An Attack Aware Cross Layer Routing Protocol for Multi-hop Cognitive Radio Network

Neha P. Gogulwar
PG student, Dept.of Electronics and Communication Engg. Ballarpur Institute Of Technology, Bamni
Ballarpur (M.H) India

Ashish R. Manusmare
Assistant Professor, Dept.of Electronics and Communication Engg. Ballarpur Institute Of Technology, Bamni
Ballarpur (M.H) India

ABSTRACT
Cognitive Radio Networks (CRNs) with such spectrum aware devices is a confident key to the spectrum insufficiency issue in wireless communication area. In this, an effective routing solution with a cross layer design is proposed for the multi-hop CRNs. The existing work uses Ad-hoc On-demand Distance Vector (AODV) routing protocol for CRNs. In cognitive radio based networks there are cross layer attack which occur due to DDOS (Distributed Denial of Attack) because of this attack efficiency is reduce. DDOS attacks which occur on cross layer routing is the biggest issue in cognitive radio . In this scheme present work is on layer for attack removal in the cross layer networks which will allow the system to offer high efficiency in routing even under attacks This will help the network to perform effective routing even if DDOS attack occur. MATLAB simulation result shows the parameter: Energy, Throughput and Delay this parameter signified graphically which shows result with attack and after removing attack the system efficiency is enhanced.

Keywords
Cognitive Radio Network, Cross layer Routing, DDOS, Multi Hop Cognitive Radio Network, RPL

1. INTRODUCTION
Cognitive Radio (CR) is an developed wireless communication model that can significantly improve the spectrum custom efficiency by offering active spectrum access. Cognitive radio networks (CRNs) are composed of cognitive, spectrum devices capable of changing their formations on the wing based on the spectral environment. In this a CR technology is provided followed by a detailed analysis of the attacks pointing Cross layer Routing protocol for multi hop cognitive radio network. The attacks aware with respect to the layer they target starting from the physical layer and moving up to the transport layer. This project worked on this layer and aware from the attack which occur on the cross layering this will improve the efficiency of network..

2. LITERATURE SURVEY
Irin Sajan , Ebin M. Manuel (feb 2015)[1] In this paper existing an effective routing solution with a cross layer design is proposed for the multi-hop CRNs. Most of the existing work uses Ad-hoc On-demand Distance Vector (AODV) protocol as the routing protocol for CRNs. In this work, a novel routing algorithm based on Routing Protocol for Low power and lossy networks (RPL) is being proposed for the CRNs. Routing is accomplished through the formation of colored Destination Oriented Directed Acyclic Graphs (DODAGs) of which the link frequencies are represented using colors. Hop count and adjacent link interference are counted as the routing metrics. Dynamic spectrum allocation is also done along with routing with the help of RPL. The CRN scenario is vulnerable to link failures due to the appearance of Primary Users (PUs). So route repairing using the Trickle algorithm offered by RPL. RPL is found to be a suitable routing protocol that can be carried out into the real CRN scenario**.**

Trong Nghia Le,[May 2015][2] In this paper, the channel-tap power is utilized as a radio-frequency fingerprint (RF) to completely identify primary user emulation attacks (PUEAs) over multipath Rayleigh fading channels. To accurately know identities of primary users (PUs) and PUEAs, the cross-layer intelligent learning ability of a mobile secondary user (SU) is exploited to establish detection databases by seamlessly combining the quick detection of physical (PHY) layer with the accuracy of higher layer authentication. The proposed method helps PHY layer completely detect the identities of PUs and PUEAs**.** The uniqueness of channel-tap powers between the SU and Txs is utilized as a RF to detect PUEA and PU in mobile CR networks. In addition, this letter proposes cross-layer design to completely detect PUEA and PU based on detection databases established by seamlessly combining the accuracy of higher layer authentication with the quick detection of PHY layer. Simulations demonstrate that the proposed technique greatly enhances detection efficiency of PHY layer.

Ramzi Saifan, Ahmed E.Kamal[3] A Cross-Layer Routing Protocol (CLRP) for Cognitive Radio Network routing protocols proposed in literature are partially cross-layer, because the information flow is only from physical layer to network layer, e.g., about channels availabilities. In this work, we introduce a cross-layer routing protocol (CLRP), which considers both the channels that are known to be available at each node, as well as other channels that may be available. The availabilities of the latter channels are considered using a stochastic approach. CLRP computes an end to end path, and feeds the physical layer with information about which channels to sense and which nodes should perform the sensing, such that the expected route quality is enhanced. Simulation results show that CLRP outperforms other cross-layer routing protocols in terms of throughput and stability of the path being setup, and increases the probability of finding an end-to-end path. In this paper we proposed a new approach for routing in CRN.

Azza Mohammed[Sep. 2015][4] MANET Mobile Ad hoc Network are evolved through various characteristics such as shared media, this property make a routing protocols vulnerable. AODV is a reactive routing where each intermediate node cooperates in the process of route discovery. In this case, the node that behaves as malicious exploit the malfunction of specified service. The black hole

attack uses the sequence number that is used to select the freshest route and attract all exchanged data packets to destroy them. Many researchers have dealt with this attack and many solutions have been proposed. These solutions target the network layer only. In this paper, we present our approach to counter black hole attack. This approach is entitled Cross AODV and it is based on verification and validation process. The key point of our approach is the use of the inter layer interaction between networks layer and medium access within the distributed coordination function (DCF) to efficiently detect and isolate malicious nodes. During the route discovery, the verification process uses the RTS or CTS frame that contains information about the requested path. The validation process consists of comparing the routing information with the result of verification phase**.** Our Approach have been implemented, simulated and compared to two related studies using the well know NS2 Simulator. The obtained results show the efficacy our proposal in term of packet delivery with a neglected additional delay.

3. RELATED WORK

3.1 Introduction

Development of a wireless sensor network which is consist of number of nodes that sense the data and communicate with each other**.** Wireless sensor networks consisting of cluster which is used to prolong the lifetime of network. Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components. A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing. WSNs can be deployed on a global scale for environmental monitoring and habitat study, over a battle for military surveillance and inspection, in emergent environments for search and rescue, in factories for condition based maintenance, in buildings for infrastructure health monitoring, in homes to realize smart homes, or even in bodies for patient monitoring.

Clustering is main technique, consist of group of nodes. Cluster having node with maximum energy becomes cluster head. The set of cluster head in a WSN forms its backbone, providing a scalable solution to various networking tasks, such as data collection and habitat monitoring. At each cluster, a cluster head is responsible for various tasks, e.g. data transmission.

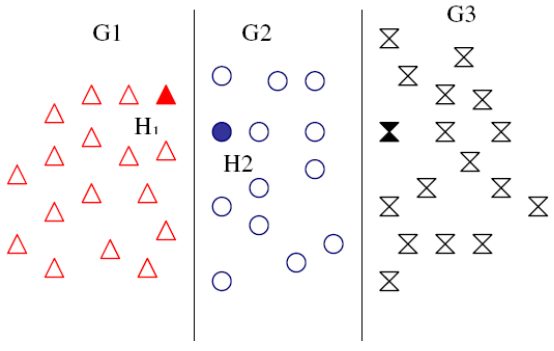
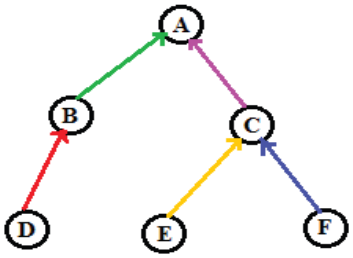


Fig. : Multiple Cluster-head in small region

CR Networks is a spectrum aware devices to the spectrum scarcity issue in wireless communication. Cognitive radio networks (CRNs) are composed of cognitive, spectrum devices capable of changing their configurations on the wing based on the spectral environment. This capability opens up the possibility of designing flexible and dynamic spectrum access strategies with the purpose of opportunistically reusing servings of the spectrum temporarily vacated by licensed primary uses. This work focuses on the problem of an attack aware cross layer routing. CR technology is provided followed by a detailed analysis of the security attacks pointing Cross layer Routing protocol for multi-hop cognitive radio network.

RPL is a distance vector routing protocol for LLNs. Network devices running the protocol are connected in such a way that no cycles are present. For this purpose a Destination Oriented Directed Acyclic Graph (DODAG), which is routed at a single endpoint is built. It is the main candidate for acting as a standard routing protocol for Internet Protocol (IP) smart object networks. RPL is based on the topological concept of Directed Acyclic Graphs (DAGs). In this algorithm, routing is achieved through the construction of a colored Destination Concerned with DAGs (DODAGs) with destination as the root and source(s) as the leaf node(s). Connection rates are represented using different It controls the best route from a source to destination. The algorithm selects the path with the minimum hop count and the minimum adjacent link interference as the best path. Also, two nodes will communicate in a CRN only if there exists a common channel between them.



Routing protocol for low power and lossy network's

A cross-layer routing protocol (CLRP), which considers both the channels that are known to be available at each node, as well as other channels that may be available. The availabilities of the latter channels are considered using a stochastic approach. CLRP computes an end to end path, and feeds the physical layer with information about which channels to sense and which nodes should perform the sensing, such that the expected route quality is enhanced. Routing in CRN requires cross layer design, where route decision that is done in the network layer should be established on the channels availability collected by the physical layer through sensing. In CLRP the network layer and the routing protocol do not coach the physical layer about which channels to be sensed. CRN cross layer routing protocols where the information flows in both directions between the physical and network layers. The physical layer informs the network layer of the initial channels available, and the network layer informs the physical layer which channels to be sensed, while taking the sensing.

3.2 Implementation

3.2.1 Design Wireless Network

In this module designing of wireless Network with 30 nodes is shown in fig 3.2.1 and these are communicating with each other without any proper communication path so it required more energy to transmit the data from source to destination.

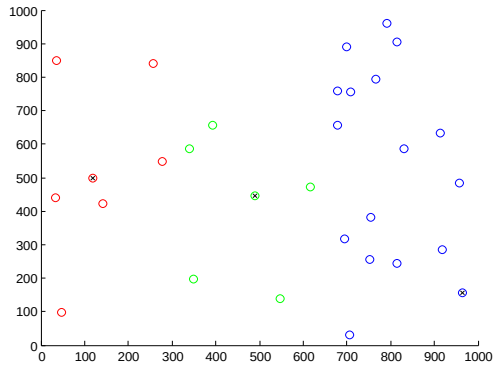


Fig: 3.2.1 Design Wireless Network

3.2.2 Design of Cognitive Radio Network:

In this module designing of the Cognitive Radio Network with 30 nodes which is shown in fig 3.2.2 which is consist of Primary User and Secondary User. The cognitive radio technique provides the opportunity for unlicensed users to share the radio spectrum with licensed users without degrading their services the fundamental objective of cognitive radio is to identify sub-bands of the radio spectrum that are currently unemployed and assign them to unlicensed secondary users**.**

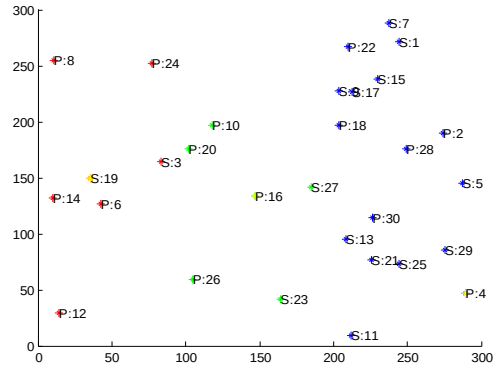


Fig: 3.2.2 Design of Cognitive Radio Network

3.2.3 Design of DDOS Attack

After creating a CR network as shown in fig 3.2.2 user will be divided into primary and secondary. Primary user will be allotted the channels while secondary user will be sensing the channel to get the free space. In case of any attack, the router will check the network layer and apply DDOS removal on network layer so that there is no interference on the routing layer. If attack occurs on the routing layer, then the packet is dropped and the network layer is informed, so that no further packets are accepted from that particular source. Figure 3.4 shows the Node discovery in the network for 30 numbers of nodes. The topology area for scenario is 300*300m with packet size of 1000 bytes**.** After routing in the network The fig3.2.3 shows DDOS attack which occur on node no 18 .Here first node no 18 detect all the nodes , blue color line shows all the node are detected by node no.18.After few second some DDOS attack detect on some node which having attack this attack is shown by red colour line .After removing this attack the graphical output is produced which shows the parameter like : Energy ,Throughput ,Delay .In this graph red line shows attack on node and green line shows after attack removal on the node. There is some changes which increase in network life time and enhance the network performance.

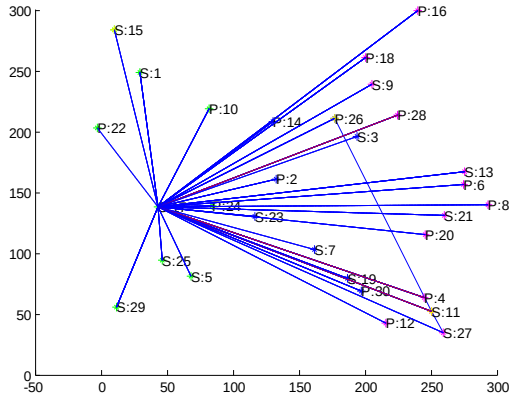


Fig: 3.2.3 DDOS Attack occur on node no.18

4. RESULTS

To analyze this project we have implemented a Cognitive radio network on Matlab Simulation consisting of 30 wireless nodes and area for scenario is 300*300m. Figure below shows the graphs for with DDOS Attack and without DDOS attack..The red color in the below shown graphs, shows with DDOS Attack and the green color shows the results after the Attack Removal.

Table 4.1: Comparison table

Parameter / DDOS	Energy	Throughput	Delay
With Attack	High	Low	High
After Attack (Removal)	Low	High	Low

4.1 Energy

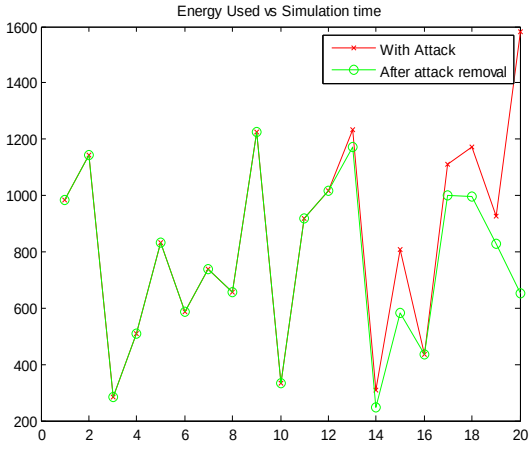


Fig:4.1 Comparative graph for energy.

The graph for energy with 30 numbers of nodes is shown in figure 4.1;in this x axis represent time (sec) ,y axis represent

energy (mJ) it indicates that Energy Consumption Decreases after attack removal so it improve the network lifetime.

4.2 Throughput

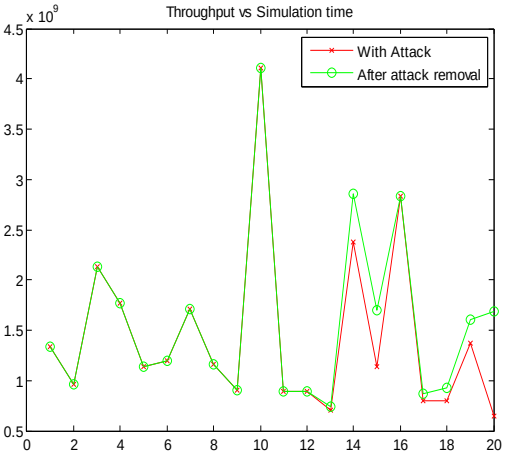


Fig:4.2 Comparative graph for Throughput.

Throughput is the amount of data transferred in a given period of time. In Figure,4.2 x axis represent time (sec) and y axis represent (Kbit/sec). The graph for throughput with 30 numbers of nodes is shown in figure 4.2; it indicates that throughput increase after attack removal.

4.3 Delay

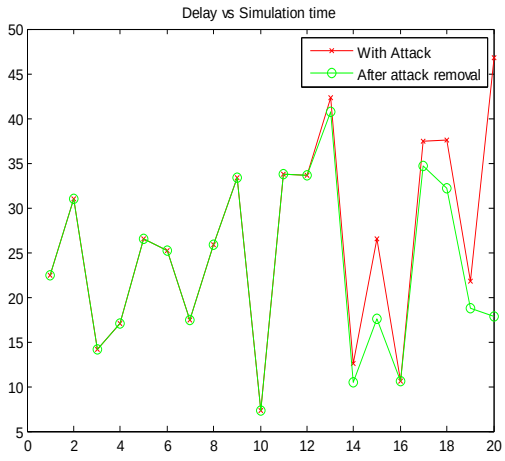


Fig:4.3Comparative graph for Delay

In Figure 4.3 x axis represent time (sec) and y axis represent delay (sec) average end-end delay with 30 numbers of nodes is shown in fig. It indicates that delay decreases after attack removal.

5. CONCLUSION

This article investigated issues arising in the cross layer routing protocol in multihop cognitive radio network. In this

the attack is occur on cross layer because of this attack efficiency of network is decreases. So the main aim of this project is to concentrated on the issue of cross layer design for routing in cognitive radio which have DDOS attacks .After removing this attack by using algorithm and working on the layer which have DDOS attack the efficiency of the network is increases. A Simulation is done in MATLAB and are analysed on the basis of critical parameters: Energy, Throughput, Delay. After analysing the graphs it shows that after removing of attack the efficiency of the network will increase. So it improves the network lifetime and increase energy in the network. In future researcher may concentrate on data transmission scheme to facilitate high throughput, high packet delivery ratio and minimum end to end delay in complex scenarios.

6. ACKNOWLEDGMENTS

Our thanks to the Ramzi Saifan, Ahmed E.Kamal , Azza Mohammed, Irin Sajan , Ebin M. Manuel, Trong Nghia Le who have contributed towards development of the template.

7. REFERENCES

[1] Irin Sajan, Ebin M. Manuel [Feb 2015] , "Cross Layer Routing Design Based On RPL For Multi-Hop Cognitive Radio Networks" 978-1-4799-1823-2/1/$31.00 ©2015 IEEE

[2] Trong Nghia Le,[May 2015] "Cross-Layer Design For Primary User Emulation Attacks Detection In Mobile Cognitive Radio Networks" IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 5, MAY 2015 Wassim El-Hajj, Haidar Safa,[March 11] "Survey Of Security Issues In Cognitive Radio Networks" JOURNAL OF INTERNET TECHNOLOGY · MARCH 2011

[3] Ramzi Saifan, Ahmed E.Kamal "A Cross-Layer Routing Protocol (CLRP) For Cognitive Radio Network."

[4] Azza Mohammed[Sep. 2015] " A Cross Layer For Detection And Ignoring Black Hole Attack In MANET" 10.5815/Ijcnis.2015.10.05

[5] Wang Weifang "Denial Of Service Attacks In Cognitive Radio Networks" 2010 2nd Conference On Environmental Science And Information Application Technology

[6] Hicham Khalife, Naceur Malouch, Sergfdida[8/10/2010] Multihop Cognitive Radio Networks: To Route Or Not To Route IEEE Network, Institute Of Electrical And Electronics Engineers, 2009, 23(4), Pp.20-25.<10.1109/MNET.2009.5191142>.<Hal 00524785>

[7] Trong Nghia Le,[May 2015] "Cross-Layer Design For Primary User Emulation Attacks Detection In Mobile Cognitive Radio Networks" IEEE Technology Communications Letters, VOL. 19, NO. 5, MAY 2015

[8] Tsvetko Tsvetkov[July 2011] "RPL: Ipv6 Routing Protocol For Low Power And Lossy Networks" 10.2313/NET-2011-07-1_09

[9] Natarajan Meghanathan [2013]A Critical Review Of The Routing Protocols For Cognitive Radio Networks And A Proposal For Load Balancing Local Spectrum Knowledgebased Routing , Doi : 10.5121/Csit.2013.3702