A Survey on Techniques for Mitigating Black Hole Attack in MANET using AODV

Praseetha S Nair[1] Sruthy R S[2]
[1,2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Musaliar College of Engg and Technology, India

Abstract— Mobile Ad hoc Network (MANET) is the type of network in which a node can send, receive and forward packets. There is no central server to authenticate and forward the activities of the network. Therefore MANET may be vulnerable to different kind of attacks. One of the major type of attack is black hole attack. In black hole attack, one false node pretends that it has the best route to destination and responds with RREP packet. In this paper, a detail study of AODV routing protocol is performed. Then some existing methods for mitigating black hole attack in MANET using AODV routing protocol has been surveyed.

Keywords: Mobile Ad hoc Network (MANET), AODV, Black Hole Attack

I. INTRODUCTION

MANET is useful in networks that has no proper infrastructure. In such scenarios, MANET is extremely helpful as it does not need any prerequisite or any infrastructure installation. Due to the flexible nature of MANET, it may be vulnerable to different attacks. Lack of security in MANET is one amongst the important issues. Due to lack of adequate security mechanism some nodes which pretend to be the member of that network but actually that may be a malicious node and try to capture the data. So, identification of such malicious nodes is very challenging issue. In MANET, if a new node wants to join the network, it has to be checked to know that the node is malicious or not. And also check how much access should be given to that node. Every node in the network performs three basic functions, i.e, transmit, receive and forward the packets. The malicious nodes may receive the packet and drop the packet. This raises security issues in MANET which needs to be prevented by effective solution.

II. WORKING OF AODV [1]

AODV uses three types of control packets for data transfer: RREQ (Route Request), RREP (Route Reply) and RERR (ROUTE ERROR). Also, this protocol has one optional control signal for maintaining the connectivity between the node which is ”Hello message”. It contains a routing table at each node which has information about routes. The fields of routing table entry used here are destination IP address, destination sequence number, hop count, and next hop.

When a source node (S) is ready to send the data to the destination node (D), it does not have a predetermined path from source to destination. Thus, the source node now initiates a route discovery procedure. The procedure starts by increasing its sequence number by one and then the source node floods the RREQ packet to all its nearest neighbours. RREQ packet has the following fields in its packet: Originator IP, Route Request Id, Originator Sequence number, Destination IP, Destination Sequence number, and Hop count. The intermediate node which receives the RREQ packet makes the entry of routing information in their routing table and checks the table for destination node information. If destination node information is not found, then it forwards the RREQ packet to its next neighbours. After getting RREQ packet, the destination node sends the RREP packet to source node. The RREP packet contains the following fields: Hop count, Destination IP address, Destination sequence number, Originator IP address, and Life Time. AODV uses one more packet, RERR (ROUTE ERROR). As network topology of MANET always changes, it may result in breaking of routes between source and destination node. This time RERR packet is generated if any route is broken.

III. BLACK HOLE ATTACK IN MANET USING AODV

In MANET, we can use three types of routing protocols, Reactive, proative or hybrid. AODV is an efficient routing protocol in MANET. However it comes with many security issues. Black hole attack is one among them. Black hole attack is an attack in which the malicious node sends the false RREP to the sender and takes all the data by giving higher random sequence number in RREP packet. After getting data packets, malicious node drops all the data packets. The black hole node can be one or more. In case of one node the solution is different and mechanism of prevention is also different. But, if the malicious node is more than one, it becomes a challenging task to detect and prevent that nodes.[2]

Black hole attack can be classified into two: Single black hole attack and Co-operative black hole attack. In single black hole attack, there is only single malicious node. Prevention and detection of that node malicious is not difficult. There are many existing techniques to deal with this type of attack. In Co-operative black hole attack, there is always more than one malicious node. It is very difficult to detect this type of attacks. Techniques used to detect single black hole attack could not work with this attack.

IV. EXISTING TECHNIQUES TO ALLEVIATE BLACK HOLE ATTACK

In this section we will discuss some of the existing techniques available to alleviate Black hole attack in MANET using AODV routing protocol.

A. Route Selection based Technique [3]

In route based selection technique, two different types of solutions is proposed.

In first solution more than one path is discovered from source to destination. Suppose that there are three different paths available between source and destination, then the source node sends the packet to the destination with different sequence number and packet ids. The source node then waits for the acknowledgement. If no acknowledgement

received from any path then source node assumes that the packet is captured by the malicious node in that path. By this method, a trusted path without any malicious node will be found.

This method is time consuming and there may be overhead for the source node to analyze all acknowledgement from all possible paths.

In the second solution, at every node there are two additional tables. One table is for storing the sequence number of the last packet sent to every node and the second table is for the sequence number of packet received from every sender. According to this method, during RREP phase, destination or any intermediate node must include the sequence number of the last packet received. When source nodes gets the RREP packet, it compares the value of sequence number by its table. If sequence number matches, the packet transmission takes place, otherwise, it sends the information about that node to others.

B. Technique Based on Reliability Check [4]

In [4], they have presented two techniques to detect more than one malicious node.

Maintenance of routing information table- Each node contains three bit information. Out of which two bits are sent to source node from the nodes those respond with the RREP message during route discovery phase and the information in third bit is broadcasted by any one of the nodes in the network. Three type of information stored are from node, through node and through by trustful node.

Reliability checking of node- In this phase, they used terms 'IN' which indicates intermediate node and 'NHN' as next hopping node. For checking out the reliability of node they applied three scenarios. They are (i) No malicious node in the network, (ii) Two malicious nodes in the network, and (iii) One reliable node in the network. By this they are making the network more reliable.

C. Honest Value based Solution [5]

In Honest Value based Solution Honest Value based Solution, the malicious node is found by using the concept of honest value. Any node on receiving RREP packet for the first time forwards it to sender and initiates the judgement process on that replier. The activities of a node are recorded by their neighbours. Information about a node is collected from their neighbors. From that information, it decides whether the node is malicious or not.

D. EDRI based approach [6]

In this approach, extended data routing information is used. They made changes in data routing information table for detecting malicious nodes in MANET. The data control packet consists of following field: Node_ID, NHN (Next Hop Node), and Random_Number. In Data Routing Information (DRI) table they have added a column named BHN (Black Hole Node) column for eliminating detected black hole nodes. They followed three steps as:

1) Finding the freshest path
2) Checking path
3) Eliminating malicious nodes

E. NHBADI technique [7]

In [6], 'A Novel Honeypot based Detection and Isolation' technique is used. This architecture consists of three layers:

1) Malicious node detection layer,
2) Route lookup in the network layer, and
3) Isolation in the network layer. For identifying the malicious node they broadcast a spoofed RREQ packet by using above three layers.

F. An Adaptive Approach [8]

This approach is an enhancement of standard AODV protocol. Here one extra table which is CRRT which stands for ''coming route reply table" is used. The source node has CRRT table, which contains destination sequence number, next hop, hop count, sender IP address, destination IP address and lifetime. The RREP packets will be collected at the source node until the lifetime of RREP get expire. It identifies the malicious node by using sequence number and a threshold value. For a node, if destination sequence number is greater than or equal to the threshold value, it means, that node is the malicious node. That node causes the black hole attack.

G. Cluster based approach [9]

Initially, a network is created having a cluster of nodes. After creation of cluster, the next step is to find the cluster head. To find the cluster head it choose two trusted nodes with high energy. Amongst the two trusted nodes the one with highest energy level works as the cluster head. Then for each node the sent and received packets are calculated. Also route response is determined. Then to identify the malicious node the number of packets and the threshold value is compared and update the routing table.

H. BDS Strategy using DYMO [10]

In BDS strategy, Nitnaware et.al have used a protocol named as 'DYMO' which stands for 'Dynamic MANET On-demand Routing Protocol".

DYMO is the modified version of AODV protocol. Following are the modifications given.

Phase I (Broadcasting of hello packets) - In the first phase all the nodes broadcast the hello packet.

Phase II (Suspicious node detection) - All the nodes which receives the hello packet check the capacity of sequence number whether it is within the range or not.

Phase III (Suspicious node prevention) - After doing step two if the value of sequence number is greater than its capacity, this indicates that, the node is malicious and thus the information about malicious node is sent to all the other nodes in the network.

I. Black hole Intensity Parameter Based Approach [11]

In this approach, a new term, black hole intensity parameter, is introduced. These parameter calculates the sequence number which is generated by the malicious node after getting the sequence number of destination node. One other new term introduced here is CUSUM (Cumulative sum), which is used to test the changes in normal behavious of sequence number. They also proposed a detection algorithm and also calculated its computational cost.

J. Watchdogs and Pathrater approaches. [12]

This protocol uses advantages of both AODV and OLSR and overcome their disadvantages using Watchdogs and Pathrater approach. This proposed model consists of three major parts, which are Gathering Reputation Values, Computing Reputation Values, and Selecting Best Route. The reputation values that are collected about a node using Watchdogs and Pathrater approaches depend on individual monitoring by the node's neighbors. Reputation values are updated using watchdogs. Finally a node should choose most reliable path to other node based on the reputation values of nodes in the paths. His reputation mechanism not only avoids black holes but also avoids benign nodes that face some environment conditions that prevent them from forwarding packet properly.

K. Fuzzy based Intrusion Detection System in MANET [13]

In this proposed intrusion detection system, it takes the advantages of both Adaptive Neuro Fuzzy Inference System (ANFIS) and Particle Swarm optimization (PSO) to detect the black hole attack. The PSO is applied to improve the performance of ANFIS by making adjustments to the membership functions and thereby minimizing the errors. The ANFIS predictions helps to predict the future behavior of attacker and thus to detect it.

V. Conclusion

In this paper, we have discussed about black hole attacks in MANET at the network layer. AODV is most commonly used reactive routing protocol in MANET. But it is highly prone to black hole attack. There are various techniques exist to identify and mitigate black hole attack. In this review paper, we reviewed some of such techniques in brief. This literature study will helps to design efficient security protocols in MANET.

References

[1] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc on-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003.
[2] Prakhar Golchha and Hemanta Kumar Pati," A Survey on Black Hole Attack in MANET Using AODV", International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018), pp. 361 – 365, 2018
[3] N. Sharma and A. Sharma, "The Black-hole Node Attack in MANET," IEEE ACCT, pp. 546-550, 2012.
[4] G. Wahane and S. Lonare, "Technique for Detection of Cooperative Black hole Attack in MANET," IEEE ICCCNT, pp. 1-8, 2013.
[5] M. Y. Dangore and S. S. Sambare, "Detecting and Overcoming Blackhole Attack in AODV Protocol," IEEE CUBE, pp. 77-82, 2013.
[6] D. Kshirsagar and A. Patil, "Blackhole Attack Detection and Prevention by Real Time Monitoring," IEEE ICCCNT, pp. 1-5, 2013.
[7] U.-H. Syed, A. I. Umar, and F. Khurshid, "Avoidance of Black Hole Affected Routes in AODV-based MANET," IEEE ICOSST, pp. 182185, 2014.
[8] V. Kumar and R. Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network," Procedia Computer Science, vol. 48, pp. 472-479, 2015.
[9] N. N. Dangare and R. Mangrulkar, "Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc
[10] D. Nitnaware and A. Thakur, "Black Hole Attack Detection and Prevention Strategy in DYMO for MANET," pp. 279-284, 2016.
[11] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, Quantifying, and Detecting the Blackhole Attack in Infrastructure-less Networks," Computer Networks, vol. 113, pp. 94-110, 2017.
[12] Qussai M. Yaseena, Monther Aldwair, "An Enhanced AODV Protocol for Avoiding Black Holes in MANET" The 5th International Symposium on Emerging Inter-networks, Communication and Mobility (EICM 2018), Procedia Computer Science 134 (2018) 371–376.
[13] Houda Moudnia, Mohamed Er-rouidib, Hicham Mouncifc, Benachir El_ Hadadia, "Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET" , International Workshop on Web Search and Data Mining (WSDM), Procedia Computer Science 151 (2019) 1176–1181.

