DETECTION OF COOPERATIVE BLACKHOLE ATTACK ON MULTICAST IN MANET

Payal J. Desai[1], Urmi Desai[2]
[1]P.G.Student, [2]Prof., CO Department,
Sarvajanik College of Engineering and Technology, Surat, India.
Email: [1]payal.2394@gmail.com, [2]urmi.desai@scet.ac.in

Abstract-- Mobile ad-hoc network is a network that comprises of many mobile nodes. MANET is infrastructure less network and has a dynamic topology. There is no central entity presents so any node can join or leave the network at any time. Therefore security is the main issue in MANET. MANETs are vulnerable to many kind of attack. One of these attacks is blackhole attack. There are two kind of black hole: single black hole and cooperative black hole. In single blackhole only one malicious node is present and in cooperative blackhole attack there is two or more malicious node attack in cooperation with each other. In this paper we propose a method that detects cooperative blackhole attack and simulate the results in NS2.

Keywords – MANET, Cooperative Blackhole attack

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of many mobile nodes in which there is no need of any access point. It is a wireless network with no any fixed infrastructure. There is no central entity required to control over the network so any node can join or leave network at any time. For this reason ad-hoc networks have a dynamic topology. Because there is no infrastructure, nodes are connected with each other by forwarding packet over network. Nodes use routing protocol like AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), and DSDV (Destination Sequenced Distance Vector) to connect with each other.

AODV is the most widely used protocol in MANET which is vulnerable to blackhole attack. In blackhole attack, a malicious node tries to fool source node by advertising that it has a shortest route to the destination. After getting the data packets, malicious node drops all the packets which it has to forward to its neighbor node. In Cooperative blackhole attack there are more than one malicious node is present in the network. In this paper we propose a solution that detects the cooperative blackhole attack.

A. OVERVIEW OF AODV

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol which is vulnerable to blackhole attack in which a route to destination is created only when required. AODV protocol makes use of three types of message

1) Route Request message (RREQ)
2) Route Reply message (RREP)
3) Route Error message (RERR)

The format of RREQ and RREP message is shown in following tables.

Table 1: Format of RREQ packet[10]

RREQ Packet					
Source IP address	Source sequence number	Broadcast ID	Destination IP address	Destination sequence number	Hop count

Table 2: Format of RREP packet[10]

RREP Packet				
Source IP address	Destination IP address	Destination sequence number	Hop count	Lifetime

Route discovery process in AODV

When a source node wants to transmit data packets it first check its routing table if there is no route is found it initiates route discovery process by sending RREQ message. Source node broadcasts RREQ message to its neighbors.

Neighbor node or intermediate having route to destination or destination node itself will generate RREP packet and send it to source node. If there is no route to destination the nodes will rebroadcast RREQ to their neighbor node. There is a timer associated with each node to destroy RREQ packet in case reply has not been received before it expires.

B. BLACKHOLE ATTACK

In blackhole attack a malicious node advertises itself that it has a shortest path to destination and tries to fool the source node. After getting response from malicious node, source node discards all other path and transferring data towards the malicious node. After receiving data packets from source node, a malicious node drops all the data packets instead of forwarding them to the next node.

Types of Black Hole attack

Black hole attack can be categorized into following two types:

1. Single black hole attack
2. Cooperative black hole attack

1. Single Black Hole attack

In single black hole attack, only one malicious node present in the network. It sends fake RREP to source node trying to fool source node that it has shortest path to destination. Sp source node ignores all other rout and sends data to blackhole node. After getting data from source node, blackhole node drop all the data packet which it has to forward to node 4 in fig. 1

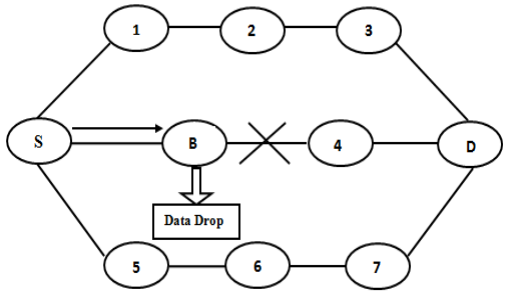

Fig.1 Blackhole attack

2. Cooperative blackhole attack

In cooperative blackhole attack, two or more node act maliciously in cooperation with each other in the network. Fig. 2 shows the cooperative black hole attack in which node B1 and B2 drops all the data packet without forwarding it to destination D.

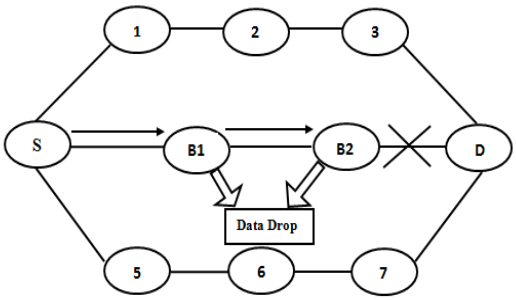

Fig. 2 Cooperative blackhole attack

This paper is organized as follows. In section II we described related work for detecting

blackhole attack. Our proposed methodology to detect cooperative blackhole attack is discussed in section III. Simulation results is discussed in section IV and finally section V, conclusion and future work is discussed.

II. RELATED WORK

In this section we discuss some existing technique to detect the blackhole attack

Latha Tamilselvan [2] proposed a method which is an enhancement of basic AODV routing protocol which is able to protect against black hole attack. In this mechanism, without sending data packets to RREP initiator at once it has to wait till other neighboring node gives information about their next hop. Upon receiving first request it sets timer in 'TimerExpiredTable', for collecting further requests from other different nodes. It will store the sequence number and arrival time of packet in a 'Collect Route Reply Table' (CRRT). It calculates the value of timeout based on the time at which first route request arrived.

Latha Tamilselvan [3] proposed a method which is enhancement of basic AODV routing protocol. This technique identifies multiple blackhole nodes which are cooperating with each other and a safe route is discovered. In this method it assumes that the nodes are already authenticated and therefore participate in communication. It uses Fidelity Table where every node will be assigned a fidelity level which is a measure of reliability of that node. If fidelity level of any node drops to 0 then this node is identified as blackhole node and it is removed from the network.

Payal N. Raj [4] proposed a mechanism which makes an additional check to find whether RREP_seq_no is high than the threshold value. The threshold value is calculated as the average of the difference of dest_seq_no in every time slot between the sequence number in routing table and RREP packet. If the value of RREP_seq_no is found to be higher than the threshold value, the node is identified to be blackhole node and adds the node to the black list. The new control packet called ALARM which contains the black list node as a parameter is send to its neighbor node so that the neighboring node knows that RREP packet from the node is to be discarded.

Jaydip Sen [5] proposed a method for preventing against cooperative blackhole attack. They modify the AODV protocol by introducing two concepts:

1. Data Routing Information (DRI) table
2. Cross checking

1. Data Routing Information (DRI) table

In this method two bits of additional information are sent by the node that responds to RREQ message sent by source node at the time of route discovery process. An additional Data Routing Information (DRI) table is maintained by each node. In this DRI table, bit 0 stands for 'false' and bit 1 stands for 'true'. The first bit 'From' stands for information on routing data packet from the node and the second bit 'Through' stands for information of routing data packet through the node.

2. Cross checking

In this paper, the proposed method relies on reliable node to transfer data packets. In modified AODV protocol, the intermediate node (IN) that generates RREP message in response of RREQ message from source node (SN) has to provide information of it next hop node (NHN) and DRI entry for that NHN. Source node will check its own DRI table upon receiving RREP message from intermediate node to see whether IN is reliable. If IN is reliable then SN starts transmitting data packets otherwise SN sends Further Request (FRq) message to NHN. After receiving FRp message, source node check whether SN has routed data packet through NHN to check NHN is reliable or not. If NHN is reliable then SN will check whether IN is blackhole or not. If through entry of DRI table of IN is 1 and from entry is 0 then IN is a blackhole. If IN is not blackhole and NHN is reliable then route is secure.

Gundeep Singh Bindra [6] proposed a mechanism which handles the blackhole and grayhole attacks by maintaining an Extended Data Routing Information (EDRI*)* Table at each node in addition to the Routing Table of the AODV protocol.

The EDRI table accommodates the gray behavior of nodes as well. Although, it gives subsequent

chances to the nodes identified as blackhole, it also keeps a record of the previous malicious instances of that node so that a better understanding of the node can be made and the node is given its next chance accordingly. A counter keeps track of how many times a node has been caught and the value of this counter is proportional to the time which has to pass before that node is given another chance. A node which is frequently being caught acting maliciously is eventually not given a chance again.

Durgesh Kshirsagar [8] have used the method which first finds the neighbor node of RREP initiator i.e. suspected node and tells that neighbor node to monitor all the packets sent by the suspicious node. To monitor packet sent by malicious node, neighbor keeps two counters: fcount – used for counting number of forwarded packets and rcount – used for counting number of received packet. Neighbor node increment fcount when it transmits a packet it increments rcount. Neighbor node forward packet suspected node until fcount reaches a threshold; thereafter if rcount is 0, RREP initiator node is identified as malicious node.

III. PROPOSED IDEA

AODV protocol is vulnerable to blackhole attack so we develop a new technique to detect a blackhole attack. In our proposed scheme, we maintained a matrix (counter) whenever a node receives a data packet from any other node a counter is increment automatically. A counter is maintained by every node which contains the trust value. Trust value is calculated based on mobility, energy of that node and stability of the node in the network. Blackhole have characteristic to move in the network very fast and it sends more RREP packets to source node so its energy level is decreased, in this way trust is calculated. The route with highest trust is decided to send the data packets. Whenever any node found which has the lowest trust value is detected as a blackhole node.

Steps of proposed idea

1. Source node starts route discovery process and after finding route it starts transmitting data packets. There is multiple paths available from source to destination.
2. When source node will not get acknowledgement from destination node within time out period it finds some malicious behavior is going on.
3. Every node in the network maintains the matrix (counter) which contains the trust value.
4. Trust value is calculated based on node's mobility, energy of that node and stability factor.
5. If the node is blackhole than it has the lowest energy and stability because it has the characteristics to move faster than any other node.
6. So the trust value of the node is decreased whenever it drops the packet.
7. The nodes with the lowest trust value are detected as a blackhole node and remove that path from the network.

IV. SIMULATION

In this section we discuss simulation environment and describe the simulation results.

We are using Network simulator NS-2 to build our simulation environment. Following are metrics which we use to evaluate our method.

1) Packet Delivery Ratio (PDR)

It can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node.

Fig. 3 shows the packet delivery ratio (PDR) Vs. the number of node with blackhole detection and without blackhole detection. It shows that with the increase in no. of node the PDR with blackhole detection get increased.

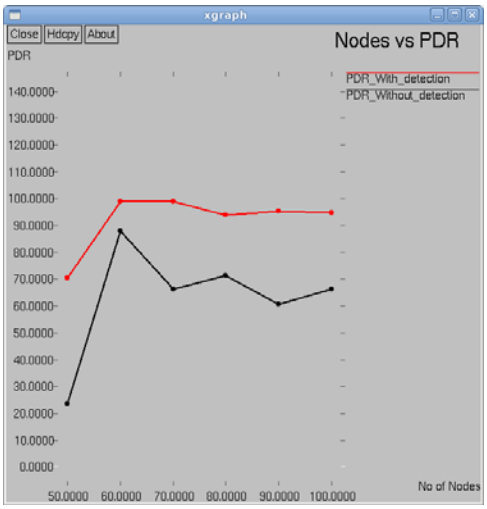

Fig. 3 Nodes vs. PDR

2) Dropping Ratio

It represents the ratio between the total no. of packets send to the packet received.

Fig. 4 shows the simulation result of number of nodes vs. dropping ratio with blackhole detection and without blackhole detection. We can see that with detection of blackhole node the dropping ratio gets decreased as compare to without detection.

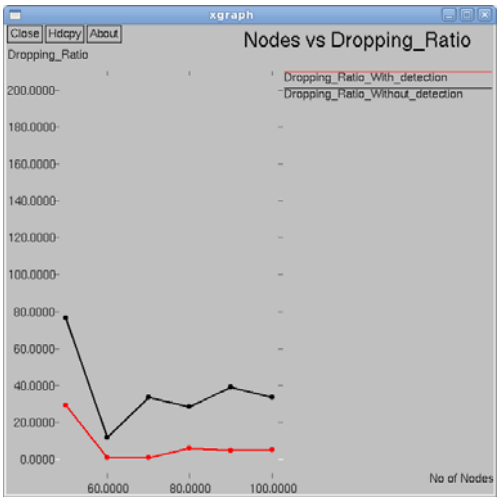

Fig. 4 Nodes vs. Dropping Ration

3) Normalized Routing overhead

This is the ratio of routing-related transmissions (RREQ, RREP, RERR etc) to data transmissions in a simulation. A transmission is one node either sending or forwarding a packet. Either way, the routing load per unit data successfully delivered to the destination.

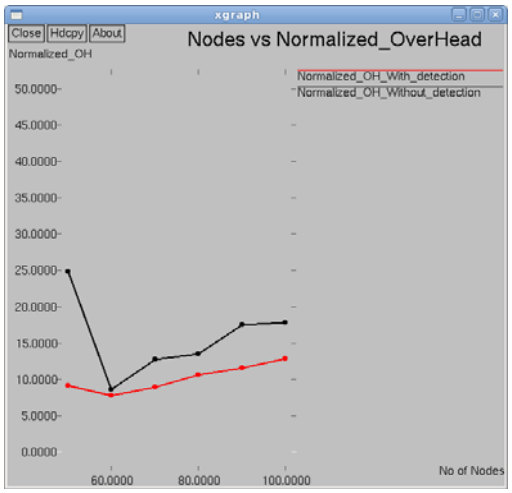

Fig. 5 Nodes vs. normalized Overhead

Fig. 5 shows the simulation result of number of nodes vs. normalized Overhead with blackhole detection and without blackhole detection. We can see that our proposed method decreases the normalized routing overhead but increasing number of node will increase the normalized overhead.

V. CONCLUSION AND FUTURE WORK

Security has become major issue in MANET and because of its dynamic topology and lack of central entity it is vulnerable to m any kind of attack and one of this is black hole attack. In blackhole attack, a malicious node tries to fool source node by advertising that it has a shortest route to the destination. After getting the data packets, malicious node drops all the packets which it has to forward to its neighbor node. AODV is vulnerable to blackhole attack so we develop a new method to detect a cooperative blackhole attack In this paper we describe a new technique to detect cooperative blackhole attack which is based on trust value.

In future, we can improve normalized routing overhead with respect to increase in number of node.

VI. REFRENCES

[1] Palanisamy, P. Annadurai, S.Vijayalakshmi," Impact of Black Hole Attack on Multicast in Ad hoc Network (IBAMA)",IEEE 2010

[2] L. Tamilselvan, V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[3] L. Tamilselvan, V. Sankaranarayanan, "Prevention of blackhole attack in MANE", Journal of networks, 13-20,May 2008.

[4] P. N. Raj and P. B. Swadas,"DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET", Intl. Journal of Computer Science Issues (IJCSI), 54-59, 2009.

[5] J. Sen, S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", second international conference on intelligent system, modeling and simulation, innovation lab, Tata consultancy services ltd. , Kolkata, 25-27 jan 2011.

[6] G. S. Bindra, A. Kapoor, A. Narang, A. Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANET", 2012 International Conference on System Engineering and Technology, Bandung, Indonesia September 11-12, 2012

[7] G. wahane, S. Lonare," Technique for Detection of Cooperative Black Hole Attack in MANET", 4th ICCCNT, Tiruchengode, India, 4-6 july 2013.

[8] D. Kshirsagar, A. Patil, "Blackhole Attack Detection and Prevention by Real Time Monitoring", 4th ICCCNT, Tiruchengode, India, 4-6 july 2013.

[9] Hiremani, M. M. Jadhao," Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET", International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, India, 12-14 December 2013.

[10] M. Y. Dangore, S. S. Sambare," Detecting And Overcoming Blackhole Attack In Aodv Protocol", International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 77-82, IEEE 2013

[11] M. Singh, G. Kaur,"A Survey of Attacks in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, pp.1631-1636, June-2013