CRYPTOGRAPHIC METHOD TO SECURE AD-HOC ON DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL FROM BLACK HOLE ATTACK

[1]Pallavi D. Ingole, [2]Yogesh A. Suryawanshi
[1]M.Tech 4th sem (Electronics Engineering) [2]Department of Electronics Engineering
[1,2]Yeshwantrao Chavan College of Engineering
Nagpur (M.S.), India
[1]ingole.pallavi233@gmail.com, [2]yogesh_surya8@rediffmail.com

***Abstract*- Secure communication is more challenging task in Mobile Ad-hoc Network (MANET). Protocols are the common sets of rules and signals that are used to communicate over network. Ad-hoc On-Demand Distance Vector Routing (AODV) is an on-demand reactive routing protocol designed for operation of MANET. Black hole attack is an attack in which a malicious node drops all packets that it receives instead of normally forwarding those packets. This attack cause to degrade the performance of AODV Protocol and hence affect the performance parameters. To secure and enhance the performance of AODV protocol under Black hole attack, cryptographic method is used. So here, we study the performance parameters like Packet Delivery Ratio (PDR), Average end-to-end delay (AETED) and Throughput under AODV routing protocol.**

***Keywords*- MANET, AODV, PDR, AETED, Throughput**

*****

I. INTRODUCTION

Network is the large number of computers that are separate but interconnected with each other to share expensive resources. Networks are divided into three different types: Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN). There are three basaic characteristics which are used to categorized networks into different types like topology, protocols and architecture. Topology means arrangement of nodes (Computers and other peripheral devices).Different types of topologies are used such as ring, star, bus, tree topology etc.

Protocols are the common sets of rules and signals that are used to communicate over network. Routing protocols in mobile ad hoc network are mainly classified into topology based and position-based approaches.

Topology-based routing protocols are further classified as proactive, reactive and hybrid approaches, use the information about the links that exists in the network to perform packet forwarding. Proactive routing protocols utilize some traditional routing strategies such as DSDV, OLSR, and TBRPF. They maintain and update information on routing between all nodes in a given network at all times. The main drawback of these protocols is that the maintenance of unused paths may occupy a significant part of the available bandwidth if the topology of the network changes frequently. Reactive routing protocols, including AODV, DSR, and TORA, maintain only the routes that are currently in use, and hence help in reducing the burden on the network when only a small subset of all available routes is in use at any time. Hybrid routing protocols combine local proactive routing and global reactive routing strategy in order to achieve a higher level of efficiency and scalability. The salient example of hybrid routing protocols is ZRP.

Position-based routing protocols require additional information about the geographical position of the participating nodes. Each node determines its own position through the use of GPS or other type of positioning services. The prominent examples of position-based routing are LAR and GPSR.

II. AD-HOC ON DEMAND DISTANCE VECTOR (AODV) PROTOCOL

AODV is an on-demand routing protocol designed for operation of mobile ad hoc network. Basically, protocol provides self starting, dynamic, loops free, multihop routing. Protocol allows mobile nodes to establish routes quickly for new destinations as well as to respond to changes in network topology and link failures as only affected set of nodes are notified. Nodes that are not in active communication do not maintain routes to the destinations. So, the new routes are created on demand and control packets are broadcast when needed and hence eliminate the need for periodic broadcast of routing updates. AODV protocol works in two phases a) Route discovery process and b) Route maintenance process.

Route discovery process uses Route Request (RREQs) and Route Reply (RREPs) messages. These routing messages contain information only about the source and the destination nodes. Whenever a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbors to find path. RREQ message contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Sequence number is used for faster convergence, route freshness and loop prevention. When a node sends any type of routing control message like RREQ/RREP, it increases its own sequence number. Every node should include the latest sequence number for the nodes in the network in its routing table. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop count represents the distance in hops from the source to destination. Each node receiving the RREQ message sets up reverse path back to the sender of the request so that RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and discards the RREQ. If the intermediate node receives RREQ with 'G' flag set, it must also unicast gratuitous RREP to the destination node. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP travels along the reverse path. Once the source node receives the route reply, it establishes a route to the destination and sends data packet along forward path set-up.

Route maintenance is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbors about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. When a node does not receive HELLO message within time period from a neighbor node then it detects that a link to that neighbor node has broken then it generates route error message (RERR). RRER message indicates those destinations that are unreachable, their IP address and destination sequence number. In order to inform the link failure information, each node maintains a precursor list for each routing table entry containing the IP address of set of neighboring nodes that are likely to use it as a next hop towards each destination. On receiving this RRER, each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In addition to these routing messages, the route reply acknowledgment (RREP-ACK) message must be sent by sender node of RREQ in response to a RREP message with the 'A' bit set. This provides assurance to the sender of RREP that the link is bidirectional. Each node maintains a routing table with knowledge about the network. AODV deals with route table management.

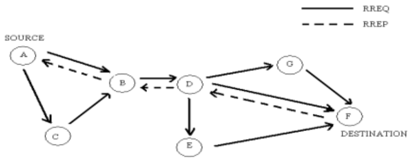


Fig.1 shows network consisting of seven nodes with route messages.

III. BLACK HOLE ATTACK

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires. Malicious nodes take over all routes by attacking all route request messages. Therefore the quantity of routing information available to other nodes is reduced. The malicious nodes are called black hole nodes. For example, source node A wants to send packets to destination node F, in figure2, source node A initiates the route discovery process. Let node C be the malicious node which has no fresh route to destination node F. Node C claims to have the route to destination and sends route reply RREP packet to node A. The reply from the malicious node reaches the source node earlier than the reply from the legitimate node, as the malicious node does not have to check its routing table as the other legitimate nodes. The source chooses the path provided by the malicious node and the data packets are dropped. The malicious node forms a black hole in the network and this problem is called black hole problem.

Fig. 1

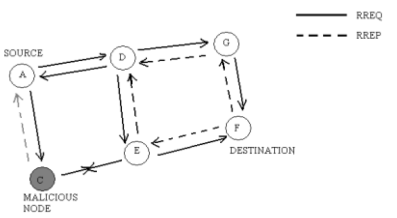


Fig.2 shows Malicious node having Black Hole Attack in the network.

The performance parameters stated above are defined as:-

Packet Delivery Ratio: It is the ratio of number of packets received at the destination to the number of packets sent from the source. The performance is better when packet delivery ratio is high. Average end-to-end delay: This is the average time delay for data packets from the source node to the destination node. To find out the end-to-end delay the difference of packet sent and received time was stored and then dividing the total time difference over the total number of packet received gave the average end-to-end delay for the received packets. The performance is better when packet end-to-end delay is low. Throughput: Packets received in the time interval.

Table1. shows simulation environment

Simulator	NS2
Routing protocol	AODV
Number of mobile Nodes	3
Medium Access Control (MAC) type	802.11
Antenna	Omnidirectional
Maximum number of packets	50
Application Traffic Type	CBR
Packet size	1000

IV. CONCLUSION

Following are the results of cryptographic method under black hole attack for AODV protocol in MANET.

Fig.3 showing network of three nodes under black hole attack after encryption and decryption method.

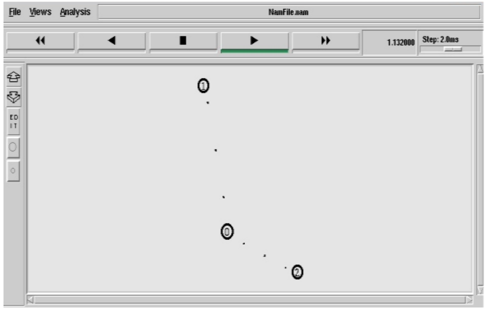


Fig. 4 showing graph of Packet Delivery Ratio for black hole attack after encryption and decryption method.

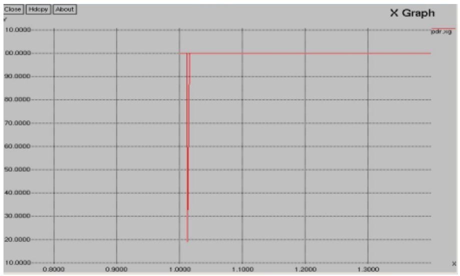


Fig.5 showing graph of Time delay for black hole attack after encryption and decryption method.

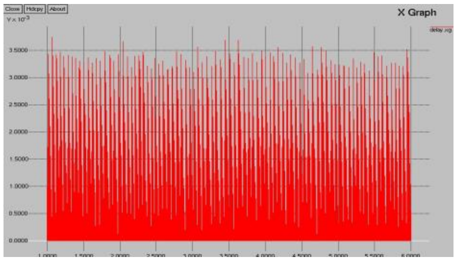
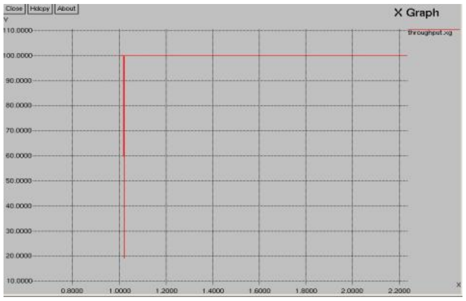


Fig.6 showing graph of Throughput for black hole attack after encryption and decryption method.



WITH BLACK HOLE ATTACK	**WITHOUT BLACK HOLE ATTACK**
PACKET DELIVERY RATIO IS LOW	PACKET DELIVERY RATIO IS HIGH
TIME DELAY IS HIGH	TIME DELAY IS LOW
THROUGHPUT IS LOW	THROUGHPUT IS HIGH

Table 2. Difference between Black hole attack and without Black hole attack on parameters

V. REFERENCES

[1] Preeti Sachan and Pabitra Mohan Khilar, "Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[2] Monika Roopak, Dr. Bvr Reddy, "Performance Analysis of Aodv Protocol under Black Hole Attack", International Journal of Scientific & Engineering Research Volume 2, Issue 8,August-2011.

[3] Mohd Anuar Jaafar, Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment" European Journal of Scientific Research,ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443 © EuroJournals Publishing, Inc. 2009.

[4] Satyendra Singh, Vinod Kumar Yadav, Ganesh Chandra, Rahul Kumar Gangwar, "An Efficient and Improving the Security of AODV Routing Protocol" IJCST Vol. 3, Issue 1, Jan. - March 2012.

[5] Emmanouil A.Panaousis, Tipu A. Ramrekha, Grant P. Millar, and Christos Politis, "Adaptive and secure routing protocol for emergency MANET", International Journal of wireless and mobile networks (IJWMN), Vol.2, No.2, May 2010.

[6] Kamarularifin Abd Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Securing Routing Table Update in AODV Routing Protocol", 2011 IEEE conference on open systems(ICOS2011),25-28Sept,2011.