

on sensing results the SU_1 enters into transmission phase and transmits. After completing the first transmission slot, it performs in-band sensing to check for reappearance of the PU whose whitespace was currently being utilized. At this particular instant, SU_M starts emulating as the PU of the network thus denying the SU_1 to enter into another transmission slot. After emulating, SU_M gets hold of the slot, and starts transmission which continues. In this way the malicious SU maximizes its own benefit selfishly, and refrains legitimate SU from transmission.

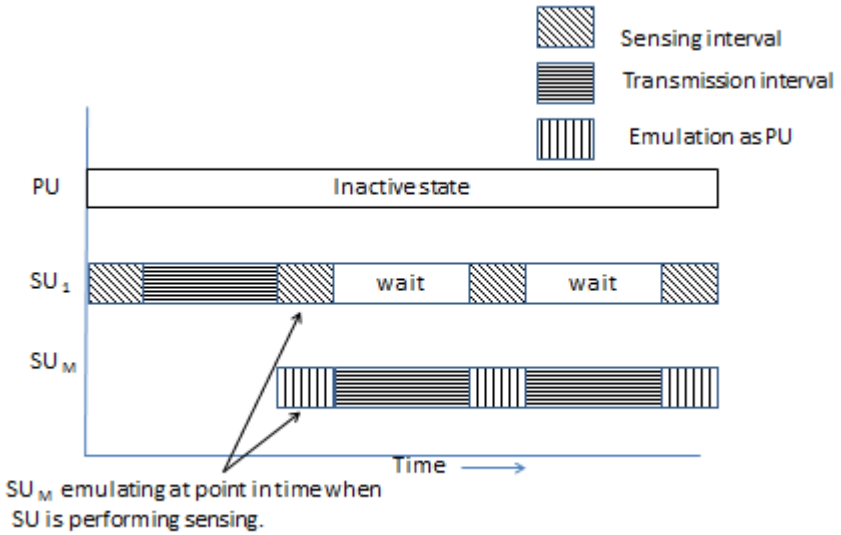


Figure4.6: Representation of selfish PUE attack scenario consisting of an inactive PU, a legitimate SU and an attacker SU_M

4.2.2.2 Malicious PUE attack

Now consider Figure 4.7 that depicts the case of malicious PUE attack. As a part of consideration the PU is inactive, and SU_1 gets a chance and transmits one time. However the difference lies in the behavior of SU_M. In the previous scenario, the SU_M after getting hold of the bandwidth started to transmit, but in malicious PUE attack the SU_M does not transmit, instead the intent here is to make the channel unavailable for others thus creating a DoS attack situation. The SU_M knows the periodic sensing slots and emulates whenever legitimate SU senses for the network availability. This sort of attack can also be termed as a

smart jamming attack. Malicious PUEA can be more frequent because emulating the characteristics of a PU at all times may not be possible due to power constraints so attacker has to switch to a smarter approach that is smart jamming or malicious PUEA.

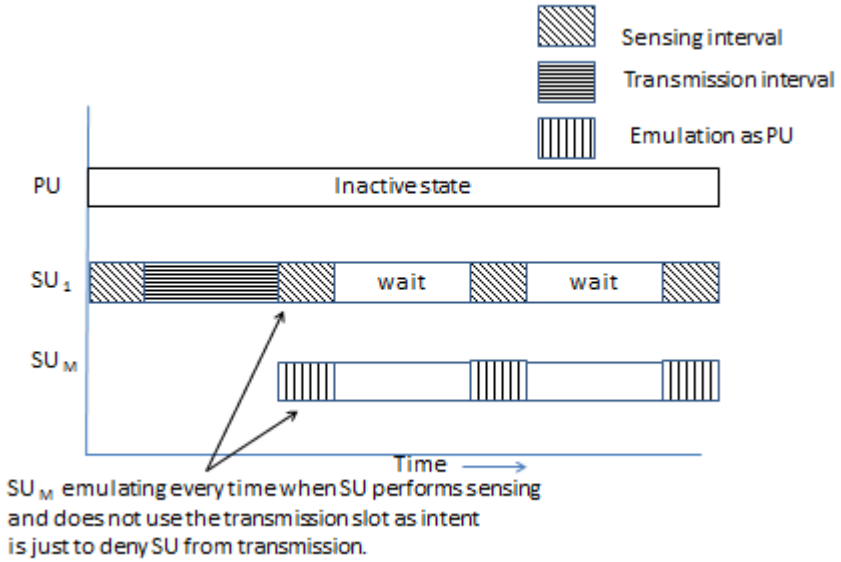


Figure 4.7: Representation of malicious PUE attack scenario consisting of an inactive PU, a legitimate SU and an attacker SU_M

4.2.3 Defending against the PUEA

Chen et al., in [4] proposed a technique that detects PUE attack based on RSS (received signal strength) value. As an extension of their work they proposed distance difference test (DDT) and the distance ratio test (DRT) [18]. Khare et al., suggested a technique that employs Time Difference of arrival (TDOA) and Frequency Difference of arrival (FDOA) for location verification. Jin et al., in [8], proposed an analytical approach employing Neyman-Pearson composite hypothesis test & Wald's sequential probability ratio test is applied which gives improvement in results by allowing user to specify thresholds for false alarms and probability of a miss. In [9] an approach independent of sensor information and employs Fenton's approximation and Wald's sequential probability ratio test for detection of the attack was proposed. Anand et al., in [10] proposed scheme that uses received power at a SU and applies Fenton's approximation to determine the mean value.

Both these values are used to determine lower bound on probability of successful PUE attack using Markov inequality.

Ramzi Saifan in [12] proposed feature detection technique that is capable of identifying modulation type of a primary signal .Using this technique the system will be able to distinguish whether the signal is generated by Primary User or by malicious Secondary User. Kaligineedi et al., in [13] proposed a technique in which all the nodes send their sensing data to an access point which makes the decision about presence or absence of Primary User.

Zhang et al., in [22] proposed an IDS based scheme consisting of six modules namely the local data collection module, local detection engine, local response module, global response module, cooperative detection engine and secure communication module. Albers et al., in [27], proposed a scheme that needs to be implemented on every node in the network. The system can be extended for global coverage by forming a network of all LIDS. Kachirski et al., in [23] proposed monitoring agent, action agent and decision agent. Monitoring agent is responsible for two functions i.e. network monitoring and host monitoring. Decision agent runs on only few nodes and its responsibility is to collet packet from all nodes running network monitoring agent and determine whether or not the network is under attack. Sterne et al., in [24] proposed a technique that introduces a hierarchy among the nodes and nodes perform at different level such as nodes that are members of first level are called leaf nodes. Nodes have different tasks such as logging, analysis, generating alerts and reporting. Sun et al., in [28] proposed a technique in which each node runs an IDS agent that has data collection module and detection engine to collect the data. The collected data is forwarded to LACE (local aggregation and correlation) or

GACE (global aggregation and correlation). These two cooperate to have more accurate information to detect anomaly.

4.3 Summary

In this chapter the attacks relevant to Cognitive Radio were discussed. In the first section all attacks (other than the PUEA) were discussed in sufficient detail along with their proposed solutions. Since focus of this research is on PUEA, therefore PUEA was discussed in detail. A simple scenario was considered to create an in depth understanding of the attack. After explanation of the attack, the types of PUEA i.e. selfish PUEA and malicious PUEA were discussed. In the end a brief description of all solutions to counter PUEA (proposed by different authors), was presented, which can be found in detail in chapter 2.

SOLUTION & RESULTS

5.1 Introduction

Primary User Emulation Attack is an attack done by a malicious user pretending to be Primary User of the network thus denying legitimate SUs from using the network. After discussion on the existing solutions to PUEA and their limitations in Chapter 4, the proposed approach will be discussed in this section.

The main objective behind the tests was to evaluate the effect of proposed technique on the radio environment. To achieve main objective different types of experiments in three different scenarios were done. 50 tests were conducted in each of these three scenarios, to record data, and average value of these tests was taken in end. In the first scenario the behaviour of nodes in attack free environment was evaluated and data like the number of packets transmitted by the PU and SU was recorded. In another scenario malicious PUEA was done on the environment and the effects of PUEA were evaluated in the attack environment and data like the number of packets transmitted by each node, emulation timing was recorded. In the third scenario, after implementation of the proposed technique, its effect against PUEA was evaluated with the same parameters as in the attack environment. The comparison between data recorded in attack free and attack environment was made to achieve the objective of setting up this test bed or in words to evaluate the effect of proposed technique.

Network Simulator 2 (NS2) version 2.31 was used to setup a test bed from which result can be generated. Open source CR patch was integrated to basic NS2 along with other files make the CR running [26]. Each test was run for 150 seconds.

Radio environment consisting of six (6) nodes was considered in which two nodes were PU, two were SU and two nodes were SU_M (whose task was to emulate as PU). The appearance of PU and SU_M was random and dependent on the generated random number

to fulfil the set condition. If the random number satisfied the condition only then PU or SU_M emerged, that depicts an environment close to the real world in which all nodes/ users can have random appearance.

Constant Bit Rate (CBR) traffic was considered among the nodes. CBR is an allocation scheme that requires the node to specify the bandwidth at the start of transmission (on basis of its QoS requirements). The allocated bandwidth remains the same throughout the transmission. CBR was preferred so that the proposed scheme is also applicable to safety critical applications (like VANET) requiring constant bandwidth, throughout the transmission, and without having to involve in TCP based handshaking steps that may add a performance overhead as well.

5.2 Evaluating behaviour of nodes in attack free environment

Firstly the behaviour of nodes in attack free environment was evaluated. The radio environment in this attack free scenario consisted of 4 nodes i.e. 2 nodes were declared was PU and 2 nodes were declared as SU. To evaluate the behaviour of nodes in this attack free environment, 50 tests were run and the number of packets sent by PU and SU were recorded, which are as shown by the table 5-1.

Table 5-1 Table of Average Number of Packets Sent by PU and SU in Attack free Environment

No. of Simulations	*Packets Sent by PU (AVERGE)*	*Packets Sent by SU (AVERGE)*
10	653.7	112.2
20	632.6	107.1
30	642.7	112.5
40	626.1	116
50	550.2	147.3
Average	621.06	119.02

5.3 Evaluating behaviour of nodes in attack environment

To see what effect the PUEA has on the environment, the transmission profile for each node was set. In accordance to which, the PU transmits around 40% of time and rest of the time is for the SUs. Although in real environment the PU profile is not controlled but here it was restricted to around 40% just to check the impact of the attack. CBR transmission was considered among the nodes and parameters like maximum numbers of packets to be sent, transmission interval, transmission rate etc. were varied during different test so that average of the all test can yield better results.

When no attack was done on the environment, the legitimate SU transmitted almost every time when the PU was not transmitting (stats shown by the Table 5-I). As the focus of this research is towards PUEA therefore malicious PUEA was done on this environment and after running 50 tests the average number of packets sent by all nodes is depicted by Table 5-2.

Table 5-2 Table of Average Number of Packets Sent all by All Nodes in Attack Environment

No. of Simulations	*Packet Sent by PU (AVERGE)*	*Packet Sent by SU (AVERGE)*	*Packet Sent by SU_M (AVERGE)*
10	612.4	73.4	15.1
20	506	73.5	14.8
30	461.2	44.7	13.7
40	595	86.3	12.4
50	479	57.6	11
Average	530.6	67.1	13.4

When the average of all simulations is taken, it can be seen that PU transmits most number of packets. This is because the rate of transmission of PU in the simulation and in reality is quite high as compared to SU. Figure 5.1 shows a graph of Table II values, plotting number of simulations versus the average number of packets sent by all nodes.

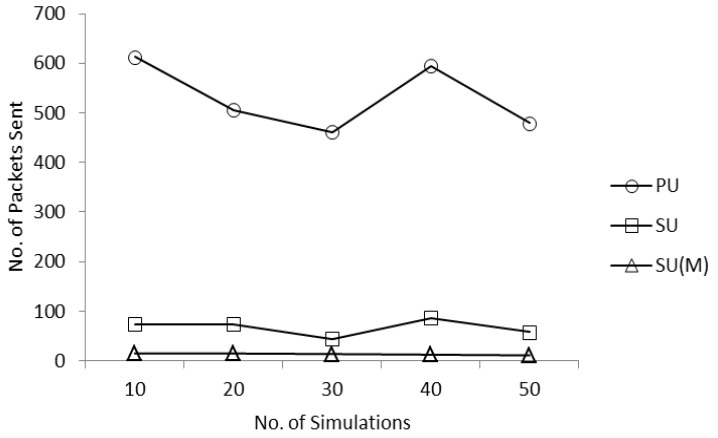


Figure 5.1: Graph showing a plot of number of simulations versus average number of packets sent by all nodes

Although PU transmitted for 40% of the total time (150 sec), which means that SU could not utilize the slots left vacant by PU because of emulation by SU_M. It is also evident that SU_M transmitted the less number of packets as compared to other two nodes. However SU_M occupied the slots for time as shown by the Table 5-3:

Table 5-3 Table of Average Emulation Timings by Malicious Secondary User

No. of Simulations	*Average Timings (sec)*
10	50.2
20	51
30	*51.3*
40	48.4
50	41.6

It is evident from the Table 5-3 stats that, SU_M emulated for almost 30% of the time in which it sent only 2.2% of the total packets. With this the intention is clear that the SU_M conducted a malicious PUEA and due to which legitimate SU has high number of dropped packets. Figure 5.2 shows a graph plotting number of simulations versus the percentage of the dropped packets at SU.

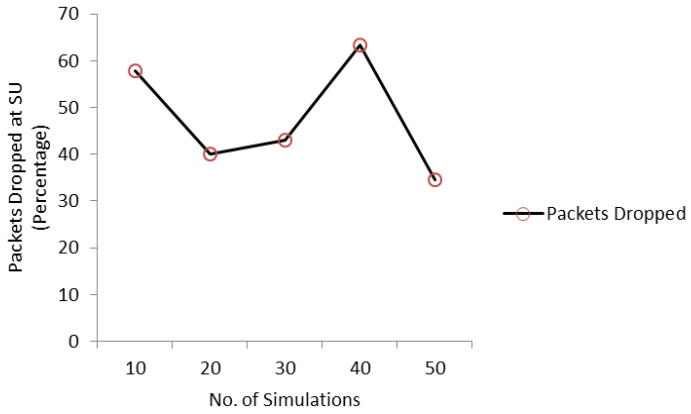


Figure 5.2: Graph showing a plot of number of simulations versus percentage of packets dropped at SU

As explained earlier that parameters like maximum number of packets to be sent, transmission rate etc. were varied during different tests, which also is the reason for variation in the line representing the number of dropped packets at SU. As an example it can be seen in Figure 5.2 that, when the number of simulations are 40, the line is showing the peak value as compared to the point when the number of simulations is 20 or 30. This is because during tests 31-40, the maximum number of packets to be sent value was more as compared to other tests, and due to the attack more numbers of packets remain unsent and it resulted in more number of dropped packets ultimately.

5.4 Proposed Mitigation Technique against Malicious PUEA

Since it has already been discussed previously, an attacker intending a malicious PUEA, emulates smartly during the sensing time; and during transmission slot lets the channel go vacant. In Figure 4.7 the malicious PUEA was described, where it was evident that SU_M does the emulation and does not use the channel for transmission. Also simulation results in the previous section show that SU_M occupied the channel and transmitted only a few packets, which may be to avoid detection but the intent is to make the channel unavailable for use by the legitimate SU.

To protect against malicious PUEA, a scheme based on randomized sensing is proposed. In the proposed technique it is suggested to have sensing randomized at various intervals, other than the defined sensing interval. Figure 4.7 is redrawn in Figure 5.3 to describe the proposed approach.

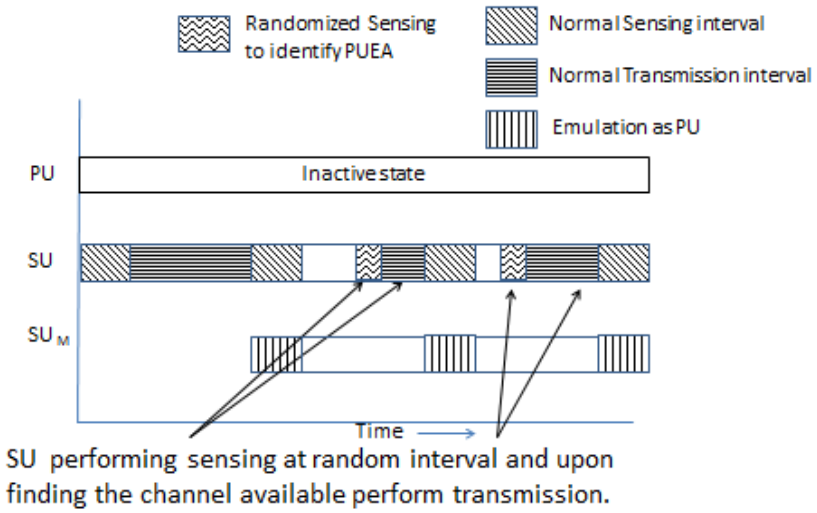


Figure 5.3: Figure representing the proposed approach to counter malicious PUEA by employing randomized sensing.

It can be seen in figure 5.3 that PU was inactive during the whole scenario. SU emerged and performed sensing for network availability and based on sensing results entered into a transmission slot. When it turned back to in-band sensing to check for reappearance of the PU, SU_M starts emulating as the PU due to which the SU is unable to continue its transmission. However in this transmission slot SU senses randomly and finds a slot as available and upon finding an available slot it does not let the slot go vacant, and utilizes the remaining time for its transmission.

With this technique SU is able to identify the vacant channel or in other words identifies the attack, since SU_M only emulates during the defined sensing slots. The advantage of this approach is not just limited to identification, but upon finding a slot to be

vacant by sensing randomly, the SU can utilize the remaining time of the slot to perform its transmission which is represented in Figure 5.3 as well.

The proposed approach is different from all other proposed solutions in a sense that it does not focus only on identification but provides countermeasures against malicious PUEA too. Since the SU, upon sensing randomly, is also able to utilize the remaining time in the transmission slot, so that's why the proposed approach does not only provide identification but provides countermeasure as well.

Implementing the proposed technique in the simulated attack environment produced better results. Using the same parameters, the tests were conducted again that yielded better results and an increase was seen in the total number of packets that the legitimate SU transmitted. Increase in total number of sent packets means decrease in the number of dropped packets.

To illustrate this, a graph plotting the average of packets sent by SU before and after implementing the solution is shown in Figure 5.4.

Implementing the proposed technique in the simulated attack environment produced better results. Using the same parameters, the tests were conducted again that yielded better results and an increase was seen in the total number of packets that the legitimate SU transmitted. Increase in total number of sent packets means decrease in the number of dropped packets.

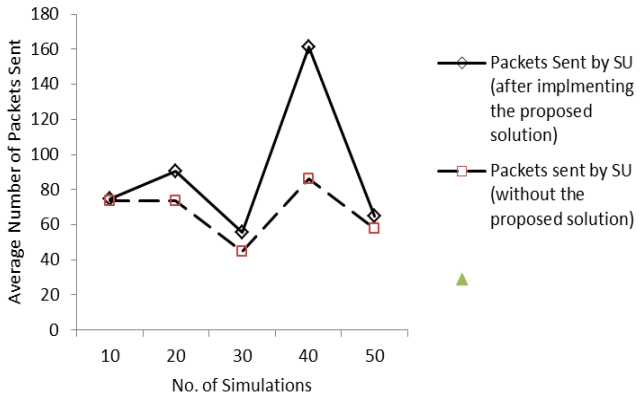


Figure 5.4: Graph showing a plot of number of simulations versus average of number of packets sent by the SU before and after implementing the solution

The solid line in the graph shows the average of packets sent by the SU after implementing the randomized sensing (which is done at random intervals other than the defined sensing intervals). The dotted line represents the same value without implementing the proposed approach (the number of sent packets by SU from Table 5-2).

The difference is clear as the solid line represents more average number of transmitted packets or in other words more efficient utilizations of slots left vacant by the PU. During simulations 31-40, SU had more number of packets to be sent than the other tests therefore that it was able to transmit more packets which is shown by the peak of the graph.

A decreasing trend can be seen in the percentage of packets dropped at the SU after implementing the proposed approach. In Figure 5.5, the solid line in the graph shows the percentage of packets dropped at SU (after implementing the proposed approach), and it is below the dotted line that represent the same before implementing the proposed approach.

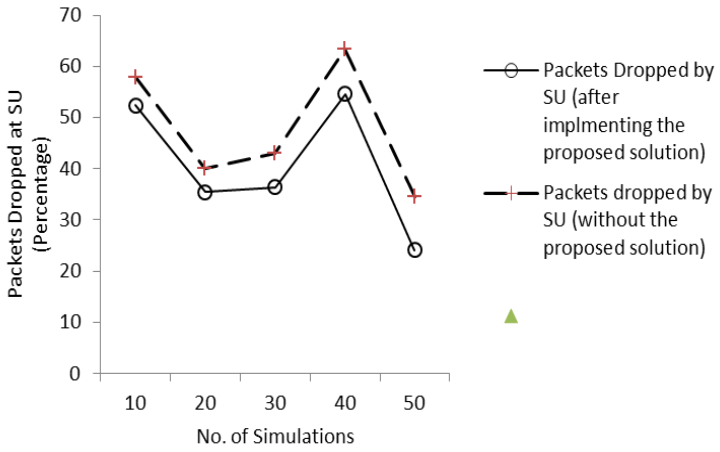


Figure 5.5: Graph showing a plot of number of simulations versus percentage of packets dropped at the SU before and after implementing the solution

5.5 Summary

In this chapter the focus was towards describing the technique adopted to generate results and also to describe the proposed approach. In the first section the test bed and the environment were discussed briefly. In the next section the results were discussed when there was no attack on the environment. After this to evaluate the impact of attack the attack node SU_M was introduced to the environment that resulted in dropped packet at SU. In the last section the proposed approach based on randomized sensing was described that not only identifies the attack but provides the counter measure as well.

CONCLUSION

6.1 Overview of the research

To counter spectrum shortage problem which is expected to get severer in the coming years, the role of Cognitive Radio technology is vital. At the same time the CR are susceptible to many security based threats among which PUEA is an important one. The PUE attack that if successful forms a basis of other attacks like a Lion attack or in extreme form it can result into a Denial of Service (DoS) attack.

To get benefited from CR, work needs to be done in developing techniques to guard against the attacks to CR in conjunction with the techniques focused towards normal working of the CRs . The work in thesis is a contribution towards protecting the CRs against malicious PUEA. Since standardization efforts are underway, therefore the work in the field can be of significant help to researchers working towards standardization efforts.

In the proposed approach a solution was presented that not only identifies the malicious PUEA but allows the legitimate user to take advantage of remaining time slot. To achieve the objectives set in the start of the thesis i.e. to provide a solution against PUEA whose applicability is not limited to static environment but can also be applied to ad-hoc environments, this approach was designed in a way that as it is independent of attributes like static location and RSS etc.

6.2 Objectives Achieved

As described previously the aim behind the work was to propose a mitigation technique against the Primary User Emulation Attack that not only focuses on the attack's identification but its mitigation/ counter measure. However the objectives achieved as a result of this thesis are as under.

a. Understanding of the Cognitive Radio principles.
b. Understanding of the Cognitive Radio standards.

c. Understanding of threats to Cognitive Radio.
d. Understanding of PUE attack and impact of this attack.
e. Proposing a solution to counter PUEA attack.
f. Proposing a solution whose applicability is not limited to static networks like 802.22 but also to ad-hoc networks.
g. Proposing a solution that not only provides identification of the attack but also its countermeasure.
h. Proposing a solution that is advantageous over other solutions.

6.3 Future Work

This work was focused on providing a solution against malicious PUEA. In future employing a reputation based mechanism in conjunction with this scheme, which will allow a node to take the decision by considering the reputation of a SU as well. Reputation based schemes would also allow to block any user who is involved in malicious activities.

6.4 Summary

In this chapter the overview of the research was described. In the next section the objectives achieved in research was mentioned. In the last section future work was described in which employing an energy detection scheme was proposed in conjunction with this technique to make it applicable to work for selfish PUEA. And also as a future work employing a reputation based scheme was proposed in which each node has a reputation and node whose reputation value is below a threshold can be blocked, thus making the radio environment safer.

References

[1] Wassim El-Hajj, Haidar Safa , Mohsen Guizani, “Survey of Security Issues in Cognitive Radio Networks” in Journal of Internet Technology Volume 12, No 2 ,2011.

[2] Internet World Stats © Miniwatts Marketing Group (2012,June,30)[Online].Available: http://www.Internetworldstats.com/stats.htm

[3] Yonghong Zeng, Ying-Chang Liang, Anh Tuan Hoang, Rui Zhang, “A review of spectrum sensing for Cognitive Radio: challenges and solutions”, EURASIP Journal on Advances in Signal Processing.

[4] Ruiliang Chen, Jung-Min Park, Jeffrey H. Reed, “Defense against Primary User Emulation Attacks in Cognitive Radio Networks” in IEEE Journal on Selected areas in communication Volume 26 No1,2008

[5] Dr. Anubhuti Khare, Mahesh Saxena, Roshan Singh Thakur, Khyati Chourasia, “Attacks and Preventions of Cognitive Radio Network- A Survey” in International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Volume 2, Issue 3, March 2013.

[6] Lianfen Huang, Liang Xie, Han Yu, Wumei Wang and Yan Yao, “Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks”, International Conference on Communications and Mobile Computing (CMC), Vol.2, Shenzhen, China, April, 2010, pp.169-173

[7] Caidan Zhao,Wumei Wang, Lianfen Huang and Yan Yao, “Anti- PUE Attack Based on the Transmitter Fingerprint Identification in Cognitive Radio”, in 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom ‘09), Beijing, China, September, 2009, pp.1-5.

[8] Z. Jin, S.Anand, K.P Subbalakshmi, “Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing”, in Mobile Computing and Communication review, Volume 13, Number 2.

[9] Z. Jin, S.Anand, K.P Subbalakshmi, “Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks”.

[10] S.Anand, Z. Jin, K.P Subbalakshmi, “An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks”.

[11] T. Charles Clancy, Nathan Goergen, “Security in Cogintive Radio Networks Threats and Mitigation”.

[12] Ramzi Saifan, “Security issues in cooperative in-band sensing for cooperative radio”, April 2010.

[13] Praveen Kaligineedi, Majid Khabbazian, Vijay K. Bhargava, “Malicious User Detection in Cognitive Radio Cooperative Sensing System” in IEEE transations on wireless communication Vol 9,No 8, Auguest 2010.

[14] Bo Sun, Lawrence Osborne, Yang Xiao, Sghaier Guizani, Intrusion detection techniques in mobile adhoc and wireless sensor networks".

[15] Amitabh Mishra, Ketan Nadkarni, Animesh Patcha, "Intrusion Detection in Wireless Ad Hoc Networks".

[16] Faisal Riaz, Imran Shafi,Syed Faraz Hassan,Waseem Akhtar " Vehicle-to-Vehicle Communication enhanced by cognitive approach and multi-radio technologies TECHNOLOGIES" in the Proceedings of IEEE, ICET 2012 Muhammad Ali Jinnah University,8-9 oct,pp.131-136

[17] Faisal Riaz, Saeed Ahmed, Imran Shafi, Faisal Iqbal, Muhammad Ibrahim, "White Space Optimization Using Memory Enabled Genetic Algorithm in Vehicular Cognitive Radio" in 11th IEEE International Conference on Cybernetic Intelligent Systems August 23-24, 2012, Limerick, Ireland pp.133-138.

[18] Mitola, J.; Maguire, G.Q., Jr., "Cognitive Radio: making software radios more personal," Personal Communications, IEEE , vol.6, no.4, pp.13,18, Aug 1999.

[19] Ruiliang Chen; Jung-Min Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop in , vol., no., pp.110,119, 25-25 Sept. 2006.

[20] Deepa Das, Susmita Das "Primary User Emulation Attack in Cognitive Radio Networks: A Survey" , IRACST – International Journal of Computer Networks and Wireless Communications ISSN: 2250-3501 Vol 3, No 3 June 2013 pp 312-318.

[21] IEEE Std 802.22TM-2011, *IEEE Standard for Wireless Regional Area Networks*

[22] Y. Zhang, W. Lee, and Y. Huang, Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET) , Vol. 9, No. 5, September 2003.

[23] O. Kachirski and R. Guha, Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks,"Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03),p. 57.1, January 2003.

[24] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade,C. Ko, R. Balupari, C.-Y Tseng, T. Bowen, K. Levitt, and J. Rowe, A General Cooperative Intrusion Detection Architecture for MANETs," Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, March 2005.

[25] B. Naqvi, I. Rashid, F. Riaz and B. Aslam, "Primary User Emulation Attack and their Mitigation Strategies: A Survey" in National Conference on Information Assurance 2013. pp 95-100.

[26] U. Shahid and T. Maqsood, "CRN Survey and A Simple Sequential MAC Protocol for CRN Learning" in CONCORA 2012, The Second International Conference on Advances in Cognitive Radio. pp. 22-27.

[27] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of

the 1st International Workshop on Wireless Information Systems (WIS-2002), pp. 1-12, April 2002.

[28] B. Sun, K. Wu, and U. W. Pooch, Alert Aggregation in Mobile Ad Hoc Networks," Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe'03) in conjunction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003.

[29] Przemysław Pawełczak, "Technical Challenges of Cognitive Radio Related Systems", Cognitive Radio defying Spectrum Management at CRNI Conference, Brussels, 2008.

[30] A. Menouni Hayar, R. Knopp and R. Pacalet, "Cognitive Radio Research and Implementation Challenges", Mobile Communications Laboratory Institute, Eur´ecom, Sophia Antipolis, France.

[31] M. Haddad, A. Menouni Hayar, H. Fetoui and M. Debbah, "Cognitive Radio sensing based on information-theoretic" CrownCom 2007, 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Orlando, USA, 2007.

[32] Peter Steenkiste, Douglas Sicker, Gary Minden, Dipankar Raychaudhuri, "Future Directions in Cognitive Radio Network Research" , NSF Workshop Report, 2009.

[33] IETF RFC 2026 (1996,October,30)[Online].Available: http://tools.ietf.org/html/rfc2026

[34] X. Zhou, K. Yazdandoost, H. Zhang, and I. Chlamtac, "Cognospectrum: Spectrum adaptation and evolution in cognitive ultra wideband radio," IEEE Int. Conf. on Ultra-Wideband, Zurich, Switzerland, Sep. 2005.

[35] S. Haykin, "Fundamental issues in Cognitive Radio", Cognitive Wireless Communications Networks, Springer-Verlag, 2007.

[36] T. Charles Clancy and Nathan Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), Singapore, May, 2008, pp.1-8.

[37] Olga León, Juan Hernández-Serrano and Miguel Soriano, Securing Cognitive Radio Networks, International Journal of Communication Systems, Vol.23, No.5, 2010, pp.633-652

[38] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, Channel Surfng and Spatial Retreats: Defenses Against Wireless Denial of Service, Proceedings of the 3rd ACM Workshop on Wireless Security, Philadelphia, PA, January, 2004, pp.80-89.

[39] Ashwin Sampath, Hui Dai, Haitao Zheng and Ben Y. Zhao, Multi-channel Jamming Attacks Using Cognitive Radios, Proceedings of 16th International Conference on Computer Communications and Networks (ICCCN 2007), Honolulu, HI, Aug,2007, pp.352-357.

[40] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, Proceedings of ACM MobiHoc, Urbana, IL, May, 2005, pp.46-57.

[41] Praveen Kaligineedi, Majid Khabbazian and Vijay K. Bhargava, Secure Cooperative Sensing Techniques for Cognitive Radio Systems, IEEE International Conference on Communications 2008 (ICC '08), Beijing, China, May, 2008, pp.3406-3410.

[42] Ankit Rawat, Priyank Anand, Hao Chen and Pramod Varshney, Countering Byzantine Attacks in Cognitive Radio Networks, 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, March, 2010, pp.3098-3101.

[43] Linjun Lu, Soo-Young Chang et al., Technology Proposal Clarifications for IEEE 802.22 WRAN Systems, IEEE 802.22 WG on WRANs, March, 2006.

[44] Joerg Hillenbrand, Timo Weiss and Friedrich K. Jondral, Calculation of Detection and False Alarm Probabilities in Spectrum Pooling Systems, IEEE Communication Letters, Vol.9, No.4, 2005, pp.349-351.

[45] Wenkai Wang, Husheng Li, Yan Sun and Zhu Han, Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks, 43rd Annual Conference on Information Sciences and Systems, 2009 (CISS 2009), Baltimore, MD, March, 2009, pp.130-134.

[46] Kaigui Bian and Jung-Min Park, MAC-Layer Misbehaviors in Multi-hop Cognitive Radio Networks, 2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006), August, 2006

[47] Chris Karlof and David Wagner, Secure Routing in Wireless Networks: Attacks and Countermeasures, Ad Hoc Networks, Vol.1, 2003, pp.293-315.

[48] Juan Hernandez-Serrano, Olga León and Miguel Soriano, Modeling the Lion Attack in Cognitive Radio Networks, EURASIP Journal on Wireless Communications and Networking, Vol.2011, Article ID 242304, 10 pages, 2011.

[49] Chris Karlof and David Wagner, Secure Routing in Wireless Sensor Networks :Attacks and Countermeasures, Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Berkeley, CA, May, 2003, pp.113-127.

[50] Chetan Mathur and Koduvayur Subbalakshmi, Security Issues in Cognitive Radio Networks, Cognitive Networks: Towards Self-Aware Networks, Wiley, New York, 2007, pp.284-293.

[51] Priyank Anand, Ankit Singh Rawat, Hao Chen and Pramod K. Varshney, Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks, Second International Conference on Communications Systems and Networks (COMSNETS 2010), Bangalore, India, January, 2010, pp.1-9.

[52] A Pandharipande et al., IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22, IEEE 802.22 WG on WRANs, November, 2005.

[53] Ruiliang Chen, Jung-Min Park, Y. Thomas Hou and Jeffrey H. Reed, Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks, IEEE Communications Magazine, Vol.46, No.4, 2008, pp.50-55.

[54] Matthew Sherman et al., “IEEE Standards for Cognitive Radio Technologies,” IDGA Software Radio Summit 2008, Vienna, VA, Feb. 25, 2008

[55] X Max Spectrum Crisis Solutions ® xG Technology Inc ® (2014,June,12)[Online]. Available: http://www.xgtechnology.com/Technology/Cognitive-Radio-Network.html