Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.466 – 473

RESEARCH ARTICLE

Detection of Black Hole & Gray Hole in MANET

Vandna Dahiya
PG Research Student (CSE)
PDM College of Engg, for Women
Bahadurgarh (Haryana)
vandnadahiya2010@gmail.com

Ajay Dureja
Assistant Professor (CSE)
PDM College of Engg, for Women
Bahadurgarh (Haryana)
ajaydureja@gmail.com

ABSTRACT: A Mobile Ad hoc system (MANET) includes a group of communicating cellular mobile nodes or equipment which do not contain any form of fixed system or centralized authority. The protection in MANET has become a considerable as well as involved issue inside the research community. This is because of higher desire in spreading online streaming videos as well as audio tracks in a variety of software, a single MANET may be installed rapidly in order to improve communications in an aggressive environment such as battleground or perhaps disaster situation likes problems in recovery procedure. Despite the countless attacks targeted at specified nodes in MANET that have recently been revealed, many attacks regarding numerous nodes even get small focus. A good reason regarding it is because individuals make usage of protection systems appropriate to wired networks in MANET and ignore the security steps which apply at MANET. Moreover, it might also need to do with the fact that no survey or taxonomy has been completed in order to make clear the qualities of several multiple node attacks. This paper covers the above mentioned gap by giving an appropriate meaning as well as categorization of collective attacks towards MANET through the variety of multiple node attacks found.

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) [1] is one kind of new wireless network structures. Unlike devices in traditional Wireless LAN solutions, all nodes are movable and the topology of the network is changing dynamically in an Ad Hoc Network, which brings great challenges to the security of Ad Hoc Networks. As a result, attackers can take advantage of detecting routing protocols to carry out various attacks [2] [3]. Black hole attack and gray hole attacks [4] are the two classical attacks under Ad Hoc networks, which could disturb routing protocol and bring about enormous damage to the network's topology.

This Mobile Ad-hoc Networks (MANETs) differ from existing networks by the fact that they depend on no fixed infrastructure. Nodes forming the network perform all functionality of the network with each node performs the functionality of both host and router.

Fig.1.1 A typical MANET

A MANET is introduced as an infrastructure less network simply because their mobile nodes in the network dynamically established routes along with them to transmit packets on a temporary basis. As a result of multi-hop routing and open working environment, MANETs are vulnerable and open to attacks by greedy or malicious nodes, these types of packet dropping (black-hole) attacks and exclusive forwarding (gray-hole) attacks. Yet another feature of a MANET is, moderate bandwidth, limited battery power. This attribute makes routing in a MANET an additionally more complicated task. Currently, several effective routing protocols have been projected. These types of protocols can be categorized into two classes: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc On Demand Distance Vector (AODV) protocol [5]

This specific paper, recommend a fresh strategy to recognize black hole and grey hole attacks by altering threshold in accordance to the network's excess . We regulate a cross layer technique to enhance the overall performance of our detection. Whereas the method recommended in this paper applies to mostly Ad Hoc protocols, we will totally focus our consideration upon overall performance evaluation of various attacks concurrently making use of numerous possible collaboration of attacks in MANET in network layer and IEEE 802.11 protocol in MAC layer.

2. RELATED WORKS

Deng et. Al. [6] has recommended an algorithm in order to minimize black hole attacks in ad hoc networks. Based on to their algorithm, any kind of node on obtaining a RREP packet, cross examinations using the next hop on the route to the desired destination coming from a different path. If the next hop choose to doesn't come a link to the node that delivered the actual RREP or possibly doesn't come a route to the desired destination then this node that sent the RREP is viewed as malicious. This particular strategy is not effective when the malicious nodes collaborate with each other.

S.Ramaswamy et. al. [7] introduced an algorithm to preclude the cooperative black hole attacks in ad hoc network. This algorithm is dependent holding a faith commitment regarding the nodes, so because of this it can't deal with gray hole attacks. Besides due to the fact intensive cross checking, the algorithm requires extra time in order to complete, even though the network is not under attack.

S.Banerjee et. al. [8] has also projected an algorithm for discovery & elimination of Black/Gray Holes. In accordance with their algorithm on the other hand of transmitting the entire data traffic at one time, they break down it into moderate sized blocks, in the desire that the malicious nodes can be recognized& eliminated in the middle of transmission. Stream of traffic is evaluated and monitored by the neighbours of each and every single node. Source node makes use of the acknowledgment delivered by the destination to examine for the data loss & in turn examines the opportunity of a black hole. Nonetheless in this mechanism mendacious positive

aspects could happen along with the algorithm may report that a node is behaving inappropriately, when in fact it is not.

In the end P.Agarwal et. al. [9] have projected an approach concerning implementing a backbone network of intense nodes. Together with the help of the central source network of intense nodes, source and destination nodes possess out an end to end verifying to discover in case any type of data packets arrived at the destination. If verifying produces a failure, then the anchor network leads to a protocol for detection the malicious nodes.

We have used this principle of backbone nodes & organized an algorithm that is much simpler. We have also made use of the principle of state full method of IP addresses assignation in ad-hoc networks as talked about by S.Indrasinghe et. al.[10] and Mansoor Mohsin et. al.[11]

A. Black and Gray hole attack

Black hole attack interrupts along with the routing protocol by confusing many other nodes regarding course-plotting information. A black hole node does work through the following pyramid scheme: as soon as obtaining RREQ and RREP messages, the assailant responses RREP messages exclusively and also claims that it is the getaway node. The source node is most likely to acquire a pseudo-RREP coming from the assailant just before the real RREP comes back. Underneath these types of ailments, this source node transmits info packets to the black hole as an alternative of the destination node. When the source node sends data packets by using the black hole, the assailant discards all of them without sending back a RERR message. As for gray hole, its exercises are like a black hole. A gray hole does not shed all the data packets except just simply part of packets. The Gray Magnitude is described once the proportion of the packets which are maliciously dumped by an assailant. For instance, a gray hole is gray magnitude of 60% will likely shed a data packet with a possibility of 60% and a classical black hole has a gray magnitude of 100%.

The black and gray hole attack [12] will bring great damage to the performance of Ad Hoc network. The malicious drop rate is defined by the ratio of dropped packet number and received packet number. Especially, the malicious drop rate of a black hole is 100%.

3. NETWORK MODEL AND ASSUMPTION

We tackle this issue through picking out a few nodes which have been reliable and also powerful in regards to power supply and also range. These types of nodes which might be labelled as Back Bone Nodes (BBN) will form a Back Bone network and has unique features in contrast to regular nodes. For any coordination involving the Back Bone Nodes (BBN) and the Normal Nodes, it is believed that this network is divided into a number of grids. It is presumed that the nodes, when primarily comes into the network is proficient of locating their particular grid locations.

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

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

- Stateless approach
- State full approach

In the stateless strategy an unconfigured coordinator should generate its individual IP address by self-appointment. This particular stateless method implements hit-or-miss address appointment and it is followed

closely by replicated address detection procedure to succeed in address originality. Stateless methods do not remember to keep any sort of allocation table

In the statefull strategy an unconfigured host demands its actual neighbor MANET to the job as being proxies to acquire an ip address. We possess designed a fresh form of state-full approach viz. Core Maintenance of the Allocation Table.

3.2Core Maintenance of the Allocation Table :-

In this method precisely the backbone network in MANET is authorized to choose the IP addresses for unconfigured hosts. The procedure is dependent on assigning a clash free address to all newly arrived nodes by using a variety of disjoint address spaces[6]. Each BBN in MANET is responsible for with regard to assigning a range of addresses disjoint from the ranges of all other BBN. In other words each BBN produces numbers that are distinctive for that host. Each and every hosts in the MANET must have the probability to get to one of the Backbone Nodes (BBN) all the time.

4. METHODOLOGY AND 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 i.e., 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. of the Back Bone Nodes(time is known only to the BBN.

4.1 Detection and removal of Black / Gray holes

In the beginning while the source node desires to produce a data transmission, it demands that the most nearby BBN for any restricted IP (RIP). The BBN on acquiring the RIP responses towards the source node with one of the untouched IP addresses preferred at random out from the pool of rarely used IP addresses. The source node sends the RREQ for both the desired destination and the RIP concurrently.

Now if the Source Node (SN) gets the RREP only for the desired destination node(which could be the normal case) and not the RIP, then the native network space is totally free from any sort of the black holes and at this time free from any gray holes too. The source node reuses the RIP for a particular duration for even more data transmissions. Until that period of time the BBN does not delegate 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 at the beginning notifies the neighbours of the node from which it got the RREP to RIP, to enter in to promiscuous form, to make sure they pay attention not simply to the actual packet bound to them, but likewise to the packet bound to the defined Destination node. Now the SN sends a small number of artificial data packets to the destination, while the neighbouring nodes start off keeping track of the packet flow. These kinds of neighboring nodes further send out the monitor message to the next hop of the artificial data packet & so on. At a point when the monitoring nodes finds out that the artificial data packet loss is way more than the standard anticipated loss in a network, it informs the SN about this particular Intermediate Node(IN). This time with regards to the critical 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.

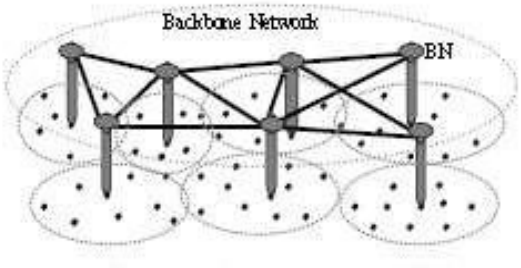

Figure 4.1. Pictorial Representation of an Ad hoc network with a back bone network.

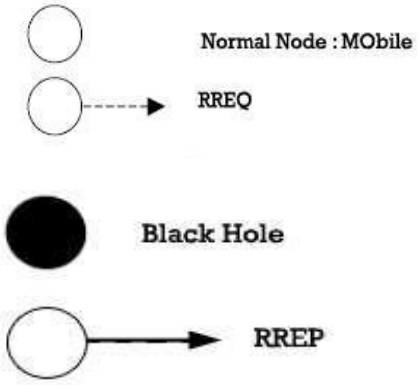

Figure 4.2. Nodes and their representation

RREQ - Route Request packet
RREP – Route Response packet

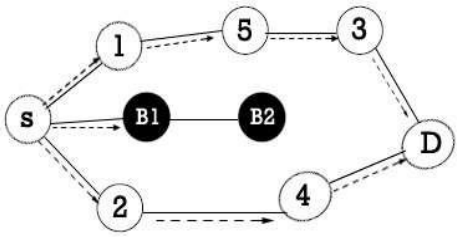

Figure 4.3. Propagation of RREQ message

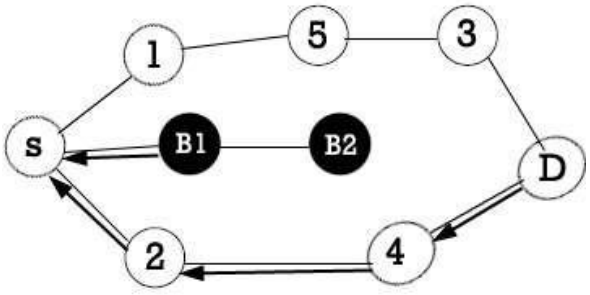

Figure 4.4. Propagation of RREP

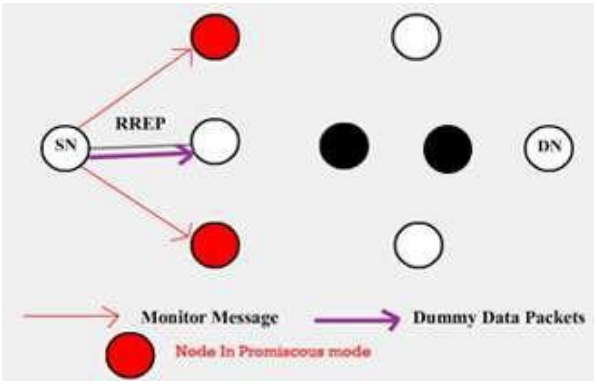

Figure 4.5. Propagation of Monitor message & dummy data packets

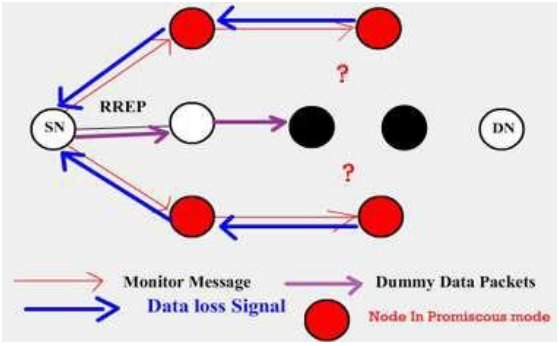

Figure 4.6. Identification of the Black Hole by promiscous nodes

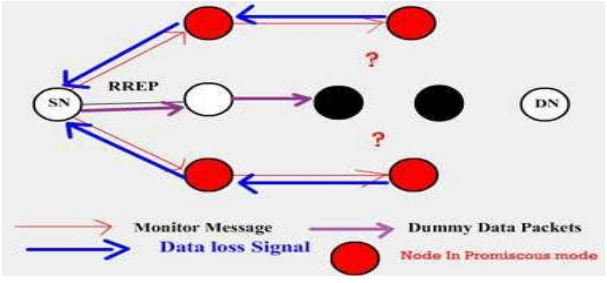

Figure 4.7. Propagation of Data loss Signal back to the Source Node

4.2 Algorithm

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 accepted only if to all the Destination & not to the Restricted IP(RIP), the connection follow through the standard operation by sending the data through the route.

Step 2: If the RREP is accepted for the RIP, it sets off the entire process of black hole discovery, by sending a inquire about to penetrate into promiscuous mode, to the nodes in an alternating path(i.e. neighbours of next hop for RIP).

Step 3: The suggestions transmitted by the alternating paths are investigated to discover the black hole & this critical information is spread through the entire network, leading to the annulment of the Black Holes certificates.

5. CONCLUSION AND FUTURE WORK

In this paper we have brought to you a possible way to identify 2 varieties of malicious nodes(Black/Gray Hole) in the ad hoc network. The suggested remedy can be applied to identify and remove any number of Black Hole or Gray Hole Nodes in a MANET and discover a assured path from source to destination by avoiding the above two types of malicious nodes.

As future work we intend to -

1. Establish simulations to evaluate the overall performance of the projected solution.
2. Examine the consequences of false feedback

REFERENCES

[1] Ajiwen CAI,Ping YI,Jialin CHEN,Zhiyang WANG,Ning LIU;An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network;2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[2] IETF MANET work group. http://www.ietf.org/dyn/wg/charter/manetcharter.html

[3] L.D Zhou;Z.J. Hans, Securing Ad Hoc Networks[j], IEEE Network, 13(6),1999.

[4] Y.C. Hu; A Perrig, A Survey of Secure Wireless AdHoc Routing[J],IEEE Security and Privacy,2(3),28-39,May 2004.
[5] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc Ondemand. Distance Vector (AODV) Routing," IETF RFC
[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.
[7] 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.
[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 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.
[10] 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)
[11] 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
[12] D.B. Johnson; D.A. Maltz; J. Broch; "DSR: The dynamic source routing protocol for multiple wireless ad hoc networks". In: Perkins C, Ed, Ad Hoc Networking. Addison-Wesley, 2001. 139- 172

