A practical approach of DoS/Jamming attack of Cognitive Radio Network

*Roshan Singh Thakur
ABHA GAIKWAD-PATIL
College of Engineering,Nagpur
roshanthakur11@gmail.com

Prof. Parul Bhanarkar
ABHA GAIKWAD-PATIL
College of Engineering,Nagpur
parulbhanarkar@gmail.com

Prof. Girish Agarwal
ABHA GAIKWAD-PATIL
College of Engineering,Nagpur
mail2girishagarwal@gmail.com

Abstract:-In the wireless communication, DoS attack is general attack. DoS (Denial of Service) attack is an attempt in which an attacker makes a network resource unavailable to the licensed user. In this paper we focus on the DoS attack of CRN (Cognitive Radio Network) using 4G communication. Cognitive radio network is nothing but a network in which two users can access the same spectrum band.These users are called licensed and un-licensed user.

Keywords:- Denial of Service (DoS) attack, Cognitive radio network (CRN).

***Author for correspondenc**

I. Introduction

In the wireless communication, a latest generation is fourth generation (4G). A 4G system will be able to provide a comprehensive IP solution where voice, data and streamed multimedia can be given to users on an Anytime, Anywhere" basis, and at higher data rates than previous generations. [1].It provide many latest applications like wireless broadband access, Multimedia Messaging Service (MMS), video chat, mobile TV, High definition (HD)TV , Digital Video Broadcasting (DVB), minimal service like voice and data, and other streaming services for anytime-anywhere.4G provide high capacity network, at least 100 M-bit/s, easy handoff across heterogeneous networks and great connectivity. It provides global roaming across multiple networks. New 4G networks will enable powerful and innovative solutions for better protecting our first responders, providing them with the real-time information, the control, the reliability, the security and the performance that are at the core of mission critical technology[2]

Without spectrum no wireless communication is possible. In this spectrum, there are many channels. These channels are used by their intended user called licensed user but some time they use minimum channels

and rest of channels are idle. To utilized these idle channel by un-licensed user to consume the time and money by establishing another network. This concept of re-use of idle channel is called as Cognitive Radio Network. Cognitive Radio and 4G are two complementary issues that will frame on the world of wireless communications. 4G networks employing cognitive radios are a solution that revolutionizes the telecommunication industry, significantly changing the way we design our wireless systems and services. [3]
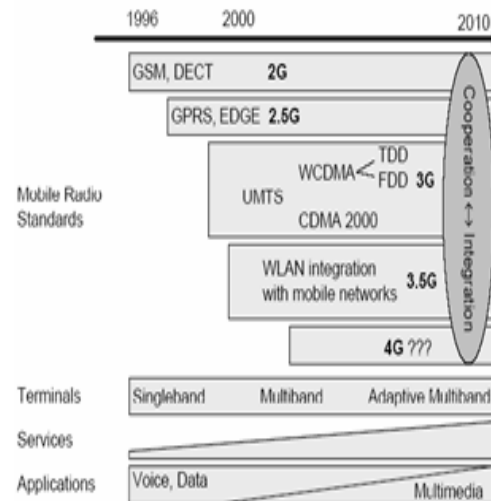

Figure 1: Evolution of 4G [3]

II. Cognitive Radio Network

CRs have the capability to sense their surroundings and actively adapt their operation mode to maximize the quality of service for secondary users while minimizing interference to primary users. [3] Cognitive radio offers the intelligent radios that can learn from and adapt to their environment. Data integrity and confidentiality can be handled by higher-layer cryptographic security, so here we focus on attacks fundamental to the cognitive radio itself, and independent of its higher-layer communications techniques. [3]
A cognitive radio is a radio that can change its transmitter parameters based on interaction with the environment it operates". [4]

In this Cognitive radio network, idle channels are called as white space or spectrum hole

Figure 2: Frequency Spectrum of Licensed User showing White Holes
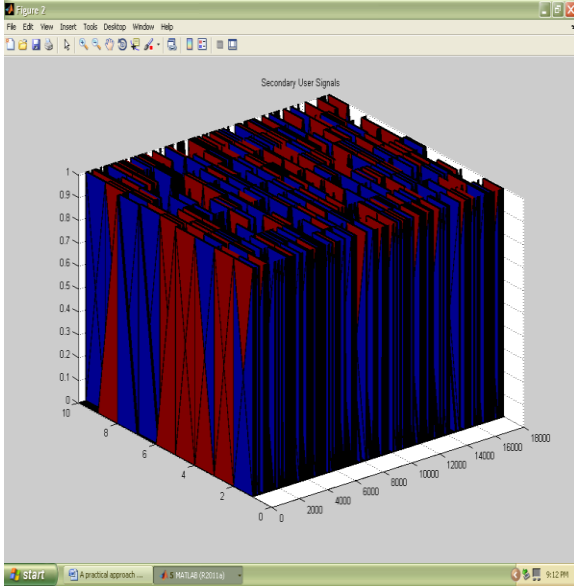
Figure 3: Frequency Spectrum of Licensed User in which Un-licensed user use above white holes.

III. Role of Cognitive Radio (Cr) in 4G.

When fully implemented, 4G is expected to enable pervasive computing, in which simultaneous connections to multiple high speed networks provide seamless handoffs throughout a geographical area. [3]As a feature of 4G,it

provide different facilities like wireless broadband access, Multimedia Messaging Service (MMS), video chat, mobile TV, High definition (HD)TV , Digital Video Broadcasting (DVB), minimal service like voice and data, and other streaming services for anytime-anywhere.4G provide high capacity network, at least 100 M-bit/s, easy handoff across heterogeneous networks and great connectivity, anywhere and anytime, so it is possible with the help of Cognitive radio because CR use every channels. Due to this 4G is far cheaper than 3G. With 4G systems there will be a need to design a single user terminal that can operate in different wireless networks and overcome the design problems such as limitations in size of the device, its cost and power consumption. This problem can be solved using Cognitive Radio approach i.e. user terminal adapts itself to the wireless interfaces of the network. [3]
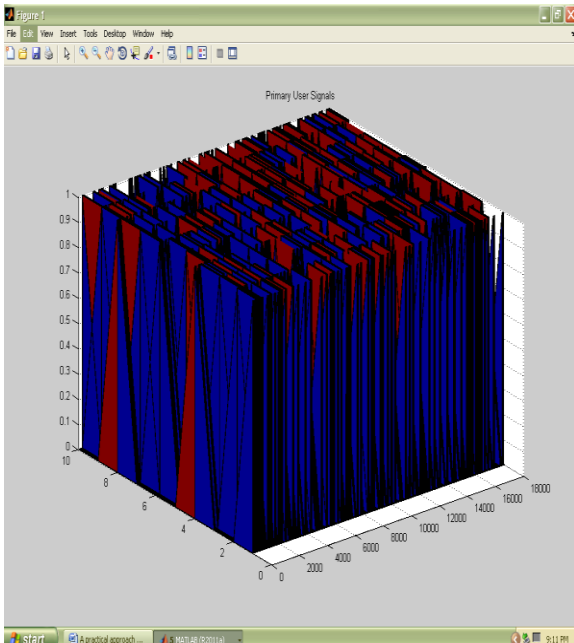
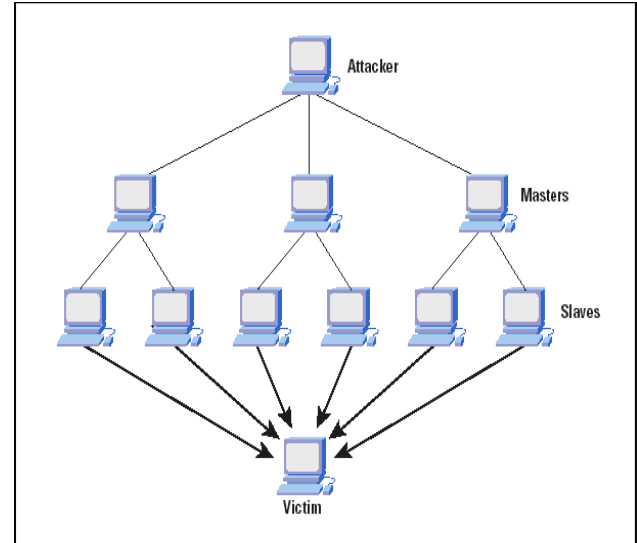## V. Denial of Service/Jamming Attacks in Wireless Networks

Figure: 4 Denial of Service attack in Wirless network

The goal of traditional DoS attacks is to overflow user in carrier sensing based networks (e.g. 802.11, sensor networks, etc.), a attacker might continually transmit electromagnetic energy on the medium, achieving the following two results: (a) the transmissions at the sender are deferred because the medium is sensed to be busy, and/or (b) the reception at the receiver is interfered with due to the jamming signals. Both these effects degrade the wireless network performance significantly. [17]

Jamming attack:
It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. If an attacker truly wanted to compromise your LAN and wireless security, the most effective approach would be to send random unauthenticated packets to every wireless station in the

network. To minimize the impact of an unintentional disruption, it is important to identify its presence. Jamming makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer. The increased noise floor results in a faltered noise-to-signal ratio, which will be indicated at the client. It may also be measurable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. From there the access points must be dynamically reconfigured to transmit channel in reaction to the disruption as identified by changes at the physical layer[18]

IV. Denial of Service (DoS) Attack of CRN

"DoS attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet" [5] .One general method of attack involves saturating or jam the target network with external communications requests or sending false data packets so much, so that it cannot respond to actual traffic, or responds so slowly or show as to be unavailable. These types of attacks usually lead to a server overload.

In general terms, DoS attacks are implemented by either forcing the targeted network(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.[5]
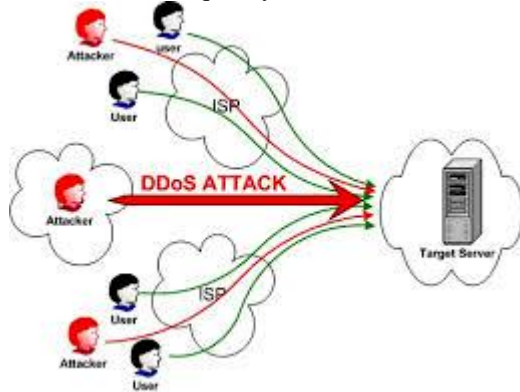

Figure 5: DoS Attack

In this practical approach,

```
Simulation time =5*60*60; 5 hours as 18000 samples,
No Of Channels=10;
PUsers=10;        % Number of Primary Users
SUsers=10;        % Number of Secondary Users.
PacketSize=128;   % Packet Size for transmission
SNR=1:3:21;       Signal to noise ratio
```

```
IntLev=0:16;      No.of intervals
BPSK=2;
Multipath=1;
Tx=1;             No.of transmitters
Rx=1;             No.of receivers
```

```
%Attack Detection Parameter
DoSData=(25e9)*(randn(1,SimTime* PacketSize));
AttDect=0;
```

```
%Wimax Parameter
fs=25e9 ;                %Sampling frequency
Ep=1;                    %Pulse Energy
tc=1e-9;                 %Pulse Width
Tf=PacketSize;           %Frame Length
Nf=4;                    %Pulse Repetition
Td=2;                    %Pulse Delay
Nc= NoOfChannels;        %Code Bin Number
 rc=.5e-9;               %time constant
t=-.3e-9:1/fs: 45e-9;
noise=(1e-50)*(randn(size(t)));  %(Noise-AWGN)Set to
1e-50 to disable
Fn=fs/2;                 %Nyquist frequency
 ht=(1/rc).*exp(-t/rc);  %impulse response
t=-5e-10:1/fs:5e-10;
a=tc /2.5;
Y=(1-(4*pi.*(t.^2))/a^2).* exp (-2*pi.*(t. ^2)/a^2) /
sqrt(Ep);
ln=length(Y);
```

```
dtpckt=DoSData(curFrame:curFrame+PacketSize-1);
%Detected spectrum hole
scode=zeros(1,PUsers+SUsers);
```

In this we will simulate whole project, like the DoS attack, and also we simulate and make cognitive radio network. Above coding in mat lab generate figure 4, 5 and 6.In figure 4 and 5; it is simply a PU's and SU's signal with white holes and with DoS attack simultaneously. In figure 6, Bit-error-rate vs Signal –to-noise ratio is shown, due to this when SNR increases the BER or Data packet has to be send decreases.
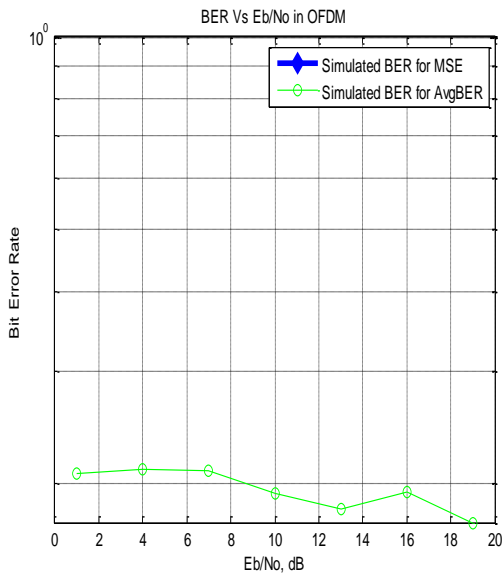
Figure 6 BER vs SNR graph.

VI. Conclusion

In this paper we analysis the DoS attack of Cognitive radio network in the platform of 4G.4G is a fourth generation network in which we access many application anywhere and anytime. Cognitive radio is very useful, because it provide cheaper and high capacity network. We can access empty channels of licensed user and provide facilities for 4G customers.In this paper we practically simulate the cognitive radio network using 4G spectrum band.In future we'll work on other attacks of cognitive radio network in 4G and make secure communication.

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/proje ctdescription.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] Denial of Service Attacks in Wireless Networks:The case of JammersKonstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy University of California, Riverside

[18] IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 5, Issue 3 (Sep-Oct. 2012), PP 13-20 www.iosrjournals.org www.iosrjournals.org 13 | P a g e Jamming Attacks Prevention in Wireless Networks Using Packet Hiding Methods Divya. S1, Manohar Gosul2