A Study of Active and Passive Attacks In Manet
Sonia Verma¹ Jigyasa Sharma² Dr. Sima³
¹,²,³DAV College For Girls, Yamuna Nagar, Haryana

Abstract— MANET (Mobile Ad-Hoc Network) is self-created and self structured by a collection of mobile nodes, interrelated by multiple-hop wireless paths in a strictly peer to peer style. DSR (Dynamic Source Routing) is an on-demand routing protocol for wireless ad hoc networks. Route caches in intermediate mobile node on DSR are used to reduce flood of route requests. But when the size of the network increase, node mobility and local cache of every mobile node cached route quickly become old or inefficient. The other major problem of DSR is that the route maintenance method does not locally repair a broken link and old cache information could also result in inconsistencies during the route finding and rebuilding phase. So to deal this problem, we have proposed an optimized cache coherence handling method for on-demand routing protocol (DSR).

Key words: MANET, DSR

I. INTRODUCTION

A mobile ad hoc network (MANET) is an endlessly self-configuring, infrastructure-less network of mobile in which devices are connected through wireless connection. In this Network Independent Mobile nodes can communicate through radio waves. The Mobile nodes that are in the range of radio waves can directly communicate with each other on the other hand the nodes that are not in the range of radio waves they need the intermediate nodes to route their packet.

All devices in a MANET are free to travel independent in any direction, and will change its links to other devices regularly. Mobile Ad-hoc Networks (MANETs) are future wireless networks consisting entire mobile nodes that communicate and move without base stations. It is IETF (Internet engineering task force) work group. This group was created in 1998 for standardize the routing protocols based on Internet protocol for ad hoc network, phones etc. It is group of large independent wireless nodes interconnected each other on peer to peer basis in the surroundings without any infrastructures. These Networks will use different routing protocols for user and application traffic generated by the network. The Main challenge in build a MANET is equipping each device to continually maintain the information required to properly route traffic. These Types of networks may operate by themselves or may be connected to the wider Internet. These may contain one or multiple and different devices that can both transmit and receive communication in between nodes. MANETs Network usually has a routable network environment on the top of Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, network. MANETs circa 2000-2015 communicate at radio frequencies (30 MHz - 5 GHz).

Fig. 1: Architecture for MANET

II. CHARACTERISTICS OF MANET

A. Autonomous

No centralized administration entity is obtainable to manage the operation of the various mobile nodes.

B. Dynamic Topology

Nodes are movable and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

C. Device Discovery

Identifying related newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

D. Limited Resources

Mobile nodes rely on battery power, which is a limited resource. Also storage capacity and power are severely limited.

E. Scalability

Scalability can be defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.

F. Limited Physical Security

Mobility implies higher security risks like peer-to-peer specification or a shared wireless medium accessible to each legitimate network users and malicious attackers.

G. Infrastructure Less and Self Operated

Self healing feature demands MANET must to adjust itself to blanket any node moving out of its vary.

H. Poor Transmission Quality

This is AN inherent drawback of wireless communication caused by many error sources that end in degradation of the received signal.

III. APPLICATIONS OF MANETs

The use of a MANETs is easy due to the absence of setting up any infrastructure for communication. Mostly such kind of networks is required in military application and emergency rescue operations. But slowly MANETs have entered with the areas of gaming, sensing, and conferencing, collaborative and distributed computing.
a) **Military Services**: Military services area unit one among the foremost common application space of mobile unplanned networks wherever installation of any mounted infrastructure isn’t attainable within the enemy territories. Here, the troopers area unit thought-about to be the mobile nodes. therefore the network is needed to stay connected albeit the troopers move freely.

b) **Emergency Services**: These arise as a result of natural disasters when the entire communications infrastructure is in out of order (for example, Tsunamis, hurricanes, earthquake etc.) where restore communications quickly is essential. By using ad hoc networks, an infrastructure can be set up in hours instead of days or weeks required for wire-line communications.

c) **Education**: Universities and college campus settings. Virtual classrooms, Temporary communications during meetings or lectures.

d) **Sensing**: Sensor network can be a special case of ad hoc networks where mobility is generally not consider. Each sensor is equipped with a transceiver, a tiny micro controller and an energy source. The sensors are used to sense the ecological circumstance such as temperature, pressure, humidness etc..

e) **Personal Area Networking**: Personal communication devices like laptops, PDAs, mobile phones produce a network to share knowledge among each other referred to as the private space Network (PAN). The PAN covers a really short range for communication and may be use for ad hoc communication along with the devices or for connecting to a backbone network.

IV. **SECURITY ATTACKS IN MANETS**

Security means protecting the privacy, availability, integrity and non repudiation. Security implies the identification of possible attacks, threats and susceptibility of a certain system from unauthorized access, use, modification or destruction. The attack may alter, release, or deny data. The attacks on the MANETs can be broadly classified into two categories.

1) Passive attacks
2) Active attacks

![Types of Attacks](fig2.png)

**A. Passive Attack**

In this attack, the intruder only performs some kind of monitoring on certain connections to get information of traffic without inject any fake information without affecting the system resources and normal functioning of the network. This type of attack serves the attacker to get information and makes the footprint of the invaded network in order to apply the attack successfully.

The different types of passive attacks are:

1) **Eavesdropping (Information leakage)**: In this attack node merely observes the unrevealed info. This info is often later utilized by the malicious node. The key info like location, public key, non-public key, password etc. are often fetched by eavesdropper.

2) **Traffic Analysis**: In MANETs the info packets furthermore as pattern each square measure necessary for adversaries. as an example, counsel regarding configuration will be derived by analyzing traffic patterns. Traffic analysis also can be conducted as active attack by destroying nodes, that stimulates organization within the network, and valuable information regarding the topology will be gathered.

3) **Snooping**: Snooping is unauthorized access to a different person’s information. It's like eavesdropping however isn't essentially restricted to gaining access to knowledge throughout its transmission. Snooping will include casual observance of an e-mail that seems on another's visual display unit or observation what some other person is typewriting. Additional refined snooping uses code programs to remotely monitor activity on a pc or network device.

Malicious hackers (crackers) often use snooping techniques to watch key strokes, capture passwords and login data and to interrupt email and alternative personal communications and information transmissions. Companies generally eavesdrop on staff lawfully to watch their use of business computers and track web usage. Governments might eavesdrop on people to gather data and stop crime and act of terrorism. Passive attacks area unit terribly tough to find as a result of they are doing not involve any alteration of the information.

The stress in dealing with passive attacks is on prevention rather than detection. One of the solutions to the problem is to use powerful encryption techniques to encrypt the data being transmitted, thereby making it impossible for the attacker to get secret information.

**B. Active Attacks**

An active attack attempts to modify or destroy system resources and the data being exchanged in the network by injecting or modifying arbitrary packets. An active attack involves information interruption, modification, or fabrication. Active attacks can be either internal or external.

1) **Flooding attack**: In this attack, invader exhausts the network resources, such as bandwidth and to consume a node’s resources, such as computational and battery power or to disturb the routing operation to cause severe degradation in network performance.

2) **Black hole Attack**: In this attack, once a malicious node listens to a route request packet within the network, it responds with the claim of getting the shortest and therefore the freshest route to the destination node.
notwithstanding no such route exists. As a result, the malicious node simply misroute network traffic to that and so drop the packets temporary to that
3) Wormhole attack: In this attack, an attacker receives packets at one purpose within the network, “tunnels” them to a different purpose within the network, then replays them into the network from that point. This tunnel between 2 colluding attacks is thought as a hole . Wormholes ar hard to discover as a result of the trail that's used to expire info is sometimes not a part of the particular network. Wormholes area unit are dangerous as a result of they will do injury while not even knowing the network.
4) Gray-hole attack: It is also called routing misbehavior attack that results in dropping of messages. Gray-hole attack has 2 phases. within the 1st section the node advertise itself as having a legitimate route to destination whereas in second section, nodes drops intercepted packets with a particular chance.
5) Link spoofing attack: In spoofing attack, a malicious node advertises pretend links with non-neighbors to disturb routing operations.
6) Malicious code attacks: It includes Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.
7) Repudiation attacks: Repudiation means a denial of participation in all or part of the communications. Many of encoding mechanism and firewalls used at completely different level aren't enough for packet security. Application layer firewalls might occur to offer security to packets against several attacks. for instance, spyware detection code has been developed so as to observe mission essential services

V. CONCLUSION

The advancement within the field of mobile computing is driving a replacement various means for mobile communication, during which mobile devices form a self-creating, self-organizing and self-administering wireless network, known as a mobile ad hoc network. Mobile ad hoc networks are typically a lot of at risk of physical security threats than fixed or hardwired networks. This paper throws a light on totally different ideas of MANETS which will facilitate researchers to the most. Its intrinsic flexibility, lack of infrastructure, simple readying, auto-configuration, low price and potential applications create it a vital a part of future pervasive computing environments. because the involvement goes on, particularly the requirement of dense preparation like battlefield and detector networks, the nodes in ad-hoc networks are going to be smaller, cheaper, a lot of capable, and are available all told forms. In all, though the widespread preparation of ad-hoc networks continues to be year away, the analysis during this field can continue being very active and inventive.

REFERENCES