RESEARCH ARTICLE OPEN ACCESS

An Methodical Encroachment on Rooting out System for Networks

T.Augusty Chandija Lincy[1], Mrs. S. Murine Sharmili[2]
Francis Xavier Engineering College, Tirunelveli-627003, Tamilnadu, INDIA.

Abstract:

Cognitive radio network is a good network, which make only users of unlicensed spectrum to use software radio.This is for making the best use of the spectrum which is available and it is unused at the network. But there are still problems to security threats for the user which are using the spectrum. In this, a Cognitive Radio Network based on wireless network on regional area.It is designed and describes that some of the security needed alerts are working against it. This function of method uses a methodical identification of distributed DOS(denial of service) algorithm to deliver the case with high mobility with speed and high protection.Hence, the Secondary user's asked the desires are processed with very much higher probable. The behaviors of the un authorized users are safely prevent by the algorithm and packets with the packets are securely transmitted to the corresponding receiver.

Keywords — **Cognitive Radio Network,Denial Of Service.**

I. INTRODUCTION:

More attention is required on the development of dynamic spectrum access schemes because members of spectrum accessers are increased. In order to avoid spectrum scarcity a new networks called CRNs is designed. It has an opportunity to make use these vacant spectrum bands by changing its parameters dynamically. In which the primary users have the priority to access the channel any time because they are the users with a specific license to communicate over the allocated licensed band. The secondary users can access the channel as long as they do not cause interconnection to the primary users. Fig 1 shows that dynamic spectrum access in cognitive radio networks. The spectrums occupied by primary users are represented as shaded portion of cubes. The unused spectrum is represented as white spaces. These are also called as spectrum holes. The spectrum holes are detected by cognitive radio for secondary users. Various security threats are involved in this spectrum sharing policy in CRNs. In computer networking, a DoS attack or distributed denial-of-service attack (DoS attack) is a technique to make a network resource unavailable to its users. It generally consists of the efforts of more people to temporarily or indefinitely interrupt or suspend services of a node connected to the Internet. There are no inherent limitations in D-Dos attack in the number of machines that can be used to create the attack. This attack uses the distributed behaviour of the internet, with hosts owned by disparate entities around the world. These types of attacks are coming from IP addresses with wide range and it is more difficult to block and detect at the firewall level. This type of service attack is a huge problem in internet today. The DoS attack aims to disrupt some authorized activities, such as browsing web pages, transferring money from bank account etc. This denial-of-service effect is achieved by sending messages to the destination that can interfere with its operation, and can make it hang, crash, reboot or do unwanted work. This type of attack is quickly becoming more and more composite. There is a variety of known attacks which creates the impression that the problem space is immense, hard to explore and tackle. The existing systems employ various techniques to tackle the problem and it is difficult to understand their similarities and differences and to evaluate their effectiveness, performance and cost**.** But an efficient intrusion detection system for combating the attacks against CRNs has not yet been designed. Lack of research work on the intrusion detection system for CRNs is motivated to design effective IDS for cognitive unlicensed users. The proposed IDS use efficient detection distributed denial of service algorithm to avoid intrusion which is lightweight and is able to discover previously unknown attacks with significantly low detection latency.

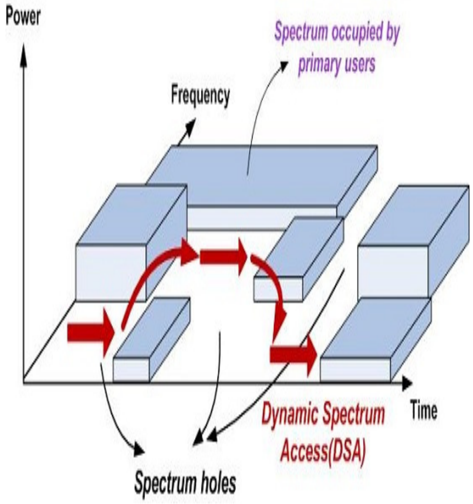

Power
Spectrum occupied by primary users
Frequency
Time
Dynamic Spectrum Access(DSA)
Spectrum holes

Fig.1. Dynamic Spectrum Access in CRN

II. PROBLEM DESCRIPTION AND PREVIOUS WORK.

It enables primary users detection in the presence of attackers in the spectrum and it approaches the integrates od method of cryptographic signatures as well as the link signatures. This approach uses a helper node which is placed very close to a primary user network. Due to the FCC constraint they cannot modify any primary user. But it provides some computational overhead. It is a rate adaptation scheme that is resilient to jamming attack in a wireless multi-hop tactical network. The detection of jamming attack improves the wireless link utilization and adapting the data transmission mode to the very successful data transmission probability.They have said the Detecting and TRAcing Back(DTRAB) scheme which is not limit to construct a apologetic mechanism to found out the attackers that detects not only a potential threat as well as investigation of the root of the threat by attempt the trace to back the attacker’s original area network. It have introduces 802.22 standard draft specification, its architecture, requirements, applications and coexistence considerations. These not only form the basis for the definition of this groundbreaking wireless air interface standard.It also serve as foundation,;mm for future research in the promising area of CRs. It has proposed adaptive selective method verification method which is an distributed adaptive mechanism for prevent attacker’s efforts to deny service to legitimate the user of clients. The level of area protection which employed by the clients is that they dynamically adjust to the current level of attack rates. At a high level of the attack, the clients exponentially rampup the number of requests they send in consecutive timewindows, up to a threshold which is maintained at the client. The server implements a reservoir-based random sampling to effectively sample from a sequence of incoming packets using bounded space.

III. PROPOSED INTRUSION DETECTION SYSTEM

Fig. 1 depicted the Cognitive Radio Network system model based on IEEE 802.22. This figure represents the television broadcasting of one tower only but multiple or many broadcasting towers may also be present. Here the TV (Television) companies have the license band of 44 to 706 MHz which is reserved for broadcasting data. So it is formulated as primary users of the system. Base station manages these networks which are having a number of cells. The service coverage radius of cells varies from 22 to 110km. Number of secondary users (i.e accessing unused spaces of spectrum which are only reserved for primary users) are supported by the cells presents in CRN. Due to different scenarios the unused spaces of the spectrum might occur. The unused spaces are also called as white spaces (i.e frequencies allocated to a broadcasting service but not used locally). In CRN each secondary user is equipped with a software radio also called cognitive radio to sense whether the primary users are currently occupying a channel or not. If the channel is occupied by the primary user, the secondary user has the ability to intelligently adapt his radio to another channel in order to sense the white spaces of that channel. The intelligent adaptation with the external environment is possible as the cognitive engine is able to continuously learn by utilizing online and offline learning policies. The plot in Fig. 2 shows that how the secondary users share the spectrum with the primary ones over time.

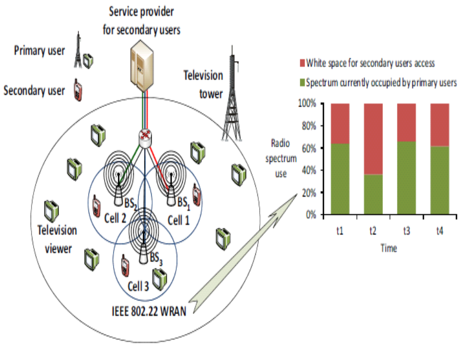


Fig.2.CRN architecture

- **Attacker Model**

The attacker operates as primary user emulator where it mimics the transmission signature of a primary user to take advantage of a secondary user's ability to avoid primary users. The secondary user is not allowed to transmit when a transmission with the signature of a primary user appears. The jammer takes advantage of this and launches a primary user emulation attack since the secondary user cannot determine if it is experiencing a true primary user or a malicious user. The attacker operates on four states similarly to secondary users. It starts out on a sensing state to detect primary users to prevent two primary user signatures to appear on one channel. Transmissions during a primary user's transmission can 33 cause the jammer to be detected. Operating without detection is ideal for a jammer. A secondary user will react to either a PU or a jammer so two transmissions is unnecessary. If a primary user exists the jammer changes channels, and starts the sensing process over. If the channel appears free of primary users the jammer will commence transmissions for a set period of time. If it detects a secondary user on the channel during this time it will place an award in that channel's to increase the probability that it will return to this channel. If no user is detected it will still transmit. It will then return to the sensing state on a new channel but no reward will be given. A full cycle of all of the user's states takes about one second. A rapid rate was chosen since prolonged contact with a secondary user is not beneficial. If the jammer is detected then it may continue on to the next channel because the secondary user acts purely on the appearance of a primary user signature so prolonged channel activity is unnecessary.

- **Learning Phase**

This phase learns the normal behavior of signal strength, flow of traffic, packet delivery ratio, accessing time of primary user in order to effectively detect unknown activities due to various types of hackers. The learned information's about normal cognitive radio conditions are stored by building a separate profile. The signal strength as well as packet delivery ratio is periodically monitored by the secondary users in order to identify attack. The information was carefully gathered to address the detection phase of the IDS that can determines unknown intrusions against the targeted CRN.

- **Detection Phase**

Algorithm: Detection of DDos attacks in CRN

```
Deploy the sensor nodes with cognitive radio platform randomly
Initialize the parameters such as sensor_id, energy, bandwidth, and routing protocol
The each secondary user senses the channel
If the channel is idle then
It transmit the data using the channel
Else channel is busy then
    Measure the received signal strength RSS=$P_tG_tG_r\frac{h_t^2h_r^2}{d^4L}$
    If RSS>threshold
    Primary user uses the channel
    Otherwise
        Malicious user access the channel
     End if
       End if
```

The algorithm depicted above represents the fast and secure protocol. It contains a sender, a receiver and an unreliable channel through which the sender and the receiver exchange data. At starting stage, sender is in the state of idle that is the secondary user sender does not have the data to transfer to its receiver. It needs to transmit the data to its receiver, first it checks the channel and then if the channel is free it takes the file to transmit as input. After that it splits the file into several packets then sends them to its receiver. The packets are waited in queue and transmitted. The packet is send continuously and it receives acknowledgement for each packet. The sender should send the packets simultaneously until receives any signal regarding the lost packet from receiver. If the lost packet signal is received by sender it retransmits the lost packet.

IV. PERFORMANCE ANALYSIS

The performance was evaluated in network simulator 2. Here the simulations are done using virtual machine with ubuntu operating system. The nodes are deployed at the bounded region of 1600 x 1600. The simulated traffic is Constant Bit Rate (CBR).

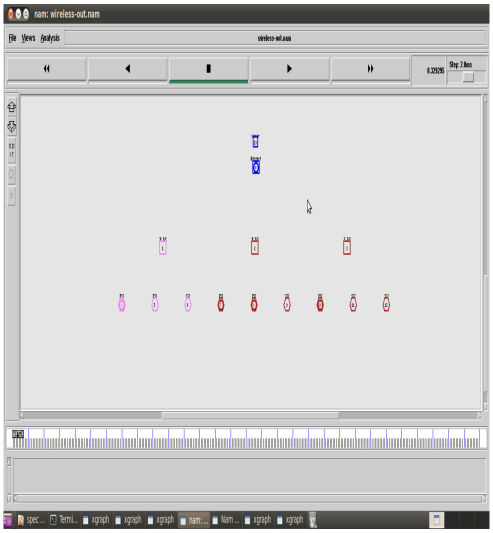


Fig .3. Network Formation

Fig 3 shows the network formation. Here the nodes deployed at the bounded region of 1600 x 1600. IEEE 802.16 is used as MAC protocol and for finding the routes dynamic source routing is used. Number of nodes deployed in this network is 14. Among that node 0 is a router, node 13 is a server and node 1, 2, 3 is act as primary and secondary base stations and other nodes are act as either primary or secondary users.

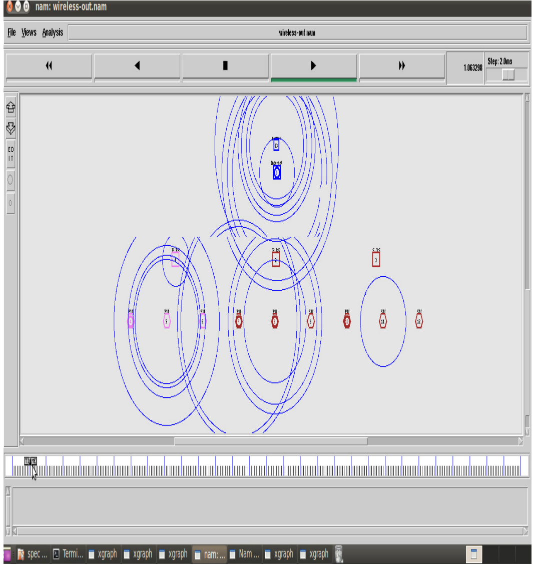


Fig.4.Data Transmission

Fig 4 shows the data transmission from server to primary or secondary users. The data is transmitted from server to client. The clients request the data to their respective base station.

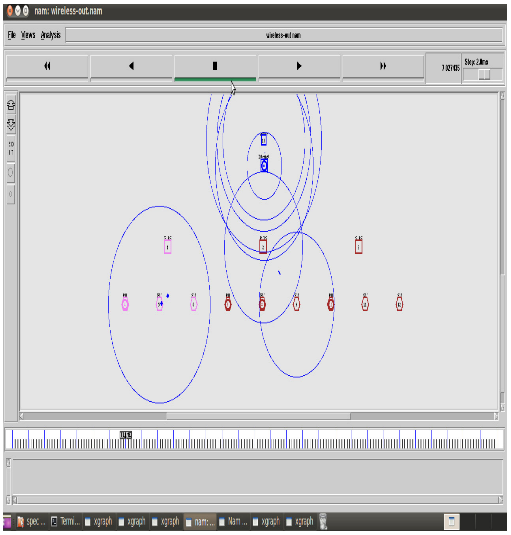


Fig.5.Packet loss due to attackers

Fig 5 shows packet loss due to attacker. Here the primary and secondary users are presented. The secondary users sense the spectrum of primary users and if the primary users spectrum is free then it transmit or receive the data from server using that channel. Suppose the secondary user is attacked by some malicious activities it may occupy the free space of spectrum of primary users and does not allow the primary users to access the spectrum again it comes to transmission. This type of attack is known as denial of service attack. Due to this attack the data transmitted to one primary user is dropped.

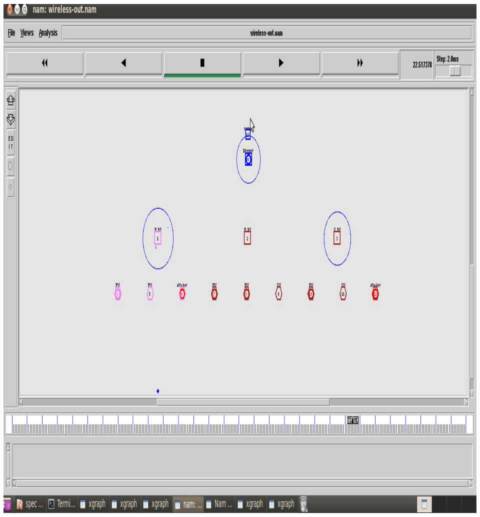
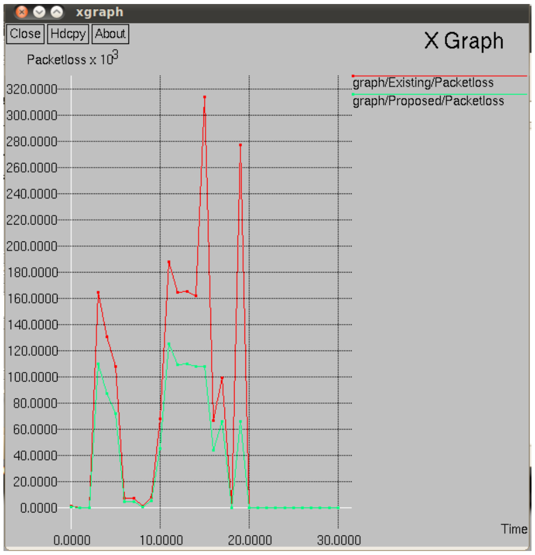


Fig.6.Attacker Node detection

Fig 6 shows the attacker node detection. The secondary users sense the spectrum of primary users and if the primary users spectrum is free then it transmit or receive the data from server using that channel. Suppose the secondary user is attacked by some malicious activities it may occupy the free space of spectrum of primary users and does not allow the primary users to access the spectrum again it comes to transmission. This type of attack is known as denial of service attack. Due to this attack the data transmitted to one primary user is dropped. The detection of denial of service is important. Here the node 6 and 10 are the attacker nodes.



Fig,7.Packet loss

Packet loss is the failure of one or more transmitted packets to arrive at their destination. Fig 7 shows the packet loss graph. The graph shows the comparison of existing system packet loss and proposed system. The red color line indicates the existing system packet loss. In this the packet loss can be decreased as the time increases. The green color line indicates the packet loss of proposed system. There is no packet loss in the proposed system.

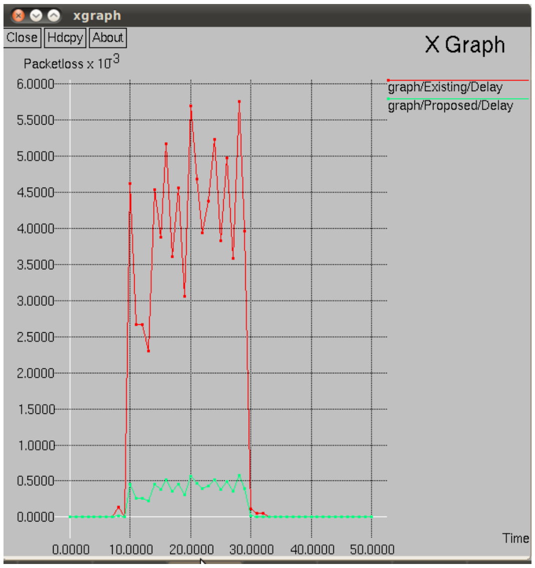


Fig.8.Delay

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. Fig 8 shows comparison graph of delay between existing detection and proposed detection method. From the observation of this graph the delay occurred in proposed method is less compared with existing.

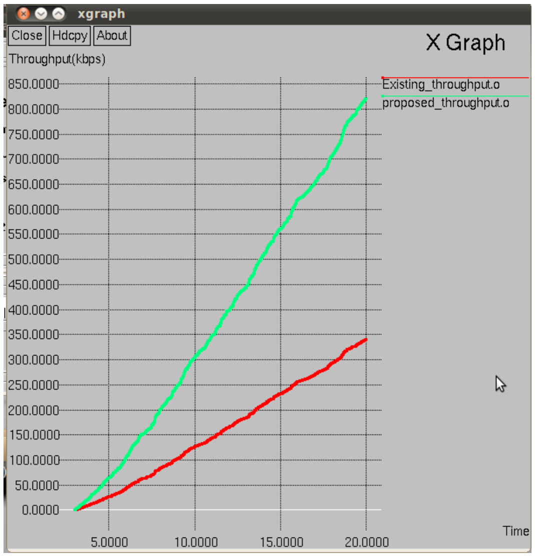


Fig.9.Throughput

Throughput is a term used in information technology that indicates how many units of information can be processed in a set amount of time. Fig shows the throughput graph. The throughput graph is plotted between time versus throughput (Kbps). Comparing with existing method this proposed method provides better throughput.

CONCLUSION:

The proposed system is based on efficient detection of distributed denial of service algorithm which is highly adaptive to the arriving attack rates. The levels of protection employed by the secondary users are dynamically adjusted to the current level of attack rates. Here the secondary user can always complete the sending and the receiver can always receive the data successfully under the presence of attackers also. This system sends the data with high rate of transmission. The performance of this protocol provides higher throughput, less loss rate and high reliability.

REFERENCES:

[1] Sanjeev Khanna, Santosh S. Venkatesh, Member, IEEE, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, Senior Member, IEEE, Member, ACM- ―Adaptive Selective Verification:An Efficient Adaptive Countermeasure to Thwart DoS Attacks‖,IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 3, JUNE 2012

[2] ZHANG FU- ―Multifaceted Defence Against Distributed Denial of Service Attacks: Prevention Detection‖, Mitigation, Division of Networks and Systems Department of Computer Science and Engineering CHALMERS UNIVERSITY OF TECHNOLOGY Gothenburg, Sweden 2012

[3] M. Abadi, M. Burrows, M. Manasse, and T.Wobber, ―Moderately hard,memory-b functions,‖ Trans. Internet Technol., vol. 5, no. 2, pp. 299–327, 2005.

[4] C. A. Gunter, S. Khanna, K. Tan, and S. S. Venkatesh, ―DoS protection for reliably authenticated broadcast,‖ presented at the NDSS, 2004

[5] M. Arshey, C.Balakrishnan, ―Adaptive defense strategy: immunizing shared channel network from dos attacks‖.International Journal of Emerging Technology and Advanced Engineering , vol. 3, no. 1, pp. 209,2013.

[6] www.icacci-conference.org

[7] SonicWALL, Inc.1160 Bordeaux Drive Sunnyvale, CA 94089-12091-888-557-6642 http://www.sonicwall.com

[8] M. AlTurki, J. Meseguer, and C. A. Gunter, ―Probabilistic modelling and analysis of DoS protection for the ASV protocol,‖ Electron. Notes Theoret. Comput. Sci., vol. 234, pp. 3–18, 2009.

[9] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing Cognitive Radio Networks," Int'l. J. Commun. Systems, vol. 23, no. 5, May 2010, pp. 633–52.

[10] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," J. Internet Technology (JIT), vol. 12, no. 2, Mar. 2011, pp. 181–98.

[11] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," Int'l. J. Network Security, vol. 5, no. 3, Nov. 2007, pp. 338–46.

[12] B. Kannhavong et al., "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Commun., vol. 14, no. 5, Oct. 2007, pp. 85–91.

[13] Z. M. Fadlullah et al., "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis," IEEE/ACM Trans. Net., vol. 18, no. 4, Aug. 2010, pp. 1234–47.

[14] K. Ju and K. Chung, "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks," Int'l. J. Security and Its Applications, vol. 6, no. 2, Apr. 2012, pp. 149–54.

[15] Yao Liu, Peng Ning Huaiyu Dai "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures", iscovery.csc.ncsu.edu/pubs/Oa-kland10.pdf

T. Augusty Chandija Lincy was born in Tirunelveli, Tamilnadu, India, in 1994. She received the B.E (Electronics and Communication Engineering) from Francis Xavier Engineering College ,Tirunelveli. She currently pursuing her Post Graduate programme in Communication System from Francis Xavier Engineering College. Her major research interests are Digital and Image Processing and Embedded system.

S. Murine Sharmili was born in Coimbatore, Tamilnadu, India. She received the B.E(Electronics and Communication Engineering) from Government College of Engineering, Tirunelveli, India in 2010 and doing the M.E(Communication Systems) in Francis Xavier Engineering College, Tirunelveli, India in 2018.