

***EFFECT OF PRIMARY USERS EMULATION ATTACKS ON
COGNITIVE RADIO NETWORKS***

Project report submitted in partial fulfillment of the requirement for the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

By

Parthsarathi Bassi (161023)

Narendra Jangid (161046)

Prashant Kumar (161118)

UNDER THE GUIDANCE OF

Mr. Alok Kumar



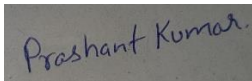
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TABLE OF CONTENTS

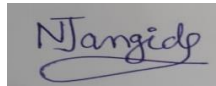
CAPTION	PAGE NO.
DECLARATION	i
ACKNOWLEDGEMENT	ii
LIST OF ACRONYMS AND ABBREVIATIONS	iii
LIST OF FIGURES	iv
LIST OF TABLES	v
ABSTRACT	vi
CHAPTER-1: INTRODUCTION	1
1.1 Introduction	1
1.1.1 Different models for the CRN	2
1.2 What is PUEA?	3
1.3 Impact of PUEA on CR Network	4
1.4 Method to mitigate PUEA	7
CHAPTER-2: LITERATURE SURVEY	10
2.1 Introduction	10
CHAPTER-3: BINARY HYPOTHESIS	24
3.1 Spectrum Sensing	24
3.2 Result	25
3.3 Conclusion	27
CHAPTER-4: MULTILEVEL HYPOTHESIS TESTING	28
4.1 Analysis of CR Network	28
4.2 The proposed multi-level hypotheses test approach	31
4.3 Results	33
REFERENCES	35

DECLARATION

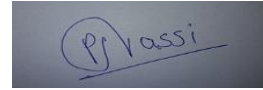
We hereby declare that the work reported in the B. Tech Project Report entitled “EFFECT OF PRIMARY USERS EMULATION ATTACKS ON COGNITIVE RADIO NETWORKS” submitted at “Jaypee University of Information Technology, Wagnaghat, India” is an authentic record of our work carried out under the supervision of Mr. Alok Kumar. We have not submitted this work elsewhere for any other degree or diploma.



Prashant Kumar
161118

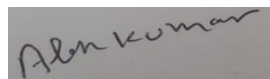


Narendra Jangid
161046



Parthsarthi Bassi
161023

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.



Mr. Alok Kumar
Date:

Head of the Department/Project Coordinator

ACKNOWLEDGEMENT

It is our privilege to express our sincerest regards to our project coordinator, Mr. Alok Kumar, for their valuable inputs, able guidance, encouragement, whole-hearted cooperation and constructive criticism throughout the duration of our project.

We deeply express our sincere thanks to our Head of Department Dr. M.J Nigam for encouraging and allowing us to present the project on the topic “EFFECT OF PRIMARY USERS EMULATION ATTACKS ON COGNITIVE RADIO NETWORKS” at our department premises for the partial fulfillment of the requirements leading to the award of B-Tech degree.

LIST OF ACRONYMS AND ABBREVIATIONS

- **CRN= Cognitive Radio Networks**
- **PU's= Primary Users**
- **SU's= Secondary Users**
- **AWGN=Additive White Gaussian Noise**
- **PUEA= Primary User Emulation Attack**
- **QoS = Quality of Service**
- **CCC = Common Control Channel**
- **LocDef = Localization based defense**
- **WSN = Wireless Sensor Network**
- **RSS = Received signal strength**
- **RF = Radio Frequency**
- **FCC = Federal communication commission's**
- **WSPRT = Wald's sequential probability ratio test**
- **OSS = Opportunistic Spectrum Sensing**
- **WRAN = Wireless regional area networks**
- **SAP = Signal activity pattern**
- **HDC = Hard combining**
- **CSI = Channel state Information**
- **DSA = Dynamic spectrum access**
- **MRC = Maximal ratio combining**

LIST OF FIGURES

Figure No.	Figure Description	Page No.
1.1	Cognitive Radio Cycle	1
1.2	Time frequency graph of different CR networks	2
1.3	Primary User Emulation Network (PUEA)	4
1.4	Network Model	6
1.5	PUEA Mitigation	7
1.6	Energy detection method	8
3.1	Binary Approach	24
3.2	Distance of Nodes from Fusion Center	25
3.3	No of CR Users Vs Probability	26
3.4	Probability of False Alarm Vs Probability of Detection	26
4.1	Network Layout	28
4.2	SNR (dB) Vs Pd (Probability of Detection)	33
4.3	Pd Vs Pf (Probability of false Alarm)	34

LIST OF TABLES

Table No.	Table Description	Page No.
1.1	SUMMARY OF VARIOUS TECHNIQUES FOR COUNTER MEASURES FOR PUEA	9
2.1 PAPER USED	KEY APPROACHES OF REFERENCE	10

ABSTRACT

The inherent nature of cognitive radio (CR) networks has brought new threats to wireless communications. Primary user emulation attack (PUEA) has been widely studied as a serious threat to cooperative spectrum sensing (CSS) in CR networks. In PUEA, a malicious user obstructs CR users from accessing idle frequency bands by imitating licensed primary user (PU) signal characteristics. The present study introduces a new CSS scheme in the presence of a malicious PUEA based on multi-level hypothesis testing (MLHT). In the proposed method, generalizing from binary hypothesis testing to MLHT, we partition the decision space to four decision options and apply minimum Bayes cost criteria to determine the channel status. We also discuss practical limitation issues that need to be considered when applying the MLHT approach. Simulation results are provided to indicate the performance improvement of the proposed MLHT method against PUEA, compared with the conventional method.

CHAPTER 1

INTRODUCTION

1.1) INTRODUCTION

The emergence of latest developments in cellular mobile and wireless broadband, alongside developments in other areas like broadcasting and innovation in multimedia accessories have resulted in increased demand for spectrum for a spread of uses. However, spectrum occupancy measurements in various countries have indicated that a big amount of the licensed spectrum remains unused in many places most of the time [1, 2]. To beat the matter of spectrum scarcity, cognitive radio (CR) has been introduced. The CR technology provides the power for wireless equipment to take advantage of the licensed spectrum in an opportunistic manner [2, 3].

Static spectrum access is that the main policy for the present wireless communication technologies. Under this policy, fixed channels are assigned to licensed users or primary users (PUs) for exclusive use while unlicensed users or secondary users (SUs) are prohibited from accessing those channels even once they are unoccupied.

All the secondary users follow a cognitive cycle having four phases namely- spectrum Sensing, spectroscopy, adaptation and act phase as shown in figure 1.

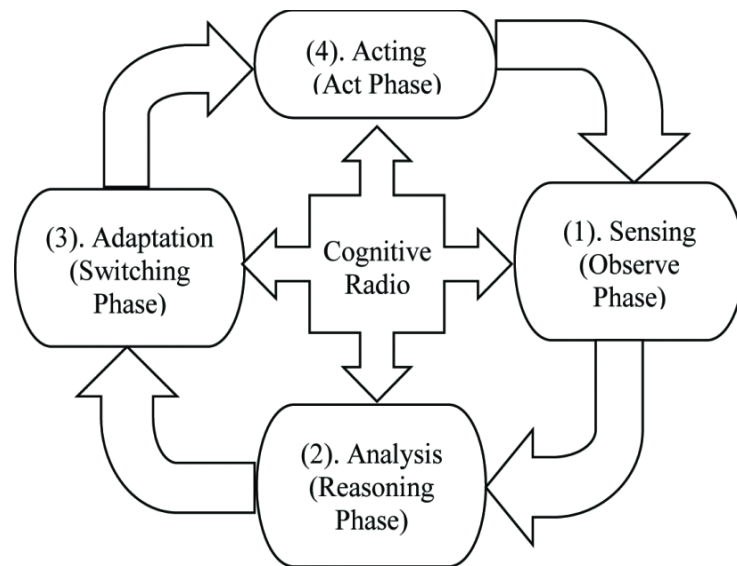


Figure 1.1

1.1.1) Different models for the cognitive radio networks (CRN):

- **Interweave Network Models:** Within the interweave network model, unlicensed or secondary users aren't allowed to access an occupied band by the licensed or primary user. In these networks, the CR has got to identify the available sub-bands of the radio-frequency spectrum, or equivalently the spectrum holes, that are under-utilized (in part or in full) at a specific instant of your time and specific geographic location.
- **Underlay Models:** Within the underlay network model, the coexistence of primary and secondary users is allowed and hence the network is additionally termed as a spectrum sharing network [8]–[10]. However, PUs are always allocated a better priority to use the spectrum than SUs.

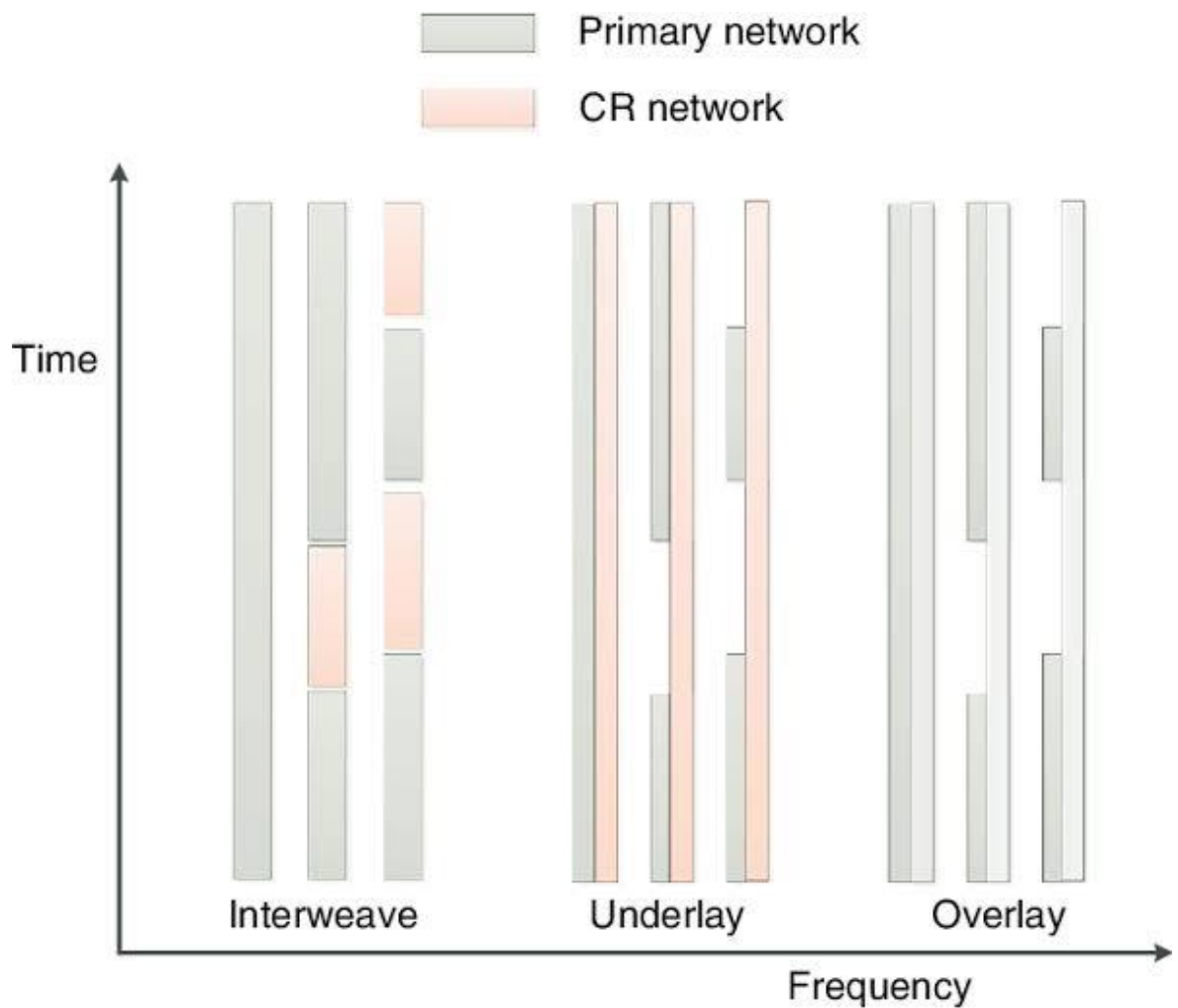


Figure 1.2

- **Overlay Models.** In overlay cognitive networks, SUs and PUs are allowed to transmit concurrently. The defining assumption made within the present overlay models is that the primary message is known to the secondary transmitter in prior [9]. There are two main approaches to know this model: (1) with the help of advanced coding techniques [11] like dirty paper coding (a technique which completely mitigates a priori known interference over an input power constrained additive white Gaussian noise (AWGN) channel), where the secondary user can precode the transmitted stream so on effectively null the interference at the secondary receiver.

1.2) WHAT IS PRIMARY USER EMULATION ATTACK (PUEA)?

PUEA is one of the foremost crucial attacks that need to be studied in CRNs because it degrades the performance to a very large extent and hence hinders the sensible implementation of CRNs. As PUEA affects call dropping and introduces delay in secondary networks [13], various techniques need to be developed to countermeasure this attack. There are often differing kinds of PUE attackers during a CRN like selfish attacker, malicious attacker. In selfish incumbent emulation attack, intruding node reserves a selected band for its own transmission. However, a malicious attacker causes denial of service attack causing the SU to switch from one band to a special. This malicious attack has more adverse effect than selfish attack in reducing the bandwidth available to SUs [4],[5], [8], [11], [13]. A selfish SU can also cause attack to a CRN to maximize its chance for spectrum access [4]. Another classification of attackers are often supported their transmission power. Attackers can have fixed power level or they're going to be power adaptive in nature. Power adaptive attackers can adapt their transmitting power relying on primary signal estimated power [13]. Attackers are often static also as mobile. things of static attackers are often easily found whereas mobile attacker can easily change its location making it difficult to trace such attackers [13].

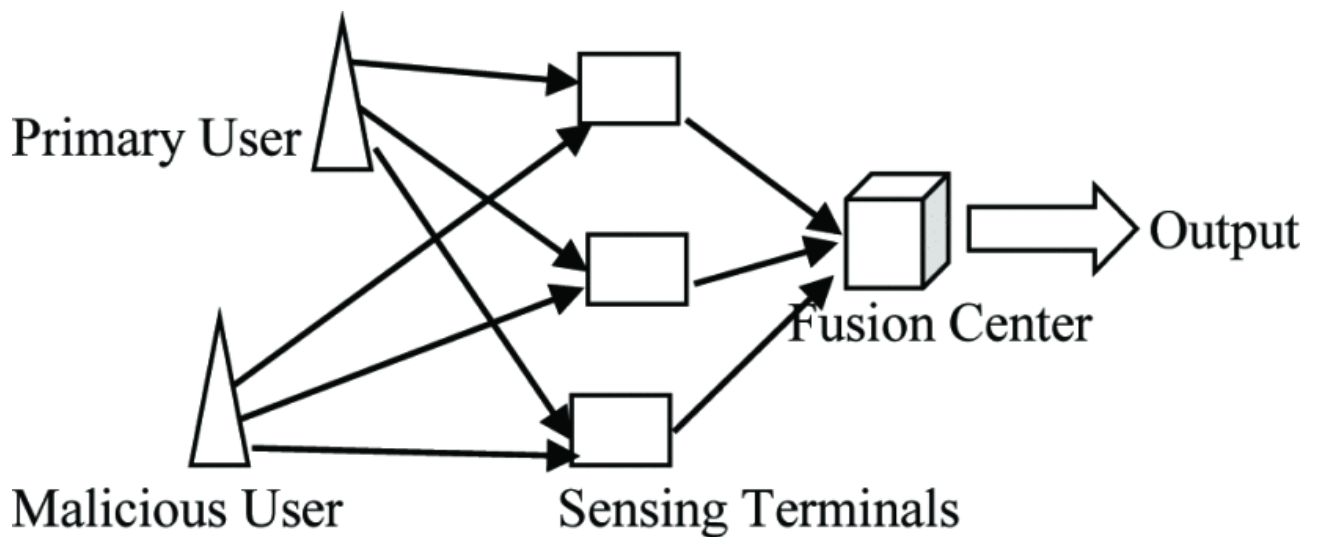


Figure 1.3: PRIMARY USER EMULATION ATTACK (PUEA)

1.3) IMPACT OF PUEA IN CR NETWORK'S

PUEA degrades the performance of a CRN to such an extent that it poses a superb threat to practical implementation of this technology. It is a singular denial of service attack and affects the choice dropping also as delay in secondary networks carrying real also as non real time traffic to an outsized extent [13]. It leads to batch of bandwidth wastage because the malicious nodes steal different spectrum holes. It also causes degradation in quality of service (QoS) because it disrupts the continuity of Sus and Sus got to frequently switch from ne spectrum hole to a special without having the power to access a selected band. If the network is effected by an outsized number of attackers, then it would be possible that the SU is left with no free spectrum hole thus making the CR a trivial technology for practical purpose. This may be termed as a denial of service attack [6]. For practical implementation of a CRN, a typical control channel (CCC) must be built up. CCC is used to exchange the control messages. However, if the attacker attacks the CCC itself, then the whole network switches to outage stage during which no spectrum band is ou t there for common control channel and thus the communication is ceased at that instant [6].

1.3.1) Several approaches have been proposed to deal with a PUEA

Localization based approaches: during this, a transmitter verification scheme, called LocDef (localization-based defense), which utilizes both signal characteristics and site of the signal transmitter to confirm primary signal transmitters. a strong non-interactive localization scheme is introduced to detect PUE attacks and pinpoint PUE attackers. The localization scheme utilizes an underlying wireless sensor network (WSN) to gather pics of received signal strength (RSS) measurements across a CR network. By smoothing the collected RSS measurements and identifying the RSS peaks, one can estimate the transmitter locations. We describe, in detail, the technique for localizing transmitters both in and out of the range of the WSN.

Frequency Fingerprinting based approaches: Recently, radio-frequency (RF) fingerprinting has been proposed for mitigating primary user emulation (PUE) attacks in cognitive radio networks (CRNs). The widespread practical implementation of cognitive radio (CR) is probably going to utilize software defined radios with a low-end (i.e. low-cost) receiver built with inexpensive analogue components. This study experimentally analyses the feasibility of RF fingerprinting for mitigating PUE attacks using low-end software-defined CRs. Seven universal software radio peripherals are used as low-end CR receivers and their resulting performance is analyzed for unplanned and infrastructure CRN scenarios. The performance analysis is performed for the most important known data set of its kind, which consists of 490 000 measurements from seven identical transmitters across eight receivers. it's found that impairments within the front-end of a low-end receiver affects the accuracy of transmitter classification and this accuracy varies across receivers. The results suggest that RF fingerprinting are often effectively used for mitigating PUE attacks in a billboard hoc CRN at high receiver signal-to-noise whereas RF fingerprinting isn't a practical solution for mitigating PUE attacks in an infrastructure CRN.

Analytical sensing approaches: An analytical approach supported Fenton's approximation and Markov inequality and obtains a boundary on the probability of a successful PUEA on a secondary user by a group of co-operating malicious users. We consider a fading wireless environment and discuss the varied parameters which will affect the feasibility of a PUEA. We show that the probability of a successful PUEA increases with the space between the primary transmitter and secondary users. this is often the primary analytical treatment to review the feasibility of a PUEA.

The network model shown in Fig. Where the attackers and secondary user (victim) are located in circular grid. the first user may be a TV tower located at a distance of d_p from the CRN and every one users' position is fixed within the network. Each attacker wants to fool the victim 10 by transmitting a sign whose characteristic emulates that of the primary user. The victim listens to the channel to differentiate between the signal coming from the primary user or the attacker

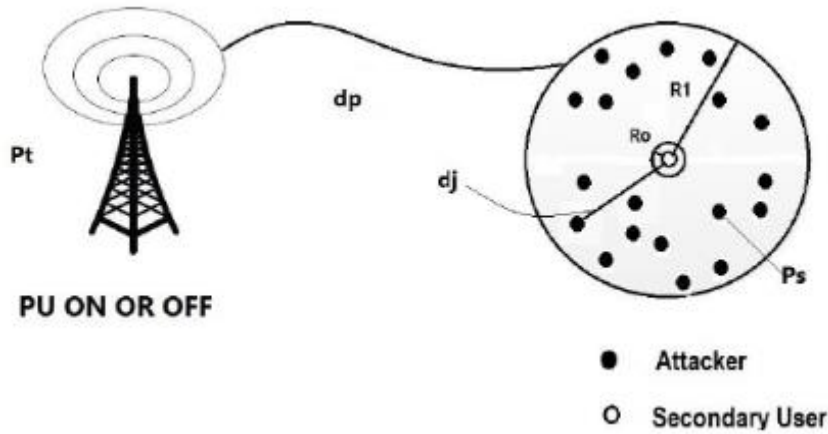


Figure 1.4

The following assumptions are considered for proposed model specification:

1. d_j is the distance between the J th attacker and the victim, the target region in which each attacker wants to fool the victim is a loop of radius R_0 and R_1 .
2. The primary transmitter located at a distance of d_p from the Cognitive Radio network.
3. The primary user transmits a power of p_t and each attacker transmits an adaptive power P_s .
4. The signal from primary and the attacker undergoes path loss and, lognormal, or fading.
5. At the victim the free space propagation model is considered for the signal from primary and two ray ground model for the signal from the attacker, respectively. The received signal at victim from the primary is proportional to d_p^{-2} , and from the attacker is proportional to d_j^{-4} .
6. The shadowing random variable for the primary transmitter is

$$G_p = 10^{\beta_p/10} = e^{a\beta_p}$$

Where $a = \frac{\ln 10}{10}$ and $\beta_p = N(0, \sigma_p^2)$ follows a normal distribution with zero mean and variance equal to σ_p^2 .

7. The shadowing random variable for the attacker is

$$G_s = 10^{\beta s / 10} = e^{a\beta s}$$

Where $a = \frac{\ln 10}{10}$ and $\beta_s = N(0, \sigma_s^2)$ follows normal distribution, with zero mean and variance equal to σ_s^2 .

8. NO cooperation is consumed between the attackers.

1.4) Method to mitigate PUEA

1.4.1) Collaborator node

to make sure proper spectrum sensing, cognitive radio doesn't perform spectrum sensing of its own. Instead, it depends on the third party called collaborator node. It's assumed that the collaborator node is extremely on the brink of the primary user. The aim of selecting collaborator node is thanks to Federal Communication Commission's (FCC) decision 'no modifications must be done to the primary user signal'.

The sample graph is shown in Figure The collaborator node senses the supply of the primary user and within the absence of the primary user conveys the message to the cognitive radio alongside the authentication tag. To elude interference with the primary user, the collaborator node communicates with the cognitive radio only within the absence of the primary user. The key to decode the authentication tag is already known to the cognitive radio. The cognitive radio accepts the knowledge only with authentication tag and discards other information. By this manner, PUEA is mitigate.

\

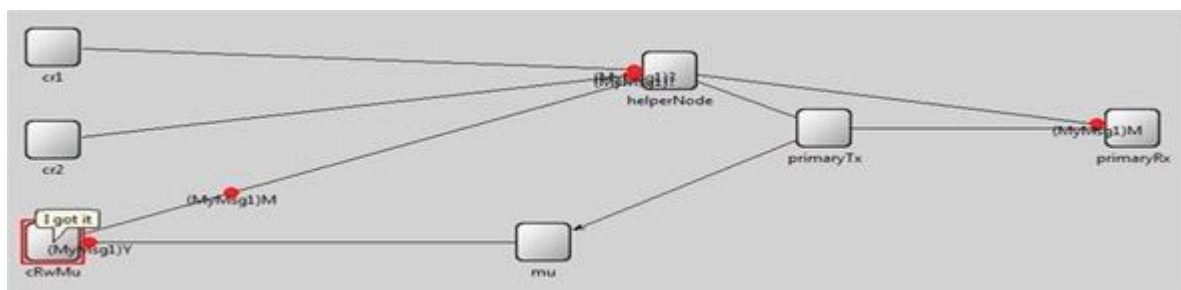


Fig 1.5 PUEA mitigation.

1.4.2) Spectrum sensing

The collaborator node senses the supply of the primary user with the help of energy detection method. The diagram of frequency domain-based energy detection method is shown in Figure. The incoming signal is filtered and passed to fast Fourier transform block. The output of FFT block is fed to windowing function block. this is often done so to scale back the irregularities and to scale back the side lobes. Various windows like Henning window, hamming window, Blackman window and Kaiser Window might be utilized. Every window has its own advantage and disadvantage. By adjusting beta parameter of Kaiser Window, side lobes are often reduced in comparison to other windows; but at an equivalent time, the width of main lobe is wider. By adjusting the dimensions of the windows, better output might be obtained. Hence, proper choice of window becomes necessary. The output of windowing block is fed to magnitude cube. the typical energy of the signal is then compared with the choice threshold.

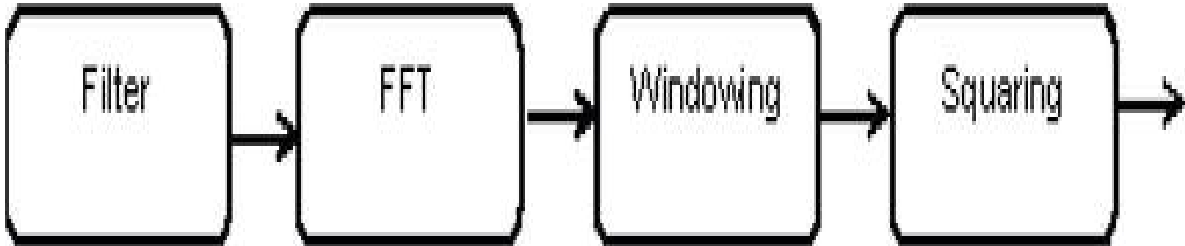


Figure 1.6:Energy detection method.

SUMMARY OF VARIOUS TECHNIQUES FOR COUNTER MEASURES FOR PUEA

Proposed Techniques	Principle Used
LocDef by R. Chen <i>et. Al.</i>	Uses non-interactive localization scheme to estimate the location and observe the Primary User signal characteristics
Belief Propagation by Z. Yuan <i>et. Al.</i>	RSS based strategy that first calculates local and compatibility function to calculate the final belief to estimate whether the suspect is an attacker or genuine primary user
PUEA for low power Transmitting devices by S. M. Mishra <i>et. Al.</i>	Relationship between acoustic information and RF signals is exploited to validate the presence of PU
Cooperative Sensing Scheme by J. S. Simon off	Optimization of weights is done at the fusion center to increase the chances of maximum available channels
Single iteration Belief propagation by S. Maric <i>et. Al.</i>	Uses simpler belief equation that achieves similar accuracy and needs less computational time than simple BP proposed by Z. Yhua <i>et. Al.</i>
PDF-BP by Y. Chen <i>et. Al.</i>	Observed signal is subtracted from the Mean of the PU which is known. If the suspect is a PU, it should satisfy pdf of noise.
Hybrid algorithm by S. Maric <i>et. Al.</i>	Combines Compressive sensing to detect the PUEA

TABLE 1.1

CHAPTER – 2

LITERATURE SURVEY

2.1) Introduction

In this section we discuss about the different types of approaches and contributions done by the different researchers on the topic PUEA.

Ref. no.	IEEE/year	Description	Key approaches	Contribution
[1]	Mishra, S. M., Sahai, A., & Brodersen, R. W. (2006).	ensure reliable Spectrum Sensing in Cognitive Radio Networks	As a way of counter this threat, they offer a transmitter verification process that can be included into the spectrum sensing mechanism. Two diverse techniques are proposed to realize position verification are Distance Ratio Test and Distance Difference Test.	The main function of this work is recognition of the PUE attack, display of its damaging effects on a CR network, and the proposal of a transmitter verification process to detect such an attack.
[2]	Chen, R., Park, J. M., & Reed, J. H. (2008).	Defense against Primary User Emulation Attacks in Cognitive Radio Networks	To oppose this threat, they suggest a transmitter confirmation scheme, called <i>Loc Def (localization-based defense)</i>	The main key of this work is First, we identify a security matter that pose a serious threat to CR networks. Second, the paper

				propose Loc Def as a transmitter confirmation scheme that is capable of detecting PUE attacks and analytical PUE attackers.
[3]	Zhao, C., Wang, W., Huang, L., & Yao, Y. (2009).	Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio	In this a new safety scenario in physical layer is planned. It takes benefit of the "fingerprint" verification of the transmitter against primary user emulation (PUE) attacks.	They use it as the basis of transmitter classification to defend PUE attack and obtain good quality result.
[4]	Anand, S., Jin, Z., &Subbalakshmi, K. (2008).	An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks	They propose a analytical approach based on Fenton's approximation and Markov inequality and obtain a lesser bound on the probability of a successful PUEA on a secondary user by a set of co-operating hateful users.	They present the first ever logical treatment of the viability of a PUEA. and derive mathematical terms for the probability of a successful PUEA and provide lower limits on the probability of a successful attack using Fenton's approximation and Markov inequality.

[5]	Jin, Z., &Subbalakshmi, K. (2009)	Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks	They present an study using Fenton's approximation and Wald's sequential probability ratio test (WSPRT) to notice PUEA	They present a Wald's sequential probability ratio test (WSPRT) to notice PUEA by first rising a mathematical formulation for the probability density function (pdf) of the expected signal from the hateful users. We also show by simulations that our planned detection mechanism can ensure that the good secondary users always obey the spectrum migration protocol.
[6]	Alahmadi, A., Abdelhakim, M., Ren, J., & Li, T. (2014).	Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard	we suggest a consistent AES-assisted DTV scheme, where an AES-encrypted position signal is generate at the TV transmitter and used as the sync bits of the DTV data frames.	The planned scheme combats primary user emulation attacks, and enables more healthy system operation and efficient spectrum distribution It is shown that with the AES-assisted DTV scheme, the primary user, as well as hateful

				user, can be detected with high accuracy and low fake alarm rate under primary user emulation attacks.
[7]	Chen, C., Cheng, H., & Yao, Y.-D. (2011).	Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack	<p>we suggest a new cooperative spectrum sensing scheme, considering the continuation of PUEA in CR networks.</p> <p>In the planned scheme, the sensing information of different secondary users is joint at a fusion center and the combining weights are optimized with the objective of maximizing the discovery probability of available channels under the restraint of a required fake alarm probability.</p>	The main role of this paper is to maximize the discovery probability of the primary user by deriving the optimal combine weights, allowing for the existence of the PUEA in a CR network.
[8]	Ma, J., Zhao, G., & Li, Y. (2008).	Soft Combination and Detection for Cooperative Spectrum Sensing in Cognitive	<p>we believe cooperative spectrum sensing based on energy discovery in cognitive radio networks.</p> <p>Soft combination of the</p>	Based on the Neyman-Pearson criterion, we have obtained the best soft combination (OC)

		Radio Networks	observed energies from diverse cognitive radio users is investigated.	scheme that maximizes the finding probability for a given fake alarm probability.
--	--	----------------	---	---

TABLE 2.1

[9]Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks:

The need to satisfy the ever-increasing spectrum demands of rising wireless applications and thus the need to better use spectrum has led the Federal Communication Commission (FCC) to re-examine the matter of spectrum management. within the traditional spectrum management paradigm, most of the spectrum is owed to licensed users for exclusive use. recognize the importance of the spectrum shortage problem, the FCC is in view of opening up licensed bands to unlicensed operations on a non-interference basis to primary users. during this new pattern, unlicensed users (a.k.a. secondary users) “opportunistically” operate in fallow licensed spectrum bands without causing interference to licensed users thereby increasing the effectiveness of spectrum utilization. This method of sharing is typically called Opportunistic Spectrum Sharing (OSS).

The flourishing deployment of CR networks and thus the belief of their benefits will depend on the situation of essential security attributes in adequately robust form to resist misuse of the system. Ensuring the constancy of the spectrum sensing process could also be a very important problem that has got to be addressed. The key to affect this problem has the power to discriminate primary user signals from secondary user signals during a strong way. Recall that, during a CR network, secondary users are permitted to figure in licensed bands only on a non-interference basis to primary users. Because the first users' usage of licensed spectrum bands could even be irregular, a CR must constantly monitor for the presence of current signals within the present operating band and candidate bands. Consider the next two scenarios. If a secondary user (with a CR) detects the presence of current signals within the present band, it must immediately switch to a minimum of one among the fallow candidate bands. On the other hand, if the secondary user detects the presence of an unlicensed user, it invokes a coexistence device to share spectrum resources.

The above scenarios highlight the importance of a CR's ability to differentiate between primary user signals and secondary user signals. Distinguishing the two signals is non-trivial, but it becomes especially difficult when the CRs are operating in hostile environments. During a hostile environment, an attacker may modify the air interface of a CR to mimic incumbent signal's characteristics, thereby causing legitimate secondary users to erroneously identify the attacker as a primary user. We coin the term primary user emulation (PUE) attack to denote this attack.

The current research and consistency efforts suggest that one of the primary applications of CR technology are getting to be its use for OSS of fallow TV spectrum bands. FCC is considering opening up TV bands for OSS because TV bands often experience lower and fewer dynamic utilization compared to other current networks like cellular networks. Throughout the paper, we suppose an current network composed of TV transmission towers and receivers placed at fixed locations. In such a setting, positions of in office transmitters are often used to distinguish primary user signals from secondary user signals. During this paper, we propose a transmitter verification procedure that employs a non-interactive location verification scheme to require advantage of the actual fact that this signal transmitters are placed at fixed locations. Because things verification scheme is non-interactive, no amendment to this signal transmitters is required, thus satisfying the necessity stated in NPRM.

[10]Defense against Primary User Emulation Attacks in Cognitive RadioNetworks:

The need to satisfy the rising spectrum demands of rising wireless applications and thus the need to better use spectrum have led the Federal Communications Commission (FCC) to revisit the matter of spectrum management. Within the traditional spectrum management model, most of the spectrum is owed to licensed users for exclusive use. Recognizing the meaning of the spectrum shortage problem, the FCC is considering opening up licensed bands to unlicensed operations on a non-interference basis to licensed users. During this new example, unlicensed users “opportunistically” operate in fallow licensed spectrum bands without interfering with licensed users thereby increasing the competence of spectrum utilization. This method of sharing is typically called Dynamic Spectrum Access (DSA).

Cognitive Radios (CRs) are seen because the enabling tools for DSA. Unlike a typical radio, a CR has the facility to sense and appreciate its environment and proactively change its mode of operation as needed. CRs are able to perform spectrum sensing for the aim of identifying fallow licensed spectrum—i.e., spectrum “white spaces”.

Once white spaces are identified, CRs opportunistically utilize these white spaces by operating in them without causing intrusion to primary users. The successful operation of CR networks and thus the belief of their benefits will depend on the situation of essential security mechanisms in adequately robust form to resist misuse of the system. Ensuring the honesty of the spectrum sensing process could also be a very important problem that has got to be addressed. The key to affect this difficulty has the power to differentiate primary user signals from secondary user signals during a strong way. Recall that, during a CR network, secondary users are allowed to figure in licensed bands only on a non-interference basis to primary users. Because the primary users' usage of licensed spectrum bands could even be irregular, a CR must constantly monitor for the presence of primary user signals within the present in commission band and candidate bands. If a secondary user (with a CR) detects the presence of primary user signals within the present band, it must directly switch to a minimum of one among the fallow candidate bands. On the other hand, if the secondary user detects the presence of an unlicensed user, it invokes a coexistence device to share spectrum resources.

Current research and regularity efforts suggest that one of the primary application of CR technology are getting to be its use for DSA of fallow TV spectrum bands. FCC is in view of opening up TV bands for DSA because TV bands often knowledge lower and fewer vibrant use compared to other primary user networks like cellular networks. within the paper, we specialize in a situation during which a primary user network consists of TV transmission towers and receivers placed at fixed locations. In such a setting, things of a given transmitter (along with other factors) are often utilized to figure out whether the transmitter could also be a primary transmitter or a PUE attacker.

[11] An Overview of Primary User Emulation Attack in Cognitive Radio Networks:

With the rising new license-exempt wireless devices, the matter of spectrum shortage has become a significant worry. Cognitive Radio could also be a replacement technology that's broadly considered nowadays to stop the matter of spectrum lack and its underutilization. the foremost task to use this technology lies in sensing the available open spectrum. Most of this research revolves around spectrum sensing in Cognitive radio Network (CRN). However, because of vibrant nature of Cognitive Radio technology, it suffers from various security intimidation . There are basically two uniqueness of CRNs- cognitive capability and cognitive reconfigurability. Attacks that associated to cognitive capability are often PUEA, SSDF and jamming attacks that occur during sensing and

acting period. While attacks associated to reconfigurability are often all the attacks which can occur during analysis or revision phase like using malicious codes.

16.

PUEA is one of the foremost critical attacks that need to be studied in CRNs because it degrades the performance to a very big extent and hence hinders the sensible execution of CRNs. As PUEA affects call dropping and introduces wait in secondary networks, various techniques need to be urbanized to countermeasure this attack. There are often similar kinds of PUE attackers during a CRN like selfish attacker, malicious attacker. In selfish current emulation attack, intruding node reserves a selected band for its own transmission. However, a hateful attacker causes denial of service attack causing the SU to switch from one band to a special. This hateful attack has more adverse effect than selfish attack in dropping the bandwidth available to SUs. A selfish SU can also cause attack to a CRN to maximise its chance for spectrum access.

[12] Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio:

During a CR network, secondary users (SUs) are only allowable to function within the licensed bands on a non-interference basis to primary users. Since the primary users' (PUs) practice of licensed spectrum bands could even be irregular, SUs should examine the presence of current signals over the in commission band and candidate bands. Two results may happen. First, if a SU detects the presence of current signals over current band, it must directly switch to a minimum of one among the fallow candidate bands. Second, if the SU detects the presence of an unlicensed user, it invokes a coexistence mechanism to separate the spectrum resources.

The above scenario highlight that it's significant for a CR to differentiate the primary user signals from the secondary user signals. unique the two signals is non-trivial, but it becomes much difficult when the CRs are in commission in aggressive environments. during a aggressive environment, an assailant may modify the air interface of a CR to imitate the individuality of current signals, and cause legitimate secondary users to incorrectly identify the attacker as a primary user, which is known as PUE attack. there is a wise option of PUE attacks since CRs are easy to be reconfigured because of their software-based air interface. The task of defensive the PUE attacks by unique the lawful transmitter from the fake becomes a superb test when considering the condition described in FCC E¹/₄s NPRM 03-322, which states that no modification to this system is required to lodge opportunistic use of the band by secondary users. For this reason, conformist approaches, like

embed a signature during a primary user's signal or employing an interactive protocol between an current signal transmitter and a verifier, aren't available.

17.

To frustrate the PUE attack, a transmitter verification format supported location confirmation was planned. They planned two other techniques that are at the center of things verification scheme. the primary technique is known as the space Ratio Test (DRT), which uses received signal strength (RSS) size obtained from a pair of verifiers to figure out the transmitter's location. The second technique is known as Distance Difference Test (DDT), which utilize the phase dissimilarity of the primary user's signal observed at a pair of verifiers to verify the transmitter's location. For a stable transmitter (e.g. TV tower), this scheme can improve the honesty of spectrum sensing mechanism.

[13] An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks:

Spectrum sharing has always been an significant feature of system design in wireless communication systems because of the shortage of the available resources/spectrum. Cognitive radio networks enable usage of vacant spectrum during a network, A, by users belong to a special network, B. These users thereby become "secondary users" to the network A. The users that originally subscribed to the network A are called "primary users" of network A. One example of cognitive radio network is that the practice of white spaces (or vacant spectrum) within the tv (TV) band. The TV transmitter then becomes a main transmitter and tv receivers are primary receivers. Other users who aren't TV subscribers but wish to use the white spaces within the TV band for his or her own message become minor transmitters/receivers. The IEEE 802.22 working group on wireless regional area networks (WRAN) offer the physical layer (PHY) and medium access control (MAC) specifications for usage of the TV white spaces. The developments in software defined radio (SDR) enables implementation of re-configurable MAC for dynamic spectrum access (DSA). "Akyildiz et al" provide a radical survey of the event in SDR, DSA and cognitive radio. The protocol followed in cognitive radios is that the minor users evacuate the used spectrum once they detect a main transmission.

In most approach, the detection of PUEA depends on the resolve of things of the primary transmitter, which, in turn, depends on the direction of signal arrival. The trust on the directionality

of the antennas at the receiver makes the detection process complex because most of the current receivers in wireless and cellular networks use anti directional antennas

18.

[14] Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing:

Conventionally, radio-frequency spectrum bands are assigned to license holders or services on an extended term basis for giant countries. This fixed spectrum task policy has led to under-utilization of the available spectrum. The incompetence in spectrum usage and therefore the limited simple use of spectrum have given rise to cognitive radio enabled dynamic spectrum access (DSA) as a replacement communication model. “Secondary” nodes during a DSA networks can use the licensed spectrum bands when it's at rest, under the condition that they leave it upon the return of the “primary” licensed users (current, primary users). within the remainder of the paper, we use the term primary or current to ask the licensed, high precedence user and therefore the term secondary to denote the unlicensed users. One example of cognitive radio networks (CRN) is that the usage of idle spectrum within the TV band. The TV transmitter and receivers are primary users who are licensed to use these bands. Other users who access the white spaces within the TV band on hit or miss basis are termed secondary users. The IEEE 802.22 working party on wireless regional area networks provides the physical layer and medium access control for usage of the TV white spaces.

Spectrum sensing in DSA is important both for recognition of empty spectral bands (white spaces) also as for prompt evacuation upon the return of current. Protocols for sensing primary transmission and spectrum mass departure are often found. Primary transmitter detection techniques include energy detection, cyclostationary feature detection and matched filter detection. Among these, energy based detection is usually more popular thanks to simple completion.

[15] Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks:

Dynamic spectrum access (DSA) networks have received tons of concentration within the recent decade due to their intrinsic ability to supply better use of limited radio resources. DSA networks

are characterized by two sorts of users: (i) the primary users who hold licenses to spectral bands and have the highest priority to access these bands and (ii) the secondaries who don't have licenses, but can use these bands when the bands are at rest. It's anticipated that the secondary users will endlessly sense the spectrum bands for the return of the primary and can vacate as soon as the return of the primary user is sensed. A radical account of the various sensing mechanisms to detect white spaces is provided in, and protocols for sensing primary transmission are often found.

19.

Since the onus of detecting the return of the primary and resulting evacuation lies entirely on the secondary and since there's no policing mechanism to make sure that this protocol is followed, several denial-of-service (DoS) attacks are possible on either the primary or the secondary users. For instance, a group of secondary users (called "hateful users") could transmit signals with characteristics just like that of a primary transmitter, leading other "good" secondary users (that follow the traditional spectrum evacuation manners) to go away from the spectrum without cause. Such attacks are called primary user emulation attacks (PUEA), and were first discussed by Chen and Park. We measured a fading wireless environment and resulting expressions for the probability of successful PUEA using Fenton's approximation. We then used Markov inequality to supply a boundary on the probability of successful PUEA. During this paper, we present a Wald's sequential probability ratio test (WSPRT) to detect PUEA by first rising a mathematical formulation for the probability density function (pdf) of the received signal from the hateful users. We also show by simulation that our proposed detection mechanism can make sure that the great secondary users always obey the spectrum evacuation courtesy.

[16] Detection of PUE Attacks in Cognitive Radio Networks supported Signal

Activity Pattern:

In this they suggest a completely unique PUE detection system, termed Signal Activity Pattern Acquisition and Reconstruction System (SPARS). Within the resulting discussion, if not otherwise noted, an attacker refers to a PUE attacker, a sign refers to a PU signal, and a transmitter refers to a PU signal transmitter, which can be a PU or an invader. We define a sign activity pattern (SAP) of a transmitter as a series of ON and/or OFF periods of the transmitter along the time. An ON period refers to the amount of a busy period that the transmitter is transmitting and therefore the SUs must refrain from communications. An OFF period refers to the amount of an idle period between two adjacent ON periods.

Different from current solutions on PUE detection, SPARS doesn't have control on the sort of PUs, i.e., SPARS are often applicable to all or any sorts of PUs. Furthermore, SPARS doesn't need any a

priori knowledge of PUs. It acquires the SAP of a transmitter through spectrum sensing, and compares it with SAPs of PUs through a SAP rebuilding model. If the observed SAP isn't 'like' the SAPs of PUs, which is measured by the rebuilding error, then the transmitter is an invader. Our inspiration is that while an invader can cheat the signal itself, it cannot defraud on its objective, i.e., causing DoS to the CRN.

20.

An invader can transmit a PU signal, but its SAP is probable to vary from those of PUs. This is often because the aim of the invader is to occupy the channel to cause DoS to the CRN. Therefore, the invader aims to considerably decrease the channel simple use to the CRN, e.g., by increasing the ON periods and/or decreasing the OFF periods. Thus the invader creates a special SAP from PUs. On the opposite hand, if an invader also cheat its SAP, i.e., manipulates its spectrum profession to be almost like the one among PUs, we dispute that such a 'mild' PUE attack is tolerable by the CRN, and hence defeats the DoS objective of the attacker. This is often because a CRN usually selects the operation channels with low spectrum occupation by PUs. An invader with a similarly low spectrum occupation isn't a significant danger to the CRN, because the CRN has been designed with the mild disturbance (from PUs) in mind, and hence is suitable to a PUE attack that causes a light disruption. Therefore, by targeting the target of the invader, SPARS is effective to detect PUE attack.

[17] Defense against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard:

Along with the rising demand in high-speed wireless communications, spectrum lack has become a significant challenge to the rising wireless technologies. In licensed networks, the primary users function in their allocated licensed bands. It's observed that the licensed bands are generally underutilized and their job fluctuates temporally and geographically within the range of 15–85%. Cognitive radio (CR) networks provide a talented solution to the spectrum scarcity and underutilization problems.

In this a uniform AES-assisted DTV scheme, where an AES-encrypted orientation signal is generated at the TV transmitter and used because the sync bits of the DTV data frames. By allowing a shared secret between the transmitter and therefore the receiver, the reference signal are often regenerate at the receiver and wont to achieve accurate classification of authorized primary users. Moreover, when combined with the investigation on the auto-correlation of the received signal, the

presence of the hateful user are often detected precisely regardless of the primary user is present or not. The proposed approach can effectively combat PUEA with no change in hardware or system structure except of a plug-in AES chip, which has been commercialized and widely accessible . It should be noted that the AES-encrypted reference signal is additionally used for organization purpose at the authorized receivers, within the same way because the conventional synchronization sequence.

21.

[18] Cooperative Spectrum Sensing in Cognitive Radio Networks within the Presence of the primary User Emulation Attack :

Cognitive radio generally includes four basic elements: spectrum sensing, spectrum management, spectrum sharing and spectrum mobility. Among them, Spectrum sensing may be a essential functionality where the secondary users check the frequency spectrum and see empty channels to use. The spectrum sensing can basically be classified as noncooperative sensing, cooperative sensing and interference-based sensing. Most research work currently specialise in the cooperative spectrum sensing method where a group of secondary users swap the sensing information or propel the knowledge to a fusion center to enhance discovery probability performance, taking under consideration that some secondary users' channels could also be deteriorate by multi-path fading or shadowing.

So far, several algorithms are planned to place into practice cooperative sensing in CR networks. during a hard combining (HDC) method is planned where the binary detection results of multiple secondary users are converge to a fusion center and therefore the final judgment is formed supported “1-out-of-n” rule. In, a soft combining method, like maximal ratio combining (MRC), is developed where the sensing statistics of various secondary users are combined by using the optimal weight coefficients determined by the immediate channel gain between the primary and secondary user. it's shown that the soft combination yields a better detection probability than the hard combination. formulate the cooperative spectrum sensing as a nonlinear optimization problem during which the interference to the primary users is minimized.

During this we establish a model of cooperative spectrum sensing within the presence of PUEA and suggest an idea to maximize the detection probability of primary user. because the PUEA is launched during a CR network using cooperative sensing method, each secondary user receives the signals from both the invader and therefore the primary user and sends its sensing information to a fusion center. The received signal (or the sensing information) is then optimally combined with some appropriate weights to maximize the detection probability with a restraint of faux alarm

probability. The optimal weights are associated with the channel state information (CSI) between the attacker and secondary users and between the primary user and secondary users, which are predictable by using existing channel judgment algorithms. The most contribution of this paper is to maximize the detection probability of the primary user by deriving the optimal combine weights, considering the existence of the PUEA during a CR network. Note that we assume the PUE attacker has been detected and this paper centers on the detection of the primary user instead of the detection of PUEA.

22.

[19] Soft Combination and Detection for Cooperative Spectrum Sensing in Cognitive Radio Networks:

Cognitive radio (CR) enables much higher spectrum effectiveness by dynamic spectrum access. Therefore, it's a possible method for future wireless communications to alleviate the spectrum lack issue. As unlicensed (secondary) users of the spectrum band, CR operators are permitted to use the spectral resources only if it doesn't cause interference to the primary (licensed) users, which entails nonstop spectrum sensing in CR networks. Therefore, it becomes a dangerous issue in cognitive radio to dependably and quickly detect the presence of the primary users.

Spectrum sensing may be a rough task due to surveillance, fading, and time-varying natures of wireless channels. To fight these impacts, cooperative spectrum sensing schemes are planned to get the spatial diversity in multiuser CR networks. In cooperative spectrum sensing, information from different CR users is combined to form a choice on the presence or absence of the primary user. In this letter, soft combination is investigated, during which the precise sensing energies from different CR users are joint to form a far better decision. Supported the Neyman-Pearson criterion, we obtain an optimal soft combination scheme that maximizes the detection probability for a given false alarm probability. It's established that soft combination schemes, even simple equal gain combination, have important performance improvement over the traditional hard combination. Confident by the performance gain of soft combination, we further propose a replacement softened hard mixture scheme with only two-bit overhead for every CR user, which, however, exhibits far better performance than the conservative one-bit hard combination scheme.

CHAPTER 3

BINARY HYPOTHESIS

3.1) Spectrum Sensing

Spectrum sensing are often viewed as a binary hypothesis testing problem during which hypothesis H_0 indicates that the first user (PU) is inactive whereas hypothesis H_1 indicates that a PU is active.

$$H_0 : \text{Only Noise}$$

$$H_1 : \text{PU} + \text{Noise}$$

$$R(t) = A * X(n) + W(n) \quad \dots(1)$$

Supposing $A = 0$, we get

$$R(t) = W(n) \quad \dots(2)$$

Supposing $A = 1$, we get:

$$R(t) = X(n) + W(n) \quad \dots(3)$$

Here:

- A is that the amplitude gain of the channel.
- Signal received at a secondary user (SU) are denoted by $R(t)$.
- $W(n)$ is the noise introduced by AWGN.
- $X(n)$ is that the primary users(PU's) transmitted signal.

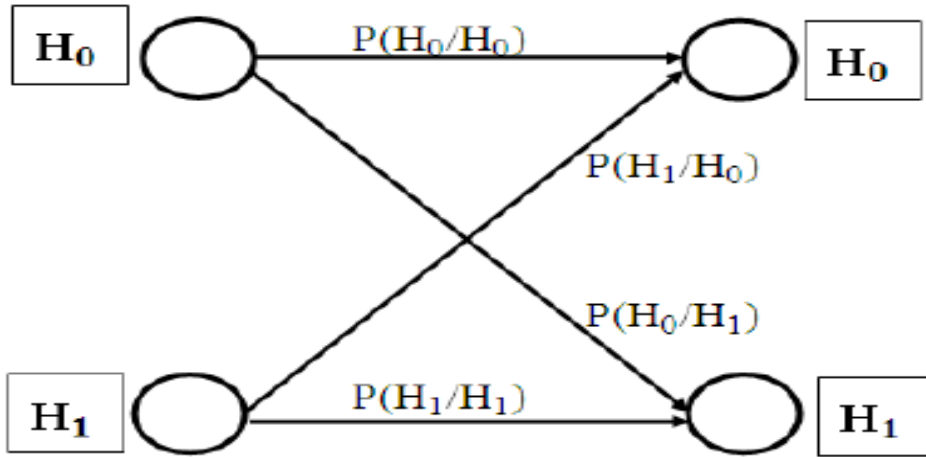


Fig 3.1

24.

We can define four possible cases for the detected signal:

- Case1:** declaring H_0 when H_0 is true ($H_0|H_0$);
- Case2:** declaring H_1 when H_1 is true ($H_1|H_1$);
- Case3:** declaring H_0 when H_1 is true ($H_0|H_1$);
- Case4:** declaring H_1 when H_0 is true ($H_1|H_0$);

The performance of spectrum sensing can be characterized by the

Probability of false alarm

$$P_f = P(H_1|H_0) \quad \dots(4)$$

Probability of detection

$$P_d = P(H_1|H_1) \quad \dots(5)$$

3.2) Result

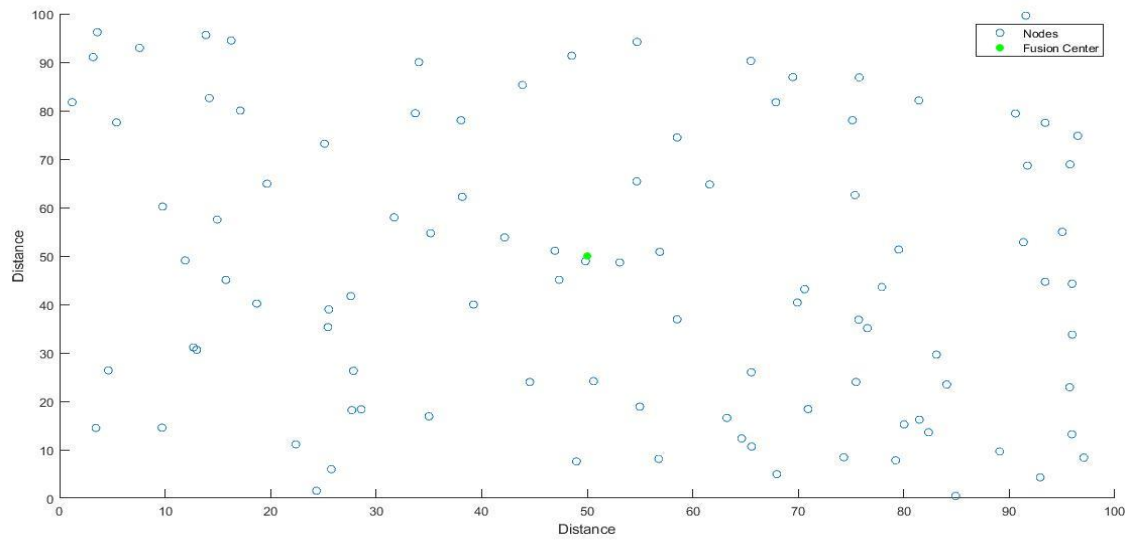


Fig 3.2

25.

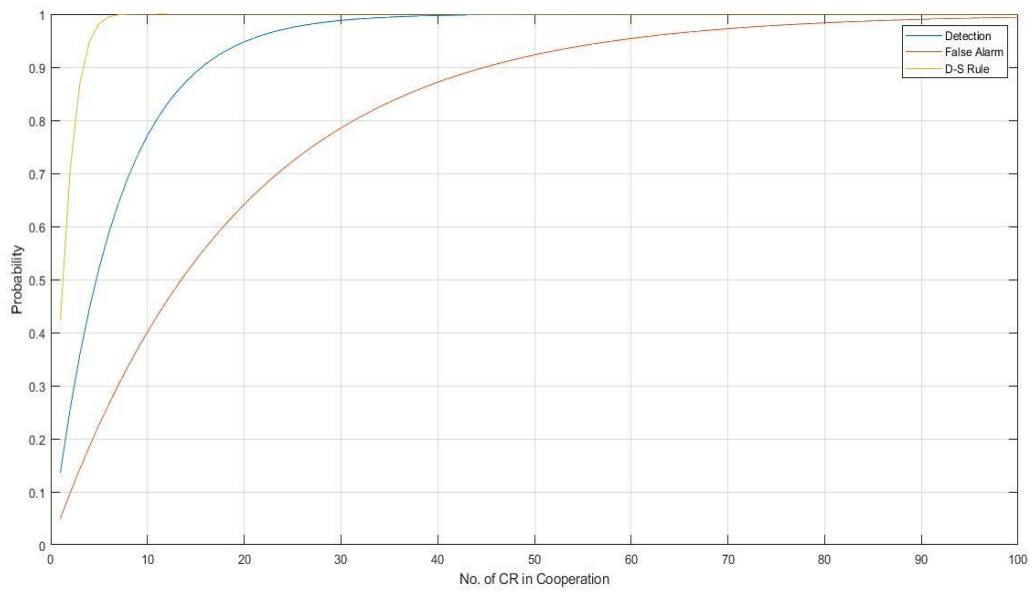


Fig 3.3

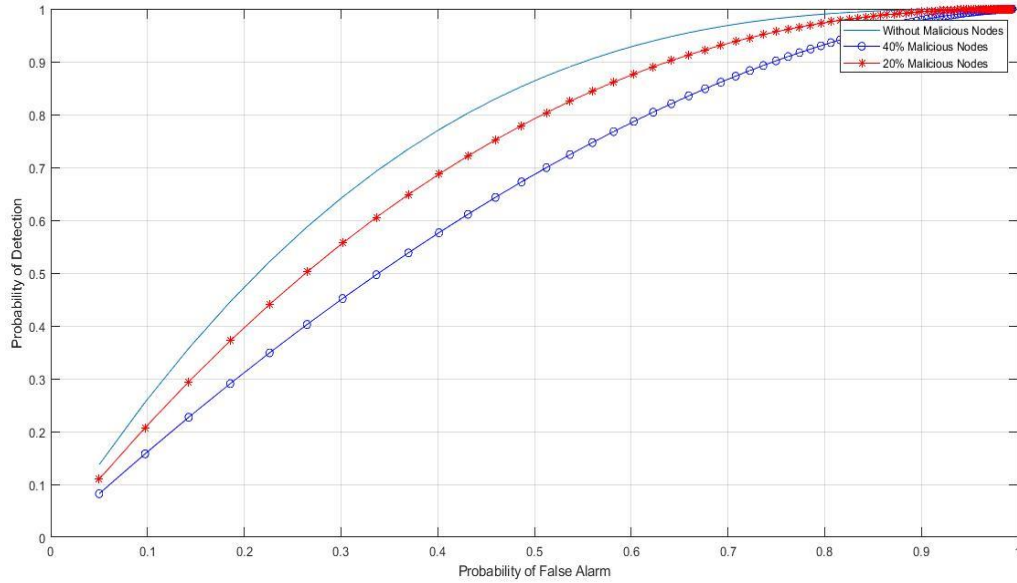


Fig 3.4

3.3) Conclusion

- Using Binary testing, we took 100 CR users and plotted their distance from the Fusion Center.
- Using This, we calculated we calculated the probability of Detection and False Alarm with varying CR users at different time.
- We calculated the Probability of Detection Vs Probability of False Alarm in the given three cases.

Binary testing assumes the case where there are only primary users and noise not taking the fact that there can be Malicious Users as well. We can overcome this drawback using Multilevel Hypotheses.

CHAPTER -4

Multilevel Hypothesis Testing

4.1) Analysis of CR Network

The planned system model may be a centralized CR network, including a PU transmitter, N Cooperative CR users, an FC, and a hateful PUEA. The network model is shown in Fig. We assume that the energy finding scheme is employed for local spectrum sensing. A hateful PUEA is present in the radio environment which tries to stop the CR users from accessing the spectrum hole.

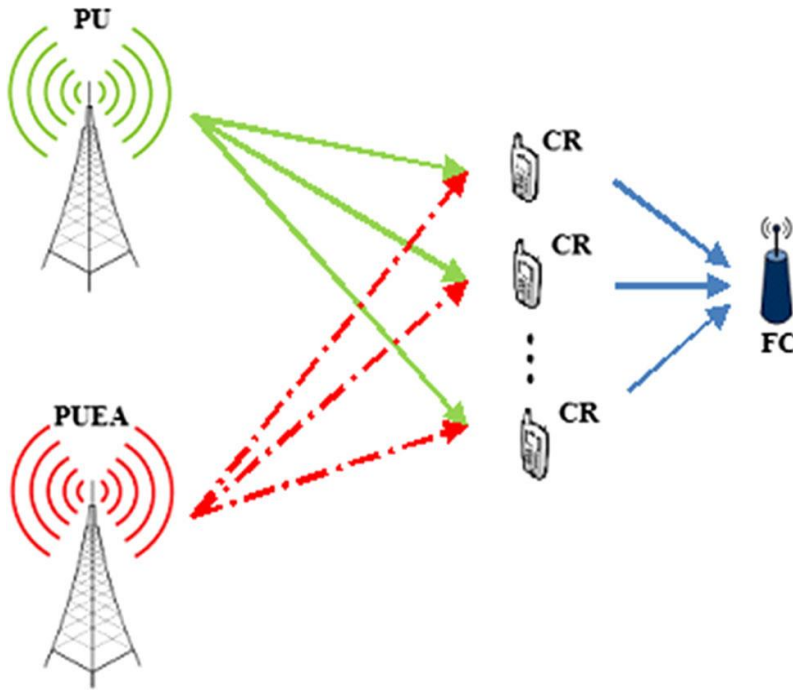


Fig. 4.1 Network layout

Depending on the presence or absence of the PU and PUEA, there are four possible states which may be expressed as:

Hs0: only Noise

Hs1: PU + Noise

Hs2: PUEA + Noise

Hs3: PU + PUEA + Noise

.....(6)

28.

The first state Hs0 occur when the CR users receive only noise. Moreover, the channel is occupied neither by PU nor by PUEA. The second state Hs1 happens when the PU transmits over the channel while the PUEA is absent. When the PU is absent and PUEA transmit the fake signal, the CR users receive only the PUEA signal plus noise, as statedby the third suggestion Hs2. Finally, the last state Hs3 indicate the immediate presence of both PU and PUEA signals. We assume that two hypothesis H1 and H0 indicate thepresence and absence of PU signal, respectively. Similarly, the presence and absence of the PUEA signal are denoted by Eon and Eoff, respectively.Based on the above mentioned assumptions, the probability of every hypothesis Hsk,denoted by pk, is decided as:

$$\pi_0 = P(H_{s0}) = P(H_0, E^{off}) = P(E^{off} | H_0) P(H_0)$$

$$\begin{aligned}
\pi_1 &= P(H_{s1}) = P(H_1, E^{off}) = P(E^{off} | H_1) P(H_1) \\
\pi_2 &= P(H_{s2}) = P(H_0, E^{on}) = P(E^{on} | H_0) P(H_0) \\
\pi_3 &= P(H_{s3}) = P(H_1, E^{on}) = P(E^{on} | H_1) P(H_1) \quad \dots(7)
\end{aligned}$$

Let two invader strategy parameters α and β be the conditional probabilities regarding the presence of the fake PUEA signals in two hypothesis H_1 and H_0 , respectively (i.e. $\alpha = P(E_{on}|H_1)$ and $\beta = P(E_{on}|H_0)$). Then, the above equation can be simplified to

$$\begin{aligned}
\pi_0 &= P(H_{s0}) = (1 - \beta)P(H_0) \\
\pi_1 &= P(H_{s1}) = (1 - \alpha)P(H_1) \\
\pi_2 &= P(H_{s2}) = \beta P(H_0) \\
\pi_3 &= P(H_{s3}) = \alpha P(H_1) \quad \dots(8)
\end{aligned}$$

By considering the four-level hypotheses, the received signal at the i th sample of the j th CR user, x_{ij} , can be formulated as

$$x_j^i = \begin{cases} n_j^i \\ \sqrt{\gamma_j} P_j^i + n_j^i \\ \sqrt{\lambda_j} e_j^i + n_j^i \\ \sqrt{\gamma_j} P_j^i + \sqrt{\lambda_j} e_j^i + n_j^i \end{cases} \quad \dots(9)$$

29.

Moreover, M samples are utilized for local energy discovery at each CR user. The observed energy of the j th user, E_j , is given by

$$E_j = \sum_{i=1}^M |x_j^i|^2 \sim \begin{cases} a_j \\ (\gamma_j + 1)b_j \\ (\lambda_j + 1)c_j \\ (\gamma_j + \lambda_j + 1)d_j \end{cases} \quad \dots(10)$$

where the random variables a_j , b_j , c_j , and d_j follow a central Chi-square allocation with M degree of freedom. But, according to central limit theorem, if a large number of samples are measured (i.e. $M > 10$), these random variables can be assumed to be Gaussian distributed.

In CSS, local measured energy of each CR user is sent to the FC to make a global decision about the presence or absence of the PU signal. The output signal at the FC is where “n” is a predefined threshold.

$$Y = \sum_{j=1}^N E_j \begin{matrix} H_1 \\ > \\ H_0 \end{matrix} < \eta \quad \dots(11)$$

Considering the Eq. (10) and (11), in the presence of the PUEA, the decision statistic Y is a Gaussian distribution as

$$Y \sim \begin{cases} \mathcal{N}(\mu_0, \sigma_0^2) \\ \mathcal{N}(\mu_1, \sigma_1^2) \\ \mathcal{N}(\mu_2, \sigma_2^2) \\ \mathcal{N}(\mu_3, \sigma_3^2) \end{cases} \quad \dots (12)$$

where one can easily verify that

$$\begin{aligned} \mu_0 &= MN, \sigma_0^2 \\ \mu_1 &= MN(\bar{\gamma} + 1), \sigma_1^2 = 2MN(\bar{\gamma} + 1)^2 \\ \mu_2 &= MN(\bar{\lambda} + 1), \sigma_2^2 = 2MN(\bar{\lambda} + 1)^2 \\ \mu_3 &= MN(\bar{\gamma} + \bar{\lambda} + 1), \sigma_3^2 = 2MN(\bar{\gamma} + \bar{\lambda} + 1)^2 \end{aligned} \quad \dots(13)$$

30.

Let Q_{fa} and Q_m be the probability of global fake alarm and miss detection in CSS, respectively. Then we have $Q_{fa} = P(D_{on}|H_0)$ and $Q_m = P(D_{off}|H_1)$, where D_{on} means that the FC's decision is the presence of PU signal and D_{off} means that the global decision declare the absence of PU signal. To evaluate the presentation of CSS in the presence of a PUEA and compare it to conventional energy discovery, in which the PUEA is not considered, we use probability of error Q_e . The parameter Q_e defines the probability of making a incorrect decision in PU detection. In general, the probability of error can be written as

$$Q_e = P(H_0, D^{on}) + P(H_1, D^{off}) = P(H_0)Q_{fa} + P(H_1)Q_m \quad \dots(14)$$

An proper spectrum sensing rule is analyze by considering the attacker. As mentioned before, the PUEA sends fake signals in the radio environment to deceive CRusers, and consequently prevent them from access idle frequency bands. Hence, the restrictive PDFs of the decision statistics Y under two hypotheses H_0 and H_1 canbe expanded as

$$p(Y|H_0) = p(Y|H_0,E^{on}) P(E^{on}|H_0)+ p(Y|H_0,E^{off}) P(E^{off}|H_0)$$

$$p(Y|H_1) = p(Y|H_1,E^{on}) P(E^{on}|H_1)+ p(Y|H_1,E^{off}) P(E^{off}|H_1).....(15)$$

Regarding the definition of the attack parameters a and b the above equation can be simplified to

$$p(Y|H_0) = p(Y | H_0, E^{on})\beta + p(Y | H_1, E^{off}) (1- \beta)$$

$$p(Y|H_1) = p(Y | H_1, E^{on})\beta + p(Y | H_1, E^{off}) (1- \alpha) \quad \dots(16)$$

4.2) The proposed multi-level hypotheses test approach

In this section, the typical minimum Bayes cost criteria is applied to seek out the hold hypothesis. The Bayesian formulationassumes that there are four hypotheses with unequal priori probabilities $\pi_k=P(H_{sk})$ determined by the Eq. (6) and therefore the decision statistic Y which admits the PDFs expressed by Eq. (12) under H_{sk} . For an accurate decision, the choice space must be partitioned into four separate regions and every point of the observation space must be generalized into one among these regions by minimizingBayesian risk function. For a four-level test, the Bayesian risk function is defined as

$$\begin{aligned}
\mathcal{R} &= \sum_{n=0}^3 \sum_{k=0}^3 C_{nk} \int P_z(Y|H_{sk}) \pi_k dy \\
&= \sum_{n=0}^3 \int \sum_{k=0}^3 C_{nk} \int P(H_{sk}|Y) p(Y) dy \\
&= \sum_{n=0}^3 \int C_n(Y) P(Y) dy \quad \dots (17)
\end{aligned}$$

where $C_n(Y) = \sum_{k=0}^3 C_{nk} P(H_{sk}|Y)$ is the average cost of deciding H_{sk} and c_{nk} is the cost of selecting H_{sn} when H_{sk} holds. A symmetric cost test is assumed, i.e.

$$C_{nk} = \begin{cases} 0 & \forall n = k \\ 0 & \forall n \neq k \end{cases} \quad \dots (18)$$

Then the parameter $C_n(Y)$ can be simplified to

$$C_n(Y) = \sum_{\substack{k=0 \\ k \neq n}}^3 P(H_{sk}|Y) \quad \dots (19)$$

to obtain the parameters that minimize $C_n(Y)$, the likelihood ratio or its logarithmic form is employed as decision statistic and hold hypothesis is identified by comparing this ratio with a predetermined threshold. In our four-level hypothesis problem, a replacement approach is provided for decision statistic by multiplying the prices $C_n(Y)$ by the scaling factor $p(Y)/p(Y|H_{s0})$. which is independent of index n . The modified costs are obtained as

$$\tilde{C}_n(Y) = C_n(Y) \cdot \frac{p(Y)}{p(Y|H_{s0})} \quad \dots (20)$$

The values of $\tilde{C}_n(Y)$; $n = 0; 1; 2; 3$ are also obtained as

$$\begin{aligned}
\tilde{C}_0(Y) &= \pi_1 A_1(Y) + \pi_2 A_2(Y) + \pi_3 A_3(Y) \\
\tilde{C}_1(Y) &= \pi_0 + \pi_2 A_2(Y) + \pi_3 A_3(Y) \\
\tilde{C}_2(Y) &= \pi_0 + \pi_1 A_1(Y) + \pi_3 A_3(Y) \\
\tilde{C}_3(Y) &= \pi_0 + \pi_1 A_1(Y) + \pi_2 A_2(Y)
\end{aligned}
\tag{21}$$

where $\Lambda_k(Y)$ is calculated in the FC as

$$\Lambda_k(Y) = \frac{P(Y|H_{sk})}{P(Y|H_{s0})} \quad k = 0,1,2,3 \dots \tag{22}$$

When the hypothesis H_{s0} or H_{s2} is held, the deduced channel is empty for CR users but H_{s2} states that the PUEA is present within the free channel. CR users must leave the channel when H_{s1} or H_{s3} are inferred due to the PU presence.

4.3) Results

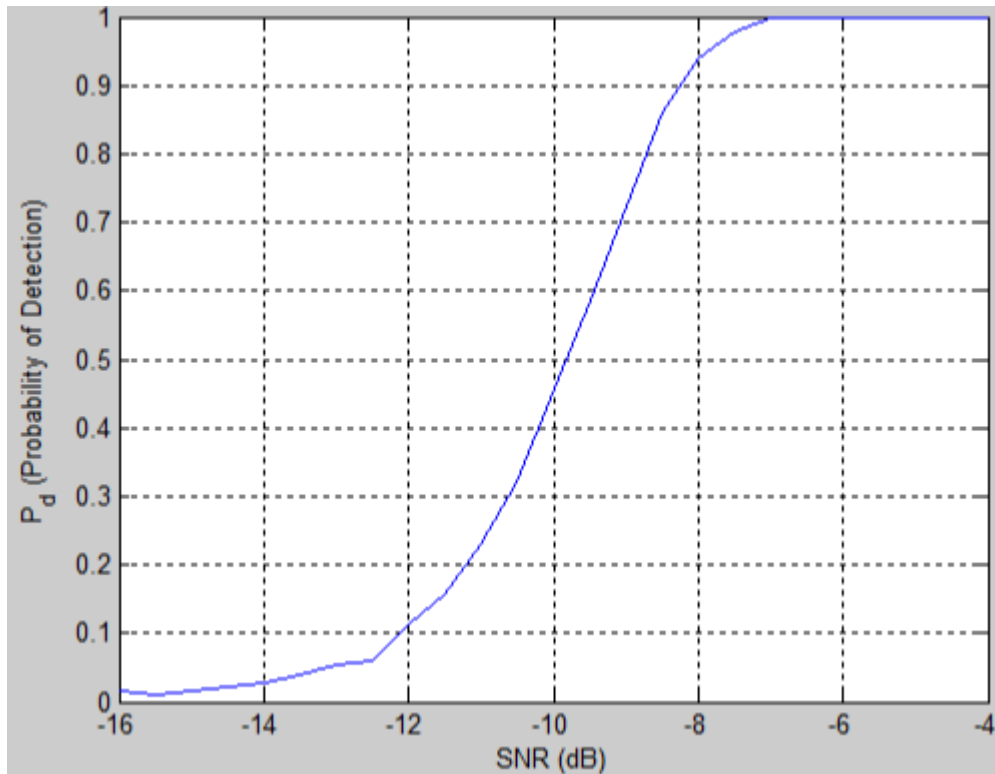


Fig 4.2

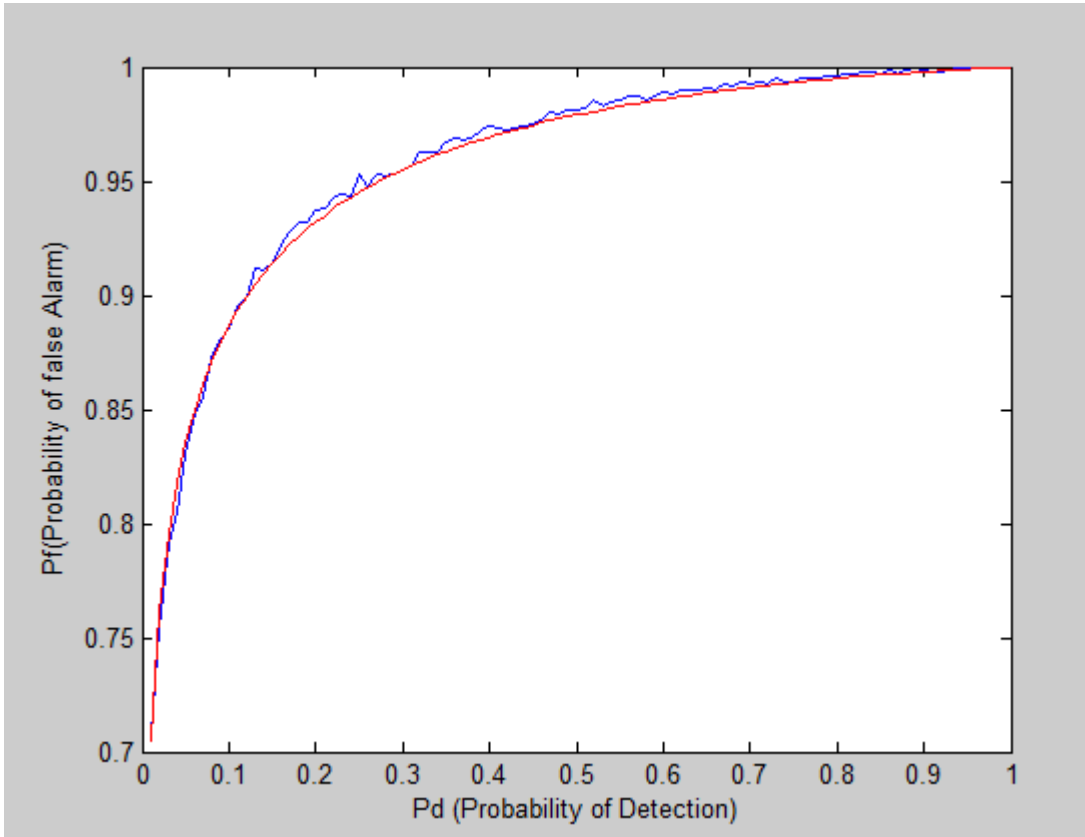


Fig 4.3

REFERENCES

- [1] A. Ali, W. Hamouda. “Advances on Spectrum Sensing for Cognitive Radio Networks: Theory and Application” *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, Vol. 19, No. 2, Second Quarter 2017
- [2] M. Sharifi, A.A. Sharifi¹, M.J. Musevi Niya. “Cooperative spectrum sensing in the presence of primary user emulation attack in cognitive radio network: multi-level hypotheses test approach” January 2018, Volume 24, [Issue 1](#), pp 61–68
- [3] I. Gupta, O.P. Sahu, “An Overview On Primary User Emulation Attack in Cognitive Radio Networks” *IEEE Conference Record*, 42656; IEEE Xplore (2018) ISBN:978-1-5386-3452-3
- [4] J. Ma, G. Zhao, & Y. Li, “Soft combination and detection for cooperative spectrum sensing in cognitive radio networks”. *IEEE Transactions on Wireless Communications*, vol.7no. (11), 2008, pp. 4502–4507.
- [5] R. Chen, J.M. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks”. In 1st *IEEE workshop on networking technologies for software defined radio networks* (2006) (pp. 110–119).
- [6] R. Chen, J.M. Park, & H.J. Reed, “Defense against primary user emulation attacks in cognitive radio networks”. *IEEE Journal of Selected Area in Communications*, vol.26(1), pp.25–37. (2008)
- [7] O. Leon, J. Hernandez-Serrano, & M. Soriano, “Cooperative detection of primary user emulation attacks in CRNs”. *Computer Networks*, 2012. Vol.56(14), pp.3374–3384.
- [8] C. Zhao, W. Wang, L. Huang, Y. Yao “Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio” *In 5th international conference on wireless communications, networking and mobile computing (WiCom '09)*(2009). (pp. 1–5).

- [9] S. Anand, Z. Jin, & K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks." *In Proceeding IEEE international dynamic spectrum access networks* (2008). (pp. 1–6).
- [10] Z. Jin, S. Anand, K. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing". *ACM SIGMOBILE Mobile Computing and Communication Review*, (2009). Vol.13, pp.74–85.
- [11] Z. Jin, K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks". *In IEEE international conference on communications* (2009). (pp. 1–5).
- [12] C. Xin, M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern." *IEEE Transactions on Mobile Computing*, 13(5), 1022–1034. (2014)
- [13] A. Alahmadi, M. Abdelhakim, J. Ren, T. Li "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard". *IEEE Transactions on Information Forensics and Security*, (2014). Vol. 9(5), pp. 772–781.
- [14] C. Chen, H. Cheng, Y. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack". *IEEE Transactions on Wireless Communications*, (2011). Vol.10(7), pp. 2135–2141.
- [15] S. Mishra, A. Sahai, & R.W. Brodersen, "Cooperative sensing among cognitive radios. In Proceedings of the IEEE international conference on communications" (2006) (pp. 1658–1663).

