www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 8 August 2016 Page No. 17648-17653

Simulation of Black Hole Attack in Manet

Chinky Jain* Pardeep Tyagi**
*M.Tech Scholar, B.M.I.E.T, Sonipat
** Assistant Professor, B.M.I.E.T, Sonipat

ABSTRACT

A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack. In this paper, we give an algorithmic approach to focus on analysing and improving the security of AODV, which is one of the popular routing protocols for MANET. Our aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node(s) in the MANET at the beginning. Also the objective of this paper is to provide a simulation study that illustrates the effects of Black hole attack on network performance.

Previously the works done on MANETs focused mainly on different security threats and attacks such as Impersonation, Wormhole, Jellyfish, and Intrusion detection. Attack of black hole is required on routing protocols AODV, OLSR and TORA. And also check which protocol performs better against black hole attack. There is a need to address all these types of protocols under the attack, as well as the impacts of the attacks on the MANETs. We want to analyse Black Hole attack in MANETs using AODV, OLSR and TORA which are reactive, proactive and hybrid protocol respectively in nature.

Keywords:-*AODV, RREQ, RREP, IP*

INTRODUCTION

Mobile ad hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed 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 black hole nodes.

A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious.

The problem is to detect and remove the proposed malicious nodes.

We approach this problem by selecting some nodes which are trustworthy and powerful in terms of battery power and range. These nodes which are referred to as Back Bone Nodes(BBN) will form a Back Bone network and has special functions unlike normal nodes. For the co-ordination between the Back Bone Nodes (BBN) and the Normal Nodes, it is

DOI: 10.18535/ijecs/v5i8.39

assumed that the network is divided into several grids. It is assumed that the nodes, when initially enters the network is capable of finding their respective grid locations. It is also assumed that the numbers of normal nodes are more than the number of black nodes at any point of time.

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

RELATED WORK

The problem of security and cooperation enforcement has received considerable attention by researchers in the ad hoc network community. In this section, some of these contributions are presented.

Nital Mistry et. al. has proposed an algorithm to counter Black hole attack against the AODV routing protocol. He observed that the proposed modification to secure AODV is indeed effective in preventing the Black hole attacks with marginal performance penalty.

Yatin Chauhan, et. al. tells the development of Mobile Ad hoc networks routing is the main issue. The blackhole 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 blackhole 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 Blackhole Attacks in MANETs (so-called DBA-DSR) was introduced. The BDA-DSR protocol detects and avoids the blackhole 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, Authenticity, Non repudiation, Authorization & Anonymity but an authenticated selfish node can infer to this protocol performance and can disturb the network by dropping packets.

Mehdi Keshavarz et. al. focus on the data packet dropping in a rather dense Mobile Ad-hoc Network. To encounter this situation, they propose a scheme based on using MAC-layer acknowledgements to detect and punish packet dropper nodes. They used simulation-based results to evaluate the performance of our scheme. All simulations have been performed using NS-2. Consider a rather dense self-organized MANET with a variable percentage of misbehaving nodes that attempt to free ride by dropping the data packets they should forward

K. Selvavinayaki et. al. gives an idea about the dynamic changing nature of network topology makes any node in MANET to leave and join the network at any point of time. There are many routing attacks caused due to lack of security. Public Key Infrastructure (PKI) is one of the most effective tools for providing security for dynamic networks.. The proposed scheme uses the route discovery scheme of DSR to issue security certificates. Since there is no fixed infrastructure, nodes carry out all required tasks for security solutions including routing and authentication in a self-organized manner.

Hidehisa Nakayama et.al. propose a new anomaly-detection scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals. Their dynamic learning process involves calculating the projection distances based on multidimensional statistics using weighted coefficients and a forgetting curve.

AODV AND ITS SECURITY PROBLEMS

In this section, a brief overview of the AODV routing protocol is presented and the security threat that are associated with this routing protocol are briefly discussed. More specifically, the cooperative black hole attack on AODV is also described.

AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination

DOI: 10.18535/ijecs/v5i8.39

node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If such a route is not available in its cache, the node initiates a route discovery process 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 source node. All the receiving nodes that do not 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 sent back to the source node when the RREQ query reaches either the destination node itself or any other intermediate node that has a current route to the destination. As the RREP propagates to the source node, the forward route to the destination is updated by the intermediate nodes receiving a RREP. The RREP message is a unicast message to the source node.

AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a node selects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count. Timers are used to keep the route entries fresh.

When a link break occurs, *Route Error* (RERR) packets are propagated along the reverse path to the source invalidating all broken entries in the routing table of the intermediate nodes. AODV also uses periodic *hello* messages to maintain the connectivity of neighboring nodes.

AODV does not incorporate any specific security mechanism, such as strong authentication. Therefore, there is no straightforward mechanism to prevent mischievous behavior of a node such as MAC spoofing, IP spoofing, dropping packets, or altering the contents of the control packets. Protocols like SAR [15] have been developed to secure AODV against certain types of attacks. However, these protocols achieve limited security at the cost of performance degradation in terms of message overhead and latency time.

B. Cooperative Black Hole Attack

The black hole attack has two phases. In the first phase, the malicious node exploits the ad hoc routing protocol such as AODV to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the attacker node drops the intercepted packets without forwarding them. There is a more subtle form of this attack when an attacker node suppresses or modifies packets originating from some nodes, while leaving the data packets from other nodes unaffected. This makes it difficult for other nodes to detect the malicious node. In this work, however, a defense mechanism has been proposed against a cooperative black hole attack in a MANET that relies on AODV routing protocol. Symbolic notations in Fig. 1 are used in all the subsequent diagrams in the paper.

In the standard AODV protocol, when the source node *S* (Fig. 1) wants to communicate with the destination node *D*, the source node *S* broadcasts the *Route Request* (RREQ) packet. Each neighboring active node updates its routing table with an entry for the source node *S*, and checks if it is the destination node or whether it has the current route to the destination node. If an intermediate node does not have the current 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* until it reaches node *D* or any other intermediate node that has the current route to *D*, as depicted in Fig.1.

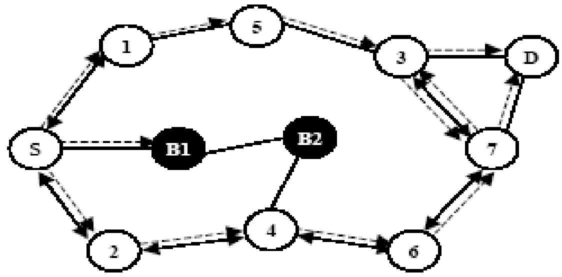

Fig.1 Network flooding by RREQ messages

The destination node *D* or any intermediate node that has the current route to *D*, initiates a *Route Reply* (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.

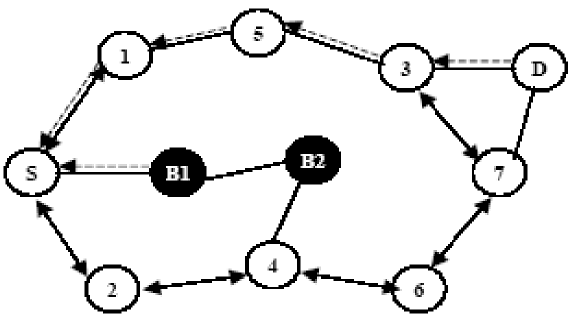

Fig.2. Propagation of RREP messages

In [2], authors have proposed a solution to identify and isolate a single black hole node. However, the security threat arising out of the situation where multiple black hole nodes act in coordination has not been addressed. For example, when multiple black hole nodes are acting in coordination with each other, the first black 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 *Further Request* (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 "*Further Reply* (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, thepackets are intercepted and then dropped by node *B1*
and the security of the network is compromised.

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/Black 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 black 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 analyzed to detect the black hole & this information is propagated throughout the network, leading to the revocation of the Black Holes certificates.

SIMULATION & RESULT

The proposed algorithm resulted two types of scenario.

Scenario 1. 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 Black 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 black hole attack.

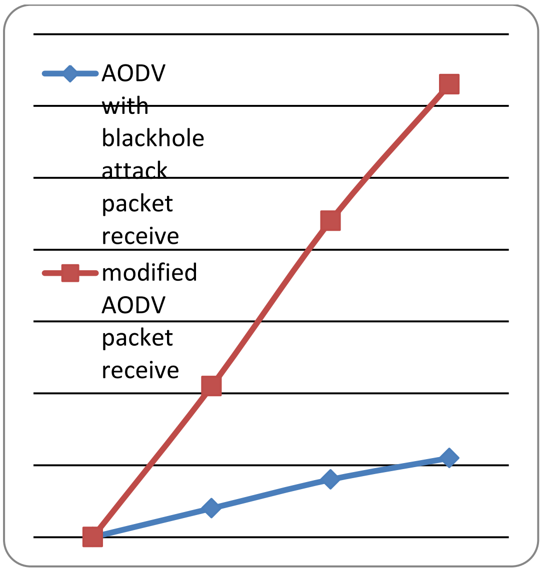

Fig 4 Packets received by the Modified AODV during attack than the traditional AODV

Scenario 2. End To End Delay in AODV and Modified AODV.

Simulation for 4 nodes: Modified AODV has more End To End Delay than the AODV with Blackhole .When the network has low no. of nodes it becomes difficult to isolate the blackholes

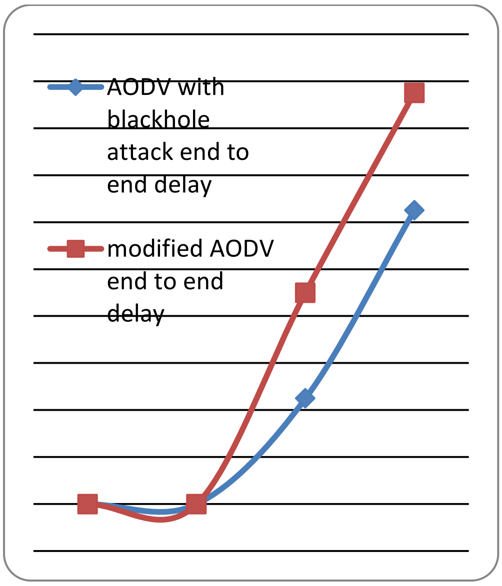

Fig 8 Modified AODV with End to End Delay

Conclusion

Black hole and gray holes attacks are the most important security problems in MANET. Black hole starts in route discovery phase and gray hole as an attack which drops packets in transmitting step. In proposed work focuses on detecting black 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 Black Hole effect the AODV protocol, also effect on packet loss is much lower as compare to effect on delay. 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 Black Hole should orient towards controlling the delay. The feasible solution to detect two types of malicious nodes(Black/Gray Hole) in the ad hoc network. The proposed solution can be applied to identify and remove any number of Black Hole or Gray Hole Nodes in a MANET and discover a secure path from source to destination by avoiding the above two types of malicious nodes.

References

[1]Mistry N, Jinwala DC, IAENG, Zaveri M "Improving AODV Protocol Against Blackhole Attacks." International Multi Conference of Engineers and Computer Scientists, Hong Kong, pp 17-19 March, 2010.

[2]Yatin Chauhan, Prof Jaikaran Singh, Prof Mukesh Tiwari, Dr Anubhuti Khare, "Performance Evaluation of AODV based on black 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, Abhishek Aggarwal,"Pooled Black Hole Attack in MANET", Volume 3, Issue 5, May 2013

[4] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Mohammad S. Obaidat,."Detecting Blackhole 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 Black Hole Attacks in MANETs", *International Journal of Computer*

Applications (0975 – 8887) Volume 7– No.11, October 2010.
[9] Mansoor Mohsin and Ravi Prakash,"IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson, TX Kaixin Xu, Xiaoyan Hong, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095 project under contract N00014-01-C-0016
[10] Akanksha Saini, Harish Kumar," Effect Of Black Hole Attack On AODV Routing Protocol In MANET", International Journal of Computer Science and Technology
[11]Vipan Chand Sharma, Atul Gupta, Vivek Dimri," Detection of Black Hole Attack in MANET under AODV Routing Protocol", Volume 3, Issue 6, June 2013 International Journal of Advanced Research in Computer Science and Software Engineering.
[12]Madhusudhananaga Kumar KS and G. Aghila " A Survey on Black Hole Attacks on AODV Protocol in MANET", in *International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011*.
[13]Rakesh kumar, Siddharth Kumar, Sumit Pratap Pradhan, Varun Yadav," Modified route-maintenance in AODV Routing protocol using static nodes in realistic mobility model",publish in International Journal on Computer Science and Engineering.
[14]Durgesh Wadbude, Vineet Richariya,"An Efficient Secure AODV Routing Protocol in MANET", Volume 1, Issue 4, April 2012 in International Journal of Engineering and Innovative Technology.
[15] Jaspal Kumar, M. Kulkarni, Daya Gupta," Effect of Black Hole Attack on MANET Routing Protocols", Published Online April 2013 in MECS (http://www.mecs-press.org/), I. J. Computer Network and Information Security, 2013, 5, 64-72
[16] K. Lakshmi, S.Manju Priya , A.Jeevarathinam3 K.Rama , K. Thilagam," Modified AODV Protocol against Blackhole Attacks in MANET", International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449
[17]Neha Kaushik, AjayDureja,PERFORMANCE EVALUATION OF MODIFIED AODV AGAINST BLACK HOLE ATTACK IN MANET*"*, European Scientific Journal June 2013 edition vol.9, No.18 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431
[18] Humaira Nishat, Vamsi Krishna K, Dr. D.Srinivasa Rao and Shakeel Ahmed," Performance Evaluation of On Demand Routing Protocols AODV and Modified AODV (R-AODV) in MANETS", pulished in International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.1, January 2011.
[19]Hidehisa Nakayama, Yoshiaki Nemoto," A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 58, No. 5, June 2009.