International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-5, May 2015

"TEMPT algorithm to defend MANET from malevolent nodes causing black hole attack"

Shweta singh, Ankita Dixit, Kushal Gupta

***Abstract*— Mobile Ad hoc network is a type of wireless network that operates without any infrastructure and base station. In MANET, communications formed are temporary. Nodes in an Ad hoc network are highly mobile thus the topology of the network formed is also dynamic, nodes may join or leave the network at any time. Mobile Ad hoc networks are mainly used at places where it is difficult to establish infrastructure like in military and rescue from disasters where a infrastructure can not be organise. Due to above mention characteristics of MANET it is highly vulnerable to security attacks. The most common attack in MANET is Blackhole attack. Blackhole attack is a security attack in which the Malevolent nodes transmits a malicious broadcast advertising that it has the shortest path to the destination and thus drops or discards all the packets without forwarding them to the real destination. In this paper, a simple algorithm is proposed to detect and prevent blackhole attack in MANET.**

***Index Terms*— Blackhole, MANET, DSR.**

I. INTRODUCTION

MANET(Mobile Ad hoc Network) is a network that consists of a number of nodes or mobile devices that organizes a network only when it is required. Connection is Connection is initiated when a source node wants to send a data packet to a destination node. Routing in MANET is necessary to find a route from the source the destination, Routing in MANET is difficult due to its changing topology and limited bandwidth thus for this purpose various routing protocols are used such as AODV(Ad hoc On demand distance vector routing) and DSR(Dynamic Source Routing)[1]

Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attack.Due to the Changing topologyand lack of a stationary infrastructure MANET is not fully secure and is vulnerable to a number of network layer security attacks like Blackhole attack.[3][2]

Blackhole attack is a security threat in which a malicious node drops all the data packets that passes through it and shows itself to be a destination to the source node by showing the highest sequence number and take all the packets from the source node and than drop those packets.[5]

In this paper a new method to detect and prevent blackhole attack in MANET is proposed by using the "TEMPT RREQ" and then Reverse Route method is applied to detect exact malicious node.

Shweta singh, Computer Science Department, DIT University,Dehradun,,India,8171424469.

Ankita Dixit, Computer Science Department, DITUniversity, Dehradun, India,8853880135.

Kushal Gupta, Computer Science Department, DIT University, Dehradun, India,8739055052

II. DYNAMIC SOURCE ROUTING

DSR is a reactive protocol and hence it establishes a route to the destination when demanded by the source node. Control messages are used by nodes to communicate with each other. Distinguish feature of DSR is the use of Source Routing i.e. the sender has the complete path information to the destination. Routes are stored in route cache. In DSR when nodes do not have a path to the destination in the route cache it initiates a Route Discovery process.[6]

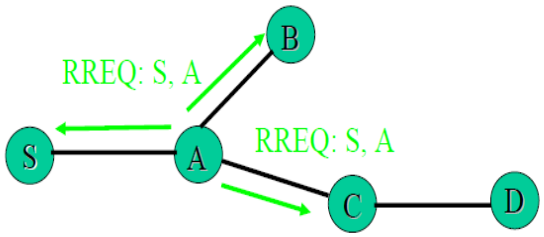

Fig 1.1 RREQ in DSR

Route Discovery phase

Route creation is the procedure used in DSR to find and create a new path between sources to destination.The Originator or the source node broadcasts Route Request (RREQ) message to its neighbouring nodes.If Intermediate node has a path to destination then they sends a RREP to the destination,otherwise rebroadcasts the RREQ to the neighbouring node.Destination node unicasts the RREP back to the originator node.RREP contains the reverse path the RREP packet had traversed.[12][15]

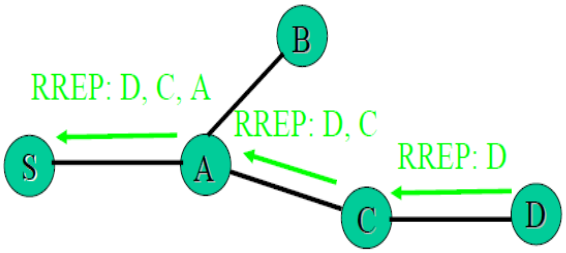

Fig. 1.2Route reply in DSR

Route Maintenance phase Route Maintenance is the mechanism in which a packet sending node S detects if the topology has changed and it can no longer use its route to the destination D because route have moved out of range of each other. When broken route is detected by using Route

Maintenance, node S is informed about it using a ROUTE ERROR packet [6][4]

III. BLACKHOLE ATTACK

In black hole attack, when an originator node broadcasts a RREQ for a destination, the malicious node upon receiving the RREQ packet it immediately sends a fake RREP to the originator node with higher sequence number showing that it has the fresh route towards destination [12]. Originator node discards the RREP packets it receives from other nodes having genuine route and forward all of its packets to the malicious node. A malicious node drops all the data packets it receives.

Fig.is an example of Blackhole attack in which node the originator node 1sends RREQ to find a fresh path to the destination node 4 but the malicious node 3 sends the RREP with the highest sequence number (or claims to have fresh route).

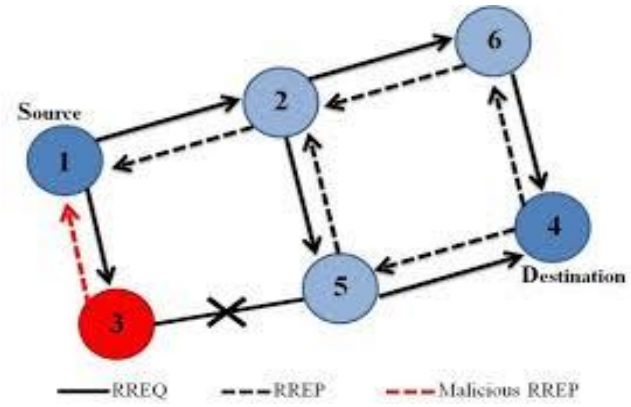

Fig.1.3Example of Blackhole attack

.Originator node 1 will send all the data packets to the malicious node, discarding other RREP. Attacker node drops all the data packets and thus real destination will never receive the data packets. Types of blackhole attack in MANET. 1.)Single Black hole Attack:In single black hole attack, only a single node acts maliciously in a network. Single Blackhole attack is easy to detect and prevent.[14][15] 2.) Collaborative Black hole Attack: In this type of attack, two or multiple nodes act maliciously in a network .It is also known as Blackhole attack with multiple malicious. Due to attacks performance of the protocol used decreases, thus to secure the network various techniques are introduced. Several research efforts were launched to counter against this attack.

Mobile Ad-hoc Networks must have a secure way for transmission of data packets and communication because attacks decrease the network performance. Thus, to provide secure communication and transmission in a network, several counter measures were launched and many of them are successful in providing security but each method has some drawbacks.[7][8][13]

IV. PROPOSED WORK

Blackhole attack is a security threat in which a malicious node attracts all the data packets by sending a fake RREP packet to a source node that initiates the route discovery and pretend to be a destination node itself or a node immediate neighbor of the destination. Source node forwards all of its data packets to the malicious node which were intended for the destination.

DSR protocol is an on demand protocol.Although, DSR knows the address of all the nodes in the route after the source node receives the RREP, but the source node cannot identify which intermediate node has the route information to destination node and reply RREP. There is no security mechanism used in this protocol and there is no attack detection mechanism in DSR, this situation make the source node sends packets to the shortest path that the malicious node claim and the network suffer black hole attack that causes packet loss. However, the network that uses DSR cannot know which malicious node cause the loss.

The proposed a technique to detect Blackhole attack named as "TEMPT RREQ", based on the DSR routing protocol which is able to detect and prevent malicious nodes launching single and cooperative blackhole attacks.

It uses a proactive defense technique, and the source node randomly cooperates with adjacent node. By using the address of the adjacent node as the new destination address, it tempts malicious nodes to reply RREP and detects the malicious nodes by using the reverse routing technique and thus prevents attacks. My Technique is based on DSR algorithm .Some Modifications are done to DSR algorithm.

Algorithm

SN: Source node

AN: Adjacent node

1.) SN broadcasts "TEMPT RREQ'"

2.) If SN receives RREP for the TEMPT "RREQ" from any node saying it has route to destination.

3.) Malicious node exists in the Reply Routing

4.) (a)SN apply Reverse Route Method to find trusted nodes in the route

4.) (b)Node switch to promiscuous mode to find malicious node

4.)(c)If a malicious node is found put that malicious node in Blackhole list

5.) else

6.) SN initiate Route Discovery

7.) If AN do not send RREP

8.) List AN directly on the blackhole list

9.) else if Only AN send RREP

10.) No malicious node exists in the network

11.) Then SN initiate Route Discovery but not using route provided by the AN.

The proposed technique to detect Blackhole attack named as "TEMPT RREQ", is based on the DSR routing protocol which is able to detect and prevent malicious nodes launching single and cooperative blackhole attacks. It uses a proactive defense technique, and the source node randomly cooperates with adjacent node. By using the address of the adjacent node as the new destination address, it tempts malicious nodes to reply RREP and detects the malicious nodes by using the reverse routing technique and thus prevents attacks. My Technique is based on DSR algorithm .Some Modifications are done to DSR algorithm.

"TEMPT RREQ"

In this technique, address of one hop neighbor node is used as destination address in the "TEMPT RREQ`" to tempt malicious node to send a RREP message, and malevolent nodes are detected using Reverse Route technique. Hello message is transmitted to help each node to identify the adjacent nodes within one hop. If other nodes in addition to adjacent nodes reply RREP then malicious nodes exist in the reply routing, and reverse route technique is applied to detect malicious nodes

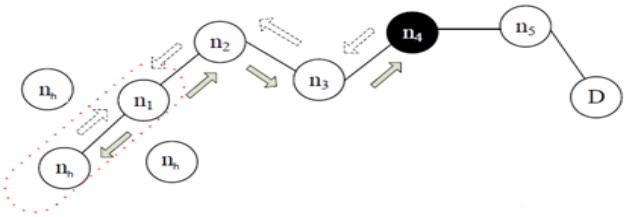

Fig.1.4Choosing a random node to send "TEMPT RREQ"

Reverse Route Technique

This technique detects the malicious node by using route reply of the "TEMPT RREQ". This method is applied on the nodes receiving the RREP, to detect the (a) information of the doubtful path and (b) temporarily trusted nodes. This method detects multiple malicious nodes.

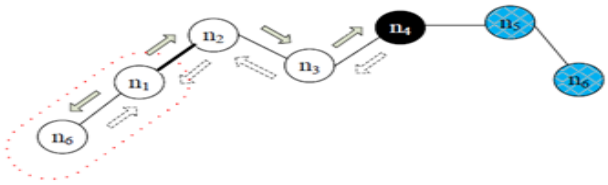

Fig1.5 Reverse route method

In the above example, Source node n1 uses the address of n6 as the destination address in the "TEMPT RREQ'" to tempt the malicious node. Suppose if only there is a malicious node n4 that replies with a fake RREP to the Tempt RREQ with the address list

A= {n1 n2 n3 n4 n5 n6}

When n3 would receive the reply RREP by n4, it will separate the list A by destination address of node n1 of RREP and get a list

H3= {n1 n2 n3}

Now the set difference is calculated between lists A and H3

H'3= A – H3

H'3= {n1 n2 n3 n4 n5 n6} – {n1 n2 n3} = {n4 n5 n6}

Result list of H'3 is stored in RREP and send to the source node. Nodes n1 and n2 also performs the same operation on receiving RREP and thus we getH'2={n3,n4,n5,n6} and H'1 ={n2,n3,n4,n5,n6} and are send back to the source node.

(a) Finding Malicious Path

To find the malicious path 'M' from the obtained lists we perform intersection of the list obtained by the set difference.

M= H'1∩ H'2∩H'3

M= {n4 n5 n6}

(b) Finding Temporarily Trusted Nodes

M is the doubtful path and a set of temporarily trusted nodes 'T' can be calculated as T = A – M

Where A = Address list obtained through RREP And M = Malicious path obtained after intersection

T ={n1 n2 n3 n4 n5 n6}- {n4 n5 n6}

T= {n1 n2 n3}

To, confirm that no malicious node exists in the Trust set. Source node sends a recheck message to node n2, requesting it to enter the promiscuous mode to listen to n3 and sends back the listening results to n1, thus node n4 is detected.

Now, n3 sends the packet to the n5 directly intercepting n4, and n5 would either drop the packet or would send the packets to the other malicious node n4 in co-operation.

Nodes n4 and n5 are detected and their co-operation is stopped. Thus, multiple blackhole attack in co-operation can be detected by using this method.

V. CONCLUSION

MANET network is a collection of mobile nodes which are dynamically and self-organized in temporary topologies, thus MANET is vulnerable to a number of attacks. Blackhole attack is a common attack in MANET. Various detection and prevention techniques for blackhole attack were given by many researchers, but every method faces some problems like delay and overhead. The proposed technique of "TEMPT RREQ" DSR routing is modified and the address of adjacent node is used as the destination address in the "TEMPT RREQ" to entice the malicious node, finally detected malicious node is listed onto the blackhole list and others nodes are inform to stop communication with the malicious node. Main Objective of the "TEMPT RREQ" method is to detect and prevent single as well as multiple blackhole in the network and the method is able to detect and prevent blackhole nodes in the network and provides security and detection mechanism which is not provided in DSR. TEMPT RREQ provides better packet delivery ratio then the DSR. Thus the proposed technique can reduce packet loss and gives better packet delivery ratio.

REFERENCES

[1] Sunil Taneja and Ashwani Kush, A Survey of Routing Protocols in MANET, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010

[2] Priyanka Goyal1, Vinti Parmar2, Rahul Rishi MANET: Vulnerabilities, Challenges, Attacks, Applications IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

[3] Dr.Wibowo, Joshua Muscatello,Joshua Martin " Wireless Network Security"

[4] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002

[5] BingWu,JianminChen,JieWu,MihaelaCardei A Survey on Attacks And Countermeasures in Mobile Adhoc Networks. WIRELESS/MOBILE NETWORK SECURITY @ 2006 Springer

[6] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.

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

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6thAnnual International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.

[9] W. Wang, B. Bhargava, and M. Linderman, “Defending against collaborative packet drop attacks on MANETs,” in *Proc.* 28*th IEEE Int. Symp.ReliableDistrib. Syst.*, New Delhi, India, Sep. 2009

[10] V. K and A. J PAUL, “Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks,” 2010 InternationalJournal of Computer Applications, Vol. 1, No.22, 2010 43

[11] Bhalaji, N. and Shanmugam, A. Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET. Journal of Advances In Information Technology, May 2011, 2(2), pp. 92-98.

[12] Dadhania, P., and Patel, S. Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks. Performance Evaluation, International Journal of Engineering Research and Applications(IJERA), 2013, 3(1), pp. 1487-1491

[13] Mittal, S., and Taluja, H. Analysis of Cooperative Black Hole Attack Using Dynamic Source Protocol. International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), August 2012, 2(8), pp. 139-142.

[14] S. amaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative blackhole attacks in wireless ad hoc networks,” in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[15] B.Revathi,D.Geetha, A Survey of Cooperative Black and Gray hole Attack in MANET, International Journal of Computer Science and Management Research,2012