A Cooperative Blackhole Node Detection Mechanism for ADHOC Networks

Moumita Deb

Abstract— **The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. A mobile node in ad hoc networks may move arbitrarily and acts as a router and a host simultaneously. Such a characteristic makes nodes in MANET vulnerable to potential attacks. The black hole problem, in which some malicious nodes pretend to be intermediate nodes of a route to some given destinations, drop any packet that subsequently goes through it, is one of the major types of attack. In this paper, I propose a cooperative mechanism to tackle the black hole problem. The mechanism is cooperative because nodes in the protocol work cooperatively together so that they can analyze, detect possible multiple black hole nodes in a more reliable fashion. The proposed algorithm works into two phases so that it can reduce the rate of false alarm.**

Key Words—**MANET, Blackhole.**

I. Introduction

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks.

Blackhole attack is one of many possible attacks in MANET. One type of black hole attack can occur when the malicious node on the path directly attacks the data traffic by intentionally dropping, delaying or altering the data traffic passing through it. In other type, a malicious node sends a forged Route REPly (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. By comparing the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the most recent routing information and selects the route contained in that RREP packet. In case the sequence numbers are equal it selects the route with the smallest hop count. If the attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than the real destination node to the source node, the data traffic will flow toward the attacker. However, once the data packets begin flowing through this route, they may just be dropped without being relayed. In this case, the node acts like a “black hole”, which consumes any incoming data packets. Therefore, source and destination nodes became unable to communicate with each other.

In this paper, we use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV)[1] routing for analysis of the effect of the blackhole attack when the destination sequence number are changed via simulation. In this work, we propose a two-step cooperative detection mechanism that would detect potential multiple black hole nodes. Every node keeps track of its neighbor by maintaining two small size tables, sequence table (SnT) to keep the neighbor node’s IP address and neighbor node’s sequence number and status table (ST) to keep track of the node’s status whether it is a safe node or a malicious one. Every node also maintains a neighbor list (N_List) and this list is updated periodically. The intermediate node with the help of the information stored in the tables can determine if the sending nodes forged the sequence number or not. Once it has detected a suspicious node then the second step detection come to existence.

II. Related work

A number of protocols were proposed to solve the black hole problem which require a source node initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination.

In [2] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park proposed two different approaches to solve the blackhole attack. In first proposal the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. The idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route are identified. Once a safe route has identified, these buffered packets will be transmitted. But the main drawback of this algorithm is time delay. In the second proposal every node stores the last sent packet sequence number and last received packet sequence number. When a node receives a RREP from another node it checks the last sent packet sequence number and received packet sequence number, if there is any mismatch then it generates an

Manuscript received July 25, 2006. Paper title is A Cooperative Blackhole Node Detection Mechanism for ADHOC Networks.

Moumita Deb is with the West Bengal University of Technology, Saltlake,India.phone:+919474581218;e-mail: moudeb@gmail.com

alarm indicating the existence of a blackhole node. But drawback of this algorithm is if the network is large, mismatch in the sequence numbers does not guarantee the existence of a blackhole node.

In [3]Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch used two additional control packets for collecting the neighborhood information for detecting the blackhole node. The formats of these packets are
RQNS {Scr_addr, Dest_Addr, Request_neighbor_seq#, Next_hop} and
RPNS {Scr_Addr, Dest_Addr, Request_neighbor_seq#, Neighbor_Set}
The basic idea of this approach is that the neighbor set difference of one node at different time instance is less than or equal to one, and the probability that the neighbor set difference of two nodes at same time instance is very small. After getting RREP from more than one node the sender sends the RQNS packet. After receiving more than one RPNS packet the sender node compare the received neighbor set, if the difference is larger than some pre defined threshold value then the current network is affected by blackhole attack. But the drawback of this approach is after comparing the neighbor set they use a cryptographic method to identify the actual infected node. This is a costly and less reliable technique in case of ad hoc network.

In [4] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang proposed a distributed and cooperative procedure to detect blackhole node. First each node detects the local anomalies, then after finding the local anomalies the sender node calls for a cooperative detective by sending a message to the neighbor of the infected node. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network. They use a voting scheme to identify the blackhole node. If all the nodes vote for the infected node, then the node is declared as blackhole node. The drawback of this algorithm is it cannot detect the cooperative blackhole attack and the voting scheme is not good.

In [5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto use an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. To express state of the network at each node, multidimensional feature vector is defined. The feature vector contain {Number of sent out RREQ messages, Number of received RREP messages, The average of difference of Dst Seq in each time slot between the sequence number of RREP message and the one held in the list}. Now they calculate the Mean vector by using some mathematical calculation. Then they compare the distance between the mean vector and input data sample. If the difference is greater than some threshold value then there is an attack. In this way they update the training data set to be used for the next detection. Then, the mean vector, which is calculated from this training data set, is used for detection of the next data. By repeating this for every time interval T, they perform anomaly detection.

In [6] Hongmei Deng, Wei Li, and Dharma P. Agrawal proposed a solution for single blackhole node detection. In the proposed method, each intermediate node to send backs the *nexthop* information when it sends back an RREP message. When the source node receives the reply message, it does not send the data packets right away, but extracts the *nexthop* information from the reply packet and then sends a *Further-Request* to the *nexthop* to verify that it has a route to the intermediate node who sends back the *Further reply* message, and that it has a route to the destination node.

In [7] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard proposed a method for identifying multiple black hole nodes. They are the first to propose a solution to cooperative or group black hole attack. The methodology works with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking. DRI table contains {Node ID, From, Through}.Every node maintains this table. They rely on reliable nodes (nodes through which the source node has routed data) to transfer data packets. When an intermediate node replies a RREP to a given source node, the Next Hop Node and DRI entry of Next Hop Node should also be sent together. The Source node will then use the information together with its own DRI table to check whether the Intermediate Node is a reliable node. If it is not reliable, then it sends a Further Route Request packet to the node next to the intermediate node and asks NHN: 1) if IN has routed data packets through NHN, 2) who is the current NHN's next hop to destination, and 3) has the current NHN routed data through its own next hop. The NHN in turn responds with Further Route Reply message including 1) DRI entry for IN, 2) the next hop node of current NHN, and 3) the DRI entry for the current NHN's next hop. Based on the Further Route Reply message from NHN, source node checks whether NHN is a reliable node or not.

III. METHODOLOGY

We use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV)[1] routing for analysis of the effect of the blackhole attack when the destination sequence number is changed via simulation. In this work, we propose a two-step cooperative detection mechanism that would detect potential multiple black hole nodes.
The proposed algorithm works in two phases i) First phase detects those nodes, which may be malicious. Then the source node initiates the next phase.

ii) In this phase neighbor of the malicious node initiates a cooperative detection mechanism to detect the actual blackhole node.

i) **First Step Detection-** In AODV routing messages contain only the source and the destination addresses. It uses destination sequence numbers to specify how fresh a route is

(in relation to another). At first the sender broadcast the RREQ message to its neighbors. Whenever a node needs to send a packet to a destination for which it has no 'fresh enough' route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in
any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast checks the destination to see if it is the intended recipient. If yes it sends a RREP message back to the originator. RREP message contains the current sequence number of the destination node. The same process continues till the packets reach to destination or reach to an intermediate node, which has a fresh, enough routes to destination.

Based on this concept the first detection algorithm works. In order to detect the blackhole attack, the destination sequence number is taken into account. In normal state, each node's sequence number changes depending on its traffic conditions. When the number of connections increases the destination sequence number tends to rise, when there are few connections it tends to be increased monotonically. However, when the attack took place, regardless of the environment the sequence number is increased largely. Every node keeps track of its neighbor by maintaining two small size tables. One is sequence table (SnT) to keep the neighbor node's IP address and neighbor node's sequence number and other is the status table (ST) to keep track of the node's status whether it is a safe node or a malicious one. Every node also maintains a neighbor list (N_List) and this list is updated periodically. When an intermediate node receives a RREP checks if the difference between the Dst_Seq present in the RREP message and the sequence no present in its table is greater than some predefined threshold value? if so then the intermediate node stops forwarding the message and mark the node as 'M' or malicious in the status table(ST) and send a notification message(NM) to source node along with the malicious node's IP address and neighbor list of the malicious node. The threshold value is the average difference of Dst_Seq in each time slot between the sequence number of RREP message and the one held in the table.

Algorithm for First step Detection-

```
Begin
{SN=Source node, DN=Destination node, ST=Status Table,
N-List=Neighbor List, SnT=Sequence Table,
IN=Intermediate Node, M=Malicious Node, M1HN=MN's 1
hop neighboring node.}


1. SN broadcast RREQ along with the Dst_Seq

2. For each IN receives the RREQ check
         If DN=IN and Dst_Seq in RREQ <= Dst_Seq in SnT?
            Send RREP with the Dst_Seq in SnT and N_List.
        Else broadcast the updated RREQ message.

  (To check the malicious node)

3.  For each node IN receives RREP.
        Checks if (Dst_Seq in RREP -Dst_Seq in SnT) >Thr
                Add the Node's IP to the ST and make the status
           as 'M', stops forwarding RREP
                Send a notification message (NM) to SN
     contains node's IP and N_List
              Else add the Node's IP to the ST and make the
     status as 'S' and forward RREP.

4.  Upon receiving the NM, SN broadcast a Further
    Detection message to all M1HNs

    End
```

As in Fig 1. Sequence Table (SnT), Status Table (ST) and Neighbor List (N_List) maintained by node 5 (assuming the sequence no)

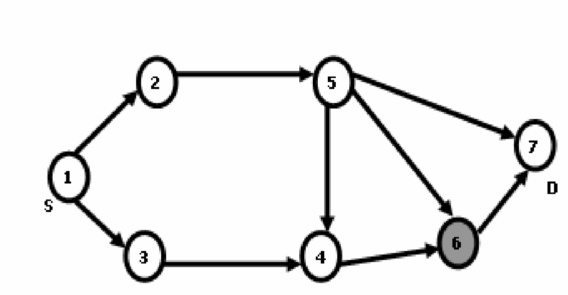

Fig 1.

Table i. Sequence Table

Node #	Dst_Seq
4	12
6	16
7	18

Table ii. Status Table

Node#	Status(S=Safe, M=Malicious, B=Blackhole)
6	M
2	S

Table iii. Neighbor List

Node#	Neighbor
5	4,7,2,6

Second Step Detection- Once the first step detection method finds a possible blackhole node, the second step detection method is activated by the initial node which proceeds by first broadcasting and notifying all the one hop neighbors of the possible suspicious node (M1HN) to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. The source node has an additional table called Voter Table which is used in second step detection. M1HN's after receiving the Further Detection message, broadcast a RREQ message by setting destination address to source node's address. If it receives a RREP message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends a Acknowledgment Packet (AP) to source node(SN) though some other route. Then the source node waits for '*wt*' time until it receives the entire test and acknowledgement packet. If, SN receives a TP, it updates the Voter Table (VT) by adding the source node ID to the table set the vote of the node as 'Y' and if an AP is received set the vote as 'N' and update the count field. If all the entries for the malicious node are 'N' then source node updates the status table (ST) by adding the MN's IP to the ST and making the status as 'B' i.e. Blackhole. The algorithm and flowchart of second step detection method is given here. As in fig 3. Voter Table maintained by SN and after confirmation of the Blackhole node the Status Table of SN is shown.

Algorithm for Second Step Detection-

```
Begin
{SN=Source node, DN=Destination node, ST=Status Table, IN=Intermediate Node, MN=Malicious Node, M1HN=MN's 1 hop neighboring node. wt=waiting time, AP=Acknowledgement Packet , VT=Voter Table}

1. SN broadcast further detection message to all M1HN's

2. For each M1HN receive further detection message

   Broadcast RREQ (with DN being set to SN)
       If  MN sends a RREP to M1HN
           M1HN send a Test packet to SN via this route
       Else
           M1HN send an acknowledgement packet (AP) to SN by using some other path.

3. SN waits for two 'wt' time
           If  a Test Packet is received then add the source node ID to VT,
           Make vote as 'Y'.
         Else
           If an acknowledgement packet is received then add the source node ID to VT,
             Make vote as 'N'.

4. If all the votes are 'N', SN update it's status table (ST) by adding MN's ID and setting
     Status as 'B'.
     Else set the status as 'S'.

End
```

As in Fig 1. Status Table (ST) and Voter Table (VT) maintained by source node are

Table iv. Status Table (ST)

Node
#
	Status(S=Safe,
	M=Malicious,
	B=Blackhole)

3	B

Table v. Voter Table(VT)

Voter	Vote
7	N
5	N
4	N

Final Reaction-

As soon as a confirmed black hole node is identified, the source node initiates a proper notification system to send warnings to the whole network. The procedure begins with the initial detection node notifying all the neighboring nodes of the suspicious node in the same way as the cooperative detection process. The notified nodes then send warning messages accordingly. When all the nodes on the network receive enough warning messages, they update their status table by adding the malicious node's IP as blackhole one. All later data transmission will not go through nodes in the black hole list.

IV. CONCLUSION AND FUTURE WORK

This is a new approach to blackhole node detection, the two step procedure helps to reduce false detection rate. This is a reliable procedure since all mobile nodes cooperate together to analyze and detect possible multiple black hole nodes.

If the neighboring nodes of the malicious nodes are also blackhole node i.e. if group blackhole attack occurs then this algorithm can't be able to detect that. So my future work would be to consider this feature. Also I have not simulated this algorithm in any real time network environment so my future work would be to test the algorithm by using NS-2 or any other network simulator.

REFERENCES

[1] C E Perkins,E M Royer,S.R Das, "Adhoc On-Demand Distance Vector(ADHOC) Routing" Internet Draft, draft-ietf-manet-aodv-08.txt, 2001.

[2] Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park," Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04,April 2-3,2004,Huntsville,AL,USA.

[3] "Detecting Black-hole Attack in Mobile Ad Hoc Network" by Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch.2003 The institute of Electrical Engineers.Printed and published by IEEE.

[4] "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" by Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and

Yoshiaki Nemoto. International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[5] "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network" by Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang. Springer-Verlag Berlin Heidelberg 2007.

[6] "Routing security in Wireless Ad-hoc Network" by Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati.

[7] "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard.