Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

Review on MANETs: Characteristics, Applications, Security Issues, Challenges and Attacks

Shilpa S G[1], Revathi K M[2]
Asst.Prof, Dept. Of CSE, DBIT, Bengaluru,India
Email:shilpasg.06@gmail.com

***Abstract*—Mobile Ad hoc Network (MANET) is a dynamic wireless network which composed of mobile nodes without any fixed infrastructure or centralized supervision. Manets are much vulnerable to security attacks because of no trusted central authority and network configuration changes dynamically due to mobility in node. Efficient and intelligent routing protocols are required for variations in network environment such as complexity, partitioning of network and size of network. In this paper we provide the characteristics of MANETs, security attacks and an overview of routing protocols to alleviate these security vulnerabilities.**

***Index Terms*— MANETs, Security, Attacks & Routing Protocols.**

I. INTRODUCTION

A mobile ad hoc network (MANET) (Fig. 1) is a dynamic self-configuring wireless network of mobile devices which are characterized by dynamic topology and no fixed infrastructure. Multi hop communication is one of feature of Manets where each node uses intermediate nodes to forward packets to the destined nodes which are not in their communication range. These devices are freely moving arbitrarily as a result they can interact with each other though there is no strictly defined structure or centralized administration , using wireless connections. These networks are fully distributive and can be freely works at any place without taking help of any fixed infrastructure and provide access points or base stations. Due to mobility nature of nodes the network topology keeps changes frequently and unpredictably over time. Routing functions are incorporated in mobile nodes as there is no centralized network, so all the networking functionalities are carried out by nodes themselves. The figure shown below is basic simple ad-hoc network having mobile nodes

The manets are framed with the following features: Multi hop communication, dynamic network topology, light-weight terminals, distributed operation, loop free, bandwidth constraints, autonomous terminal, energy constrained nodes, limited security, Quality of Service support. The set of applications for manets is miscellaneous (ranging from large scale networks to small scale). Manets are suitable for applications in which no infrastructure is required such as military battlefield, commercial sector and mining operations etc. Due to its wireless and distributed nature there is a great challenge for system security designers. In the last few years security problems in manets have attached much attention; most of the research efforts focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or intrusion

Grenze ID: 02.ICCTEST.2017.1.126

detection and response.

First section will describe security goals required for secure routing in MANET. Second Section gives detailed description of various attacks on MANET. Third section will provide various solutions proposed by the researchers against these attacks. Last section provides future directions for a secure MANET

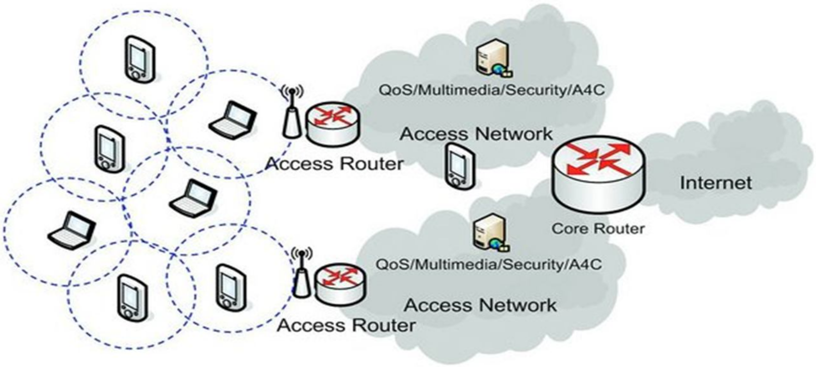

Figure 1. MANET

II. SECURITY GOALS

A crucial barrier with wireless network is its security. MANETs are more liable to security attacks because all networking functions are performed by nodes themselves. In order to provide a secure networking environment some security goals are needed. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment.

Confidentiality:

It ensures that only the authorized nodes should be able to interpret the transmitted data. No other node except sender and receiver node can read the information. This is implemented through data encryption techniques.

Integrity:

Data should not change during the transmission process, i.e., Message being transmitted is never altered.

Availability:

It ensures that the services are only accessible to authorized nodes and should be available even in the presence of the attacks. Availability applies both the data and services as an assurance of survivability despite a DOS attack, energy starvation attacks and anode misbehavior.

Authentication:

Every transmitting or receiving node has its own signature. It is essential to check whether the nodes participating in the communication are genuine or not. Nodes involved in network communication have to prove their identities or the origin of communication as what they have claimed using some techniques so as to ensure the authenticity and identify the impersonators.

Authorization:

It is a process in which an entity is issued a credential, which means different privileges and permissions it can have and it cannot be falsified by the certificate authority. Authorization is used to assign different access rights to different level of users.

Non-repudiation:

It ensures that the sender and receiver of a message should not deny that they have sent or received such message. This is helpful when we need to differentiate a node with some abnormal function is compromised or not.

All these security mechanisms must be implemented in any ad-hoc networks so as to ensure the security of the transmissions along that network.

III. Mobile Adhoc Network Attacks

Providing security in wireless Adhoc networks is a major challenging issue. Due to the inherent property of the MANETs like infrastructure-less, self-configuring, dynamic topology there exists some vulnerability in MANETs which can be attacked by malicious and undesirable nodes to disturb the network environment. These attacks can be classified mainly into two types:

Passive Attacks

In this attack the attacker doesn’t disrupt the function of routing protocol if the network but tries to snoop the data exchanged in network without altering it. Achieving confidentiality will be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

Active Attacks

In this attack, the attacker injects the arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication or attract packets which are routed to other destined nodes. Here the main aim of the attacker is to attract all packets in the network for analysis or to disable the network. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be classified into external and internal.

- External Attacks: The main objective of the attacker is to cause congestion, broadcast false routing information or disrupt nodes from providing services.
- Internal Attacks: These attacks are initiated by the authorized nodes in the network. The internal nodes are compromised nodes when the external attackers hijack the authorized nodes and utilizing them to initiate attacks against the network.

The internal attacks are more dangerous and hard to detect than external attacks. In internal attacks the malicious nodes are the gentle users of adhoc network and they can easily share the authentication information and get protected from security mechanisms. The adversaries make use of these compromised nodes get normal access to network services. Therefore we should pay more attention internal attacks initiated by the compromised nodes when we consider the security challenges.

In the following, we discuss the some of the main attack types that emerge in the mobile ad hoc networks:

Black hole Attack

In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

Wormhole Attack

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

Sink-hole Attack

The idea of the attacker in this attack is to attract all the network traffic towards itself. The attacker executes this attack by making the neighboring nodes believe that the shortest path to the destination is through it. This attack causes the other nodes to relay all the traffic through the malicious node so that the attacker can modify, fabricate or just listen to the received packets.

Rushing Attack

The purpose of this attack is to include the malicious node in the routing path. During the route discovery phase the RREQs are forwarded by the malicious nodes to the neighbors of the target node. These RREQs are quick to reach the neighboring nodes. When a neighboring node receives this hurried RREQ from the attacker, it will not forward any request originated from the source node that initiated route discovery. By executing this attack the attacker includes itself in the routing table and can then tamper with the packet.

Gray hole Attack

This attack is an advanced form of black hole attack. A malicious node leaves out selective packets and forwards the other packets, depending on the source or the destination of packets. Another kind of gray hole attack may behave maliciously for a given interval by dropping all packets then it switches to normal behaviour later on. This attack defeats trust-based mechanisms and the detection of malicious node becomes more complicated to attain

Denial of Service (DoS) Attack and Flooding

The aim of this attack is to cripple the smooth functioning of the network. This attack is accomplished by continually sending packets into the network causing the targeted node in the network to process them and keep them occupied resulting in the crashing of that node. By executing this attack, the attacker keeps the targeted node busy in processing its fabricated packets and depriving the legitimate RREQs to be dropped. This attack can cause the network infrastructure to collapse.

Sybil Attack

If a malicious node pretends to be some nonexistent nodes, it behaves as group of malicious nodes conspiring together, which is called a Sybil attack. The sybil node can find an identity with these two ways either by stealing other node's identity or by producing fake identities. This attack damages geographic routing protocols, and node localization.

IV. Routing Protocols In MANET

The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the data packets through an internetwork. Efficiency of the route is measured using various parameters like traffic, number of hops, energy of nodes, trust values, security etc. The main goal of routing protocols is to maximize network throughput, minimize delay, maximize network lifetime and maximize energy efficiency.

The routing protocols in MANET can be classified in to three main categories:

Proactive routing protocol:

In this scheme every network node use the routing table to store the information of routes for all other nodes, each entry in the table contains the path to the destination with next hop node, regardless of whether the route is currently needed or not. Node has to update the table to reflect the frequent changes in network topology. But the overhead of sharing and maintaining the routing information in this routing protocol is more in high mobility networks. But whenever a packet data is needed to be forwarded the route is already known and can be immediately used. Examples: DSDV, WRP, CGSR etc.

Reactive routing protocol:

The on-demand routing protocols are based on some sort of query-reply dialog. The route for forwarding a packet to destination is discovered only on demand. In this the nodes do not need periodic transmission of topological information of the network. Firstly the node that is willing to communicate with other nodes looks up for a route in its routing table. If it is found, the routing starts immediately, otherwise the node goes for a route discovery phase. Once the route is established, it is maintained until the route is no longer used, or expired. In this routing protocol maintains only the information of active paths to the destination nodes is maintained. Examples: AODV, DSR, CBRP etc.

Hybrid Routing Protocols:

Often reactive or proactive properties of a particular routing protocol might not be enough. This protocol combines features of proactive and reactive routing protocols. Examples: ZRP, ZHLS.

Some of the proactive and reactive routing protocols are discussed briefly:

Destination Sequence Distance Vector Routing (DSDV)

The destination sequenced distance vector routing protocol (DSDV) is a table driven or proactive routing protocol [10]. It is extension of conventional bellman ford routing algorithm. This protocol uses a new attribute, sequence number, to each route table entry at each node. Every node in the network maintains a routing table which contains information about all destinations i.e. sequence number, the total number of hops needed to reach these nodes and next hop to reach the destination. The route with the recent sequence number is considered as a fresh route. In order to maintain reliability each station transmits and updates its routing tables periodically. DSDV provides an option of route updates using the full or incremental update strategies. By using Sequence number DSDV protocol guarantees the loop free routes; it also keeps only the optimal path to every node, rather than keeping multi paths which will help to reduce the total size of routing table. However, it becomes difficult to maintain routing table's advertisements for large networks using this technique.

Optimal Link State Routing (OLSR)

OLSR is a proactive routing protocol and it is an optimization of pure link state protocol by reducing the global broadcast operation or flooding. OLSR defines multipoint relay to minimize the broadcast packets which are flooded in the network by reducing the number of retransmissions at same region. OLSR uses MPR for two reasons: First it reduces the size of the control packets: instead of all links it declares only a subset of links with its neighbors who are selected as MPR and secondly it minimizes flooding of control traffic by using the selected nodes called multipoint relays to defuse its messages in the network. Each node has the knowledge as to for which node it acts as a MPR as they periodically announce this information in their control messages. The routing overhead in OLSR is reduced as MPR alone is used for retransmitting control messages. This routing protocol is best for large and dense network as optimization is done by using MPR nodes.

DSR

Dynamic Source Routing protocol (DSR) is designed for multi-hop wireless ad hoc networks [13]. This protocol made up of two main mechanisms “Route Discovery” and “Route Maintenance” that makes it self-configuring and self-organizing. Route discovery stage is used to discover the routes from source node to destination. A node caches multiple routes to any destination which support rapid reaction to routing changes as another cached route can be tried if the one it has been using should fail. It also avoids the overhead of need to perform a new Route Discovery each time a route in use breaks. In DSR, data packets store information about all the intermediate nodes in its header to reach at a particular destination. Intermediate routers don't need to have routing information to route the data packets, but they save routing information for their future use. The intermediate node which detects broken link through route maintenance also notifies the source node using a route error packet identifying the link over which packet cannot be forwarded.

AODV

The AODV (Ad hoc On-Demand Distance Vector) routing protocol [3] is another well-known reactive protocol and it works purely on demand basis. AODV starts route discovery by broadcasting a route request packet to its neighbouring nodes. After receiving the RREQ from source node, the intermediate nodes forwards this packet to their next node and also creates a reverse route for itself back to the source node. Once the route request packet reaches a node with a route to destination node that node generates a route reply that contains the number of hops necessary to reach destination and the sequence number for destination most recently seen by the node generating the reply. The state created in each node along the path from source to the destination is hop-by-hop state; that is each node remembers only the next hop and not the entire route, as would be done in source routing. The main features of AODV are quick response to link breakage in active route and loop-free routes by using destination sequence numbers.

V. Conclusion

Self-organization is a key property of ad-hoc networks. Besides authentication, confidentiality, integrity, availability, access control, and nonrepudiation being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as location confidentiality, cooperation fairness and the absence of traffic diversion. This paper gives the overview of the characteristics, challenges and solutions for the security risks in Manets. Security is a major issue in mobile adhoc networks as they are vulnerable to many types of attacks. Active attacks are considered more dangerous as they disrupt the proper operation of the MANET. While passive attacks are not necessarily harmful as standalone attacks, they could be used as a first step to more serious and harmful attacks like black hole attacks. Thus, passive attacks should not be overlooked or ignored.Some of such active attacks has been discussed in this study.

Classification of routing protocols for MANET has been done on the basis topology of the network i.e. proactive or table- driven and reactive or demand- driven. Few routing protocols belonging to each type of classification has been discussed in this survey. Thus, the Manet routing protocols are designed based on the application area and environment and it is not possible to design a single protocol which is suitable for all Manets.

REFERENCES

[1] Mohit Kumar and Rashmi Mishra "An Overview of MANET: History, Challenges and Applications" , Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[2] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044

[3] C. Siva Ram Murthy, and B.S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall communications engineering and emerging technologies series Upper Saddle River,New Jersey, 2004.

[4] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi,"A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET), International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013 DOI: 10.7763/

[5] P. Visalakshi, S. Srikanth Balaji. An overview of security factors of routing in Mobile Adhoc Network (MANET). International Journal of Modern Engineering Research (IJMER).

[6] J. Godwin Ponsam, Dr. R.Srinivasan, A Survey on MANET Security Challenges, Attacks and its Countermeasures, Web Site: www.ijettcs.org Email: editor@ijettcs.org, Volume 3, Issue 1, January – February 2014 ISSN 2278-6856

[7] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.RajasekhararaoA Survey on Attacks and Defense Metrics of Routing IJACSA,Vol. 2, No.3, March 2011