Numerous Approaches to Overcome From Black Hole Attack in MANET

Prema Jagtap , Seema Ladhe ,Sachin Chavan

Abstract — Mobile Ad hoc network (MANET) has many applications. Police and military make use of it such as connecting each other or connecting units to each other on the battleground. MANET also useful during disaster relief operations, urgent business meeting, etc. Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. To maintain information security three major requirements should be fulfilled i.e. confidentiality, integrity and availability. Security of the MANET has been challenged by malicious attacks in MANET i.e. eavesdropping, spoofing, control packet modification and denial of services(DOS).

This paper we primarily focus on the black hole attack in MANET and methods used to overcome this attack. The main impact of this paper is we yield detail comparison of various approaches used to avoid and mitigate this attack.

Index Terms—Ad hoc network , AODV, black hole, DOS, , EAVESDROPPING, MANET, SPOOFING

1. Introduction

Mobile Ad-Hoc Networks are self-directed and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes can be the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They are interrelated by using Bluetooth or Wi-Fi . They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be organized urgently without the need of any frame. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met.

MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no strong defence mechanism.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a very challenging issue so due to this there is increasing threats of attack on the Mobile Networks. To give more secure communication and transmission, we must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central management in network and changing topology.

This paper we mainly concentrations on the various protocols used for communication in MANET, various attacks, threats and methods used to overwhelmed on these attacks. The main contribution of this paper is we produce detail comparison of various approaches used to avoid and mitigate these attacks.

2. Classification of MANET protocols

- *Prema Jagtap*,Dept Computer Engineering,MGMCET,Mumbai University,India, E-mail:prema.jagtap11@gmail.com*
- *Seema Ladhe,Dept Computer Engineering,MGMCET,Mumbai University,India, E-mail:seemaladhe@yahoo.com*
- *Sachin Chavan,Dept Computer Engineering,MGMCET,Mumbai University,India, E-mail:ssschavan2003@gmail.com*

Routing protocol in MANET classified into following types based on network structure, communication model, and routing strategy. Based on the routing strategy the routing protocols can be classified into two parts:
1.Table driven
2. On demand.

Routing protocols in MANETs can be classified into three different types, i.e.
1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

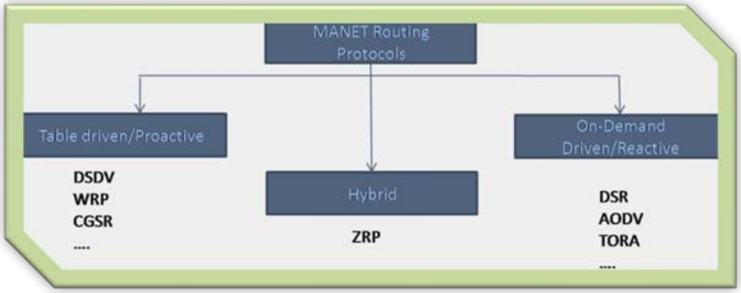

Fig1. Classification of MANET routing protocol

2.1 Reactive Protocols:

Reactive protocols also known as on demand driven protocols. Unless and until source node doesn't request, this protocol doesn't initiate root discovery process so called as on demand. Root is setup when demanded. When any node don't have path to reach to the destination then reactive routing protocol establishes path between the source and destination node.

- **Ad-Hoc on Demand Distance Vector Protocol (AODV):**

AODV is a type of reactive protocol so that it does not require to maintain route to the destination which are not part of active communication, instead of it allows mobile node to obtain route rapidly to the destination via another path. AODV performs loop free operations, it avoids Bellman-Ford count to infinity problem and provide quick convergence when network topology changes. In the following section most fundamental functionality has given i.e. route discovery and route maintenance process.

AODV is used to find the path to the destination if any node wants to transfer the packet to particular destination hence it is purposely used in mobile ad hoc networks. Within a network those routes are needed that all are maintained by the source node. All intermediate nodes maintain the route table which contain route information needed for the route discovery process. Each node in the network maintains its own routing table. Routing table has fields like <destination, next hop, number of hops, destination sequence number, active neighbours, lifetime>.AODV make use of several control packets,

1) RREQ(route request packet)=It is broadcasted by node which want the route to the another node.
2) RREP(route reply packet)=It is unicasted packet back to the source of RREQ.
3) RERR(route error packet)=It notify the other node that loss of link.
4) HELLO(hello message)=It help to find active neighbors.

Route request(RREQ) message format:

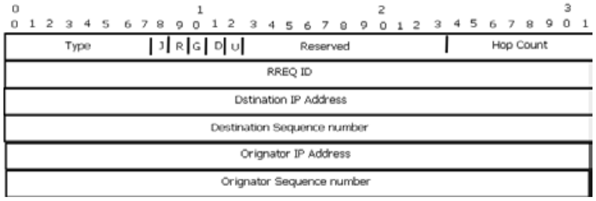

Fig 2- Route request (RREQ) message

Route reply(RREP) message format:

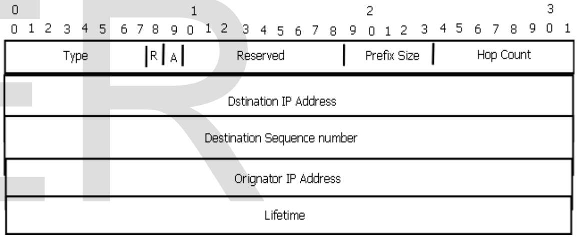

Fig 3- Route reply(RREP) message

2.2 Proactive Protocols:

Proactive routing protocols work opposite to reactive routing protocols. These protocols always maintain the updated topology of the network. Every node in the network knows about the other node beforehand. All the routing information is regularly kept in tables. Whenever there is a change in the network topology, these tables are updated according to the change. The nodes exchange topology information with each other; they can have route information any time when they needed.

2.3 Hybrid Protocols:

Hybrid protocols combines the strengths of both reactive and proactive protocols to get better performance. The network is divided into regions, and use different protocols in two different regions i.e. one protocol is used within region, and the other protocol is used between them. e.g.- Zone Routing Protocol (ZRP). ZRP uses proactive mechanism for route establishment within the nodes neighborhood, and for communication amongst the neighborhood it takes the advantage of reactive protocols. These local neighborhoods are known as zones, and the protocol is named for the same reason as zone routing protocol. Each zone can have different size and each node may be within multiple overlapping zones. The size of zone is given by radius of length P, where P is number of hops to the perimeter of the zone.

2.4 Classification of proactive and reactive protocol.

TABLE 1
DIFFERENCE OF PROACTIVE AND REACTIVE

Proactive Protocols	Reactive Protocols
Attempt to maintain consistent, up-to-date routing information from each node to every other node in the network.	A route is built only when required.
Constant propagation of routing information periodically even when a topology change does not occur.	No periodic updates. Control information is not propagated unless there is a change in the topology.
Incurs substantial traffic and power consumption, which is generally scare in mobile computers.	Does not incur substantial traffic and power consumption compared to table routing protocols.
First packet latency is less when compared with on-demand protocols.	First-packet latency is more when compared with table-driven protocols because a route need to be built.
A route to every other node in ad-hoc network is always available.	Not available.
e.g.- DSDV,STAR,WRP	e.g.- AODV,DSR,TORA

3. VARIOUS ATTACKS IN MANET

3.1 ACTIVE ATTACK

A. Black Hole Attack

Black hole attack performs through malicious node. Malicious node act as false node in the network and says that it having fresh route to the destination. Source node broadcast RREQ packet and that packet will be forwarded by each intermediate node until destination node does not reach. If malicious node is present in the network and if that node receive RREQ packet, it immediately sends false RREP packet with high sequence number and minimum hop count. In this way malicious node claims that it having fresh route information to the destination. In this way malicious node will drops the packets by sending false RREP packet to the source node.

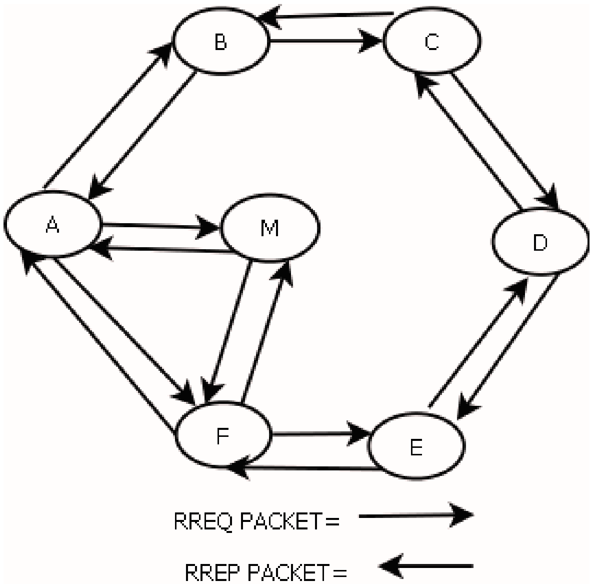

Fig.4- Black hole Attack

B. Gray Hole Attack

In this type of attack the attacker lies the network by supportive for forwarding the packets in the network. When it receive the packets from the neighbouring node, the attacker drop the packets. This is a type of active attack. At the starting the attacker nodes behaves ordinarily and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and introduction Denial of Service (DoS) attack.

C. Flooding Attack

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such IP addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an huge amount of useless data packets into the network which is directed to all the other nodes in the network. These huge unwanted data packets in the network block the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

D. Selfish Node

In MANETs the nodes perform collaboratively in order to forward packets from one node to another node. When a node refuse to work in partnership to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disturbance.The worry of the node is only to save and conserves it resources while the network and traffic disturbance is the unexpected result of this behaviour. The node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network.The selfish node can sometime drop the packets.

F. Denial of service attack

In a DoS attack, the attacker sends unnecessary messages requesting the network or server to validate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the verification approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more verification messages with invalid return addresses. Hence, the process of verification and server wait will begin again, keeping the network or server busy.

G. Byzantine Attack

In this attack an intermediate node or a set of intermediate nodes work in collusion and carry out attacks such as creating routing loops, forwarding packets on non – optimal path which results in ruin of the routing system.

3.2 PASSIVE ATTACKS

- **Traffic Monitoring**

Traffic monitoring specifies for MANET and also other wireless network such as cellular, satellite and WLAN to developed or identify the communication and functional information for the launching of attacks.

- **Eavesdropping**

The main goal of eavesdropping is to obtain some confidential information that should be secret during communication. This confidential information may include the location of public key or private key and also the password of the nodes.

- **Traffic Analysis**

Traffic analysis is a passive attack used to increase the information from which node can communicate with each other and also how data should process.

4. VARIOUS APPROACHES USED TO OVERCOME FROM SECURITY THREATS

Kamarularifin Abd et.al.[1] have designed an EAODV solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep_tab to store incoming RREP Packet, parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table and to control the process of accepting RREP message for routing updates. Source will send request packet to the destination. To find the shortest path that packet will be forwarded to all its neighbour nodes. Destination node will send reply packet to the source node. Along with destination node MALICIOUS NODE will also send reply packet to source node. Reply packet received by node 'S' will be stored in rrep_tab table until rt_upd=true. Upon receiving RREP message from destination node rt_upd turns to false. Source will update its routing table with later entry. If rt_upd=false then no more RREP message accepted. RREP message come after this are rejected. When rt_upd=FALSE that time process for detecting malicious node start. rrep_tab table is analysed & NODE ID which has high destination sequence number will be isolated as MALICIOUS NODE. After detecting malicious node it will be stored in mali_list. And again rt_upd set to TRUE.

EAODV method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP. It only detect & isolate malicious node but doesn't announces black hole to its neighbors. It doesn't taking any preventive measures.

Mohammad Taqi Soleimani [2] have designed Black hole attack detection method to detect black hole attack based on neighbor's information. First node after receiving RREP packet it will check validity of that packet. To check correctness, node will broadcast NREQ packet to all its 2-hops neighbours to find that there is destination node or suspicious node in its neighbourhood or not. In response to this each node is neighbour of destination node and suspicious node send back NREP packet along with its neighbours list. When node receives NREQ packet, it searches its blacklist to check whether there is suspicious node is in list or not. If found then it send alarm packet. But when destination node receives NREQ packet it send NREP packet if suspicious node is member of its neighbour set otherwise it send alarm packet too. If receiving node is in neighbourhood of dest. Node, it relies on the destination to check and forward NREQ instead of sending NREP packet. After validating RREP by other node then node removes RREP from queue and forward it to source node. If there is no received NREP it will supposed that destination node is located far away from suspicious node. So it is assumed that malicious node is present in network .To check this sequence number is compared in NREQ packet with dest. Node if found large seq no in NREQ then node declared as malicious node. hence it drops corresponding RREP from queue and keep that node in blacklist. Alarm is broadcasted for all its two hops neighbours.

In this solution neighbour nodes may give false information. Each node have to maintain blacklist, so extra database have to maintain. Generation of ALARM packet will considerably increase the routing overhead.

Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU [3] proposed an adaptive approach to detect black and gray hole attacks in ad hoc network based on a cross layer design. In network layer, a path-based method to overhear the next hop‟s action. Every node should have FwdPktBuffer which is packet digest buffer. When packet is forwarded out that time digest is maintained in FwdPktBuffer and detecting node overhear. When next hop forward packet is overheard then digest released from FwdPktBuffer. In fixed time period node should calculate overhear rate of next hop and compare with threshold. If forwarding packet is lower than threshold then detecting node consider as black hole node.This scheme does not send out extra control packets and saves the system resources of the detecting node.

In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. Two counter added i.e. collisionpktnum and noncolpktnum added to standard 802.11 protocol. If collision occurs then collisionpktnum increases to 1,if packet being received successfully then noncolpktnum increases to 1.These two counter are used to calculate detection threshold value.If node drops a packet in probability higher than detection threshold then detecting node will declare as malicious node.

This method doesn’t taking any preventive measures.Every node have to maintain buffer and formulating threshold and overhear rate is a bit overwhelming.

Jie Yang[4] have designed Recording packet exchange solution to secure the history records of packet delivery information at each contact so that other node can detect insider attack by analyzing these packet delivery records.Each node in the network generate public-private key pair. Wait until node A encounters node B. Node A request node B’s RRT and compute packet forwarding percentage. If packet forwarding percentage less than threshold then node B may be malicious node.But if it is more than threshold then node A compare node B’s RRT with its SRT to check that node B has dropped records in RRT. If yes then node B may be malicious node.

But if not then packet will be exchange between node A and node B. Packet record generation and storage in node A and B.If it m time positive for checking violation then node B declare as Black hole.But if not then again wait until node A encounters node B.

It doesn’t taking any preventive measures. Each node have to maintain two extra table,each node have to calculate packet forwarding percentage,overhead for updating threshold value.

Nital Mistry, Devesh C Jinwala, Mukesh Zaveri[7], In solution the source node stores all the RREPs in the table called Cmg_RREP_Tab until receiving first RREP packet waits for MOS_WAIT_TIME. Meanwhile, the source node analyses all the stored RREPs from Cmg_RREP_Tab table, and discard the RREPs having a very high destination sequence number. Every node in the network maintains a table called Mali_node for storing the malicious node details to isolate the malicious node in the network.

Moreover, in order to maintain freshness, the Cmg_RREP_Tab is flushed once an RREP is chosen from it. However, it has high processing delay. It doesn’t taking any preventive measures.

5. CONCLUSIONS

This paper mainly concentrate on various routing protocols, their taxonomy based on various factors and their working used in MANET. This paper mainly discuss about various techniques used to prevent black hole attack MANET and to provide security.This paper focuses on security approaches based on various routing protocol and provide comparison of these techniques.

.

REFERENCES

[1] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Black hole effect mitigation method in AODV routing protocol", 2011 IEEE Conference

[2] Mohamad Taqi Soleimani, Abdorasoul Ghasemi. "Secure AODV against Maliciously Packet dropping",2011 IEEE.

[3] Jiwan 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.

[4] Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen. "Detecting blackhole attacks in Disruption –Tolerant Network through packet exchange recording" 2010 IEEE.

[5] Junhai Luo, Mingyu Fan, Danxia ye."Black Hole attack prevention based on Authentication mechanism" 2008 IEEE..

[6] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Securing Routing Table Update in AODV Routing Protocol ", 2011 IEEE Conference on Open Systems(ICOS2011),September 25-28,2011,Langkawi,Malaysia.

[7] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri.,"Improving AODV Protocol against Blackhole Attacks",Proceedings of the International MultiConference of Engineers and Computer Scientists 2010 Vol II,IMECS 2010,March 17-19,2010,Hong Kong.

[8] Payal N..Raj,Prashant B.Swadas.,"DPRAODV:A Dynamic Learning System Against Blackhole Ataack In AODV Based MANET",International Journal of Computer Science Issues,vol.2,pp 54-59,2009.

[9] Mohammad Abu Obaida,Shahnewaz Ahmed Faisal ,Md. Abu Horaira, Tanay Kumar Roy4 "AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes ",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 8, 2011.

[10] Subash Chandra Mandhata,Dr.Surya Narayan Patro,"A counter measure to Black hole Attack on AODV-basedMobileAd-hocNetworks"International Journal of Computer and Communication Technology(IJCCT),Volume 2,IssueVI,2011