International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-4)

Research Article | **April 2015**

Survey on Detection of Gray Hole and Black Hole in Mobile Ad-Hoc Network

Sushma B. Akhade
Department of CSE ,TPCT, COE,
Osmanabad, India

Prof. Dr. S. M Jagade
TPCT, COE, Osmanabad, Dr..BAMU,
Aurangabad, India

***Abstract*—**

Mobile Ad-hoc N/w is a network in which different mobile nodes or devices are present and they wants to communicate with each other using shared wireless medium. In this network all nodes are having their own communication range. During communication each nodes acts as router to forward packets to another node. In MANET there is no centralised administration. So, there is high possibility of different types of attacks on network. Gray Hole attack and Black hole attack are such attacks. In this Gray hole and Black Hole are the malicious nodes which forward wrong information about communication route. So for good communication it is very important to keep communication rout free from these type of attacks many people have worked on this. In this paper different ideas of different peoples are provided to detect Gray Hole and Black Hole attacks.

***Keywords*— MANET , Gray Hole, Black Hole, AODV, DSR.**

I. INTRODUCTION

In mobile Ad-Hoc network all mobile devices are present without any fixed N/w infrastructure & without centralised administration all the nodes are movable so network topologies can change dynamically each node has limited communication range. At the time of communication each device acts as router that forwards the data to the next node. It is very important to find & select suitable and nearest device as next node for data transmission. In this way data is transferred from node to node up to its destination routes are discovered as needed I.e. it is on demand. Basically this is the job of routing protocols, so for selection of effective, suitable, adaptive and robust routing protocol is important each node present in the network participates in routing protocol to find path between sources to destination. Routing relies on trust relationship among participating devices. Main routing responsibilities are exchanging routing information, finding feasible path between source & destination, path maintenance.[1]

Each node present in network maintains routing table. Each routing table entry consists of following information

-Destination
-Next node
-No. Of nodes
-Sequence no. For destination
-Active nodes for this route .
- Expiration time for route table entry [2]

There is some time period for each route entry called as timeout; it is set to current time plus active rout timeout. If new route is offered for communication then mobile nodes compare the destination sequence number of new route with destination sequence number of current route and the route having greater sequence number is selected for communication the main goal of routing protocol is to make secure communication. Depending upon routing information update mechanism routing protocols in Ad-Hoc network can be classified as

1. Proactive protocols
2. Reactive protocols
3. Hybrid protocols

Proactive protocol –

In this type of protocol all the nodes present in network shares the routing information with each other periodically, because of this consistent and accurate routing information is always updated. In this path is computed rapidly only when source want to communicate with destination. This path formation is based on the updated information in routing table.

Example – Destination sequence distance vector (DSDV), wireless routing protocol (WRP), Optimized link state routing (OLSR). It has a disadvantage that, high overhead needed to maintain up to date routing information.

Reactive Protocol-

In this type of protocol when source does not know the path between Source and destination only at that time rout discovery mechanism is initiated. In mobile Ad-Hoc network (MANET) performance of reactive protocol is better than proactive protocols and it needs lower overhead than proactive routing protocol.

Example – Ad-Hoc on demand distance vector (AODV), Dynamic source routing (DSR), temporally ordered etc. [3]

II. WORKING OF AODV PROTOCOL

When source wants to communicate with destination source broadcast a Route Request packet to all its neighbours this packet consists of sequence number generated by source node if any of neighbour s not having direct path to destination then they will again retransmit this Rout Request packet to its neighbours ,So there is possibility of loop formation &retransmission of same packet to same node .

To avoid this, intermediate node checks the sequence number of packets. if the packet is not duplicate then only it add its own identifier in sequence number & then forward the packet the destination node when receives the Rout Request packet then it sends back rout reply packet with higher sequence number along the reverse route which is followed by Rout Request packet. When source receives Rout Reply packet at that time source can send data to destination. Next important thing is maintenance of route. If a node detects any failure then it sends Route Error message to source [4]

Following figure will explain the working of AODV with example

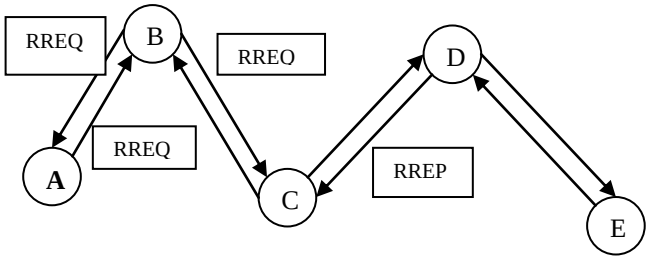

Fig.1 working of AODV Protocol.

There are 5 nodes present in MANET A, B, C, D, E. as shown in figure. Circle shows the limited communication range of each node. Node B wants to communicate with node E then B will broadcast RREQ to all its neighbours i.e. A & C. Now node A does not have direct path to destination, so it rebroadcast RREQ to its neighbour. It is received by B itself & discards it. On the other hand node C is there if it has greater sequence number than RREQ then it discards RREQ and replies with RREP having higher sequence number if not then it update sequence number in routing table and reforward RREQ packet to node D. Now node D has path to node E so it send back RREP packet with greater sequence number and the path B->C->D->E is selected for communication.

Now suppose there is a node which forwards wrong routing information in network then route discovery Process is difficult as shown in following example.

In figure S node is source and E is destination. Node S broadcast the RREQ packet to node A and B .they don't have path to destination so B retransmit RREQ to Node D. Node A retransmit RREQ to node C. Now node D has the path to destination so it sent back RREP packet with higher sequence number indicating that i have path to destination. On the other hand node C is a malicious node which sends wrong routing information it does not have path to destination then also it replies to node A with fabricated higher sequence number indicating that I have path to destination but actually this is wrong information. Now source node observe that RREP coming from node C is having greater sequence number than RREP coming from Node D so it will select path which goes through node C. During data transfer this malicious node can drop some or all data or can alter data which causes problem in network operation this is nothing but security attacks

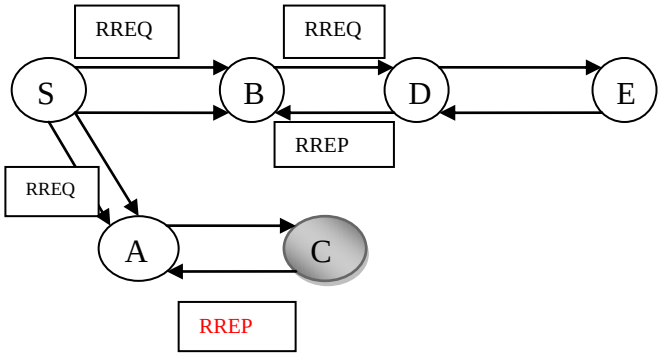

Fig.2 working of AODV Protocol in presence of malicious node.

There can be two kinds of attacks

1. Passive attack
2. Active attack

1. Passive attack –

This type of attack does not disturb the network operation. In this the aim of attacker is only obtain the information being transmitted without making any changes in that message so it will violate the message confidentiality detection of these type of attacks is difficult. Powerful encryption mechanism can avoid these types of attacks

2. Active attacks -

This type of attack badly affect on network operation . In this attacker node creates attack by making changes in data packet or by dropping data packets or by adding some wrong data in packet. Gray Hole and Black Hole attacks are active attack. [5]

III. LITERATURE REVIEW

1. Rutvik Jhaveri, Sankita Patel and Devesh Jinwala proposed a fantastic method for detection of gray hole. This method finds the gray hole during the route discovery process. For this they have used the sequence no with the RREP packet. It compares the sequence no. with the sequence no. in the routing table. If it is greater than one in RREP, then packet is accepted. As it works during route discovery process, there is no or less chance of losing data. This comes as a great advantage for secure transmission of data in MANET, which is highly susceptible for different types of attack [6].

2. A mechanism is proposed by Sukla et. al in which before sending any block, source sends a prelude message to destination to make it aware about communication; neighbors monitor flow of traffic; after end of transmission, destination sends postlude message containing the number of received packets. If the data loss is very large , the process of detecting and removing all malicious nodes is initiated by collecting response from monitoring nodes and the network. In this mechanism the routing overhead is increased because of additional routing packets. [7]

3. The mechanism proposed by Onkar Chandure and V.T.Gaikwad involves recognition & eradication technique to identify any malicious gray hole node in the network. It focuses on effect of gray hole attack in mobile ad hoc network and its outcomes. [8].

4. A trust-based approach is proposed by Arshad et. that uses passive acknowledgement as it is simplest; it uses promiscuous mode to observe the channel that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for. Thus, a node can make sure that packets it has sent to the neighboring node for forwarding are indeed forwarded. The process of routing is decided based on two parameters: trust and hop-count; therefore, it gives routing path which is shortest and trusted . Though, monitoring overall traffic would have been a better choice instead of monitoring one node's request.[9]

5. An approach is discussed by Latha et. al [12] in which the requesting node waits for a specific time for replies from neighbors. That reply is consisting of the next hop details. After the specific time, it will get the reply then it will check Route Reply Table to know whether there is any repeated node or not. Existence of repeated node in the reply paths indicates the truthful paths or limited chance of malicious paths..so in this mechanism the main thing is to find repeated next hop node , and this process increases Overhead. [10]

6. The method proposed by Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU is based on a cross layer design to detect the Gray hole attack. In network layer, they have proposed a path-based method to overhear the next hop's action and a collision rate reporting system is established in MAC layer to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload [11].

7. Onkar Chandure and V. T. Gaikwad proposed a method which is finding out the gray hole using route discovery process. It works on AODV protocol. Here different metrics are used to check the performance namely, Packet delivery ratio, End to end delay, Packet loss ratio. With the help of these metrics we can analyze the performance of network [12].

8. The method proposed by Disha Kariya, Atul Kathole, Sapana Heda works on cross layer design. They have used course based detection method for detection of gray hole. Here node does not observe every node in neighbor, only observes next hop in the current path. Because of this work of every node is reduce, it only have to concentrate on the behavior of next hop in the current path [13].

9. The scheme proposed by Jaydip Sen, M.Girish Chandra,Harihara, Harish reddy, Balmurlidhar consists of four security procedures which are invoked sequentially. In the first procedure Neighborhood Data Collection Module, each node in network collects the data forwarding information in its neighborhood and store it in table called as Data Routing information table. The second procedure Local anomaly detection module invoked by a node when it identifies a suspicious node by examining its DRI table. The third procedure Cooperative anomaly detection module is used to increase the detection reliability by reducing the probability of false detection of local anomaly detection procedure. The fourth procedure Global alarm raising module is invoked to establish a network wide notification system for sending alarm messages to all the nodes in the network about the gray hole node(s) that has been detected by the cooperative anomaly detection algorithm. It also ensures that the identified malicious node(s) is isolated so that it cannot use any network resources [14].

TABLE I SUMMARY TABLE

Sr.no	Title	Publication	Authors	Facts
1	MANET Routing Protocols and Wormhole Attack against AODV	International Journal of Computer Science and Network Security, vol. 10 No. 4, 2010	Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah	Method is developed for detection of gray hole this method works during path finding process it uses sequence no. with each packet And by comparing these sequence no. It can find malicious nodes

2	Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks	World Congress on Engineering and Computer Science 2008	Sukla Banerjee	The method is developed which first find the packet forwarding misbehaviour of network and then develop the mechanism to find & to discard the malicious nodes. This method can find the sequence of malicious nodes.
3	A Mechanism for Recognition & Eradiction of Gray Hole Attack Using AODV routing protocol in MANET	(IJCSIT) International Journal of Computer Science and Information Technologies 2011	Onkar V. Chandure, Prof.V.T.Gaikwad,	In this misbehaviour of malicious nodes can be detected on the basis of routing protocols. Like AODV
4	An Outlook on the Impact of Trust Models on Routing in Mobile Ad Hoc Networks (MANETs)	Warwick Computer Science Repository 20 Oct 2010	Arshad Jhumka, Nathan Gri_ths, Anthony Dawson and Richard Myers	The concept of trusted routing is developed to handle the problem created because of selfish and malicious nodes. It is shown that trust model helps in achieving the efficiency in MANET in presence of malicious nodes in network.
5	Prevention of Co-operative Black Hole Attack in MANET	JOURNAL OF NETWORKS, VOL. 3, NO. 5 , MAY 2008	Latha Tamilselvan and Dr. V Sankaranarayanan	The different method is developed in which it uses fidelity level & that is the measure of reliability of that node. Fidelity level of node is checked, when it falls to 0 then that node is considered as malicious node.
6	An Adaptive approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network	24th IEEE International conference on Advanced Information Networking and Applications 2010	Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU	The adaptive mechanism is presented to detect black and gray holes it is based on cross layer design.
7	Detection & prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol	International Journal of Computer Applications(0975-8887) 2012	Onkar V. Chandure, V.T.Gaikwad	In this basic idea is given to implement AODV protocol. And mechanism to detect gray hole and black hole is based on the PDR & e2e values
8	Detecting Black and Gray hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method	International Journal of Emerging Technology and Advanced Engineering 2012	Disha G. Kariya, Atul B. Kathole, Sapna R. Heda	Adaptive mechanism is developed .it is based on cross layer design. Course based method is developed of detection of malicious nodes.
9	A Mechanism for Detection of Gray HoleAttack in Mobile Ad Hoc	IEEE, ICICS	Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P.	In this mechanism used to detect malicious nodes is effective and efficient. The detection rate is high and low false positive rate.

	Networks	2007	Balamuralidhar	

IV. CONCLUSIONS

Gray hole and black hole attacks disturb the working of network. Because of them data communication between source and destination can not done securely. These attacks drop some data packets or all the data packets. Which is harmful for network In this paper we are over viewing techniques which are used in detection and removal of gray hole and black hole. This paper will provide the person who reads with the groundwork for research in detection of gray hole and black hole attacks.

REFERENCES

[1] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala,"A Novel Approach for GrayHole and Blackhole Attacks in Mobile Ad-hoc Networks", Second International Conference on Advance Computing & Communication Technologies,2012, pp. 556-560

[2] Charles E_ Perkins , Elizabeth M_ Royer "Ad_hoc On_Demand Distance Vector Routing" Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on

[3] Dr.S.S.Dhenakaran, A.Parvathavarthini "An Overview of Routing Protocols in Mobile Ad -Hoc Network" International Journal of Advanced Research in Computer Science and Software Engineering © 2013.

[4] Elizabeth M. Royer , Charles E. Perkins "An Implementation Study of the AODV Routing Protocol" , Wireless Communications and Networking Confernce, 2000. WCNC. ,2000 IEEE (Volume:3)

[5] Mahendra Kumar , Ajy Bhushan, Amit Kumar , "A Study of wireless Ad -Hoc Network attack and Routing Protocol attack" Volume 2, Issue 4 , April 2012

[6] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah "MANET Routing Protocols and Wormhole Attack against AODV "IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[7] Sukla Banarjee,"Detection/Removal of Cooperative Black and Gray Hole Attack in mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and

[8] Onkar V. Chandure, Prof.V.T.Gaikwad,"A Mechanism for Recognition & Eradiction of Gray Hole Attack Using AODV routing protocol in MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2(6), 2011, pp.2607-2613

[9] Arshad Jhumka, Nathan Gri_ths, Anthony Dawson and Richard Myers "An Outlook on the Impact of Trust Models on Routing in Mobile Ad Hoc Networks (MANETs)"

[10] Latha Tamilselvan and Dr. V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5 , MAY 2008

[11] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network" , 24th IEEE International conference on Advanced Information Networking and Applications,2010, pp. 775-780

[12] Onkar V. Chandure, V.T.Gaikwad,"Detection & prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International Journal of Computer Applications(0975-8887) Volume 41-No.5, March 2012, pp.27-32

[13] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda,"Detecting Black and Gray hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method", 2012(ISSN 2250-2459, Volume 2, Issue 1), January 2012, pp. 37-41

[14] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar,"A Mechanism for Detection of Gray HoleAttack in Mobile Ad Hoc Networks ", 2007 2007

