Advanced AODV Protocol for the Detection and Elimination of Black Hole Attack in MANET's

Bharathi M[#1], Dr. Mydhili K Nair[#2], Sukruth Gowda M A[#3]

[#1]*PhD Student, Dept., of IS&E, MSRIT, Bengaluru, Karnataka, India*

[#2]*Associate Professor, Dept., of IS&E, MSRIT, Bengaluru, Karnataka, India*

[#3]*M.Tech Student, Dept., of CS&E, SJCIT, Chickaballapura, Karnataka, India*

Abstract* — *A temporary network established when only the communication is required, which is a collection of wireless nodes, communicating with the wireless links is MANET's. Because of its dynamic, distributed, infrastructure less and decentralized nature, it will be in more risk of attacks. Due to which secured routing protocols are used to overcome it. One among such attack is black hole attack, where a malicious node pretends itself as authentic and stating that it has path from source to destination and access all the information and drops it. The present reactive protocol AODV fails much in the detection of malicious node due to which the functionality is disturbed. In this proposed methodology, we present a novel security based AODV protocol for detection an elimination of black hole attack.

Keywords: MANET's, Reactive Protocol, AODV, Black Hole.

I. INTRODUCTION

A MANET is a collection of mobile nodes which communicates with wireless links. It is a temporary network, which is decentralized and dynamic. The nodes in MANET's acts as both host and router. These mobile nodes form different topologies based on their connectivity and communication purpose. Due to these characteristics, MANET's are more prone to attacks.

In order to provide complete protected communication and allow for the transmission of packets, the various types of attacks should be understood [12] along with their effects on the MANETs. Wormhole attack [9], Black hole attack, Gray hole attack, Sybil attack, routing table overflow attack, flood attack, selfish node misbehaving, impersonation attack, Denial of Service (DoS) are kind of attacks that a MANET can suffer from.

A security mechanism [8] has to be implemented in the protocol to overcome it. There are various protocols like AODV (Ad hoc On-Demand Distance Vector), OLSR (Optimized Link State Routing), DSR (Dynamic Source Routing), DSDV (Destination Sequence Distance Vector), ZRP (Zone Routing Protocol) and so on. Most of the implementations make use of AODV protocol in MANET's.

The main goal of AODV security mechanism is to provide security concerns [10-11] like authentication, confidentiality, integrity etc.. But the present protocol structure still has deficiency in identification of the black hole attack. In this research paper, we propose an advanced AODV protocol to detect and eliminate the black hole attack and increase the performance of communication in terms of packet delivery ratio, detection of malicious nodes etc..

II. RELATED WORK

Many updations have been going on with regard of securing the attacks by providing secure protocols.

T. Manikandan et.al [2] in their research work proposed a method to detect selective black hole by using the promiscuous mode implementation technique after identification of black hole attack which is applicable only for proactive protocols.

Ei Ei Khin and Thabdar Phyu [3] simulated for the analysis of impact of the black hole attack on AODV protocol by using metrics like packet delivery ration, average end to end delay etc. which results in stating that the AODV performance is decreased due to black hole attack.

Latha TamilSelvan et.al [4] proposed a modified version of AODV protocol, which avoids the black hole nodes which are in group. They used a fidelity table, where each node will be assigned with fidelity level specifying the reliability of that node. If the level is 0 means, it indicates black hole and is eliminated from network. It adds more delay in network communication.

Romina Sharma and Rajesh Shrivastava in their work [1] proposed modified AODV protocol. The protocol is added with FRREQ (Further route request) which will be sent after RREQ and FRREP (further route reply) which will be generated only by the reliable nodes, so that the malicious nodes can be avoided. But this may increase the routing overhead.

Ramanpreet Kaur et.al [7] in their research presented an artificial neural network approach for the detection of black hole. A Feed Forward Back propagation learning algorithm for network type is implemented.

Bhoomika Patel and Khusboo Trivedi [5] in their survey paper against the AODV protocol for detection of black hole attack, has mentioned various ways of AODV protocol like ABM (Anti-Black Hole Mechanism), DPRAODV (Detection, Prevention and Reactive AODV), Honeypot based detection, ERDA (Enhance Route Discovery for AODV), Cryptographic based technique.

Abolfazl Akbari et.al [6] proposed a new AODV protocol for route breaks in the network. A new route maintenance algorithm is proposed where an active node detects the link break to maximum level and re-establishes a new route before break.

III. BLACK HOLE ATTACK

Black hole attack is a type of Daniel of Service attack, where the malicious node or the black hole advertises itself to the source node or the neighbouring nodes that it has the shortest path to the destination or will request for path to perform communication as if a source node. By accessing all the information when it receives the data packets from the source node or other nodes it drops all the packets or may forward to the nodes whose address in undefined. Due to which there will not be any communication between source and destination, which will not even known to them.

There are various types of black hole attacks. Based on the count of malicious nodes, there are single black hole attack, where only one attacker node will make the routing malfunction and cooperative black hole, where multiple malicious nodes will combine together for disturbing the functionality by overcoming the security mechanisms.

Based on the position of attacker, there are internal black hole attack which will be in the interior of existing network topology where the malicious node will be present and external black hole attack, where in which the malicious node which will be in some other network behaves as it belongs to the current network by updating the routing table even though it belongs to different network.

Based on the modification of control packet, there may be RREQ type attack where the black hole nodes sets its hop count minimum so that all the nodes will use this malicious node for broadcasting the RREQ packet and RREP based attack, where the attacker node will generate the fake RREP message after receiving the RREQ from the source node.

The above figure 1 explains the black hole attack. The node S which is the source node sends RREQ to packets to all the neighbouring nodes. The node A, node B, node M in turn will send the RREQ to other nodes since it doesn't have route to destination node D.

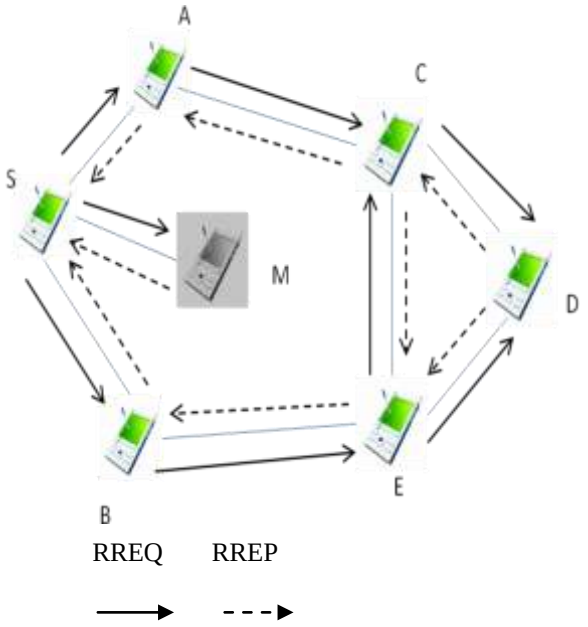

Fig 1: Black Hole Attack

After reaching there is path from node C and node E to the destination node with the hop count and sequence number will return the path to source using RREP packet. But the node M which is the attacker node will reply to the source node S stating it has the minimum path to the destination D and drops all the packets received from the source node S.

IV. AODV

AODV is a reactive routing protocol where in which each node maintains a routing table and updated as per the changes in the topology or network. Based on the receival of control packets like RREP and RREQ there will be regular updations to the routing table, which even maintains the sequence number along with the hop count information.

Two phases in the protocol Route Discovery and Route Maintenance. In the first phase route discovery, the source node sends a RREQ packet to its neighbouring nodes to find the path to the destination.

The nodes receive the RREQ and modify the routing table and if no route is available in the routing table it again broadcasts the RREQ to other nodes. This process continues until the destination is reached with RREQ. Once the destination receives the control packet RREQ, it creates a reverse route to source and sends unicast RREP to source node with the sequence number or hop count.

When the node receives the RREP, it changes the route to the destination node in the routing table and forwards in reverse route until the source node is reached. Source node receives the RREP, updates its routing table and continues communication with destination.

During the route maintenance phase, to make sure the connectivity of the mobile nodes as they move in or out of the network, a HELLO packet is broadcasted periodically. A timer is set for HELLO packet and broadcasted to the neighbouring nodes, if within the specified time there is no reply from the nodes, then it is assumed that there may be a link failure or any other problem in the network. This will be updated to all the other nodes which are connected with in the network. If there is communication going on between source and receiver then the source node again has to establish a new route to its destination with same route discovery process.

V. Proposed Approach

In the proposed methodology a two way authentication is provide for exchange of control packets and data packets. For each RREQ packet, it will be provided with two security mechanisms, password and digital signatures which mainly uses the quantum cryptography mechanism, due to which even its difficult to analyse the secret key values by analysing the traffic. The secret information will be provided to all the authenticated nodes by the trusted authority.

So whenever the source node sends a RREQ packet, the receiving node has to decrypt it without which it cannot access any information and not able to send RREP packet. The packet will be protected by the password and the digital signatures where the quantum cryptosystem will send the secret information in the form of quanta which will be very complex and difficult to identify and modify it or recover it. The malicious node which generates an RREP to the source node telling it has the shortest path to the destination also has to encrypt the packet making use of password and digital signature.

When the neighbouring node receives the RREP and tries to encrypt it, which leads to the wrong RREP. It identifies the node which has sent the RREP and identifies that it is the malicious node and updates the information. it also generates an alarm packet regarding the malicious node which is a black hole and broadcasts t o all other neighbouring nodes, informing not to include that malicious node for any further communication or to send or receive RREQ or RREP from that malicious node.

In this way we can detect the black hole attack internally or externally by the password security system along with the digital signature method. And also eliminate the black holes by making use of alarm packets generated by the nodes updating the information to trusted authority also for further processing of information with those nodes. To overcome the overhead of the routing table it can be refreshed at regular intervals.
Algorithm:

Step 1: The trusted authority will issue the privacy information to all the authenticated nodes in the network.

Step 2: The source node forwards a RREQ packet by providing the password and digital signature quantum cryptyfied.

Step 3: The node receives the RREQ encrypts with the secret information provided by the trusted authority.

If the node is destination node
Then it generates a unicast RREP encrypts and send back in the reverse route.

Else if the node is intermediate node it again broadcasts to the neighbouring nodes.
END

Step 4: When an RREP packet is received and decrypted

If the node is authenticated node then it updates the routing table and sends in the reverse route.

Else if the decryption of that packet is not possible or gives an error then the node which has sent RREP is treated as malicious node.

An alarm signal packet is generated regarding the malicious node and broadcasts to all the nodes to updated their routing table regarding the attacker node. The same information is updated to trusted authority also for further action.
END

Step 5: Once the RREP is received by the sender from destination through the intermediate nodes the communication will be established.

Step 6: Stop.

The main advantages of the system is high level security is provided by the two way secure mechanism using quantum cryptography. Even it will be difficult to analyse the data or control packet information by the traffic analysis. So that the protocol works well in the detection and elimination of black hole attack.

VI. Experimental Setup.

The experimental work is still ongoing making use of ns2 simulator and verification has to be done for parameters like packet delivery ratio, end to end delay, throughput, packet drop ratio, packet misroute ratio.

VII. Conclusions

Making the communication secure is the main goal in any network. Many challenges have to be faced while implementing any protocol in MANET's. In this paper we propose an adaptive AODV protocol which makes use of secure mechanisms available to overcome almost all types of black hole attacks. This improves the performance in detection and elimination of attacks.

REFERENCES

[1]Romina Sharma, Rajesh Shrivastava, "Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network", IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[2]T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj, "Removal of Selective Black Hole Attack in MANET by AODV Protocol", International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014, ISSN (Online) : 2319 – 8753, ISSN (Print) : 2347 – 6710.

[3]Ei Ei Khin and Thandar Phyu, "Impact Of Black Hole Attack On Aodv Routing Protocol", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014 DOI : 10.5121/ijitmc.2014.2202 9.

[4]Latha Tamilselvan, V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET", Journal of Networks, vol. 3, no. 5, pp. 13-20, May 2008.

[5]Bhoomika Patel, Khushboo Trivedi , "A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET", International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2816-2818, ISSN:0975-9646.

[6]Abolfazl Akbari, Mehdi soruri and Ali Khosrozadeh, "A New AODV Routing Protocol in Mobile Adhoc Networks", World Applied Sciences Journal 19 (4): 478-485, 2012 ISSN 1818-4952; © IDOSI Publications, 2012 DOI: 10.5829/idosi.wasj.2012.19.04.2574.

[7]Ramanpreet Kaur, Anantdeep Kaur, "BLACKHOLE Detection In Manets Using Artificial Neural Networks", International Journal For Technological Research In Engineering Volume 1, Issue 9, May-2014 ISSN (Online): 2347 – 4718.

[8] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks," In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, 12-15 Nov. 2002.

[9] J. W. Creswell, Research Design: Qualitative, Quantitative and Mixed Methods Approach, 2nd Ed, Sage Publications Inc, California, July 2002.

[10]V.Mahajan, M.Natue and A.Sethi, " Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[11] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.

[12] H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.