Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks

Vishnu K
B.tech V sem
MNNIT Allahabad
INDIA

Amos J Paul
B.tech V sem
MNNIT, Allahabad
INDIA

ABSTRACT

Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. Later on they may split into smaller groups. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes.

Keywords

Mobile Ad-hoc Networks, Black Holes, Gray Holes,Routing, AODV,Routing Table

1.Introduction

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to its dynamic nature MANET has larger security issues than conventional networks.

AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself.

Each intermediate node receiving the RREQ, makes an entry in its routing table for the node that forwarded the RREQ message, and the source node. The destination node or the intermediate node with a fresh enough route to the destination node, unicasts the Route Response (RREP) message to the neighboring node from which it received the RREQ. An intermediate node makes an entry for the neighboring node from which it received the RREP, then forwards the RREP in the reverse direction. On receiving the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP.

A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack.

A gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later.

In this paper we present a mechanism to detect and remove the above two types of malicious nodes. Our proposed technique works as follows. Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted(unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP(RIP)also. If any of the route responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

The rest of the paper is organized as follows. In section 2, we discuss the related work on detection/prevention of black hole attacks. In section 3, we discuss the network model and assumption. In section 4, we present the methodology and algorithms. Finally the conclusion & discussion of future work is discussed in section 5.

2.Related Work

Deng et. al. [2] have proposed an algorithm to prevent black hole attacks in ad hoc networks. According to their algorithm, any node on receiving a RREP packet, cross checks with the next hop on the route to the destination from an alternate

path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This technique does not work when the malicious nodes cooperate with each other.

S.Ramaswamy et. al. [3] presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks.Besides due to intensive cross checking, the algorithm takes more time to complete, even when the network is not under attack.

S.Banerjee et. al. [4] has also proposed an algorithm for detection & removal of Black/Gray Holes. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks, in the hope that the malicious nodes can be detected& removed in between transmission. Flow of traffic is monitored by the neighbours of each node. Source node uses the acknowledgement sent by the destination to check for data loss & in turn evaluates the possibility of a black hole. However in this mechanism false positives may occur and the algorithm may report that a node is misbehaving, when in fact it is not.

Finally P.Agarwal et. al. [5] have proposed a technique of establishing a backbone network of strong nodes. With the assistance of the backbone network of strong nodes, source and destination nodes carry out an end to end checking to determine if all the data packets reached the destination. If checking results in a failure, then the backbone network initiates a protocol for detecting the malicious nodes.

We have used this concept of backbone nodes & designed an algorithm that is much simpler. We have also made use of the concept of statefull approach of IP addresses allocation in ad-hoc networks as discussed by S.Indrasinghe et. al.[6] and Mansoor Mohsin et. al.[7]

3.Network Model & Assumption

We approach this problem by selecting some nodes which are trustworthy and powerfull in terms of battery power and range. These nodes which are referred to as Back Bone Nodes(BBN) will form a Back Bone network and has special functions unlike normal nodes. For the co-ordination between the Back Bone Nodes(BBN) and the Normal Nodes, it is assumed that the network is divided into several grids. It is assumed that the nodes, when initially enters the network is capable of finding their respective grid locations.

It is also assumed that the number of normal nodes are more then the number of black/gray nodes at any point of time.

3.1Statefull Allocation of IP address-

The IP address configuration in case of MANETs can broadly be classified into-

i.Stateless approach

ii.Statefull approach

In the stateless approach an unconfigured host must obtain its own IP address by self assignment. This stateless approach adopts random address assignment and is followed by duplicate address detection mechanism to achieve address uniqueness. Stateless approaches do not keep any allocation table .

In the statefull approach an unconfigured host asks its neighbouring MANET to work as proxies to obtain an ip address. We have devised a new type of state-full approach viz. Core Maintenance of the Allocation Table.

3.2Core Maintenance of the Allocation Table :-

In this approach only the backbone network in MANET is permitted to select the IP addresses for unconfigured hosts. The mechanism is based on allocating a conflict free address to all newly arrived nodes by using multiple disjoint address spaces[6]. Each BBN in MANET is responsible for allocating a range of addresses disjoint from the ranges of all other BBN. In other words each BBN generates numbers that are unique for that host. Every hosts in the MANET must have the possibility to reach one of the Backbone Nodes (BBN) all the time.

4. Methodology & Algorithm

The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table ie, whenever a new node joins the network, it sends a broadcast message as a request for IP address.

The backbone node on receiving this message randomly selects one of the free IP addresses . The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes(BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.

4.1 Detection and removal of Black / Gray holes

Initially when the source node wants to make a data transmission, it requests the nearest BBN for a restricted IP (RIP). The BBN on receiving the RIP answers to the source node with one of the unused IP addresses selected randomly out of the pool of unused IP addresses. The source node sends the RREQ for both the destination and the RIP simultaneously.

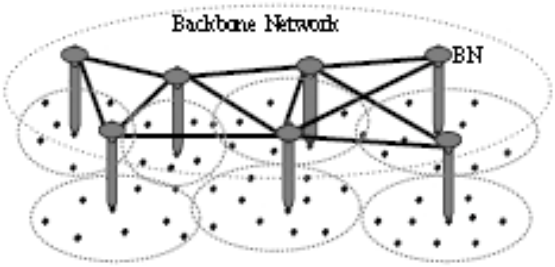
Now if the Source Node (SN) gets the RREP only for the destination node(which is the normal case) and not the RIP, then the local network space is free from any of the black holes and currently free of any gray holes too. The source node reuses the RIP for a definite period of time for further data transmissions. Until that period of time the BBN does not assign any other node, this recently given out RIP.

However in case the SN gets an RREP for the RIP, then it means that, there is a black hole in that route. In this case the SN initiates the process of Black Hole detection.

The SN initially alerts the neighbours of the node from which it got the RREP to RIP, to enter into promiscous mode, so

that they listen not only to the packet destined to them, but also to the packet destined to the specified Destination node. Now the SN sends a few dummy data packets to the destination, while the neighbouring nodes start monitoring the packet flow. These neighboring nodes further transmit the monitor message to the next hop of the dummy data packet & so on. At a point when the monitoring nodes finds out that the dummy data packet loss is way more than the normal expected loss in a network, it informs the SN about this particular Intermediate Node(IN). Now depending on the information received by the various monitoring nodes, the SN detects the location of the Black Hole.

This information is propagated throughout the network leading to its listing as black hole and revocation of their certificates. Further all nodes discards any further responses from this black hole and looks for a valid alternative route to the destination.



The above technique also works for gray holes also, as we are not using any trust based relationship between nodes i.e. even if a normal node turns into a black at any point of time, it is detected by normal Data transmission process by any of its neighbouring normal nodes.

Even in the case of cooperative black holes, the node that ultimately eats up the data packets, gets caught. Besides the Source Node decides the location of a black hole by the feed back of more than just one neighbouring node. Hence it will lead to the detection and elimination of the malicious node.

Figure 1. Pictorial Representation of an Ad hoc network with a back bone network.

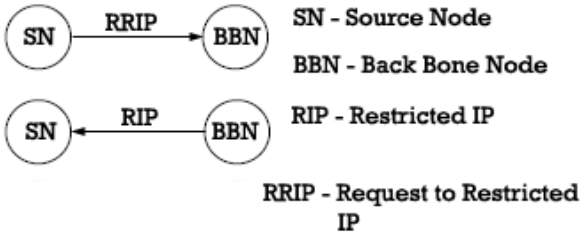


Figure 2. Request for RIP & RRIP packet

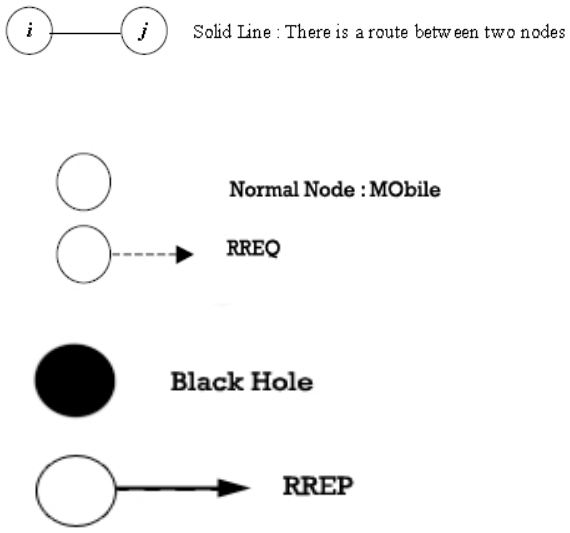


Figure 3. Nodes and their representation

RREQ - Route Request packet
RREP – Route Response packet

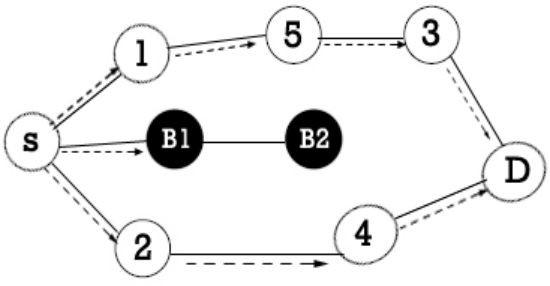


Figure 4. Propagation of RREQ message

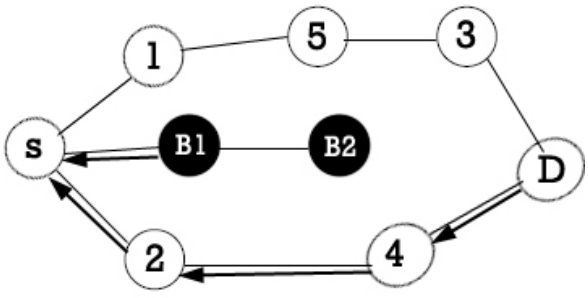


Figure 5. Propagation of RREP

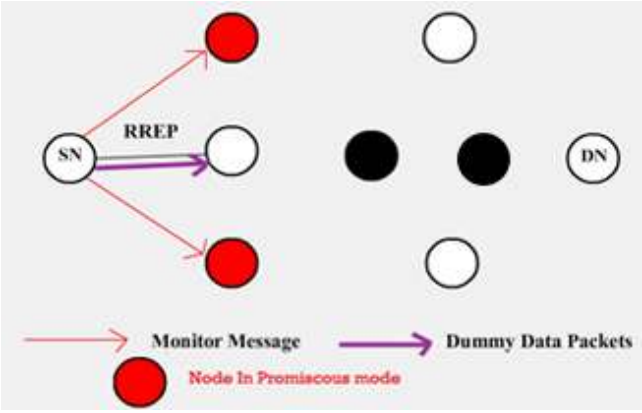


Figure 6. Propagation of Monitor message & dummy data packets

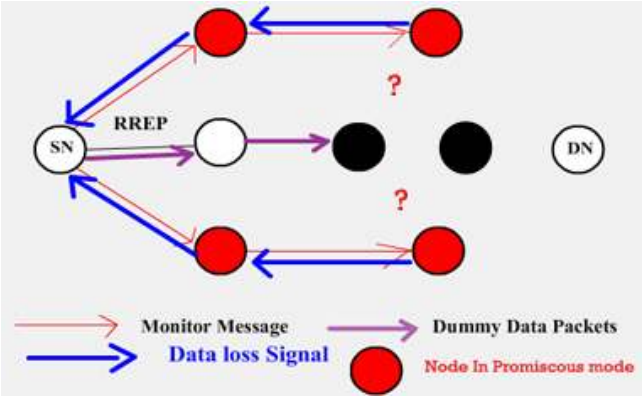


Figure 7. Identification of the Black Hole by promiscous nodes

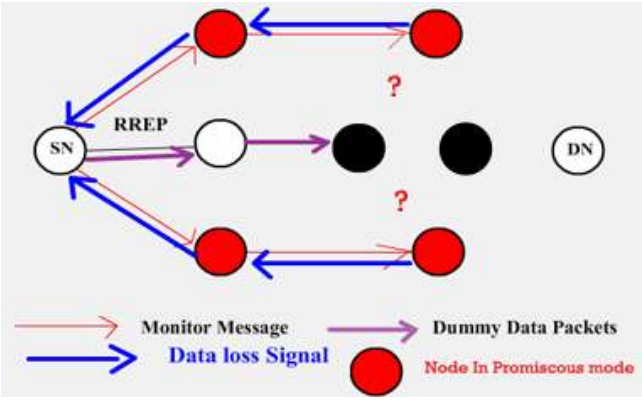


Figure 8. Propagation of Data loss Signal back to the Source Node

4.2Algorithm

Actions by Source Node (SN)

Step 1: Source Node(SN) sends a Request to Restricted IP(RRIP) to the Back Bone Node(BBN).

Step 2: On receiving the Restricted IP(RIP), from the BBN it sends the RREQ for the Destination as well as for the RIP simultaneously.

Step 3: Awaits for RREP.

Actions by Intermediate Node/Destination Node

Step 1: On receiving the RREQ it first makes an entry in its Routing table for the node that forwarded the RREQ.

Step 2: If it is the Destination node or if it has a fresh enough route to the Destination node, it replies to the RREQ with an RREP.

Step 3: If it is nether the destination nor does it have a fresh enough route to the Destination, then it forwards the RREQ to its neighbours.

Step 4: On receiving an RREP, it again makes a note of the node that sent the RREQ in its routing table & then forwards the RREP in the reverse direction.

Step5: On receiving a request to enter into the promiscous mode, it starts listening in the network for all the packets destined to that particular IP address & monitors its neighbours, for the movement of the dummy data packet.

Step6: In case, it finds out that the dummy data packet loss is exceptionally more than the normal data packet at any particular node, it informs back the IP of this IN.

4.2.1Gray/Black Hole Removal process

Actions by Source node on receiving the RREP

Step 1: If the RREP is received only to the Destination & not to the Restricted IP(RIP), the node carries out the normal functioning by transmitting the data through the route.

Step 2: If the RREP is received for the RIP, it initiates the process of black hole detection, by sending a request to enter into promiscous mode, to the nodes in an alternate path(i.e. neighbours of next hop for RIP).

Step 3: The feedback sent by the alternate paths are analyzed to detect the black hole & this information is propagated throughout the network, leading to the revocation of the Black Holes certificates.

5.CONCLUSION AND FUTURE WORK

In this paper we have presented a feasible solution to detect 2 types of malicious nodes(Black/Gray Hole) in the ad hoc network. The proposed solution can be applied to identify and remove any number of Black Hole or Gray Hole Nodes in a MANET and discover a secure path from source to destination by avoiding the above two types of malicious nodes.

As future work we intend to -

1. Develop simulations to analyze the performance of the proposed solution.

2. Study the effects of false feedback.

6.REFERENCES

[1] "Security Issues in Mobile Ad Hoc Networks- A Survey" Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.

[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.

[3] Sanjay Ramaswamy, Huirong 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.

[4] 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

[5] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black 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.

[6] Sudath Indrasinghe, Rubem Pereira, John Haggerty,"Conflict Free Address Allocation Mechanism for Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)

[7] Mansoor Mohsin and Ravi Prakash,"IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson, TX Kaixin Xu, Xiaoyan Hong, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095 project under contract N00014-01-C-0016