Securing MANETs against Malicious Node Attacks with the Help of Back Bone Nodes (BBN)

Mariam Khan/Mrs. Anuradha Sharma

ABSTRACT-*A Mobile Ad-Hoc Network (MANETs) mainly consist of a collection of wireless mobile nodes which are capable enough to communicate among themselves without the requirement of any fixed network infrastructure or any centralized administration. In todays era, MANETs are basically an emerging research area with many practical applications. However, wireless MANETs in particularly vulnerable due to certain fundamental characteristics which includes open medium, dynamically changing topology, distributed cooperation, and constrained capability. Routing protocols plays a major role in providing the security of the entire network. However providing security to wireless MANETs is a big concern issue and that too is not easy to be removed .In this paper we have proposed the mechanism to detect and recover from the black/gray hole attacks in MANETs with the help of Back Bone Network (BBN).*

KEYWORDS: *Mobile Ad Hoc Network, Black hole, AODV.*

1. INTRODUCTION

MANETS are basically the collection of various mobile nodes which requires no central nodes or authority to manage the networks, also these nodes do not require any expensive base station due to which it work appropriately for a large no. of applications and are easily deployable and dynamic in nature. There are many ways to communicate wirelessly which provides communication means over large areas but with the help of MANETs we can communicate short as well as long distance [1] [4] .Since the nodes are mobile and communicate over a wireless channel, message security and transmission are a major concern. Nodes that are within each other's radio range can communicate directly via wireless links while the ones that are far apart totally depends on intermediate nodes to forward their packets to destination node. Each node can function as a host and as well as a router or provides functionality of both at the same time.

Many routing protocols are defined in order to provide efficient routing in MANETs. e g. AODV, DSR etc.

AODV [5] is basically a continuous improvement of the Dynamic Destination-Sequenced Distance Vector (DSDV) routing protocol. It is a reactive routing protocol, i.e routes are determined only when needed. It helps in the minimization of the number of broadcast by establishing routes based on demand. When any source node present in a network wants to communicate with destination node then it broadcast the route request (RREQ) packet. The neighbouring nodes on receiving the route request (RREQ) packets in turn broadcast the packet to their neighbours and the process goes on until the packet reaches the specified destination. During the process of forwarding the route request (RREQ) packets, intermediate nodes record the address of the neighbour from which the first copy of the broadcast packet is received. This record is then stored in their route tables, which finally helps in establishing a reverse path from destination to source to send route reply (RREP) packets. If additional copies of the same route request (RREQ) are later received, then these packets are discarded.

Now a days, providing security for the proper functionality of MANETs is the major concern . With the availability of current network services, confidentiality and integrity of the data sent through the network can be achieved by assuring that security issues have been met. MANETs usually suffer from network security attacks. The main purpose of these attacks in MANETs is to alter the parameters of routing messages or change the parameter of packets such as sequence no. , or even though not forwarding the packets and to exhaust the battery of nodes by making them traversing in wrong direction. Since till now, we are using the preventive mechanism of authentication and cryptography against attackers . But these can help in preventing attacks from outside the network but they are not appropriate enough to handle the attacker who resides inside the network. Any node present inside can cause major harm to the network by using this information. The presence of wireless links makes the MANETs more susceptible to attacks, they give open invitation to the attacker to penetrate inside the network and gain access to the resources as well as disrupt the communication going on among various nodes present in the network. [2], [3].

A black hole is the malicious node present along with other normal nodes in the network ,

pretends as having a shortest route to the destination. This node waits for the neighbouring node RREQ message. As soon as it receives RREQ it replies to them with a RREP to establish a communication route. When the data packets is actually started transferring it drops all the data packets which are meant for the destination. These nodes are difficult to find once if they start generating sequence number which are comparable to the current sequence number of network.

A gray hole attack has a slight variation to the black hole in a way initially is not malicious , it turns malicious after some time for a short period of time and start dropping the data packets destined to them after that it start behaving like a normal node. So it's become difficult to detect such behaviour of nodes.

In this paper we try to developed a mechanism to recover from these 2 attacks viz. black hole and gray hole attack. Our technique works as follows , we maintain a network of Back Bone Nodes(BBN) which operates at a level above the ad-hoc network. In this algorithm, this idea of establishing a network of BBN is used to monitor the traffic flow between various nodes present in the network. We have also used the concept of core formation and maintenance i.e., whenever a new node joins the network, Back Bone Node (BBN) sends an invitation message as a request to join one of the BBN. These BBN helps in monitoring the flow of traffic with the help of neighbouring nodes and analyses of the result generated by these neighbouring nodes help in the detection of various malicious nodes present in the network.

The rest of the paper is organized as follows. In section 2, we discussed the related work on detection and removal of black hole/gray hole attack. In section 3, we discuss network model and assumptions. In section 4, we present the methodology and algorithm. Finally the conclusion and Future work is discussed in section 5.

2. RELATED WORK:

S. Ramaswamy et . at. [6] has proposed an algorithm which prevents the MANETs from co-operative black hole attack . This algorithm is purely based on trust between the nodes present in the network hence it can't handle the gray hole attacks. Also due to intensive cross checking this algorithm is more time consuming and even though it consumes time when the network is not under attack.

Deng et.al. [7] has presented an algorithm which helps in the detection as well as the removal of black hole attack in MANETs .In this any node when receives a route reply (RREP) cross check with the next hop present on the route to the destination node from an alternate path .In case next hop does not have a route to the destination or does not have any link to the node that sent the RREP then in that case the node which responded with RREP is considered as malicious node .This algorithm does not work when malicious node is gray hole .

S. Banerjee et .al. [8] has presented an algorithm for the mitigation of Black/gray hole attacks in MANETs. According to their approach, instead of analysing the total data traffic at once , they divide the traffic into smaller blocks, so that it becomes easier to detect malicious nodes in between transmission. Traffic flow is monitored by the neighbouring nodes. Source node uses the scheme of acknowledgement received by the destination node to check data loss and in turn analyse black hole in the network. However in this case , it becomes difficult to analyse false positives as if it assumes that the node is misbehaving even though it is not.

Finally P.Agarwal et. al.[9] define a technique for establishing a back bone network of strong nodes. With the help of these back bone nodes , source and destination nodes can determine easily whether all the packets reached destination by carrying out end to end checking. If this check result shows some inconsistencies then the back bone nodes initiate the process of detecting malicious nodes in the network.

We have used the concept of back bone nodes and proposed an algorithm that is much simpler and helps in detecting black/gray hole attacks . For achieving this we have made use of the concept of back bone networks discussed by Rubin et.al [10]

3. NETWORK MODEL AND ASSUMPTION:

Many solutions have been proposed for black hole attack detection as well as removal. The approach that we are discussing here is based on the backbone network. In this approach , we maintain a backbone network consisting of back bone nodes(BBN), which works at a level above the ad-hoc network. In this algorithm , the idea of backbone network is used to monitor the traffic

flow between various nodes present in the network.

In our approach, we assume that the network consist of two types of nodes.

I . Regular nodes(RN)

These nodes are the ones which have low power and low transmission range as compared to other nodes present in the network and also these nodes are not trustworthy.

II . Back Bone Nodes(BBN):

These are the nodes having high transmission range and also higher power as compared to regular nodes and also they help in the formation of core which monitors the nodes present in the network.

We consider that the network is divided into various grids. The BBN present in a particular grid are allowed to roam in their specified area in search of regular nodes to send them an invitation message so that if on receiving positive reply from them can add those nodes into their associated node list after checking that they are reachable to BBN in a specified no. of hops .The BBN present in one grid are allowed to communicate with the back bone node present in other grids.

Black Hole Attack Detection:

It consist of following 2 steps:

1. Core Formation as well as Maintenance

2. Detection of Malicious nodes.

CORE FORMATION AND MAINTENANCE :

It progresses incrementally. During this phase, Back Bone Node(BBN) performs some tasks which are as follows:

i). Back Bone Node(BBN) roams throughout the network to detect regular node (RN) present in its neighbourhood , so that whenever it finds some node it broadcast the invitation message.

ii). If regular node(RN) positively responded to the invitation message received from the Back Bone Node(BBN), then immediately the BBN checks whether this regular node(RN) is reachable in a specified no. of hops. If yes then add to it in its association node list else forwarded it to unassociated node list , so that other back bone nodes present in the network can send invitation message to this regular node(RN).

Actions Performed by Regular Node(RN):

i). All the regular node(RN) present in the network must have to be associated with one of the Back Bone Node(BBN). Once if it is associated with any of the Back Bone Node(BBN) then only it can broadcast the RREQ message to established path for communication.

ii). If the regular node(RN) receives an invitation message requested it to join the Back Bone Node(BBN) , regular node(RN) must give the positive reply to it unless and until it is not associated with any Back Bone Node(BBN).

4. METHODOLOGY & ALGORITHM

The main purpose of this approach is to list out the set of all malicious nodes locally at each node present in the network whenever they act as a source node.
As mentioned above our proposed algorithm uses the concept of core formation and maintenance i.e., whenever a new node joins the network, BBN sends an invitation message as a request to join one of the BBN.

4.1 DETECTION and REMOVAL OF BLACK HOLE (MALICIOUS NODE):

Whenever the source node wants to send the data packets to the destination node, it broadcast a route request (RREQ) message throughout the network , a route reply (RREP) is received from the destination node or from the intermediate node having fresh enough route to the specified destination and a path for communication is established from source to destination node. In our approach, before the source node starts sending the data, it divides these data packets into small equal parts {1,….,k}.
After every block of data sent, the source node informs the Back Bone Node(BBN) through sending check message to perform a check at the destination node , whether the data packet sent by source node is reachable to the destination node.

If the data packets are safely reachable to the destination node , then BBN informs the source node . After confirmation from BBN , source node sends further data packets incrementally. If in case, the data packets are not reachable to the destination node then the source node is informed by BBN about the presence of some malicious node so that source node does not send further data packets and BBN initiates the process of detection of chain of malicious nodes.

Let us consider,

S=Source node
D= destination node
B1=Back Bone Node to which source node (S) is associated.
B2= Back Bone Node to which destination node (D) is associated.
R= Regular node
Im =Intermediate node which sends RREP to source node specifying that it has possible route to destination node.

ACTION PERFORMED BY SOURCE NODE(S):

1).Before sending any data packets divide these data packets into k equal parts i.e. {1,..,k}.

2).Once the route is established from source to destination node, source node starts sending data packets one by one. Initially when the source node send first data packet to D, it informs the B1 node by sending a check message containing Nm to perform end to end check whether the data packet has reached the destination node.

3). If 'OK' is received from B1 to S, then it continues sending data packets to D.

4). If 'NOT OK' is received from B1 ,then it indicates the presence of malicious node and a timer is set by source node for removal of malicious node .

5).If a message is received about the removal of malicious node then go to step 2 else terminate D.

ACTION PERFORMED BY BACKBONE NODE TO DETECT & REMOVE BLACK HOLE:

1). Back Bone node B1 informs the other BBN B2 about the presence of malicious node in the network.

2). Back Bone node B1 sends monitor message to all the neighbours of source node (S) and ask them to enter into promiscuous mode and start monitoring the data sent by S and wait for the result message. In the same way BBN B2 also performs the same action to monitor the data received by destination D.

3). Source node start sending dummy data packets to the destination node .

4). If the result of the monitor message is received within specified time then these result are analysed i.e. if the amount of data sent is same as the data received ,then it indicates destination node D in not malicious else D is malicious node.

5). If the destination D is not malicious then BBN instruct all the neighbours of Im to vote for the next node to which Im is forwarding packets originating from S to D.

6).On receiving the node id's from neighbouring node, BBN find the node to which Im is forwarding the data packets.

7).If no node is getting packets , then it indicates that Im is dropping all the packets . Hence, node Im is malicious and declared black listed .

8).In case, if the destination node(D) or intermediate node (Im) is black listed then message is broadcasted across the network to inform all other nodes about this malicious node.

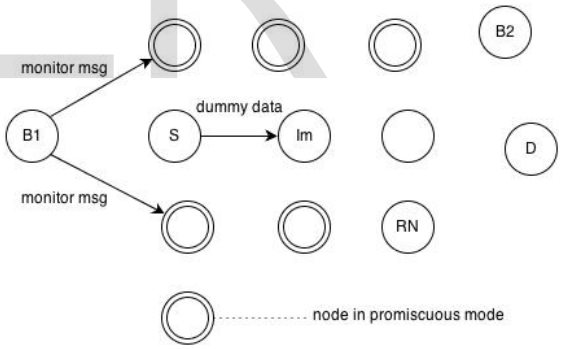

Fig1. Propagation of Monitor message & dummy data packets.

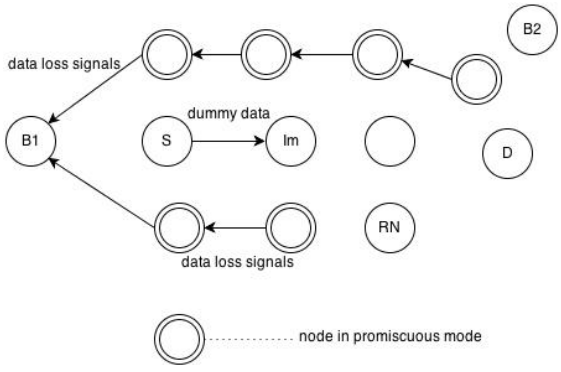

Fig2. Identification of Black hole node by promiscuous nodes.

The above technique is also useful for the detection of gray hole also , as there is no trust relationship between regular nodes(RN) present in the network i.e. if at any instant the regular node becomes malicious then it can be detected by data transmission through neighbouring nodes .

This algorithm also help in the detection of cooperative black hole attack , as back bone node decides the location of the black hole with the reply message of majority of neighbouring nodes . So any node which is cooperating with a single black hole can easily be caught by the neighbouring nodes .

5. CONCLUSION & FUTURE WORK:

In this paper we have presented a solution to detect and remove the malicious nodes in the ad hoc network with the help of BNN . The proposed solution can be applied to identify and remove any no. of black hole/gray hole in MANETs and finally helps in discovering a secure path from source to destination node by avoiding these malicious node.

In Future work-

1.Try to simulate this algorithm to analyse and compare the result from previously defined algorithms.
2. We can study the effect of false feedback i. e we analyse that the node is misbehaving even though it is not.
3. This algorithm can also be applied to detect malicious nodes in other routing protocols of MANETs.

6. REFERENCES:

[1] A. Babakhouya, Y. Challal, and Bouabdallah. " A simulation analysis of routing misbehaviour Report. University of Maryland at College. Park. In mobile ad hoc network" pp.592{597,2008.Ding,W. and Marchionini,G.1997 A study on video browsing strategies. Technical

[2] P.V.Jani, "Security within Ad-Hoc Networks,". Position Paper, PAMPAS Workshop, Sept. 16/17 2002

[3] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[4] S.Abbas, M. Merabti, and D. Llewellyn-Jones, " The e_ect of direct interaction Reputation based scheme in mobile ad hoc network"pp.297{302,2011

[5] I. Raza and S. Hussain, " Identi_cation of malicious nodes in an aodv pure ad hoc network through guard nodes" Computer Communications, vol. 31 , no. 9, pp.1796{1802,2008.

[6] Sanjay Ramaswamy , Huriong Fu, Manohar SreeKantaradhya, John Dixon, and Kendall Nygard , "Prevention of Cooperative Black hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks(ICWN'03), Las Vegas Nevada, USA,pp.570-575.

[7] Hongmei Deng, Wei Li, and Dharma P. Agarwal , "Routing Security In Wireless AD Hoc Network," IEEE Communications Magazine ,vol. 40, pp. 70-75, 2002.

[8] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer science 2008 wcecs 2008, October 22-24, 2008, San Francisco, USA

[9] Piyush Agarwal , R. K. Ghosh , Sajal K. Das, Cooperative Black hole and Gray hole Attacks in Mobile Ad hoc Networks In Proceedings of the 2nd International Conference on Ubiquitous information management and communication , pages 310-314, Suwon, Korea , 2008

[10] I . Rubin, A. Behzad, R.Zhang, H.Luo and E.Caballero. Tbone: A mobile back bone protocol for ad hoc wireless networks. In Proceedings of IEEE Aerospace Conference ,volume 6, pages 2727 2740, 2002.

.