Modified AODV Techniques for Detection and Prevention of Gray Hole Attack in MANET

Shayog Sharma[1], Gyanender Kumar[2], Kapil Saini [3]
Assistant Professor, ECE Department, GEC, Panipat[2]
Assistant Professor, CSE Department, GEC, Panipat[1, 3]

***Abstract*- Compared the On-Demand (DSR and AODV) and Table-Driven (DSDV) routing protocols by dynamic the nodes variety and evaluated the metrics end-end late, packet delivery ratio, packets dropped, throughput. Just in case of packet delivery ratio, AODV performs high than DSDV once variety of nodes are high, however DSDV performs higher than 2 protocols in as so much as throughput is concerned. So, in real time traffic state of affair AODV is favoured as compared to DSR and DSDV.**

Further, the gray holeattacker selects solely those real nodes through quite a threshold variety of different methods gothrough, thereby facilitating the gray hole attacker to use less variety of nodes. Therefore, the gray holeattack scheme is power aware. Finally we have a tendency to additionally proposeIDSto discover the proposed energy aware Grayhole attack. NS2 experimental results show the validity of the proposed attack.

Keywords:- AODV, RREQ, RREP, IP

I. INTRODUCTION

Mobile ad hoc network (MANET) could be assortment of wireless mobile nodes that have the flexibility to connect with one another while not having mounted network infrastructure or any central base station. They have unrestricted mobility and connectivity to others. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore act as a router. Due to limited transmission power, multi hop architecture is needed for one node to communicate with another through network. Due to its dynamic nature MANET has larger security issues than conventional networks. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. The major problem in the MANET is malicious nodes. When data is transmitted among nodes it may reach to the destination node with response time less than the threshold value. Such types of nodes are known as Grayhole nodes.

A Gray hole could be a malicious node that incorrectly replies for any Route Requests (RREQ) while nothaving active route to such destination and drops all the receiving packets. If these malicious nodes work along as a cluster then the damage can be terribly serious. The problem is to discover and take away the projected malicious nodes.

We approach this drawback by choosing some nodes that are trustworthy and powerful in terms of battery power and variety. These nodes that are referred to as Back Bone Nodes(BBN) can type a Back Bone network and has special functions unlike traditional nodes. For the co-ordination between the rear Back Bone Nodes (BBN) and the traditional Nodes, it's assumed that the network is divided into various grids. It is assumed that the nodes, when initially enters the network is capable of finding their various grid locations. It is also assumed that the numbers of normal nodes are quiet more than the number of Gray nodes at any point of time.

The rest of the paper is organized as follows. Section II introduces related work of Gray hole. The literature survey is determines in this section and III regarding about AODV &its security issues. Section IV tells the proposed algorithm. Simulated results of the proposed network are discussed in Section V. The conclusions are given in Section VI.

II. LITERATURE REVIEW

The problem of security and cooperation social control has received considerable attention by researchers within the impromptu network community. during this section, a number of these contributions ar given. NitalMistryet. al. has projected associate degree algorithmic program to counter grey hole attack against the AODV routing protocol. He determined that the projected modification to secure AODV is so effective in preventing the grey hole attacks with marginal performance penalty. YatinChauhan, et. al. tells the development of Mobile Ad hoc networks routing is the main issue. The Gray hole attack can affect the performance of different routing protocols. During this attack, a malicious node captures packets and not forwards them in the network. This paper illustrates how Gray hole attack can affect the performance of routing protocol, AODV, in Mobile Ad hoc networks by using NS-2.34 simulator. Isaac Woungang,et. al present a novel scheme for Detecting Gray hole Attacks in MANETs (so-called DBA-DSR) was introduced. The BDA-DSR protocol detects and avoids the Gray hole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes R. Sudha,et. al. tells about MANETs. The majority of these MANET secure routing protocols did not provide a complete solution for all the MANETs' attacks and assumed that any node participating in the MANET is not selfish and that it will cooperate to support different network functionalities. One of the solution to the problem is ARAN – (Authenticated routing protocol) which is a secure protocol and provides Integrity, availability,

Confidentiality, genuineness, Non repudiation, Authorization & namelessness however associate degree attested egotistical node will infer to the current protocol performance and may disturb the network by dropping packets. Mehdi Keshavarzet. al. concentrate on the information packet dropping during a rather dense Mobile Ad-hoc Network. To encounter this example, they propose a theme supported exploitation MAC-layer acknowledgements to discover and penalise packet eye dropper nodes. They used simulation-based results to guage the performance of our theme. All simulations are performed exploitation NS-2.

It take into account a rather dense self-organized painter with a variable proportion of misbehaving nodes that decide to free ride by dropping the information packets they must forward K. Selvavinayaki et. al. provides a plan regarding the dynamic dynamic nature of topology makes any node in painter to go away and be part of the network at any purpose of your time. There ar several routing attacks caused because of lack of security. Public Key Infrastructure (PKI) is one in all the foremost effective tools for providing security for dynamic networks.. The projected theme uses the route discovery theme of DSR to issue security certificates. Since there's no mounted infrastructure,nodes do all needed tasks for security solutions as well as routing and authentication during a self-organized manner.

Hidehisa Nakayama et.al.propose a replacement anomaly-detection theme supported a dynamic learning methodthat enables the coaching information to be updated at explicit time intervals. Their dynamic learning method involves conniving the projection distances supported 3dimensional statistics exploitation wei ghted coefficients and a forgetting curve.

III. AODV AND ITS SECURITY ISSUES

In this section, a quick summary of the AODV routing protocol is given and also the security threat that ar related to this routing protocol ar shortly mentioned. a lot of specifically, the cooperative grey hole attack on AODV is additionally delineated.. AODV could be a reactive routing protocol that doesn't need maintenance of routes to destination nodes that aren't in active communication. Instead, it permits mobile nodes to quickly get routes to new destination nodes. each mobile node maintains a routing table that stores subsequent hop node info for a route to the destination node.

once a supply node desires to route a packet to a destination node, it uses the required route if a recent enough route to the destination node is offered in its routing table. If such a route isn't on the market in its cache, the node initiates a route discovery method by broadcasting a Route Request (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the supply node. All the receiving nodes that don't have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ.

A Route Reply (RREP) message is distributed back to the supply node once the RREQ question reaches either the destination node itself or the other intermediate node that features a current route to the destination. because the RREP propagates to the supply node, the forward route to the destination is updated by the intermediate nodes receiving a RREP. The RREP message could be a unicast message to the supply node. AODV uses sequence numbers to work out the freshness of routing info and to ensure loop-free routes. just in case of multiple routes, a node selects the route with the best sequence variety. If multiple routes have identical sequence variety, thenthe node chooses the route with the shortest hop count.Timers ar wont to keep the route entries recent.When a link break happens, Route Error (RERR) packets ar propagated on the reverse path to thesource unsupportive all broken entries within the routing table of the intermediate nodes. AODV additionally uses periodic how do you do messages to take care of the propertyof neighbouring nodes.AODV doesn't incorporate any specific security mechanism, like robust authentication. Therefore,there is no simple mechanism to forestall mischievous behavior of a node like mack spoofing, information science spoofing, dropping packets, or fixing the contents of the management packets. Protocols like SAR [15] are developed to secure AODV against bound varieties of attacks. However, these protocols deliver the goods restricted security at the price of performance degradation in terms of message overhead and latency time.

B. Cooperative Gray Hole Attack

The Gray hole attack has 2 phases. Within the initial section, the malicious node exploits the impromptu routing protocol like AODV to advertise itself as having a sound route to a destination node, with the intention of intercepting packets, despite the fact that the route is spurious. Within the second section, the wrongdoer node drops the intercepted packets while not forwarding them. there's a a lot of refined variety of this attack once associate degree wrongdoer node suppresses or modifies packets originating from some nodes, whereas departure the information packets from different nodes unaffected. This makes it tough for different nodes to discover the malicious node. During this work, however, a defence mechanism has been projected against a cooperative grey holeattack during a painter that depends on AODV routing protocol. Symbolic notations in Fig. one ar utilized in all the

next diagrams within the paper .
In the customary AODV protocol, once the supply node S (Fig. 1) needs to speak with the destination node D, the supply node S broadcasts the Route Request (RREQ) packet. every neighbouring active node updates its routing table with associate degree entry for the supply node S, and checks if it's the destination node or whether or notit's this route to the destination node. If associate degree intermediate node doesn't have this route to the destination node, it updates the RREQ packet by increasing the hop count, and floods the network with the RREQ to the destination node D till it reaches node D or the other intermediate node that has this route to D, as delineated in Fig.1.

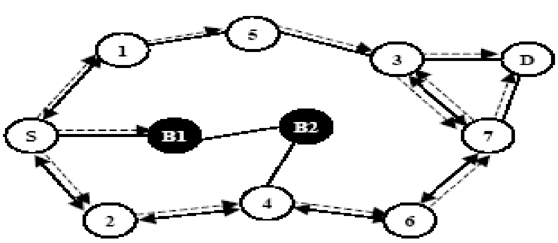

Fig.1 Network flooding by RREQ messages

The destination node *D* or any intermediate node thathas the current route to *D*, initiates a *RouteReply* (RREP) in the reverse direction, as depicted in Fig. 2. Node *S*starts sending data packets to the neighboring node that responded first, and discards the other responses. This works fine when the network has no malicious nodes.

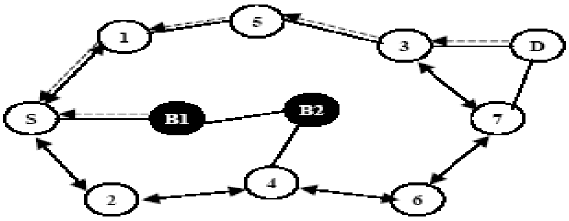

Fig.2. Propagation of RREP messages

In [2], authors have proposed a solution to identifyand isolate a single Grayhole node. However, the security threat arising out of the situation where multiple Grayhole nodes act in coordination has not been addressed. For example, when multiple Grayhole nodes are acting in coordination with each other, the first Gray hole node *B1* refers to one of its partners *B2* as the next hop, as depicted in Fig. 2. In the mechanism propose in [2], the source node *S*sends a *FurtherRequest* (FRq) to *B2* through a different route (*S-2-4-B2*) other than via *B1*. Node *S*asks *B2* if it has a route to node *B1* and a route to destination node *D*. Because *B2* is cooperating with *B1*, its "*FurtherReply* (F p)" will be "yes" to both the questions. According to the solution proposed in [2], node *S* starts sending the data packets assuming that
the route *S-B1-B2* is secure. However, in reality, the packets are intercepted and then dropped by node *B1*
and the security of the network is compromised.

IV. THE PROPOSED ALGORITHM

Actions by Source Node (SN)

Step 1: Source Node (SN) sends a Request to Restricted IP(RRIP) to the Back Bone Node(BBN).

Step 2: On receiving the Restricted IP(RIP), from the BBN it sends the RREQ for the Destination as well as for the RIP simultaneously.

Step 3: Awaits for RREP.

Actions by Intermediate Node/Destination Node

Step 1: On receiving the RREQ it first makes an entry in its Routing table for the node that forwarded the RREQ.

Step 2: If it is the Destination node or if it has a fresh enough route to the Destination node, it replies to the RREQ with an RREP.

Step 3: If it is nether the destination nor does it have a fresh enough route to the Destination, then it forwards the RREQ to its neighbours.

Step 4: On receiving an RREP, it again makes a note of the node that sent the RREQ in its routing table & then forwards the RREP in the reverse direction.

Step 5: On receiving a request to enter into the promiscuous mode, it starts listening in the network for all the packets destined to that particular IP address & monitors its neighbours, for the movement of the dummy data packet.

Step 6: In case, it finds out that the dummy data packet loss is exceptionally more than the normal data packet at any particular node, it informs back the IP of this IN.

4.3.1 Gray/Gray Holes Removal process

Actions by Source node on receiving the RREP

Step 1: If the RREP is received only to the Destination & not to the Restricted IP(RIP), the node carries out the normal functioning by transmitting the data through the route.

Step 2: If the RREP is received for the RIP, it initiates the process of Gray hole detection, by sending a request to enter into promiscuous mode, to the nodes in an alternate path(i.e. neighbours of next hop for RIP).

Step 3: The feedback sent by the alternate paths are analysed to detect the Gray hole & this information is propagated throughout the network, leading to the revocation of the Gray Holes certificates.

V. SIMULATION & RESULT

The proposed algorithm resulted two types of scenario.
Scenario1. Packet Receive in AODV and Modified AODV
Simulation for 4 nodes: When 4 nodes used in the network then the packet received in the AODV with Gray hole and Modified AODV have large difference. Large no of packets are received in the modified AODV and less packets are received in the AODV with Gray hole attack.

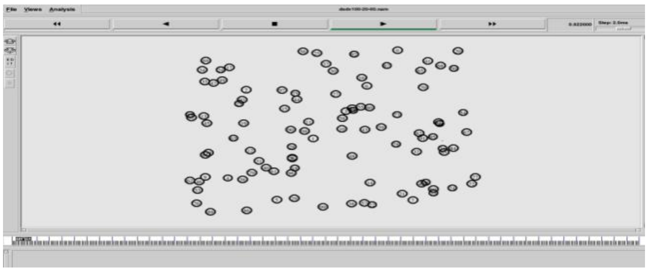

Figure 3 - Nodes position in NAM File

Figure 4 shows position of nodes in a network animator file. Every node is written with a number from 1 to 100. We can start the network animation on clicking play button which is available on the top of network animator window.

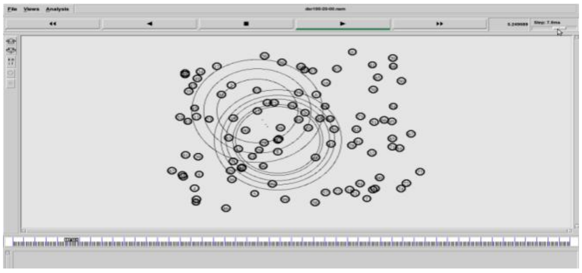

Figure 4 Packet sending animation in NAM File

Figure 4 shows the location broadcast by the nodes and data transfer in the form of packets from one node to another node in network animator.

VI. CONCLUSION

Gray hole attacks are the most important security problems in MANET. Gray hole starts in route discovery phase and gray hole as an attack which drops packets in transmitting step. In proposed work focuses on detecting Gray and gray holes attacks, pointed out their advantages and disadvantages and at the end. Protection against both attacks in one detection system and decreasing number of errors is the main motive. It is observed that the Gray Hole effect the AODV protocol, also effect on packet loss is much lower as compare to effect on late. As malicious node is the main security threat that effect the performance of the AODV routing protocol & their detection is the main matter of concern. Improvement for overcoming the effect of Gray Hole should orient towards controlling the late.The feasible solution to detect two types of malicious nodes(Black/Gray Hole) in the ad hoc network.

REFERENCES

[1] Mistry N, Jinwala DC, IAENG, Zaveri M “Improving AODV Protocol AgainstGrayhole Attacks.” International MultiConference of Engineers and Computer

[2] YatinChauhan, Prof Jaikaran Singh, Prof MukeshTiwari,Dr AnubhutiKhare,“Performance Evaluation of AODV based on Gray hole attack in ad hoc network”,Global Journal of researches in engineering Electrical and electronics engineering Volume 12 Issue 2 Version 1.0 February 2012.

[3] Sonia, AbhishekAggarwal,”Pooled GrayHole Attack in MANET”, Volume 3, Issue 5, May 2013

[4] Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheerajPeddi, and Mohammad S. Obaidat,.”Detecting Grayhole Attacks on DSR-based Mobile Ad Hoc Networks”, 978-1-4577-1894-6/11/$26.00©2011 IEEE.

[5] R. Sudha, Dr. D. Sivakumar, “A Temporal table Authenticated Routing Protocol for AdhocNetworks” , IEEE , Dec 2010

[6] Mehdi Keshavarz, Mehdi Dehghan “MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks”,WCNC 2012 Workshop on 4G Mobile Radio Access Networks.

[7] VISHNU K, AMOS J PAUL “Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks”, International Journal of Computer Applications (0975 - 8887)Volume 1 – No. 22 , Dec2010.

[8] K.Selvavinayaki, K.K.Shyam Shankar, Dr.E.Karthikeyan, “Security Enhanced DSR Protocol to Prevent Gray Hole Attacks in MANETs”, *International Journal of Computer Applications (0975 – 8887)Volume 7– No.11, October 2010.*