International Engineering Journal For Research & Development

Vol.2
Issue 6

E-ISSN NO:-2349-0721

Impact factor : 2.25

A DEFENSIVE APPROACH AGAINST CROSS LAYER ATTACKS IN COGNITIVE RADIO

Shwetali V. Wankhede [1], Prof. M. N. Thakare[2], Prof. S. R. Vaidya[3]

[1] Student Mtech 4th Sem, Electronics (Comm), SDCE ,
[2] Assistant Professor, Department of Electronics & Telecomm. Engg, BDCE Sevagram,
[3] Assistant Professor, Department of Electronics Engg, SDCE Selukate, Wardha, Maharashtra, India
[1]shwetali.wankhede@gmail.com,[2]mnt_ent@rediffmail.com,[3]vaidyarsumit@gmail.com

ABSTRACT –

A latest communication technology named "CRN" is a network in which an un-licensed user can use a freed channel in a spectrum band of licensed user without causing interference to the incumbent transmission. Cognitive Radio networks are vulnerable to attacks, as some unwanted user can use this empty channel through attacks and threats. The existing research on security issues in cognitive radio networks mainly focuses on attack and defense in individual network layers. Cross-layer design is a concept introduced to increase network efficiency through information exchange among different layers, has brought revolutionary view change to the networking research community in the past. In this paper, we are working on detecting and defeating attacks in cross layer. .

Key Words: *Cognitive Radio Network (CRN)1…*

1. INTRODUCTION

Communication is a transfer of information from one point to another. Today's communication is very advance; we use many new technologies as if Cognitive radio network is latest one. The term Cognitive Radio was first presented by Mitola and Maguire in 1999. In Cognitive radio network an unlicensed 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. 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. Un-licensed user called secondary user uses these empty channels. 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.

Meanwhile if a SU detects any PU signal in its currently used band it should vacate this band for PUs and senses another vacant band in its environment and switches to new sensed hole. Essential security mechanisms should be used for successful deployment of cognitive radio networks (CRNs) to prevent misuse of valuable spectrum bandwidth.

Two types of Band based on frequency spectrum

1. Licensed Band CR
2. Unlicensed Band CR

Two types of Users of CRNs

1. Primary Radio (PR) user, which operates in its licensed spectrum band.
2. Cognitive Radio (CR) user, which operates either in unlicensed spectrum band or in the licensed spectrum band of PR nodes while ensuring that it does not interfere with PR nodes.

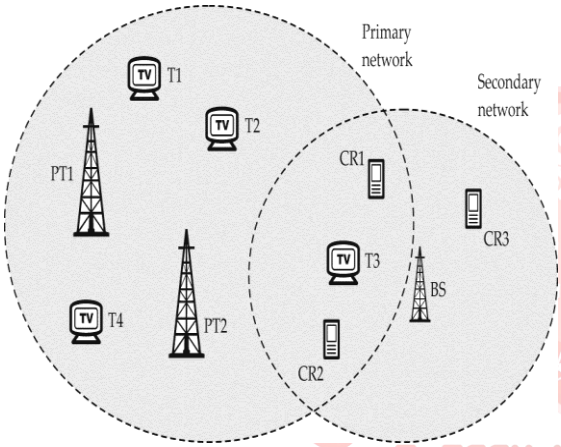

Fig -1: Cognitive Radio

Four main functions of CR

1. Spectrum sensing: It determines which portions of the spectrum are available and detect the presence of licensed users.
2. Spectrum management: It is to select the best available channel.
3. Spectrum sharing: It coordinates access to this channel with other users.
4. Spectrum mobility: It vacates the channel when a licensed user is detected.

This radio spectrum sharing policy among the licensed and unlicensed users, however, opens up the possibility of various security threats. A number of attacks targets CRNs in different layers i.e physical layer, link layer, network layer, transport layer and solutions have been presented to detect those attacks. Here, we are focussing on cross layer attacks in CRNs.

1.1 Attacks in Cognitive Radio

There are many attacks in wireless communication, only few attacks we categorized through four major layers: physical layer, link layer (also known as MA++ layer), network layer and transport layer. In physical layer there are three main attacks- Primary User Emulation (PUE), Objective function attack and jamming. In Link layer- 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- Lion Attack. This are the attacks on the physical layer, link layer, network layer and transport layer which are yet been detected and defeated.

1.2 Cross Layer attacks

Cross-layer design is a concept introduced to increase network efficiency through information exchange among different layers, has brought revolutionary view change to the networking research community in the past. Nowadays, the increasingly ubiquitous and distributed networking systems are facing vicious and intelligent attacks that exploit almost all network protocols and surely do not restrict themselves within the boundaries of network layers. Attackers have the capability to launch attacks in multiple layers simultaneously. Smart attackers can coordinate the attack activities in different layers to better achieve their goals. A smart attacker can launch several attacks co-ordinately, referred to as cross layer attacks.

E-ISSN NO:2349-0721

Cross-layer design emphasizes on the network performance optimization by enabling different layers of the Communication stack to share state information or to coordinate their actions in order to jointly optimize network performance. Hence the concept of cross layer design must be compared with the traditional layered architecture so that people can be motivated towards the use of the violation of the layered design.

2. LITERATURE REVIEW

This paper describes that Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client or to create multiple illegitimate identities [1]. Peng Zhang, Yixin Jiang, Chuang Lin proposed P-Coding which is a novel security scheme against eavesdropping attacks in network coding [2]. This paper discusses the challenges and opportunities of using cross-layer techniques for enhancing wireless network security. It investigate the impact of cross-layer techniques on security and network performance [3]. It propose a trust-based cross-layer defense framework that relies on abnormal detection in individual layers and cross-layer trust fusion. Simulation results demonstrate that the proposed defence framework can significantly reduce the maximum damage caused by attackers [4]. It proposes that in the upper layer, the spoofing attack is considered similarly to the bad data injection toward the power system. A trustworthiness evaluation, which is based on both the physical layer information and power grid measurements, is applied to identify the PMU being attacked [5]. 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 [6]. This paper describes a CRN based on IEEE wireless regional area network (WRAN) and describes some of the security threats against it [7].

3. PROBLEM DEFINATION

Various types of attacks in individual layers i.e physical layer- PUE attack, objective function attack, jamming attack, network and transport layer has been studied, detected and defeated. But the attacks on cross layer are not yet been discussed much. Thus, we will focus on the attacks on cross layer that will be detected and endeavour a solution to these problem.

4. OBJECTIVE

The main objectives for proposed work are as mentioned below:

1) To defeat the spoofing attack in cross layer

2) To defeat the spying attack in cross layer

3) To decrease energy consumption.

4) To increase the throughput

5. TYPES OF CROSS LAYER ATTACKS

Spoofing Attack: In Communication the attacker may get access and sends fake information to destination.

Spying Attack (Eavesdropping): refers to the unauthorised monitoring of other people's communications. Its activities do not affect the normal operation of network transmission, but sends fake data to destination.

6. DESIGN MODULE

During the communication, data flows from sender node to destination node. During the secure

communication packets flows efficiently to the desired node. But whenever there is packet drop i.e the data has been dropped meanwhile in between communication before reaching to destination node. Thus, the data get leaked in between or the destination node won,t get the desired message, and hence spoofing or spying are assumed to be occurred there.

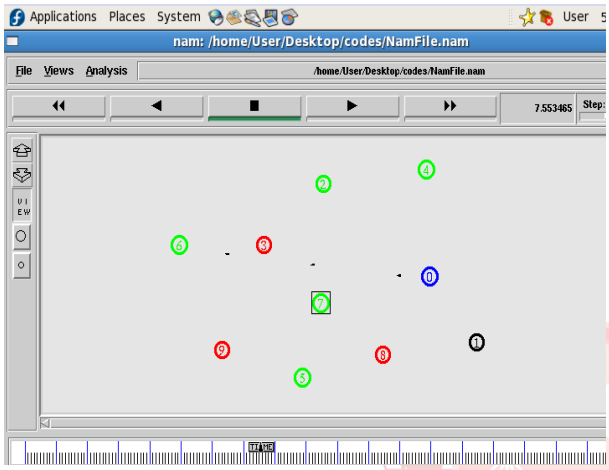

Fig 2: Secure Communication

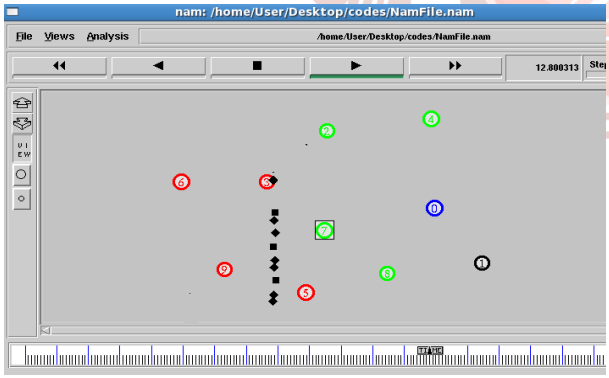

Fig 3: Occurrence of attack

After the spying and spoofing attacks occurrence within the network the graphs for delay, energy and throughput are plotted and its values are noted after the are observed within the transmission.

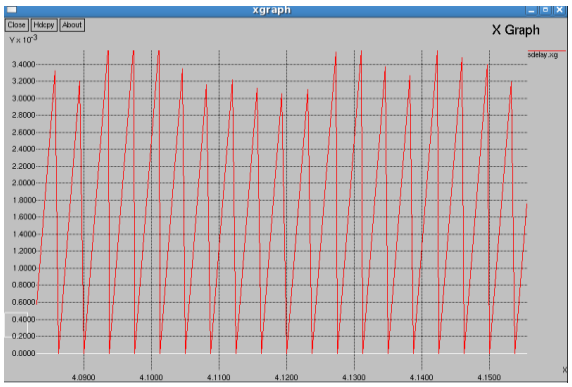

Fig 4: Graph of delay after attack

In the above graph of delay, we can observe that at time 4.1ms delay is 2.4ms.

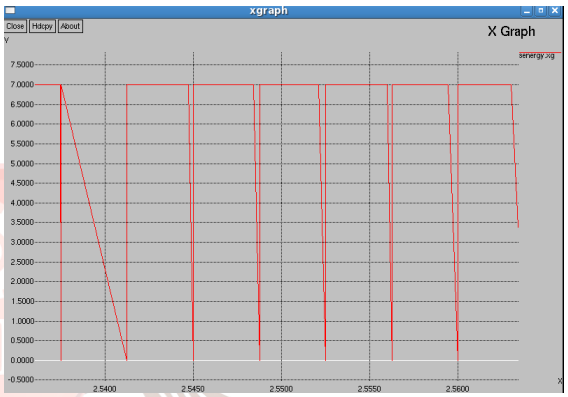

Fig 5: Graph of energy after attack

In the above graph of energy, we can observe that at time 2.54ms energy is 2.3 joules.

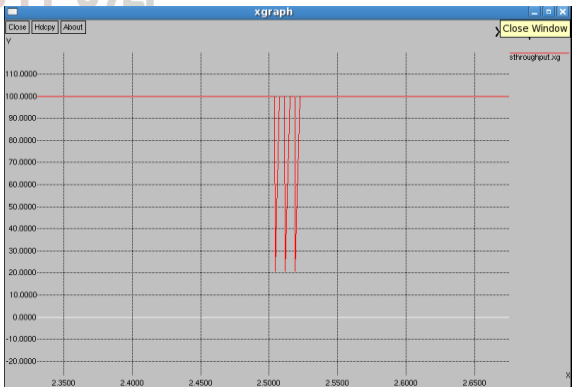

Fig 6: Graph of throughput after attack

In the above graphs of throughput, throughput is 100% at most of the points, but we can notice in the interval 2.5000-2.5500s the throughput falls to 20%.

Table No: 1

Delay Throughput Energy

Sr. No.	Parameters	Before attack removal and without CR	After attack removal and with CR
1.	Delay	1.25ms	0.3000ms
2.	Throughput	Falls to 20% in 3-3.5ms	Near about 100%
3.	Energy	$2.5* 10^{-3}$joules	$0.3* 10^{-3}$joules

6.1 Global Inspector/ Global Authority (GI):

GI is technique which is being used to detect and defeat the attack that occurred between the transmission of data from particular node. Whenever the data or packet is being send from source node to destination node, then packet from source node first passes through the GI and then to the destination node.

Selection of GI:

3 clusters are to taken comprising of 30 nodes, i.e 10 nodes in each cluster. The node with two maximum energy from each of the cluster are considered as GI.Through GI only packet is forwarded to destination, it is responsible to examine whether packet is eavesdrop or not by the adversary. The GI will check whether the incoming message is eavesdrop by the adversary by checking its source address. If the message is eavesdrop then it will get dropped otherwise GI will pass it ahead. At the destination node, it will be checked if packet has come from the trusted node i.e GI, if so the packet will be accepted otherwise it will get dropped.

7. RESULTS

Cognitive radio along with attack removal can be categorized in 4 ways:

i) Without attack removal without cognitive radio.

ii) Without attack removal with cognitive radio.

iii) With attack removal without cognitive radio.

iv) With attack removal with cognitive radio.

Depending upon this categories graphs for Delay, Throughput & Energy can be plotted and comparison can be shown.

i) Delay should get reduced.

ii) Throughput should get increased.

iii) Energy consumption should get reduced.

Results for Delay:

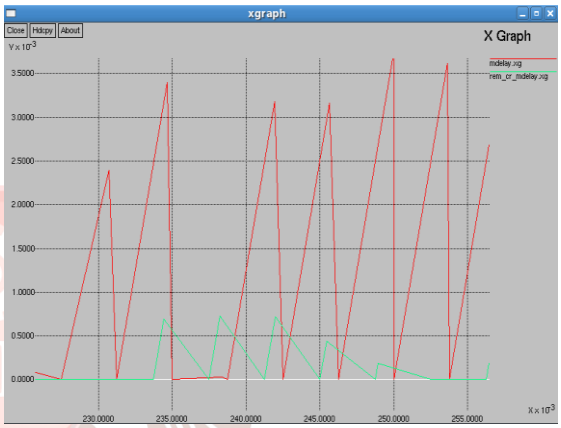

Fig 7: Graph of delay for without attack removal and without cognitive radio

In without attack removal and without cognitive radio at time 0.240s the delay is between 1.000-1.5000*$10^{-3}s$, approx. 1.25*$10^{-3}s$, whereas with attack removal and with cognitive radio at time 0.240s delay reduced to 0.000-0.5000* $10^{-3}s$, approx. 0.3000 *$10^{-3}s$.

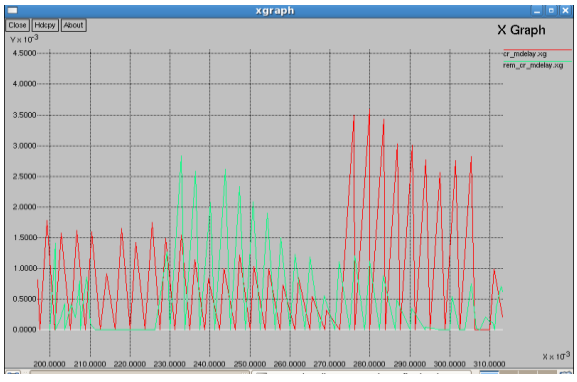

Fig 8: Graph of delay for with cognitive radio and without attack removal

In with cognitive radio and without attack removal at time 0.280s the delay is between 3.500-4.000*$10^{-3}s$, approx. 3.100*$10^{-3}s$, whereas with attack removal and with cognitive radio delay reduced to 1.000-1.5000* $10^{-3}s$, approx. 1.25*$10^{-3}s$.

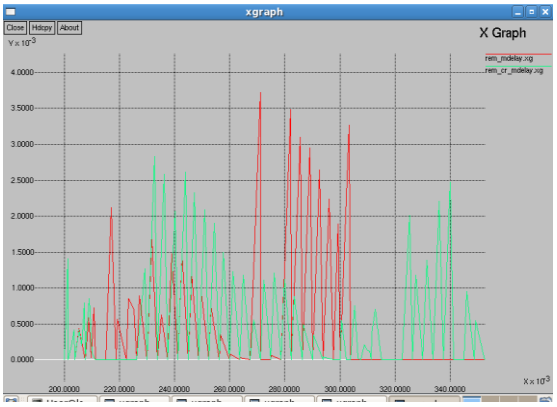

Fig 9: Graph of delay for with with attack removal and without cognitive radio

In with attack removal and without cognitive radio at time 0.280s the delay is between 3.000-3.5000*$10^{-3}s$, approx. 3.500*$10^{-3}s$, whereas with attack removal and with cognitive radio delay reduced to 1.000-1.5000* $10^{-3}s$, approx. 1.25*$10^{-3}s$.

Results for Throughput:

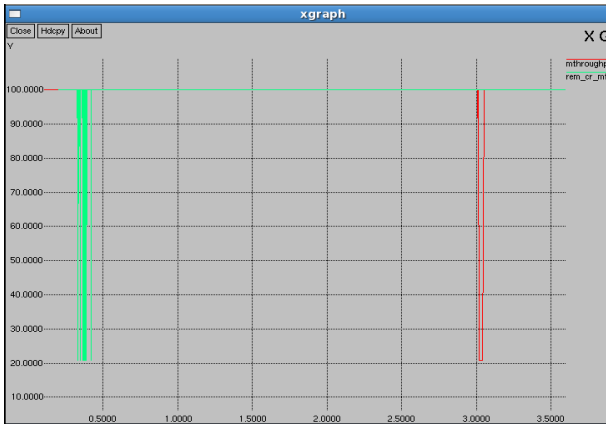

Fig 10: Graph of throughput without attack removal and without cognitive radio

Throughput is 100% at most of the points but in without attack removal and without cognitive radio it falls to 20% in between 3.000-3.5000s.

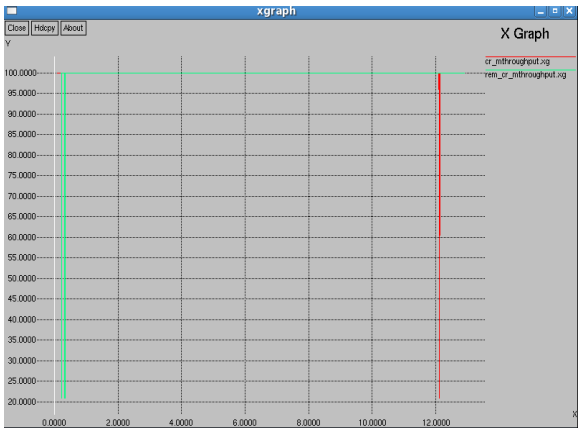

Fig 11: Graph of throughput for without attack removal and with cognitive radio

Throughput is 100% at most of the points but in without attack removal and with cognitive radio it falls to 20% after 12.000s.

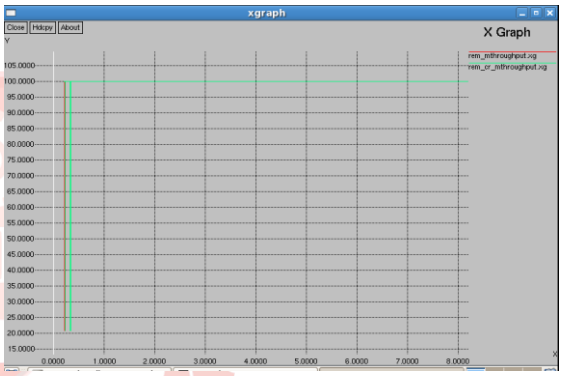

Fig 12: Graph of throughput for with attack removal and without cognitive radio

Throughput is 100% at most of the points but with attack removal and without cognitive radio it falls to 20% in between 0.000-1.000s.

Results for Energy:

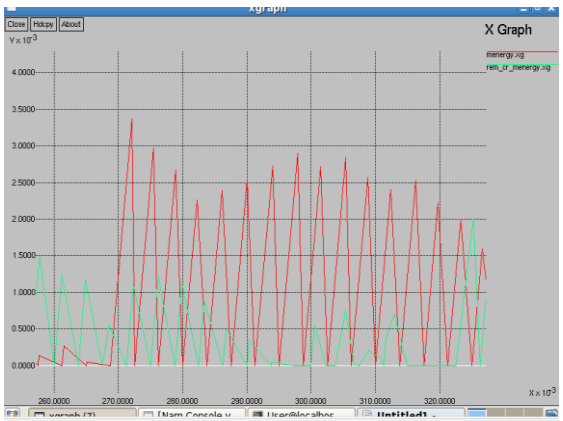

Fig 13: Graph of energy for without cognitive radio and without attack removal

In without cognitive radio and without attack removal the energy is $2.5* 10^{-3}$joules at 0.290 ms, whereas with attack removal and with cognitive radio the energy consumption is reduced to $0.3* 10^{-3}$joules.

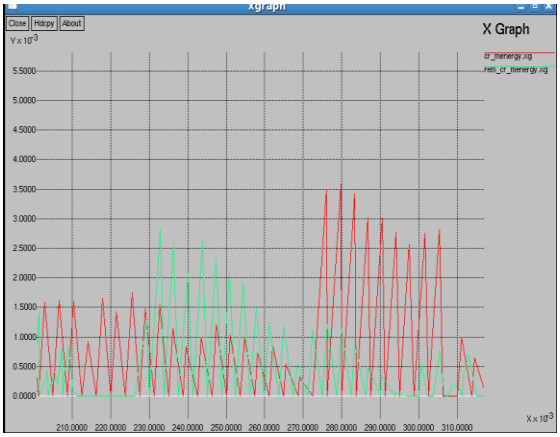

Fig 14: Graph of energy for cognitive radio and without attack removal

In cognitive radio and without attack removal the energy is $3* 10^{-3}$joules at 0.290 ms, whereas with attack removal and with cognitive radio the energy consumption is reduced to $0.3* 10^{-3}$joules.

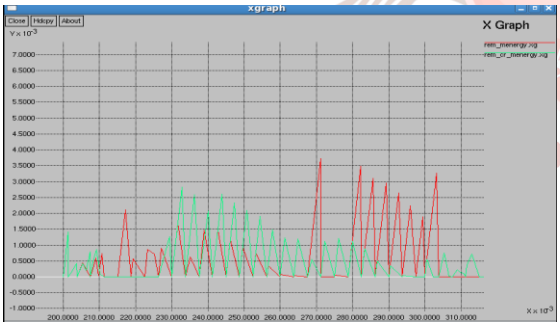

Fig 15: Graph of energy for without cognitive radio and attack removal

In without cognitive radio and attack removal the energy is $3* 10^{-3}$joules at 0.290 ms, whereas with attack removal and with cognitive radio the energy consumption is reduced to $0.3* 10^{-3}$joules.

Table 2:

Qualitative performance comparison

Sr No.	Parameters	Without attack removal and without cognitive radio	With attack removal and with cognitive radio	Without attack removal and with cognitive radio	With attack removal and with cognitive radio	With attack removal and without cognitive radio	With attack removal and with cognitive radio
1.	Delay	1.25 ms	0.3000 ms	3.100 ms	1.25 ms	3.50 ms	1.25 ms
2.	Throughput	Falls to 20% in 3-3.5s	Near about 100%	Falls to 20% after12.000s	Near about 100%	Falls to 20% in between 0.0-1.000s	Near about 100%
3.	Energy	$2.5* 10^{-3}$joules	$0.3* 10^{-3}$joules	$3* 10^{-3}$joules	$0.3* 10^{-3}$joules	$3* 10^{-3}$joules	$0.3* 10^{-3}$joules

CONCLUSION

CR technology can solve the problem of spectrum utilization. Here cross layer attacks in Cognitive Radio i.e spoofing and spying are detected and defeated using GI. With this GI technique the cross layer attacks in CRN are mitigated. The graphs of delay, throughput and energy are drawn and their values are evaluated. The delay and energy consumption is reduced, throughput is improved after applying cognitive radio and removal of attack and their respective values with graphs are shown.

REFERENCES

[1] Mukesh Barapatre, Prof. Vikrant Chole, Prof. L. Patil. "A Review on Spoofing Attack Detection in Wireless Adhoc Network". (IJETTCS)Volume 2, Issue 6 November-December 2013.

[2] Peng Zhang, Yixin Jiang, Chuang Lin. "P-Coding: Secure Network Coding against Eavesdropping Attacks". INFOCOM, 2010 Proceedings IEEE.

[3] Geethapriya Thamilarasu and Ramalingam Sridhar, "Exploring Cross-layer techniques for Security: Challenges and Opportunities in Wireless Networks" 2007 IEEE.

[4] Wenkai Wang and Yan (Lindsay) Sun, Husheng Li and Zhu Han. "Cross-Layer Attack and Defense in Cognitive Radio Network" Conference (Globecom 2010)

[5] Yawen Fan, Zhenghao Zhang, Matthew Trinkle, Aleksandar D. Dimitrovski, Bin Song, and Husheng Li. "A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids" 1949-3053 _c 2014 IEEEY.

[6] Pooja Dubey and Prof. Sapna Choudhury. "A Survey- Cognitive Radio Network Attacks & Preventions". (IJAFRC) Vol.1, Issue 2, Feb 2014. ISSN 2348 – 4853

[7] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks" IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, May-June 2013.

[8] Khaleel Husain, Premala Patil, "A survey on different cross-layer attacks and defenses in manets" IJRET eISSN: 2319-1163 | pISSN: 2321-7308.

[9] Wassim El-Hajj, Haidar Safa*l*, Mohsen Guizani. "**Survey of Security Issues in Cognitive Radio Networks".** Journal of Internet Technology Volume 12 (2011) No.2.

[10] Ms. Shikha Jain and Ms. Anshu Dhawan, Dr. C.K Jha. "Emulation Attack in Cognitive Radio Networks: A study". (IJCNWC), ISSN: 2250-3501 Vol.4, No2, April 2014.

[11] Hong-Ning Dai, QiuWang, Dong Li and Raymond Chi-Wing Wong, "On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas". International Journal of Distributed Sensor NetworksVolume 2013, Article ID 760834S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

IJRD
E-ISSN NO:2349-0721