International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 2 (2015) pp. 3827-3842

http://www.ripublication.com

Intense Explore Algorithm – A Proactive Way To Eliminate PUE Attacks In Cognitive Radio Networks

A.C.Sumathi [1*] and Dr.R.Vidhyapriya [2]

[1]Associate Professor, Department of Computer Science and Engineering,*
SNS College of Engineering, SNS Kalvi Nagar,
Sathy Main Road, Coimbatore, Tamilnadu,641107, India
Tel : +91 - 9443893535, Email ID : sumathi.ac@gmail.com
[2] Professor , Department of Information Technology,
PSG College of Technology,Coimbatore

Abstract

In cognitive radio network, secondary users (without license) are allowed to access the licensed spectrum if primary users (having licensed) are not present. A serious threat in physical layer of this network is that a malicious secondary user exploiting the spectrum access etiquette by mimicking the spectral characteristics of a primary user known as Primary User Emulation Attack (PUEA). The main objective of this paper is to eliminate the PUE attack that may arise from one of the secondary users. We propose our Intense Explore algorithm to eliminate the PUE attack in a proactive way. Our simulation results proved that our proposed Intense Explore algorithm yields better results than existing techniques.

Key words: Intense Explore, Cognitive Radio Network, PUEA.

1. INTRODUCTION

The Federal Communication Commission (FCC) defined Cognitive radio (CR) as the radio that can change its transmission parameters based on interaction with the environment in which it operates [1].

The Wireless communication has been increased and requirement of high data rate has also been increased. The licensed spectrum space remains idle at most of the times [1] due to inefficient allocation of frequencies and the cellular bands are overloaded. To meet the spectrum demands and to utilize the spectrum, FCC revisited the problem of spectrum management [2]. This inventiveness focused on Cognitive Radio (CR). The IEEE 802.22 is the standard for cognitive wireless regional area

networks (WRANs). The main goal of CR is to identify the unused licensed spectrum for secondary users without causing interference to the Primary User (PU). As the Cognitive Radio can dynamically adapt to its operating environment they face many security issues [3].

Due to Dynamic Spectrum Access (DSA) CR network gives opportunity to the attacker to damage the routine activities of the communication networks. CR are capable of sensing the unused spectrum—i.e., spectrum "whitespaces" [4]. The key problem is to distinguish the primary user signal from the secondary user in an efficient way. On the other hand, the detection of Primary User Emulation (PUE) attack is important. The secondary users must sense and identify the emulation attacker.

2. OVERVIEW OF SECURITY ISSUES

The dynamic spectrum allocation facilitates the secondary usage of licensed band. The spectrum must be carefully used by the Secondary User (SU) in order to avoid interference with the Primary User (PU) [5]. Based on the behavior of the protocol stack various attacks are categorized [5] as follows.

2.1 Physical Layer

In cognitive radio network, secondary users (without license) are allowed to access the licensed spectrum if primary users (having license) are not present. To protect the priority of primary users, secondary users must quit the spectrum when primary users emerge. Therefore, secondary users need to carry out spectrum sensing to detect the existence of primary users.The primary user emulation attack (PUEA) is performed in the physical layer, in which the PU signal characteristics are impersonated by the malicious user (MU) therefore the SUs may think the MU as the PU [6]. Jamming may be possible in this layer when the jammer sends the data packets continuously to the channel. Thus causes the SU unable to sense the idle channel [6]. The CR cannot adapt to the changing environment when the utility resource parameters are modified, thus causes the objective function attack (OFA) [6]. The spectrum sensing information to the attacker and the transmission can be interrupted by preventing the channels from sharing information leads to the common control data attack (CCDA) [5]. If the parameters are not up to the threshold level the communication stops.

2.2 Link layer

The data transfer takes place from one node to another in the link layer and three types of attacks suck as spectrum sensing data falsification (SSDF) or the byzantine attack where the fusion centers decision is falsified because of the wrong spectrum sensing results [5]. This attack targets both centralized and distributed CRNs. In a centralized CRN, a fusion center is responsible for collecting all the sensed data and then making a decision on which frequency bands are occupied and which are set free. Fooling the fusion center may lose some legitimate users. This type of attack is defensive by calculating the threshold value. It is calculated by finding the sum of the collected spectrum that is sensed. The malicious user can change the route

information of the node by providing wrong information about the node called the selfish channel negotiation (SCN) [5]. The control channel is reserved by the attackers and is saturated such attack is called the Control channel saturation Denial-of-service (DoS) [5]. This attack degrades the end to end throughput of the whole cognitive radio network. The sequential probability ratio test can be used for this purpose in order to prove its efficiency in terms of detection time.

2.3 Network Layer

The attacks in network layer are sink hole attack and hello flood attack. In sink hole attack the attacker mocks itself as the best route and pulls the neighbors to use this route to forward the packets and to discards those packets. This attack is effective in infrastructure and in a mesh architecture as all the traffic moves through the base station allows the attacker to falsely claim as a best router for packet forwarding. Thus the traffic will be routed to the physical location of the base station and it is difficult to go elsewhere to create a sinkhole. In the hello flood attack the attackers uses enough power and sends broadcasting signals to all the nodes in the network to convince them that it is the closest neighbor. When this attack is detected there occurs a possibility of packet loss, absence of neighbors to forward the packets.

2.4 Transport layer

In transport layer the possible attack is LION attacks. In LION attack, it uses the primary user emulation attack to disrupt transmission control protocol (TCP) connection. It's said to be a cross layer attack pointed at the transport layer where imitating a licensed transmission will force a CRN to achieve a frequency handoffs and thus degrading TCP performance. The attacker intercepts the messages, and it predicts to be in hand off when the frequency band is tested and by claiming it using the PUE results in a total network starvation.

2.5 Application Layer

Since each layer is interconnected to each layer the attacks performed in other layers may cause adverse effect on the application layer.

3. PRIMARY USER EMULATION ATTACK

PUEA is performed in the physical layer. The CR environment allows dynamic spectrum access, the authorized spectrum band is used by the PU and the SU can make use of this spectrum band when the PU is not using it. In PUEA, the attacker is capable of generating the similar signal as the PU, in order to confuse the SU. The incumbent SU identifies the attacker as the PU and vacates the channel immediately. This kind of attack is known as PUEA. The PUEA can cause intervention to the spectrum sensing and reduces the availability of channel to the incumbent SU. This attack is of two types [9].

They are malicious PUEA and selfish PUEA.

(1) *Selfish PUEA:* The attacker's objective is to maximize its own spectrum

usage. Here, the goal of the attacker is to increase its share of spectrum resources. This attack is carried out between two attackers and establishes a dedicated link between the malicious PUE.

(2) *Malicious PUEA:* The attacker's objective is to obstruct secondary user's access to the spectrum. In malicious PUE, attackers try to prevent the legitimate secondary users from using the holes found in the spectrum.

4. PUEA DEFENSE TECHNIQUES

Despite of all the attacks in CRN the PUEA causes adverse effects so the prevention of PUEA is important in CRNs. The methods discussed here focus on the mitigation of PUEA and some assumptions are made to produce better results. Here the PU is TV transmitters. AT first mobile FM wireless microphone is considered as PU and PUEA is defined by Shaxun Chen et al in [7].

4.1 PU Authentication

The stationary helper nodes are used to authenticate PU using link signature and the broadcast spectrum availability information to the SU [8]. The extra helper nodes which are fixed must be authenticated by the trusted authority with the help of public key and certificate. The helper resolution (HR) algorithm is used for the mobile users and the analysis has been done on different attacks. Without repeated training more SU can be served and the successful defense against the attack can be provided.

4.2. Location based method

Based on the location of PU there are three types of defense techniques. In the wavelet transform scheme the fingerprint is extracted using the multi-resolution time frequency property which can be used to distinguish the PUE attacker and the incumbent PU signal. The Time Difference of Arrival (TDOA) scheme is used to detect the PUE attack and to find the position of the emitter. The quadratic error can be minimized by the Weighted Least Square (WLS) method. In order to find the PUEA, tier hierarchical CRN and M-ary hypothesis is done in the two-tier scheme [10].

4.3 Fingerprint verification method

The phase noise is extracted from the received signal in the ANN based scheme. The ANN can identify the transmitter by using the wavelet analysis [11]. Fingerprint is considered as the unique characteristics in [11]. To get the false alarm rate the channel based hypothesis testing can be done. The OFDM uses this technique. Hence the detection probability can be increased by increasing the SNR.

4.4 Transmitter verification scheme

In this scheme three defense techniques are used. In the Distance Ratio Test (DRT), using the pair of verifiers the distance ratio of received signal strength can be obtained. To identify the transmitter location the phase difference of the received signal is obtained using the Distance Difference Test (DDT). In this method the

location of all the users is assumed to be fixed and the verifiers must have tight synchronization. When the attacker is close to the SU performance of the system will be degraded. The peak of the RSS signal can be used to locate the transmitter by using the Location-based Defense (LocDef) [12].

4.5 Sybil attack

Sybil attack is similar to the Byzantine attack in which the Sybil identities are created to modify the decision of SU and launches PUEA. Spider radio, the CR test-bed is used to prove the feasibility [13]. With the decrease in the number of good nodes the cost increases adversely. The fusion center helps to estimate the expected cost.

4.6 Belief Propagation

Belief propagation of the location information can be calculated. Here the location and compatibility function, the message computation, message exchange between neighboring users and until its coverage calculation of belief is done. The PUE attacker can be found when the calculated mean of belief is less than the threshold [14]. Markov random process can be used to achieve better results. The attacker's transmission power and range is limited. All the SUs must be aware of the location information of the PU. When the distance between the PU and the attacker is less, then the calculated belief mean will be more.

5. PROPOSED SOLUTION

5.1 Introduction

An introduction to Primary user emulation attack was given in Section 3 of this paper. Also, various existing defense methods are discussed in the section 4. According to FCC, no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by secondary users. Hence, usual approaches, such as embedding a signature in a primary user's signal or employing an interactive protocol between a primary user and secondary user, cannot be used. Identifying the primary user signal is considered to be a major challenging task.

Our proposed method consists of detecting malicious user signal by a novel approach called Intense explore. It is a continual diagnosis of existing secondary users signal in which few of them may threatens to be a malicious user in future. This proactive detection method is done in a cooperative way.

It has been already shown that, to enhance the sensing performance, cooperative spectrum sensing [15] is involved. A centralized fusion centre will collect the sensing results from the cooperating secondary users. In our proposed method, we consider the centralized cooperative pre-detection. Here, a central identity called fusion centre (FC) [16] will collect the diagnose results from the cooperative secondary users.

5.2 Intense Explore System Model

For our novel Intense explore model, we consider the infrastructure based network of CRs where multiple nodes (or Secondary Users, SUs) may be associated with a

centralized fusion centre as stated in [15], [16]. For the sake of simplicity, we assume the existence of only one fusion centre. The fusion centre will collect the diagnose results from the cooperative secondary user in a regular interval. Each of the cooperative secondary users will diagnose the signals of other neighbor secondary users at a regular interval. The main objective of diagnosing neighboring secondary users signal is to anticipate that any of these secondary users may become a malicious user in future and threaten the cognitive radio network with PUE attack. Assuming any of the neighboring secondary users signal suspected to emulate the primary signal, then it is reported the fusion center. The fusion centre which may receive similar reports from other cooperative secondary users ,in turn alert all the cooperating secondary users in the network about the anticipated PUE attack and relinquishes the suspected secondary user from the CRN.

5.3 Intense Explore Algorithm

In this section the Intense Explore Algorithm is explained in detail. In the Intense Explore algorithm two set of secondary users (SUs) such as At and Bt are considered. The fusion center takes the decision about the suspected malicious user based on the reports from the At. Each users in At is assumed to be sensing their neighboring users in Bt. Assume that if any two SUs in At reports the same sensing result about the same SU in Bt say Bj, whereby the energy level of it exceeds the threshold, then it is suspected to be the malicious SU. Thus the fusion center alerts all other SU about the suspected user as the malicious SU.

The energy detection of Bj is done by the separate function specified as Energy detection. The energy detection function exploits spectral correlation property of cyclostationary feature for detecting the energy. This function reports At about the suspicious secondary user Bj if any. The Intense Explore algorithm and Energy detection function is as follows:

Algorithm: Intense Explore

1 **Input:** Set of SUs
2 **Output:** Decision report from fusion center
3 **for each** slot t do
4 f ← Fusion Center
5 A_t ← Set of cooperative SUs
6 B_t ← Neighboring SUs of A_t
7 **for each** A_i in A_t do
8 Assume *Bt* as neighboring SUs of A_i
9 **for each** B_j in B_t do
10 //Call function for Energy detection of *Bj*
11 R(A_i,B_j)←Energy Detection (B_j)
12 **end for**
13 // Fusion Center Decision
14 for the same B_j
15 **if** (R(A_i, B_j) ← True) for all A_i **then**

16 B_j ← Suspected SU
17 f alerts all the SUs about B_j

Function: Energy Detection

---

1 Input: Bj
2 Output: SCF(Bj), the suspected malicious Su
3 Pi ← Threshold
4 Si ← Sensed Signal of Bj
5 for Si in Bj do
6 I ← Identify the autocorrelation function
7 C ← Fourier transform of autocorrelation function
8 SCF(Bj) ← Sensing result of Bj obtained from SCF generator
9 if (SCF(Bj) > Pi) then
10 SCF(Bj) ← True // Here Bj is suspected to be malicious user
11 return SCF(Bj)

5.4 Energy Detection using Cyclostationary feature

The cooperative secondary users diagnose the neighboring signals by means of exploiting the energy level in the signal. Energy detection uses the energy spectra of the received signal in order to identify the frequency locations of the transmitted signal. Energy detection approach relies only on the energy present in the channel.

In this paper we use the cyclostationary feature detection method to read the signal energy of secondary users. A cyclostationary process has statistical properties that vary periodically over time. Cyclostationary feature detection method [18] deals with the inherent cyclostationary properties or features of the signal. Cyclostationary spectrum sensing method performs better in low SNR regions, because of its noise rejection capability. Two-dimensional spectral correlation is the way to extract the periodic features of the signal. These signals are cyclostationary processes that are periodic in time t. They also possess a periodic autocorrelation function.

$$R_x(t,\tau) = R_x(t + T_0, \tau) \tag{1}$$

The Fourier transform of the autocorrelation function is given as follows

$$R_x^{\alpha}(\tau) = \lim_{T \to \infty} \frac{1}{T} \int_T x(t + \frac{\tau}{2}) x(t - \frac{\tau}{2})^* e^{-j2\pi\alpha t} dt \tag{2}$$

In the above equation, α is the fundamental cyclic frequency and $R_x^{\alpha}(\tau)$ is the

cyclic autocorrelation function.

Fourier transform of the CA function is defined as the cyclic spectral density (CSD) function

$$S_x^{\alpha}(f) = \sum_{\tau=-\infty}^{\infty} R_x^{\alpha}(\tau) e^{-j2\pi f \tau} \tag{3}$$

This function is also called the spectral correlation function. The spectral correlation characteristic of the Cyclostationary signals gives us a richer domain signal detection method.

The block diagram of a cognitive radio network for energy detection is shown in Figure. 1.

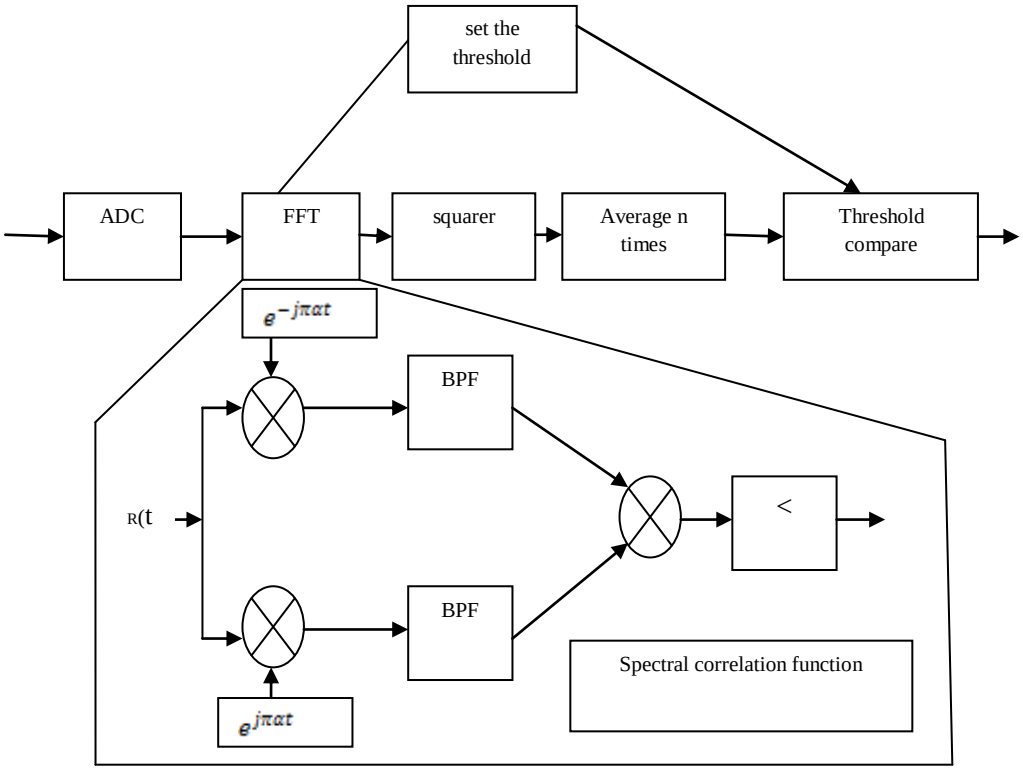

Fig 1 Block diagram of Energy detection

When SCF is plotted, the occupancy status of the spectrum can be found out. If a malicious secondary signal is present in the operating frequency range, the SCF gives a peak at its centre. The peak will not be present in the case when the secondary user is operating in its normal scenario without any intention of creating a PUE attack.

6. SIMULATION RESULTS

6.1 Cognitive Radio Network

A cognitive radio network is simulated in MATLAB 2012(b). In a frequency range of 54-864 MHz, five channels have been allotted each with bandwidth of 6-8 MHz. The Fig 2 shows a network with three primary users in three channels at frequencies 54MHz, 663MHz and 864 MHz. Two channels at the frequencies 257 MHz and 460 MHz are idle. The Received Signal Strength (RSS) levels of about 5 dB imply the primary signal. Using energy detection techniques, white holes are identified which can be utilized by the secondary user for efficient utilization of the spectrum.

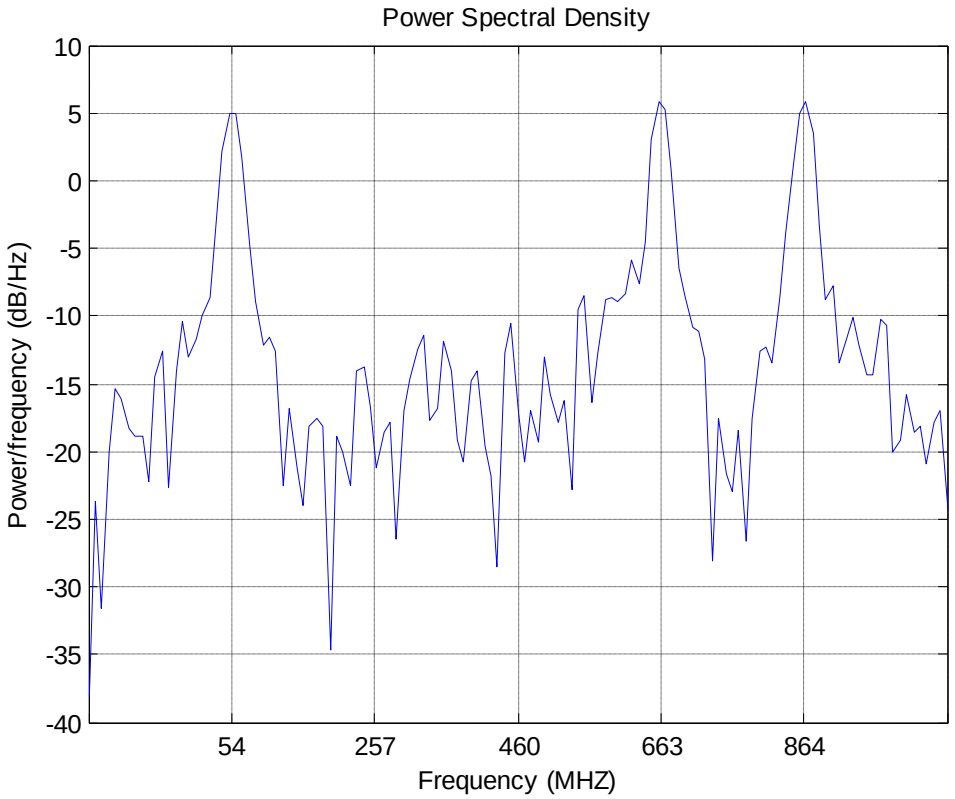

Fig 2. Periodiogram Graph of CRN with 3 primary users, Frequency range 54-864 MHZ, Power level – 5dB

6.2 Intense Explore Algorithm

In the Intense Explore Algorithm the number of SUs in set At senses the neighboring SUs in Bt. Fig.3 represents the number of cooperative SUs in set At senses the neighboring SUs in Bt at the regular interval. In the same time interval, one SU in Bt will be sensed by more than one SU in At. For instance in Fig 3, B9 is sensed by A2 and A3 at the time slot 6. The sensing of B9

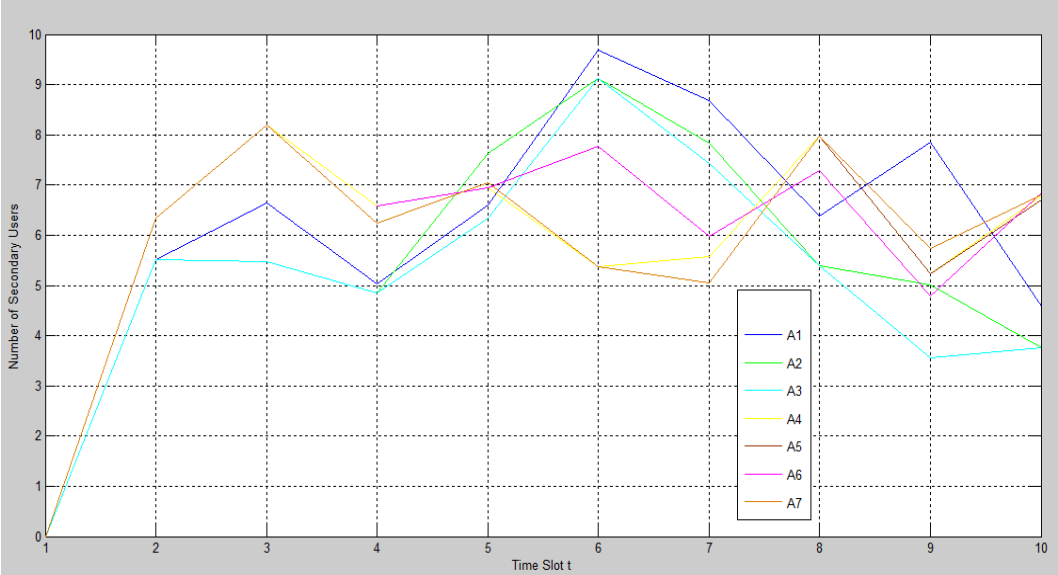

Fig.3. Each SU in At senses same SUs Bj in Bt by A2 and A3 is done through the SCF function. The results of SCF function is explained in section 6.4.

The Fig.4 represents the average detection latency of the Intense Explore Algorithm. As the number of SUs increases the detection latency of the algorithm will increase.

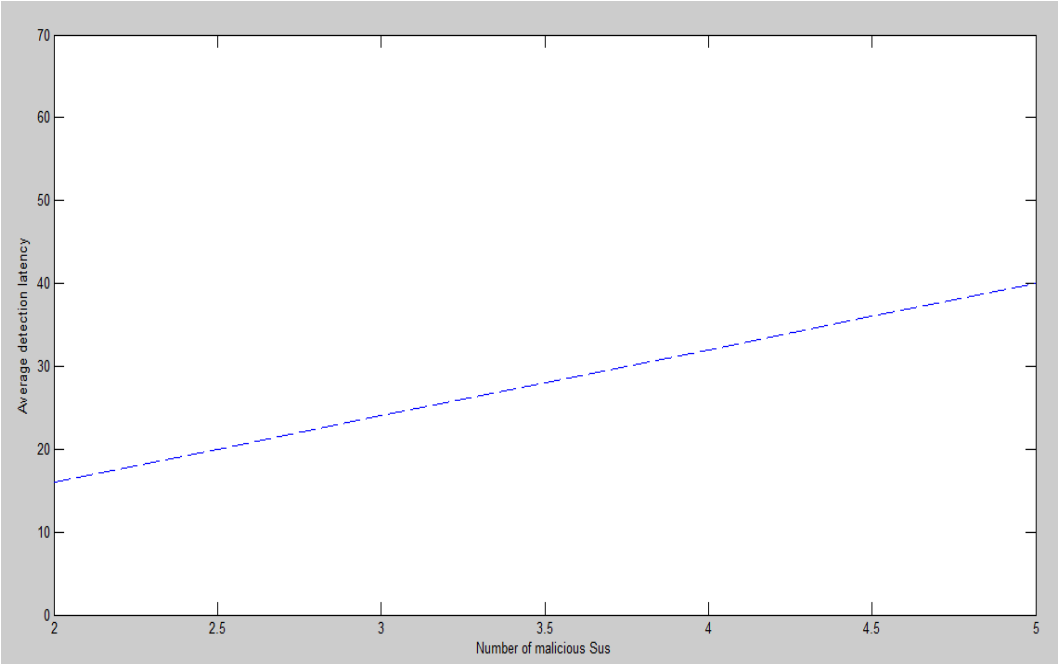

Fig.4. Average detection latency with the number malicious SUs.

6.4 Energy detection

The cooperative SUs in At senses their neighboring SUs in Bt using the spectral correlation function (SCF). The Fig.5 shows the SCF plot of suspected secondary signal. The SCF plots the normalized correlation between the two frequencies f and α against the magnitude of the signal. The peaks represent the spectral lines, which contains finite- strength additive sine wave components with frequencyα. The peak at the center identify the modulation scheme used is DQPSK and number of peaks notify whether the signal is from a suspected or normal secondary user. By setting the magnitude of the signal (Sx) as the threshold value, the number of peaks found to be eight; this clearly shows that this is the suspected secondary user signal. The suspected result of respective Bj will be reported by sensing cooperative SUs in At to Fusion centre, which then decides upon Bj as suspected SU and alerts the all other Secondary Users in network.

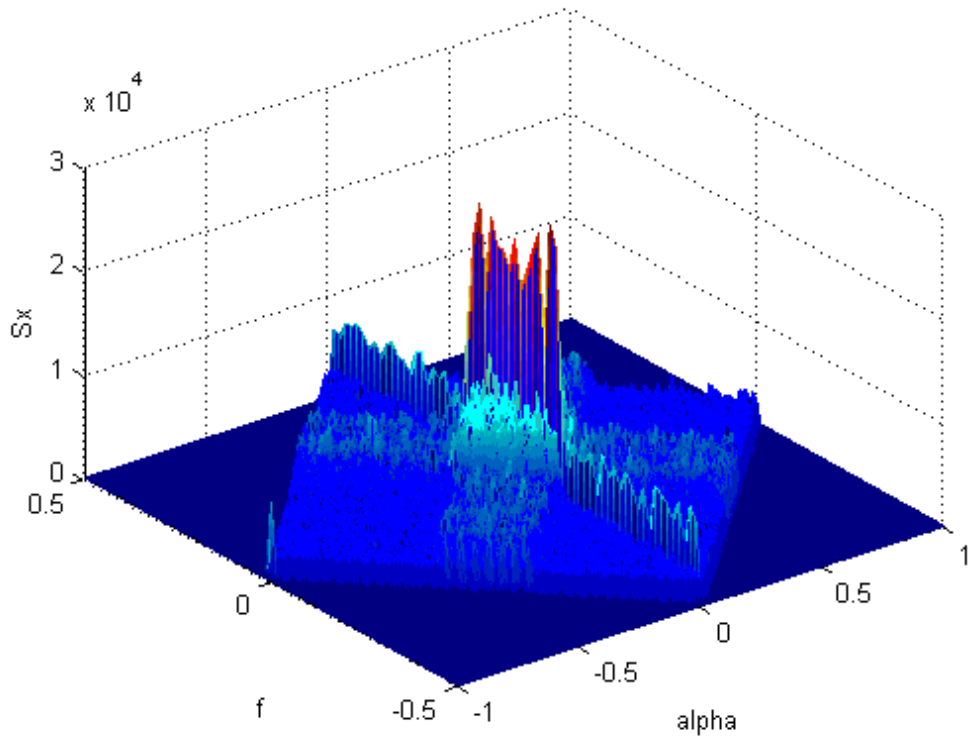

Fig.5 SCF plot of Malicious user signal at fc2 = 257 MHZ, α = 0 Hz and Sx = 0.5 Hz

6.3 Comparison Tests

The Fig 6 represents the throughput loss rate in Intense explore method compared with other methods such as Blind Spectrum and IS3. It can be seen that Intense

explore method produces less throughput loss rate when compared to Blind spectrum and IS3.

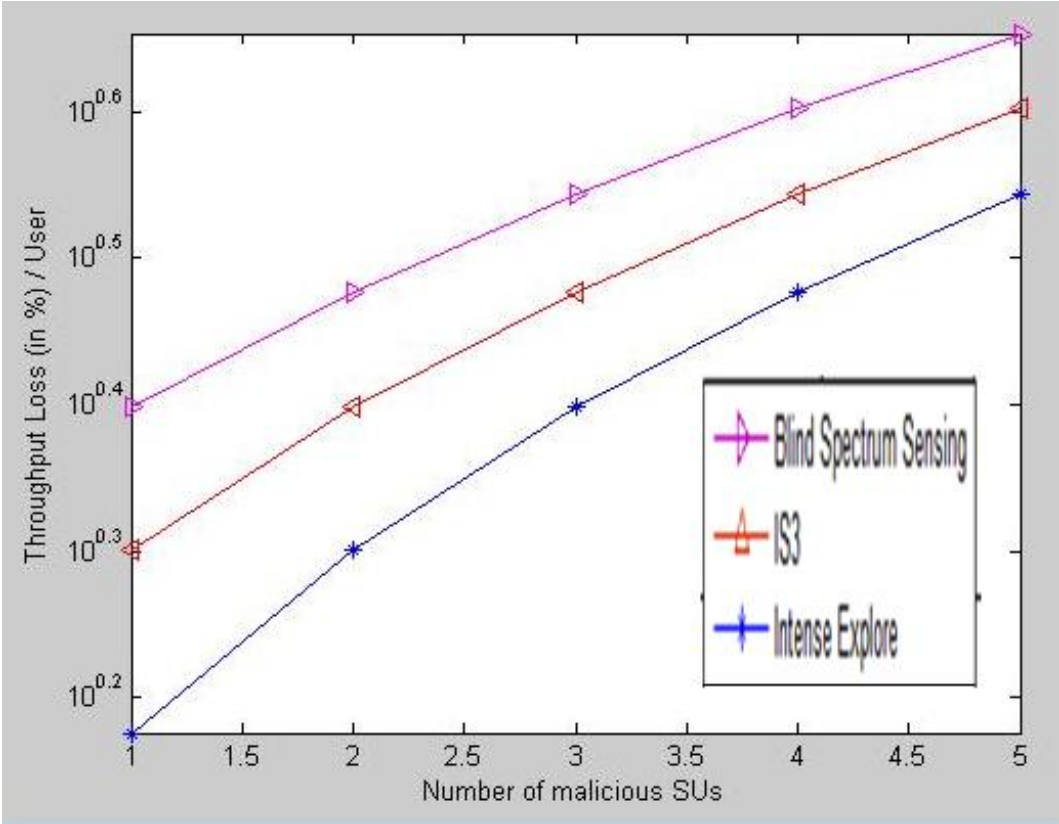

Fig 6. Comparison results of throughput loss with variations in number of malicious SUs.

The Fig 7 represents the detection accuracy in Intense explore method compared with the same two methods Blind Spectrum and IS3. It can be witnessed that detection accuracy is high in Intense Explore method when compared to Blind spectrum and IS3.

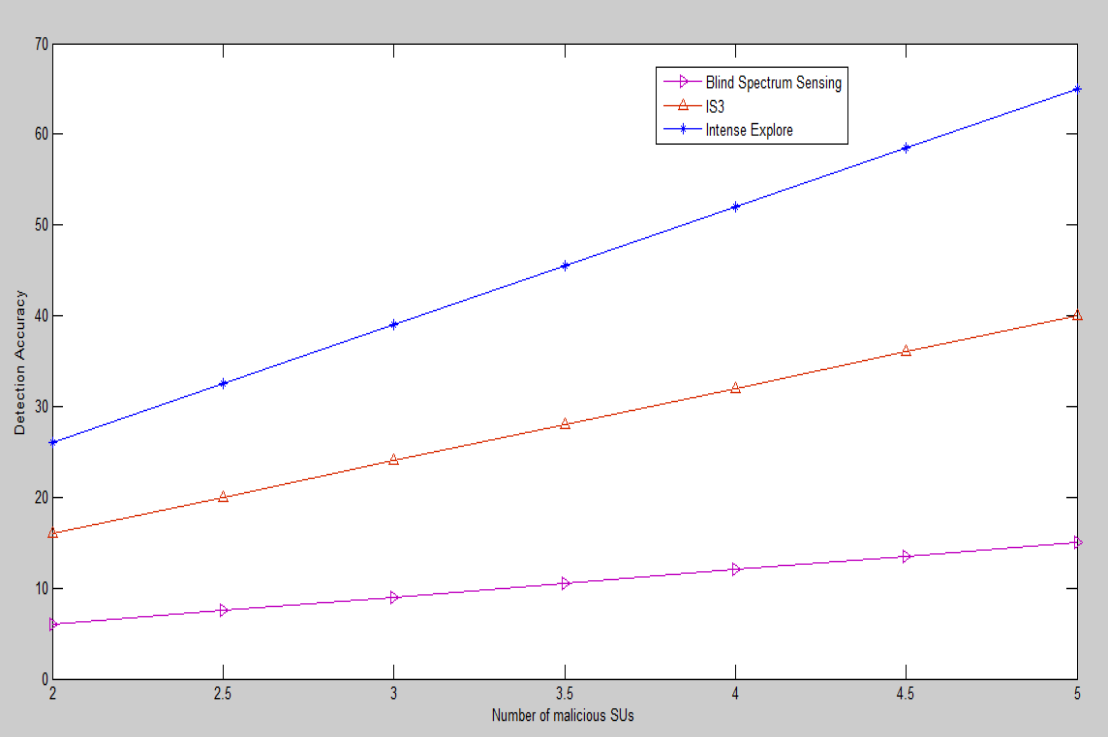

Fig 7. Comparison results of detection accuracy

7. CONCLUSION AND FUTURE WORK

We have discussed about the threats in all protocol layers of cognitive radio networks. The physical layer attack namely PUEA and its various detection methods are also presented. Mitigation of PUE attack is considered in this paper through our novel approach, Intense Explore algorithm. This algorithm proactively identifies the suspected malicious Secondary user. The simulation results prove the algorithm is robust. The throughput loss and detection latency can be minimized for about 65%. Comparisons with existing methods Blind spectrum and IS3 also proves that our proposed algorithm achieves better results. In our future work, we will improve the accuracy of detecting malicious user by acquiring their signal activity patterns.

References:

[1] Deepa Das, Susmita Das, "Primary User Emulation Attack in Cognitive Radio Networks: A Survey", IRACST, Vol.3, No3, June 2013.

[2] Carl R. Stevenson, Gerald Chouinard, "IEEE 802.22: The First Cognitive Radio Wireless Regional Area Network Standard", IEEE Communications Magazine, January 2009.

[3] M. T. Mushtaq, M. S. Khan, M. R. Naqvi, R. D. Khan, M. A. Khan, Prof. Dr. Otto F. Koudelka," Cognitive Radios and Cognitive Networks: A short Introduction", J. Basic. Appl. Sci. Res., 3(8)56-65, 2013.

[4] Abhilasha Singh, Anita Sharma," A Survey of Various Defense Techniques to Detect Primary User Emulation Attacks", International Journal of Current Engineering and Technology, Vol.4, No.2 ,April 2014.

[5] Shaxun Chen, Kai Ceng, and Prasant Mohapatra,"Hearing is believing: detecting wireless microphone emulation attacks in white space", IEEE transactions on mobile computing, Vol. 12, No. 3, March 2013.

[6] Elena Romero, Alexandre Mouradian," Simulation Framework for Security Threats in Cognitive Radio Networks", vol., no., pp. 1--7, 15--17 May 2009.

[7] 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 on , vol., no., pp.110,119, 25-25 Sept. 2006.

[8] Caidan Zhao; Wumei Wang; Lianfen Huang; Yan Yao, "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio," Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on , vol., no., pp.1,5, 24- 26 Sept. 2009.

[9] Caidan Zhao; Liang Xie; Xueyuan Jiang; Lianfen Huang; Yan Yao, "A PHY-layer Authentication Approach for Transmitter Identification in Cognitive Radio Networks," Communications and Mobile Computing (CMC), 2010 International Conference on , vol.2, no., pp.154,158, 12- 14 April 2010.

[10] Zhou, Xiao; Xiao, Yang; Li, Yuanyuan, "Encryption and displacement based scheme of defense against Primary User Emulation Attack," Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on , vol., no., pp.44,49, 27-30 Nov. 2011.

[11] Yi Tan; Kai Hong; Sengupta, S.; Subbalakshmi, K. P., "Using Sybil Identities for Primary User Emulation and Byzantine Attacks in DSA Networks," Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , vol., no., pp.1,5, 5-9 Dec. 2011.

[12] Chandrashekar, S.; Lazos, L., "A Primary User authentication system for mobile cognitive radio networks," Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on , vol., no., pp.1,5, 7-10 Nov. 2010.

[13] Zhou Yuan; Niyato, D.; Husheng Li; Ju Bin Song; Zhu Han, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," Selected Areas in Communications, IEEE Journal on , vol.30, no.10, pp.1850,1860, November 2012.

[14] Zhou, Xiao; Xiao, Yang; Li, Yuan yuan, "Encryption and displacement based scheme of defense against Primary User Emulation Attack," Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on , vol., no., pp.44,49, 27-30 Nov. 2011.

[15] Sanket S. Kalamkar and Adrish Ananya Roychowdhury,"Malicious user suppression for cooperative spectrum sensing in cognitive radio networks

using Dixon's outlier detection method", ",Proc,IEEE Conf on Communications, 2012, , Page(s): 1-5.

[16] Ian F.Akyildiz, Brandon F.Lo *, Ravikumar Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey", Iournal Physical Communication, Volume 4 Issue 1, March, 2011 Pages 40-62.

[17] Tarun Bansal, Bo Chen and Prasun Sinha, "FastProbe: Malicious User Detection in Cognitive Radio Networks Through Active Transmissions", INFOCOM, May 2014.

[18] Gardner, W.A. ,"An Introduction to Cyclostationary Signals, Chapter 1,Cyclostationarity in Communications and Signal Processing", IEEEPress,Piscataway,NJ,1993.

Biographical Sketch

Author 1 :

A.C.Sumathi received her Bachelor's degree in Computer Technology in 1997 and her Master's in Computer Applications in 2000. In 2005, she did another Master's in Computer Science Engineering in 2005. From June 2000 to till date, she worked in leading Engineering colleges in Tamilnadu, India. She is currently working as a Associate Professor in SNS College of Engineering, Coimbatore. She is currently a Part-time PhD student in Anna University, Chennai. Her research interests include Security in Cognitive radio networks, denial-of-service attacks, wireless security, and Spectrum utilization of cognitive radio networks. She is an member of IEEE,ISTE & IET. Email id: sumathi.ac@gmail.com

Author 2:

Dr R. Vidhyapriya obtained her Bachelor's Degree in Electrical and Electronics Engineering her Master's Degree in Applied Electronics from PSG College of Technology (Bharathiar University), Coimbatore. She did her doctoral research in the area of Energy Efficient Routing in Wireless Sensor Networks. Presently she is working as a Professor in the Department of Information Technology, PSG College of Technology, and Coimbatore. She has around 15 years of teaching experience. Her research interests include energy optimization in heterogeneous wireless networks, location identification and data compression. She has published several papers in National and International Journals. E-mail: vidhyar@mail.psgtech.ac.in