Analysis & Implementation of PUEA in Cognitive Radio Network

Manish Saxena [1], Khyati Chourasia [*2], Vipin D.Bondre [3]

[1]Assistant Professor of Electronics and Communication Department, Bansal Institute Of Science & Technology Bhopal, manish.saxena2008@gmail.com, Mobile : +919826526247

[*2] Student, Mtech (Digital Communication), Bansal Institute Of Science and Technology Bhopal. Email- khyati.chourasia@gmail.com, Mobile: +9730960500

[3] Assistant Prof. of Electronics Dept., Yeshwantrao Chavan College of Engineering,Nagpur. Email -vipin.bondre@gmail.com mob.0966135855

Abstract:- Cognitive radios have enabled the opportunity to transmit in several licensed bands without causing harmful interference to licensed users. Along with the realization of cognitive radios, new security threats have been raised. Security threats are mainly related to two fundamental characteristics of cognitive radios: cognitive capability, and re-configurability. Threats related to the cognitive capability include attacks launched by adversaries that mimic primary transmitters, and transmission of false observations related to spectrum sensing. Reconfiguration can be exploited by attackers through the use of malicious code installed in cognitive radios. Cognitive radio networks are wireless in nature, they face all classic threats present in the conventional wireless networks. In this paper we analyses and implement the PUEA in the CR network.

Keywords:-Cognitive Radio network, primary user emulsion attack (PUEA) , probability density function (pdf).

**Author for Correspondence*

I. Introduction

A word cognitive is for pertaining to the act or process of knowing, perceiving, remembering etc. Cognitive radio network is a network which manages their spectrum band intelligently or logically by itself. In cognitive radio network, Primary users have licensed spectrum band in which primary user send their information in the form of data packet but some of channels of spectrum band would be empty, these empty channels are called Spectrum Holes. An empty Channel can further used by un-licensed user also called as Secondary Users (SU's).Secondary User are unlicensed but registered user, they have particular identity no. Due to this, cognitive radio network consume time, and also increase the efficiency of the network. CRNs solve the spectrum shortage problem by allowing unlicensed users to use spectrum band of licensed user without interference. The term *Cognitive Radio* was first officially presented by Mitola and Maguire in 1999 [1].

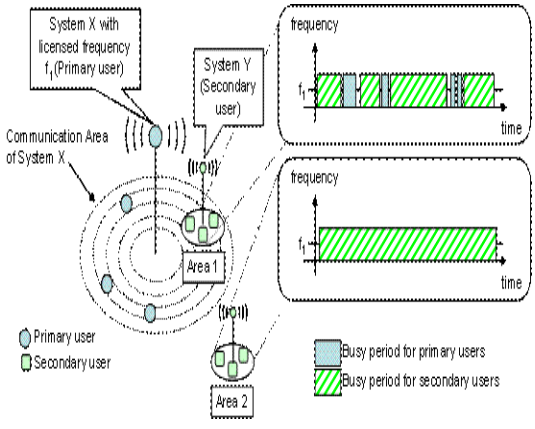


Figure-1 Basic cognitive radio Network

Figure-1 shows the basic structure of cognitive radio network. In this secondary user occupy the space called white space of primary user band which is under-

utilized. Normally primary user has own communication area, in which secondary user utilized the empty channel without any interference

.

II. Architecture of cognitive Radio Network

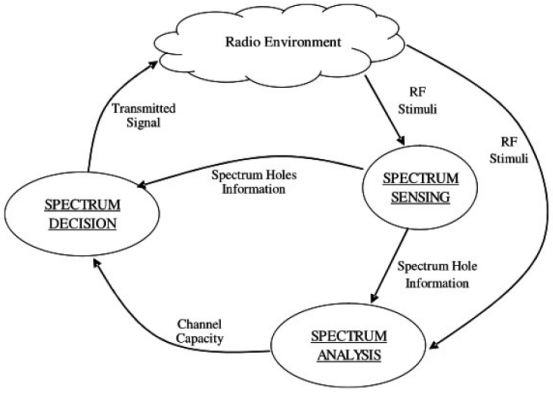


Figure- 2 General Architecture of Cognitive Radio

In figure -2 & figure-3 shows the architecture of cognitive radio network. When a primary user (PU) transmits data signal from a licensed spectrum band, it may be possible that it use only few channels of spectrum other channels are empty. These empty channels are sensed by secondary user (SU) which has no license for using this spectrum. Firstly secondary users sensed the spectrum and send the information of spectrum holes to the SU's. SU analyses the spectrum that PU ever uses these channels or not, because sometime PU use the empty channels which they not use before operation. After spectrum analysis SU's decide how many channels they required to send their data signal.

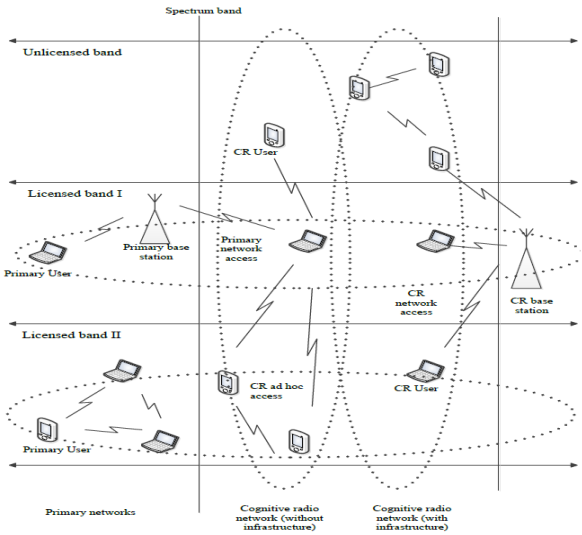


Figure- 3 Basic Cognitive Radio Network Architecture.

III. Proposed Architecture of Cognitive Radio Network

The proposed system architecture of a cognitive network is shown in Figure 4. The main aim of the proposed architecture is:

(i) To increase system stability, reliability and spectral efficiency through collision-free sharing of spectrum;

(ii) To resolve the collision between spectrum reuse.

(iii) To amplify the system flexibility and scalability.

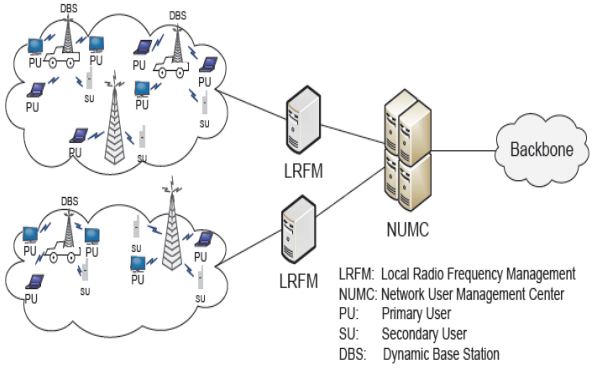


Figure-4 Proposed Architecture of Cognitive Radio Network

In the proposed architecture of Cognitive radio Network, there is fixed and dynamic BSs introduced. Also there is a concept of LRFM (local radio frequency management) and NUMC (Network user management center).In this all the users like PUs and SUs are registered in NUMC to get the authorization. In wireless systems, one spectrum reuse region may contain one or more cells, and is generally referred to as a cluster [3].An LRFM is joined to each cluster. The LRFM concerned about the continuous spectrum sensing and dynamic allocation for collision –free sharing of spectrum among all the PUs and SUs within the cluster. NUMC concerned about the authentication of users, handover and access control.

In the following, we will explain how the system works within each cluster, and how the clusters are connected into a network. [3]

First, the subscribers register with the system through the NUMC. In reality, the system generally has some fixed PUs, like those involved in TV/radio broadcasting and public safety systems. All the other users access the network in a random manner. An authorized user can request PU service or SU service based on the user's need and resource availability at each communication event. PUs will be granted higher priority and higher Quality of Service (QoS), at a higher service cost. For a time sensitive signal, like a phone conversation, the user can claim itself as a PU. While for a less time

sensitive and short delay tolerable signal, like transmitting a short message or email, the user can claim itself as an SU to get a better price deal. [3]
QoS for PUs will be divided into different levels, with a minimum information rate guarantee for all the PUs. PUs has higher priority for all the unassigned frequency bands. At the same time, the system can still support a considerable number of SUs due to the wide existence of spectrum holes or under-utilization.[3]
Spectrum allocation for all the users (including both PUs and SUs) within a cluster is managed by the LRFM attached to the BSs. Spectrum sensing of the PUs will be performed by the LRFM, and the detected spectrum holes are distributed among the SUs. Note that the LRFM can be equipped with advanced receivers and strong data processor and controller, and it also has the real-time information of the frequency band occupied by each PU. The LRFM can perform much more accurate spectrum sensing and highly efficient dynamic resource allocation. As a result, transmission collisions can be completely resolved, and each user terminal no longer suffers from the burden of continuous spectrum sensing and access frequency selection. [3]
When the user is moving from one cluster to another cluster, it will be handed over to the LRFM in the new cluster through the NUMC. NUMC is also responsible for other network management tasks, including user authentication, access control, and accounting (for billing and record tracking purpose) etc. [3] Below figures are Primary User and Secondary User

IV. Performance Study of PUEA in CRN

Major issues in spectrum sensing are how perfectly it can differentiate incumbent signals from secondary user signals? An attacker can easily exploit the spectrum sensing process. For example, an attacker may imitate as an incumbent transmitter by transmitting unrecognizable signals in one of the licensed bands, thus preventing other secondary users from accessing that band. Primary user emulation (PUE) attack is considered to be one of the severe threats to cognitive radio systems. It poses a great threat to spectrum sensing. In this attack, a malicious node transmits signals whose characteristics emulate those of incumbent signals. There are two types of behavior associated with the primary user emulation attack, which are discussed as follows.

- **Selfish PUE attacks**: The main objective is to maximize attacker's bandwidth. For an instance, when malicious node identifies vacant band, it will prevent other secondary users from using that band by transmitting signals that resembles the incumbent signals.
- **Malicious PUE attack**: The main objective is to obstruct the secondary users from identifying and using vacant spectrum bands. Malicious attacker does not necessarily use vacant bands for its own communication purposes. It is important to note that in PUE attacks, malicious nodes only transmit in vacant bands.

Primary Exclusive Region
One of the deployment schemes in current related research is the primary exclusive region (PER). It sets a safeguard for primary receivers. The secondary network must be deployed outside PER. The exclusive zone is also called as keep-out region. It gives primary receiver a protection area. It is a way of imposing a certain distance on cognitive users from the primary user thereby reducing interference to the primary receiver. Within this region cognitive users are not allowed to transmit. This type of deployment scheme is suitable to a broadcast network. For an instance, network in which there is one primary transmitter communicating with multiple primary receivers. TV network or the downlinks in the cellular network are the good examples of a broadcast network. In such type of networks, primary receivers may be passive devices. Such a primary-exclusive region has been proposed for the upcoming spectrum sharing of the TV band. The secondary users are randomly and uniformly distributed within a network radius from the primary transmitter, outside the PER.

System Model of CRN

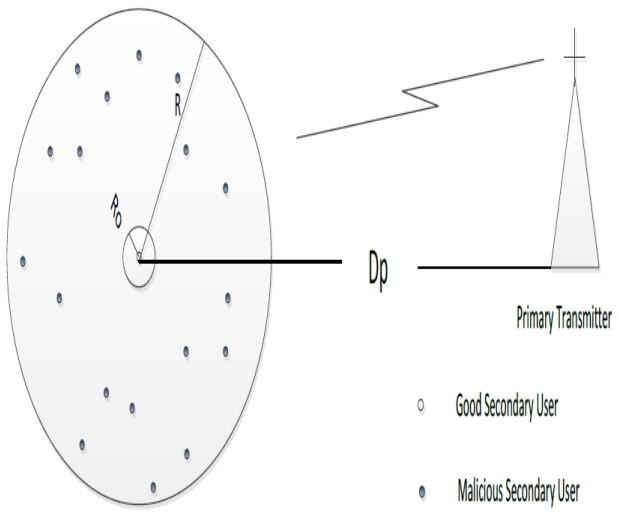
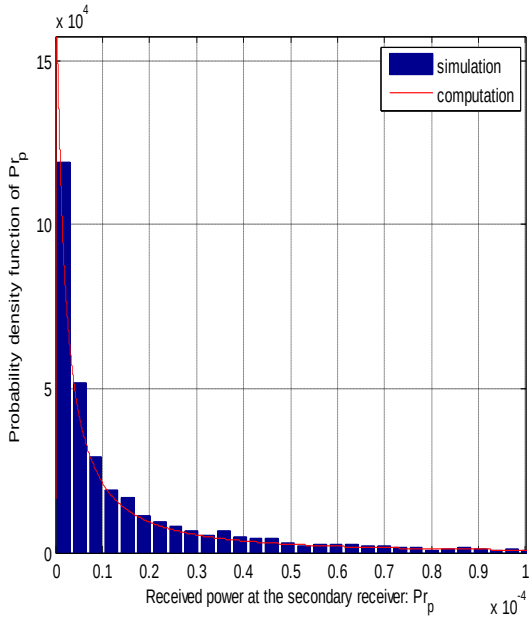


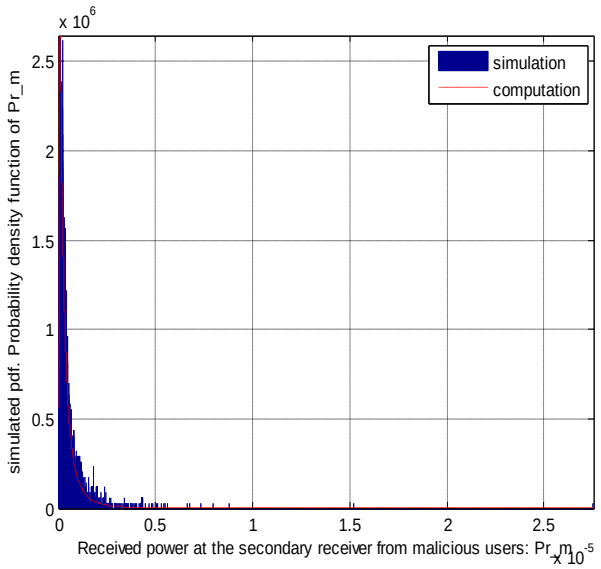
Figure-5 System model of CRN

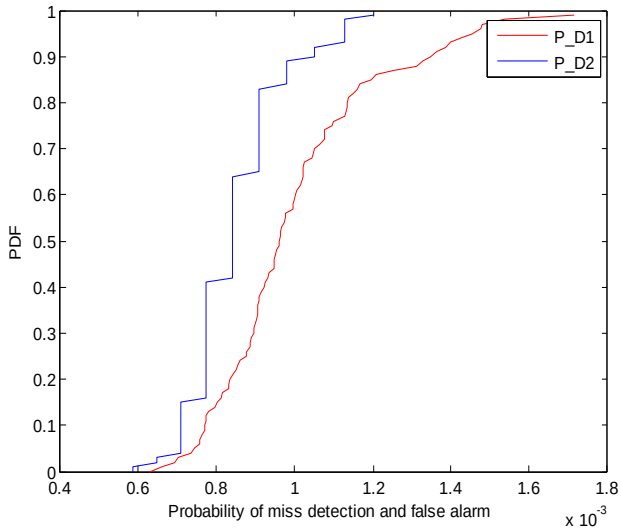
Following assumptions are made for this system model.There is M malicious users in the system and they transmit at power 'Pm'. The distance between primary transmitter & all the users is 'Dp' and transmits at power 'Pt '. The position of secondary user is at the center of the exclusive region. Malicious users are uniformly distributed in circular region of radius R and are statistically independent of each other. Co-ordinates of primary transmitter are known to all the users and are fixed at (rpt,t). The transmission from primary transmitter and malicious users undergo path loss and log normal shadowing. The path loss exponent chosen for transmission from primary transmitter is 2 and from malicious user are 4. No malicious users are present within a circle of radius Ro, called as the exclusive radius from secondary user. There is no co-operation between the secondary users.

V. Simulation Results and observations

Below Figures shows the Probability Density Function (pdf) of the received power at the secondary user when the primary transmitter is at distance 200Km, Primary transmitter power Pt=300Kw, σm= 5.5dB, σp= 8dB, $R0$= 40m, R= 1200m, Pm= 5W. Probability Density Function of Received power is calculated for 5000 times. Both simulated and computed PDF are plotted in the same figure for easy comparison.







VI Conclusion

We have done a detailed analysis and simulation of the network for PUE attack. Simulations were carried out to determine the performance of the proposed system model for PUEA attack in terms of probabilities of miss detection and false alarm. We showed various simulation results under different configuration of primary transmitters. Our experimental results demonstrate the statistical characteristics of the probability of false alarm and miss detection in the proposed system. I plan to make comprehensive performance comparison with existing research results in the future work.

Reference

[1] 4G MOBILE ARCHITECTURE Rhituparna Paul,Nishat Kabir,Tahnia Farheen Department of Electrical and Electronic Engineering Bangladesh University of Engineering and Technology December 31st, 2008.

[2]THE BEGINNING OF THE FUTURE: 4G PUBLIC SAFETY COMMUNICATIONS SYSTEMS white paper by Motorola, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorola.com/nextgen**

[3] Role of Cognitive Radio on 4G Communications A Review VOL. 3, NO. 2, February 2012 ISSN 2079-8407Journal of Emerging Trends in Computing and Information Sciences ©2009-2012 CIS Journal. All rights reserved.

[4] A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION [5] Denial-of-service attack From Wikipedia, the free encyclopedia

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

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

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

[8] Kwang Cheng Chen, Y. J. Peng, Neeli Rashmi Prasad, Y. C. Liang and Sumei Sun, *Cognitive Radio Network Architecture: part I -- General Structure*, *Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication*, Suwon, South Korea, January, 2008, pp.114-119.

[9] Vinod Sharma and ArunKumar Jayaprakasam, *An Efficient Algorithm for Cooperative Spectrum Sensing in Cognitive Radio Networks*, *Proceedings of National Communications Conference (NCC)*, Guwahati, India, January, 2009.

[10] Cognitive Radio Ad Hoc Networks, Broadband Wireless Networking Lab, School of Electrical and Computer Engineering, Georgia Inst of Tech. URL: http://www.ece.gatech.edu/research/labs/bwn/CRAHN/projectdescription.html

[11] Wenjing Yue and Baoyu Zheng, *A Two-Stage Spectrum Sensing Technique in Cognitive Radio Systems Based on Combining Energy Detection and One-Order Cyclo-Stationary Feature Detection*, *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09)*, Nanchang, China, May, 2009, pp.327-330.

[12] Rajesh K. Sharma and Jon W. Wallace, *Improved Spectrum Sensing by Utilizing Signal Autocorrelation*, *Proceedings of IEEE Vehicular Technology Conference*, Barcelona, Spain, April, 2009, pp.1-5.

[13] Ruiliang Chen, Jung-Min Park and Jeffrey H. Reed, *Defense against Primary User Emulation Attacks in Cognitive Radio Networks*, *IEEE Journal on Selected Areas in Communications*, Vol.26, No.1, 2008, pp.25-37.

[14] Huahui Wang, Leonard Lightfoot and Tongtong Li, *On PHY-Layer Security of Cognitive Radio: Collaborative Sensing under Malicious Attacks*, *44th Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March, 2010, pp.1-6.

[15] Eric Wong and Rene Cruz, *On Physical Carrier Sensing for Cognitive Radio Networks*, *Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing*, Allerton House, UIUC, IL, September, 2007.

[16] Bertrand Mercier, Viktoria Fodor, Ragnar Tobaben et al., *Sensor Networks for Cognitive*

[17]from internet

