ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Peruse Of Black Hole Attack and Prevention Using AODV on MANET

Vasanthavalli.S [1], R.Bhargava Rama Gowd [2] , Dr.S.Thenappan[3]

P.G. Student, Department of ECE, The Oxford college of Engineering, Bangalore, India[1]

Assistant Professor, Department of ECE, The Oxford college of Engineering, Bangalore, India[2]

Professor, Department of ECE, SEA College of Engineering, Bangalore, India[3]

Abstract: Mobile Ad-hoc Network (MANET) has been an active research area as it has the special features such as fast, dynamic and easy to deploy anywhere. Absence of central monitoring unit, MANET highly depends on mobile nodes reliability. This leads MANETs are more vulnerable to various communication security attacks. One of the main active attacks is Black hole attack, it is a denial of service attack and it drops entire incoming packets between one source to destination. The attempt is to focus on analyzing and strengthening the security of routing protocol Ad-hoc On Demand Distance Vector (AODV) for MANET. The Proposed Method PL2 has the modification done in AODV protocol for ensuring the security against the Black hole attack using NS2 Simulation.

Keywords: MANET, AODV, Black Hole Attack, NS2.

I. INTRODUCTION

There has been tremendous growth in the use of wireless communication over last decade. MANET is a collection of wireless mobile nodes that can communicate with each other by point to point transmission type. Due to the limited transmission range, multiple hops are essential for one node to communicate with faraway node in the network. In such a network each mobile node act as a host as well as a router, receiving and forwarding packets for other mobile node that may not be within transmission range of each other. MANET is an infrastructure less network, used in battlefields, military, emergency and disaster such as search and rescue [1].

Absence of fixed base station in MANET makes many security issues than conventional wireless network. Because of MANET uses open air medium, continuously changing topology, absence of central administration, multi-hop routing and distributed cooperation, is vulnerable for several types of attacks. One of the main active attacks is Black hole attack which takes place in network layer. In Black hole attack, a malicious node or group of malicious node drop the entire packets between source to destination [2].

In this paper, we attempt in analysing and upgrading the security of the AODV routing protocol against Black hole attack. AODV is an on demand, dynamic routing protocol and consumes less bandwidth than table driven protocol. Protecting against Black hole attack, additional commands are included in AODV.

Our proposed method is a PL2 method is a combination of postlude and prelude control messages. Source based detection method is used to mitigate the Black hole attack is possible by customizing the original AODV. The simulation is done in ns2.

II. RELATED WORK

Sun B et al [3] used neighbourhood based method to detect malicious node in the network. In detection procedure neighbourhood set of information is collected, further collected information is used to determine whether there Black hole attack exists. In response procedure source node sends Modify-Route-Entry (MRI) control packet to destination node to build a correct path by modifying entries of intermediate nodes. This simulation fails to detect forged fake RREPs.

Tamilselvan T [4] proposed a solution based on time based threshold detection scheme. The main concept is setting timer for collecting all other RREQ from other nodes after receiving the first request. Collect Route Reply Table is used to store the packet's sequence number and the received time. In Route Discovery, the validity of route is checked based on the

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

arrival time of the first request and the threshold value. This simulation shows that a higher packet delivery ratio is obtained and end to end delay might be increased when the malicious node is away from the source node.

Djenouri D et al [5] proposed a solution based on Random two hops ACK and Bayesian detection scheme. In monitor phase two hop ACK used to check the reliability of the intermediate node. In detection and removal process, Bayesian approach is used for node accusation. This simulation is efficient for all types of packet drops and has reduced overhead. This solution is not suitable for multiple Black hole attack.

DPRAODV [6] scheme has Detection, Prevention and Reactive AODV scheme. The solution is based on the validity of the RREP sequence number. If the RREP sequence number is higher than threshold value, that node is added to the Blacklist. Further receive reply from that malicious node is ignored. This simulation shows that improved packet delivery ratio at the cost of higher routing overhead.

Tsou Po-Chun et al [7] designed unique solution named Bait DSR based on Hybrid Routing scheme. Initially the source node sends Bait RREQ, having destination address which does not exist. This bait RREQ can attract the forged RREP and can remove Black hole nodes. This simulation results show increased packet delivery ratio and acceptable overhead.

III. AN OVERVIEW OF AODV

AODV is the on demand routing protocol uses purely reactive method. It creates routes only when desired by source node [3], composed of two main process, Route Discovery and Route Maintenance. When a source node requires a route to the destination node, it initiates a Route Discovery process by broadcasting RREQ-Route REQuest to its entire neighbour. Once an intermediate node receives a RREQ, it checks its routing table for route to the destination. If found send RREP - Route REPly back to source. If not found, it further keep forward RREQ to their neighbour until get destination address. If a node receives the same RREQ again, it will be ignored.

Finally RREQ reaches destination node, it unicasts RREP to source node by using reverse route to source node. In Route Maintenance, the source node will be informed by RERR-Route ERRor Packet if any connection failure between intermediate nodes or topology changes. Fig.1 and Fig.2 are the packet format of RREQ, RREP respectively.

Source Address	Request ID	Source Sequence number	Destination Address	Destination Sequence Number	Hop count

Fig.1 RREQ format

Source Address	Destination Address	Destination Sequence Number	Hop Count	Life time

Fig.2 RREP format

Each mobile node in the network can get to know its neighbourhood by using periodic HELLO messages [8]. HELLO messages are used to inform the neighbouring node that the link is still alive and never be forwarded [9].

IV. BLACK HOLE ATTACK

Black hole attack is a Denial-Of –Service attack that could easily happen in wireless MANET. To carryout Black hole attack in the network, a malicious node waits for the neighbouring node to send RREQ messages [10][11]. After getting RREQ messages, it sends fake RREP at once, as it has route over destination without checking routing table by assigning high sequence number. So requesting node assumes that Route Discovery process is completed and starts transmitting data packets over that malicious node, without knowing about malicious activity. Black node drops the incoming entire packets between the source to destination, instead of transmitting to destination. As a result the source and destination node unable to communicate with each other. Since AODV treats RREP messages having higher sequence number to be fresher, the malicious node always send the RREP having higher sequence number [12].

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

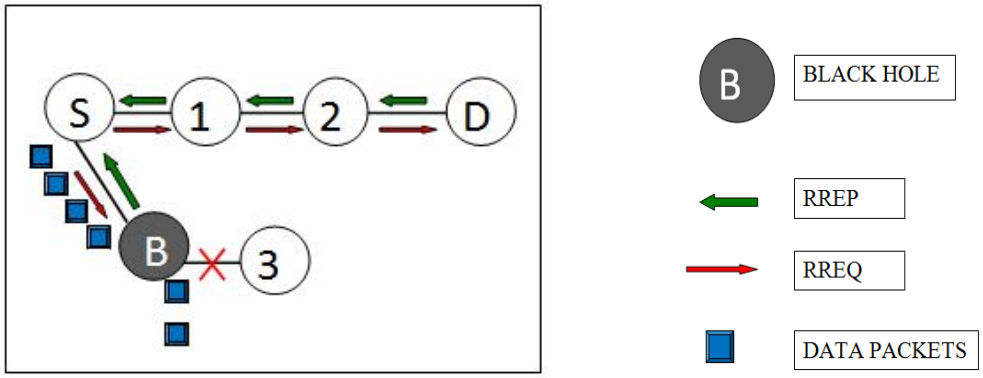

Fig.3 Black Hole Attack

For example node S wants to send data packets to destination node D in Fig. 3 and initiates Route Discovery process. Malicious node B claims that it has shortest path to the destination, whenever it receives RREQ packets. So that Source node think that Route discovery process is completed and ignore all other RREP messages, begin to send packets over malicious node B.As a result all packets send through Black hole node B are simply lost or send to unwanted destination.

v. PROPOSED METHOD—PL2 METHOD

PL2 method is PreLude, PostLude method. The proposed solution is an enhancement of the original AODV routing protocol to find a secure routes and prevent Black hole attack on MANET. The Major concept is based on time and neighbourhood parameters. This method first check for malicious activity exists, and then starts detect and remove the Black hole nodes. Route discovery is same as original AODV, but when sending data packets, prelude and postlude messages are added.

Detection of Black Hole Activity

Initially, data packets are divided into equal parts as Data (1… K) Where K=ceiling of (n/w).Where n is the number of data and w is the window size. Apart from the source, destination, some intermediate nodes are assigned as monitor nodes, given powers to overhear data packets and watching other intermediate nodes. After Route Discovery process, monitor(S, D, NNR) nodes are broadcasted to all other NNR-Next Nodes in the Route. Source node sends prelude (S, D, ni) message with every equal block of data and waits for special type of acknowledgement as postlude (D, S, d_count) message from destination node after receiving data. ni is the number of data in particular block i and d_count is the number of data received by destination node. If source node not receive postlude message within timeout period TS, malicious activities are confirmed in the network. Windowing mechanism is used to reduce the end to end delay and data loss. Detailed processes are as shown in flowchart Fig.4.

Black Hole Removal Process

In Black hole removal process, source node sends query BQ (S, D, NRREP, ni) to monitor node to find out malicious node.NRREP is the ID of the node sending RREP to source. In response monitor nodes sends back result to source node. If source node receives result before a particular time TRES, predicted that the particular monitor node itself is a malicious node. So Source node depends on other monitor node's results to build a secured path.

Based on monitor nodes result, source node starts votecount. Votecount is a count, for not forwarding the data packets of the particular node, when it receives from other node. If votecount of the particular node is greater than the threshold value, the source node confirms that the node as a Black hole node and will be listed in Blacklist. Threshold value is a variable depends on the size of the network. As source node knows the location of the Black hole nodes, it ignores the RREPs from these nodes. The flow chart for detailed process is as shown in Fig.5.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

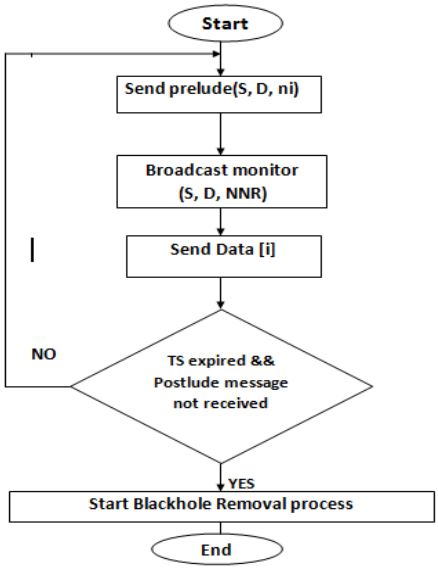

Fig.4 Detection of Black Hole Activity

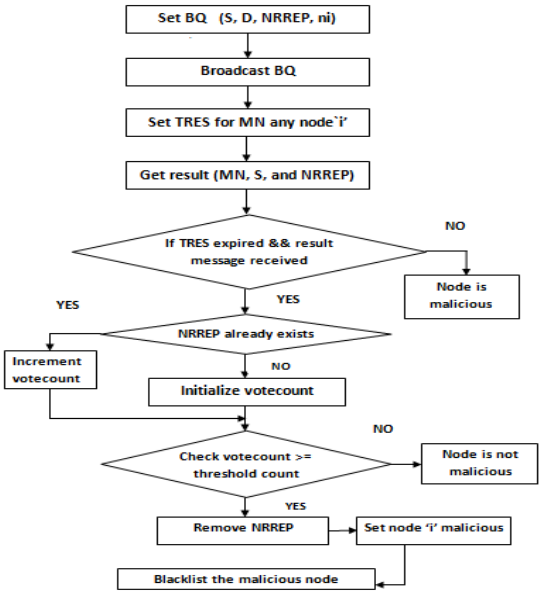

Fig.5 Flow Chart for Black Hole Removal

PARAMETER	VALUE
AREA	1000 x 1000
Simulation Time	50 S
Number of nodes	30
Traffic Model	CBR
Protocol	AODV
Number of Attackers	3
Drop Rate	2 Mbps
Packet Size	512 bytes

Table .1 Simulation Parameters

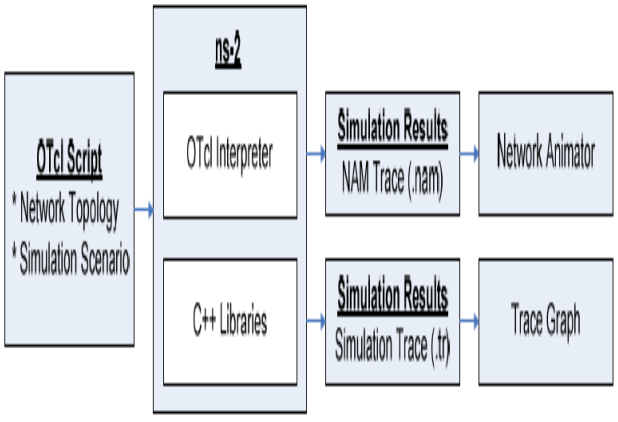

Fig.6 Network Simulator-2

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

VI. SIMULATION AND ANALYSIS

The simulation has been carried out using NS-2.35. In ns2, two languages are used, tcl-tool command language as front end and c++ as back end .The user writes in tcl script, are interpreted by network simulator and give two output files. They are NAM and tr files.NAM is for visual animation of output and tr is the large text trace file consists of simulation Results. In this simulation 30 mobile are considered in the terrain area of 1000x1000. Malicious activity in the network is assumed as 10% i.e. 3 Black hole nodes are included in the simulation. Simulation parameters are considered as shown in the Table.1

Performance of AODV can be analyzed by different simulation metrics such as end to end delay, packet delivery ratio, throughput and etc...

Packet Delivery ratio

It is a ratio of total number of packets received by the destination node to the total number of packets sent by the source node. PDR simply describes the level of delivered data.

$$PDR = \frac{\sum \text{Number of data packets received}}{\sum \text{Number of data packets sent}}$$

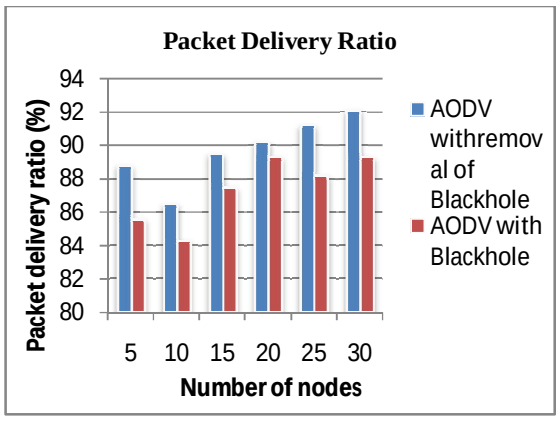

Fig.7 Packet Delivery Ratio

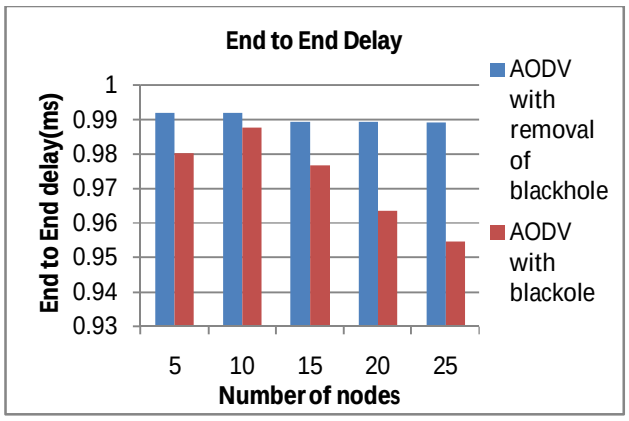

Fig.8 End to End Delay

In fig.7 shows that PDR of the proposed PL2 method is higher than AODV with Black holes. As Black holes induce packets drop, the PDR of original AODV decreases with increase in number of nodes.

Average End To End Delay

It is the average time taken by the data packets travel from source to destination. This includes all types of delay caused by buffering of data, Route Discovery latency, queuing, processing at intermediate nodes, retransmission delays, propagation time and etc [13]. End to End Delay=∑ (arrival time - send time)

End to End Delay must be low to get better performance of AODV. Fig.8 shows that the proposed PL2 method has lower End to End Delay than original AODV with Black holes.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Throughput

The number of bits received over the time difference between the first and the last received packets. Throughput graph is plotted by varying number of nodes. Presence of malicious node in MANET is degrading the performance of AODV. In fig.9 shows that the proposed PL2 method has good throughput comparably 10% higher than original AODV with Black hole attack and throughput decreases as increase in number of nodes.

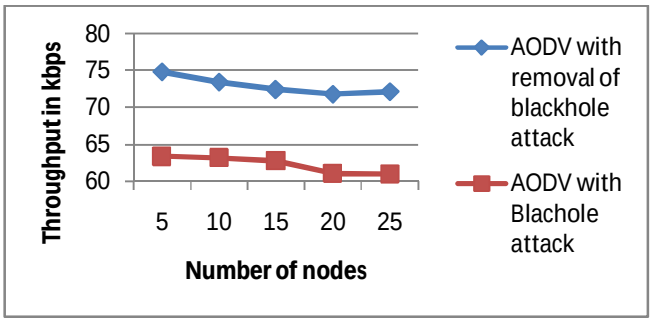

Fig.9 Throughput

VII. CONCLUSION AND FUTURE WORK

In this paper, we proposed PL2 method.PL2 is a source, neighbour, time based and modified AODV routing protocol to mitigate Black hole attack. We simulated our proposed solution using ns-2 and compared our modified AODV with original AODV in terms of packet delivery ratio, end to end delay and throughput. Simulation results show that the proposed method has good performance against Black hole attack and not much overhead. This solution holds good for gray hole attack also. In our future work, we may propose a feasible solution which will strengthen original AODV against cooperative Black hole attack.

REFERENCES

[1] Homgmei Deng, Wei Li and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Networks", IEEE communication Magazine, vol.40, no.10, pp. 70 -75, October 2002.

[2] A. Baadache,and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks", International Journal of Computer Science and Information Security,vol.7,no.1,2010.

[3] Sun B, Guan Y, Chen J, Pooch UW, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, . 22-25 April 2003.

[4] Tamilselvan L,Sankaranarayanan V, "Prevention of Blackhole Attack in MANET", International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[5] Djenouri D,Badache N, " Struggling Against Selfishness and Black Hole Attacks in MANETs",Wireless Communications and Mobile Computing, vol.8, no 11, 2008.

[6] Raj PN ,Swadas PB, , "DPRAODV: A Dynamic learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issue,vol.2,pp.54-59 ,2009.

[7] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, " Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, pp.755-760, Feb. 13-16, 2011.

[8] Nisarg Gandhewer and Rahila Patel, "Performance Evaluation of AODV protocol in MANET using NS2 simulator", 2nd National Conference on Information and communication Technology (NCICT) 2011, Proceeding published in International Journal of Computer Applications (IJCA).

[9] Hilmani Yadav, Rakesh kumar, "A Review of Black Hole Attack in MANET", International Journal of Engineering Research and Applications, vol.2, issue.3, pp.1126-1131, may-june 2010.

[10] Umang S, Reddy BVR, Honda MN, " Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption", IET Communications,vol.4,Issue.17,pp.2084-2094, 2009.

[11] EA Mary Anita and Vasudevan V, "Black Hole Attack Prevention in Multicast Routing Protocol for Mobile Adhoc Networks using Certificate Changing",International Journal of Computer Applications,vol.1, issue.12,pp.21-28, 2010.

[12] Satoshi Kurosawl, Hidehisa ,Nakayama, Nei Kato,Abbas Jamaipour and Yoshiaki Nemoto, , " Detecting Blackhole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security,vol.5,no.3,pp.338-346,2007.

[13] Nital Mistry, Devesh cJinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", Proceeding of the International Multi conference of Engineers and Computer Scientists, Hongkong,vol.2, March17-19, 2010 .