# Implementation of MANET Application, Attack and Challenges

N. Bhaskar
N. Sakthivel, MCA
Department of master of computer application

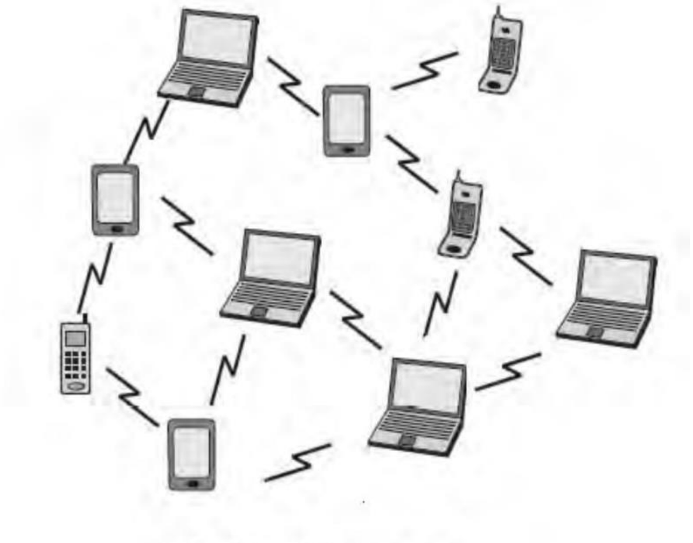
***Abstract*: Advancement in the field of internet due to wireless networking technologies gives rise to many new applications. Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications. This paper provides insight into the potential applications of ad hoc networks, various attacks and discusses the technological challenges that protocol designers and network developers are faced with.**

***Keyword : MANET; Applications; Attacks and Challenges***

## INTRODUCTION:

MANET is a self configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move haphazardly and organize random themselves arbitrarily. Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET. MANET have given rise to many applications like Tactical networks, Wireless Sensor Network, Data Networks, Device Networks, etc. With many applications there are still some design issues and challenges to overcome. The main goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes which may be combined routers and hosts--they form the network routing infrastructure in an ad hoc fashion. Lot of security vulnerabilities in a wireless environment, such as MANET, has been identified and a set of countermeasures were also proposed. However, only a few of them provide a guaranty which is an orthogonal to security critical challenge. Taking these factors into concern, the main vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks

by incorporating routing functionbile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing,



Mobile ad hoc network

## 1. History of MANET:

Basically, MANET can be categorized into first, second and third generations. The first generation came up with "packet radio" networks ( PRNET), and were sponsored by DARPA in the early 1970s. It has evolved to be a robust, reliable , operational experimental network. The PRNET used a combination of ALOHA and CSMA approaches for medium access, and a kind of distance-vector routing to provide packet-switched networking to mobile battlefield elements in an infrastructureless, hostile environment. The second generation evolved in early 1980's when SURAN (Survivable Adaptive Radio Networks) significantly improved upon the radios (making them smaller, cheaper, power-thrifty), scalability of algorithms, and resilience to electronic attacks. Important developments during this period include GloMo ( Global Mobile Information System) and NTDR ( Near Term Digital Radio) The goal of GloMo was to provide office-environment Ethernet-type multimedia connectivity anytime, anywhere, in handheld devices. Channel access approaches were now in the CSMA/CA and TDMA molds, and several novel routing and topology control schemes were developed. The NTDR used clustering and link- state routing, and self-organized into a two-tier ad hoc network. Now used by the US Army, NTDR is the only "real" (non-prototypical) ad hoc network in use today. The third generation evolved in 1990's also termed as commercial network with the advent of Notebooks computers, open source software and equipments based on RF and infrared. IEEE 802.11 subcommittee adopted the term "ad hoc networks." And the concept of commercial (non-military) ad hoc networking had arrived. Within the IETF, the Mobile Ad Hoc Networking (MANET) working group was horn, and sought to standardize routing protocols for ad hoc networks. The development of routing within the MANET working group and the larger community forked into reactive (routes on- demand) and proactive (routes ready-to-use) routing protocols 141. The 802.1 1 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable, if not optimal, for building mobile ad hoc network prototypes out of notebooks and 802.11 PCMCIA cards. HIPERLAN and Bluetooth were some other standards that addressed and benefited ad hoc networking.

## 2. Applications of MANET:

With the increase of portable devices as well as progress in wireless communication, ad- hoc networking is gaining importance with the increasing number of widespread applications in the commercial, Military and private sectors. Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure.

Military Sector : Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field

Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. This may be because all of the equipment was destroyed, or perhaps because the region is too remote. Rescuers must be able to communicate in order to make the best use of their energy, but also to maintain safety. By automatically establishing a data network with the communications equipment that the rescuers are already carrying, their job made easier. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

Low Level: Appropriate low level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

Data Networks: A commercial application for MANETs includes ubiquitous computing. By allowing computers to forward data for others, data networks may be extended far beyond the usual reach of installed infrastructure. Networks may be made more widely available and easier to use.

Sensor Networks: This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad-hoc network.

| MANET security Layer | Attacks |
|---|---|
| Application Layer | Malicious code, Repudiation |
| Transport Layer | Session hijacking, SYN Flooding |
| Network Layer | Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing etc. |
| Data Link Layer | Traffic analysis and monitoring. |
| Physical Layer | Traffic Jamming, Eavesdropping |

Attacks on mobile ad hoc networks can be classified into following two categories:
Passive and Active attacks

1) Passive attack: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information . This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:

Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

Traffic Analysis: In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered.

Snooping: Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism. Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function.

1) Active attack: in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker’s threat can be performed

## CONCLUSION:

The evolution in the fields of mobile computing is driving a new alternative of mobile communication,in which mobile device from a self –creating,self-organising and self administering wireless network,called a mobile ad hoc network.This generally more vulnerable to physical security hardwired network.In all,althrough the widespread development of ad-hoc network is still year away,the research in this field will continue being very active and imaginative.

## REFERENCE:

1. Jeoren hoebeke,Ingird Moerman,Bart Dhoedt and Piet Demester “An Overview of Mobile ad hoc Network:Application & Challenges.

2. Krishna Moorthy Sivalingam, “Totorial on Mobile Ad Hoc Network”,2003.

3.Chalmtac, I, Conti, M, and Liu,J.j.-N. Mobile ad hoc network:imperatives and Challenges.Ad Hoc Network,1(1),2003,pp. 13-64.