# A STUDY ON MOBILE AD-HOCK NETWORKS (MANETS)

*P. Senthilkumar[1], M. Baskar[2] and K. Saravanan[2]*

[1]*Assistant professor, MCA, Coimbatore Institute of Management and Technology, Tamilnadu.*

[2]*III$^{rd}$ MCA, Coimbatore Institute of Management and Technology, Tamilnadu.*

**Abstract**

As we know that wireless technology becomes very famous among all the aspects of different technologies of computer networking of present era, the Wireless networks really provide the convenient and easy approach to communications between different areas. Wi-Fi is commonly called as wireless LAN, it is one of those networks in which high frequency radio waves are required for transmission of data from one place to another. Wi-Fi operates on several hundred feet between two places of data transmission. This technology only works on high frequency radio signals. Nowadays this technology is used as office or home network and in many electronic devices. Wireless LAN or Wi-Fi is divided into three main parts on which its whole working depends and all of its applications depend on these parts such as infrastructure mode and ad hoc mode of networking. However, the important type that plays a vital role almost in application is the Ad Hoc mode of networking.

This type of networking is also commonly called as peer-to-peer networking or P2P networking. Mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. There is still ongoing research on mobile ad hoc networks and the research may lead to even better protocols and will probably face new challenges. The current goal is to find an optimal balance between scalable routing and media access control, security, and service management.

**Keywords:** VANETs, InVANETs, iMANETs, DTNs, ALARM, PRISM

## 1. INTRODUCTION

Information technology is rapidly changing from regular desktop computing, where isolated workstations communicate through shared servers in a fixed network, to an environment where a large number of different platforms communicate over multiple network platforms. In this environment the devices adapt and reconfigure themselves individually and collectively, to support the requirements of mobile workers and work teams.

The **mobile phones** records the development of interconnection between the public switched telephone systems to radio transceivers. From the earliest days of transmitting speech by radio, connection of the radio system to the telephone network had obvious benefits of eliminating the wires. Early systems used bulky, high power consuming equipment and supported only a few conversations at a time, with required manual set-up of the interconnection. Today cellular technology and microprocessor control systems allow automatic and pervasive use of mobile phones for voice and data.

The transmission of speech by radio has a long and varied history going back to Reginald Fessenden's invention and shore-to-ship demonstration of radio telephony, through the Second World War with military use of radio telephony links. Mobile telephones for automobiles became available from some telephone companies in the 1950s. Hand-held radio transceivers have been available since the Second World War. Mobile phone history is often divided into *generations* (first, second, third and so on) to mark significant step changes in capabilities as the technology improved over the years. The purpose of outdating is only to improve the save the times and improve the network reliability. Because of, the MANETs have improved.

MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid 1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

## 2. MANETs

A **mobile ad hoc network** (**MANET**) is a self-configuring less infrastructure network of mobile devices connected by wireless links. ***Ad hoc*** is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

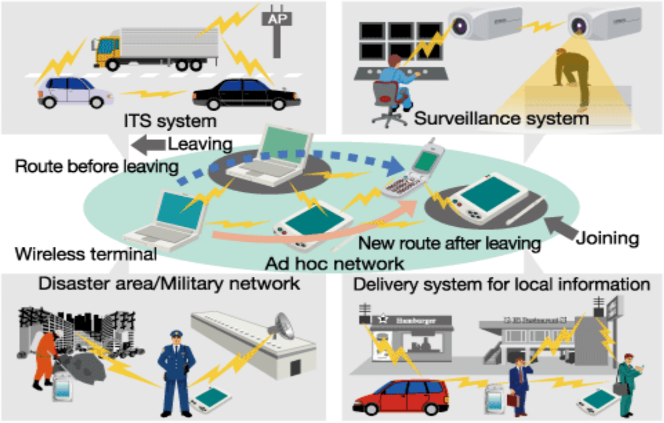

Figure 1.Example of MANETs

An ad hoc wireless network should be able to handle the possibility of having mobile nodes, which will most likely increase the rate at which the network topology changes. Accordingly the network has to be able to adapt quickly to changes in the network topology. This implies the use of efficient handover protocols and auto configuration of arriving nodes.

**Definition**

Mobile ad hoc network is a wireless network that transmits from computer to computer. Instead of using a central base station (access point) to which all computers must communicate, this peer-to-peer mode of operation can greatly extend the distance of the wireless network. To gain access to the Internet, one of the computers can be connected via wire or wireless to an ISP.

### 2.1 Characteristics of MANETs

- Dynamic topology - links formed and broken with mobility
- Possibly unite-directional links
- Constrained resources - battery power
- wireless transmitter range

### 2.2 Examples for MANET

- Computer science classroom Ad-hoc network between student PDAs and workstation of the instructor.
- Large IT campus
- Employees of a company moving within a large campus with PDAs, laptops, and cell phones.
- Moving soldiers with wearable computers.
- Eavesdropping, denial-of-service and impersonation attacks can be launched.
- Shopping mall, restaurant, coffee shops Customers spend part of the day in a networked

### 2.3 Types of MANET

- **Vehicular Ad Hoc Networks** (VANETs) are used for communication among vehicles and between vehicles and roadside equipment.
- **Intelligent vehicular ad hoc networks** (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.
- **Internet Based Mobile Ad hoc Networks** (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly.

### 2.4 How to Setup Ad Hoc Network

There are different steps that are used to build or setup the Ad Hoc networking for the transmission of data from one place to another. The devices for the working of the Ad Hoc network is designed in such a way that it will operate directly with other devices without the involvement of the access points and provide the networking in the narrow range. The steps that are involved in the setup are as follows

#### Required Hardware

The hardware or different types of devices that are used to configure the Ad Hoc network is fall in this category. Different types of hardware is required to build the network such as required network adapters, wired or wireless local area network LAN, routing devices, computers among which the network has to be configured etc. service set identifier is also the requirement of the setting of the ad hoc networking.

#### Network Adapter Configuration

After the collection of the required hardware then the setup moves to the installation of the required network adapter. It is the important step in the setting of the ad hoc networking; the installation process is as follows i.e. first place the adapter in the system correctly and then turns on the system. When the system is completely ready to use then insert the CD in the CD Rom of the required software of the network adapter and follow the instruction given on the screen.

#### Setting of Network

The basic process that is used for setting the Ad Hoc networking or peer-to-peer networking on the personal computers is as follows

1. For the configuration of the peer-to-peer network, your computer should be attached with the required wireless LAN technology or the Wifi device.
2. First of all, configure the settings of the network on the one computer this is called as server for that process then configure the required ad Hoc network on the other personal computers.
3. After settings open the tab for the configuration of the wireless network by open the wireless network icon and change the properties of the wireless networking to the required setting of Ad hoc network.
4. Then check the properties of the service set identifier box and type the name of the SSID box attached to your computer and then press the Add button to add the box next to you
5. The last step is that if you are not using the WEP then disables such security mode. After all, click the OK button and save the settings and the Ad Hoc network has been setup.

## 3. AD-HOC ROUTING PROTOCOLS

An **ad hoc routing protocol** is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In *ad hoc networks*, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

#### Pro-active (table-driven) routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

### Reactive (on-demand) routing

This type of protocols finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.

### Flow-oriented routing

This type of protocols finds a route on demand by following present flows. One option is to unicast consecutively when forwarding data while promoting a new link. The main disadvantages of such algorithms are:

1. Takes long time when exploring new routes without a prior knowledge.
2. May refer to existing traffic to compensate for missing knowledge on routes.

### Hybrid (both pro-active and reactive) routing

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are:

1. Advantage depends on number of nodes activated.
2. Reaction to traffic demand depends on gradient of traffic volume.

### Hierarchical routing protocols

With this type of protocols the choice of proactive and of reactive routing depends on the hierarchic level where a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attribution for respective levels. The main disadvantages of such algorithms are:

1. Advantage depends on depth of nesting and addressing scheme.
2. Reaction to traffic demand depends on meshing parameters.

### Backpressure Routing

This type of routing does not pre-compute paths. It chooses next-hops dynamically as a packet is in progress toward its destination. These decisions are based on congestion gradients of neighbor nodes. When this type of routing is used together with max-weight link scheduling, the algorithm is throughput-optimal. See further discussion here: Backpressure Routing.

### Host Specific Routing protocols

This type of protocols requires thorough administration to tailor the routing to a certain network layout and a distinct flow strategy. The main disadvantages of such algorithms are:

1. Advantage depends on quality of administration addressing scheme.
2. Proper reaction to changes in topology demands reconsidering all parameters.

### Power-aware routing protocols

Energy required to transmit a signal is approximately proportional to $d^{\alpha}$, where d is the distance and $\alpha \geq 2$is the attenuation factor or path loss exponent, which depends on the transmission medium. When $\alpha = 2$ (which is the optimal case), transmitting a signal half the distance requires one fourth of the energy and if there is a node in the middle willing to spend another fourth of its energy for the second half, data would be transmitted for half of the energy than through a direct transmission - a fact that follows directly from the inverse square law of physics.

The main disadvantages of such algorithms are:

1. This method induces a delay for each transmission.
2. No relevance for energy network powered transmission operated via sufficient repeater infrastructure.

### 3.1 Examples of such networks

**Sensor networks**

- Networks deployed in random distribution
- Low power
- Delivering sensor data to a central site for some purpose

**Traffic networks**

- "Smart cars" and "smart roads"
- Onboard systems "talk" to the "road":
  - Map obstacles and delays
  - Obtain maps
  - Inform the road of its actions

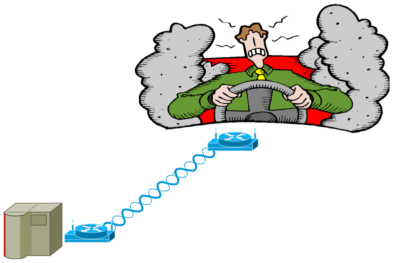

Figure 2.Example of Traffic networks

**Military applications**

- Combat regiment in the field Perhaps 4000-8000 objects in constant unpredictable motion.
- Intercommunication of forces Proximity, function, plan of battle
- Special issues
  - Low probability of detection
  - Random association and topology

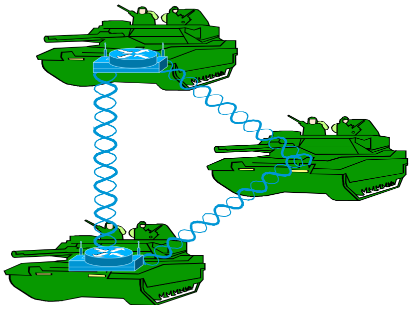

Figure 2.Example of military applications

**Security and Privacy in Location Based**

In many traditional mobile networking scenarios, nodes establish communication on the basis of public identities. However, in some settings, node identities must not be exposed and node movements should not be traceable. Instead, nodes need to communicate on the basis of their current locations. Such scenarios are encountered in mission critical mobile ad-hoc networks (MANETs), Vehicular ad-hoc networks (VANETs) and delay-tolerant-networks (DTNs) and in the near future geo-social mobile networks.

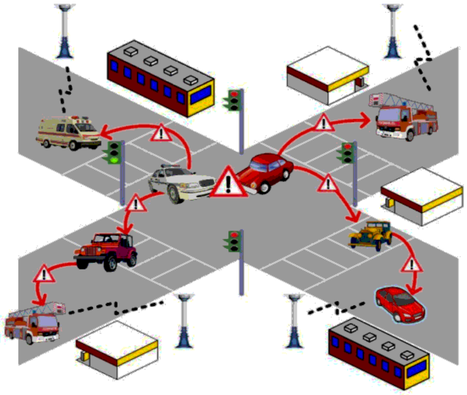

Figure 2.Example of Security and Privacy in Location Based

For the security and privacy, we consider a number of issues arising in such settings by designing anonymous location based routing protocols. We have designed two protocols so far: ALARM and PRISM. ALARM is a link state based protocol which uses nodes' current locations to disseminate and construct topology snapshots. PRISM is a reactive protocol based on AODV which achieves similar goals. With the aid of advanced cryptographic primitives (i.e., group signatures), both protocols provide a mix of security and privacy features, including: node authentication, data integrity, anonymity and intractability (tracking-resistance). ALARM also offers protection against insider attacks.

The key differences between MANETs and other wireless networks (Cellular Networks or Wireless LANs) are:

**No Fixed Routing/Forwarding Infrastructure**

Unlike the Internet or other forms of wireless networks (e.g., cellular mobile networks) MANETs don't have a fixed infrastructure that nodes can rely on for forwarding messages. This is the main reason why the design and operation of such networks is challenging. This also raises new security and privacy concerns.

**Collaboration**

Due to the lack of forwarding infrastructure, MANET nodes have to rely on each other in forwarding traffic. This gives attackers who control MANET nodes the ability to drop packets, reroute them. Attackers can also easily impersonate other nodes and/or violate their privacy by tracking their movements.

**Unbelievable Environment**

One of the main uses of MANETs is in mission critical networks. Such networks are used in military, law enforcement and search/rescue operations. MANETs may thus be deployed in hostile environments where adversaries will try to disrupt the operation of the network and compromise the security and privacy of the nodes.

**No PKI and On-line Security Infrastructure**

Unlike the Internet or other forms of wireless networks most MANETs don't have a fixed on-line security infrastructure. Any solution relying on **on-line** trusted third parties will thus be challenging to implement and operate.

**Advantages**

- Wireless communication
- Mobility
- Do not need infrastructure
- but can use it, if available

- Small, light equipment

**Disadvantage**

- Mobile - Random and perhaps constantly changing
- Ad-hoc - Not engineered
- Networks - Elastic data applications which use networks to communicate

## 4. CONCLUSION

In this paper, we proposed an overall process of the MANETs. In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of **Mobile Ad Hoc Networks**. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes.

## References

[1]. Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". *O'Reilly Wireless Dev Center*.
[2]. H K SONI (2011-03-22). "Ad hoc network". *DoS attack in MANET*.
[3]. http://en.wikipedia.org
[4]. http://www.ics.uci.edu/~keldefra/manet.htm
[5]. http://www.wifinotes.com/how-to-setup-ad-hoc-network.html
[6]. http://www.antd.nist.gov/wahn_mahn.shtml
[7]. http://www.oreillynet.com/pub/a/wireless/2004/01/22/wirelessmesh.html

Received June 2011
Accepted July 2011
Final acceptance in revised form September 2011