Chapter – 1

INTRODUCTION

CHAPTER -1

Chapter - 1. Introduction

CHAPTER - 1
INTRODUCTION

Irrespective of their geographic locations, users nowadays opt for wireless connectivity, which is why wireless networks are gaining much popularity. Wireless systems have been in use for the past three decades. Traditional wireless systems are initially designed to function with the backing of a federal supporting infrastructure named as an access point. The mobile users take the support of these access points while they roam from one place to another to keep connected with the wireless systems. The communication between the wireless systems takes place, via open access radio channels, thus sharing information and resources among users. The existence of a federal supporting infrastructure limits the adaptability of a conventional wireless system. The dependency of the wireless system to the access point restricts its easy and quick deployment.

Recent past advancements of wireless technologies like IEEE 802.11-WLAN/Wi-Fi, IEEE 802.15.1–Bluetooth and IEEE 802.15.4-ZigBee facilitate the network designers in introducing a new type of wireless system which functions in the absence of a federal supporting infrastructure well known as a Mobile Ad hoc Network (MANET) [1],[2].

MANET facilitates the user’s high mobility and device portability that enables them to connect to the network, even while roaming and communicating to each other. These unique features of MANET allow the users to enter and leave the network easily at their wish. The fascinated user can devise such a network at the lowest cost and bare minimum time as it provides a greater flexibility.

MANETs are the prime variants of wireless networks. Apart from being decentralized, autonomous and self-configured, MANETs are self-maintained and self healing wireless systems. MANET comprises freely moving mobile nodes such as a Personal Digital Assistance (PDA), laptop, mobile phone, and other portable devices that participate in the network. Each node that participates in the network acts both the ways as a host and a router as well. Apart from doing work on their own, the nodes must be willing to relay the packets for other nodes. The nodes can form random topologies within the network based on their connection with each other. The self reconfiguration capabilities of MANET go a long way in meeting emergency situations, albeit in the absence of organized infrastructure; be it a military battlefield, a fire rescue operation or a natural disaster.

1.1. THE CLASSIFICATION OF WIRELESS NETWORKS

In a broad sense the wireless networks can be categorized into two types [3] based on its formation and architecture.

- Infrastructure networks
- Infrastructure less networks

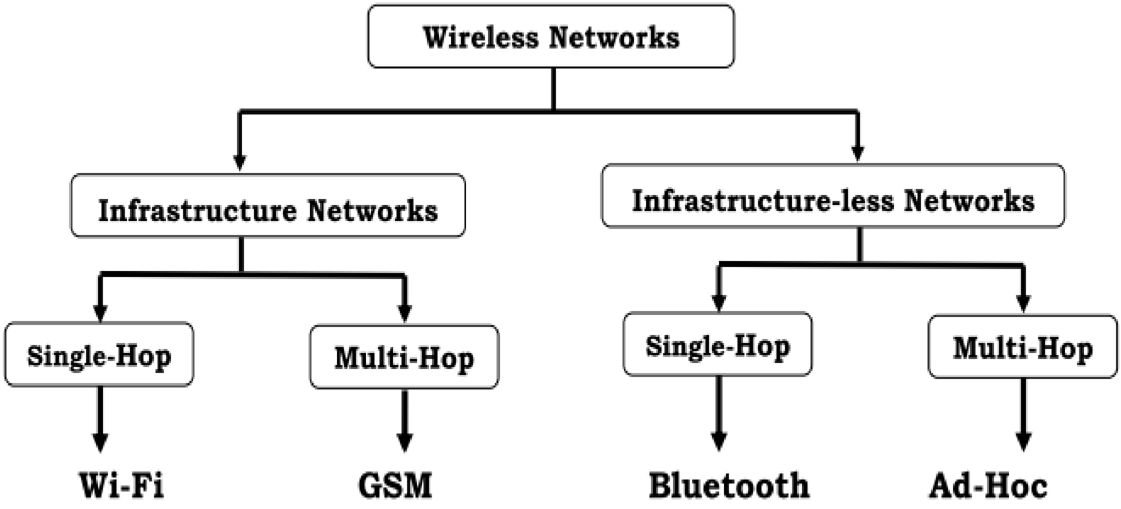

Fig 1.1: Types of wireless networks

1.1.1. Infrastructure Network

A network infrastructure includes computer systems which are interconnected by the various parts of telecommunications architecture. This infrastructure ranges from individual networked computers to switches, routers, cables, backbones, network protocols, network access techniques and wireless access points. The infrastructure can run over wired or wireless network connections or both and is of either open or closed architecture. The mobile node in a wireless infrastructure network communicates with centralized base station within its radio communication range. The mobile node moves geographically even while it is communicating with the others. The mobile devices try to connect to the new base station when they go outside the range of the present base station and starts communicating in the course of it. This method of call routing from a standalone base station to the other is called a handoff. In which the base station refers to the fixed, centralized infrastructure as shown in the figure below.

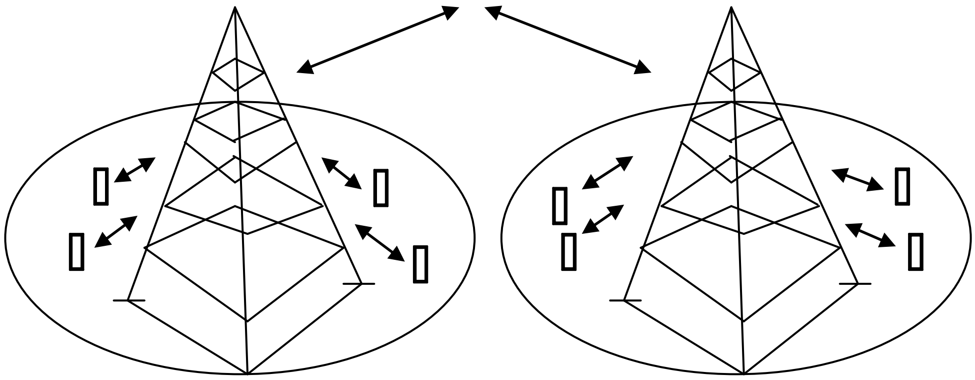

Fig 1.2: Infrastructure network

The Cellular Networks are so popular that they fall under the category of wireless infrastructure networks. A cellular network that consists of a group of cells spreading over the geographical area is a class of the radio network. Each cell is equipped with at least one central infrastructure transceiver, well known as a base station or cell site. To avoid interference and to provide the assured bandwidth each cell in a cellular network uses diverse frequencies from its next-door cells.

These cells in cooperation with each other provide a wide range of coverage area. This facilitates the huge number of mobile users to communicate with each other and also with fixed land line telephone users everywhere in the network through the base stations being some of the mobile users still short lived through more than one cell at some point of transmission.

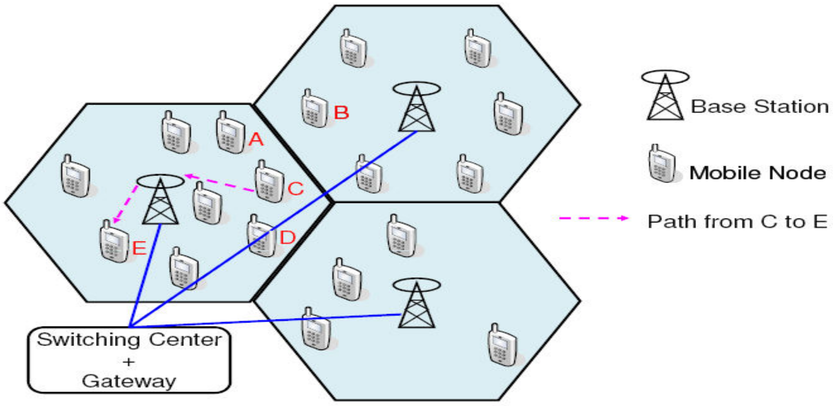

Fig 1.3: Cellular network

Cellular networks may be categorized into one of the following two types. They are

- Single-hop cellular network
- Multi-hop cellular network

1.1.1.1. Single-hop Cellular Network

The source node in a single-hop communication, for any pair of communication entities, can reach to its destination node directly. In this conservative cellular network, all the users within their radio range can communicate directly with the base station or cell site that controls the number of mobile users.

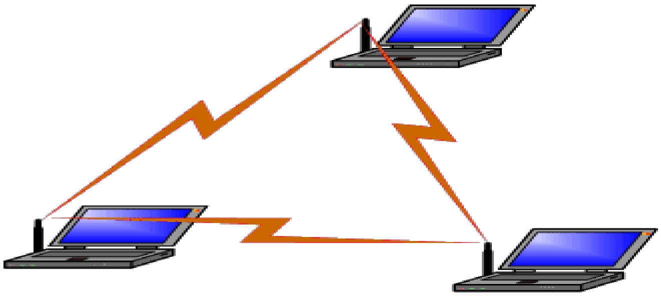

Fig 1.4: Single-hop cellular network

However, there is a need to explore all the possibilities, including novel network architectures as well as new access strategies to enhance the obtainable cell capacities without upgrading the required radio frequency spectrum, as the demand for cellular phone communications is mounting day by day.

1.1.1.2. Multi-hop Cellular Network

The class of fixed infrastructure cellular network, with a multi hop forwarding capability is called a Multi-hop Cellular Network (MCN). In a multi hop communication the source node can reach at its destination node after passing only through two or more intermediate nodes. The intermediate nodes rest on the lane between the source and destination nodes and would play the role of a forwarding station.

The primary thought behind the multi hop communication is to divide an actual long communication channel into two or more shorter links for sinking the necessary transmission power of every participating node in a communication structure. It sounds as if that the interference levels and frequency reuse distance are lowered due to the diminished transmission power requirements. The less interference in the network allows more users and it could lead to its increased capacity. Another important benefit of multi hop communication is the coverage improvement apart from power saving and capacity improvement of the network. The short range transmission in multi-hop cellular networks also opens the prospects of utilizing any other wireless technologies like IEEE-802.11 Wi-Fi (Wireless Fidelity) that supports higher data rates, in combination with the cellular technology.

1.1.1.2.1. Applications of Multi-hop Cellular Network

The Wi-Fi refers to Wireless Fidelity and is a popular short distance wireless transmission technology being used all over the globe in most of the offices, homes etc. The Wi-Fi simultaneously uses the following two unique technologies.

- DSSS - refers to Direct Sequence Spread Spectrum and it works based on a single carrier radio technology.
- OFDM - refers to Orthogonal Frequency Division Multiplexing and it works based on a multi carrier radio technology.

Internet access is a happening mode with any device such as personal digital assistance, Personal Computer (PC), laptop, game console, mobile phone etc which are enabled with Wi-Fi technology.

Cellular networks carry a number of advantages and disadvantages as compared to the traditional wired networks. They are listed below.

The advantages of cellular networks

- Reduced power use
- Increased network capacity
- Reduced interference levels
- Larger coverage area

The disadvantages of cellular networks

- Data charges are on a recurring basis
- Network outages-high call and data volume
- Position update latency

- Prioritized to voice over data
- First responders are not given with any priority.

1.1.2. Infrastructure less Network

The significant increase in the role of computers in our daily life is creating new demands for connectivity. In spite of the existence of wired solutions around us for quite a long time, there is a mounting demand to work with wireless network solutions to connect to the World Wide Web for online reading, chatting, sending e-mails etc. The Wireless LAN normally based on 802.11 IEEE standard looks to be the serious solution for all these needs. But the Wireless LAN technology works based on centralized base stations. On the other hand, there is a growing need for connectivity in situations like disaster environments where there is no existence of backbone connection, i.e. base station (for instance two or more laptops need to be linked). This is the place where special class of networks called wireless ad hoc networks step in.

The phrase ad hoc is taken from the very old Latin language meaning, "for this", another context being "for this purpose only”. It is an illustrative narration of the thought as to why ad hoc networks are much more desirable. Irrespective of the geographical location the ad hoc networks can be set up in no time as they don’t require a centralized infrastructure like base stations or wires. So this special class of networks is quite opt for emergency situations like fire rescue operations, military battlefield, disaster recovery etc. They are available quite often and are commonly known as Mobile Ad hoc Networks (MANET).

A MANET is more often a set of autonomous mobile nodes that communicate with each other through wireless channels without relying on the centralized base stations or fixed infrastructure. The nodes of a MANET are mobile in nature and play a dual role as a host and a router as well. The nodes of MANET are free to move haphazardly and they are also self configurable. Thus, the wireless topology of the network may perhaps change quickly and arbitrarily. Such a network solution either works in a separate kind of approach or may be associated with the larger internet.

The power of open access connections can change quickly in time or even fade away completely. The nodes may become visible, invisible and re-visible as the time progresses and all the times the network link that is a part of it is supposed to work between the nodes. Anyone can easily sense that the ensuring connectivity and robustness are in much more demand for MANETs than its contemporary wired networks.

The MANETs are not inevitably connected to any wired or static centralized infrastructure. The MANET is a Local Area Network (LAN) or any small scale network, particularly the one with a wireless connection, in which a few of the network devices are a part of the network for the session only. The communication takes place during that session even in closer immediacy to the remaining part of the network. In other words, the MANET can be referred as a communication network with no pre-exist network infrastructure. The MANETs may be of a single hop or a multi hop in nature.

1.1.2.1. The Single-hop Ad hoc Networks

The source node in a single hop Ad hoc network, for any pair of communication entities, can reach to its destination directly to carry out the peer to peer communication.

1.1.2.1.1. The Advantage and Disadvantages of Single-hop Ad hoc Networks

The Bluetooth networks fall under this class of networks. The Bluetooth is a secure, fast and point to point wireless communication technology for exchanging data over devices like laptops, handheld workstations, consumer electronic appliances etc, which operates over very short distances ranging 10 meters approximately. It uses short wavelength Ultra High Frequency (UHF) spectrum in the ISM1 unlicensed frequency band from 2.40 to 2.485 GHz for building personal area networks. It was invented by Ericson, the reputed telecom vendor, in the year 1994 as an alternative to RS-232 standard communication cables. It is maintained by a group called Bluetooth Special Interest Group (SIG), which has more than 20,000 companies as the members from different sectors like networking, telecommunication, computing, consumer electronics etc. The international standards organization, namely the Institute for Electrical and Electronics Engineers (IEEE) has standardized the Bluetooth communication as IEEE 802.15.1, but it is no longer maintained. Further being a standard, Bluetooth is also defined as a protocol heap for allowing hierarchical networking on an ad hoc basis to form piconets. In piconets, the Bluetooth devices form themselves into a point to multipoint picocells of seven slaves under the control of a master. Multiple piconets overlapping over the coverage areas form "scatter nets". Despite the fact that the standardization of Bluetooth has been done for quite a long time; still the Bluetooth enabled devices are not yet extensively available. The present available Bluetooth devices are either point to point or point to multipoint devices. Even today also the proper multi hop ad hoc Bluetooth devices are not yet commercialized.

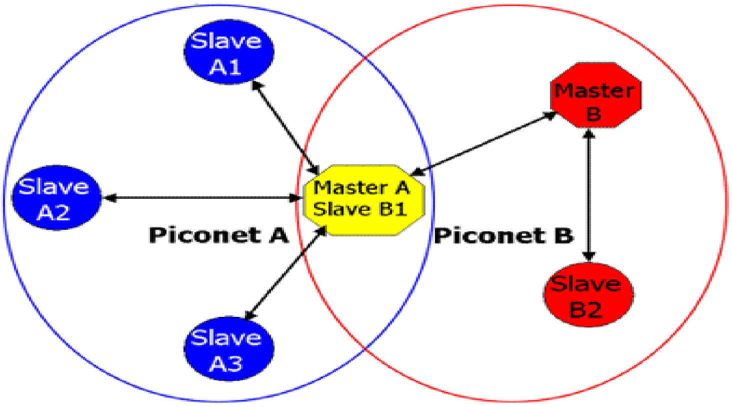

Fig 1.5: The Bluetooth scatter net

1.1.2.2. The Multi-hop Ad hoc Networks

In Ad hoc networks every Communication Terminal (CT) communicates with its own associate to execute peer to peer communication. Outside the radio range of CT, the other intermediary CTs can be used to execute the communication if the required CT is not a one hop neighbor to the call initiated CT. This will be referred as a multi hop peer to peer communication and the existing team work among CTs is very significant in Ad hoc networks. All the communication network protocols in Ad hoc network should be scattered throughout the communicating devices which are highly cooperative and independent.

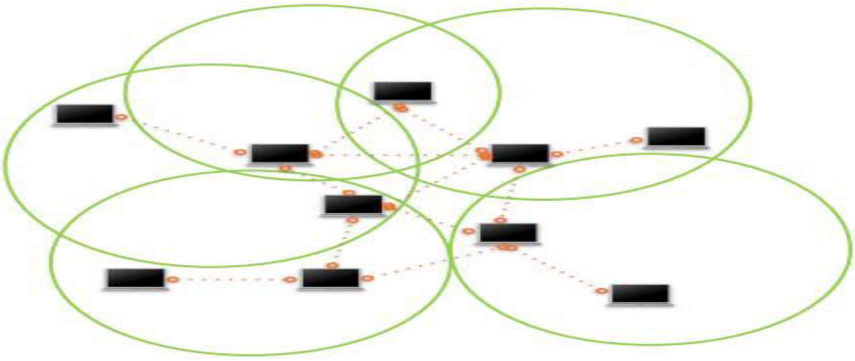

Fig 1.6: The scenario of multi-hop ad hoc network

1.1.2.2.1. The Advantages of Multi-hop Ad hoc Networks

The advantages of multi hop ad hoc networks are as follows

- ❖ Regardless of geographic location ad hoc networks provide services and access to the information.
- ❖ This class of networks can be deployed in no time in any place.
- ❖ No pre-existing infrastructure is required to set up this type of networks.

1.1.2.2.2. The Disadvantages of Multi-hop Ad hoc Networks

The disadvantages of multi hop ad hoc networks are as follows.

- ❖ Resource constraints.
- ❖ Vulnerable to security threats due to intrinsic mutual trust.
- ❖ Open access limited bandwidth wireless channels.
- ❖ Lack of centralized administration.
- ❖ Dynamic network topology creates troubles in noticing adversary nodes.

- Security extensions of traditional wired networks may not work properly with ad hoc networks.

1.2. THE CHARACTERISTICS OF MOBILE AD HOC NETWORKS

As discussed earlier, MANET is a set of autonomous mobile devices that can communicate with each other through open access wireless channels. The mobile devices can directly communicate with each other when they are in the radio range, otherwise they need the help of other intermediary node to forward or route their packets. This class of the network is completely scattered in general and can work irrespective of the geographical location without the use of any centralized equipment. This unique feature of MANET makes them exceedingly robust and flexible in nature.

The distinctiveness or characteristics [4] of MANETs can be summarized as follows.

Communication via open access wireless media:

Mobile nodes communicate through shared wireless media such as radio or infrared media. Basically, in single-hop wireless network mobile node communicates with the aid of fixed infrastructure. But MANET offers multi hop communication by using the intermediate nodes to forward the packets without the aid of any centralized infrastructure.

Dual role of nodes as hosts and routers:

Every node in MANET can play the dual role as a host and a router as well. No dedicated routers are necessary as every node can act as a router and relay each other’s data. This unique feature facilitates the users in a MANET to communicate even in the absence of base stations.

No need of centralized administration and infrastructure:

There is no need of any pre-established infrastructure and centralized administration to control the network operations in MANET. Every node is self configurable and acts as a forwarding station as if needed to relay the packets of each other's node. Nodes also mutually cooperate with each other to implement the network functions like security.

Dynamic network topology:

The topology of MANET is highly dynamic as it comprises independent mobile nodes. So the traditional protocols of static wired networks are not directly applicable to MANETs.

Quick deployment:

The MANET can be setup in no time at any place as it is an infrastructure less network. This unique feature makes the MANETs suitable for emergency situations like fire rescue operations, military battlefield, disaster environments etc.

Mobility:

The participating nodes are free to move in and around within the MANET while communicating with the other nodes. So the topology of an ad hoc network is dynamic in nature causing the intercommunication patterns to continuously change among the nodes.

Variable channel capacity:

The open access wireless channels of high error rates may be further insightful in a MANET. Several sessions may possibly share the same end to end path. The bandwidth of the link over which the terminals will communicate is subjected to noise, fading, interference etc. In some situations, the communicating path can interchange multiple wireless links between any pair of users and the links themselves could be heterogeneous. As such the assured channel capacities are not possible with these types of networks.

Resource constrained (i.e. Light weight) terminals:

In general, the MANET is composed of mobile devices with low processing power, limited memory storage and less battery backup. Such devices are very much needed to implement proper algorithms and mechanisms that result in less computing and effective communication.

Vulnerable security:

The characteristics of MANET such as available open access channels, dynamic network topology, limited resources, lack of centralized administration and others to make them more vulnerable to the adversary (i.e. malicious) attacks. That's why the implementation of security mechanisms is very significant in MANETs.

By and large, the communication terminals of this distributed network being mobile in nature make the topology of the network to change dynamically with respect to time. The nature of dynamically changing network topology of an ad hoc network increases the design challenges. Every mobile terminal in MANET is normally powered by limited power storages like rechargeable batteries. The power expenditure of the mobile terminals is usually results due to the following three reasons.

- Data processing inside the mobile terminal
- Transmission of own packets to the destination
- Lastly the power expenditure when the mobile terminal is used as a relay station, i.e. to forward the packets for other mobile terminal in the network. The energy spending is said to be a critical issue in the design of an Ad hoc network.

As discussed earlier, the mobile terminals typically have restricted storage capabilities and small computational processing powers. So, special strategies and procedures are required to be implemented with MANETs that produce less CPU overhead, occupies less memory space and drains negligible power storage of the mobile terminals. In this regard, efficient and secure routing protocols that have the features mentioned earlier are quite essential for MANETs.

1.3. THE IMPORTANT APPLICATION AREAS OF MANETS

With the increased usage of hand held devices as well as advances in wireless communication, the ad hoc networking is becoming so popular within view of its rising number of extensive applications. The ad hoc networking can be implemented wherever there is no static infrastructure or the accessible infrastructure is so dear or problematic to use. The ad hoc networking allows easy addition and removal of mobile devices to and from the network and also the devices to preserve connections to the network while moving in and out of the network. The collection of applications of MANET is diverse, ranging from small-scale fixed infrastructure networks to large-scale mobile highly dynamic networks that are highly constrained by power sources. Besides passing the inherited applications of conventional fixed infrastructure networks into the ad hoc contest, a great deal of new services can be fashioned for the new environment.

The important applications of MANET are discussed below [5, 6].

Military combat zone:

The military uses ad hoc networking to sustain an information network among the soldiers, vehicles, and military headquarters by taking the advantage of usual network technology. Furthermore, in military surroundings, conservation of latency, security, dependability, deliberate congestion, and breakdown recovery are very important concerns. Mostly the military networks are designed to maintain a low likelihood of intercept and/or a little likelihood of detection. Hence, nodes have a priority to radiate the power to the least possible extent as required and broadcast as rarely as possible, consequently diminishing the likelihood of detection or interception. The performance and reliability of the network may degrade when there is a slip in any of these requirements.

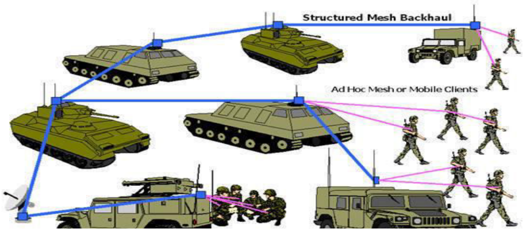

Fig 1.7: Millitary ad hoc network

Emergency/Rescue operations:

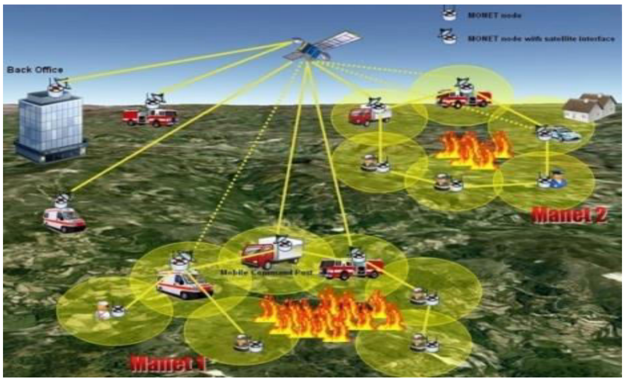

Fig 1.8: Emergency ad hoc network

The quick deployability of MANETs makes them suitable for emergency/rescue operations from fire, flood or earthquake kind of disaster reprieve efforts. The disaster salvage operations should take place where there is no accessible infrastructure or broken infrastructure and in such an environment quick deployment of a communication network is required. Information is forwarded using small hand held portable devices from the member of one rescue team to another. MANETs can also be used with commercial scenarios like law enforcement, ship to ship ad hoc mobile communication etc.

Local level applications:

The MANETs can be used to link an instant and temporary multimedia network using hand held devices like palmtop computers or notebook computers and also to extend and share information among different participants at conferences or in classrooms. Additionally, MANETs might be used with appropriate neighborhood level applications such as residential networks where devices exchange information by communicating directly with each other. Similarly MANETs can also be used with other civilian surroundings such as sports stadium, taxicab, small aircraft, boat and mobile ad hoc communications.

Personal Area Network (PAN):

The short range MANET can make things easier for providing intercommunication among various mobile devices such as a laptop, a personal digital assistance and a mobile phone. The PAN is potentially a gifted application in the pasture of MANET being the prominent future computing resource.

1.4. CHALLENGES WITH MOBILE AD HOC NETWORKS

During the past few years, the MANETs have been explored to certain satisfactory levels as it is the most accepted field of study. But unfortunately, none of the problems of MANET is completely addressed with decisive resolution so for or at least agreed upon. The main challenges one has to face while working with MANET are [7] [8] [9] as follows.

1. Routing in more dynamically changing topologies
2. Scalability to the large number of nodes
3. QOS (i.e. Quality of Service) maintenance
4. Efficient energy utilization
5. Maintaining security in vulnerable environment

Routing – The dynamically changing topology of MANET poses serious problems in adopting the conventional routing protocols of fixed infrastructure networks. The limited transmission range, the low bandwidth and battery lifetime of mobile radio terminals of MANETs also leads to more troubles in designing a new routing protocol.

Scalability- The reasonable level of service the network provides even in the existence of a hefty number of nodes is normally defined as the scalability of the network. Scalability is the most prominent one among the open problems of the MANET. The following are the main reasons for scalability problems in MANETs.

- Limitations of routing protocols to adjust to the size of the network
- MANETs experience the capacity degradation, in nature, with the growing size of the network.

Encryption key exchanges, service and route acquisition are examples of responsibilities that will require considerable overhead, which will increase rapidly with the size of the network. MANETs would never see dawn in practice if the inadequate resources are washed out with increased control traffic.

Quality of Service (QoS) - The assurance the network provides for certain performance for a data flow in terms of the parameters such as throughput, delay, bandwidth, packet loss probability etc is defined as the QoS of the network. Even today also the QoS maintenance is still an open problem in fixed wireless networks. Furthermore, the nature of MANETs such as the link quality variation with time makes the quality of service maintenance an even more demanding problem than ever before and cannot be guaranteed for a long time. There is a need to investigate the procedures in order to notice and report changes in the link quality in the near future.

Energy Efficiency - In the absence of static infrastructure, the MANETs have to rely on portable and constrained power sources. Apart from self receiving and transmitting messages, a node in a

MANET requires forwarding and routing messages for the remaining nodes in the network. Hence the issue of energy efficiency has become one of the most important problems in MANETs. The most accessible solutions for energy saving in MANETs spin around the decrease of power used by the radio transceiver, which is often the single largest consumer of power.

Security - Security is considered to be the gravest issue of MANETs and is still not yet explored to satisfactory levels even today. As nodes use the open access broadcast medium in the potentially apprehensive surroundings, they are prone to adversary attacks, such as DoS, impersonation etc. The lack of central authority makes the MANET structure very susceptible to eavesdropping, interference, infiltration etc. Very often, the security is considered to be the major obstacle in business applications of MANETs.

Security is the extreme concern in MANET, especially in critical situations, such as in disaster management and in military battlefields. More often, MANETs experience the problems from security attacks because of their peculiar features like open access radio medium, dynamically changing topology, the absence of central monitoring and administration**,** cooperative algorithms and indistinguishable defense mechanism. All these factors have changed the battlefield situation for MANETs in view of the security threats.

Characteristics like dynamically changing topology, the lack of centralized administration, pathetic physical shielding of nodes and high dependency on intrinsic node cooperation affiliate to MANETs in contrast with traditional infrastructure networks that have a superior level of security for routers and gateways. Due to the dynamically changing topology, the well defined boundary does not exist in MANETs and hence network based control access mechanisms such as firewalls are not directly applicable. Moreover, the lack of centralized administration makes the things very difficult for bootstrapping of cryptographic systems. In comparison with conventional wired networks, wireless communication is sensibly more vulnerable to attacks in the wake of the shared nature of open access and noise prone wireless channels, and mobility caused instability. The presence of highly dynamic nature of MANETs alongside the dependency on cooperative communication among nodes makes them more vulnerable to malicious attacks than normal wireless networks that are supported by the centralized base stations.

Generally MANET is considered as a peer friendly design as it is assumed that each node provides accurate routing information and acts as a router to cooperatively forward the packets of other nodes. There has been a huge probability of effortlessly exploiting all such assumptions and humiliating the routing capability of the network by sending erroneous routing messages [10], [11], [12] in case of malicious nodes. That is, things become extremely easy for a malicious node to compromise the entities in a network, be it a send out of erroneous routing messages either by initiating fraudulent packets or by modifying the forwarded packets. Resultantly, the MANETs are more vulnerable to numerous routing attacks.

1.5. NEED FOR SECURITY IN MANETS

Network security is one of the significant aspects that tend to be ignored during continuing studies of MANETs in spite of creating many fascinating and demanding research areas. MANETs are intrinsically more vulnerable to security threats compared to conventional fixed infrastructure networks as they are made up of completely wireless mobile nodes. The malicious security events such as Denial of Service (DoS), impersonation, jamming, spoofing, and eavesdropping kind of attacks are more easily accomplished in MANETs as the open access to radio wireless channels is practically almost impossible to be controlled. To enable the potential MANET users to consider this new prototype as an alternate in networking for providing their mobile network services, these security threats must be condensed to a level good enough to maintain an adequate network performance and quality of service.

The working with a limited amount of bandwidth and typically restricted computing and battery resources enforces the MANET nodes to compound with several security problems. This imposes a sensible limit on the security procedures and policies for MANETs against the available fixed infrastructure networks. Thus, for MANETs, it is a compulsion to have effective security mechanisms.

For instance, assume an expeditionary warfare support network is required to prop up thousands of military personnel by setting a bare base station setup by an Air Expeditionary Force (AEF). To a great extent, MANET would trim down the need for a cable to be laid to every workplace as the base station is being set up. It is of utmost importance to substantiate every node of MANET as this bare base setup is in or near adversary province. The possibility of an enemy gaining access to the network cannot be ignored by posturing as a valid MANET node.

Moreover, the inadequate bandwidth can quickly become overcrowded as the base grows by adding MANET capable devices to the network. Thus the security mechanism must not consume too much of inadequate bandwidth of the MANET to ensure the required level of security for a particular situation. To deal with this problem, several solutions have been designed for fixed and access point wireless networks but nothing is standardized specifically for MANETs so far in this regard.

1.6. GOALS AND OBJECTIVES

Substantially the goal of this investigation is to develop an efficient secure mechanism for a MANET that can be incorporated directly into the on hand MANET routing protocol. This security mechanism should achieve a required level of security and authentication, but not at the expense of quality of service of the network. The theory is that an efficient secure mechanism providing a high degree of security and versatility is one that is directly incorporated into the MANET routing protocol versus performing bulk encryption at the time of transmission. The analysis will take in fixed network authentication mechanisms, the development of present encryption technologies, and a new routing protocol as they needed for this research. In order to achieve the goal stated earlier, one has to meet the following objectives.

1. To understand and evaluate the existing secure routing protocols for MANET
2. To acquire more information about Intrusion Detection Systems (IDS) and propose a new security framework for detecting and overcoming the impact of invaders in MANET as a second wall of defense.
3. To acquire more information about Cryptographic security and propose a new security framework in order to prevent the MANETs from adversaries by overcoming the shortfall of the existing systems.
4. Determine the appropriateness of the security extension through simulation as it provide an insight into the basic operations and performance of an experimental protocol prior to performing a prototype implementation.
5. Determine how much is the network performance affected by the deployment of the secure routing protocol compared to the original routing protocol based on which it was devised.
6. Provide input to the further development of the protocol and recommendations for real-world implementations.

Many researchers have devoted their efforts in developing protocols that will enable the MANET model to work properly in an adversary prone environment, as authentication and security for MANET is treated as an area of research all by itself. This study will provide a security and authentication system as well as help in determining the impact of such system on network performance.

1.7. Documentation Overview

This chapter provides a basic introduction and background to the problem of security vulnerabilities in MANETs. It defines the goal of this research. Chapter 2 provides background information in the areas of MANET routing protocols, security attacks, and the performance comparison of different secure routing protocol. Chapter 3 provides the methodology of this research as applied to approach the security problems of the MANET. Chapter 4 describes the design and implementation of the new secure routing protocols to defend MANETs form the blackhole attacks which are more likely in MANETs. Chapter 5 presents the simulation results of the new implementations and subsequently the chapter 6 illustrate the analysis of these results. Finally, chapter 7 presents the summary of the results, conclusion and the future scope of this investigation.