Single and Co-Operative Black Hole Problem in Aodv Protocol in MANETS: A Review

Ankur Thakur
Department of Computer Science Engineering
RIMT, M.G.G, Punjab, India

Anuj Gupta (HOD)
Department of Computer Science Engineering
RIMT, M.G.G, Punjab, India

Abstract - The security threats is one of the common problem ocuuring in MANETS. In black hole attack, a attacker enters the network and show that they having a shortest path for the destination. In that way, the data is captured by the attacker. In this paper, we have discussed about two possible types of attacks, Single black hole and multiple black hole attack in a group. We have here tried to understand the black hole attack and how to prevent the data from black hole problem having single malicious node and cooperative malicious node

Keywords: MANETS, AODV, Attacker, Node.

I.INTRODUCTION

Mobile networks are of great popularity in today's world, as the users need wireless connectivity which does not depend on geographic position. MANETs are autonomous wireless systems. MANETs nodes are free to move in the network. Nodes may be any devices like mobile, personal computers etc. Although wireless networks provide many advantages over wired networks, but there occur many challenges also like security. Security in nodes is very important for the network. The various features like availability of the network, & integrity can be achieved only if security issues are clear and there is no problem with security of MANETS. Security attacks can occur mainly because of many factors like dynamic topologies, absence of central monitoring, open medium & no clear mechanism [1]. The black hole attack is one of the major security threats in MANETs. Black hole means when things enter in it & disappear. In networking, black holes attack is that where incoming or outgoing traffic is silently discarded (or "dropped"), & Source node does not having information that data is not reached at their destination location. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic, hence the name. In Black hole attack, the node represent itself a shortest path so that the source node sending data to the node which is not present in the network. MANETs having a security problem while transmission the data. So communicate between the nodes must be secured.

II.BLACK HOLE ATTACK

In black hole attack [2] [3], a attacker node introduce as the shortest path to the destination node. A malicious node uses the same routing protocol which used in the network Thus attacker node always has the availability to replay the route request. [4]. The malicious node reply to the source node that they will have a route to the destination. When source node will be received the requesting node before the reply from actual node and hence a route is created between the source node and a attacker node. Malicious node will get the data. Now attacker node decides whether to drop all the packets or forward it to the unknown address [5]. The scope of this paper is to study the effects of the Black hole attack in MANET using Reactive routing protocol Ad-Hoc on Demand Distance Vector (AODV).

2.1 *Black hole attacks are of two types*

2.1.1. Internal black hole attack

2.1.2. External black hole

2.1.1INTERNAL BLACK HOLE ATTACK

Internal black hole attack is that when internal node act as a attacker. It is also called active attack. Internal attack is that when the internal node is misbehaving, such as not using proper bandwidth or processing Capability also the misbehaving node tells all the node that it will be a shortest path to reach the destination. The internal malicious node also changes the data when it sends from source to destination.

2.1.2 EXTERNAL BLACK HOLE ATTACK

External black hole attack is called passive attack. It stays outside the network, but disturb the network by creating congestion and want a control over the internal node of the network by sending a RREQ to the source that it's a shortest path to reach the destination and carry data from the source. [6]

2.2 *Black hole Attacks are classified into two categories*

2.2.1 SINGLE BLACK HOLE ATTACK [7, 8]

In Single Black Hole Attack in which one node acts as attacker. It is also known as Black Hole Attack with single malicious nodes.

2.2.2 COLLABORATIVE BLACK HOLE ATTACK [9,10]

In Collaborative Black Hole Attack two or more than two nodes act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

III.AODV ROUTING PROTOCOL

Adhoc Demand Distance Vector Routing Protocol is reactive Protocol.They are basically used in Mobile ad-hoc network. It enables dynamic, self sorting, multihop routing between the nodes to create and maintain a network. AODV help the nodes to exchange the information of link breakage and network topology change in a timely manner. It is an On-demand routing protocol that creates routes only when reqiured. When a source node want to send data to the destination, it initiates a "route discovery process" within the network. It send a route request (RREQ) packet to the neighbor, the neighboring node, then sends the RREQ to its own neighbor till then they reach the destination. Once the RREQ reach the destination, then the nodes send the RREP to the neighbor nodes from when it receives the RREQ.

IV.BLACK HOLE PROBLEM IN ADOV PROTOCOL

In AODV protocol when RREQ message arrive every node responds to its previous neighbor node after checking its destination sequence number already contained in the RREQ packet. This is used for decreasing in the routing delay, But the various malicious nodes may get active with this method. The malicious node easily enters in our network and disturb the functioning of the routing protocol [11].

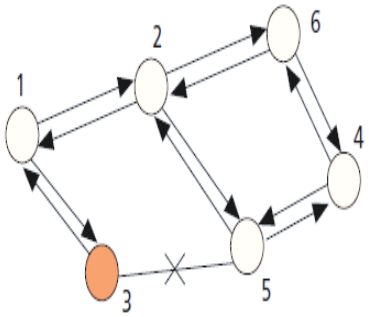

Fig 1: The Black Hole Problem

Example: In Fig 1, node 1 want send data packet to the node 4 and start the route discovery process. Let us assume that the node 3 is the malicious node. A malicious node doesn't have the destination path. But when it receives the RREQ packet from the source node then it sends a response to them. The other nodes near to the source node send a reply to the source node. If the neighbor node request receives first, then data will normally sent. No problem will occur. But if the malicious node reply first, then the route discovery process is complete and then source node ignore all the other node reply message and sending data to the attacker. So all the data will be passed through the malicious node and the data will be lost. This is called the black hole problem.

V. SOLUTION TO THE BLACK HOLE PROBLEM

When adjacent node cannot reply to the source node, only the destination node can send a reply to the source node. In that way we can avoid the black hole problem. But some limitation will occur with that method. The routing delay is increased, and the malicious node acts as a destination node which cannot be identified easily. So this solution is not much suitable.

Another solution is that we send a request to more than one node which are nearer to the source node to check whether the intermediate node having a destination address or not. If it exists, we can send data packet to the nodes, else we discard the reply message to the intermediate node and also tell the other node that the malicious node are in the network extract that node from the network.

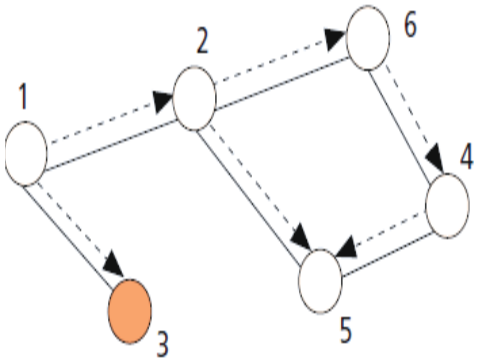

Fig 2: Propagation of Further Request

In Fig. 2, we take node 3 as a malicious node. In this method, we require each intermediate node to send the next node information when it sends back a RREP message. Node 3 sent a reply that next node is node 5. When node 1 get message from node 3, it does not send the data packets, but it further request to node 5 by node 2 and confirm that node 5 having an intermediate node route or not. In which the node 5 directly reply to the source node that node 3 is intermediate node or not.. If the node 5 or nexthope node send a reply 'yes' then the source node send the data packet to the destination, but if the nexthope node send that they do not have any route to that intermediate node. Then the source node discards that route immediately and send a data packet from another route and send an alarm message to all the node that there is a malicious node present in our network. So with this method we avoid the black hole problem. But, it will not work properly if there is more than one malicious node.

VI. LIMITATION

This method is based upon the assumption on that the malicious node are not working as a group. But in real situation this would be possible

VII. COOPERATIVE BLACK HOLE ATTACK PROBLEM

We can prevent the black hole problem if there is a single malicious node. But what would happen if the malicious node are more than one. In cooperative black hole attack the malicious nodes coordinate the other malicious node and attack the network [12].

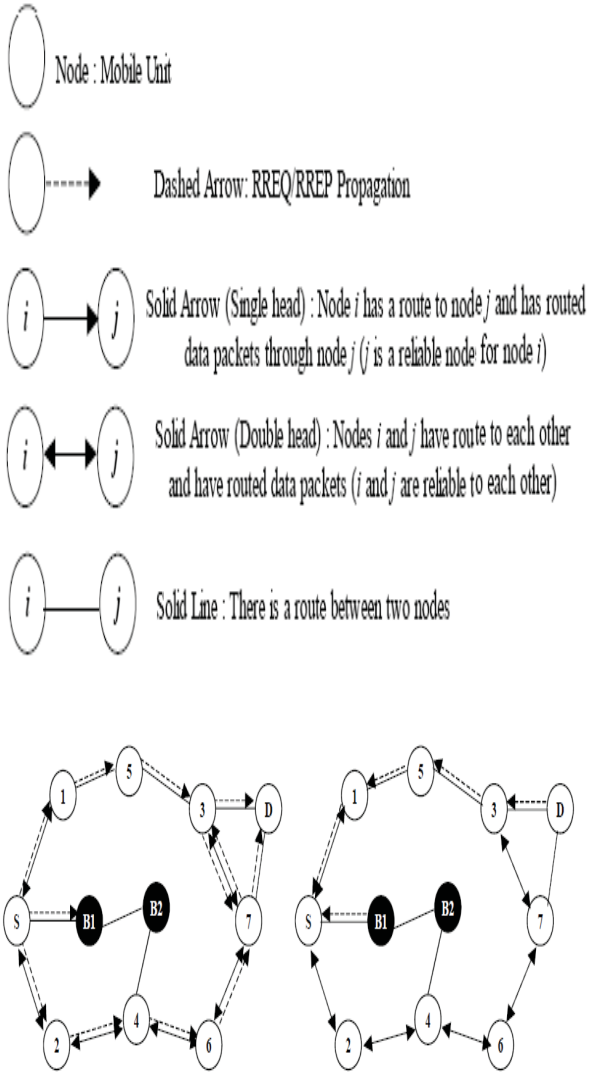

Fig 3a Neighboring RREQ (b) Propagation of RREP message

In multiple black hole nodes every node coordinates each other. They work together to destroy the system. In Fig 3(a), Source S sends a request to each intermediate node i e: (1, B1, 2). Every intermediate node sends an address to its further node. The first attacker is B1, When source S send request to the malicious node B1 then the node sends the address of their neighbor node which is B2. Then the source node send a "Further Request" to node B2 through a different route say (S-2-4-B2) other than through B1. Then source node S ask to the node B2 that it has a path to B1 and the destination node. B2 is coordinated with B1 So its reply "yes" to the source node. So that the source node will confirm the route (S-B-B2) will secure and send information to that path. In this way the security is ensured.

VIII. SOLUTION TO THE COOPERATIVE BLACK HOLE

For identifying the multiple black hole we just changed AODV protocol by adding Data routing information table in AODV protocol

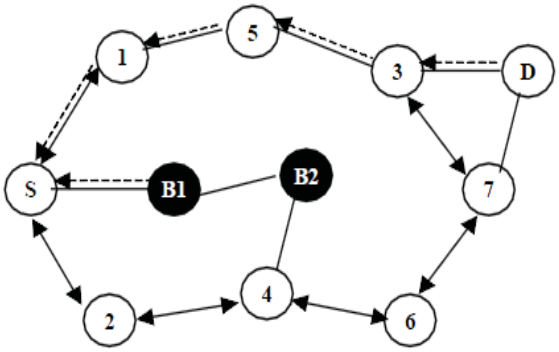

Fig 5 : Secured Multiple Black hole

The multiple black hole problem will be reduced by maintaining Data routing information table by each node. In Data routing information table it contains two values, i.e. 1 and 0. One stands for true and zero stands for false. In which we use two bits "From" and "Through". The first bit "from" tells that the information is coming from that node. The second bit "through" tells that the information passes through the node. In fig 5, A node 4 maintained a database in which a node 3 entry 1 0 state that node 4 has a route to transfer packet "From" 3 but no packet has been transferred "Through" node 3. For node 6 entries 1 1 state that node 4 has a specific route to transfer data packet"From" node 6 and also "Through" node 6. For node B2 entry 0 0 states that in node 4, no data packet has been transferred "From" and "through" B2. For node 2 entries 1 1 specify that node has a particular route for transfer packet from node 2 and also transfer data packet "Through" node 2.

Table1: Data routing table for node 4.

NODE	DATA ROUTING INFORMATION	
	FROM	THROUGH
3	1	0
6	1	1
B2	0	0
2	1	1

IX.CONCLUSION

In which we study how black hole node works, how it enter in our network & perform the malicious activities such as packet dropping. In this we studied how a single malicious node and cooperative black hole node attack our network and how we prevent our network from this multiple malicious node. As a future scope of the paper deals is an attempt to survey various solutions to this black hole attack and determine the best one among these

REFERENCES

[1] N. Raj and Prashant B. Swadas, Dpraodv: a dyanamic learning system against blackhole attack in aodv based manet, International Journal of Computer Science Issues, Vol. 2, 2009, pp 54-57.

[2] Mary. E. A .Anita and V. Vasudevan, Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Adhoc networks using Certificate Chainin, International Journal of Computer Applications, Vol. 1, 2010, pp 21-28.

[3] S. Umang, B.V.R Reddy, M.N Hoda, Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption, IET Communications Vol.4, 2009, pp 2084–2094.

[4] K. Biswas and Md. Liaqat Ali, Security threats in Mobile Ad-Hoc Network, Master Thesis, Blekinge Institute of Technolog, Sweden, 22nd March 2007.
[5] G. A. Pegueno and J. R. Rivera, Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.
[6] P. Kamra, T. P. Singh and R.K Singh, Preventing Black hole Attacks in Mobile adhoc Networks: A Review, Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering , pp 285-287.
[7] N. Bhalaji and A. Shanmugam, A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet, European Journal of Scientific Research, Vol.50, 2011, pp 6-15.
[8] L. Tamilselvan and V Sankaranarayanan, Prevention of Blackhole Attack in MANET, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07, 2007.
[9] C.W. Yu, T.K. Wu, R.H. Cheng, and S. C. Chang, A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks, PAKDD 2007 Workshops, LNAI 4819, 2007, pp. 538–549,.
[10] S. Krishna , A.L Vallikannu, Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism, International Journal of Scientific & Engineering Research, Vol. 1, 2010, pp 1-8.
[11] H. deng, W. Li and D.P. Agarwal, Routing security in wireless AD Hoc networks, IEEE Communications Magazine, 2002, pp 70-75.
[12] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon and K. Nygard, Prevention of cooperative black hole attack in Wireless Ad Hoc network, pp 1-7.