International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-3, February 2013

Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol

Nishu kalia, Kundan Munjal

Abstract: *Mobile Ad hoc Networks (MANET) is a self-configuring, infrastructure less network consists of independent mobile nodes that can communicate via wireless medium. Each mobile node can move freely in any direction, and changes their links to other devices frequently. Security is an essential part of ad hoc networks. Due to its dynamic topology, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks and black hole attack is one of them. In this attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. In this paper, a mechanism to detect the multiple black hole nodes has been proposed by modifying AODV protocol.*

Keywords: *MANET, fake RREQ, Record field, multiple black hole nodes.*

I. INTRODUCTION

Wireless networks have been gaining popularity to its peak today, as the user wants wireless connectivity irrespective of their geographic position. The nodes in wireless network can communicate with each other directly or via some centralized infrastructure. With centralized infrastructure, we need a central controller like base station to provide communication and authentication. But in ad hoc networks, there is direct communication between nodes without any central controller which leads to security threats. The nodes in ad hoc networks act as a host as well as router to forward the data packets. MANET is widely used in military purposes, sensor networks, rescue operations, personal area networks etc.

As the topology of MANET changes frequently, it is vulnerable to various security threats. The routing protocols are exploited by the attackers with the aim to intercept the data packets. In MANET, we have three types of protocols i.e. Proactive, Reactive and Hybrid protocols. Proactive protocols (DSDV, OLSR) are table-driven protocols in which the nodes maintain and update the routing tables periodically even when there is no communication. But in reactive protocols (AODV, DSR) or On-Demand Protocols, the routes are discovered on the demand of the source node. Proactive protocols have low latency rate in discovering the route but high routing overhead. This is because the nodes periodically exchange control messages and routing table information in order to keep up-to-date routes to any active node in the network. The reactive protocols have the low routing overhead at the expense of delay to discover the route when desired by the source. Due to periodically exchange of routing information, the proactive protocols are less prone to security attacks (black hole, Sybil attack etc) as compare to reactive protocols. The hybrid protocols (ZRP) have the combined features of both reactive and proactive protocols. The control packets (Route Request, Route Reply) can be forged to intercept the normal functioning of reactive protocols. Mostly, the researchers have more focused on securing the AODV and DSR from different types of attacks and black hole attack is one of them. A lot of schemes have been proposed on detecting and preventing the black hole attack but these schemes have some pros and cons too.

In AODV, the RREQ (Route Request) packet is sent by the source to discover the route. If the intermediate node has the fresh enough route towards the destination, it can reply the RREP packet back to the source. Otherwise, broadcast the RREQ packet to other nodes in the network. In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. If the source node receives more than one RREP packets, it will select the route with highest destination sequence number or minimum hop count. In case black hole attack, the malicious node forges the RREP packet by having the highest destination sequence number to advertise itself as a shortest path towards the destination. Then, the source node believes the malicious node and starts sending the data packets towards that node and malicious node will start dropping the data packets. It may happen that more than one malicious node exists in the network at different places.

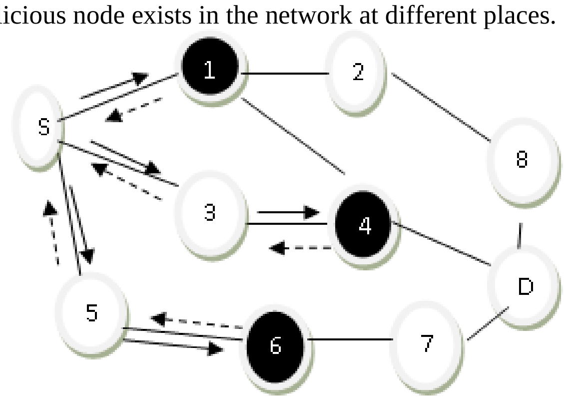

Figure 1. Multiple Black hole nodes.

Manuscript published on 28 February 2013.
***** Correspondence Author (s)
Ms. Nishu Kalia, Research Student, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.
Mr. Kundan Munjal, Assistant Professor, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.

In above figure, there are more than one black hole node i.e. 1,4 and 6 exists in the network at different places in order to drop the data packets.

II. RELATED WORK

H. Deng [4] proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. By using this method, the routing overhead and end to end delay will be increased. If the black hole nodes work as a group in an attempt to drop packets, then this method is not efficient.

Mohammad Al-Shurman [15] proposed the two methods to avoid the black hole attacks. According to the first solution, the source node verifies the validity of the route by finding more than one route to the destination. It waits for RREP packets to arrive from more than two nodes. When the source node receives RREP packets and the routes to destination have shared hops, the source node can then recognize the safe route. This method causes routing delay. The second solution is to store the last packet sent sequence number and the last packet received sequence number in a table. When node receives reply message from another node it checks the last sent and received sequence number. If there is any mismatch, then the ALARM packet is broadcasted which indicates the existence black hole node. This mechanism is reliable and faster having no overhead.

Latha Tamilselvan [9] proposed the solution in which the source node waits for the responses including the next hop details from other neighboring nodes for a predetermined time value. After the timeout value, it first checks in the CRRT (Collect Route Reply Table) table, whether there is any repeated next-hop-node or not. If any repeated next-hop node is present in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited. The solution adds a delay and the process of finding repeated next hop is an additional overhead.

Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan [12] provide an improvement over the solution given in the paper [1] in which Source Intrusion Detection (SID) method is used. The SID mechanism is good for small scale MANET but when this mechanism is applied in a large scale MANET and the distance between the source node and the intermediate node is long, then the above solution is not sufficient. Secondly, if the distance between the source node and the intermediate node is long, the delay in the discovery period of the route will be high, which causes an overall network performance degradation. In order to mitigate the drawbacks in SID security routing mechanism, a new mechanism called Local Intrusion Detection (LID) security routing mechanism is proposed to allow the detection of the attacker to be locally; which means that when the suspected intermediate node unicast the RREP towards the source node, the previous node to the intermediate node performs the process of detection and not the source node.

Yiebeltal Fantahun Alem, Zhao Chenh Xuan [13] proposed an Intrusion Detection using Anomaly Detection (IDAD) technique to prevent the black hole attack. IDAD assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. To do so an IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data is collected and is given to the IDAD system, the IDAD system can compare the every activity of a host with the audit data on a fly. If any activity of a host (node) resembles the activities listed in the audit data, the IDAD system isolates the particular node by forbidding further interaction. It minimizes the extra routing packets which in turn minimizes the network overhead and facilitates faster communication.

S.Marti, T.J.Giuli, K.lai and M.bakery [14] proposed the Watchdog/Pathrater as a solution to the problem of selfish (or “misbehaving”) nodes in MANET using DSR protocol. The Watchdog method is used to detect misbehaving nodes and the Pathrater, to respond the intrusion by isolating the selfish node from the network operation. Watchdog runs on each node. When a node forwards a packet, the node’s watchdog module verifies that the next node in the path also forwards the packet. The Watchdog does this by listening in promiscuous mode to the next node’s transmissions. If the next node does not forward the packet, then it is considered to be misbehaving and is reported. The Path rater module uses the information generated by Watchdog to select a better route to deliver the packets, avoiding the selfish nodes.

K. Lakshmi et al [11] enhances the AODV protocol. In AODV protocol, the destination sequence number is 32-bit integer associated with every route and is used to decide the freshness of a particular route. If the sequence number is largest, the route will be fresh enough. In this method, all the sequence numbers mentioned in RREP packet is stored along with the corresponding node ID in a RR-table (Route Request). Then, if the first destination sequence number in table is much greater than the sequence number of source node. That node will be identified as malicious node and the entry will be immediately removed from the table. The proposed solution also maintains the identity of the malicious node as MN-Id, so that the control messages from that node can be discarded. In addition, there is no need to forward the control messages from that malicious node.

Moreover, in order to maintain freshness, the RR-Table is flushed once a route request is chosen from it.

DRI Table and Cross Checking [16] Scheme is used to identify the cooperative black hole nodes. Each node maintains the extra DRI table with two entries ‘From’ and ‘Through’, where 1 represents for true and 0 for false. These entries stand for the information on routing data packet from and through the node. In this solution, the Intermediate node replies the next hop information and DRI entry about next hop node along with RREP packet. The source node then checks the reliability of intermediate nodes by using cross checking scheme via alternate paths by using DRI table information. It provides 50 % throughput but increases end to end delay and routing overhead.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

III. PROPOSED SCHEME

In this paper, we proposed the solution to detect the multiple black hole nodes that can exist in the MANET. This method uses the fake RREQ message to attract the malicious node to respond the fake RREP message. In our scenario, there is more than one malicious node who will reply the fake RREQ packet. In this mechanism, before discovering the actual route for data transmission in AODV, a fake RREQ packet is broadcasted which includes the target or destination address which does not exist in reality. The multiple black hole nodes will immediately respond to the fake RREQ packet as they do not care about whether the fake target addressed node exists or not in the network

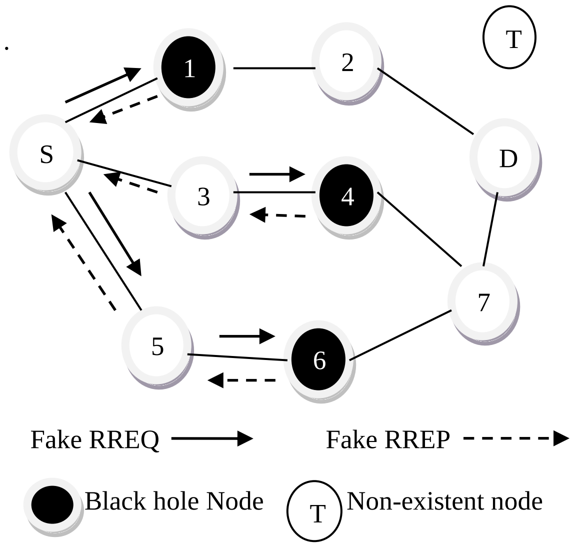

Figure 2. Sending fake RREQ packet.

Then, the RREP packet will be sent by those multiple black hole nodes. The RREP packet is here enhanced by adding one more field as Record Field using the reserved bits of RREP packet. This field is used to contain the information about the identity of the node who replies the RREP packet to the source node. When any node in the network reply RREP packet, its identity will be recorded into Record field. So, if any intermediate node sends the RREP packet in response to the fake RREQ, it can be easily traced or detected.

In figure 2, we have three black hole nodes located at different places in the network named as 1, 4 and 6. Before the initiating the actual route discovery process in AODV, the source node broadcast the fake RREQ message with fake target address of node T (non-existent node) to the neighboring nodes 1, 3 and 5. The normal nodes having no malicious behavior will not reply to the fake RREQ message as they have no route to that virtual node T. The malicious nodes 1, 4 and 6 will reply the RREP packet as advertising the shortest path towards the destination node (T). The identity of these nodes will be recorded into the Record field of the RREP packet. When the source node S receives the multiple RREP packets, from the Record field it will be able to trace the identity of malicious nodes. These identities will be added to the black list and this list will be broadcast as an ALARM packet to all the nodes in the network. Then, these multiple black hole nodes will be isolated from the network. After isolating the multiple black hole nodes, the normal route discovery process in AODV will be initiated. The data is then routed to the destination. If the packet delivery ratio is down to some threshold value that has been decided on the basis of average packet delivery ratio (threshold value). Also, the end to end delay is checked if it is more than the average end to end delay of data packets, then there will be chances of attack. The threshold values for packet delivery ratio and end to end delay is taken as the average of normal PDR and end to end delay of data packets respectively. Then, again the source node will restart the process of broadcasting fake RREQ packet to detect the single or multiple black hole nodes.

IV. ALGORITHM:

Notations:
SN: Source Node IN: Intermediate Node
DN: Destination Node

1. Start();{
2. SN broadcast the fake RREQ packet with non-existent target address;
3. If(one or more IN or Non-existent target nodes reply back the fake RREP packet to SN){
4. Trace the single or multiple black hole nodes from Record field of RREP packet;
5. Add the traced malicious nodes to the black list;
6. Broadcast an ALARM packet (having black list) to let the other nodes know about the traced malicious nodes;
7. Isolate the black listed nodes from the network;
8. Normal_AODV();{
9. Start();{
10. SN broadcast the fake RREQ packet with non-existent target address;
11. If(one or more IN or Non-existent target nodes reply back the fake RREP packet to SN){
12. Trace the single or multiple black hole nodes from Record field of RREP packet;
13. Add the traced malicious nodes to the black list;
14. Broadcast an ALARM packet (having black list) to let the other nodes know about the traced malicious nodes;
15. Isolate the black listed nodes from the network;
16. Normal_AODV();{
17. Initialize the normal AODV route discovery process and route maintenance process;
18. Routing the data packets;
19. If(packet delivery ratio<threshold_value1 and end to end delay>threshold_value2)
20. Start();
21. }}
22. Else
23. Nodes in the network are safe;
24. Normal_AODV();
25. }
26. }

Basically, this mechanism enhances the security of AODV protocol with low routing overhead than other methods [14] [16] [17] in MANET. The detection of single or multiple black hole nodes have done early before initializing the route discovery process in AODV. It makes this method more effective. After the detection process, there is an additional check to find out the packets are again dropped or not during normal transmission of data packets after normal route discovery process.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This additional check is calculating the packet delivery ratio, if it comes down to some threshold value (average PDR). And also, if end to end delay, the time taken for the data packets to transfer from source to destination, is more as compare to the average end to end delay of data packets (threshold_value2). Then, there is the maximum chance of existence of black hole nodes. Again, the detection mechanism will be started.

V.CONCLUSION & FUTURE WORK

This paper is an enhancement to the AODV protocol by proving more security after detecting the single or multiple black hole nodes in MANET. By using fake RREQ packet and modified RREP packet, the multiple black hole nodes are detected at the initial stage before the actual route discovery process of AODV. It leads to less routing overhead and high packet delivery ratio. The parameters like PDR, end to end delay is used for checking if packets are dropped again or not, so that again detection can be done. So, whenever there is change in PDR and end to end delay as compare to average PDR and average end to end delay, there is need to detect the malicious node. In future, we will implement this mechanism in network simulator (NS2). And also, do experiments in enhancing the AODV protocol to detect the cooperative black hole and gray hole attacks.

REFERNCES

[1] http://cwi.unik.no/images/Manet_Overview.pdf

[2] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Issue 3, Nov 2007, pp 338–346.

[3] Wu B, Chen J, Wu J, Cardei M , " A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Network Security. On Signals and Communication Technology. Springer, New York,2009

[4] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[5] Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[6] S. Ramaswamy, H.Fu, M.Sreekantaradhya, J. Dixon, and K.Nygard, "Prevention of Cooperative black hole attack in wireless ad hoc networks," International conference (ICWN‟03), Las Vegas, Nevada, USA,2003, pp 570-575.

[7] Hesiri Weerasinghe "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, 2008, pp 362-367.

[8] N.Mistry, D.C.Jinwala and M.Zaveri, "Improving AODV protocol against black hole attacks", international multiconference of engineers and computer scientists 2010, vol 2, IMECS 2010, march 17-19 2010, Hong Kong.

[9] LathaTamilselvan and V Sankarnarayana, " Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.

[10] E.A. Mary Anita, V. Vasudevan, "Black Hole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", IJCA, Volume 1, 2011

[11] K. Lakshmi et al. "Modified AODV Protocol Against Black hole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.

[12] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia.

[13] Yiebeltal Fantahun Alem, Zhao Chenh Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anamoly Detection",2nd International Conference on Future Computer and Communication, IEEE, Volume 3, 2010

[14] S.Marti, T.J.Giuli, K.lai and M.bakery "Mitigating routing misbehaviour in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.

[15] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference , 2004, pp 96-97.

[16] 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, 25-27January 2011.

[17] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng (2007) "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network". Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007.

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