A Survey on Techniques of Identifying Black Hole in MANET

Renuka[1], Sandeep Tayal[2]
[1]Mtech, Student, [2]Associate Proffesor
Department of Electronics and Communication.
Vaish College Of Engineering, Rohtak, Haryana, India.

ABSTRACT:

MANET stands for mobile ad-hoc network where group of mobile nodes can move freely and communicate with each other. These nodes are not bound to fixed infrastructure. Hence are vulnerable to attacks and one such common attack is black hole attack. Black hole attack is an attack where one malicious node tries to disguise itself in having address and shortest path to any destination. And as the source transmits its data to this node it grabs all the data and do not send it further to the destination and as a result disrupt the communication. In this paper we have surveyed many mitigation methods to detect and prevent black hole attack and all used AODV protocol.

KEYWORDS:

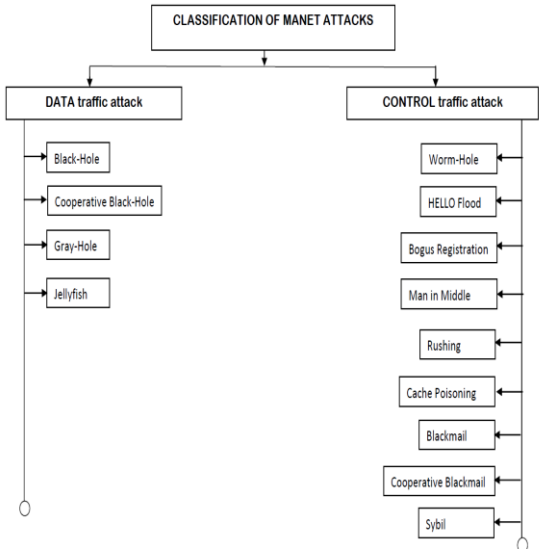
MANET, AODV routing protocol, Black hole attack

INTRODUCTION:

MANET is an infrastructure less network where all nodes are connected wirelessly. Since it is prone to errors and miscommunication due to its infrastructure less nature thus some routing protocols are designed to avoid any attack. There are three types of routing protocols namely: Proactive protocol, reactive protocol and Hybrid Protocol. **Proactive Routing Protocol** uses pre establish path and has to maintain all the routing information in the table. In **Reactive routing Protocol** the path is established when needed thus it is also called **Demand Routing Protocol.** One common such protocol is AODV (Ad-hoc on demand Distance Vector) protocol. **Hybrid Protocol** is the combination of the two. [1][2]. We normally be using AODV protocol where RREQ (route request) is sent by source node to destination node which in reply send RREP (route reply) and then the path will be established and data is transmitted. If the next node is not the destination node then the node will further pass on the RREQ to other nodes in the network and in this way the route is established. An example of mobile ad hoc network is as shown:

Fig-1 Mobile ad-hoc network example

This MANET is prone to many attacks like gray hole attack, wormhole attack, Sybil attack, jelly fish attack, man in middle attack and many more. One most prominent attack is black hole attack. Other attacks in MANET are as shown:



Print-ISSN: 2319-9512 e-ISSN: 2319-9520

BLACK HOLE ATTACK:

Attacks can be classified as passive attacks and active attacks. In passive attack the attacker tries to listen to the valuable information. In active attack the attacker tries to modify and delete the information. [10-2012]. Black hole attack is one such active attack where the malicious node act as innocent node and absorbs all the data and do not forward it to the required destination though it disguise itself as it has the path to the destination though it may not have it. It is active in transport layer of OSI model. And the common protocol used is AODV protocol.

AODV PROTOCOL

This protocol works in two phases: Route discovery phase and route maintenance phase.

(1) **Route Discovery Phase:** In it source node creates a RREQ packet and broadcasts it in the network. That network consists of black hole node as well. Following information is contained in RREQ packet :

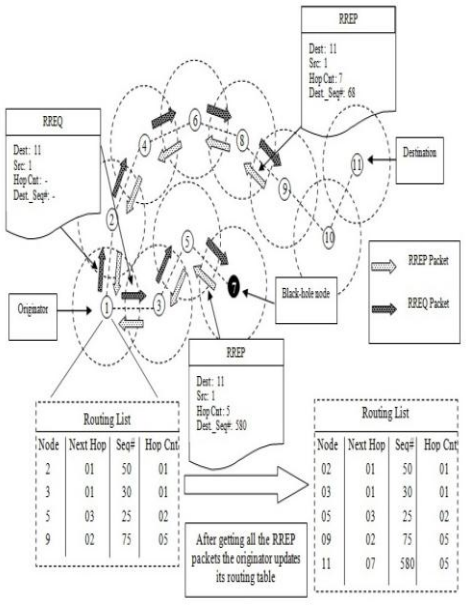
Destination IP	Destination Sequence Number	Originator IP	Originator Sequence Number

Each originator node maintains a monotonically increasing integer value called Sequence Number. The freshness of the information contained in the packet is represented by this sequence number only. This is that particular number which malicious node send to the sender with very high value to indicate the fresh route.The source node when receives that RREQ packet it selects that route for having high Sequence Number which is actually contained the malicious node in the path. Then the sender node starts to send packets through that path. On receipt of the packets the malicious node starts to drop the packets without forwarding it to the destination. Hence as a result data is lost.

(2) **Route Maintenance Phase:** Here when any node goes down than RERR (route error) message is sent to the nearby nodes to inform them about the node condition so that they can choose some other path to transmit their data.

Let's understand it with an example:

Consider below figure of 11 nodes. Let the sender be Node, receiver be node 11 and node 7 be the malicious node. Now the sender will best possible route to destined node by flooding the network with route request (RREQ) packets as shown in the fig. Now all other nodes present in the network will receive RREQ. Route reply (RREP) packets now will be sent by node 9 and 7 to the sender. Since the black hole node does not have a valid path thus it will send wrong RREP packet to the sender with a very high sequence number (here sq# is 580) which is greater than the original one that the node 9 replied (which is 68). Thus the sender would choose the node with higher sequence number. Thus Black-hole node will start dropping packets received from node 1 rather send it to the destination which is node 11. [6]



Print-ISSN: 2319-9512 e-ISSN: 2319-9520

LITERATURE SURVEY:

I have surveyed many papers and selected following renowned paper form my literature survey.

Heta Changela and Amit Lathigara proposed an algorithm in Aug 2015. [2] In it they proposed two way handshaking methods where when the source node sends RREQ to the destination node then this node will send RREQ_ACK to the source node to check the validity of the route and the route will be discovered by the AODV. As this handshaking signal is not known by the malicious node thus it will transmit RREP to the source node but the source node is waiting for the RREQ_ACK hence that node will be added by the source node in the blacklist and the same broadcasted in the network. But in case the malicious node knows that it has to send RREQ_ACK instead of RREP then also the malicious node can be checked by comparing the Destination Sequence Number (DSN) and Source Sequence Number (SSN). If DSN>>SSN then the node is considered as malicious.

K.R.Viswa Jhananie and Dr.C.Chandrasekar proposed a method in Apr 2015. [3]In this they formed routing table and used handshake mechanism. In this method the nodes are supposed to generate periodic same value. When the source node transmits RREQ then as a result when it receive RREP then before accepting it the reply it will first compare the periodic Id. If the value is same then the node is considered good else malicious. Since the malicious node do not anything about the dynamic Id hence it will not transmit this Id hence the nodes will not consider its reply message hence black hole attack is prevented.

Ayesha Siddiqua et al proposed a solution to prevent black hole attacks using Secure Knowledge Algorithm in 2015.[4] Every node in promiscuous mode maintains a table ontaining two fields ‘fm’ and ‘rm’

fm is Packet forwarded by node‘m’ to ‘i’.

rm Information about forwarded packet by ‘i’node, which is forwarded by ‘m’.

Where, **fm** maintains recent packet forwarded, **rm** maintains information of neighboring node related to recent packet.

STEP 2: Comparing ‘fm’ and ‘rm’ If fm and rm threshold value is reached then Modification Attack otherwise node is trusted node. **OR** If no ‘rm’ Check Packet Properties. (i) Destination address (ii) Time To Live(TTL) **OR** If ok, Check Node Properties (Energy) **and** If no ‘rm’ and Threshold Value is reached then Black Hole Attack.

Nidhi Choudhary et al introduced a timer based solution in 2015. [5] In proposed approach initially each node in the network assigns a max trust value to all its neighbouring nodes. A node will not do any further communication with a neighbour whose trust value is less than min_trust value(trust value <min_trust). When a source node receives a RREP message it update its routing table and start transmitting the data packets and also insert a unique sequence number with each transmitting data packet. When a node (N) initiates or forwards a data packet it sets a timer of T secs with it and listen the wireless link for transmissions. When the timer T expires node N will check that weather it has been received the same data packet from its next hop neighbor (N+1) for which the timer is expired. This can be done by listening to the wireless channel in promiscuous mode. If node N hasn’t heard for the packet for which the timer has expired then node N will reduce the trust value for its next hop node. This information is also disseminated in the network so that other nodes can also update or create an entry for the new trust value of that node. In this way, if node N’s next hop neighbour (N+1) will keep on dropping the data packets then its trust value will keep on decreasing and when it will reach below min_trust value in the

Print-ISSN: 2319-9512 e-ISSN: 2319-9520

network all the nodes in the network will put it into their black list table. In this way, all the black hole nodes will be eliminated from the network after few seconds of network start-up.

Subhashis et al proposed following method in 2014. [6] In it they proposed detection and prevention of black hole attack by first transmitting fake RREQ packet. After getting number of RREP it will retransmit RREQ with highest destination sequence number which it gets in earlier fake RREQ. If the same node transmit RREP with highest destination sequence number than that node is considered malicious and thus removed from the list.

Vani A. Hiremani et al proposed a MEDRI table in 2013. [7]They proposed a method to detect as well as prevent cooperative black hole attack using MEDRI (Modified Extended Data Routing Information) table.

FROM*:* 0 - node has not routed data packets and 1- node has routed data packets.

THROUGH*:* 1- node id has successfully routed data packets that were sent by node else 0.

CTR: Keeps a count of number of times the node behaved maliciously.

BH: 1- node id has been identified to be malicious in its latest interaction else it is 0.

TIMER: consider duration for which node act maliciously.

PACKET SIZE (S): Calculate data packet size at source node

PACKET SIZE (D): Calculate data packet size at destination node

RESULT: This field shows Boolean value (Yes/ No) for the comparison of fields packet size (S) and packets size (D) if packet size are equal then yes else no.

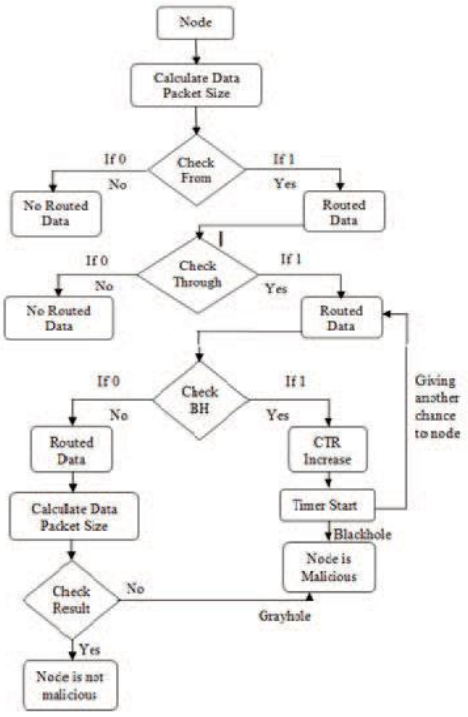


Fig-2 Flow Chart for MEDRI Table

Kamatchi et al proposed following method in 2013. [8] in it they first compare the destination sequence number received by neighbouring nodes, if found greater than threshold than that node is considered malicious else not. After that the whole data is divided into pieces (Shamir's Algorithm) and transmitted randomly so that in case there is malicious node it would be able to hear only part of the message. After receiving message receiver intimate the sender about the received message.

Chandni Garg, Preeti Sharma, Prashant Rewagad proposed a method in 2012. [9]In it Wu Chang et al. proposed a four step method to detect black hole attack namely (1) local data collection (2) Local detection (3) Cooperative detection (4) Global reaction.

In local data collection, each node gets information from neighbouring node about suspicious node. If finding one, then local detection procedure is initiated to check whether the suspicious one is a malicious one. Subsequently, the cooperative detection procedure is initiated to let the neighbouring nodes decide whether the

Print-ISSN: 2319-9512 e-ISSN: 2319-9520

node is malicious or not. As soon as the node identified as black hole malicious node then the global reaction is activated to let know all other nodes about it. It results in considerably very high PDR.

Latha Tamilselvan and Dr. V Sankaranarayanan proposed following method in 2007[10]. They used timer to collect route reply and when timer expires then no route reply are entertained. Then the source will select one of the route replies. Normally it will choose that reply which is repeated. Incase all route reply are new then it will randomly choose the route reply and send the data. Since number of route reply is present hence the probability that a black hole is chosen decreases. Thus data can be sent safely.

CONCLUSION:

In the survey paper I compare these techniques according to the following parameters: End to end delay, Packet Delivery ratio, Throughput, Routing overhead and whether they can detect and prevent black hole attack and came to a conclusion that the method proposed by **Latha Tamilselvan and Dr. V Sankaranarayanan** was very effective as it decreases the overhead and end to end delay and increases packet delivery ratio.

REFERENCES:

1) Ms. Ankita M.Shendurkar and Prof. Nitin R.Chopde proposed "A Review of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET" in Mar 2014 proceedings of International Journal of Engineering Trends and Technology (IJETT)

2) Heta Changela and Amit Lathigara proposed "Algorithm to Detect and Overcome the Black Hole Attack in MANETs" in Aug 2015 paper of International Journal of Computer Applications

3) K.R.Viswa Jhananie and Dr.C.Chandrasekar2 proposed "Detection and Removal of Blackhole Attack Using Handshake Mechanism in MANET and VANET" in Apr 2015 paper published in IOSR Journal of Mobile Computing & Application (IOSR-JMCA)

4) Ayesha Siddiqua Kotari Sridevi Arshad Ahmad Khan Mohammed proposed "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm" in 2015 proceedings of SPACES

5) Nidhi Choudhary, Dr.Lokesh Tharani proposed "Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism" in 2015 proceedings of SPACES

6) Subhashis Banerjee, Mousumi Sardar, and Koushik Majumder proposed "AODV Based Black-Hole Attack Mitigation in MANET" in 2014 proceedings of Springer

7) Vani A. Hiremani and Manisha Madhukar Jadhao proposed "Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET" in 2013 proceedings of IEEE

8) V. Kamatchi, Rajeswari Mukesh, and Rajakumar proposed "Securing Data from Black Hole Attack Using AODV Routing for Mobile Ad Hoc Networks" in 2013 proceedings of Springer

9) Chandni Garg, Preeti Sharma, Prashant Rewagad proposed "A Literature Survey of Black Hole Attack on AODV Routing Protocol" in 2012 proceedings of International Journal of advancement in electronics and computer engineering (IJAECE)

10) Latha Tamilselvan and Dr. V Sankaranarayanan proposed "Prevention of Black Hole Attack in MANET" in 2007 proceedings of IEEE

Print-ISSN: 2319-9512 e-ISSN: 2319-9520

Techniques By	Method proposed	End to end delay	Packet Delivery Ratio(PDR)	Throughput	Routing Overhead	Detection(D) and Prevention(P)
Heta Changela and Amit Lathigara	Transmission of REQ_ACK by receiver	↓	↑	↑	↔	D,P
K.R.Viswa Jhananie and Dr.C.Chandrasekar	Periodic Id of each node exchanged	↓	↑	↑	↔	P
Ayesha Siddiqua et al	Secure knowledge algorithm	↓	↑	↑	↔	P
Nidhi Choudhary et al	Timer based detection mech.	↔	↑	↔	↔	D,P
Subhashis et al	Fake RREQ	↔	↑	↔	↑	D,P
Vani A. Hiremani and Manisha Madhukar Jadhao	MEDRI table	↔	↔	↔	↑	D,P cooperative black hole attack
Kamatchi et al	Data divided and transmitted	↔	↑	↑	↔	P
Chandni Garg, Preeti Sharma, Prashant Rewagad	Local data collection, Local detection, Cooperative detection, Global reaction.	↔	(92.93%) ↑	↔	↔	D,P
Latha Tamilselvan and Dr. V Sankaranarayanan	Timer	↓	↑	↑	↔	P

Increases ↑ **Decreases** ↓ **not mentioned** ↔

Print-ISSN: 2319-9512 e-ISSN: 2319-9520