A Study on Black Hole and Gray Hole Attack in MANET

Shweta Goswami[1] Nidhi Bajpai[2] Brajesh.K.Shrivash[3]
[1,2,3]Department of Computer Science
[1,2,3]GITS, Gwalior

Abstract— Mobile Adhoc Network are widely used all around world, due to the ability to communicate without any infrastructure or fixed network. In MANET, no central authority who manages network. Due to this node rely on another node to maintain network connected. In this paper we surveyed various kinds of attacks occurred in network layer. Black hole and Gray hole attack in manet is one of them. Also study of various researchers work in Manet.

Key words: MANET, Routing Protocols, Black hole, Gray hole

I. INTRODUCTION

Mobile ad-hoc network (MANET) is a collection of mobile nodes that forms dynamically by autonomous system of mobile nodes that are connected through wireless link. In MANET infrastructure is not fixed and it's changed dynamically. In it there is not any centralized administration or base station. In this network mobile nodes communicate with each other without any fixed infrastructure and all of the transmission links are established via wireless links. Network topology of MANET changes very frequently. Each node in it performs as a router. Application of MANET includes military communication, search and rescue operations, disaster recovery, personal area network etc. MANET also involves some challenges like fewer infrastructures, dynamically changing topology, limitation of mobile nodes (short battery life and limited capacity) and network security. Characteristics of MANET like dynamic topology, less infrastructure, decentralized network and limited resources enforce ad-hoc network to vulnerable of different attack like black hole attack, spoofing, denial of service etc. to secure MANET from these kind of attack only prevention is not enough for these kind of attack next level of defense is required.

II. SECURITY GOALS IN MANET

There are some mechanisms for providing solution in MANET. These mechanisms are used to prevent from any attack, to detect any attack and to respond any attack. They are mainly confidentiality, availability, integrity and authentication and non reputation.

A. Availability:

This type of mechanism ensures that the service in the network is provided in timely manner even though there is any problem in the system.

B. Confidentiality:

it ensures that the certain type of information is never shared with the unauthorized entities.

C. Integrity:

It ensures that the information is sharing between the nodes is not corrupted or not modified with any unauthorized user.

D. Authentication:

It ensures that the network node is only accessed by the authenticated node not any unauthorized user can't be access the node.

E. Non reputation:

It ensures that the information send by the any source node cannot deny by that information or massage (2).

III. CHALLENGES IN MANET

A. Dynamic topology:

In Manets node may join or leave dynamically. As node a move frequently establishing trust among nodes is very difficult.

B. Battery Constraints:

Mobile nodes will be running with battery. If node power utilized unnecessarily then node may comes to idle state.(4)

C. Lack of Central Authority:

In MANET there will be no centralized authority like infrastructure network. So implementing security without centralized authority is a challenging task.

D. Insecure Environment:

Nodes may move randomly in MANET. So malicious node may attack and steal the data.

IV. ROUTING PROTOCOLS IN MANET

Routing protocol in MANET are categories into three parts they are reactive, proactive and hybrid. Proactive protocol is table based routing protocol. Reactive is on demand protocol. And hybrid is combination of both above protocols i.e. proactive and reactive protocol.

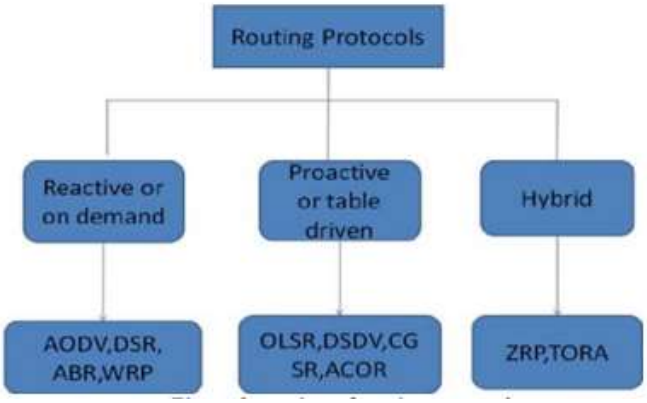


Fig1: Routing Protocol in Manet (16)

A. Proactive Routing Protocols:

In this protocol nodes periodically broadcast their information to the neighbors. Each node has to maintain their routing table which contains the adjacent nodes

All rights reserved by www.ijsrd.com

reachable nodes and number of hops. We can also say that in this protocol each node has to evaluate their neighborhood and network topology has changed. Disadvantage of this topology is that as the network size raises the expenses rises, it has got an advantage that we can recognize network status immediately and if the malicious network joins we can find them easily. Some examples of this are destination sequence distance vector routing protocol (DSDV) and optimized link state routing protocol (OLSR).

B. Reactive Routing protocol:

This is an on demand protocol. This protocol starts working when source mode wants to transmit data packet. The advantage of this routing protocol is that it reduces the wastage of bandwidth indulged from the cyclic broadcast. And disadvantage of this routing protocol is that it loses some packets during transmissions. Examples of this routing protocol are ad hoc on demand distance vector routing protocol (AODV) and dynamic source routing protocol (DSR).

1) AODV Protocol:

AODV stands for ad-hoc on demand distance vector routing protocol. This type of routing protocol is used when on demand approach is required for searching route. In this type of protocol route is establish from source to destination when it is required by the source. For establishing a route source node broadcast a Route Request (RREQ) each neighboring node updates its routing table and checks weather it has the destination node. If any node has the destination node then that node sends back Route Reply (RREP). If not then that node sends the Route Request (RREQ) to it's neighboring node and this process continued until the destination node or any other node which has the fresh route to the destination node. So the source node starts the transferring data from that route.

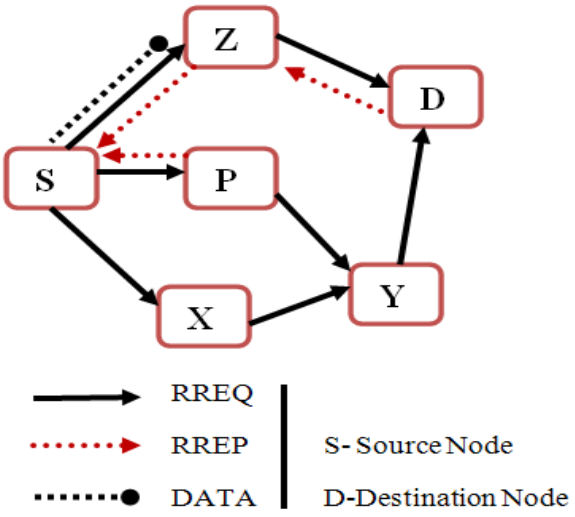


Fig 2: Propagation Of RREQ And RREP From A To E (14)

C. Hybrid protocol:

It is combination of reactive and proactive routing protocol. This is designed to overcome the disadvantages of both proactive and reactive routing protocol. Design of hybrid routing protocol is heretical or layered network framework. Proactive routing is employed to collect unknown routing information and then reactive routing protocol is used to maintain the routing information and the network topology changes. Example of this type of protocol is zone routing protocol (ZRP) and temporary ordered routing algorithm (TORA) (5).

V. SECURITY ATTACKS IN MANET

Mobile ad hoc networks are weak to both outside and inside of the network. Ad hoc networks consist of two different levels of attacks. The first level is observed on routing whereas the second level tries to attack the security of the network. An attack can be classified into two type's internal and external attack (1).

A. Internal Attacks

These attacks begin from the compromise node in the MANET. In this intruders node gets the unauthorized access pretended as a normal mobile node. Analysis is done during the flow of data in the nodes.

B. External Attacks

Outside nodes create the external attacks.
These can be classified into two types

(1) Passive attack
(2) Active attack

1) *Passive attack*

Passive attacker's only snoops the data transferred in the network and don't make any changes to data. This type of attack targets the confidentiality attribute of the system. To find out this kind of attack is very difficult because the operation of the network is not changed by this type of attack. This type of attack is basically is used to collect the information about the network and to find out the communication pattern between the communication parties. Different types of passive attacks are eavesdropping, location disclosure and traffic analysis.

2) *Active attack*

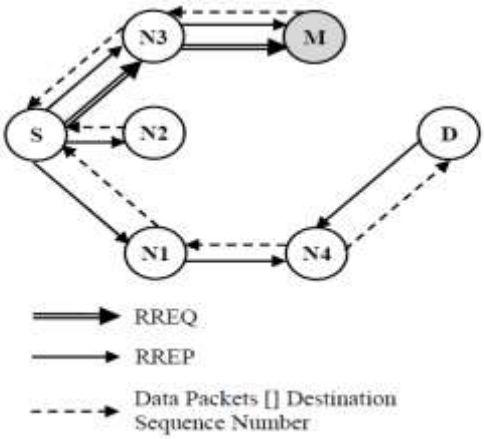
In active type of attack attacker tries to modify or alter the data. This type of attack affects the functionality of the network. In active type of attack intruder can modify the packet, inject the packet or drop the packet. Active attacks are very dangerous. Different types of active attacks are sleep deprivation, worm hole attack, gray hole attack, black hole attack, sink hole attack, rushing attack, Sybil attack and DDoS attack.

a) Black hole Attack

It is a most frequent occurring attack. It stops forwarding the data from source to destination. In this attack malicious node which keeps waiting for its neighbor node to broadcast route request packet (RREQ) when a nodes receive the route request packet it will transmit false router reply packet (RREP) by modifying its high sequence number which intendeds source node to assumed that a fresh route is available to destination by checking the sequence the source node is declining the correct node and the correct route and select the false route for transferring packet and all routes are taken towards itself by malicious nodes not to allow forwarding packets anywhere. This is very difficult to find out such type of attack and solve them. When route request (RREQ) is broadcast then many nodes sends fake route reply (RREP) to the source node claiming that it has the

All rights reserved by www.ijsrd.com

shortest route to the destination. So all packets are send through malicious node. So it acts as a black hole in the network (6).



S<<=Source Node
D<<= Destination Node
M<<= Malicious Node

Fig. 3: Black Hole Attack (3)

Black hole attacks are classified in two types:

(1) Single black hole attack: In this type of attack only node acts as a malicious node.
(2) Collaborative attack**:** In this type of attack multiple nodes in a group acts as a malicious node (7).

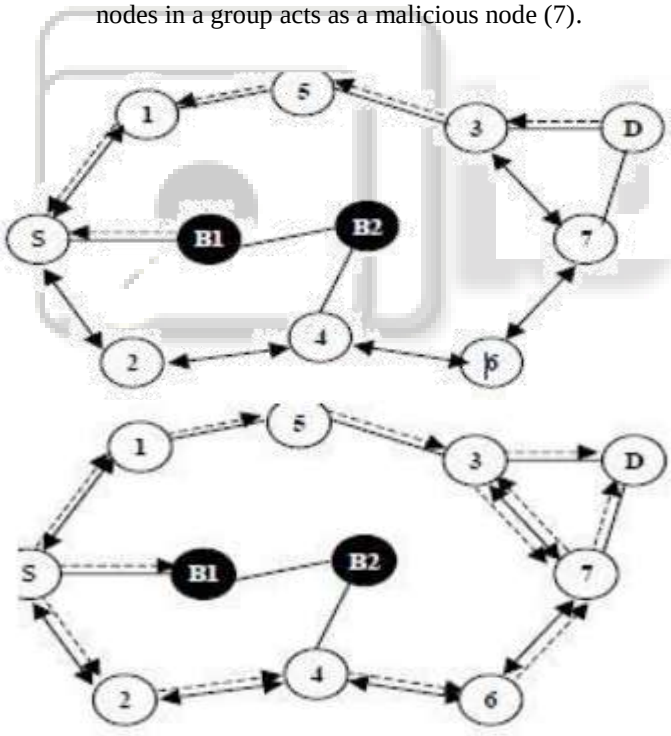


Fig. 4: Cooperative Black Hole Attack (8)

In above Example, when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its teammates B2 as the next hop, as depicted in Figure 4. According to Hongmei Deng , the source node S sends a "Further Request (FRq)" to B2 through a different route (S-2-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "yes" to both the questions. Now per the solution proposed in [13], node S starts passing the data packets assuming that the route S - B1-B2 is secure. However, in reality, the packets are consumed by node B1 and the security of the network is compromised.

b) Gray hole Attack

It is a variation of black hole attack. In this attack node drops the packet selectively. Selective forward attack is of two types:While forwarding TCP packet dropping all UDP packets
Dropping 50% of packets.

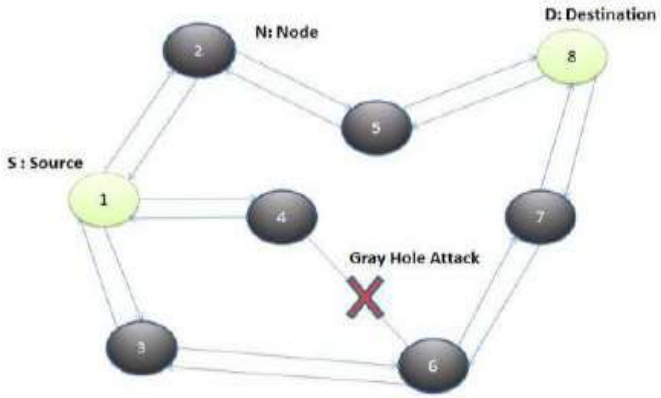


Fig 5: Gray Hole Attack (15)

In gray hole attack a node can behave as a normal node or a black hole node. So it is very difficult to find out the attack when it's behaving as a normal node. Gray hole attack has two phases:

Phase I: intruder node pretend the AODV protocol to advertise to having a valid destination node.

Phase II: in this phase the node drops the selective packets. In gray hole attack intruder behave as a malicious node until the packet are drooped and then switched to the normal behavior. Due to this reason it is very difficult to find out these kinds of attacks. Gray hole is also known as misbehaving attack (6).

VI. LITERATURE REVIEW

Mahesh Kumar Kumawat et al,[13] (2014) presented a survey on detection and prevention of gray hole attack in MANET. There is still more computational need to detect and prevent gray hole attack. Requirement to explore new kinds of attacks applied in manet networks, due to such attacks the degrade in small amout of time and result in large performance damage. In our future work we are going to propose a new algorithm based on trace gray and course based algorithm which can improve the gray hole detection rate and reduce network load as well.

Rashmi and Ameeta (2014) (11) proposed a technique in AODV protocol using clustering that helps in detection and prevention of black hole attack in mobile ad hoc network. The proposed technique is based on simple acknowledgment scheme to prevent black hole nodes in MANET. By the proposed method malicious nodes can be finding out by the intrusion detection system. This method is also applicable for multiple malicious nodes.

Disha et al (2012)(12) in routing protocol black hole and gray hole attack is serious problem and huge affect the network. For this an efficient algorithm is required to detect and prevent such attacks. In this paper explain an adaptive method to detect

All rights reserved by www.ijsrd.com

black and gray hole attack in ad hoc network based on a cross layer design, and proposed a course-based method in network layer, to overhear next hop action. In this method extra control packet does not send, by this system resources for detecting nodes saves.

Sanjay Rama swamym et.al proposed a mechanism to prevent from corporative black hole network attack. In this mechanism a technique is represented to identify multiple black hole cooperating with each other and a solution to discover a safe route to avoid cooperative black hole attack. It proposed a feasible solution for it in the AODV protocol (8).

Jaydeep sen et.al proposed a mechanism for detection of gray hole detect in MANET. This proposed mechanism increase the reliability of detection by proactively calling a collaborative and distributed algorithm by involving the neighbor nodes of a malicious gray hole node (9).

Shukla Banerjeeet.al (10) proposed a mechanism for detection and prevention of cooperative gray hole and black hole attack in mobile ad hoc network. This technique is capable for finding chain of cooperating malicious nodes which drop a signification fraction of packet. For the solution of this each node can locally maintain its own table of blacklisted nodes. So when any source tries to send data to any destination node it can also aware the network about the black list nodes. This table can help to discover a secure path.

VII. Comparison of Various Black Hole Detection Techniques in MANET

Proposal name	Approach	Assumption	Philosophy
Cooperative black hole node detection using DRI and cross checking	AODV	Cooperative black hole	Single non-black hole node detects
Black hole node detection using two different solutions	AODV	Multiple black hole	Single as well as Multiple non- black node detects
Distributed and cooperative mechanism	AODV	Distributed & Cooperative	Cooperative detection
Detecting black hole attack on AODV-based Mobile Ad Hoc using dynamic anomaly detection.	AODV	Multiple black hole	Single non-black hole node detects
Single black hole node detection	AODV	Single black hole	Single non-black hole node detects
Prevention of black hole attack using fidelity table	Enhancement on AODV	Multiple black hole	Multiple non-black hole node

VIII. Conclusion

In this paper we have discussed for detection and prevention of black hole/ gray hole in manet. In Manet, black hole and gray hole are serious attacks. Black hole is an attack where a malicious node do not forward the data packets to the destination and gray hole attack is a special variation of black hole attack which is difficult to detect. Based on the above survey, it can be concluded that Black Hole and gray attacks are severe attacks and can affect the AODV routing protocol in MANET negatively. Hence, there is need for good detection and elimination mechanisms for these attacks.

Reference

[1] Mobile Ad Hoc Networks 1-4244-0983-7/07/$25.00 ©2007 IEEE (9)
[2] 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.
[3] Rashmi , Ameeta Seehra "A Novel Approach for Preventing Black-Hole Attack in MANETs" International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.3, September 2014.
[4] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" IJTAE, JAN-2012.
[5] Mahesh Kumar Kumawat et al, / "A Survey on Detection and Prevention Techniques for Gray-Hole Attack in MANET" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1288-1290.
[6] Jasvinder, Monika Sachdeva "A Survey of Behavior of MANET Routing Protocols Under Black-hole Attack" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 8, August 2013.
[7] Amit A. Bhusari, Pradeep M. Jawandhiya, "Detection and Prevention Techniques for Gray Hole Attack in MANET: Review" *International Journal of Computer Applications (0975 – 8887) National Level Technical Conference "X-PLORE 13.*
[8] Harjeet Kaur, Varsha Sahni, Dr. Manju Bala "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 498-500.
[9] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

All rights reserved by *www.ijsrd.com*