ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

Attacks & Preventions of Cognitive Radio Network-A Survey

Dr. Anubhuti Khare[1], Manish Saxena [2] ,Roshan Singh Thakur [3] , Khyati Chourasia [*(4)]

Abstracts-In this paper we analyze and surveyed a latest communication technology named "Cognitive Radio Network". Cognitive radio network is a network in which an un-licensed user can use an empty channel in a spectrum band of licensed user. It is useful as well as harmful too. Because of this some unwanted user can use this empty channel through attacks and threats. In this paper we focus on cognitive radio network attacks and how to prevent our network through these attacks.

Keywords: Cognitive radio network, Pus, SUs, Spectrum sensing, spectrum holes, LRFM, NUMC

Author For correspondence

I. Introduction

Communication is a transfer of information from one point to another. Today's communication is very advance; we use many new technologies like Cognitive radio network is latest one. The term *Cognitive Radio* was first officially presented by Mitola and Maguire in 1999 [1].Cognitive radio network is a network in which an un-licensed user can use an empty channel in a spectrum band of licensed user. Cognitive Radio Networks (CRNs) is an intelligent network that adapt to changes in their network to make a better use of the spectrum. CRNs solve the spectrum shortage problem by allowing unlicensed users to use spectrum band of licensed user without interference. Generally licensed users are known as primary users and un-licensed users *are secondary users.When information is send through a* licensed spectrum band is a primary user, only some channel of band is used, others are empty. These empty channels are used by un-licensed user called secondary user. Secondary users always watch the activities of primary user, and detect the empty channel and occupy the channel without disturbing the primary user. When the primary users are active, the secondary user should either avoid using the channel. An Empty channel also known as spectrum holes.

[1]*Reader, Department of Electronics and Communication, University Institute ofTechnology, Rajeev Gandhi Technical University, Bhopal (M.P), Mob: +919425606502*

[2] *Asst.Professor, Head of Electronics and Communication Department,Bansal Institute Of Science and Technology Bhopal (M.P)-, Mob: +919826526247*

[3]*Asst.Professor, Department of Information Technology, Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur (M.S), Mob: +919552002195*

[*(4)] *Student, M.Tech (Digital Communication),Electronics and Comm.DeptBansal Institute Of Science And technologyBhopal (M.P) ,mob:-+919730960500*

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. [2]

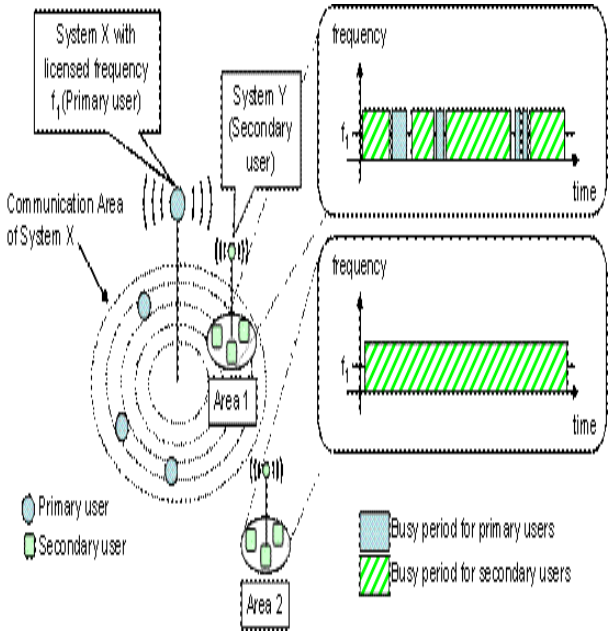

Figure-1 Basic cognitive radio Network

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

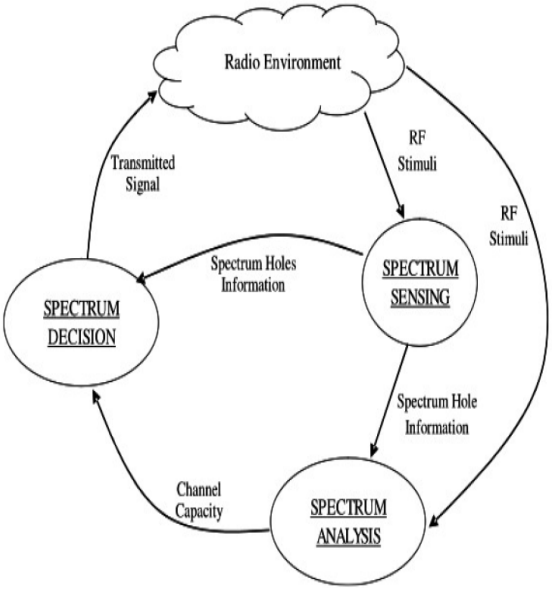

Figure 2:- General Architecture of Cognitive Radio

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.

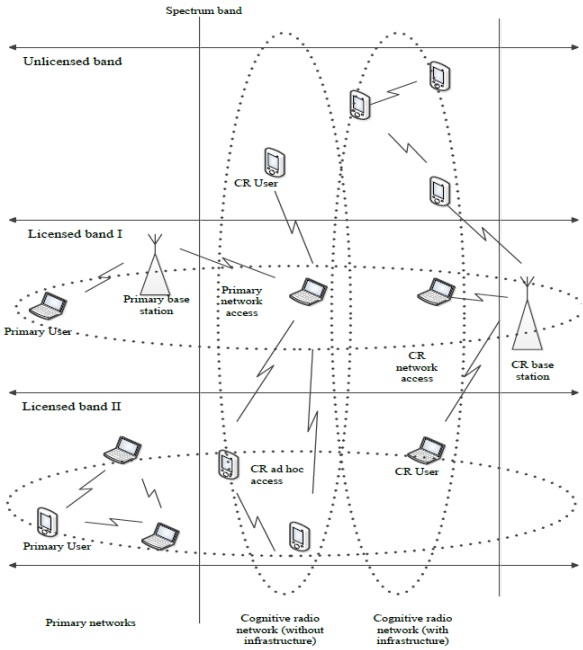

Figure- 3:- Basic Cognitive Radio Network Architecture.

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.

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.

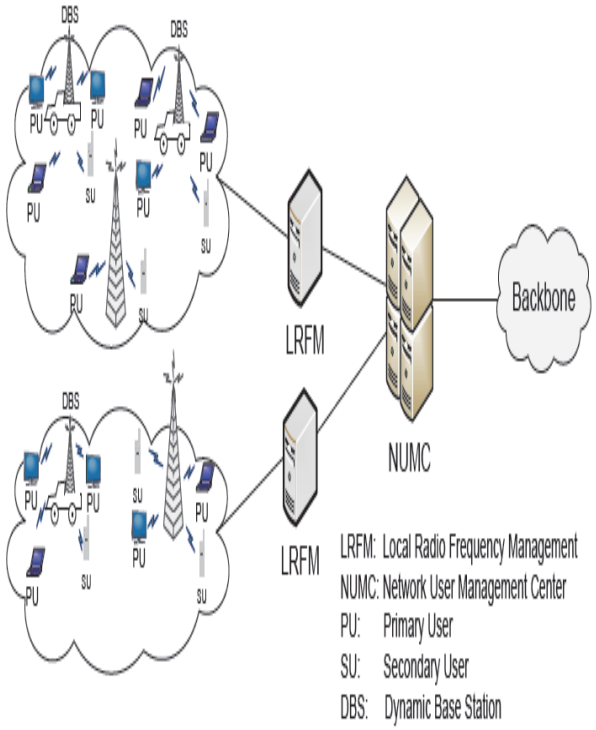

Figure-4 Proposed Architecture of Cognitive Radio Network

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]

IV. Attacks of Cognitive Radio Network

There are many attacks in wireless communication, only few attacks we categorized through four major layers: physical layer, link layer (also known as MAC layer), network layer and transport layer. In physical layer there are three main attacks in which we focused - Primary User Emulation (PUE), Objective function attack and jamming. In Link layer we focused on Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation DoS Attack (CCSD), and Selfish Channel Negotiation (SCN). In Network Layer, the routing attacks, HELLO Flood attack and Sinkhole attack. In transport Layer, we focused the Lion Attack. It may be possible that jamming attack done on physical layer or MAC layer.

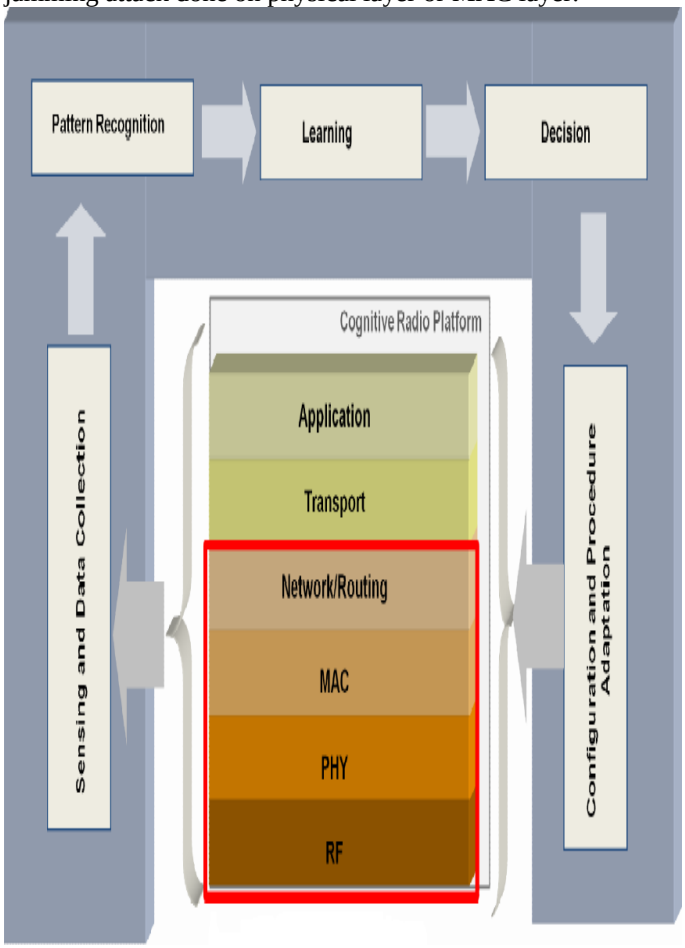

Figure-5 Layered Diagram of Cognitive radio network

[A] Physical layer Attacks

a) Primary User Emulation Attack: - Primary User Emulation (PUE) attack is attack carried out by a malicious secondary user emulating a licensed primary user to obtain the resources of a given channel without having to share them with other secondary users. [4] Due to this, the attacker is able to utilized full bands of a spectrum. This attack is divided into two categories: Self PUE attack and Malicious PUE attack.
The attacker can then perform the PUE attack during these idle times

b) Objective Function Attack:- The cognitive engine in the adaptive radio is the one responsible for adjusting the radio parameters in order to meet specific requirements such as low energy consumption, high data rate, and high security. Radio parameters include center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size. The cognitive engine

calculates these parameters by solving one or more objective functions, for instance find the radio parameters that maximize data rate and minimize power[4][5]

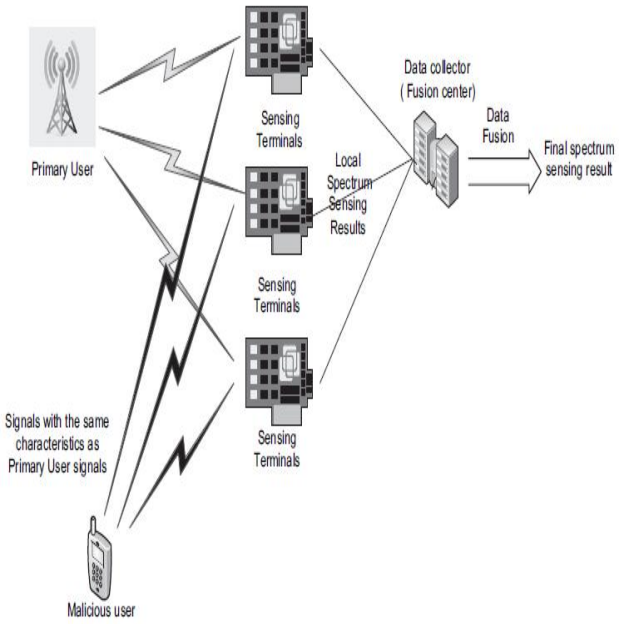

Figure 6:-Primary User Emulation Attack

c) Jamming Attack: - Jamming attack is an attack in which the attacker can sends packets to hinder legitimate participants in a communication session from sending or receiving data; consequently, creating a denial of service situation.[4]. There are four types of jammers: Constant Jammer, Deceptive Jammer, Random Jammer, and Reactive Jammer.

[B] Link Layer Attacks

a) Spectrum Sensing Data Falsification (SSDF)

Spectrum Sensing Data Falsification, also known as the Byzantine Attack, takes place when an attacker sends false local spectrum sensing results to its neighbors or to the fusion center, causing the receiver to make a wrong spectrum-sensing decision [5][6][7]. This attack mainly targeted to centralized as well as distributed CRNs. SSDF attack is more harmful in a distributed CRN.

b) Control Channel Saturation DoS Attack (CCSD)
When many CRs want to communicate at the same time, the common control channel becomes a bottleneck as the channel can only support a certain number of concurrent data channels. An attacker can utilize this feature and generate forged MAC control frames for the purpose of saturating the control channel and thus decreasing the network performance due to Link layer collisions.[5] .

c) Selfish Channel Negotiation (SCN)
In a multi-hop CRN, a CR host can refuse to forward any data for other hosts. This will allow it to conserve its energy and increase its own throughput which resulted from selfish channel concealment [5]. Similar objectives can be achieved if the selfish host was able to alter the proper MAC behavior of the CR devices. For instance, if the host decreases its own back-off window size, it will have a higher chance of claiming the channel at the expense of other CR hosts. This attack can also severely degrade the end-to-end throughput of the whole CRN [5].

[C] Network Layer Attacks

a) Sinkhole Attacks
In a sinkhole attack, an attacker advertises itself as the best route to a specific destination, during neighboring nodes to use it to forward their packets [5]. An attacker may use this way to perform another attack called selective forwarding where an attacker is able to modify or discard packets from any node in the network. The attack is particularly effective in the infrastructure and mesh architectures as all traffic goes through a base station allowing the attacker to falsely claim that it is the best route for packet forwarding.[5]

b) HELLO Flood Attacks
The HELLO flood attack is accomplished when an attacker sends a broadcast message to all the nodes in a network with enough power to convince them that it is their neighbor [5].

[D] Transport Layer Attacks

c) Lion Attack
The Lion attack uses the primary user emulation (PUE) attack to disrupt the Transmission Control Protocol (TCP) connection. The Lion attack can be considered a cross-layer attack performed at the physical link layer and targeted at the transport layer where emulating a licensed transmission will force a CRN to perform frequency handoffs and thus degrading TCP performance. [5]

V. Prevention against Attacks of cognitive radio network

a) Physical layer: - Two approaches have been suggested to prevent our network to PUE attack on physical layer: Distance Ratio Test (DRT) which is based on received signal strength measurements and Distance Difference Test (DDT) which is based on signal phase difference. [5].Both approaches are based on a transmitter verification procedure. Defending against jamming attack, we use CSMA (carrier sensing multiple access) in which a device will continuously sense a channel until it finds to be empty. A jamming detection technique that investigates the relationship between Signal Strength (SS) and Packet Delivery Ratio is suggested. [5]

b) Link layer: - Defending against SSDF we suggested a decision fusion techniques, If the sum is greater than or equal to a certain threshold (which is a specified value between 1 and the number of sensing terminals), then the final sensing result is "busy," i.e., it denotes the presence of incumbent signal. Otherwise, the band is determined to be "free," i.e., it denotes the absence of incumbent signal. [5] Defending against Control Channel Saturation and selfish channel negotiation. Mitigating CCSD and SCN can be done by adapting a trusted architecture where any suspicious CR host will be monitored and evaluated by its neighbors. A neighbor can then perform a sequential analysis on the set of observation data, and conclude a final decision whether it is misbehaving or not. [5]

c) Network Layer: - Defending against a sinkhole attack is hard to detect because it exploits the very design of the routing protocol and network architecture. To countermeasure the HELLO flood attacks, a symmetric key should be shared with a trusted base station [42]. The base station will act as a Trusted Third Party as in Kerberos and facilitate the establishment of session keys between parties in the network; in order to protect their communication. [5]

d) Transport Layer:- The CRN devices will be able to freeze TCP connection parameters during frequency handoffs and adapt them to the new network conditions after the handoff. To secure the control data in order to prevent the attacker from eavesdropping current and future actions of the CRN, a group key management (GKM) can then be used to allow CRN members to encrypt, decrypt and authenticate themselves. Finally, a cross-layer IDSs specifically adapted to CRNs can be used as a technique to find the attack source if it still exists. [5]

VI. Conclusion

In this paper we, only discuss about the attack of cognitive radio network. How these attacks happened and how these attacks harmed Cognitive radio network. In this, many of attack can attack in different layers of cognitive radio network. Some of them can advertise itself as licensed PUs, or some of them can send false data to the network.

Reference

[1] Mitola III J, Maguire Jr G. Cognitive radio: making software radios more personal. *Personal Communications, IEEE* [*see also IEEE Wireless Communications*] 1999; 6(4):13–18. DOI: 10.1109/98.788210.
[2] Simon Haykin, *Life Fellow, IEEE*. Cognitive Radio: Brain-Empowered Wireless Communications IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 2, FEBRUARY 2005
[3] Towards Secure Cognitive Communications in Wireless Networks Tingting Jiang, Virginia Tech Tongtong Li and Jian Ren, Michigan State University
[4]Survey of Security Issues in Cognitive Radio Networks *Wassim El-Hajj1, Haidar Safa1, Mohsen Guizani2,*
Journal of Internet Technology Volume 12 (2011) No.2
[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 Radio: Theory*