Detecting and Eliminating Cooperative Black Hole Nodes Using EDRI Table in MANET

M.Brindha Devi[1], T.Kalaikumaran[2], and S.Karthik[3]

[1]PG Scholar, Dept. of CSE, SNS College of Technology, Coimbatore, India, Email: brindhabala244@gmail.com
[2]HoD, Dept. of CSE, SNS College of Technology, Coimbatore, India, Email: proftkalaikumaran@gmail.com
[3]Dean, Dept. of CSE, SNS College of Technology, Coimbatore, India, Email: profskarthik@gmail.com

***Abstract-** MANET (Mobile Ad hoc Network) is having several nodes .They are configurable. The nodes which are in the network having mobility. Due to moving nature of the nodes in the network, the topology of the network is not stable. Security is a big challenge in the MANET. To transfer the data in the network, many protocols are used. As well as, many attacks may happen in the network, due to low security. Ad hoc On Demand Distance Vector (AODV) routing protocol is one of the protocol used for the data transfer which is also affected by the attacks in the network. In this paper, an approach known as EDRI table is used to eliminate the black hole nodes in the MANET.*

***Keywords:** AODV, Attacks, Data packets ,Mobile ad hoc networks (MANET), Security,*

Introduction

Mobile Ad hoc Network

MANET (Mobile Ad hoc Network) is having several nodes .They are configurable. The nodes in the network are wireless in nature and having higher mobility. Due to mobility of nodes, the topology is unstable. The communication range also vary, any node may enter or exit the network. The packets format is used in the network for transferring the data. During the transformation, packet loss may occur when an intermediate node is in out of range or when an intermediate node is go to out of range or when an attack is done. Security is one of the main challenges in MANET. Some of the attacks in the MANET are Denial of Service (DOS) attacks and Man in Middle attacks.

Ad hoc On Demand Distance Vector Routing (AODV)

Ad hoc On Demand Distance Vector Routing (AODV) is a routing protocol which is a source started protocol. Whenever a source requisite to lead data to the destination, the path is getting established. So it is known as a reactive protocol. Many malicious nodes in AODV occur either as single node or as cooperative nodes. Gray hole attack, Worm hole attack, black hole attack are the attacks may occur in AODV. Sniffing, Trust Model, Estimate Sequence Number, DRI Table changing are the attacks which may done by the malicious nodes. Control packets and data packets are the two types of packets in AODV. The control packet contains routing information and sequence number. The data packets contain data. RREQ (Path Request), RREP (Path Reply) and RRER (Path Error) are the control packets. RREQ packet is disseminated by the sender when it needs the data transformation. This packet voyages through the network. When it touches the destination, the destination unicast the RREP packet and it will reach the source. The source chooses the freshest path. The freshest path should have highest sequence number. After this control packet transformation, the data packets are get transferred through this path. In Black hole attack, the malicious node inoculates the fault information and diverts all the packets to it. Then it will drop the data packets.

Literature Survey

In [1] the promiscuous mode method is used. Here a threshold value is used for detecting the malicious nodes. Whenever, the value of a node is greater than the threshold value, then it will be considered as a malicious node. In [2] Friendship table is created for every cluster heads and for each members of the cluster. A trust estimator method is used in which the trust level of cluster head's neighboring node is calculated.

In [3] Watchdog Mechanism is used. Other two extra tables are used. They are Pending Table and Node Rating Table. Packet overhead and delay is increased in this method. In this paper, a threshold value is evaluated. If the dropped packets surpass the threshold value, the node symbols its neighbor node as malicious node. The energy of the node in the network is wasted. In [4] end to end checking is done. Two mechanisms are done here. They are postlude mechanism and prelude mechanism. The source node monitors the data transformation. The energy of the node is wasted and it is not works in the cooperative malicious node. In [5] there are three parameters are used such as RREQ sequence number, sequences of each node and number of received RREPs.

In [6] Elliptic Curve Cryptography is used. ECC key exchange is protected from man in middle attack. The software complexity is increased. In [7] DRI table is used. The Refresh packet is used. In [9] the random number is used to identify the malicious node. The random is not recognized by the malicious node. The false positive effect is decreased. In [10] there are two node information is done. They are Next Hop Node (NHN) information and Previous Hop Node (PHN) information. There is very low processing speed and packet overhead. In [11] Density Calculation is done. Based on this calculation, a change is done in information table. If the density value is higher than the threshold value, then it will be marked as malicious node and it will be eliminates from the network. The bandwidth consumption is very high. Speed is low and the energy is also getting drained during transformation.

Proposed Approach

The proposed approach uses Extended Data Routing Information (EDRI) table for the security mechanism. Each and every node in the network having the EDRI table. It will be periodically updated by the nodes in the network. The table is update for its own neighbors. Because of the dynamic topology, the neighbors of the node get changed. The proposed EDRI table is having three columns. They are Neighbor node's ID, Data Routing Information and BHN. The Data Routing Information is further divided into 'From' and 'Through'. In addition to the control packet, another data control packet is used. This packet is cannot forwarded by the malicious node. The data control packet consists of NODE_ID, NH and Random Number. The Random Number is generated by the source and it should be constant. First, the data control packet is broadcasted for checking the nodes in the path. Next the source node uses the control packet for the evaluation of the node.

The security mechanism is having three steps:

Step 1: Finding Freshest Route

Step 2: Checking Route

Step 3: Isolating Malicious Node

Step1: Finding freshest route

After receiving RREQ packet, the malicious node will produce RREP packet with highest sequence number. The NH and EDRI entries for next hop node in the RREP packet is placed in the RREP generator. According to the cooperative malicious node, it will make known their neighbor as its NH.

Step 2: Checking Route

The source node will analyze the safety of the route. The hopable node is defined as follows:

Definition 1 Node Y is trustable node for node X, if both ''From'' and ''Through'' columns in node X's EDRI table, have been set as '1' for node 'Y'.

The source starts the process by producing a random number and directing the data control packet to the next hop node. Each node excerpt random number and producing the new data control packet without changing the properties on the receipt of the data control packet. The mechanism is repeated until the following happens:

- Data packet touches the destination
- Received random number is not equal with sent number
- An Node Intermediate's Next Hop does not send reply for data packet

Definition 2 Node X will be marked as malicious by node Z if ''Through'' column in node X is set as '1' and ''From'' column in node Y is set as '0'(Node Y is Neighbor of node X).

The security mechanism is repeated until the following happens:

- Previous node is marked as mischievous
- Touches to a hopable node which is located after RREP generator

Step 3: Isolating Malicious Node

After identifying mischievous nodes, a packet containing the mischievous node's ID, is produced by the source node for isolating detected mischievous nodes. On receipt of this packet, each Node Intermediate sets ''BHN'' column in its own EDRI table for identified nodes as ''1'', then re-broadcast the packet.

Algorithm: The security mechanism process

```
1.Initiator:  Create a random number
2.Initiator: set initiating node as NI
3.NI: Create data control packet and forward it for NH
4.NI: Stay for response
5.IN: If response is received
6.   {
7.If received random number is equal with sent number
8.  {
9.    Apprise EDRI table
10.             If NH is destination
11.                     {
12.                       Route is safe
13.                       End:
14.                     }
15.             Set NH as NI
16.             Jump to Line 3
17.           }
18. Else
19.           {
20.             Mark NH as mischievous node
21.             Jump to Line 28
22.           }
23.   }
24. Else
25.           {
26.            Jump to Line 28
27.           }
28. NI: Aware initiator node of NH's ID
29. Initiator: Set NH as NI
30. If NI is RREP originator
31.           {
32.           set RREP generator's NH as NI
33.           Jump to Line 35
34.           }
35. Initiator: Find a route to NI
36. Initiator: ask for NI's NH and EDRI entries
37. Initiator: check previous node for mischievous
38. Initiator: If previous node is mischievous
39.           {
```

```
40. Spot as Black hole
41. Jump to Line 49
42.          }
43. Initiator: If NI is hopable and placed after RREP originator
44.          {
45.           Route is safe
46.           End
47.          }
48. Initiator: Jump to Line 29
49. Initiator: Aware network about mischievous nodes
```

Simulation Results

NS2: The Network Simulator (ns2) is an event driven simulator. It offers considerable support for simulation of TCP, routing and multicast protocols over wired and wireless networks. Ns-2 code is transcribed either in C++ and OTCL and is kept in a separate file that is performed by OTCL interpreter, thus producing an output file for NAM (Network animator). It then designs the nodes in a position defined by the code script and shows the output of the nodes communicating with each other. 25 nodes are used for the simulation.

Following are the performance metrices:
Throughput: It is the volume of data per time unit that is delivered from one node to another through the communication link
Packet Drop: It indicates total number of data packets that could not touch destination successfully
End to End delay (End2End delay): This metric provides the overall delay, from packet transformation by the agent at the initiative node till packet reception by the agent at the target node

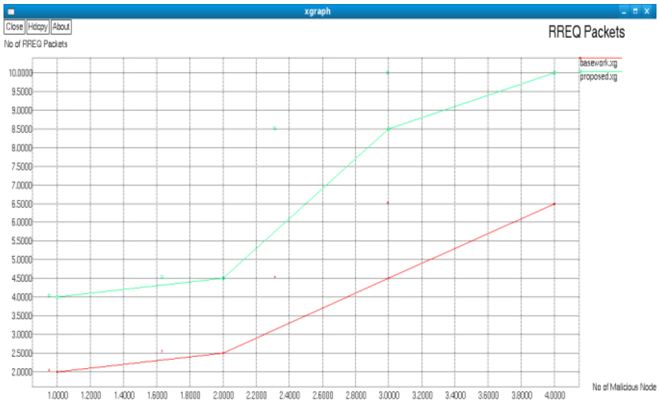

Figure 1: graph of time of detection

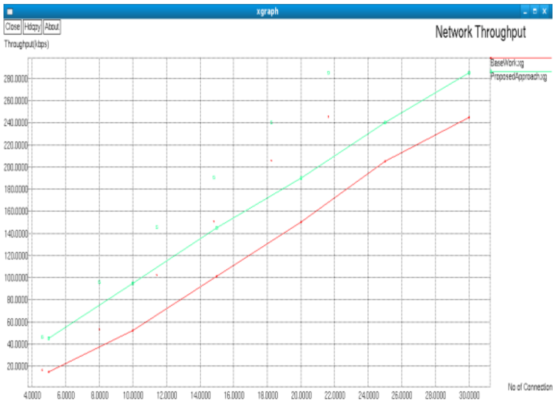

Figure 2: graph of network throughput

Conclusion

In MANET security is one of the challenges in routing protocols. AODV is one of the routing protocols which was effected by several attacks such as black hole, worm hole, gray hole attacks.. Using EDRI table is one of the best ways to mitigate the effects of attacks and also improve the performance. Furthermore, the Elliptic Curve Cryptography Scheme is another way to mitigate the black hole attack in AODV.

References:

[1] Jaisankar, N., Saravanan, R., &DuraiSwamy, K. (2010), “A novel security approach for detecting black hole attack in MANET.” Information Processing and Management Communications in Computer and Information, Science, 70, 217–223.

[2] Nath, I., &Chaki, R. (2012),”BHAPSC: A new black hole attack prevention system in clustered MANET.” International Journal ofAdvanced Research in Computer Science and Software Engineering,2(8), 113–121.

[3]Surana, K. A., Rathi, S. B., Thosar, T. P., &Mehatre, S. (2012),”Securing black hole attack in routing protocol AODV in MANETwith watchdog mechanisms.” World Research Journal of ComputerArchitecture, 1(1), 19–23.

[4] Jain, S., Jain, M., &Kandwal, H. (2010),”Advanced algorithm fordetection and prevention of cooperative black and gray hole
attacks in mobile ad hoc networks.” International Journal of Computer Applications, 1(7), 37–42.

[5] Rutvij, H. J., Sankita, J. P., &Devesh, C. J. (2012). “A novel approach for gray hole and black hole attacks in mobile ad hoc networks.” In Second international conference on advanced computing and communication technologies, IEEE.

[6] Sharma, D., Gajkumar Shah, P., & Huang, X. (2010). Protecting from attacking the man-in-middle in wireless sensor networks with elliptic curve cryptography key exchange. In NSS ‘10 proceedings of the fourth international conference on network and system security.

[7] Bindra, G. S., Kapoor, A., Narang, A., &Agrawal, A. (2012),”Detection and removal of cooperative black hole and gray hole attacks in MANETs”. In International conference on system engineering and technology, IEEE.

[8]Sen, J., Koilakonda, S., &Ukil, A. (2011).”A mechanism for detection of cooperative black hole attack in mobile ad hoc networks.” In Second international conference on intelligent systems, modeling and simulation (ISMS).

[9] Weerasinghe, H., & Fu, H. (2007),”Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation.” In Future generation communication andnetworking, FGCN (Vol. 2).

[10]Dorri, A., &Nikdel, H. (2015),”A new approach for detecting and eliminating cooperative black hole nodes in MANET.” In 7th conference on information and knowledge technology (IKT), (pp. 1–6). 26.

[11] Khan, Z. A., & Islam, M. H. (2012),”Wormhole attack: A new detection technique.” In International conference on emerging technologies (ICET).