

# Mobile Ad-Hoc Network: Applications and Challenges

<sup>1</sup>Karan Singh, <sup>2</sup>Anil Kumar

<sup>1</sup>Research Scholar, Department of Comp. Sc. & App. K.U., Kurukshetra, Haryana, INDIA

<sup>2</sup>Assistant Professor, Department of Comp. Sc., University College, K.U., Kurukshetra, Haryana, INDIA

<sup>1</sup>karanola123@gmail.com, <sup>2</sup>taparwal80@gmail.com

**Abstract:** Mobile Ad-hoc network (MANET) is decentralized, without any fixed infrastructure, temporarily and multi-hop network, which adds many wireless mobile nodes (laptops, sensors etc.). MANETs formed by many wireless hosts without central control and established their own dynamic network. Mobile Ad-hoc Network makes a network that is without any pre-existing communication infrastructure e.g. disaster recovery environments. There are many research fields in wireless networks like routing protocols, bandwidth utilization, synchronization and power consumptions etc. The most research area in MANETs is its dynamic topology and used routing protocols. Here only introduction, characteristics, application and challenges are discussed.

**Keywords:** Routing protocol, MANET.

## 1. INTRODUCTION

Wireless Networks provides connection flexibilities for communication among users and offers dynamic network which is movable with its nodes. In MANET approach network can be move from one place to another without making any wired network. However, Wireless networks can be broadly divided into two parts [1] (see in Figure 1):

- 1) Infrastructure Based Networks (With Access Point),
- 2) Infrastructure Less Networks (Without Access point OR Ad-hoc Networks).

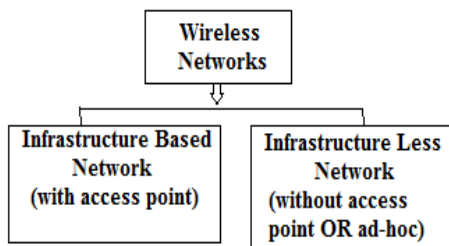


Figure 1: Wireless Networks Categories

**1.1) Infrastructure Based Networks:** Infrastructure Based Network is central idea of using an Access Point (AP) [2]. This AP can add a node to its network and manages overall communication between nodes. Main disadvantages of this AP based wireless service is maintaining and making Routing Tables for all nodes. AP keeps ready its BSS (Basic Service Set), for communication within network (see in Figure2).

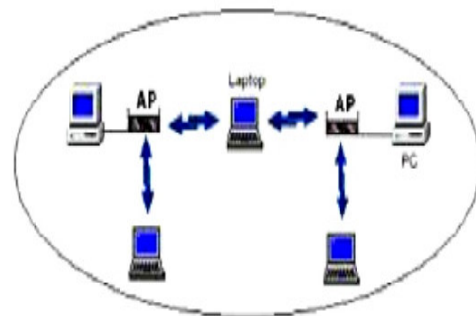


Figure 2: Infrastructure Based Network (with Access Point)

**1.2) Ad-hoc Networks:** Ad-hoc Networks (see in Figure 3) operates without any fixed infrastructure (infrastructure less) [3] and without any central control. Unlike AP based networks in MANET each node within range of network acts as a point to connect for make a dynamic network. Mobility is most required feature in Ad-hoc network for makes this network movable within range. This Mobility Concept makes this network as Mobile Ad-hoc Network (MANET). MANET is a network of mobile nodes sharing a wireless channel with decentralized control. MANET has dynamic movable topology within range having bounded resources such as battery, memory, power consumptions. MANET is useful where wired network is not feasible like battlefields, natural disasters etc. The nodes which are within the transmission range of each other communicate directly otherwise messages are forwarded through intermediate nodes which are willing to forward packet hence these networks are

also called as multi-hop networks.

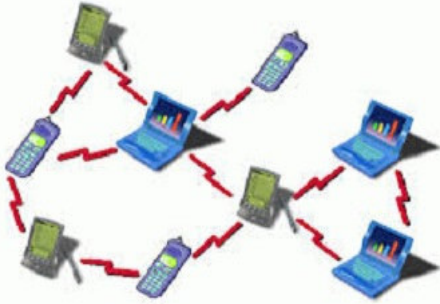


Figure 3: Infrastructure Less Network  
(Mobile Ad-hoc Network)

## 2. CHARACTERISTICS OF MANET

MANET'S are made of wireless transmitters and receivers using antennas which may be point-to-point, broad-cast etc. This ad-hoc topology having dynamic topology in nature may modify its network with time as the nodes move or adjust their transmission and reception parameters [4].

- i) Autonomous Behavior:** Each node in MANET can act as both routers (source for switching) and hosts (sink or endpoints) [5].
- ii) Distributed nature of operation:** This is decentralized in nature so the control and operation of the network is distributed among the nodes.
- iii) Multi-hop transmission:** When delivering data packets from a source to its destination out of the direct wireless transmission range, the message have to be forwarded through one or more intermediate nodes. This communication via intermediate node concept is Multi-hop transmission.
- iv) Dynamically changing topology:** Due to mobile nodes, the change in topology is frequent and dynamic in nature [5]. The connectivity in network dynamically changes as they move geometrically.
- v) Light weight features:** MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage.
- vi) Symmetric environment:** All nodes have identical features with similar responsibilities and capabilities. Every node can function as a router or host and hence it forms completely symmetric environment.
- vii) Absence of infrastructure:** Mobile ad-hoc networks are supposed to operate independently of any fixed infrastructure.

## 3. MANET's APPLICATIONS

Ad-hoc networks may be very useful in some specific areas as follows:-

- i) Military battlefield:** Ad-Hoc networking provides temporarily communication in battlefield between the

soldiers, vehicles, and military information head quarter.

- ii) Collaborative work:** For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

- iii) Local level:** Ad-Hoc networks help in sharing of information among participants at an e.g. conference or classroom and at home networks where devices can communicate directly to exchange information.

- iv) Personal area network and Bluetooth:** A personal area network is a short range, network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

- v) Natural Disaster:** MANET can be used in rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake.

## 4. MANET's CHALLENGES

Mobile Ad-hoc Networks faces many challenges some are as follows:-

- i) Packet losses due to transmission errors:** Ad hoc wireless networks faces packet loss due to factors such as increased collisions due to the presence of hidden terminals.
- ii) Mobility-induced route changes:** The network topology in an ad hoc wireless network is dynamic in nature due to the movement of nodes; hence an on-going message transfer session suffers frequent path breaks. This situation leads to frequent route changes.
- iii) Battery constraints:** Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.
- iv) Security threats:** Mobile ad hoc networks are basically exposed and open for communication and thus this leads to numerous security attacks.
- v) Limited bandwidth:** Wireless link continue to have pointedly lower bandwidth capacity than infrastructure based networks.
- vi) Dynamic topology:** Dynamic topology relationship may bother the trust rapport among nodes. The trust may also be disturbed if some nodes are detected as cooperated.
- vii) Routing Overhead:** In MANET, nodes are movable and dynamically change their location within network. So, some stale routes are produced in the routing table which leads to unnecessary routing overhead.
- viii) Hidden terminal problem:** The hidden terminal problem refers to the collision of packets at a

receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

### 5. SECURITY IN MANET

There are several security criteria to secure the important information. These are as follows-

- i) Confidentiality
- ii) Availability
- iii) Integrity
  - a. malicious altering
  - b. Accidental altering
- iv) Authentication
- v) Authorization
- vi) Non-repudiation
- vii) Attacks using fabrication

**i) Confidentiality:** Providing information only for those who have been authorized to access that accessible information is called confidentiality. Ad-hoc network needs to keep confident about sensitive information.

**ii) Availability:** This is necessary for the sender's end. It shows the receiver is available or not.

**iii) Integrity:** This ensures that the message has not any changes during the communication in the network. It can be done in two ways:-

**(a)** when the information is demolished and pretend by an attacker with some malicious term, is called the malicious altering.

**(b)** When the information is lost or its some elements are changed due to some kind failure, then it called the accidental altering.

**iv) Authentication:** It is based on the right access of a user. In ad-hoc network there may be numerous unidentified user with the current users. Which one is authorized to message? This answer will find out by the authentication policies.

**v) Authorization:** Any unauthorized person cannot behave like as the authorized person to access any confidential information. This is used to provide various different access rights to various types of users.

**vi) Non-repudiation:** Non-repudiation is a term that source and destination of information cannot deny that they have sent or received information. This is useful at that time when we try to search about the malicious nodes which are always tries to interrupt the network operations between various authorized nodes [6, 7].

**vii) Attacks using fabrication:** Data alteration is not only called the attack [8]. Idle, annoying packet generation is also comes under the attack. This is

known as fabrication attack. Here the nasty node create the large number of packets and send it into the network.

### 6. CONCLUSION

In this study it seems to be that there are many advantages of Ad-Hoc Network. It can apply in Battlefield by Military; can be used in small network at home and offices, in business and at natural disaster for establishment of temporarily flexible networks. Having these facilities there are some loop holes to establish such kind of dynamic infrastructure less network. This paper is introduction to Ad-hoc networks, characteristics their applications and at last challenges faced by these networks. This paper also throws some light on possible attacks in Mobile ad-hoc network. In future there is a possibility to detect & deter melisicious node from attacking in the network.

### REFERENCES

- [1] Robinpreet Kaur & Mritunjay Kumar Rai, A Novel Review on Routing Protocols in MANETs, Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012
- [2] L Raja et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 408-417
- [3] C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers, 2002.
- [4] G.Vijaya Kumar , Y.Vasudeva Reddyr , Dr. M. Nagendra, Current Research Work on Routing Protocols for MANET: A Literature Survey, International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713
- [5] <http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/>
- [6] Sheikh, Rashid, Singh Chande, M., Mishra, Durgesh Kumar "Security issues in MANET: A review" IEEE 2010, 1-4.
- [7] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, "Security in mobile ad hoc networks: challenges and solutions", IEEE 2004, pp 38-47.
- [8] Ankit Mehto, Hitesh Gupta, "A Review: Mobile Ad-hoc Network Protocols and Security Issues", IJEAT ISSN 2231-1963.