ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(33), DOI: 10.17485/ijst/2016/v9i33/65159, September 2016* ISSN (Online) : 0974-5645

Cancellation of Interference and Malicious User in Cognitive Radio

J. Avila* and K. Thenmozhi

Department of ECE, School of EEE, SASTRA University, Thirumalaisamudram, Thanjavur – 613401,Tamil Nadu, India; avilaprem@gmail.com, thenmozhik@ece.sastra.edu

Abstract

Background: Cognitive Radio Networks (CRN), one of the emerging technologies in the wireless communication domain, is primarily used for spectrum sensing and proper allocation of the unused licensed bands to the Secondary Users (SU) without producing any intervention to the Primary user (PU) in a dynamic manner. However, security to the physical layer becomes a major problem here. Security pressures in a cognitive radio network are taken into consideration. **Method:** The performance of the Primary User Emulation Attack (PUEA) from the Neyman-Pearson criterion's perspective has been analysed. In addition, the work also proposes an enhanced interference elimination method to diminish the interference between the cognitive users and others operating in the same wireless environment. **Result:** The results are plotted using MATLAB. Simulation results show improved interference cancellation between the cognitive user and primary user. **Application:** Data transfer to remote places utilizing the spectrum that remains idle or underutilized.

Keywords: Cognitive Radio, Enhanced Interference Cancellation, Neyman-Pearson Criterion, PUEA

1. Introduction

Spectrum demand has become a significant matter of concern because of the utilization of wireless systems. Nonetheless, it has been extensively surveyed that not all frequency bands are being utilized to the fullest. The Federal Communications Commission (FCC), after an exhaustive survey, has mandated that some bands are over -crowded while others are highly and inefficiently utilized[1]. Thus, an optimum solution to overcome the spectrum crisis would be to completely utilize the unused components of the spectrum. An instance of this scenario is IEEE 802.22, which proposed the reutilization of television bands without creating any interference to the TV receivers[2].

Cognitive radio (CR) is the best fit in regard to spectrum efficient utilization[3,4]. While a cognitive radio network can have its indigenous operating frequency, it detects spectral holes, which are also called white spaces, in frequency bands of the primary network and utilizes them. In addition it can also adjust its operating parameters such as the power of the transmitter and the scheme employed in modulation with respect to the variation in a real time scenario[5,6]. This feature enhances performance and provides a better Quality of Service (QoS).

Security issues in a cognitive system have become a matter of serious concern[7,8]. The primary goal of the security system is to prevent the masquerading of malicious users as primary users[9,10]. Primary users are those who have the right to use the frequency spectrum band[11]. While unlicensed/Secondary users are defined as users who can utilize the band when it is not used by primary users while ensuring no interference to them[12,13]. In cognitive radio networks, an attack is a phenomenon in which the primary user's signal transmission is hindered. In addition to a cognitive user there are person who do not hold any license to use the spectrum, even in the absence of the primary user, and who try to use the spectrum. This results in a loss of spectrum use for the secondary user termed PUEA[14,15].

In addition ,an analytical method to find the

* *Author for correspondence*

probability of a false alarm is proposed to study the performance of the primary user emulation attack and an enhanced active interference cancellation mechanism to combat the interference between the cognitive users and others.

2. Proposed Methodology

2.1 Interference Cancellation Method

The block diagram for interference cancellation is shown in figure 1. QPSK modulation is carried out and the modulated data is grouped. The grouping of subcarriers can be done in three ways

- Adjacent Partition: The sub carriers adjacent to each other are grouped[16,17]
- Interleaved Partition: The alternate sub carriers are grouped.
- Random Partition: The sub carriers are chosen and grouped randomly.

The proposed system uses 128 sub carriers out of which three sub-tones (85, 86 and 87) are assumed to be interfering tones. The sub carriers are grouped into four groups with 32 sub carriers in each. The output produced by the grouping block is then given as the input to the shifting block where two types of shifting are carried out.

The first method exploits the principle of cyclic shifting. Shifting is done in the clockwise direction and this method produces minimum squared error value. A cyclic value is obtained as the result of shifting. This value is used to shift the original data and the shifted data is placed in the data sequence. The order of the tones is also shifted. At the receiver the shifting values have to be known so that the original data can be obtained by shifting back in the anti clockwise direction[18].

In the second method AIC is enriched by phase shift. The phase of the data is used for shifting in the clockwise direction. For retrieving the original data the phase values should be known at the receiver. This method is little complicated because the data symbol has to be multiplied with the phase values at the receiver.

The shifting block's output is then fed as the input to the AIC block. The MIMO AIC algorithm is given by[19,20].

The transmitted signal is written in matrix form as S=pq

Where $p=[p(0)p(1).....p(i-1)]^T$ (1)

$q=[q(0)q(1).....q(s\times i-1)]^T$ (2)

$$S=\begin{bmatrix} S_{11}.....S_{1i} \\ . \\ . \\ . \\ S_{si,1} .....S_{si,i} \end{bmatrix} \quad (3)$$

$$S_{ki}=S(k,l)=\sum_{j=0}^{N-1}\exp(j2\pi\frac{p}{N}(i-\frac{k}{s}))$$

$$c=\arg_c \min\|E_1 c+v_1\|^2 \quad (4)$$

The interference vector is given by

$$v_1=v\left(fr_1+y:f(r_n-1)-(y+2)\right), y\geq 0 \quad (5)$$

The minimization problem is given by

$$\min_x\|S_x-F\|^2 \text{ subject to }:\|G_x-H\|^2<\alpha \quad (6)$$

$$c_{opt}=\arg_c \min\|S_1 c+v_1\|^2$$

Subject to: $\begin{cases} |c_{ET.1}(k)|^2\leq\varepsilon_i; i=1,.....N_{ET}/2 \\ |c_{ET.2}(k)|^2\leq\varepsilon_j; j=1,.....N_{ET}/2 \end{cases}$ (7)

$$c=[c_{ET.1}c_{null}c_{ET.2}]^2 \quad (8)$$

Lagrange optimization algorithm is used to optimize the problem which is given as

$$f(c,\lambda_i,\lambda_j)=\|S_1 c+v_1\|^2+\sum_{i=1}^{N_{ET}/2}\lambda_i(|c_{ET.1}(i)|^2-\varepsilon_i)+\sum_{j=1}^{N_{ET}/2}\lambda_j(|c_{ET.2}(j)|^2-\varepsilon_j) \quad (9)$$

$$(S_1^H S_1+\Lambda)c_{opt}=S_1^H v_1 \quad (10)$$

$$c_{opt}=-(S_1^H S_1+\Lambda)^{-1}S_1^H v_1$$

$$\Lambda=diag[\lambda_1.....\lambda_\alpha 0.....0\lambda_\beta.....\lambda_{N_{tr}}]$$

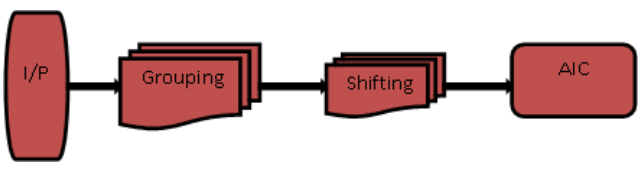


Figure 1. Enhanced Interference Cancellation method.

2.2 Security Issues

Figure 2 shows the flow chart of the steps used to mitigate

the primary user emulation attack. There are more chances for attackers in a cognitive radio network in comparison with traditional wireless networks. This can be attributed to the following issues:

- Sensitivity to primary user signal- should be high to prevent interference caused by the secondary users.
- Primary receiver location-not known by the secondary user, hence, interference is not subject to minimization.

Hence, the main objective is to prevent malicious users from attacking the system. The Neyman Pearson criteriaare as follows.

The decision variable used here is α, where

$$\alpha = \frac{P^{(m)}(x)}{p^{(P_r)}(m)} \quad (11)$$

and $p^{(m)}(x)$ and $p^{(p_r)}(x)$ are the probability distribution function of the power received at the secondary due to malicious and primary user respectively. X is the power of the received signal. λ is threshold value. If α is less than the threshold value primary transmission occus else PUEA occurs.

$\alpha \leq \lambda$: Primary transmission, $\alpha \geq \lambda$: PUE

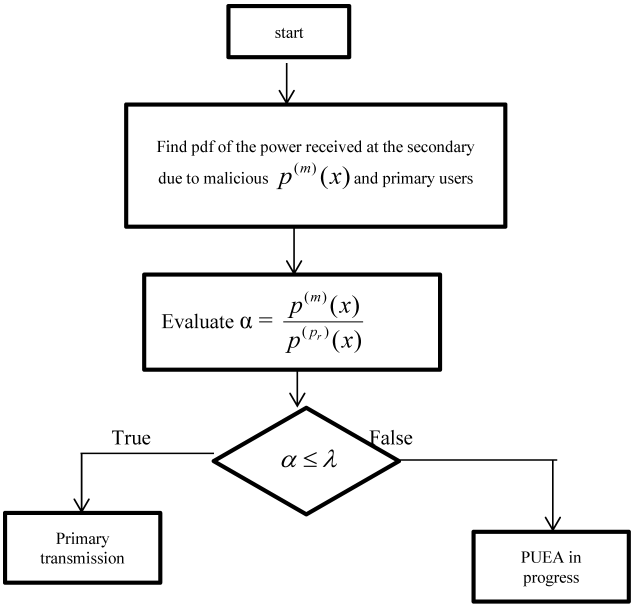
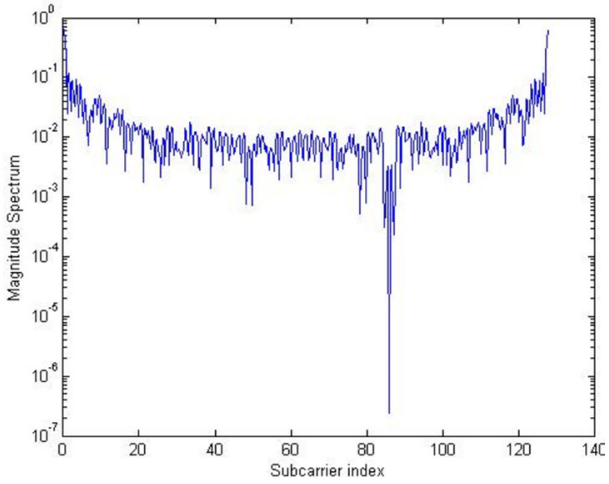


Figure 2. Flow chart of the proposed method.

3. Results and Discussion

Figure 3a shows the Active Interference Cancellation with adjacent partition and cyclic shift. Figure 3b shows the Active Interference Cancellation with adjacent partition and phase shift. From the figure it is clear that cyclic shift case offers better results when compared to the partition with phase shift because it changes the order of the tones and it is assumed that the amount of cyclis shift is known at the receiver. In Phase shift the phase of the tones is altered. When compared, cyclic method minimizes the mean square error.



(a)

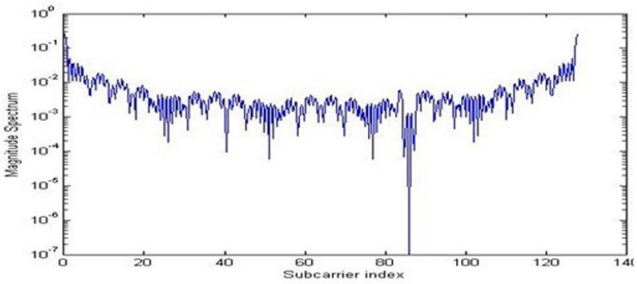
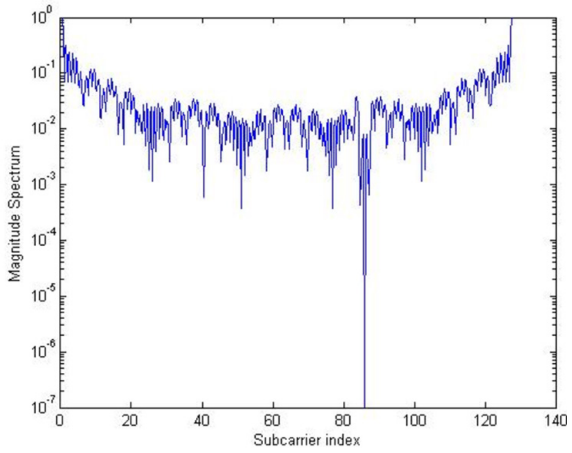


Figure 3. (b)Adjacent partition with cyclic shift and phase.

Figure 4a shows the Active Interference Cancellation with interleaved partition and cyclic shift. Figure 4b shows the Active Interference Cancellation with interleaved partition and phase shift. From the figure it is clear that cyclic shift case offers better results when compared to the partition with phase shift. When compared with the adjacent partition method interleaved partition gives poorer results.



(a)

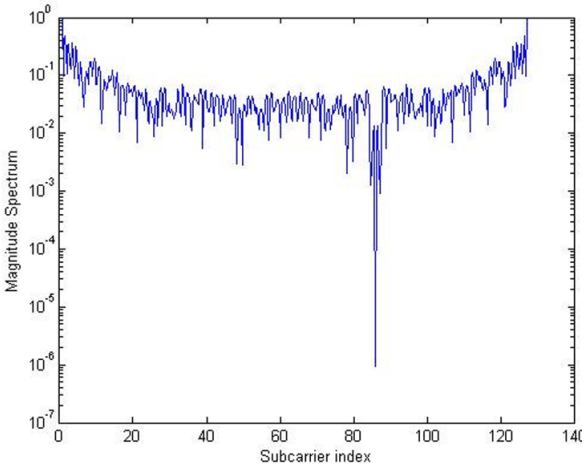
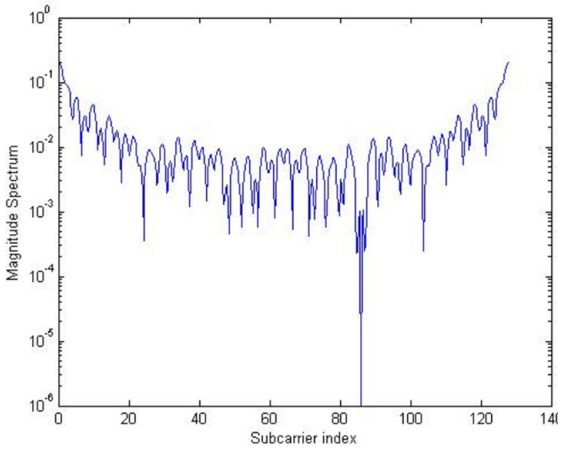


Figure 4. (b) Interleaved partition with cyclic shift and phase shift

Figure 5a shows the Active Interference Cancellation with random partition and cyclic shift. Figure 5b shows the Active Interference Cancellation with random partition and phase shift. Here also cyclic shift case offers better results when compared to the partition with phase shift.When compared with the adjacent partition method interleaved partition gives poorer results. When compared with the first two methods random partition offers good result. In the previous methods the grouping pattern is fixed whereas here care is taken in grouping the subcarriers in such a way that is good scrambilng of datas which in turn outcomes in good notch depth.



(a)

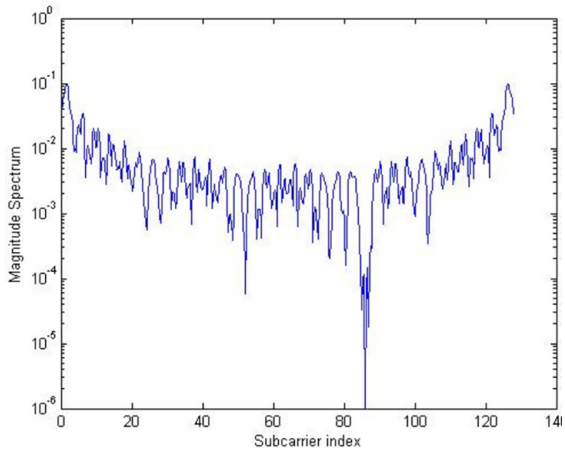


Figure 5. (b) Random partition with cyclic shift and phase shift.

Figure 6 and 7 show the missed detection and false alarm probability respectively. It can be observed that a value for the network radius, R exists for which the probabilities attain a maximum value. The reason that can attributed to this is that for a given secondary exclusive region radius, R_0, when R is small, the secondary is prone to closely located malicious users and, hence, the cumulative power from all of the malicious users might be larger than the primary user's power. Thus, it is more probable. When the radius R is large, the cumulative power from the malicious users is not strong to arrive at the secondary user and to provide a successful PUEA.

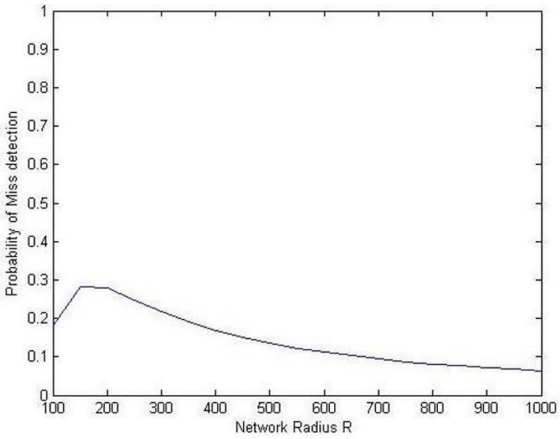


Figure 6. Probabilityof false alarm versus network Radius.

Figure 7 provides a comparison plot for a different number of malicious users in the system. It shows that as the number of malicious users increase the system performance decreases. For the network radius of 300 the probability of false alarm is 0.25 for malicious user count of 30 whereas the probability of false alarm for the same network radius is 0.5 for the malicious user count of 5.

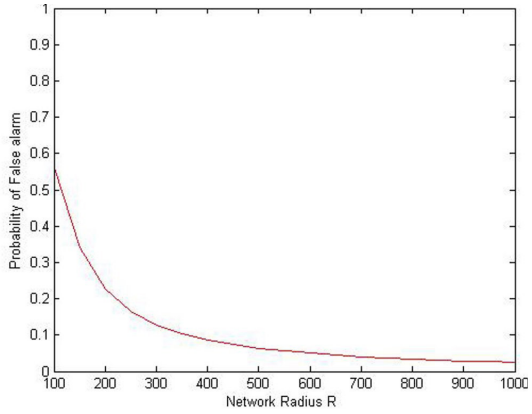
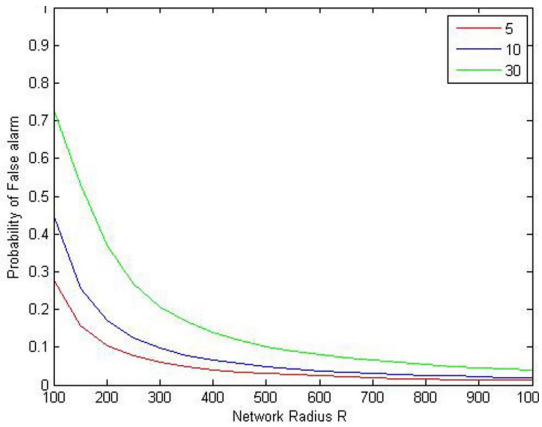


Figure 7. Proability of false alarm versus network radius for 5,10 and 30 malicious users.



4. Conclusion

This work focusses on two issues. First one is the enhanced interference cancellation technique to overcome the interference between the cognitive radio and other system in the same environment. Second thing is to analyse the PUEA from the Neyman Pearson test and simulation results proves that as the number of malicious users increases the cognitive performance is degraded.

5. References

1. Federal Communications Commission, Spectrum Policy Task Force Report. ET Docket No. 02-135. 2002 Nov.
2. Mitola III. J. Sweden: Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. Doctoral Dissertation; 2000 May; p. 1-313.
3. Haykin S. Cognitive Radio: Brain-Empowered Wireless Communications. IEEE Journal On Selected Areas In Communications. 2005 February; 23(2):201-20. DOI:10.1109/JSAC.2004.839380.
4. Vijayakumar P, Malarvizhi S. Reconfigurable Filter Bank Multicarrier Modulation for Cognitive Radio Spectrum Sharing - A SDR Implementation. Indian Journal of Science and Technology. 2016 Feb; 9(6). DOI:10.17485/ijst/2016/v9i6/80403.
5. Yucek T, Arslan H. A survey of spectrum sensing algorithms for cognitive radio applications. Communications Surveys & Tutorials IEEE. 2009 March; 11(1):116-30. DOI: 10.1109/SURV.2009.090109.
6. Avila J, Thenmozhi K. Upgraded Spectrum Sensing Method in Cognitive Radio Network. Indian Journal of Science and Technology. 2015 July; 8(16). DOI:10.17485/ijst/2015/v8i16/57499.
7. Sethi A, Brown TX. Hammer model threat assessment of cognitive radio denial of service attacks. Chicago, IL: Proceedings IEEE International Symposium of New Frontiers in Dynamic Spectrum Access Networks; 2008 Oct 14-17; p.1-12. DOI: 10.1109/DYSPAN.2008.32.
8. Clancy TC, Goergen N. Security in cognitive radio networks: Threats and mitigation. Singapore: Proceedings of International Conference on Cognitive Radio Oriented Wireless Networks and Communications; 2008 May 15-17; p. 1-8. DOI: 10.1109/CROWNCOM.2008.4562534.
9. Burbank JL. Security in cognitive radio networks: The required evolution in approaches to wireless network security. Singapore; Proceeding IEEE Cognitive Radio Oriented Wireless Networks and Communications; 2008 May 15-17; p. 1-7. DOI: 10.1109/CROWNCOM.2008.4562536.
10. Senthil Kumar B, Srivatsa SK. An Efficient Spectrum Sensing Framework and Attack Detection in Cognitive Radio Networks using Hybrid ANFIS. Indian Journal of Science and Technology. 2015 October; 8(28). DOI: 10.17485/ijst/2015/v8i28/71246.

11. Padmavathi G, Shanmugavel S. Performance Analysis of Cooperative Spectrum Sensing Technique for Low SNR Regime over Fading Channels for Cognitive Radio Networks. Indian Journal of Science and Technology. 2015 July; 8(16). DOI:10.17485/ijst/2015/v8i16/64746.
12. ModarSafirShbat, VyacheslavTuzlukov. Spectrum Sensing under Correlated Antenna Array Using Generalized Detector in Cognitive Radio Systems. International Journal of Antennas and propagation. 2013 May; 2013:1-8. DOI: org/10.1155/2013/853746.
13. Cheerla Sree Vardhan, Venkata Ratnam D, Nitin Allada Sai, Durga Sai Sruthi T. Spectrum Sensing for Cognitive Radio using Hilbert-Huang Transform Average Ratio Detector. Indian Journal of Science and Technology. 2015 Dec; 8(34). DOI:10.17485/ijst/2015/v8i34/70785.
14. Chen R, Park JM. Ensuring trustworthy spectrum sensing in cognitive radio networks. Reston, VA, USA: Proceedings IEEE Workshop on Networking Technology for Software Defined Radio Networks (SDR). 2006 Sept 25-25; p. 110–19. DOI: 10.1109/SDR.2006.4286333.
15. Bhagavathy Nanthini S, Hemalatha M, Manivannan D, Devasena L. Attacks in Cognitive Radio Networks (CRN) - a Survey. Indian Journal of Science and Technology. 2014 Jan; 7(4). DOI: 10.17485/ijst/2014/v7i4/48646.
16. Tarasak Poramate, Zhiwei Lin, Xiaoming Peng and Chin Francois. Partial Transmit Sequence-Active Interference Cancellation for UWB OFDM Transmission. Tokyo: IEEE 20th International Symposium on personal Indoor and Mobile Radio. 2009 Sept 13-16; p. 943-47. DOI: 10.1109/PIMRC.2009.5450339.
17. Tarasak Poramate, Chin Francois, Zhiwei Lin, Xiaoming Peng. Further Enhancement for Active Interference Cancellation on MB-OFDM UWB Transmission. Calgary, BC: IEEE 68th Conference on vehicular technology. 2008 Sept 21-24; p. 1-5. DOI: 10.1109/VETECF.2008.244.
18. Avila J, Praveen E, Varadharajan Brinda. ANN assisted-Augumentation of AIC for MIMO Multiband OFDM System. Nagapattinam, Tamil Nadu: IEEE International conference on Advances in Engineering, Science and Management. 2012 March 30-31; p. 228-32.
19. Yamaguchi H. Active Interference Cancellation technique for MB-OFDM Cognitive radio. Amsterdem, The Netherlands: Proceedings of 34th European Microwave conference. 2004 Oct 12-14; p. 1105-108.
20. Sarabchi Farshad, Nerguizian Chahe. Interference cancellation Technique for MIMO MB-OFDM UWB Cognitive Radio System. Valencia: 6th International Conference Wireless and Mobile Communications. 2010 Sept 20-25; p. 472-77. DOI: 10.1109/ICWMC.2010.53.