Survey on Security Issues in Mobile Adhoc Networks

Shashikala S R[1] B P Savukar[2]
[1]M.Tech Student [2]Assistant Professor
[1]Department of Electronics and Communication Engineering [2]Department of Computer Science
[1,2]BLDEACET, Bijapur, Karnataka, India

Abstract— A wireless mobile ad hoc network (MANETs) consists of number of nodes. During the communication they need to cooperate with each other. The main problem with the wireless networks is the security because of the open medium and no centralized base station. There are many security issues related to wireless network. The most of the wireless networks faces the problem of black-hole attacks and gray-hole attacks by the malicious nodes. Here a solution is provided to come out of these problems.

***Key words*:** mobile ad hoc network (MANET), dynamic source routing (DSR), collaborative bait detection scheme (CBDS)

I. INTRODUCTION

A wireless network is a collection of nodes which uses wireless connections for providing links between one node to another node. Wireless network is a decentralized and self-configuring. It means that it is not having the centralized base station which can control the transmission of the packets and all the nodes are moving independently in any direction in any time therefore the topology of the network changes every time and therefore there is no any fixed configuration for the network. There are many types in wireless networks: wireless sensor networks (WSN), mobile wireless sensor networks, ad-hoc wireless sensor network and mobile ad-hoc networks (MANETs).

II. MOBILE AD-HOC NETWORKS (MANETS): AN OVERVIEW

In MANETs, Mobile is nothing but 'moving' and Ad hoc is nothing but 'temporary with no configuration'. Here the nodes in the network are able to move in all the direction in any time. The mobility of the nodes leads to a sudden change in the topology of the network.

Each host in the network is having a limitation in the transmission range. The source can transmit the packets to the destination through the intermediate nodes using multi-hop routing. Therefore a MANET is having a number of nodes, with each node having a wireless transmitter and receiver that communicate with each other without any central base station because of this they need cooperation among themselves.

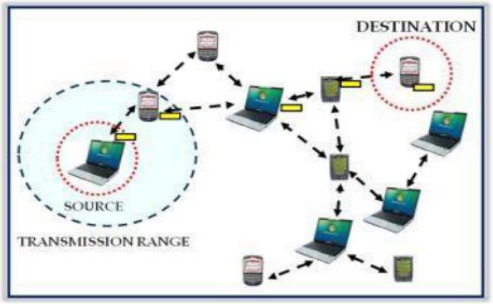

Fig 1: Transmission of packets from source to the destination

In the fig 1 we can see the transmission of packets from source node to the destination node through the several intermediate nodes. Here the laptop is acting as a source node and mobile is acting as a destination. Routing protocols, consumption of the battery and bandwidth decides the goodness of the networks [1].

A. *Types of MANETs*

There are mainly three types in mobile Ad hoc networks (MANETs) [11].

iMANETs: Internet based mobile Ad hoc networks. It is used to join the moving nodes with the static internet gateway. It is self-organizing.

VANETs: vehicular Ad hoc networks are the form of 'mobile Ad hoc networks'. It provides the communication between the nodes in the roadside. In this vehicles acts as nodes which is fixed with the VANET device.

In VANETs: Intelligent vehicular Ad hoc network are having the intelligence which helps them to avoid accidents. Here the nodes make use of WiFi and WiMAX for the communication.

B. *Advantages of MANETs*

MANETs establishes a communication between the nodes that can be easily managed. This makes them to use in a region where there is a need of totally distributed network system without any fixed base station. It may be applied in battlefields, military applications, earthquakes and any other disaster or unexpected situations [2]. The fig 2 shows an example for applications of MANETs.

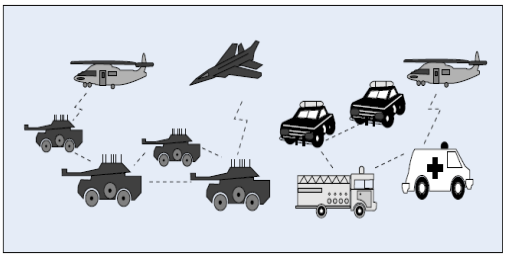

Fig. 2: Applications of MANETs

C. *Challenging issues in MANETs*

Due to the infrastructure less property of the mobile Ad hoc network there are many security issues associated with it. The issues listed below causes the degradation of the performance of the network in terms of reliability and throughput.

1) Every information in the network pass through a fixed bandwidth these can be easily captured and modified by the attacker. Because of no central base station, the authentication using the cryptography technique cannot be used here.
2) Any security solution with fixed configuration cannot be applied to a network which is having a rapidly changing topology where the hosts in the network are able to move everywhere. In this kind of network all

the nodes exchange the routing information any of the thrust may send the false information about the routing causing denial of service (DoS).

3) The network with no centralized base station needs the cooperation between all the nodes which are present in the network. The malicious node can modify the routing information resulting in breaking of the cooperation between the nodes.
4) All the nodes in the network require energy to be active while routing. The node in the network depends on the batteries for their energy. The limited energy of the batteries may cause frequent disconnection of the break.

III. TYPES OF SECURITY ATTACKS

A. *Passive attacks:*

It does not alter the usual operation of the network. The attacker looks over into the exchanged data between the two nodes without altering it. These kinds of attacks are difficult to detect. The only way to come out of this attack is to encrypt the information strongly. Thereby making the attacker unable to decrypt the message

B. *Active attacks:*

This kind of attacks may change the information present in the packets or it may drop the packet itself. This kind of attack may be external or internal to the network [3].

IV. MALICIOUS NODE

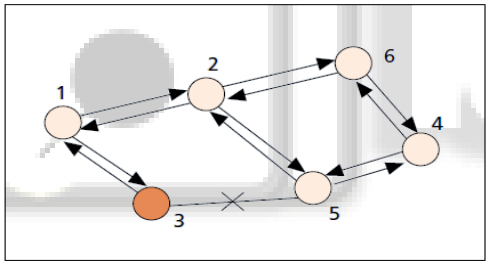

Fig. 3: Presence of malicious node

Many of the attacks against the Ad hoc wireless network are present. Any node in the network which is misbehaving and not properly supporting the routing can be called as malicious. Fig 3 shows the network containing the six nodes and transmission of packets between them. The node numbered three is acting as a malicious node. There are mainly two types of routing attacks which are commonly caused by malicious nodes:

A. *Black-hole attack:*

While transmitting the packets from source node to the destination node, any intermediate node in the network so called malicious node replies with the false RREP indicating that it has the shortest path in the routing. When the communication begins it discards all the packets without passing it to the destination node. This results in the breaking of the communication. This kind of nodes should be avoided for the proper communication.

B. *Gray-hole attack:*

In this case, when the communication begins, initially the node gains the trust of the network. Once the communication begins it selectively discards and forwards the packets making interruption in the communication. These kind attacks are very difficult to identify.

A cooperative black-hole attack is when the many of the malicious nodes acts together.

V. ROUTE DISCOVERY AND ROUTE MAINTENANCE

In the route discovery step the Dynamic source routing (DSR) technique involves the broadcasting of Route Request (RREQ) message to all the nodes by the source node [4]. Once the RREQ message reaches to all the nodes in the network, the node which is having shortest path to the destination replies with the Route Reply (RREP) message. All the intermediate nodes add its address information to the RREQ message packet.

The destination node can easily came to know the address of each intermediate node from the RREQ message packet. Thus the whole communication depends on the intermediate nodes. Therefore the presence of any misbehaving node can make the communication unreliable.
The Route maintenance step handles the situation when there is a disconnection between the nodes because of link breakage. The breaking of link occurs because of limited transmission range of nodes. Then it sends the information of breaking of a link between the nodes to the source node informing that to search for another route to the destination to forward the packets [6].

VI. ROUTING PROTOCOLS IN MANETS

Proactive MANET protocols: These protocols maintain the routing information of every path to a particular destination. These routing information are stored in a table and distributes these information throughout the network. The disadvantage of this protocol is that it needs specific amount of data for maintain the routing information. One example of proactive routing protocol is Optimized Link State Routing protocol (OLSR) [10].

Reactive routing protocols: These protocols are also called as on-demand routing protocol. These protocols search on demand by sending the route request message throughout the network. The disadvantage of this protocol is that it takes much time for searching the path. One example of reactive routing protocol is Ad hoc on-demand distance vector (AODV).

Hybrid routing protocols: These protocols combines both the proactive and reactive protocols. The routing begins proactively and reactive protocols are activated only on demand. The disadvantage of this protocol is that it depends on the number of active nodes in the network. The example of hybrid routing protocol is Zone Routing Protocol (ZRP).

VII. EXISTING SYSTEMS

Since the proper routing of the information depends on the behavior of the intermediate nodes. There is a mechanism to check the performance of intermediate nodes when transmitting the packets from source to the destination. The idea is based on the Markle tree and it also makes use of AODV protocol.

A Merkle tree is a binary tree in which, each leaf carries a given value and the value of an interior node (including the root) is a one-way hash function of the node's

children values. It checks how well the intermediate node carries data to the destination node [5]. It avoids the black-hole attack and cooperative black-hole attacks. It is not much useful when applied to cooperative black-hole attacks because it consumes much time in calculation.

Next the improvement is done in recognizing the malicious node by using the watchdog and pathrater. The watchdog is used to detect the malicious nodes and pathrater is used to avoid the malicious node by rating each of the nodes in the network. When transmitting the packets from source to the destination the path with highest metric value is chosen for the transmission. If the watchdog is not active then the pathrater is not able to decide the misbehaving nodes. It increases the throughput of the network [6]. There is not a optimal watchdog threshold to decide the nodes as misbehaving.

Later the solution to the black-hole attack is provided based on the demand distance vector routing protocol. Here they used the RREP and RREQ message to verify that there is a route between intermediate node and the destination node. If it exists, the packet can be sent through this intermediate node. This method can increase the throughput while maintaining the transmission overhead minimal [4]. The drawback of this method is that it is implemented assuming that the malicious node cannot work in cooperative group. The team work of the malicious node may lead to problem.

Next step is taken to prevent the cooperative black-hole attack. A cooperative black-hole attack is when the several malicious nodes acts together to produce attack. It is based on the modified AODV (Ad-hoc on demand distance vector) routing protocol [7]. This method makes use of the Data Routing Information (DRI) table along with the cache and current routing tables. It consists of from and through routing information of every node, so that source node makes use of these nodes while transmitting. It is only for the black-hole attacks and there is a need to implement mechanism for gray-hole attack which is the variant of black-hole attack.

Next the improvement is for providing fault tolerant Ad hoc routing service in the adversarial environments. The method is called Best-effort Fault-tolerant Routing (BFTR) service [8]. It is similar to DSR. It evaluates the routing performance of a path by the end to end behavior of nodes. The goal of BFTR is to provide packet routing service with high delivery ratio and low overhead in presence of misbehaving nodes. BFTR provides an efficient and uniform solution for a cooperative malicious node by assuming very few security conditions. Its drawback is that it does not detect any malicious node along the route from source to destination.

Next a mechanism is provided for defending against collaborative packet drop attacks on MANETs. In this method they design a hash function based method to generate node behavioral proofs that contain information from both data traffic and forwarding paths. There is only some of the computations are in the intermediate node. This method is very strong for the collaborative attacks [9]. It is not applicable to gray-hole attacks. Therefore the improvement has to be done for the gray-hole attacks.

VIII. CONCLUSION

As mechanism based on the demand distance vector routing protocol it can easily detect the malicious nodes easily hence avoids the black-hole attack but it cannot detect the cooperative black-hole attacks. This leads to unreliable communication. BFTR provides the efficient solution for the cooperative black-hole attack but it does not detect the malicious node. It just avoids the malicious nodes along the path and it is not applicable to gray-hole attacks. In order to overcome the gray-hole attacks a scheme is introduced which makes use of proactive and reactive routing protocols. It makes use of valuable points of both proactive and reactive protocols.

REFERENCES

[1] R. Kaur and J. Singh "Towards the security against the Malicious node attack in Mobile Ad hoc Network" Intl. J. Advanced research in Computer. Sci. and software engineering, vol. 3, issue 7, July 2013.
[2] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.
[3] M. Kumar, A. Bhushan and A. Kumar "A study of Wireless Ad-hoc network attack and routing protocol attack" Intl. J. Advanced research in Comput. Sci. and software engineering, vol. 2, issue 4, April 2012.
[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.
[5] A. Baadache and A. Belmehdi, "Avoiding black-hole and cooperative black-hole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.
[6] David B. Johnson and D. A. Maltz "Dynamic source routing in Ad hoc wireless networks" Comput. Sci. dept. Carnegie Mellon University.
[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative black-hole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.
[8] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp. 367– 388, 2004.
[9] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.
[10] N. Kaur and M. Joshi "Implementing MANET security using CBDS for combating sleep deprivation & DOS attack" ISSN no 2277-8136, June 2014.
[11] V. Rani "A study on Ad-hoc network: A review" Computer, Sci Dept. ISSN vol 3, March 2013.

