Chapter 1
Introduction to Wireless ad hoc Networks

Chapter 1
Introduction to Wireless ad hoc Networks

The word “ad hoc” comes from Latin. Language which means ‘for this purpose only’, Ad hoc Networks are the small area networks, especially designed with Wireless/Temporary connections to the different computer assisted nodes. Basically, an ad hoc network is the temporary network connections made to the information transferring purpose, so hence if the networks are designed for longer period connections then it acts as plain old network connections.

1.1 An overview of Wireless Adhoc Networks

A mobile ad hoc network is a collection of mobile nodes forming an ad hoc network without the assistance of any centralized structures. These networks introduce a new art of network establishment [Das 2000, Jinyang2000] and can be well suited for an environment where either the infrastructure is lost or where an infrastructure is not very cost effective. The whole life-cycle of ad hoc networks could be categorized into the first, second, and the third generation ad hoc network systems. Present ad hoc networks systems are considered to be the third generation.

The first generation goes back to 1972. At that time, they were called PRNET (Packet Radio Networks). In conjunction [Conti 2003, Conti 2004] with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing

PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The second generation of ad hoc networks emerged in 1980s, when the ad hoc network systems were further enhanced and implemented as a part of the Survivable Adaptive Radio Networks program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial to improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

Wireless Ad hoc networks deployed in 1990s, have been widely researched for many years. [Broch 1998, Demers 1994, Matthias 2001] Wireless Ad hoc Networks are a collection of two or more wireless communications devices with which networking capability. These wireless devices can communicate with other nodes immediately within their radio range or one that is outside their radio range. For the later, the nodes should deploy an intermediate node to be the router to route the packet from the source toward the destination. The Wireless Ad hoc Networks do not have gateway; every node can act as the gateway. Since 1990s, lot of research has been carried out on wireless communication medium. Hence in the 1990s, the concept of commercial ad hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of the collection of mobile nodes was proposed at several research conferences.

In the third generation level of technology, some standard was introduced by the IEEE. The IEEE 802.11 subcommittee had adopted the term "ad hoc networks" and the research community [Brad 2000, Matthias 2001, Royer 1999] had started to look into the possibility of deploying ad hoc networks in other areas of application. Meanwhile, the work was going on to advance the previously built ad hoc networks. GloMo (Global Mobile Information Systems) and the Near-term Digital Radio are some of the results of these efforts. GloMo was designed to provide an office

environment with Ethernet-type multimedia connectivity anywhere and anytime in handheld devices.

A Wireless ad hoc network is a collection of heterogeneous network node forming the temporary networks without the aid of any infrastructure or any centralized administrator. In such an environment, it may be necessary for one wireless host to enlist the aid of other hosts in forwarding a packet to its destination; this is because of the limited range of each wireless host's transmission. Wireless ad hoc networks (WANETs) Figure 1.0 do not rely on any fixed infrastructure but communicate in a self-organized way.

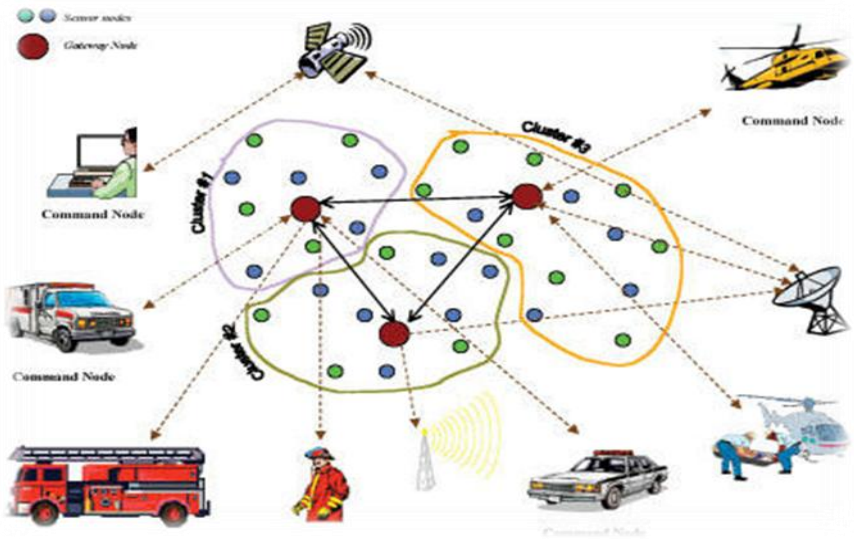

Figure 1.0: Wireless ad hoc Networks

The above figure 1.0 depicts the information about the different kind of application of WANETs. As the number of applications [Liu 2003 Turi 2004, Dahill 2002] of wireless ad hoc network grow, the size of the network varies greatly from a network of several mobile computers in a classroom, to a network of thousands of mobile units deployed in a battle field. The variability in the network size is also true for a particular network over the course of time; a network of a thousand nodes may be split into a number of smaller networks of a few hundred nodes or vice versa, as the nodes dynamically move around a deployed area. Accordingly, a good ad hoc

routing protocol should also be scalability and reliable is major concern. There are quite a number of uses for wireless ad hoc networks. For example, the military can track an enemy tank as it moves through the geographic area covered by the network. Your local community can use an ad hoc network to detect your car moving though an intersection, checking the speed and direction of the car. In an environmental network, you can find out the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations.

The wireless arena has been experiencing exponential growth in 21ST Century. Recently we have seen very technological advancement [Capkun 2001, Wicker 2002, Macker 1998, Zhou 1999] in the network infrastructures, growing availability of wireless applications, and the emergence of omnipresent wireless devices such as portable or handheld computers, PDAs, and cell-phones, all getting more powerful in their capabilities. These devices are now playing an ever-increasingly important role in our lives. To mention only a few examples, now a days wireless users can rely on their cellular phone to check e-mail and browse the Internet; travelers with portable computers can surf the internet at airports, railway stations, cafes, and other public locations; tourists can use Global Positioning System terminals installed inside rental cars to view driving maps and to locate tourist attractions, files or other information can be exchanged by connecting portable computers via Wi-Fi and other wireless technology like Bluetooth and chirping technology in the latest phone of the apple after apple-3 series of company phone. While attending conferences or meetings and celebrating occasions, and at home, a family can synchronize data and transfer files between portable devices and desktops.

The cost of the technology downing in the fold, now we can see that the mobile devices getting smaller, cheaper, more convenient, and more powerful, they also run more applications and network services. All of these factors are fueling the explosive growth of the mobile computing equipment market seen today.

1.2 Why Wireless Communication Technology?

The wireless communications technology [Capkum 2004] is holds much importance because in the recent era, this was not possible to have very complicated wired network to fulfil the requirement of the network users, because the traditional network system were very expensive and more complicated.

1.2.1 Wireless Communication Characteristics

Here are some inherent characteristic of wireless communications [Zhang 2005, Kong 2001] that make the networks more efficient in usability to the users of networks nodes. Keeping in the view, as given below, the Wireless Networks become useful:

a) **User Mobility:** Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the organization. The Wireless users are provided with access to the real time information even when they are away from their home/offices and even from their society.

b) **Rapid Installation:** The time required for installation is reduced as network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or by making modifications to the infrastructure cable plant.

c) **Flexibility:** Enterprises can also enjoy themselves the flexibility of installing and taking down wireless devices in locations as necessary. Users can quickly install small wireless devices for temporary needs such as a conference, trade show, or standards meeting. The Wireless users are provided with access to the real time information even when they are away from their nativity.

d) **Scalability:** Wireless network topologies can easily be configured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming in a

broader area. Wireless networks offer more and adapt easily to changes in the configurations of the networks.

e) **Cost:** Networks can be extended at any level with limited cost or almost no cost, as this facility is not available with wired system and hence setting up a wireless networks are so much easy and fast that it eliminates the need for pulling out the cable through walls and ceilings.

1.2.2 Wireless Networking Division

In the recent era of technology the wireless communication is becoming [Hass 2002, Zhang 2002] more relevant in each passing year. In addition to stand-alone systems such as those field personnel using laptop computers need to be connected to the Internet wherever they go using the some means of wireless communication modes. Systems such as Wireless-IP allow a wireless node to attach itself to the Internet through a system of proxy server. When a group of two or more wireless nodes need to set up an ad hoc network either at a small meeting or a large international conference, a Wireless ad hoc Network (WANET) can be operationalized.

1.2.2.1 Multiple Access Technology

Frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA) are the three major [Zapata 2002, Stinson 1995] access techniques used to share the available bandwidth in a wireless communication system. These techniques can be grouped as narrowband and wideband systems, depending upon how the available bandwidth is allocated to the users. Multiple access schemes are used to allow many mobile users to share simultaneously a finite amount of radio spectrum. This technology shares the spectrum for achieving high capacity by simultaneously allocating the available bandwidth (or the available amount of channels) to multiple users. For high quality communications, this must be done without severe degradation in the performance of the system. There are various different ways to have multiple stations access the

shared medium simultaneously. Different frequencies, time, and codes are used to achieve this result. These multiple access methodologies are discussed below as Frequency Division Multiple Access.

1.2.2.1.1 Frequency Division Multiple Access

Since all wireless technologies use different frequencies to transmit the datum information, the frequency band allocated to the particular device can be divided into channels to be used for uplinks and downlinks [Stinson 1995]. An uplink is the process of sending information from the mobile unit to a base station; while a downlink is the sending of information in the reverse direction, from a base station to the mobile unit. The band used to uplink information is known as the reverse channel; while the band used to downlink information is known as the forward channel. One's car radio uses this technology to receive information. There are set frequencies (for example: 87.9 MHz) that stations use as their base frequency to transmit their broadcast signal. Even though many radio stations transmit at the same time, one can listen to a particular station without interference from the other radio stations by tuning to the different frequencies.

1.2.2.1.2 Time Division Multiple Access

In another multiple access scheme, all data is transmitted using the same set of frequencies but at different times. The entire timeline is broken into fixed time slots that different users can transmit on. Unlike FDMA, multiple users share the same frequencies. Collisions can and do occur when two or more users transmit at the same time. For example, two people in the room talk at the same frequencies (400 - 4,000 Hz), but a meaningful conversation can occur only when they take turns and allow the other person to talk. A standard T1 (DS1) line uses this multiple access technology, as well as the classic Slotted ALOHA.

1.2.2.1.3 Code Division Multiple Access

In CDMA, different users transmit their data on the same frequencies at the same time, but the data is "spread" over the entire frequency band with different "codes." The receiver, who knows the code can reassemble the message and process the information. While this sounds less intuitive than FDMA and TDMA, it occurs in life. When a multitude of people get together at a party, many conversations usually occur between different sets of participants. Everyone uses the same voice frequency at the same time, but the brain recognizes the voice ("code") of a person with whom one is talking.

1.2.3 Wireless Communication Standards

In this new phase of technologies and standards, some of the new wireless communication devices are available, these are Bluetooth, Infrared Data Association (IrDA), HomeRF, and Institute of Electrical and Electronic Engineers (IEEE) 802.11 standards and [Robert 2002, Seung 2001] these are the new advanced devices having certain kind of advance features which help in wireless communication technology. So, in order to have acquaints with research we must have the complete knowledge about the strengths and weaknesses of the existing wireless communication devices and also the application domains of each of these standards and technologies. Bluetooth, Wi-Fi, Wi-Max, HomeRF and Chirping are quite new and has emerged as the front-runner in this so-called battle between competing technologies with the coming section from the different technology.

This section and all its sub sections will expand some basic standard of wireless communication such as 802.11, Bluetooth, infra Red (IR) and IEEE standard and DES Standards are available for the purpose of the protocol fabrications.

1.2.3.1 Bluetooth

The name Bluetooth supposedly comes from a Scandinavian history-enthusiast engineer involved in the early stages of developing and researching this short-range technology, and the name stuck; nobody [Robert 2002] being able to propose a better one. Bluetooth was the nickname for Harold Blatand—"Bluetooth,"—King of Denmark (940–985 A.D.). Bluetooth conquered both Norway and Denmark, uniting the Danes and converting them to Christianity. One of the major goals of the Bluetooth standard is to unite the "communication worlds" of devices, computers, and peripherals and to convert "the wired" into wireless; thus the analogy. The figure 1.1 depicts the Bluetooth devices and hence Bluetooth device was named after Harold Bluetooth, the 10th century Viking King.

Bluetooth SIG was formed in May 1998 by the so-called promoter companies, consisting of Ericsson, IBM, Intel, Nokia, [Hass 2002] and Toshiba, and later on 3Com, Lucent, Microsoft, and Motorola but now so many famous companies are dealing in the technology of Bluetooth. The SIG also contains associate members; participating entities pay membership fees and, in turn, can vote or propose modifications for the specifications to come. Adopter companies can join the SIG for free but can only access the oncoming specifications if these have reached a given evolutional level.

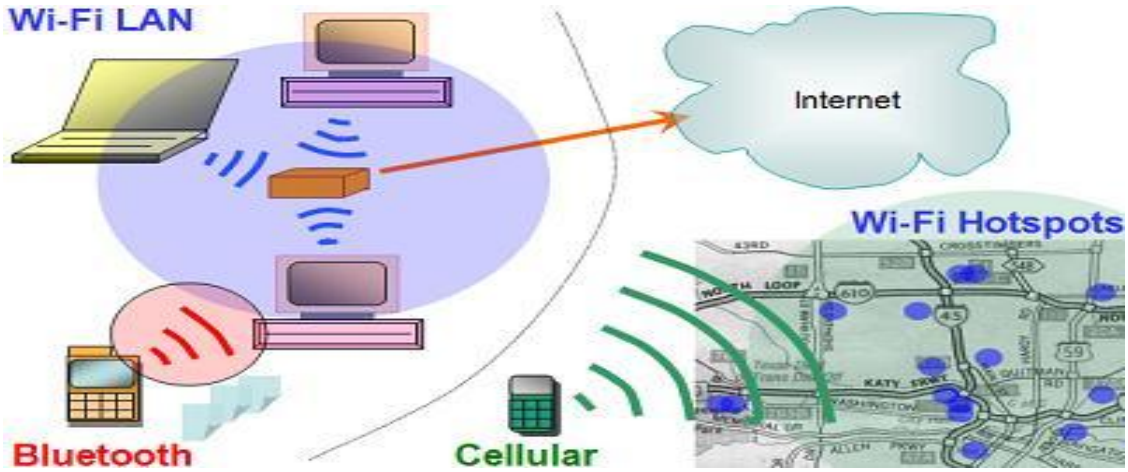

Figure 1.1: Bluetooth Device

The hardware consists of a microchip with a radio transceiver. It can be incorporated into a laptop or wireless phone. It can access other ad hoc networks or local access points. The Bluetooth device having the very short range system and this is the drawback for this device, it operate at a normal range of 10 m (0 dBm) and an optional range of 100 m (+20 dBm) and this is the case similar to wireless standard of IEEE 802.11 and so it uses 2.4 GHz as its base frequency. It can reach 6 Mb/s in a multiple piconet ad hoc structure. However, it differs from IEEE 802.11 in that it is a "Wireless Personal Area Network (WPAN) and was specified in IEEE 802.15 wireless standards, Working Group for Wireless Personal Area Networks. The 802.15 standards work is a cooperative effort with the Bluetooth SIG. The IEEE 802.15 Working Group provides it in the IEEE 802 family, standards for low complexity and low-power consumption wireless connectivity. The cooperative effort resulted from a convergence of IEEE standards development activities underway coupled with the formation of the Bluetooth SIG in 1998. IEEE 802.11 is a physical and data link layer protocol implementing a Wireless Local Area Network (WLAN). It is a subset of the IEEE 802 family of protocols, such as 802.2 (Token Ring) and 802.3 (Ethernet). It offers wireless networking with 1–2 Mbps data transfer rate using Spread Spectrum or Infrared technologies and 11 Mbps data

transfer rate for IEEE 802.11b. While some 802.11 products are in the market, it is still a relatively new technology.

1.2.3.2 Infrared Communication System (IR)

Infrared communication is an internationally approved having interoperable, low-cost, infrared data wireless interconnection communications system. Infrared also having a set of protocols for all type of data transfer and, in addition [NIST 800-12], has some network interoperability designs. Infrared's protocols have IrDA (Infrared Data) which act as the data bus for data delivery and IrDA control for sending the control information. In general, Infrared device is basically used to provide wireless connectivity technologies for devices that would normally use cables for connectivity. Infrared wireless communication devices are a point-to-point, narrow-angle (30° cone), ad hoc data transmission standard designed to operate over a distance of zero to one meter and at speeds of 9600 bits per second (bps) to 16 Mbps adapters now include the traditional upgrades to serial and parallel ports.

Infrared communications device has the following features:

- **Range:** The range from the connecting device should be at least one meter, but not more then two meters. A low-power version relaxes the range objective for operation from contact through at least 20 centimeters (cm) between low-power devices and 30 cm between low-power and standard-power devices. So this kind of devices provides the very cumbersome and less time less power consumption.

- **Bidirectional communication**: These communications have more benefit as well as the drawback of these devices because it provides only point to point communications and one to one device specifications.

- **Data transmission:** Primarily its speed is 9600 bps with cost steps of 115 kilobits per second (kbps) and maximum speed of up to 4 Mbps and so this is

not the good speed if we compare this with other wireless communication devices.

- **Data packets:** These are protected using a Cyclic Redundancy Check (CRC) (CRC-16 for speeds up to 1.152 Mbps, and CRC-32 at 4 Mbps).

1.2.3.3 IEEE Standards

Generally, 802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specify an over-the-air [NIST 800-12 Pietro 2007] interface between a wireless client and a base station (i.e. infrastructure mode) or between two wireless clients (i.e. ad hoc mode). The IEEE accepted the specification in 1997. As one of the 802.11 standards, 802.11 is applied to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). Most 802.11-family commercial products adopt DSSS. This standard defines the medium access control (MAC) and physical layers (PHY) for a LAN with wireless connectivity. It addresses local area networking where the connected devices communicate in the air to other devices that are within close proximity to one another. As an optional feature, the 802.11 standard includes the RTS/CTS (Request to Send/Clear to Send) function to control station access to the medium, in particular to handle the problem of hidden terminals. From early stages of wireless ad hoc networks research, 802.11 technologies have often been assumed and used as an underlying layer of Wireless ad hoc Networks routing protocol.

IEEE 802.11 has so far derived many supplemental and extended specifications of wireless LAN technologies. They are individually having wide variety of sophisticated features relative to the original 802.11: 802.11a, 802.11b, and 802.11g basically the were designed to provide higher-speed data transmissions up to 54 Mbps, 802.11e supports Quality of Service (QoS) in wireless LANs for multimedia applications, streaming video and provides the means of prioritizing the radio channel access by different stations and data streams, where as 802.11h

standards are try to avoid wireless interference by changing the frequency dynamically and enhance channel energy measurement and reporting mechanisms to improve spectrum and transmit power management of 802.11a, and 802.11i improves and enhances security and authentication mechanisms of 802.11 MAC.

1.2.3.4 Wi-Fi Devices

So we used to concern here with 802.11b, a, and g, since these would seem to be most appropriate wireless technologies for MANET. 802.11b (also referred to as 802.11 High Rate or Wi-Fi) is an extension to 802.11 and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet [Xiuli 2006David 2008]. 802.11b-compatible commercial wireless LAN products are most dominant, and most laptop computers install 802.11b wireless LAN interfaces by default. 802.11a is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing (OFDM) encoding scheme rather than FHSS or DSSS. 802.11g applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band. 802.11a and g compatible products have currently appeared to public, several advanced notebooks implement these wireless interfaces in the default.

1.2.3.5 Wi-Max

Wi-max technology is another and advance class of the 802.11 family is also known as 802.16 standards because this is also having the advance version of the Wi-Fi devices. Wi-Max (Worldwide Interoperability for Microwave Access) is a superset of Wi-Fi and is designed specifically for last-mile distribution and mobility [Gole 2004]. Wi-Max works with high speed (30 Mbps+). Wi-Max is a relatively new standard and thus, Wi-Max device products are expensive. Wi-Max specifically designed for wide area networks communications, but this advance technology having more expensive than Wi-Fi.

The bandwidth and range of Wi-MAX make it suitable for the following potential applications:

- Providing portability to the wireless node for the broadband connectivity across cities and countries through a variety of devices.
- Providing a wireless mode of communication alternative to cable and digital subscriber line for broadband access.
- Providing informational data, telecommunications (VoIP i.e. Voice Over Internet Protocol) and IPTV i.e. Internet Protocol Television services or triple play.
- Providing a source of Internet connectivity as part of a business as well as the educational and personnel purposes.

1.3 Applications of Wireless ad hoc Networks

Whenever a new technology or tool emerges for public use, the first question is how will it help me or what can it do for me? Here we will discuss in this section about the various benefits from applications [Xiuli 2006, Hyung 2006, Zhou 1999] of wireless networks in the private/Public and government sector. On the basis of the benefits, the technology becomes very much important to the people.

In the world recently we used to see around us different major applications of ad hoc wireless networks, but the main field is the digital battle field. In the tactical environment, mobile nodes could be individual soldiers, artilleries, missile/rockets launchers, trucks, helicopters, support vehicles, flying machines in the sky and even satellites at higher elevations. Each different kind of entity has different communication capabilities. So, it is reasonable to assume that the whole network is a heterogeneous environment. In this environment, different types of mobile nodes will have different types of motion behavior. Therefore, a flexible, portable and independent mobility platforms are required to model this hybrid motion patterns **Figure 1.2** depicts the application of wireless ad hoc networks figure(a) highlight the

applications Area of ad-hoc networks and the figure (b) depicts the information's about the disaster area like flood, earthquake etc. Some of the Wireless Networks applications are as below:

- Tactical Networks

  Military Communications and operations controls in the battle field environment

- Sensor Networks
  a) Collections of embedded sensor devices used to collect real time information to automate every functions of the system.
  b) Weather Monitoring.
  c) Earth movement sensing activities
  d) Ocean Engineering or well known as Underwater Sensor Networks

- Emergency Services
  a) Search and rescue operations and disaster recovery.
  b) Patient record retrieval system.
  c) Catastrophic disaster.
- Commercial Environment
  a) E-Commerce and online bill payment system
  b) Access the customer records from the fields
  c) Vehicular ad hoc Networks system.
- Educational Applications

  Video conferencing system and Virtual class room system

- Entertainment Applications

  Video on demand

- Other Applications
  a.) Cellular Phone
  b.) Bluetooth System

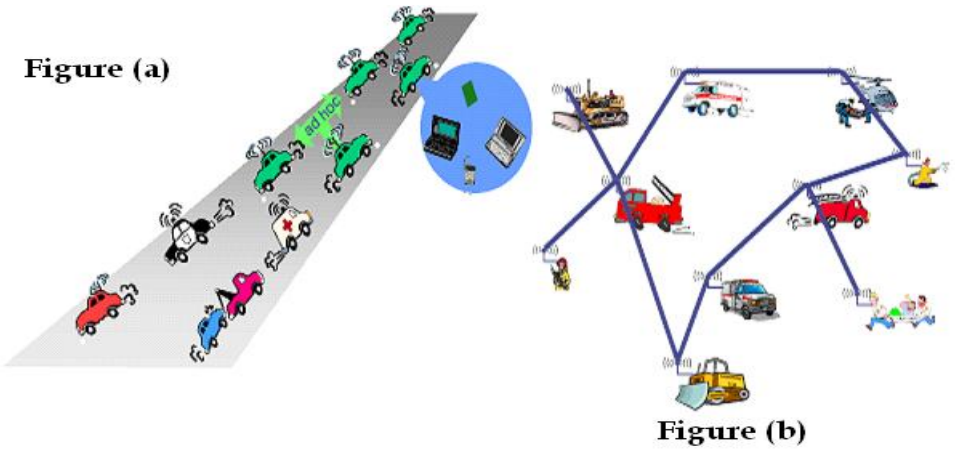

Figure 1.2: Applications of Wireless Networks

As the technology raises the need and importance of the resource become very high, and hence the Wireless ad hoc Networks have certain advantages over the traditional communication networks. Some of these advantages are:

- Use of ad hoc networks can increase mobility and flexibility, as ad hoc networks can be brought up and turn down in a very short time, as the Bluetooth device moves its information to its connective device, like other mobile and nodes without the concern of their internal technology of the nodes.

- Ad hoc networks can be more economical in some cases, as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes, like if the connections are to be needed for more devices the more cabling is required but for connecting the same with wireless communications no cost will be other than their energy efficiency.

- Ad hoc networks can be more robust than conventional wireless networks because of their non hierarchical distributed control and management mechanisms.

- Because of multi-hop support in ad hoc networks, communication beyond the line of sight is possible at high frequencies.

- Ad hoc networks may reduce the power consumption of wireless devices. More transmission power is required for sending a signal over any distance in one long hop than in multiple shorter hops. It can easily be proved that the gain in transmission power consumption is proportional to the number of hops made.

- Because of short communication links (multi-hop point-to-point communication instead of long-distance node to central base station communication), radio emission levels can be kept low. This reduces interference levels, increases spectrum reuse efficiency, and makes it possible to use unlicensed and unregulated frequency bands.

Examples of potential applications of Wireless ad hoc Networks are only limited by imagination. We may think of a group of people with laptop/computers at a conference who wish to exchange files and data without medium of any additional infrastructure. We also can think of deploying ad hoc networks in homes for communication between smart household appliances. Ad hoc networks are suitable to be used in areas where earthquakes or other natural disasters have destroyed communication infrastructure. Ad hoc networks perfectly satisfy military needs like battlefield survivability, operation without pre placed infrastructure and connectivity beyond the line of sight. **Figure 1.3** shows an interesting commercial application of ad hoc networks for local hazard warning on the road. Real-time hazard warning is just one possible commercial application of ad hoc communication networks.

A specific kind of ad hoc network is the sensor network [Secuk 2008,Wood 2003, Chris 2003Boyle 2007], where the nodes forming the network do not or rarely move. Sensor networks received much attention in recent years because they have huge potential applications. A sensor network is composed of a large number of sensor nodes which are densely deployed either inside the phenomenon to be

observed or very close to it. The positions of sensor nodes need not to be engineered or pre-determined. This allows random deployment in inaccessible terrains or in disaster relief operations. The physical dimensions of sensor nodes which can be in the order of a few cubic millimeters along with their low costs due to mass production make them suitable for many applications. Weather and seismological monitoring, inventory control, chemical and biological monitoring, and defense-related networks are just a few examples

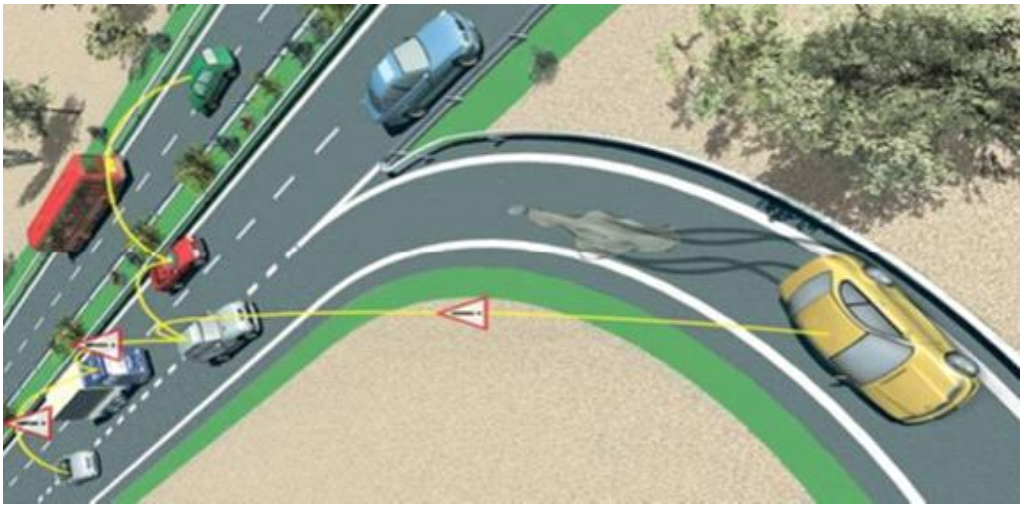

Figure 1.3: Commercial Application of ad hoc Networks

1.4 Challenges & Issues in Wireless adhoc Networks

In this technological era, when it becomes very dependable on the technology so now major requirement for the next generation wireless network is mobility management and performance enhancement [Pathan 2006, Xukai 2002, Padmavati 2009, Rouba 2005] which are the main concern. Mobility management implies the ability of the network to locate a Wireless node, routing incoming/outgoing cells/information(s) regardless of its network point of attachment and maintain connection while the wireless node roams in other different networks or network's loop. There are certain research methodological issues that need to be probed to improve the mobility management and

performance of envisioned next generation. The below written section will give the information regarding the challenges faced by the Wireless ad hoc Networks communications systems.

The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in in-depth protection that offers multiple lines of defense against many both known and unknown security threats. This new design perspective is what we call resiliency-oriented security design.

1.4.1 Technical and Research Challenges

Wireless ad hoc Networks having several technical and research challenges that need rectification. Although WANET's having so many benefits,[Wiechao 2003, Pathan2006, Haubaux 2004] such as self-reconfiguration, self healing and adaptability to highly variable nodes characteristics such as energy efficiency over information and data transmission and load balancing. These benefits pose new challenges which mainly reside in the unpredictability of network topology due to the mobility of nodes, which, coupled with the local broadcast capability, problems in protocol design for communication system, ad hoc wireless networks. To deal with such kind of issue, many verified potential approaches have been proposed: Dynamic routing, Service Location Protocol, Wireless configuration Protocol, and quality-of-service (QoS) based routing technique.

1.4.1.1 Technical Challenges in WANET's

Security has always been a major concern in networks where sensitive or confidential information is transferred. The vitality of the security is the most important thing in the wireless ad hoc networks as compared with other

traditional networks. In wireless communications [NIST 800-186, Goff 2001], an attacker can have the access over the network and steals or sniff the information without any physical connection to the network. So many wirelesses communicating technologies such as 4G Mobile, the recent technology and other many wireless technologies such as 3G mobile technologies and WLANs are already supporting the basic security mechanisms such as access security. However, some emerging wireless technologies such as wireless ad hoc and sensor networks have brought new and challenging security problems. Ad hoc networks have wide range of applications from military operations to civilian applications including disaster recovery and emergency services where the existing infrastructures get damaged. In ad hoc networks, mobile nodes act as a router in order to convey information from one node to another node. As the result, malicious nodes can not only eavesdrop and modify data packets but also launch a denial of service (DoS) attack by injecting bogus packets or simply dropping data packets. Identity spoofing, message tampering, black hole attack and Wormhole attack are a few examples of the attacks that can be employed by malicious nodes. Moreover, providing security in ad hoc networks is a very challenging problem due to the unique network characteristics such as dynamic topology, lack of centralized infrastructure and limited bandwidth, battery lifetime and computational power. Effective security solutions require considering not only all these characteristics but also all possible attacks in the entire protocol stack. Clearly, ad hoc networks security requirements such as key distribution, secure routing and intrusion detection need to be addressed in order to deploy them in a potentially hostile environment. Wireless mesh network (WMN) is also a promising wireless technology with many emerging applications such as broadband home networking and community networks. WMNs and ad hoc networks have similar security problems. However, WMN may need different security mechanism as it has a rather different architecture than an ad hoc network. Providing security for WMNs is also challenging problems which need to be addressed in order to convince the customers to

subscribe to the service, energy efficiency, unpredictability about networks topology due to nodes mobility, broadcast capability regarding communications.

1.4.1.2 Research Based Challenges

However, many other research areas are very important including: protocols, Security, localization, topology control, dependability, self-calibration, self-healing, data aggregation, group management, clock synchronization, query processing, sensor processing [NIST 8000-186], fusion under limited capacities, and testing and debugging. Wireless networks are a fascinating area with great potential. The impact of this area on the world can rival the impact that the Internet has had. Exciting and difficult research challenges lie ahead before this becomes reality.

Wireless Networks are limited in their energy, computation, and communication capabilities. In contrast to traditional network, network nodes are often deployed in accessible areas, presenting a risk of physical attacks. A key to the growth of WSN is raising the level of abstraction for programmers. Currently, programmers deal with too many low levels details regarding sensing and node to node communication. For example, they typically deal with sensing data, fusing data and moving data. They deal with particular node to node communication and details. If we raise the level of abstraction to consider aggregate behavior, application functionality and direct support for scaling issues then productivity increases.

1.5 Analytical Characteristics of Wireless Networks

The technology of wireless communication landscape has been changing dramatically, driven by the rapid advances in wireless technologies and the greater selection of new wireless services and applications [Liu 2003, Capkun 2001]. The emerging third-generation cellular networks have a greatly improved data

transmission speed, which ensures a variety of higher-speed mobile data services. Meanwhile, new standards for short-range radio such as Bluetooth, 802.11 and infrared transmission are helpful in creating a wide range of new applications for enterprise and home networking, enabling wireless broadband multimedia and data communication in the office and at home.

Before making any technical comments on these technologies and applications, we first examine some of the main characteristics of wireless communication as related to specification, configuration and classification of these networks, and then review the key capabilities exhibited by various types of wireless networks.

1.5.1 Wireless Communication Characteristics

In general, wireless networking refers to the use of infrared or radio frequency signals to share information and resources between wireless communicating devices. Many different types of wireless devices are available today like mobile terminals, pocket size PCs, hand-held PCs, laptops, Mobile Phones of different companies, PDAs, wireless sensors, and satellite receivers, among others.

Ad hoc network gives a major silent feature[Capkun 2003, Stephen 2002, Charles 2002, NIST 180-1] over the Traditional Network System, these characteristics are dynamic network topologies, bandwidth-Constrained and variable-capacity link, energy efficiency technological operations and but the networks have very limited physical security and the maximum work is done on the security aspects of the system because this is the infancy phase of the security, due to the varying capacities found in the available layer of these systems; wireless devices and network show the distinct characteristics as compared to the existing traditional networks/Wired networks counterparts, specifically, if we see in the existing wired networks are:

1. Higher interference results in lower reliability.

a. In the traditional networks, like Infrared signals suffer interference from sunlight and heat sources, and can be shielded or absorbed by various objects and materials. Radio signals usually are less prone to being blocked; however, they can be interfered with by other electrical devices.

b. The broadcast nature of transmission means all devices are potentially interfering with each other.

2. Low bandwidth availability and much lower transmission rates, typically much slower-speed compared to traditional networks, causing degraded quality of service, including higher jitter, delays, and longer connection setup times.

3. Highly variable network conditions:

    a. Higher data loss rates due to interference

    b. User movement causes frequent disconnection

    c. Channel changes as users move around

    d. Received power diminishes with distance

4. Limited computing and energy resources: limited computing power, memory, and disk size due to limited or low battery capacity, as well as limitation on device size, weight, and cost.

5. Limited service coverage: Due to device, distance, and network condition limitations, service implementation for wireless devices and networks faces many constraints and is more challenging compared to wired networks and elements.

6. Limited transmission resources:

a. Medium sharing

b. Limited availability of frequencies with restrictive regulations

c. Spectrum scarce and expensive

7. Device size limitation due to portability requirements results in limited user interfaces and displays.

8. Weaker security: because the radio interface is accessible to everyone, network security is more difficult to implement, as attackers can interface more easily.

1.5.2 Types of Wireless Networks

Many types of wireless networks exist, and can be categorized in various ways set out in the following subsections depending on the criteria chosen for their classification.

1.5.2.1 Network Formation and Architecture

Wireless networks can be divided into two broad categories [Xukai 2002, Aime 2006, Zhou 1999] based on how the network is constructed and the underlining network architecture:

a) **Infrastructure-based network:** A network with pre-constructed infrastructure that is made of fixed and wired network nodes and gateways, with, typically, network services delivered via these preconfigured infrastructures. For example, cellular networks are infrastructure-based networks, base stations, and mobile hosts. Each node has its specific responsibility in the network, and connection establishment follows a strict signaling sequence among the nodes.

b) **Infrastructure-less** (ad hoc) network. In this case a network is formed dynamically through the cooperation of an arbitrary set of independent nodes. There is no prearrangement regarding the specific role each node should assume. Instead, each node makes its decision independently, based on the

network situation, without using a preexisting network infrastructure. For example, two PCs equipped with wireless adapter cards can set up an independent network whenever they are within range of one another. In mobile ad hoc networks, nodes are expected to behave as routers and take part in discovery and maintenance of routes to other nodes.

1.5.2.2 Communication Coverage Area

As with wired networks, wireless networks can be classified into different types based on the distances over which data is transmitted:

a) Wireless Wide Area Networks (Wireless WANs): Wireless WANs are infrastructure-based networks that rely on networking infrastructures like MSCs and base stations to enable mobile users to establish wireless connections over remote public or private networks. These connections can be made over large geographical areas, across cities or even countries, through the use of multiple antenna sites or satellite systems maintained by wireless service providers. Cellular networks (like GSM networks or CDMA networks) and satellite networks are good examples of wireless WAN networks.

b) Wireless Metropolitan Area Networks (Wireless MANs): Wireless MAN networks are sometimes referred to as fixed wireless. These are also infrastructure-based networks that enable users to establish broadband wireless connections among multiple locations within a metropolitan area, for example, among multiple office buildings in a city or on a university campus, without the high cost of laying fiber or copper cabling and leasing lines. In addition, Wireless MANs can serve as backups for wired networks should the primary leased lines for wired networks become unavailable. Both radio waves and infrared light can be used in wireless MANs to transmit data. Popular technologies include local multipoint distribution services (LMDS)

and multichannel multipoint distribution services (MMDS). IEEE has set up a specific 802.16 Working Group on Broadband Wireless Access Standards that develops standards and recommended practices to support the development and deployment of broadband wireless metropolitan area networks.

c) Wireless Local Area Network (Wireless LANs): Wireless local area networks enable users to establish wireless connections within a local area, typically within a corporate or campus building, or in a public space, such as an airport, usually within a 100 m range. WLANs provide flexible data communication systems that can be used in temporary offices or other spaces where the installation of extensive cabling would be prohibitive, or to supplement an existing LAN so that users can work at different locations within a building at different times. Offices, homes, coffee shops, airports etc. represent the typical hotspots for wireless LAN installations. Wireless LANs can operate in infrastructure-based or in ad hoc mode. In the infrastructure mode, wireless stations connect to wireless access points that function as bridges between the stations and an existing network backbone. In the ad hoc mode, several wireless stations within a limited area, such as a conference room can form a temporary network without using access points, if they do not require access to network resources. Typical wireless LAN implementations include 802.11 (Wi-Fi) and Hiperlan2. Under 802.11a and 802.11b, data can reach transmission speeds between 11 Mbps to 54 Mbps.

d) Wireless Personal Area Networks (Wireless PANs): Wireless PAN Technologies capacitate users to setup ad hoc, wireless communication among personal wireless devices such as PDAs, cellular phones, or laptops that are used within a personal operating space, typically up to a 10 meter range. Two key Wireless PAN Technologies are Bluetooth and infrared light. Bluetooth is a cable-replacement technology that uses radio waves to transmit data to a distance of up to 9–10 m, whereas infrared can connect devices within a 1 m range. Wireless PAN is gaining momentum because of its low

complexity, low power consumption, and interoperability with 802.11 networks.

1.5.2.3 Access Technology

Depending on the specific standard, frequency, and spectrum usage, wireless networks can be categorized based on the access technology used. These include:

GSM networks

TDMA networks

CDMA networks

1.6 Wireless ad hoc Networks in present Scenario:

The problem with defending wireless ad hoc networks [Selcuk 2008, Songbo 2009, Rivest 1978] is that existing security technologies are meant for the purpose of traditional networks i.e. wired networks, so the exiting technologies are static to the wired rather than wireless technologies. Security protocols used for the wireless to inspect the suspicious behavior are not completely fit for the existing one. In case of wireless ad hoc networks where the network entities often move around and this results in frequent changes in the structure of the network. The traditional security protocols which exist are also dependent on a few centrally located devices for managing the security of the network. So it doesn't provide better solutions which can be completely applicable to wireless ad hoc network on account of the existing architecture of these networks. The increased vulnerabilities of ad hoc networks and the limitations of existing security solutions are designed for woks only for wired networks.

1.6.1 Threats, Attacks and Vulnerability

Wireless ad hoc networks are having so many limitations [Karlof 2003, Hu 2003, Imad 2004, Perrig 2003, Chun 2003] on which there are having some relatively problems to this networks as are threat, attacks, and vulnerabilities. In this world, if there exists a system based on more security techniques then also it will always be

effected by it weakness and vulnerability also, hence no system is perfect in this new technological world, there will always be the problems of attack from the unauthorized source of technology of logics and will always be targeted. Hence, one approach to designing security mechanisms for systems is to look at the threats that the system would face and the possible attacks given the vulnerabilities. The designed security protocols should then ensure that the system is secure in the views of these threats, attacks, and vulnerability paradigms. So in this section we are moving to have acquaintance with the definitions of the terms, threat, vulnerability, and attack.

- **Threat** is the thought of technology [Johnson 2003, Zhang 2000, Seung 2001] through which to provide the ability or intent of an agent to adversely affect an automated network system, facility or operation can be manifested. All methods or things used to exploit a weakness in a system, operation, or facility constitute threat agents. Examples of threats include hackers, employees, industrial espionage, national intelligence services, and criminal organizations.
- **Vulnerability** is any hardware, firmware, or software flaw [Golle 2004] that leaves an information system open for potential exploitation. The exploitation can be of various types, such as gaining unauthorized access to information or disrupting critical processing.
- **Attacks** are an attempt to have control over the security [Baghtiar 1995, Safdar 2010, Jose 2011] of any system or organizations. The attack may alter, release, or deny data. The success of an attack depends on the vulnerability, and the effectiveness of existing technology. Examples of attacks include actions such as spoofing, obtaining illegitimate privileges, inserting false information, modifying information, analyzing and modifying network routes, obtaining illegitimate access to systems through social engineering, or disrupting network operation using malicious software. Although the attacks are of many categories but the every concerns with two

main categories of Attacks on Wireless ad hoc Networks []. Hence we divides them into two main categories:

a) **Passive Attacks:** In such types of attack an attacker passively listens to the packet or a listener is just the wireless medium by sniffing the mode of route. Since an attacker only listens to the packets that are passing by without modifying or tampering with the packets, these attacks mainly target the confidentiality attributes. Typically such kind attacks are much easier to launch than the next type of attacks.
b) **Active Attacks:** such type of active attacks are those attacks where the attacker takes malicious action in addition to passively listening to on-going route. For example an attacker might choose to modify packets, inject packets, or even disrupt network services. Ad hoc networks that make extensive use of wireless links are vulnerable to several types of attack due to the inherent nature of the network.

Hence some technical thoughts of mechanisms such as encryption and authentication can greatly mask the vulnerabilities on the wireless communications, but these are not the only insufficient but also vulnerabilities in ad hoc networks. Since wireless ad hoc networks cannot depend upon infrastructure-based resources or centralized form of resource, such as stable power source, high bandwidth, continuous connectivity, or fixed routing, so it become more easy to launch attacks on them.

1.6.1.1 Threats

This is a scientific based pragmatic approach to building a secure system or the organization is to consider the threats that the system might face after the installation in real world and that can categorize it in three ways such as amateur, professional and well-funded adversary. Examples of amateur adversaries are script kiddies or hobbyist hackers. Criminal person or terrorist organizations can be considered to be professional adversaries. Foreign intelligence based services can be regarded as a well-funded adversary. The above categorization implicitly governs the types of

attacks that can be launched by each type of adversary. Amateur adversaries can launch unsophisticated attacks such as wireless sniffing or denial of service. A professional adversary can launch more sophisticated attacks such as layer two hijacking, man-in-the-middle attack, or Sybil attack. A well-funded adversary does not have any constraints on money. Such an adversary can launch very sophisticated attacks such as rushing attacks, wormhole attacks.

A malicious node can modify the correct functioning of a routing protocol by making modifications in routing information, by fabricating false routing information and by impersonating other networks nodes. In recent days the maximum research work is carried on attacks and threats and on the basis of various attacks the threats is again categorized as given below:

1.6.1.1.1 Using Modifications

In Networks technology, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out motives for the targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Existing routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Malicious nodes can easily cause traffic subversion and denial of service (DoS) by simply altering these fields. Such attacks compromise the integrity of routing computations. By modifying routing information, an attacker can cause network traffic to be dropped, be redirected to a different destination, or take a longer route to the destination, thus increasing communication delays.

Below are details of several attacks that can occur if particular fields of routing messages in specific routing protocols are altered or falsified.

a) **Redirect modified route sequence**

Some of the protocols instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes toward specific destinations, any node may divert traffic through itself by advertising a route to a node with a *destination sequence num* greater than the authentic value.

b) **Redirect modified hop counts**

A redirection attack is possible by modification of the hop count field in route discovery messages. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, malicious nodes can increase the chances they are included in a newly created route by resetting the hop count field of the RREQ to zero. Similarly, by setting the hop count field of the RREQ to infinity, created routes will tend not to include the malicious node.

c) **DoS with modified source routes**

In the denial-of-service, a malicious node in between can successfully send an erroneous route message to the source route to disrupt the service. Dynamic source routing techniques utilize the source routes, so this techniques explicitly stating routes in data packets. These routes lack any integrity checks and a simple denial-of-service attack can be launched in DSR by altering the source routes in packet headers, such that the packet can no longer be delivered to the destination.

d) **Tunneling**

Ad hoc networks have an implicit assumption that any node can be located adjacent to any other node. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. Vulnerability is that two such nodes may collaborate to falsely represent the length of available paths by encapsulating and tunneling between them thus legitimate routing messages generated by other nodes. In this case, tunneling prevents honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

1.6.1.1.2 Using Impersonations

This is a one kind of act performed by the unauthorized person for showing himself as different as he. So this is the one kind of cyber attack on the networks technology. Impersonations by Spoofing: Since current ad hoc routing protocols do not authenticate or tends to find genuineness of routing packets, a malicious or unauthenticated node can launch many attacks in a network by masquerading as another node (spoofing i.e. a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage). Spoofing occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather. As an example, a spoofing attack allows one to create loops in routing information collected by a node with the result of partitioning the network.

1.6.1.1.3 Using Fabrications

The generation of false routing messages can be classified as fabrication attacks. Such attacks can be difficult to verify as invalid constructs, especially in the case of fabricated error messages that claim that a neighbor cannot be contacted. The notation “fabrication” is used when referring to attacks performed by generating false routing messages or self generated routing massages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages claiming that a neighbor can no longer be contacted. This is like a Falsifying Route Errors in protocols; Protocols implement path maintenance to recover broken paths when nodes move. If the source node moves and the route is still needed, route discovery is re-initiated with a new route request message. If the destination node or an intermediate node along an active path moves, the node upstream of the link break broadcasts a route error message to all active upstream neighbors. The node also invalidates the route for this destination in its routing table.

1.6.1.2 Attacks

As we come to depend more and more on network services, so the stability and security of those networks become much more important than ever. The world of business and mass practice has adopted information technology to help various processes, increase productivity, and cut costs. As such, a company's IT infrastructure is often a core asset, and many businesses would cease to function if disasters were to significantly disrupt their network operations. At the same time, the widespread adoption of the Internet as a global communication medium has also brought computer network out of the business and academic world into our personal lives. That largest of networks is now used not only for information and entertainment, but also as a means to keep in touch with friends, family, and loved ones. In this sub section we discuss the various kind of attacks that can have on recent network services.

1.6.1.3 Vulnerability in WANET's

The vulnerability in that routing attacks can be launched by sending false route error messages. Suppose node S has a route to node X via nodes A, B, C, and D, as in Figure 1.4. A malicious node M can launch a denial-of-service attack against X by continually sending route error messages to B spoofing node C, indicating a broken link between nodes C and X. B receives the spoofed route error message thinking that it came from C. B deletes its routing table entry for X and forwards the route error message on to A, who then also deletes its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to X, M can successfully prevent communications between S and X.

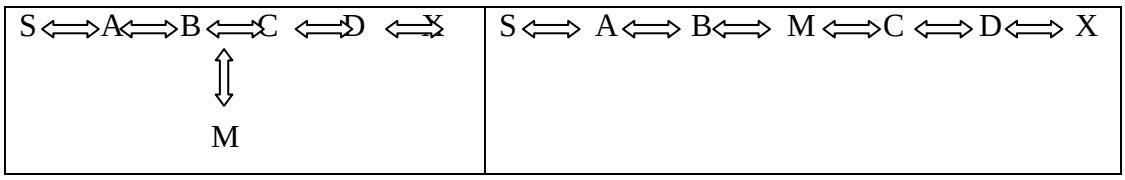

Figure 1.4: DoS Attack on WANETs

1.7 WANetworks Contribution In Present Era

A major contribution of the research is review of both proactive and reactive routing protocols used in WANETs Applications likes Vehicular adhoc Network, Wireless Sensor Network (WSN) environment. Previously, the available research work was focused on the evaluation of reactive routing protocols, and very little works is includes in proactive routing protocols. This study has been carried out with the intention to fill this gap. Moreover, another significant contribution of this thesis is the use of simulators and their integration at the runtime, to facilitate a realistic simulation scenario. With the help of this integration we were able to create an emergency scenario and study its effects on the performance of the secure routing protocols. This technique is still maturing and is at very early stage of its development.

1.8 Problem Description:

Objective of this thesis is to propose and implement the security techniques based on cryptographic techniques so as to protect the Wireless adhoc Networks and the work is carried out theoretically as well as on simulator based analysis and the research study is based on the existing security techniques and protocols and different kinds of attack on routing protocols.

The thesis also attempt to include the goal to generate a Simulated environment that could be used as platform for further studies within the area of Wireless adhoc Networks. This simulated environment is implemented on NS-2.29 simulator.

The goal of this thesis is to:

a) Get a general understanding of Wireless adhoc Networks.
b) Generate a simulation environment for further research and studies.
c) To implement some New Security Techniques and methodology for Wireless adhoc Networks.

d) Analyzing the security methodology/Techniques theoretically as well as through simulator tolls.
e) Recommends an Optimized Security Techniques (OST) for Wireless adhoc networks.

1.9 Summary

Previously, the available research wok was focused on the evaluation of reactive or proactive routing protocols only, and did not secure routing protocols. This study has been carried out with the intention to fill this gap. Moreover, another significant contribution of this thesis is the use of both wireless nodes and network simulators and their integration at the runtime, to facilitate a realistic simulation scenario. With the help of this integration we were able to create an emergency scenario and study its effects on the performance of the routing protocols. This technique is still maturing and is at very early stage of its development by the research community.

At the time of writing, this thesis is the only research work that makes use of integrated approach and evaluated routing protocols. We present our new protocol; it ensures a high detection rate and minimizes the risk of a denial of service caused by false alarms, even in the presence of a large number of malicious nodes.