ABSTRACT:- Manets are extensively used these days for communication and there are various communication networks with different standards and computing techniques and as days are passing by the size of manet is increasing day by day and its expansion is inevitable due to its high penetration and popularity for the usage of mobile application but at the same time it is also prone to many attacks and network failure due to technical vulnerability of the network. The most common attack is isolation of a node from the main network leading a dos attack for that particular node. So due to which a legitimate/genuine node gets isolated from the network. Therefore we need a detection mechanism which would need to overcome such scenarios.

Keywords: types of attacks on manet, security, malicious nodes

INTRODUCTION

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. A MANET is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In a MANET, nodes within each other’s wireless transmission ranges can communicate directly; however, nodes outside each other’s range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers; the attacker could bring down high level services.

Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

Integrity: Message being transmitted is never altered.

Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

SECURITY ATTACKS

1. External vs. Internal attacks

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

2. Passive Attacks

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn’t
get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead.

2.1. Eavesdropping
Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

2.2. Traffic Analysis & Monitoring
Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

3. Active Attacks
An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication.

3.1. Jamming attack
Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

3.2. Wormhole attack
An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols.

3.3. Blackhole attack
The blackhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks.

3.4. Routing Attacks
There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network.

3.4.1 Routing Table Overflow: In this attack, the attacker attempts to create routes to nonexistent nodes.

3.4.2 Routing Table Poisoning: Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.

3.4.3 Packet Replication: In this attack, an adversary node replicates stale packets.

3.4.4 Route Cache Poisoning: In this case each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past.

3.4.5 Rushing Attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. An adversary node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same Route Request packet can react. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node.

4. Other attacks

4.1 Denial of Service attack
Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. For example, consider the following Fig. 3. Assume a shortest path exists from S to X and C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial of service attack. Suppose S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet toward X with the source route S ---> A ---> B ---> M ---> C ---> D ---> X contained in the packet’s header. When M receives the
packet, it can alter the source route in the packet’s header, such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet to X. Since X cannot hear C, the transmission is unsuccessful.

4.2 Sybil attacks

A Sybil attack is one in which an attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous entities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically.

An entity on a peer-to-peer network is a piece of software which has access to local resources. An entity advertises itself on the peer-to-peer network by presenting itself with an identity. More than one identity can correspond to a single entity. In other words the mapping of identities to entities is many to one. Entities in peer-to-peer networks use multiple identities for purposes of redundancy, resource sharing, reliability and integrity. In peer-to-peer networks the identity is used as an abstraction so that a remote entity is aware of identities without necessarily knowing the correspondence of the identities with their local entities. By default, each distinct identity is usually assumed to correspond to a distinct local entity. In reality many identities may correspond to the same local entity.

A faulty node or an adversary may present multiple identities to a peer-to-peer network in order to appear and function as distinct nodes. By becoming part of the peer-to-peer network, the adversary may then overhear communications or act maliciously. By masquerading and presenting multiple identities, the adversary can control the network substantially. This attacks aims at network services when cooperation is necessary, and affects all the auto configuration schemes and secure allocation schemes based on trust model as well. However, there is no effective way to defeat Sybil attacks.

METRICS USED IN DETECTION

1. Throughput

Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. Throughput is essentially synonymous to digital bandwidth consumption.

2. PDR

It the ratio of number of packet actually delivered without duplication to destination verses the number of packet supposed to be received. This number represent the effectiveness and throughput of a protocol in delivering data to the intended receiver within the network.

\[ PDR = \frac{\text{TOTAL NO. OF PACKET RECEIVED}}{\text{TOTAL NO. OF PACKET SEND}} \]

3. ENERGY CONSUMPTION

The total energy consumed in the network is energy consumption. It is measured in whr.

4. NUMBER OF COLLISIONS

In a network, when two or more nodes wants to transmit data at the same time network collision occurs. When a packet collision occurs the packet is either discarded or sent back to their originating stations and again retransmitted in a times based sequence to avoid collisions. Collisions can result in loss of packet integrity or can impede the performance of a network. This metric is used to measure such collision in the network.

5. PLR

Packet loss ratio =

Number of lost packet / (Number of lost packet + Number of packets received successfully)

Knowing your packet loss ratio will help you determine if the slowness issue is based on your connection to the nodes, or it stems from a different problem. Poor communication connections can be caused by a number of reasons, so using a packet loss ratio formula is a part of the detection process.

PROPOSED METHOD

Our proposed method primarily based on detection of DOS attacks and isolating these malicious nodes from the network, so that rest of the genuine nodes can work peacefully.
Sybil attack: If a malicious node impersonates some nonexistent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack. This attack aims at network services when cooperation is necessary, and affects all the auto-configuration schemes and secure allocation schemes based on trust model as well. However, there is no effective way to defeat Sybil attacks.

FLOWCHART

The flowchart is divided into 2 parts

1. Normal flow
In this part, the flowchart shows the working of the algorithm when no denial of service attacks or any other kind of threats is there in the network.

In the given figure node 3 is the target node and node 1, node 2, node 4 are illegitimate nodes and node 5, node 6 are genuine nodes. Node 5, node 6 are communicating properly with all other nodes present on the network. But node no. 1,2,4 are busy in sending requests to node no. 3 so that this node will get busy in handling their requests and sending back ACK (acknowledgement). So that when any genuine node send request to node 3 its communication channels are already so fill that it will not be able to reply it back hence resulting a DOS ATTACK (DENIAL OF SERVICE ATTACK).
2. In attack mode flow

In this part, the flowchart shows the working of the algorithm when denial of service attacks or any other kind of threat is there in the network. The flowchart for the attack mode originates from the normal mode from the node B.

![Flowchart](image)

**B**

- Introduce attack
  - Introduce illegitimate nodes that broadcasts data to a specific node (target node)

- Illegitimate nodes do not change their position inspite of fact that they are part of MANET

- They broadcast and wait for ACK from the target node; if ACK is received they will establish the link with target node

- Similarly more nodes attacks and establish links, isolate target node from network

- And our algorithm is to detect and isolate these nodes from the network

**RESULT**

*Graph 1*

It is clear from the first graph that, in attacks there is reduction in throughput of system with respect to message arrival time

The 2nd graph shows that when the network is running smooth and fine without any introduction of any attack there is normal communication of packet being send and receive which leads to packet delivery ratio above 90% which can be seen in the session of IDS but when there is an attack occurring there is a sudden dip in throughput as well as PDR about 10% less than normal.

*Graph 2*
**Graph 3**

3rd graph is also a reflection of how no. of message packets are affected when there is an attack being introduced. This graph shows how many packets have been lost (control message) when there was no. of attacks and after attack.

**Graph 4**

4th graph shows that there are less checksum errors before attack and after attack there are increase in checksum errors.

**CONCLUSION**

This paper concludes that with the introduction of any attack in any network there is a reduction of throughput in the network. Packet delivery ratio also drops and there is an increase in checksum errors and packet loss ratio. So it is very important for any network to detect these malicious nodes and isolate them from the network for the proper and smooth functioning of MANET.

**FUTURE SCOPE**

There are other possible attacks also which needs to be understood and detection mechanism needs to be researched build and made. So therefore in future we suggest that some bio inspired defense mechanism and detection mechanism to be explored, in the way nature helps to detect and defend anomalies in our system, similarly we should be able to develop a mathematical model for detection many types of attacks.

**REFERENCES**


