Prevention of black hole attack by different methods in MANET.

Nakka Nandini, Reena Aggarwal

Lovely Professional University, Phagwara, Punjab

Abstract: **An ad-hoc network is a temporary infrastructure less network which is a collection of mobile nodes in the dynamically form. This network is always independent and a isolated network. Due to the limitation power and mobility there is less sufficiency among them. In these wireless networks, the main things like confidentiality, availability authentication, anonymity, integrity to all the users of mobile communication. There are many security attacks in MANET in which these are responsible for the failure in communication from source to destination. Among such attacks black hole attack is one of such serious attacks in MANET. In this paper, we compared the existing solutions and discussed different methods to eliminate the black hole attack in MANET.**

Keywords: **ad-hoc networks, security attacks, black hole attack.**

I. INTRODUCTION

Mobile Ad hoc Networks are the self configuring networks in which it is composed of several movable user equipment. MANETs are decentralized and autonomous wireless systems. The presence of mobile nodes in the network is free in moving in and out in the network. These nodes can form arbitrary topologies depending on their connectivity with the each other in the network. These also act as systems (or) devices such as mobile devices like personal mobile phones, digital cameras, laptops, MP3 players, and personal computers that are participating in the network and as well as they act as host(or) router (or) both at the same time. They have the self configuration ability in which they can self configure themselves because they can be deployed urgently without the need of any infrastructure. IP routing protocols are developed by the most devoted working group that is Internet Engineering Task Force (IETF). There are many routing protocols which are developed for MANETs which are challenging and interesting in the research areas. Such protocols are AODV, DSR, OLSR, ZRP etc., The basic functionality of network is mainly decided by most important concern i.e. security in MANETs. The data which is confidential, available and secured can be achieved by assuring that security issues which can be met. MANETs are prone to security attacks because of its features like open medium, topology changing dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism.

In MANETs there is mutual trust among the mobile nodes in which they can communicate with each without any help of centralized administration. This is the special and specific characteristic in MANETs which makes more vulnerable to be exploited by an attacker inside the network. The wireless links which make it easier for attacker to go inside the network and get access to ongoing communication are more susceptible to attacks. The main types of attacks which the MANETs mainly suffers worm hole attack, black hole attack, Sybil attack, denial of service(DOS), selfish node misbehaving, impersonation attack.

II. LITERATURE SURVEY

Fun-Hsun Tseng et.al discussed the different methods for detecting and eliminating the black hole attack in a secure and sophisticated way in order to provide the accurate communication in wireless mobile ad-hoc networks.[1]

Khushbu Patel proposed a mechanism for the nodes which are deployed in MANETs in order to detect and prevent black hole attacks .[2] They have surveyed and compared the existing solutions to black hole attacks on AODV protocol.

III. MANET AND ITS ATTACKS

As MANETs are more prone to the threats due to the unauthorized nodes those are outside the network or from the nodes inside the network. The threats which are outside of the network are easily detected when compared to the inside as

ISSN: 2278 – 1323

the network as the internal nodes are difficult as they are from trusted sources. Security threats can be broadly divided into mainly two ways. One is external threats and internal threats [3]. The external threats are mostly detected at physical and data link layers due to the presence of the authentication protocol to protect the upper layers. But to detect the internal nodes, the necessary information is required to participate as it is very difficult at distributed operations. Packet dropping is the main attack by the malicious nodes as the most of the routing protocols have no mechanism to detect whether data packets have been forwarded (or) not.

There are many types of attacks in MANET. These are classified as passive and active attacks.[4] [5]. In passive attacks, the attackers have the interception of communication of data, in which the interception of communication of data, in which the information of the location and move patterns of the nodes are disclosed. As the attacker doesn't exhibit any of the abnormal activities it is highly difficult to detect this type of attacks. While in the case of active attacks, involves the intruders' actions. The main target of the attack can be either data traffic (or) routing traffic [5]. The large volume of extraneous data packets are inserted into network by the intruders. They can also intentionally drop, corrupt and delay data packets passing through it.

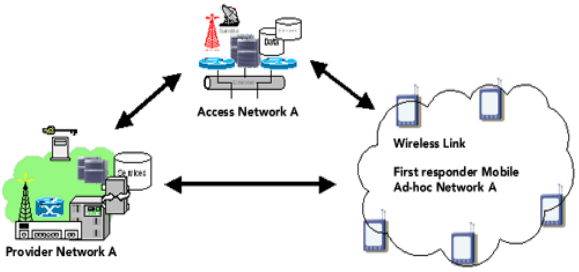

Figure 1: Representation of MANET

Black hole attack is a special attack in which there are many types it can be occurred. One type of black hole attack can occur when the malicious node on the path directly attacks the data traffic by intentionally dropping, delaying (or) altering the data traffic passing through it [5]. By setting the promiscuous node to each node and listening to see if the next node on the path forward the data traffic as expected, this type of black hole attack can be easily mitigated. Another type of black hole attack used by a malicious node which makes all the traffic travel through it by claiming to have the shortest route to all other nodes in the network[5]. So after this, the malicious node simply drops the packets instead of forwarding the packets. The main concept of black hole attack is that it creates a fake root reply packet that initiates a route delivery to a source node. A variant of black hole is the gray hole attack in which it transmits some packets selectively and drops others.

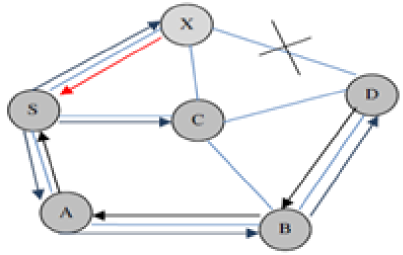

Figure 2: Black hole attack

IV. SINGLE BLACK HOLE ATTACK

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks [6]. An example is shown as Figure 3, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely.

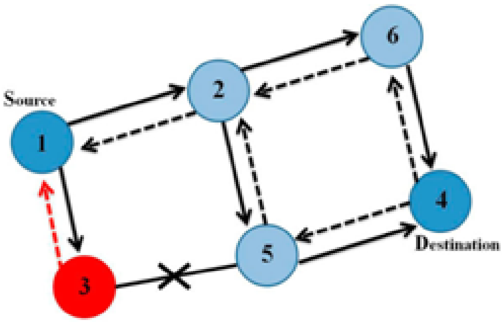

Figure 3: Single black hole attack

A. Reactive routing protocol:

ISSN: 2278 – 1323

Another appellation of on demand routing protocol is equipped with named on reactive routing protocol. When nodes desire to transfer the data packets, then reactive routing protocol comes to the play. The periodically broadcasting can be reduced as induced bandwidth which is wasted is the main strength. And also in the particular environment of network, if there is presence of any malicious nodes, then there will be a dreadful wound in the network. The packet loss is main disadvantage in the passive routing method. The two protocols which work under this protocol is Ad hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocol. The DSDV routing is main base for the construction of AODV, in which in its routing table, next hop information is recorded by each node only, but for to keep the existence a routing path between source to destination node, it maintains it. The execution of route discovery path is done immediately, when the source node is not reached from the destination node. In this process, the source node request packets first. Then the reception of the RREQ packets are done by the intermediate nodes and also route reply(RREP) is sent by the parts from source node only if the information of the destination node was performed at their routing table. The process of route maintenance is started when the topology of network's connection has failed (or) changed. To decide the new routing path, is utilized to present the information of routing (or) by restarting the process of route discovery for information to be updated in the routing table. The idea for designing the DSR is based on source routing. The source routing means that each data packet contains the routing path from source to the destination in their headers [5]. The recording of next hop information is taken by AODV in the routing table, but the maintenance of the route cache is maintained by DSR from source to destination node. As the routing information is recorded in route cache of each node, the source node determines the routing path. As the network mobility increases, the DSR performance decreases, higher network mobility along with packet delivery ratio.

B. Proactive Routing Protocol:

The proactive routing is also called as Table driven routing protocol [1]. In this particular protocol, the routing information to the neighbors is broadcasted by the mobile nodes. The routing table is maintained by each and every node which not only records the reachable and adjustable nodes but also the hops number. As long as the topology of network is changed, the neighborhoods have to be evaluated by the nodes. Within the larger topology of network, along with significant overhead communication, the network size increases along with the rising of the overhead which is the great disadvantage. The reflection of the status of network is the great advantage by adjoining the malicious attackers. The familiar types of proactive routing protocols are Destination Sequenced Distance Vector (DSDV) routing protocol and Optimized Link State Routing (OLSR) protocol.

C. Hybrid Routing Protocol:

The hybrid routing protocol combines the advantages of proactive routing and reactive routing protocol to overcome the defects of them [1]. The hierarchical (or) layered network framework is mostly used in the hybrid routing protocols. The proactive routing is employed to completely gather the unfamiliar routing information, then using the reactive routing to maintain the routing information when network topology changes. The familiar hybrid routing protocols are zone routing protocols (ZRP) and Temporarily Ordered Routing Algorithm (TORA) [7] [8].

V.SCHEMES FOR DETECTING THE BLACK HOLE ATTACK

A. Neighborhood based and routing recovery:

In this detection scheme, this is mainly used to identify the black hole attack and to find the accurate path. This method is approached to recognize the fake nodes in the neighborhood. At first in the recovery protocol a *modify_route_control* packet will be sent to get the routing path at the destination node.

Advantages:

In this scheme, the correct detection probability is also achieved with lower detection time and higher throughput.

B. Redundant route method:

In this method, between the source and destination we find more than one route. The mechanism is followed as, at first the ping packet is sent by the source node to the destination. The request is replied by the receiver to the destination and the execution takes place at source node. If there is presence of two received RREP packets, it is buffered and transmitted after identifying the safe route. The lowest routing paths come into existence at the same time. From the number of nodes and hops the accurate and secure node is identified by the source node and the black hole attack is prevented.

C. Detection, Prevention and Reaction AODV (DPRAODV) scheme:

In this scheme, mainly the threshold value is checked unlike the normal AODV. By sending the RREP_seq_no we can check whether the sender is attacker (or) not. If suppose the value of RREP_seq_no is higher, then the sender will be considered as attacker and it will be added to the black list and then the node will be considered as the malicious node and it will be blocked and it will not be processing any of the RREP. And also by the calculation of the average dest_seq_no between the sequence number RREP packet, the threshold value keeps on changing, by this we can not only detect the black hole attack but also we can prevent them by the threshold value updating.

VI. CONCLUSION

In this paper, the detection methods and schemes for identifying the black hole attack is proposed in which the first method called neighborhood based and routing recovery discover the unauthorized nodes to find the correct routing path. In the next method, redundant route method we send the ping packet and find the existence of two routes, and find the best route among them. In third method, i.e. detection, prevention and reaction AODV (DPRAODV) by updating the threshold values and changing them between the sequence number and the RREP packets, we can prevent the black hole attack to some extent in the networking environment. Black hole attack being one of the severe security threats in MANETs we can prevent this attack by implementing AODV protocol and getting the accurate threshold value as the future work.

REFERENCES

[1] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao “A survey of black hole attacks in wireless mobile ad-hoc networks” on Human Centric Computing and Information Sciences 2011, a Springer Open Journal.

[2] Khushbhu Patel “Survey of Black Hole Attacks on AODV protocol in MANET” International Journal for Technological Research in Engineering volume1, Issue 6, February 2014.

[3] Reena Sahoo and Dr.P.M.Khilar “Detecting Malicious nodes in MANET based on a Cooperative Approach” IJCA special issue on 2nd National conference-Computing, Communication and Sensor Network, CCSN,2011.

[4] Bo Sun, Yong Guan,Jian Chen, Udo.W.Pooch “Detecting Black hole Attack in Mobile Ad Hoc Networks” Department of computer Science, Texas A&M university.

[5] Nishant Sitapura and Prof. Sandeep.B.Vanjale “Detection and Prevention of Black hole attack in Mobile Ad Hoc Attacks”, International conference ICETE-2010 on Emerging Trends in Engineering.

[6] Jasvinder, Monika Sachdeva “A survey of behavior of MANET routing protocol under black hole attack” International Journal of Advanced Research in Computer Science and Software Engineering, vol 3,issue 8, august 2013.

[7] Haas ZJ, Pearlman MR, Samar P “The Zone Routing Protocol(ZRP) for Ad Hoc Networks”.

[8] Park V Corson S “Temporary Ordered Routing Algorithm(TORA)” version 1 functional specification.