IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 12-15
www.iosrjournals.org

Risk Mitigation of Black Hole Attack for Aodv Routing Protocol

[1]Varsha Patidar, [2] Rakesh Verma
[1,2]Department of Computer Science and Engineering MITM Indore, RGPV University India

Abstract : *Due to the flexibility and independence of network infrastructure, MANET is a hot research topic among researchers. MANET is dynamic infrastructure less in nature and lack of centralized monitoring points and such network are highly vulnerable to attacks. The performance and reliability is break by attack on Ad hoc routing protocols. Nodes can leave and join the network at any time. AODV is an on demand routing protocol for MANET. In AODV protocol, security is compromised by "Black Hole "attack. A black attack is a severe attack that can easily employ against routing in MANET. In black hole attack, a malicious node that falsely replies for an rout request without having an active route to specified destination and drops all the receiving packets. In this paper we will focus on various techniques on how black hole attack can be detect and mitigate in AODV routing protocol and will also compare the existing solution to black hole attack on AODV protocol and their drawback.*

Keywords: *Ad hoc network, AODV, black hole attack, malicious node, routing protocol.*

I. INTRODUCTION

Ad Hoc network provide a possibility of creating a network in situation without using predefine infrastructure or centralized administration and is a collection of mobile devices that can communicate with each other. Nodes in MANET act as a router node as well as host node for forwarding the data packets. Due to the lack centralized administration, most of the routing protocol depend on cooperation between nodes and assume that all nodes are trust worthy and are well behaved. But if a node if compromised and become malicious then such nodes can launch routing attacks in order to degrade the performance of network. In recent years, many security issues have been studied. There exist many open issues like finite transmission bandwidth, reliable data delivery, security problem. There are mainly three types of routing protocol and they are proactive, reactive and hybrid routing protocol. Proactive routing protocol is table driven where as reactive routing protocol are on demand routing protocol. AODV and DSR both are on demand protocol. But the difference between both of these is, DSR a route cache is maintained and due to this over head of memory increases. But in case of AODV, it is a source initiate routing protocol. I n this, routing table is maintained by every mobile node and this routing table consist of next node information for a route to the destination node. The intermediate nodes between the source and destination are responsible for finding a fresh path to the destination in route discovery process of AODV protocol. Malicious node immediately responses to such route discovery process giving false information of having a fresh enough path to destination. Source node assumes that it is sending data packets through a true path but actually it sending the data packets to malicious node. Apart from the malicious node, black hole attack can occur due to damaged node, unintentionally dropping of data packets.

II. OVERVIEW OF AODV ROUTING PROTOCOL

AODV is on demand routing, means it start its routing process only when any node in the network desire to transmit the data packets. In AODV, next hop information is started by each node in it a routing table. When a source node cannot reach to the destination node directly, then the source node will immediately initiate a route discovery process. AODV uses several control packets like Route Request (RREQ), Route Reply (RREP) and Route Error Process (RERR). RREQ message is broadcasted, RREP message is uni casted back to source of RREQ, and RERR message is used to notify the loss of link to other node. Route discovery is initiated by broad casting a RREQ to its neighbor and this RREQ is rebroadcasted to their neighbor until it reaches to the destination node. When destination node receives the RREQ, it sends the RREP message to the sender node Routes are maintained in the source node as long as they are needed. Routing table are maintained by every node and have fields like destination, number of hops, next hops, destination sequence number, life time, active neighbor. To find the freshness of route towards destination, sequence number is used. Attacks on AODV can be performed easily as AODV does not have any centrally administered secure routers. Attackers from outside or inside can easily exploit the network. AODV supports shared wireless medium and dynamic topology. It is capable of both unicast and multicast routing. It avoids count to infinity problem of other Distance -vector protocol. It is flat routing protocol and does not need any central administrative system to handle the routing process. It does not require any permanent link between the nodes to transfer data. For transferring the data,

temporary link would suffice for time being. AODV needs less protection of control message. It is enough to protect RREQ and RREP message in order to provide the security to the protocol.

Table: Attacks on Different layers

Layer	**Attacks**
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, black hole, Byzantine, flooding, resource consumption, location disclosure attacks, table over flow attacks, impersonation, cache poisoning
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11)
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

III. BLACK HOLE ATTACKS ON AODV ROUTING PROTOCOL

The Black Hole attack occurs at Network layer. Black Hole attack comes under the category of Distributed Denial of Service (DDoS) attack. In this attack, it involves breaking in to hundred or thousand of machine and for this reason this attack is called Distributed Denial of Service. At network layer, variety of attacks has been identified. An attacker can absorb the network traffic, injecting themselves between sender and receiver. In AODV protocol, black hole attack is performed by malicious node. When sender wants to send data packet to destination node and this destination is not directly reachable then with the cooperation of the intermediate node data packet is reached to destination node and this process takes place in following manner- When a node request a route to destination, it initiates a route discovery process within the network. When this route request (RREQ) is received by malicious node from neighboring nodes, it immediately sends a fake RREP message to sender and this RREP message contains false routing information. This RREP message has a higher sequence number indicate the freshness of the path. This sequence number is higher or equal to that one contained in RREQ. Malicious node immediately sends a false RREP message without checking its routing table. After getting the RREP, the sender start sending the data packet through the path specified by malicious node. In Black hole attack, packets are forwarded to a non-existent path and get absorbed without being forwarded to other node. By creating routing loops, network congestion and channel contention, attackers degrades the network performance. In AODV protocol, Black hole attack can occur in two ways- RREQ Black Hole Attack and RREP Black Hole attack.

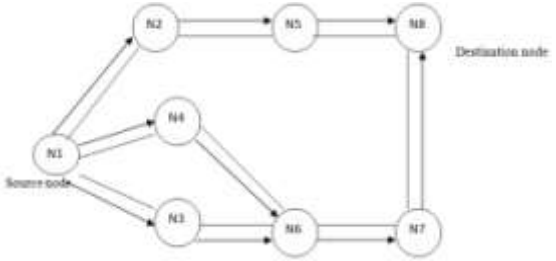

Figure 1. RREQ Propagation

In fig 1. When a node N1 requires a route to a destination node N8, it initiates a route discovery process within the network. It broadcasts a route request (RREQ) packet to its neighbors.

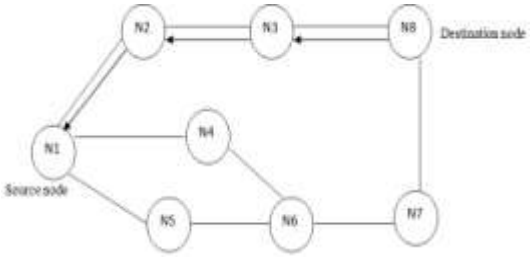

Figure 2. RREP Propagation

In figure 2.once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. Here Destination Node 8 unicast the RREP back to source node 1. Any intermediate node may respond to the RREQ message if it has a fresh enough route. The malicious node easily disrupts the correct functioning of the routing protocol and make at least part of the network crash. The attack

will become even more difficult to understand when an attacker forwards the packets selectively. Attacker modifies the packets originating from some specified nodes and leaving the data unaffected from other nodes and thereby limiting the mistrust of its wrong doing.

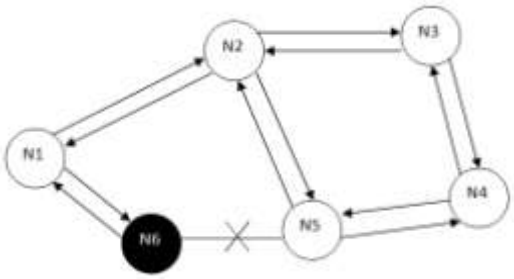

Figure 3. Black Hole Attack

IV. NETWORK LAYER DEFENSE AND RELATED WORK

Security-aware ad hoc routing protocol (SAR) can be used to defend against black hole attacks. AODV and DSR are based on Security-aware ad hoc routing protocol. Along with RREQ packet, security metric is added. When Intermediate nodes receive the RREQ packet, the security and trust level will increase. If this security and trust level does not hold or satisfied by intermediate nodes then the RREQ will drop. If destination node is not able to find the required security metric or trust level, then sender will get the notification in order to adjust security level for finding the desired route.

To defeat the effect of Black Hole attack in AODV a lot of attention is given by researchers. In [1], the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the black hole attack. By using this method, RREP is send to the source node and CREQs to its next hop toward destination. Now the next hop will search a route in its cache and if route is available, it sends CREP to source. When source node receives this CREP, it becomes assure for the validity of the path. This surety is achieving by comparing the path in RREP and in CREP. If comparison is true than source node gets the surety that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion. In S. Jain [2], a different technique is proposed in which data is send in small blocked size and in equal size. In [3], the authors proposed a solution in which source node have to wait until a RREP packet arrives from more than two nodes. After this the source node checks whether there is a shared hop or not. If yes, then source node get the surety that the route is safe. But the drawback of this solution is that source node has to wait until it gets multiple RREP packets. In [4], the authors has proposed a method to defeat the effect of Black hole attack and this method is based on Merkle tree which requires hashing technique to detect the malicious node in the network. In [5], the authors had analyzed the black hole attack and found that sequence number of destination is increased by malicious node so that it can convince the source node that particular route is a fresh route. To overcome from this problem, authors proposed a statistical based anomaly detection approach. In this, the black hole attack is detected on the bases of difference between the destination sequence numbers of received RREPs. The advantage of this approach is that it does not require any modification in the existing protocol and can detect the black hole attack without any extra routing traffic. In [6] authors have proposed a solution to defeat black hole attack by modifying the AODV protocol. In this approach, it avoids malicious nodes to advertise the route that is not existed. This is achieved by including the address of next hope node in RREP packet of intermediate node. The next hop node of the neighbor node replies the Further reply packet back to the source node to confirm the route information. If Further reply is not receive by source node than it means the route contains the malicious node and is removed from the routing table to avoid future attack. But this approach is not strong enough to cooperative black hole attacks. In [7], authors proposed a solution to avoid multiple black hole attacks in group. In this, every participating node is uses a fidelity table to know the reliability of any node. A node is considered as malicious node if it is having 0 values. If the trusted level of participating node increases than fidelity level will also increase. An acknowledgment is send by destination node to source node when a data packet is received and level of intermediate node will be incremented. The level of intermediate node will decrement if no acknowledge is received. But due to this whole process, there will be processing delay in the network. In [8], author had proposed a mechanism which is based on ignoring the first established path. According to his analysis, the first RREP message received by source node would normally come from malicious node. But this condition does not hold true in all cases. It may be possible that the second RREP would also come from a malicious node.

V. Conclusion

In this paper, we studied the various solutions and proposals given by different authors. We identified their working process, advantages and as well as their drawbacks. Some solutions performed well in the presence of malicious node and protect the network from degradation. But some proposed solutions do not perform well due to the presence of multiple malicious nodes in the network. In AODV protocol, the route discovery process is vulnerable to Black Hole attack. So some efficient security method is needed to mitigate the effect of Black Hole Attack. We also observe that there are various mechanisms that detects black hole node, but no one is reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations.

References

[1] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," *2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.*

[2] Shalini Jain, Mohit Jain, Himanshu Kandwal, "Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Applications Volume 1 (2010)*

[3] M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," *ACM Southeast Regional Conf. 2004*

[4] *Abdurrahman* Baadache, Ali Belmehdi,Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks *(IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010*

[5] S. Kurosawa *et al.*, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," *Proc. Int'l. J. Network Sec.*, 2006.

[6] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.*

[7] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET*", Journal of Networks, Vol 3, No 5, 13-20, May 2008*

[8] Dokurer, S.:" Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, Atılım University (September 2006)