Detection of Black Hole using Time Difference and Neighborhood nodes

[1]K.Lalramhluni, [2]Aditya Bakshi
[1]Student of Lovely Professional University
[2]Assistant Professor

Abstract

A mobile adhoc network is an adhoc network which means that computer can connect or communicate each other without the need of wires and cables i.e, it is wireless. The device has the capability to move freely. The node would be laptop, mobile phone, personal digital assistance, MP3 and personal computer. The nodes can act as a router or host that means they can be deployed urgently without the need of infrastructure. A blackhole doesn't send the packets to destination instead a blackhole nodes forge a routing message, the sequence number and hop counts to forcibly acquire the route and then further drops the packets. The proposed algorithm is to find the blackhole route using threshold and blackhole nodes using neighbor nodes. The proposed algorithm is very efficient in finding all the malicious route and further the malicious nodes in that detected route.

Keywords: MANET, AODV, Black hole attack, Wireless, Threshold, Malicious route, Malicious Node.

1. INTRODUCTION

There are two sorts of communication: wired and wireless. Wired networks are communication with the need of wires and cables. Wireless networks are communication without the need of wires and cables. In wireless the objective must lie within the ratio range of each other. The transmission of data in wireless sensor network is done using electromagnetic waves. Wireless are well known for its simplicity and cost sparing.

1.1 MANET

Mobile adhoc networks comes under wireless networks. The nodes are moved freely. Wireless networks are easy to install than wired networks. There can be thousands of client connecting to each other. Manet are independent and decentralized wireless system. Nodes are free to move in and out of the network. Nodes maybe laptop, mobile phones, personal digital assistance, MP3 player, and personal computer. Nodes can act as host or router or both.

1.2 AODV

AODV initiates route discovery process routes only when there is any need to find node. In Route Discovery Process of AODV there are types of messages: Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages. RREQ- whenever a node obliges a route to the node, it transmits the route request message. A time to live (TTL) value is carried by every route request which states the number of hops it has to be forwarded for. This value is first initialized at a predefined value at first transmission and afterwards it goes on incrementing at retransmissions. Retransmissions occur when there is no reply. Every node is supposed to maintain two counters: node sequence number and broadcast id. RREP- a route reply message isunicast to the originator of the RREQ if the receiver is either the node using the requested address or is having a valid route to the requested address. RRER- nodes keep on monitoring the link status of the next hop in the active routes. Whenever a link breakage is detected in the active route, a RERR message is broadcasted to the other nodes to notify about the loss of the link.

1.1 BLACKHOLE ATTACK

A Black Hole attack scrambles the route by forging a routing message, and then, further either eavesdrops or drop the packets, posing a possible threat to safety properties. A Black Hole attack forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all data packets that pass. A malicious nodeimpersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery.

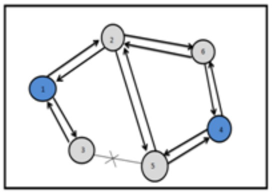


Fig 1:Black Hole Attack

In figure 1, Node 1 is source node whereas node 4 is destination node. Source node broadcasts route request packet (RREQ) to find a route to destinationnode with the normal intermediate nodes receiving and continuously broadcasting the RREQ, except the Black Hole node. Everything works well if the RREP from anormal node reaches the source node first. Here node 3 is attacker and acts as black hole. Node 3 sends a route replypacket(RREP) to the source node. But a route reply from node 3 reaches to source node before any other intermediate node. This makes the source node to conclude that the route discovery process is complete, ignoring all other RREPs and beginning to send data packets.The Black Hole node would directly send a route reply (RREP) to the source node S, with an extremely large sequence number and hop count of 1.1. The destination node D would also select a route with a minimum hop count uponreceiving RREQs from normal nodes, and send a RREP packet. In this case source node sends the data packet to destination node through node 3. But as the property of black hole node that this node does not forward data packets further and dropped it. But source node is not aware of it and continues to send packet to the node 3. In this way the data, which has to be reached to the destination, fails to reach there. There is no way to find out such kind of attack. These nodes can be in large number in a single MANET, which makes the situation more critical.

2. LITERATURE SURVEY

Author Neetika Bhardwaj and Rajdeep Singh (May 2014) proposed “Detection and Avoidance of Blackhole Attack using AOMDV Protocol in Manet’s”. AOMDV is a multipath, on-demand(as soon as or whenever required), distance-vector(router inform all nodes when topology changes) mobile adhoc routing. It purges(remove) the previous sequence number when a new node is added. In AOMDV new node is added to get away from the blackhole in between. So the previous route and the route in which a new node is added are disjoint to each other. In their proposed methodology:

- Broadcast the packets.
- The destination send FINISH to sender as it has not received data from the sender through the active route.
- When the sender receives FINISH from the destination, it stop forwarding the packets by removing the current entry from the routing table and send packets packets through alternate (substitude) route present in the routing table.
- The proposed approach can detect single, multiple as well as cooperative Blackhole attacks because it exploits the basic functioning of malicious nodes.

Author Muhammad Al-Shurman and Seong Moo Yoo, Seungjin Park proposed “Black Hole Attack in Mobile Adhoc Networks”. It has two solutions. The first solution is to find more than one route to the destination. The second is to exploit the packet sequence number included in anypacket header. The next packet must have higher value than the current packet value. It uses AODV protocol to calculate the distance vector. This solution only detect a single Black Hole attack. First solution is that Sender sends RREQ broadcast. Sender pass packet only when RREP is granted.When sender receives RREP it sends the packet. Second solution is that every packet has a unique sequence number. The next packet have a higher sequence id value than the current packet. very node contains update tableto find if the packets are send or received by their sequence number.

Author Eiko Yoneki and Fehmi Ben Abdesslem proposed “Finding a Data in Bluetooth Scanning”. It finds out how many number of missed devices in an environment by using GPS and Bluetooth scanning. Bluetooth enquiry can only scan other device for 10.28 seconds. It uses GPS to find other devices around him i.e, multihop. Bluetooth range is 10 m, if there are no obstacles 20m range. It uses around you software to detect other device in the environment.

Author Fei Shi, Weijie Liu, Dongxu Jin, Jooseok, Song (Aug 2013) proposed “A cluster Based Countermeasure against Black Hole Attack in Manet”. Here they introduce a cluster based scheme. An algorithm AHP (analytic hierarchy process) is used to elect CH (clusterheads). Clusterheads not only detect blackhole but also identify blackhole nodes. The source or destination node are treated as monitor or detector for detecting BH nodes. We can elect the most suitable node to be the CH for each cluster. After locating the BH nodes the CH will spread alarm to expose the BH nodes to the whole network. Three parameters are utilize to weight each node for the election of CHs. They are: Relative stability value – the longer lifetime of clusters can be guaranteed. Connectivity value – the good connectivity used to shape communication between CH and cluster members. Credit value – packets dropping behavior by BH nodes. Proposed methodology states that, If the RREQ generated by the next-hop node of the intermediate node cannot reach the destination node, timeout which indicates that the intermediate is the blackhole node.

Author Bo Sun, Yong Guan, Jian Chen and Udo W. Pooch (2003) proposed “Detecting Black Hole attack in Mobile Adhoc Networks”. Here it uses neighborhood based method to detect Black Hole attack and Routing Recovery protocol tofind the safest path to the destination.

Route request neighbor(RRN)+RRN+RREQ+RREP

Author Payal N. Raj, Prashant B. Swadas (2009) proposed “DPRAODV: A Dynamic learning system against Black Hole Attack in AODV based Manet”. DPRAODV isolates malicious node from thenetwork. DPRAODV (Detection, Prevention and Reactive (on demand=nodes exchange routinginformation only when needed) AODV) to prevent security threats of blackhole. DPRAODV:Solution against blackhole attack can be stated that the RREP packet is accepted if it has RREP_seq_no higher than the one in routing table. Our solution does an addition check to find whether the RREP_seq_no is higher than the threshold value.As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and ALARM to its neighbors. The malicious node is isolated from the network by the ALARM packet. The continuous replies from the malicious node are blocked, which results in less Routing overhead.

Author Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur and Prashant Khurana (2013) proposed “GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs”. It means Gratuitous (give freely) AODV. Here it diverts the traffic from the Black Hole. The control packets such as CONFIRM, CHKCNFIRM and REPLYCNFIRM are used to detect the presence of Black Hole and divert all the traffic. Active attacks=malicious node can enter and modify or corrupt it. Passive attacks=the malicious node listens the traffic and remove or extracts the data from the ongoing transmissions.

Algorithm 1

Sender sends RREQ. Next node send RREP to sender. If next node is not Blackhole node it sends CONFIRM to destination. If next node has a blackhole address it drops or Discard the RREP Else If intermediate node reply that thereis a route, the sender checks the route to the destination. Else Send packets. If the intermediate node is confirmed that it is not blackhole, pass the packet to the other node Else Drop the packets. When destination receives confirmation it sends broadcast to the sender RREP. If sender receives RREP from the destination before timeout it sends the data Else Discard the packets because there is blackhole. Try the RREQ again from the beginning.

Algorithm 2

Sender sends RREQ. Next node sends RREP. If next node is not blackhole it sends RREQ to destination. If next node is blackhole sender discards the packet Else If RREP from intermediate node sender, checkconfirm route to destination. Else Route data. When intermediate receives checkconfirm and confirm it to the sender, it sends replyconfirm to the sender. If sender receiver replyconfirm, it checks its checktable and updates tables. If sender receives replyconfirm from destination with no timeout it deletes checktable and sends the packets. Else Checks all the ID from next node to intermediate node whether there is collaborative blackhole and start RREQ again from the sender.

Author Muhammad Raza and Syed Irfan Hyder (2000) proposed “A forced routing information modification model for preventing blackhole attacks in wireless ad hoc networks”.

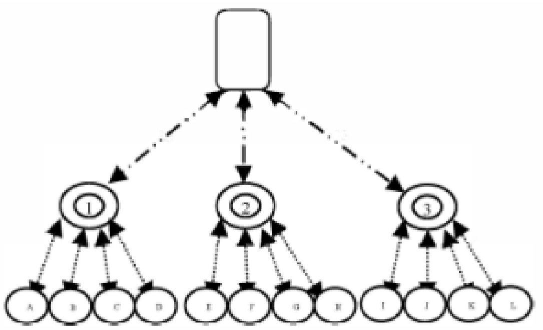


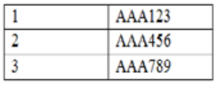
Fig 2:Model of Wireless Network

Here they routing information modification model. For communication between server and access point they used WiMax technology (IEEE 802.16 to 66 GHzrange) and for communication between access point and node they used WiFi technology (IEEE 802.11 to 2.400 GHz range). The nodes first communicate with access point and to the server. And server to access point and then to nodes.

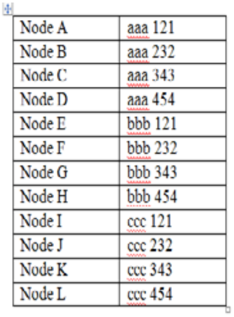
Nodes->access point->server

Server<-access point<-nodes

Its methodology states that: There is one server having 3 access point. Each access point have 4 nodes each as shown in figure 2.Server and access point are fixed and have permanent infrastructure. It uses AODV (on demand) model. Nodes can be laptop, ipod, mobile devices etc. Nodes cannot directly communicate with server because server has only WiMax capability and no WiFi capability. All the nodes are assigned a unique ID number. Mac address point and Mac address nodes is given as:



1	AAA123
2	AAA456
3	AAA789



Node A	aaa 121
Node B	aaa 232
Node C	aaa 343
Node D	aaa 454
Node E	bbb 121
Node F	bbb 232
Node G	bbb 343
Node H	bbb 454
Node I	ccc 121
Node J	ccc 232
Node K	ccc 343
Node L	ccc 454

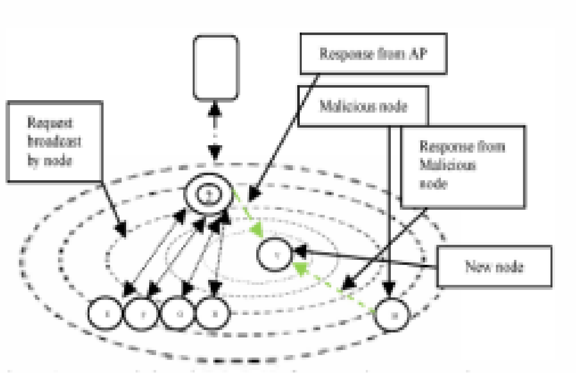


Fig 3:New Node broadcast request to access point

If another node wants to enter in the routing table say access point 1 has the nearest distance, so the node gets added in access point 1 as shown in figure 3. The access point adds Mac address and ID number of that added node say nodeN.Now if another node broadcast request.He get responses from malicious node as shown inthe figure.When the nodes gets response malicious node,the access point scans the networkwhether the node has leaved thenetwork or became a victim of the blackhole.After scanning it detects both the node and malicious node. The access point fetches MAC address from the malicious node. It listens the traffic and came to know that it is a blackhole. So the access point 2 alerts all other access point and server that there is blackhole in the network. To identify this blackhole the access point sends the MAC address of that blackhole to all other neighbors so they will notice that it is a blackhole by his MAC address. The server attack the blackhole by using access point introducing jamming such as DoS. With this the server can now force the node to divert its traffic with the help of access point.

3. PROPOSED WORK

There maybe one or two or cooperating Black Hole in the network. By using our method if we detect the path or route of the Black Hole we can easily detect the Black Hole nodes in the route. So, Packets to be send by the sender will not send to that path where there are Black Holes. The method states that, to detect the Black Hole route we calculate using Time Differences. And to detect Black Hole nodes we use the Neighborhood nodes. To calculate the distance between the nodes and route discovery the method uses AODV protocol. AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings.To discover route delivery packets we use the control packets, the RREQ, RREP and RRER. Retransmissions occur when there is no reply. If Route is having a valid route it send RREP to the requested address. Whenever a link breakage is detected in the active route, a RERR message is broadcasted to the other nodes to notify about the loss of the link. The link breakage are handled in this methodology. There will be less delay in the connection so the packet data will be delivered very fast. To stimulate using Matlab we have to do the following terms:

- Create Deployment Area
- Create Network with all Nodes
- Run Proposed Algorithm to detect black Hole Detection
- Analyze Results , calculation time and transmission period.

3.1To calculate neighbor of nodes.

Algorithm 1

Notations:

M = Total number of nodes
X_i= x-coorinate of the ith Node
Y_i= y- coorinate of the ith Node

```
Begin
For i= 1 : M
Dist() ← calculate distance
End
If dist < Range of Node
$N_x$ = M
Where, $N_x$ is adding node in neighbor set
End
End
```

3.2 To Broadcast the Route Request messages.

Algorithm 2

Notations:

N = Set of neighbor nodes
Tinitial = 0; initial time

```
Begin
2For i = 1 : M
Start clock
For j = 1 : N
Broadcast();
Node i → Node j
#Node i send route request message to Node j
End
End
```

3.3 Route Reply

Algorithm 3

Notations:

NR = Nodes which received Route Request

```
Begin
For i = 1 : NR
For j = 1 : N
If Nj == destination
#any Node has route to destination
Reply()
End
End
End
Stop time
```

3.4 Comparing Time to Replies

Algorithm 4

Notations:

TR = Set of time values taken to receive Reply
Avg Time = average value of time to reply of different path
SP = suspected path

```
Begin
For i = 1 :TR
If $TR_i$< Avg Time
Add to suspected path
SP = suspected path
End
End
```

3.5 To find the Nodes in suspected path

Algorithm 5

Notations:

SPN = Nodes in suspected path

```
Begin
For i = 1 : SPN
For j = 1 : N
If data $Received_j$< Avg DR
#If data received of jthNode is less than average value of data received
Node = BlackHole Node
End
End
End
```

4. CONCLUSION

MANET is wireless and has no network management that's why malicious node like the Black Hole node can enterinto the network to gain access trying to corrupt, modify or drop the packets send by the source to the destination. So, the main aim is to detect those Black Hole route using Time Differences and Black Hole nodes using neighborhood nodes.

5. REFERENCES

[1]Marina, M.K.; Das, S.R., "On-demand multipath distance vector routing in ad hoc networks," Network Protocols,2001. Ninth International Conference pp.14,23, 11-14 Nov. 2001.

[2]Tamilselvan L, Sankaranarayanan V, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[3]B. Sun, Y. Guan, J. Chen and U.W. Pooch, "Detecting blackhole attack in mobile ad hoc networks", Proc. 5thEuropean Personal Mobile Communications Conference, Apr. 2003, pp. 490-495.

[4]Priyanka Goyal; Vinita Parmar; Rahul Rishi,"MANET: Vulnerabilities, Challenges, Attacks, Application",International Journal of Computational Engineering and Management, vol. 11, January 2011.

[5]Nishant Sitapara; Sandeep B.Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks," International Conference" ICETE-201O" on Emerging trends in engineering on 21st Feb 2010.

[6]Samba Sesay, Zongkai Yang and Jianhua He, "A Survey on Mobile Ad Hoc Wireless Network", Information Technology Journal 3 (2): 168-175, 2004.

[7]Muhammad AI-Shurman, Seong-Moo Yoo and Seungjin Park, Black Hole Attack in Mobile Ad Hoc Network, , Huntsville, AL, USA, April 2-3, 2004.

[8]T. Nicolai, E. Yoneki, N. Behrens, and H. Kenn. Exploring social context with the wireless rope. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 874–883. Springer, Nov. 2006.

[9]Al-Shurman, M., Yoo, S. and Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[10]C Perkins, E Belding-Royer and S Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", Internet RFCs Volume: 1, Issue: 3561.

[11]Bhalaji,N.; Kanakeri, A.V.; Chaitanya, K.P.; Shanmugam, A.:Trust based strategy to resist collaborative blackhole attack inMANET. Int. J. Inf. Process. Manag. 70, 465–474 (2010).

[12]Djenouri, D.; Badache, N.: A gradual solution to detect selfish nodes in mobile ad hoc networks. Int. J. Wirel. Mob. Comput. 4, 264–274 (2010).

[13] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.

[14]Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[15]Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007.

[16]Hu Y, Perrig A, Johnson DB (2002) Ariadne: a secure on-demand routing protocol for ad hoc networks. In: Proc of ACM Mobicom, pp 12–23.

[17]Karlof C,Wagner D (2003) Secure routing in wireless sensor networks: attacks and countermeasures.

In: First IEEE international workshop on sensor network protocols and applications (SNPA 03), May
2003, pp 113–127.

[18]Yu, W., & Ray, K. (2005). Defence against injecting traffic attackin cooperative ad hoc networks. In IEEE global telecommunicationconference Globecom.