A NOVEL APPROACH AGAINST BLACKHOLE ATTACK IN AODV PROTOCOL FOR WIRELESS NETWORKS

Nishant Doshi[1], Girish Tiwari[2]

[1]*PG Scholar, Department of Electronics & Communication Engineering, Ujjain Engineering College Ujjain, Sanwer Road line Ujjain, India*

[2]*Associate Professor, Department of Electronics & Communication Engineering, Ujjain Engineering College Ujjain, Sanwer Road line Ujjain, India*

Abstract

In present current situation Cognitive Radio (CR) is new evolving and very popular technology due to its intelligent working. It has become one of the best available options for many of the problems faced today in other technologies. In addition to this, for data security, this is most preferable option. In this paper we have presented a unique and generalized solution for one of the attack i.e. blackhole attack. We have dealt in this paper with parameters PDR and Throughput. This paper also tells about the importance of cognitive radio in present scenario about various features of CR like spectrum sensing, management, mobility, sharing and many more. There is description about the blackhole attack. Then in later part of the paper we have shown through graphs our simulated result in which there is comparative analysis of the previously applied algorithm. There is improved version of the algorithm and it is showing the better performance as we got result in our simulations.

Keywords: *Black Hole, Cognitive Radio, AODV Routing, PDR, Throughput*

----------***----------

1. INTRODUCTION

In Cognitive radio [1] (CR) there is considerably higher expectations than any other because of its features. Most important features of CR are its learning, adaptability, awareness, intelligence, reliability, reconfigurability. There are sorts of technologies which are distinctly classified like digital signal processing (DSP), Software defined radio (SDR), networking, computer software and hardware and machine learning helped to bring these features together in the form of Cognitive radio.

SDR: It works through the usage of software to keep trace on working of communication system of radio. It includes the sorts of parameters like frequency used for carrier and message signal, modulation process and its type, bandwidth of channel, also the network access, and this whole process is done using software. Nowadays these SDR systems are being performed many more functions in addition to previously doing functions viz. Cryptography for decoding, Forward Error Correction, Source Coding of Voice, Video or Data for live streaming, and Coding for code detection.

Some of the definitions are being offered by the various regulatory bodies and several working groups on SDR technology. SDR [2] may also be defined as: "The radio which contains transmitter having the parameters for its operation of modulation type, range of frequencies used, or the output power used maximum for operation, or a kind of condition in which operations of transmitter can be changed or modified by doing a little in the software itself and it donot need to make any further modifications into the hardware components which in turn will affect the emissions of radio frequencies."

However, there are many certain problems with this network of attack but it is due to usage of AODV protocol usage. Though the protocol is vulnerable to different types of attacks but we cannot avoid this due to its better performance in various parameters i.e. PDR, Throughput and End to End delay. But in this different types of attack are inevitable. Thus there are many researches going on for its appropriate solution which can become the best solution available to this problem of attack.

2. RELATED WORK

CR is an intelligent technology which can also be utilized by the secondary users to utilize the bandwidth of spectrum for their usage and ensuring that no interference is experienced by primary users. CR is the best technology evolved in the field of wireless communication; in this technology either wireless node or network gets changed. In addition to this either its receiver or transmission parameters preventing any kind of interference between a primary user i.e. licensed user and the secondary user i.e. unlicensed user. The cognitive radio operates on technique of efficient utilization of spectrum. In fact it makes a very good usage of spectrum utilization is regulated by government agencies in many countries across the whole world because of limited resource of the spectrum they are:

- Telecom Regulatory Authority of India (TRAI) in India.
- Federal communications commission (FCC) in United States.
- Post of Telecom Services (PTS) in Sweden.
- Bangladesh Telecommunications and Regulatory Commission (BTRC) in Bangladesh.
- Canadian Radio television and Telecommunications Commission (CRTC) in Canada.

Many more countries have their own regulatory bodies. In reality, the spectrum is not being properly utilized even in very densely populated city areas. According to FCC, there are spectrums which are available not utilized greater than 70%. Thus to enhance the level of the utility of the spectrum; there can be two kinds of users:

1. Primary users (licensed users)
2. Secondary users (unlicensed users).

If any assigned spectrum partially or fully cannot be used effectively partially or completely by the licensed users then that part is which cannot be utilized in a spectrum is known to be a white space or a spectrum hole. However CR locates these and allots it to secondary users ensuring no obtrusion happens to any licensed users. Hence CR is a better technique to manage the efficient usage of RF spectrum. The licensed and unlicensed users are being able to utilize the frequency spectrum using cognitive radio [5] technique. Secondary user plea to the primary user for few usage of spectrum, and then if Primary user wants, then it can allocate the spectrum to the secondary users by its own without degradation in its own performance using spectrum sharing techniques.

2.1 Learning and Decision Making

CR has a skill of collecting and sensing information of its surrounding environment, then to make decision in certain situations and take particular action, for giving better performance in new situations it learn from past experiences. For collecting the information of a rapidly changing radio environment, and to neglect obtrusion to other users, the radio requires advancement in techniques it is using. More sophisticated techniques are needed. Decision making is based on previous results and observed parameters from the environment.

As stated in [10] the CR will enable the user:

- **Spectrum Sensing**: It determines about the availability of portions of the spectrum and also it is able to identify the existence of licensed users when the usage of primary user is in a licensed band.
- **Spectrum Management**: It always selects the best available channel to provide user‘s communication requirements**.**
- **Spectrum Sharing:** It maintains the coordination of the channel access among the other users**.**
- **Spectrum Mobility**: It empties the channel whenever any licensed user is detected**.**

3. AODV PROTOCOL

This is a protocol which comes under category of reactive unicast routing protocol. It is descendent of Destination Sequenced Distance Vector Protocol (DSDV) [4]. Being a reactive routing protocol, it is only required to see after routing information about the active routes. In Ad Hoc On-demand Distance Vector Routing (AODV) [3], the routing information is maintained in the Routing Table (RT) for all the nodes in the network. Every mobile node has address of next hop in the RT, which is having the destination address to which it is currently having a pathway. A RT values get exhausted if it has not been soon activated again or reused for a particular pre-defined exhausting time.

In AODV, whenever a source node requires initiating the communication but no path is in existence then, it just starts a path searching operation. In this operation the discovery of route, the source nodes send RREQ packets which include Destination Sequence Number (DSN).

Whenever destination **no**de or an intermediate node is having path to destination, it fetches the RREQ, it checks the DSN which it is having presently and that also which is specified in the route request. In order to ensure the updation of the routing information, a RREP packet is created and forwarded back to the source only if the DSN is equal to or greater than the specified in RREQ.

The symmetric links are used in Ad Hoc On-demand Distance Vector Routing and a route reply follows the reverse path of the respective route request. On receiving the route reply packet, every intermediary node with the path maintains and updates the next hop address of it, and database of destination node respectively. The redundant rote reply packets or packets with lower DSN will be dropped.

3.1 Working of AODV

Use hello messages for local connectivity maintenance.
It uses a RT with [destination sequence number, next hop, destination id, life time].

- Forward path setup.
- Backward path setup.
- Route failure, RERR.
- Route expires after route life time.

Can receive multiple RREP, will use only with recent seq. no or smallest hop no.

AODV protocol permits movable nodes to search and get path for new destinations quickly; also it does not need nodes to manage paths to destinations which are not in active communication. Moreover Ad Hoc On demand Distance Vector Routing permits mobile nodes to reply back for modify in the network and link breakages in a regular manner.

The main aim of the AODV protocol is to adjust for modifications in criteria in the network route dynamically and quickly, like AODV protocol runs as a pure on demand route obtaining system due to mobility of nodes the.

3.1.1 Control Messages [11] Deployed in AODV is:

- Route Request Message (RREQ).
- Route Error Message (RERR).
- Route Reply Message (RREP).
- HELLO Messages.
- Route Reply Acknowledgment (RREP ACK).

4. BLACKHOLE ATTACK

Defining blackhole attack [1] once again here it is a Denial of Service (DoS) type of attack in any wireless network. In this attack the malicious node pretend to have the most optimal path i.e. having lowest hop count and highest destination sequence number (DSN). Thus it gets success taking the source node into belief that it is most suitable path for which it was searching for, and it forwards all packets through this malicious node. Then further it either diverts the route to another node/destination or drops all packets or it can drop some of them and divert another. In this way this malicious node is termed as Blackhole.

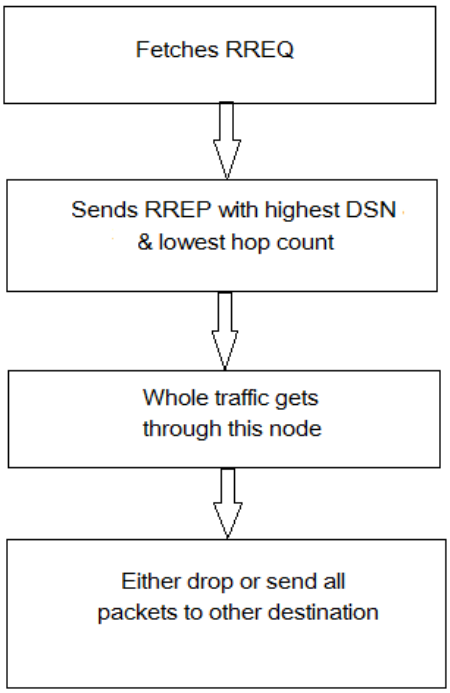

Fig 1. Flow chart of Blackhole Attack

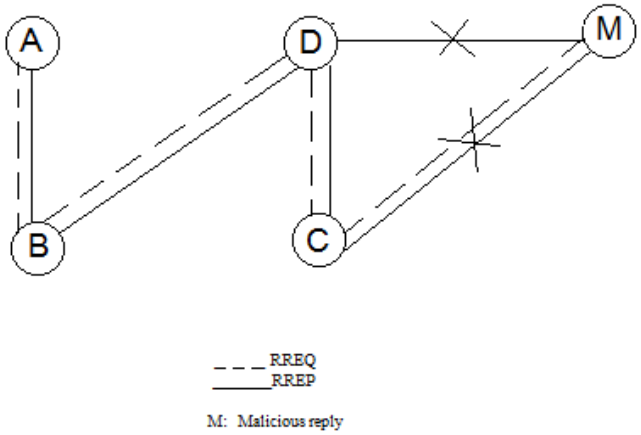

Fig 2. Blackhole Attack

In fig. 2 A, B, C, D is the normal nodes while M is malicious node. When network starts communication its data packets are transmitted with the help of AODV protocol control packets RREP and RREQ. As soon as it identifies the malicious node on transmission of data packets from node C it is declared malicious nodes and thus all communication to this node stops provided an improved algorithm is followed for AODV. While if doesn't identifies the malicious node then whole transmission will be through this node itself and it will degrade the performance of network certainly.

5. PROPOSED SOLUTION

The proposed algorithm deals with the mischievous behaviour of the malicious node. Hereby we present a solution to detect and present a robust and simple solution for which the network need not to face the problem again if following this algorithm. The results are compared to the results on the previously applied algorithm itself. The most wonderful thing about the solution is that it doesn't require any additional mechanism of extra bit or anything.

In this algorithm we have dealt with all conditions as in previous paper too, we got a conclusion that if we are able to impart a solution which very little modification. The algorithm improves the results of the previously applied algorithm used in [1]. We will be able to justify our result on different parameters.

In this paper we have introduce "ROUTE TRACE MTEHOD" which will reflect our results in paper. Description of this method is as follows:

At first the source node will broadcast RREQ, then it will get a RREP packet and thus in basis of lowest hopcount and highest DSN we will decide the suitable node through which the transmission is being forwarded. The change we have done in this algorithm is from here, now we are transmitting a blank packet and observing it whether it reaches the destination or not and if reaches then the path is correct, and thus we will send the packet. As we know blackhole and other types of attacks are inevitable so as to avoid these all we will do this first for testing and further we will move on. Moreover if packet doesn't reply back in a given specific time then the route and node will be discarded from RT. Thus it helps to prevent the blackhole attack and we can have our network without these types of attacks.

Now the steps involved:

1) As usual the source node will initiate the broadcasting of RREQ to all of its neighbouring nodes.
2) RREP received will obviously contain the node with lowest hop count and highest DSN.
3) Select that node.
4) Now we will send a packet to towards that node and will wait for its proper acknowledgement.
   A) As the packet replies with positive acknowledgment, transmission will begin.
   B) If the negative acknowledgement is received then will remove the node from RT. And further move to bottom node which was second to the applied and tested above.
5) This process will be repeated again and again till we don't get any positive acknowledgement as soon as we will get the positive reply transmission will start soon.
6) End.

6. SIMULATION AND DESCRIPTION

The simulation for this algorithm has been done in the Network Simulator version 2.35 (NS-2.35). The TCL (Tool Command Language) of these modules is simulated for 20 to 100 nodes, with an interval of 20 nodes, separately. The two ray ground radio propagation model is used and the 802.11 IEEE standards is considered for the MAC layer.

For this paper, a network with 800×800 meters dimension is created in a domain where all the nodes are kept under the AODV routing protocol.

The simulation time is set to 415 sec and the time of connection end is set to 500 sec. Each node is selected with the range of its transmission of 220 meter. Initially, nodes are static and then that are located dynamically i.e. nodes are being mobile now. The scenario of mobility file is generated to define the original location of the nodes and also the movement of nodes from one location to another location with the mobility of 22 meter per second. The simulation is considered for all the 20 to 100 nodes, with an interval of 20 nodes, out of them 22 nodes are kept as the communicating nodes to analyze the network's performance in all the three modules.

1. Packet delivery ratio (PDR): The ratio of absolute number of packets sent from the source node defined as S to total number of packets fetched successfully at each destination nodes defined as D and it is called PDR [6].

$$PDR = S/D$$

2. Throughput: It can be stated as the rate of successfully delivered packets in the network to the rate of received file by a host over a period of time is called as Throughput [7]. Unit of the throughput is bits per time.

$$\text{Throughput} = \frac{\text{Total number of bits transmited}}{\text{Total time taken for transmission}}$$

From figure 3 and 4 we can conclude and justify the comparative graph of previous and proposed algorithm. Figure 3 depicts the graph between numbers of nodes vs. PDR the graph is first degrading and then it increased and gives improved result. The degradation of graph is because of the testing packet but when the communication is established it is having the improved results. Also results in figure 4 graph are drawn between Throughput and Number of nodes. In this also there is first degradation and then it just go on improving the graphs.

Simulation parameters:
Channel type: Wireless channel
Radio propagation model: Two ray
Routing protocol: AODV
Topographical area: 800*800 meters
Number of nodes: 100
Number of mobile nodes: 22

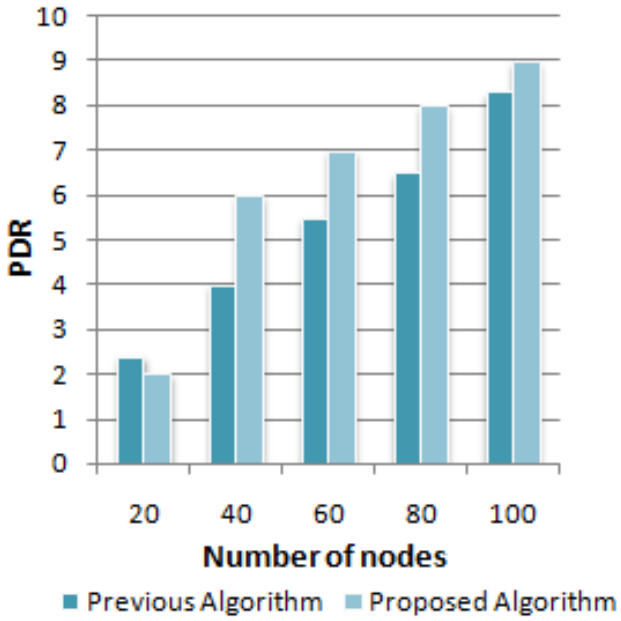

Fig 3. Comparison graph PDR vs. Number of Nodes

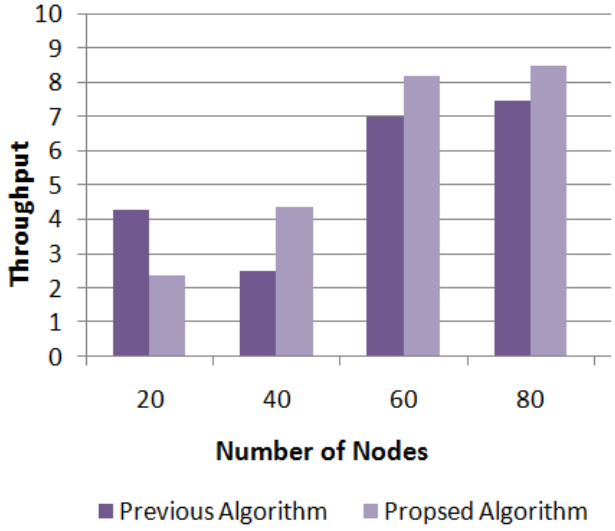

Fig 4. Comparison graph Throughput vs. Number of Nodes

7. CONCLUSION

The solution which is proposed in this paper is able to identify blackhole nodes and then reducing its effect. It removes the malicious node from the network and discovers new path for the requested route. As shown in result it gives the improved results than the previously applied algorithm. We have suggested an appropriate answer for this is in the AODV protocol. Also we have shown that the effect of packet delivery ratio and Throughput with respect to the variable node mobility. Though there is enhancement in Packet Delivery Ratio and Throughput. Here the attacker node is making severe harm in network and nodes. It can also be verified with the simulation result. The detection of malicious node can be in any form in any of the networks is still considered to be a challenging. Simulation results shows the comparatively better performance with the algorithm used.

REFERENCES

[1]. Girish Tiwari and Nishant Doshi "A Ubiquitous Solution for Mitigation of Black Hole Attack in Cognitive Radio", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 4 Issue: 6, pp 398-403, June 2016.

[2]. US FCC's Cognitive Radio Report and Order adopted 2005-03-10.

[3].P. Manickam, T. Guru Baskar, M.Girija, Dr.D.Manimegalai "Performance Comparision of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, pp. 98-106, February 2011.

[4]. Pankaj Rohal, Ruchika Dahiya, Prashant Dahiya "Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV)", International Journal for Advance research in Engineering and Technology, Vol. 1, Issue II, pp. 54-58, Mar. 2013.

[5]. Nandkishor joshi, Bhavana Jharia "Optimized fuzzy power control over fading channels in spectrum sharing cognitive radio using ANFIS" in 2nd International IEEE conference on Signal Processing and Integrated Networks (SPIN) ,2015 pp.104.

[6]. Shalini Sharma, Girish Tiwari "A new IDS scheme against blackhole attack to enhance security in wireless network" International journal of research in engineering and technology (IJRET) vol. 9, no. 8,pp 429-433,aug 2015

[7]. Zainab Dalaf Katheeth, Prof. K.K. Raman "Performance Evaluation with Throughput and Packet Delivery Ratio for Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2014.

[8]. S. Haykin, "Cognitive radio: brain empowered wireless communications," IEEE J. Selected areas in Comm. vol. 23, pp. 201-220, zeb. 2005.

[9]. S. Haykin, "Cognitive Radio: Brain-Empowering Wireless Communications," IEEE Journal on Selected Area in Communication, Vol.23, No.2 February 2005.

[10]. Teerawat Issariyakul, Ikram Hossain "Introduction to network simulator NS2" 2nd edition.

[11]. Patil V.P. "Efficient AODV Routing Protocol for MANET with enhanced packet delivery ratio and minimized end to end delay", International Journal of Scientific and Research Publications, Volume 2, Issue 8, pp 1-6, August 2012.

[12]. J. Mitola III and G. Q. Maguire, "Cognitive radio: making software radios more personal," IEEE J. personal communications, vol. 6, pp. 13-18, Aug. 1999.

[13]. Manish Giri and Girish Tiwari "Enhancing Voice Quality through Improved E-Mode: A mathematical Analysis "IJETCR, vol.3 issue4, July 2016

[14]. J. Neel, "Analysis and Design of Cognitive Radio Networks and Distributed Radio Resource Management Algorithms" PhD thesis, Virginia Tech, Sep 2006.

[15].F. Rosenblatt, "The Perceptron: A probabilistic Model for Information Storage and Organization in the Brain," Cornell Aeronautical Laboratory, Psychological Review, Vol. 65, No. 6, 1958, pp. 386–408.

[16]. Girish Tiwari and Manish Giri, "A Survey on Enhancing QoS through voice quality for voice over wireless LANs (VOWLAN)", International Journal on Recent and Innovation trends in Computing and Communication, vol 3, issue 5,pp 3256-3260