BETC (BLACK-HOLE ERADICATION TECHNIQUE BASED ON CLUSTERING) FOR SECURING MANET BASED AODV

Sonam Yadav[1], Kanika L. Choudhary[2]

[1,2] *Assistant Professor, Department of Computer Science and Engineering, MRIU, (India)*

ABSTRACT

Securing Mobile Ad-hoc network against various kinds of attacks has become a crucial agenda now days because mobile ad-hoc network covers a wide range of application and overall cost of establishing an ad-hoc network and implementing security algorithm is still lesser than establishing an infrastructure based network. Therefore numerous security solutions have been proposed so far. In this paper we are implementing the BETC technique based on clustering for securing Routing protocol AODV against black hole attack. Our proposed algorithm works as a hierarchal intrusion detection system in mobile ad-hoc network.

Keywords: AODV, Black-hole node, Cluster, IDS.

I. INTRODUCTION

Computing world has been changed to a large extent in last decade. Along with various useful researches, malicious activities have also grown up as weeds. Mobile ad-hoc network has proved itself as an efficient tool to establish communication in areas where infrastructure cannot be build.

Mobile ad-hoc network can be seen as an autonomous ,dynamic system in which wireless devices are capable of communicating with each other within a radio range without any pre defined infrastructure.[5] has defined that topologies of ad-hoc network is mainly interdependent on two factors: transmission power and location of nodes.

The Ad-hoc On Demand Distance Vector (AODV) routing protocol establishes path between two nodes only when need arises. AODV is capable of both unicast and multicast routing. AODV acts as a reactive protocol, which search for path, only when two nodes intend to communicate with each other. AODV works on route request and route reply packets. When a node intends to establish path with other node for which source node does not have a route, it broadcasts a route request (RREQ) packet across the network. Intermediate nodes receiving this packet update their information for the source node and set up backward pointers to the source node in the routing tables. RREQ packet contains source node's IP address, current sequence number, and broadcast ID, and most recent sequence number for the destination of which the source node is aware. Intermediate node receiving the RREQ may unicast a route reply (RREP) in two cases: if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. Otherwise, RREQ is rebroadcasted. In case of some error, route error (RRER) packet is generated and forwarded.

Attackers can access mobile ad-hoc network in similar manner as legitimate users do because since there is no

infrastructure, so no security parameters are implemented. Attacks can be classified into two categories, active attacks and passive attacks. When attacker just snoops the information without disrupting network operation it comes under passive attack. Whereas when network operations are disrupted by directing data packets to false routes or by modifying routing parameters like hop count or sequence number, it is called as active attack.

Black hole attack is a kind of internal active attack in which the malicious node advertises itself to have shortest path to the destination, by sending fake route reply to source node in which it pretends to have highest destination sequence number. Instead of forwarding data packet to destination, malicious node drops it, resulting into denial of service attack. Next section includes related work and proposed BETC technique, which eradicates malicious node and secures AODV routing protocol against black hole attack.

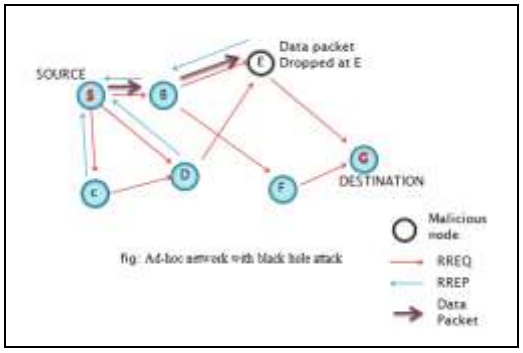

Fig. 1: Ad-Hoc Network With Black Hole Attack

II. RELATED WORK

So far many algorithms have been proposed to secure AODV against black hole attack. [3] has proposed a mobile agent based approach to detect selfish node by using a mobile agent that can freely move inside network and report for any misbehavior of node while forwarding data packet. Implementing Intrusion detection system in MANET is a tedious task. Hierarchal based IDS, provides multilayered architecture, whereas Distributed Intrusion Detection System uses multiple sensors etc.

M.Umaparvathi et.al in [4] has proposed two-tier architecture to secure AODV. They have proposed a tier – based algorithm which is capable of detecting single malicious node as well as group of nodes, collectively working to create black hole attack in a mobile ad-hoc network. Tier 1 detects single black hole node using verification message. Whereas tier 2 detect group of nodes, using Rc number of Control messages and Rm number of data packets. In [2] Murugan et.al has proposed cluster based technique to detect misbehaviour of nodes. Nodes are authenticated by implementing Proactive Secret sharing technique in a cluster based environment.

III. PROPOSED WORK

In this paper we are combining AODV routing protocol with Cluster based intrusion detection system. As mentioned above hierarchical based IDS is a multilayered architecture which means that nodes are divided into clusters and a cluster head inside each cluster posses more responsibilities like granting permission to a particular node to send data packet on behalf of its trust value. Our algorithm raises an alarm after identifying malicious node so that other legitimate nodes can be informed.

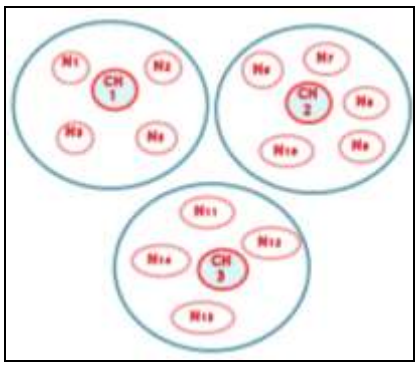

Fig.2: Division of nodes among Clusters

We have discussed in [1] that suppose N1 be the source node, D is the destination node which can be either in same cluster or different cluster. Let us suppose IMn be the intermediate nodes where n= 2, 3, 4…

During route discovery phase source node N1 request cluster head (CH1) to issue certificate. CH issues certificate to source node, after checking its trust value. Source node broadcast RREQ (route request) to all its neighbors. Format of RREQ is as follows:

RREQ< IPs, IPd, IDb, Seqs, Seqd, Cert, Hop_count >

Here IPs, IPd, is the IP address of source and destination respectively. IDb denotes the broadcast Id, Cert represents Certificate issued by Cluster Head. Hop_count depicts number of nodes message have passed. Since nodes are highly dynamic so it may be the case that destination may receive RREQ. We have categorized the entire scenario in three cases which are as follows:

CASE1: IMn has no route to destination.

In this case IMn would rebroadcast RREQ to its neighbors; a reverse path pointer is set to the node from which it received RREQ or source node. Hop_count field is incremented by 1. IMn would also add its own IP address to the rebroadcasted RREQ.

CASE2: IMn is Destination itself.

Destination unicast Reply to next hop towards source node. Source node on receiving Reply from source node, transfers the data packet to destination and waits for acknowledgement.

CASE3: IMn has fresh route to destination.

If IMn has fresh route to destination, it generates RREP and forwards it towards source along with IP address of the nodes which comes in between the path from source to destination.

Source node chooses IMn with higher sequence number and extracts the path details mentioned in RREP. Source stores the path details until it receives acknowledgement from destination. The format of RREP will be as such:

RREP < IPs, IPd, IDb, Seqs, Seqd, SeqIM, Cert, Hop_count , detail (IPi) > where i=1, 2, 3, 4…

IPi is the IP address of all the nodes which comes in between the path. i denotes the number of nodes. IPi is stored temporarily and dumped when source receives acknowledgement from destination.

In proposed method all the nodes that receive data packet send acknowledgement to the node from which it received it. If source node receives acknowledgement from destination within threshold time, path is found to be secure against black hole node and no further action is taken. Otherwise source starts verifying nodes. Source node unicast verification message to all the nodes whose details it had stored during RREP process. Through

verification message source asks the corresponding nodes to reply either TRUE or FALSE. If IMn has received acknowledgement from its next node it replies TRUE otherwise FALSE. We assume that hijacked node would always intend to hide itself. Suppose in above figure N6 is the source node and N10 is the destination. N7, N8, N9 are the intermediate nodes whose details has been stored by N6. N6 unicast verification message to N7, N8, N9 and N10. Upon receiving verification message each IMn replies either TRUE or FALSE to source. N6 might receive TRUE, FALSE or no reply.

Suppose a scenario where N7 replies TRUE, N8 and N10 replies FALSE, and N9 does not reply at all. In that case N9 is found to be malicious which acts as black hole node and did not forward the data packet. Alarm is raised by source node and N9 is excluded from network.

Source node analyze black hole node by considering different combination of TRUE or FALSE messages. The pseudo code is as follows:

Event: Source broadcast RREQ

Send cert_request; // *S sends Cert_request to cluster head*.

If[Cert_request = granted]

Send route_request ; // *Start to search the Route for Destination ;*

Initialize_timer T_Route_Request ; *// denotes threshold time*

Event: Route Reply

flag = true ;

while (flag = true)

Case 1: Destination received RREQ

if [route_reply from destination]

then

set destination_path = true // *flag used to check that destination is connected or not ;*

flag = false ;

end if

Case 2: IM_node received RREQ

if [Route_reply from Intermediate _node]

then

add_IM_node(IM_node_id, Sequence_no. Path_node_list) ; // *Adding intermediate node ids and their respective sequence numbers to path node list.*

end if

if [T_Route_Request expire]

then

flag = false ;

end if

if[IM_node consist no path towards destination]

set reverse_path_pointer;

hop _count=hop_count+1;

end if

end while

if [destination_path = true]

then

establish path ; // *IM_node having greatest sequence number.*

send data ;

end if

for i=1: 1:d *// i denotes total number of nodes in path and d denotes last node*

if [ack received]

then

flag=false;

else

send Rverify;

end if

Case 3: Duplicate RREQ received

if [route_request_id and destination_id is not in cache] // *Checking for duplicate request*

if [destination_id = node_id || destination_id= fresh route]

then

send route_reply ;

else

set reverse path_pointer

end if

Event: Verification

While(flag=true)

For i=1:1:d

Send Rverify;

If[Reply Rverify=true|| Rverify=false]

then

Check next _Rverify;// check next node's Rverify.

If[next_Rverify=NULL]

Break;// *node is found to be hijacked, alarm is raised.*

end if

end if

end while

We have implemented this algorithm in Matlab, by taking a scenario in which there is a cluster of 12 nodes. Node 1 and 12 is the source and destination respectively. Inside a network we have introduced that node 11 is a malicious node causing black hole. Our proposed algorithm detects Node 11 and broadcast a message in order to inform other nodes regarding malicious node. Implementation result has been shown by snapshots.

When proposed algorithm was simulated in NS-2, we found that is has very closed packet delivery ratio with AODV. Simulation parameters are as follows:

Parameters	Value
Area	670mx670m
Total Number of nodes	50
Application Payload data size	512/Kb
Radio Model	IEEE 802.11
Wireless propagation Model	Two Way
Antenna type	Omni directional
Mobility pattern	Uniform
Packet type	UDP

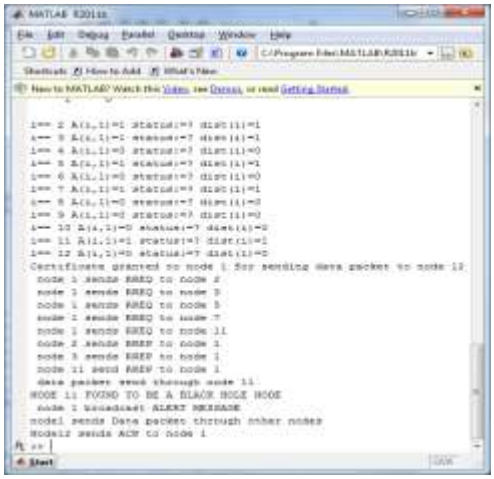

Fig.3: Snapshot of Implementation of Proposed Algorithm in Matlab

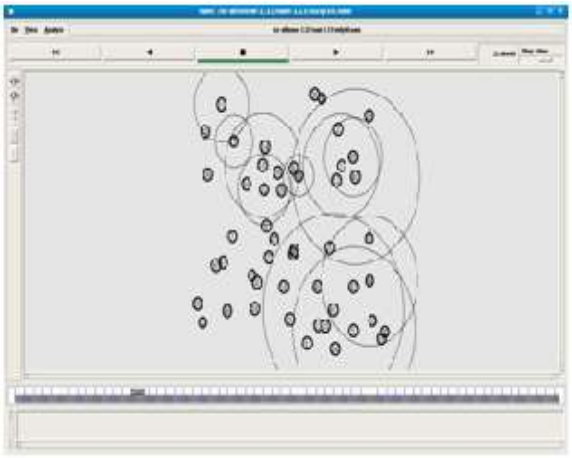

Fig.4: Simulation Of 50 Nodes In NS-2

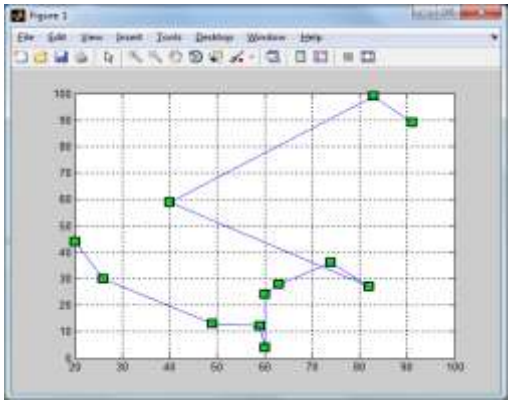

Fig.5: Graph Showing Path From Source To Destination

Fig.6: Packet Delivery Raito Of AODV

Fig.7: Packet Delivery Ratio of Proposed Algorithm

Although, at earlier stage packet delivery ratio of BETC is lower than AODV. It is so because, in our proposed algorithm source node needs to seek permission from cluster head, whereas AODV establishes communication path faster. But once the route is build, BETC has Packet delivery ratio very close to AODV.

IV. CONCLUSION

In Proposed algorithm Black hole node is identified and an alert message is broadcasted against it. The security solution proposed in this paper combines hierarchal IDS with AODV. In order to find Packet delivery ratio, a network of 50 nodes has been simulated in NS-2 and it was found that packet delivery ratio of proposed algorithm is quite close to AODV routing protocol. This algorithm can further be developed to be more energy efficient with respect to throughput and high packet delivery ratio.

REFERENCES

[1] Kanika L.Chaudary and Sonam Yadav, "A Cluster Based Technique for Securing Routing Protocol AODV against Black-hole attack in MANET", International Journal of Distributed and Parallel System(IJDPS), Australia,ISSN-0976-9757 [online]; 2229-3957[Print], Vol.4, No.2, March 2013 http//airccse.org/journal/ijdps/current2013.html

[2] R.Murugan, A.Shanmugam,"Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks"International Journal of Computer Science and Security ISSN 1985-1553 volume :6;Issue:3;Start page:188;Date:2012

[3] Debdutta Barman Roy and Rituparna Chaki, "MADSN: Mobile Agent Based Detection ofSelfish Node in MANET", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.

[4] M. Uma and G. Padmavathi, "A comparative Study and Performance Evaluation of Reactive Quality of Service Routing Protocols in Mobile Ad Hoc Networks", Journal of Theoretical and Applied Information Technology, Vol. 6, No. 2, 2009, pp. 223-22

[5] Mohd Izuan Mohd Saad and Zuriati Ahmad Zukarnain, "Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol", European Journal of Scientific Research, Vol. 32, No. 4, 2009, pp. 444-454.