ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Detection of Malicious Secondary User Using Spectral Correlation Technique in Cognitive Radio Network

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

[1]*Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, India*
[2]*Department of Information Technology, PSG College of Technology, Coimbatore, Tamil Nadu, India*

ARTICLE INFO

Article history:
Received 12 November 2014
Received in revised form 26 December 2014
Accepted 29 January 2015
Available online 10 February 2015

Keywords:
Cognitive Radio Technology, Spectrum, Television Broadcast Services, Primary User Emulation Attack, Cyclo-stationary Detector.

ABSTRACT

Cognitive radio technology is seen as a potential solution to the efficient utilization of available spectrum by the unlicensed legitimate users. The development of the IEEE 802.22 WRAN standard is aimed at using cognitive radio techniques to allow sharing of unused spectrum allocated to the television broadcast service on a non-interfering basis to bring broadband access to rural environment and during the emergency period. Due to open nature of CRN and lack of proactive security protocols, IEEE 802.22 networks are vulnerable to Denial-of-Service attack known as Primary User Emulation Attacks (PUEA). The main objective of this paper is to distinguish the primary user signals from secondary user signals by investigating the use of cyclo-stationary detection and its simulation in MATLAB. Cyclo-stationary detector enables operation under low SNR conditions. Simulation results show that implementing spectral correlation detection technique help in better performance in terms of detection.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: A.C. Sumathi and Dr.R. Vidhyapriya, Detection of Malicious Secondary User Using Spectral Correlation Technique in Cognitive Radio Network. ***Aust. J. Basic & Appl. Sci.,*** *9(5): 185-191, 2015*

INTRODUCTION

A. Background:

The electromagnetic radio spectrum is a natural resource and hence, for the proper utilization of the same is licensed by the Government. The necessity of effective utilization of wireless spectrum in view of ever increasing demands by emerging wireless applications have led the Federal Communications Commission (FCC) to revisit the problem for proper management. A spectrum hole is a band of frequencies assigned to a primary user, but, at a particular time and specific geographic location, the band is not being utilized by that user. The FCC is considering opening up such licensed bands to unlicensed user for the operations on a without-interference basis to licensed users otherwise known as Primary users (PU). The unlicensed users or Secondary users (SU) “opportunistically” operate in fallow licensed spectrum bands without interfering with licensed users, thereby increasing the efficiency of spectrum utilization (Haykin, 2005). This method of sharing is often called Dynamic Spectrum Access (DSA). The goal of DSA is expected to be achieved via innovative emerged technology called Cognitive radios. Cognitive radio network is emerging as a prominent solution to improve the efficiency of spectrum usage to meet the increasing user demands on broadband wireless communication.

B. Cognitive Radio Network:

The cognitive radio concept dates back to 1998 when the idea was first conceived by Sir Joseph Mitola III at the Royal Institute of Technology in Stockholm. Cognitive radio is an intelligent wireless communication system also known as Software defined radio (Haykin S., 2005; Clancy, 2008) that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters such as transmit-power, carrier-frequency, and modulation strategy. Haykin also proposes three cognitive tasks such as radio scene analysis, Channel identification and transmit power control with dynamic spectrum management. The above three tasks forms a cognitive cycle later developed as cognitive radio network with the transceiver called cognitive radio (Stevenson, 2009).

The cognitive radio presents a very lucrative area of the research field. Inefficient spectrum utilization is the driving force behind cognitive radio

Corresponding Author: A.C. Sumathi, Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, India.
E-mail: sumathiac2@gmail.com

and adopting it can lead to a reduction of spectrum scarcity and better utilization of the spectrum resources. Spectrum Sensing i.e. checking the frequency spectrum for empty bands forms the foremost part of the cognitive radio. There are number of schemes for spectrum sensing like energy detector and matched filter. But the former functions properly for higher signal to noise ratio (SNR) value whereas the latter's complexity is very high. These constraints led to implementing a detector which performed well under low SNR conditions as well and with complexity not as high as the matched filter. Cyclo-stationary detector turned out to be the choice for such specifications.

The Cognitive Radio enabled IEEE 802.22 Wireless Regional Area Network (WRAN) is designed to opportunistically utilize the unused or under-utilized TV bands (54 – 864Mhz). Cognitive radio is a promising technology which observes its environment and modifies its transmission characteristics accordingly. Cognitive Radio Networks (CRN) is composed of smart devices which can sense and identify "white spaces"—or vacant areas—in the spectrum. CR enables the unlicensed (Secondary) users to coexist with incumbent (primary) users in licensed spectrum bands while causing no interference to incumbent communications.

C. IEEE 802.22 Standard:

The development of the IEEE 802.22 WRAN standard (Stevenson, 2009) (802.22 or 802.22 WRAN herein) is aimed at using cognitive radio techniques to allow sharing of geographically unused spectrum allocated to the television broadcast service, on a non-interfering basis. The standard aims at bringing broadband access to low populated or rural areas where lying of separate wireless network might be worthless. It is designed to operate in the TV broadcast bands like digital TV, analog TV broadcasting and also low power licensed devices such as wireless microphones. The application for the IEEE 802.22 WRAN standard will be providing wireless broadband access to a rural area of typically 17–30 km or more in radius (up to a maximum of 100 km) from a base station (BS) and serving up to 255 fixed units of customer premises equipment (CPE) with outdoor directional antennas located at nominally 10 m above ground level, similar to a typical VHF/UHF TV receiving installation.

C1. Physical Layer:

According to paper [3], IEEE 802.22 defines a single air interface based on 2048-carrier orthogonal frequency-division multiple access (OFDMA) to provide a reliable end to end link suitable for NLOS operation. Also IEEE 802.22 initially defines single time domain duplex (TDD) mode and provides an opportunity to enhance to frequency-division duplex (FDD). Various common TV channel bandwidths such as 6,7, and 8Mhz channels will utilize the channel bandwidth by scaling the sampling frequency, carrier spacing, symbol duration, signal bandwidth and data rates. WRAN systems use a common oversampling factor and the same frame/symbol structure, coding schemes, interleaving and so on. The physical layer parameters for WRAN can be tabulated as in table 1.

Table 1: Physical layer parameters of IEEE 802.22

Parameters	Specifications
Frequency range	54-862 MHz
Channel bandwidth	6,7,or 8 MHz
Data rate	4.54 to 22.69 Mbps
Spectral Efficiency	0.76 to 3.78 bits (s.Hz)
Payload Modification	QPSK, 16-QAM, 64-QAM
Multiple Access	OFDMA
FFT Size	2048
Cyclic Prefix Mode	1/4 ,1/8, 1/16, 1/32
Duplex	TDD
Coding	Block Convolution Code

The paper [3] states modulations such as quaternary phase shift keying (QPSK), 16-quadrature amplitude modulation (QAM), 64-QAM and four coding rates for data communications depending on data rate, robustness, and channel and interference condition.

C2. MAC Layer:

The IEEE802.22 MAC (Clancy, 2008) employs a super frame structure for data communication and to facilitate numerous cognitive functions for licensed user protection, WRAN synchronization and self-coexistence. The cognitive functions are done by spectrum manager, geo-location, database and spectrum sensing. The spectrum manager resides at BS (Base Station) and get inputs from spectrum sensing function, geo-location and database for channel utilization on TV band. According to IEEE 802.22 all devices in the network must be installed in a fixed location and equipped with satellite-based geo-location technology such as GPS, Galileo etc. Also the Base stations must have the access to the database service which provides the accurate and up-to- date information about the broadcast operation in the specified area.

Table 2: Modulation and Coding rate for IEEE 802.22.

PHY mode	Modulation	Coding rate	Peak data rate in 6MHz (Mb/s)	Spectral efficiency (BW = 6MHz)
1	BPSK	Uncoded	4.54	0.76
2	QPSK	½ and repeat 3	1.51	0.25
3	QPSK	1/2	4.54	0.76
4	QPSK	2/3	6.05	1.01
5	QPSK	3/4	6.81	1.13
6	QPSK	5/6	7.56	1.26
7	16-QAM	1/2	9.08	1.51
8	16-QAM	2/3	12.10	2.02
9	16-QAM	3/4	13.61	2.27
10	16-QAM	5/6	15.13	2.52
11	64-QAM	1/2	13.61	2.27
12	64-QAM	2/3	18.15	3.03
13	64-QAM	3/4	20.42	3.40
14	64-QAM	5/6	22.69	3.78

D. Cognitive Functions:

In order to operate in TV broadcast bands without affecting digital TV, analog TV, and licensed wireless microphones operated by TV broadcasters and other eligible licensees, 802.22 systems will have to be cognizant of all incumbent operations in their vicinity. The necessary tools are being included in the standard to fulfill these cognitive functions. First, the location of each BS and CPE unit will be accurately established. This is described in detail in the geolocation section below. The second tool is access to a channel availability database that will provide reliable information on channel availability for WRAN use at any given location. The third tool is the sensing capability included in the standard to sense the presence and identify the type of incumbent signals in channels of interest. These capabilities will, by allowing the BS to control channel usage and CPE maximum EIRP, constitute the set of cognitive functions needed to allow operation of 802.22 systems in the TV broadcast bands on a noninterference basis with the incumbents.

Denial of service:

A. Primary User Emulation Attack:

In recent years, the security issues of the cognitive radio (CR) networks have drawn a lot of research attentions. Primary user emulation attack (PUEA), as one of common attacks, compromises the spectrum sensing, where a malicious user forestalls vacant channels by impersonating the primary user to prevent other secondary users from accessing the idle frequency bands. The cognitive radio enabled IEEE 802.22 wireless regional area network (WRAN) is designed to opportunistically utilize the unused or under-utilized TV bands. However, due to the open nature of cognitive radio networks and lack of proactive security protocols, the IEEE 802.22 networks are vulnerable to various denial-of-service (DoS) threats.

The IEEE 802.22 is an emerging standard for CR-based wireless regional area networks (WRANs). The IEEE 802.22 standard aims at using DSA to allow the unused, licensed TV frequency spectrum to be used by unlicensed users on a non-interfering basis (Stevenson, 2009). To protect the primary incumbent services, IEEE 802.22 devices (e.g., base station and consumer premise equipment) are required to perform periodic spectrum sensing and evacuate promptly upon the return of the licensed users [3]. Even though primary user protection mechanisms have been specified, neither the secondary-secondary interaction mechanisms nor the protection of secondary devices/networks have been specifically addressed in IEEE 802.22 standard (Bian, 2008). Hence, the IEEE 802.22 networks are vulnerable to denial of-service (DoS) attacks, where the attacker prevents the secondary networks from using the spectrum band effectively or at all. Several security aspects of CR networks have been investigated (Clancy, 2008), (Chen, 2008). However, most of these either deal with single malicious node or uncoordinated attacks by multiple malicious nodes, or are not specific to IEEE 802.22.

As far as the security is concerned, the intrinsic properties of CR networks pose new challenges to wireless communications. To date, there have been several research literatures studying the security issues of CR networks.

Spectrum sensing techniques:

A. Concept of Basic Hypothesis:

The spectrum sensor essentially performs a binary hypothesis test on whether or not there are primary signals in a particular channel. The channel is idle under the null hypothesis and busy under the alternate:

H0 (idle) vs. H1 (busy)

Under the idle scenario, the received signal is essentially the ambient noise in the RF environment, and under the busy scenario, the received signal would consist of the PU signal and the ambient noise. Thus, this yields the following mathematical representation,

$H0: y(k) = w(k)$

$H1: y(k) = s(k) + w(k)$

For k = 1, .., n, where n is the number of received samples,

w(k) represents ambient noise,

s(k) represents the PU signal.

B. *Energy Detector:*

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.

$$E = \int_{-\infty}^{\infty} |x|^2 dt < \infty$$

The underlying assumption is that with the presence of a signal in the channel, there would be significantly more energy than if there was no signal present. Therefore, energy detection involves the application of a threshold in the frequency domain, which is used to decide whether a transmission is present a specific frequency. The block diagram of a cognitive radio network for energy detection is shown in Fig. 1. A power spectrum describes an energy distribution of a time series in the frequency domain. Statistical spectral estimation methods are classified as parametric methods, nonparametric methods and subspace methods.

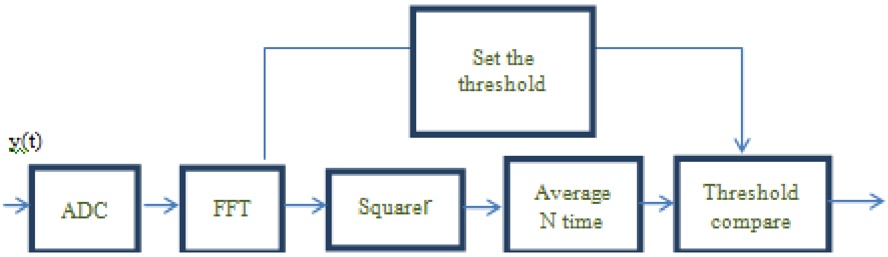

Fig. 1: Block diagram of Energy detection in CRN.

C. *Matched Filtering:*

The few known transmission properties of possible primary users, such as transmission bandwidths and center frequencies, signal types, duplexing and multiple accessing methods of potential users are used to develop a partial match filtering method. In this method, the cognitive radio parameters estimated from the received signal are matched to the possible transmission parameters for achieving a more robust and reliable sensing. The output of the partial matched filtering is used for making decisions on the presence of an anticipated transmission. It also gains knowledge on complete multi-dimensional spectrum awareness in cognitive radio network.

D. *Bayesian Compressive Sensing Technique:*

Primary User signals can be directly estimated from the compressed measurements. The Bayesian Compressive Sensing (BCS) framework is used to reduce the computational complexity. The main advantage of this technique is the elimination of reconstruction work by the cognitive radio. The Multi-Resolution Bayesian Compressive Sensing provides an iterative optimization strategy to acquire the minimum number of samples in a dynamic sparsity model without any prior assumptions.

Proposed method:

In this paper, a Cognitive radio network environment is simulated. Five channels have been used to transmit either primary or secondary signals. Different scenarios of Primary and secondary signals transmissions are done and they are shown in the simulation snapshots. Primary user emulation attack is simulated by generating malicious secondary user signals, which mimic with the energy level of primary signal. The malicious secondary signal is identified using SCF function. The detailed description of SCF functionality and its detection method is given in the following section.

The threshold set by SCF is compared to differentiate between legitimate primary user and malicious secondary user. If the result identifies it as a primary user, the slot is vacated and allotted to the primary user signal, else if it is a malicious attack, the slot is not vacated and secondary user will continue with their data transfer.

A. *Cyclostationary Feature Detection:*

A cyclostationary process has statistical properties that vary periodically over time. Cyclostationary feature detection method [4] deals with the inherent cyclostationary properties or features of the signal. Such features have a periodic statistics and spectral correlation that cannot be found in any interference signal or stationary noise. It exploits this periodicity in the received primary signal to identify the presence of primary users, and that is why the cyclostationary feature detection method possesses higher noise immunity than any other spectrum sensing method. In this method, the cyclic spectral correlation function (or SCF) is the parameter that is used for detecting the primary user signals.

Cyclostationary spectrum sensing method performs better in low SNR regions, because of its noise rejection capability. This occurs because noise is totally random and does not exhibit any periodic form of behavior. When we have no prior knowledge about primary user’s waveform, which is the scenario in real life, the best technique to be adopted is cyclostationary feature detection. As an advantage, the cyclostationary method can be used to find out the type of modulation scheme used by the primary user signal.

B. *Spectral Correlation Function:*

Two-dimensional spectral correlation is the way to extract the periodic features of the primary user signal. These signals are cyclostationary processes that are periodic in time t. They also possess a periodic autocorrelation function.

$$R_X(t,\tau) = R_X(t+T_0,\tau)$$

The Fourier transform of the autocorrelation function is given as follows,

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

$R_X^{\alpha}(\tau)$ In the above equation, α is the fundamental cyclic frequency and is the cyclic auto-correlation function. Fourier transform of the CA function is defined as the cyclic spectral density (CSD) function.

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

It was proved in [8] that the cyclic spectral density function could be measured by the normalized correlation between two spectral components of x(t) at frequencies (f +α/2) and (f-α/2) over an interval of length Δt.

$$S_X^{\alpha}(f) = \lim_{\Delta t\to\infty} \lim_{T\to\infty} \frac{1}{\Delta t}\frac{1}{T} \int_{-\Delta t/2}^{\Delta t/2} X_T(t, f+\frac{\alpha}{2})X_T^*(t, f-\frac{\alpha}{2})dt$$

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. We can accomplish the detection task by searching the unique cyclic frequency of different modulated signals. Also, information such as the carrier frequency, chip rate could be calculated according to the unique cyclic frequencies. Another motivation of implementing the spectral correlation function for signal detection lies on its robustness to random noise and interference.

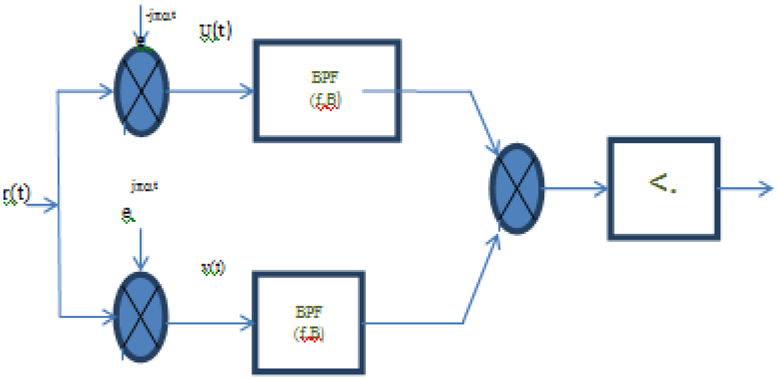

Fig. 2: Spectral Correlation Function Generator.

The Fig. 2 shows the spectral correlation generator. When SCF is plotted, the occupancy status of the spectrum can be found out. If a primary user 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 there is no primary user signal present in the concerned frequency range. In addition to this, the SCF can be used to find out the type of modulation scheme used by the primary user signal. This can be achieved by counting the number of secondary peaks at the double frequencies.

The signals which are used in several applications are generally coupled with sinusoid carriers, cyclic prefix, spreading codes, pulse trains etc. which result in periodicity of their statistics like mean and auto-correlation. Such periodicities can be easily highlighted when cyclic spectral density (CSD) for such signals is found out.

Primary user signals which have these periodicities can be easily detected by taking their correlation which tends to enhance their similarity. Fourier transform of the correlated signal results in peaks at frequencies which are specific to a signal and searching for these peaks helps in determining the presence of the primary user. Noise is random in nature and as such there are no such periodicities in it and thus it doesn’t get highlighted on taking the correlation.

Cognitive radio network environment simulation results:

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 3 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.

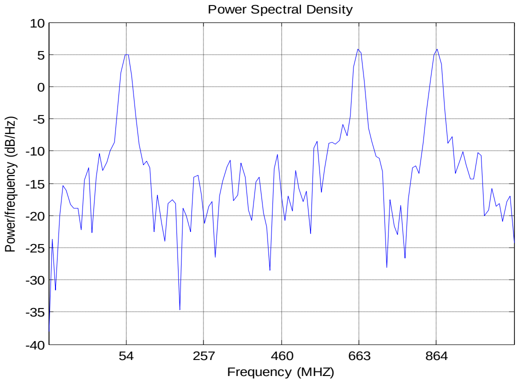

Fig. 3: Periodiogram Graph of CRN with 3 primary users, Frequency range 54-864 MHZ, Power level – 5dB

In Fig. 4, two secondary users are allotted in the two free channels at the frequencies 257 MHZ and 450 MHZ. Also the periodiogram graph clearly shows that the RSS of the primary user signals is more when compared with the secondary user signals. In this cognitive radio network, there are three primary users and two secondary users, implies all the five channels are occupied.

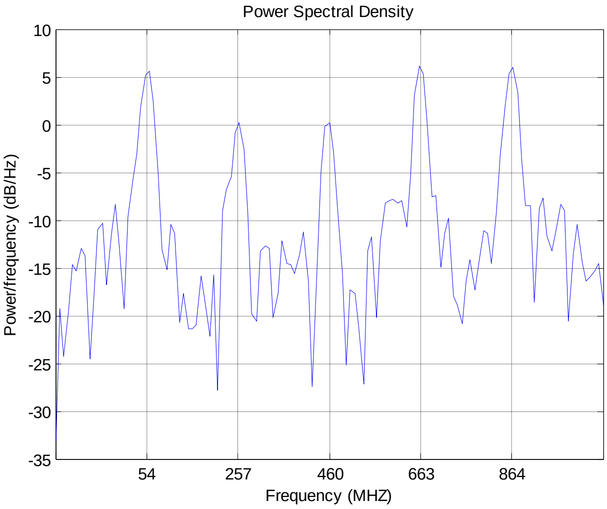

Fig. 4: Periodiogram Graph of CRN with 3 primary users and 2 secondary users, Frequency range 54-864 MHZ

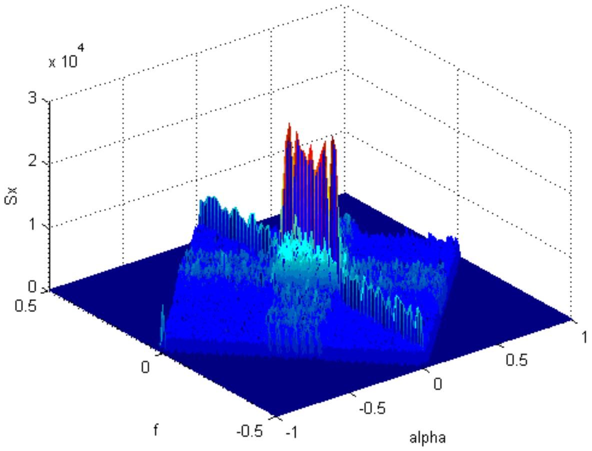

Fig. 5: SCF plot of primary user signal at fc1=54 MHZ, α = 0 Hz and Sx = 0.5 Hz.

The Fig. 5 shows the spectral correlation function plot of primary user 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 frequency α. The peak at the center identify the modulation scheme used is DQPSK and number of peaks notify whether the signal is from a primary user or a malicious 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 primary user signal.

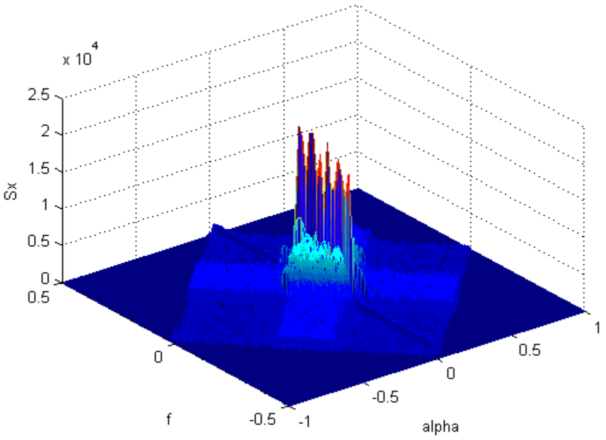

Fig. 6: SCF plot of Malicious user signal at fc2 = 257 MHZ, α = 0 Hz and Sx = 0.5 Hz

The Fig. 6 shows the spectral correlation function plot using DQPSK modulation scheme of malicious user signals. At the center α =0, the number of peaks are only 3, which is less compared to that of the primary user signal, it is identified as malicious user signal.

Conclusion and future work:

Our main objective of this paper is to distinguish the primary user signals from secondary user signals in Cognitive Radio enabled IEEE 802.22 Wireless Regional Area Nettwork(WRAN). It has been accomplished by simulating the CRN environment in MATLAB. The investigation was done using cyclo-stationary detection. The Cyclo-stationary detector enables operation under low SNR conditions. Simulation results show that implementing spectral correlation detection technique helps to efficiently distinguish primary signal from malicious. SCD of white noise shows no spectral correlation density, which provides an easy method of channel sensing and spectrum allocation.

In this paper, DQPSK modulation scheme is used as a single parameter to simulate Primary signal. In future, different parameters can be used to simulate the cognitive radio network environment and the primary user emulation attack will be addressed more effectively.

REFERENCES

Bian, K. and J.M.J. Park, 2008. Security vulnerabilities in IEEE 802.22. WICON ’08: Proceedings of the 4th Annual International Conference on Wireless Internet, pp: 1–9.

Chen, R., 2008. Defense against primary user emulation attacks in cognitive radio networks. IEEE J. Sel. Areas Commun, 26(1): 25–37.

Clancy, T. and N. Goergen, 2008. Security in cognitive radio networks: Threats and mitigation. Cognitive Radio Oriented Wireless Networks and Communications, 2008. Crown Com 2008. 3rd International Conferenceon, pp: 1–8.

Clancy, T.C. and N. Goergen, 2008. Security in Cognitive Radio Networks :Threats and Mitigation. International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Crown Com.

Gardner, W.A., 1993. An Introduction to Cyclostationary Signals, Chapter 1,Cyclostationarity in Communications and Signal Processing. IEEE Press, Piscataway, NJ.

Haykin S., 2005. Cognitive radio: brain-empowered wireless communications. IEEE J. Select. Areas Communication, 23(2): 201–220.

Stevenson, C., 2009. IEEE 802.22: The first cognitive radio wireless regional area network standard. IEEE Communication magazine, 47(1): 130–138.