CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Wireless networks are gaining popularity to its peak today, as the user’s wants wireless connectivity irrespective of their geographic position. Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them. One of the reasons for popularity of these networks is wide penetration of wireless devices. Wireless applications and devices mainly emphasize on Wireless Local Area Networks (WLANs). This has mainly two modes of operations, i.e. in the presence of Control Module (CM) also known as base stations and ad hoc connectivity where there is no control module. Ad hoc networks do not depend on fixed infrastructure to carry out their operations. The operation mode of such network is stand alone, or attached with one or more points to offer internet and connectivity to cellular networks. These networks exhibit the same conventional problems of wireless communications i.e. bandwidth limitations, battery power, enhancement of transmission quality and coverage problems.

1.1.1 Network

Before going into the details of wireless network it is important to understand the concept of network and different kind of networks available today.
Any collection of devices/computers connected with each other by means of communication channels that help the users to share resources and communicate with other users. There are two main types of network i.e. wired network and wireless network.

1.1.2 Wired Networks

In wired network the devices are attached to each other with the help of wire. The data is transmitted from one point of the network to other point of the network by using wire as a medium of communication.

1.1.3 Wireless Networks

Wireless network is a network in which, computer devices communicates with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lay within the radio range of each other. Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

1.2 TYPES OF WIRELESS NETWORKS

Wireless networks are getting popular due to their ease of use. Consumer/user is no more dependent on wires where he/she is, easy to move and enjoy being connected to the network.

One of the great features of wireless network that makes it fascinating and distinguishable among the traditional wired network is mobility. This feature gives user the ability to move freely, while being connected to the network. Wireless networks are comparatively easy to install
than wired network. There is nothing to worry about pulling the cables/wires in wall and ceilings. Wireless networks can be configured according to the need of the users, which can range from small to large number of users. Wireless networks are very useful for areas where the wire cannot be installed like hilly areas. On the basis of coverage area the wireless network can be divided into three types as follows

1) Personal Area network
2) Local Area Network
3) Wide Area Network

**Personal Area Network:** Personal area network is used for communication between computer devices close to one person. Some of the personal area networks are zigbee, Bluetooth and sensor networks. Bluetooth is low cost wireless connection that can link up devices. These devices normally work within 10 meters, with access speed up to 721 Kbps. This technology is widely used in a range of devices like computer and their accessories i.e. mouse and keyboard, PDAs, printers and mobile phones etc. It is important to understand that Bluetooth as Wireless Personal Area Network (WPAN) is not 802.11 wireless as it do not perform the same job, rather used as wireless replacement for cable to connect devices. Bluetooth works at 2.4 GHz band and this may cause interference with wireless LAN equipments (802.11b, 802.11g).

**Local Area Network:** Wireless local area network (WLAN) is standardized by Institute of Electrical and Electronics Engineer (IEEE). In local area network the users communicate with each other in local coverage area i.e. building or a campus. WLANs are the substitute for the conventional wired LANs. WLAN is wireless medium that is shared by the devices within the WLAN. WLANs have gained a great amount of popularity. Keeping in mind
their mobility feature, they are implemented in mobile devices like laptop, PDAs, mobile cell phones etc. as indicated by Dow et al (2005). In WLAN, wireless ethernet protocol, IEEE 802.11 is used.

WLAN proposed by Crow et al (1997) is mainly used for establishing the connection with internet. The data rate of WLAN is low that is between 11 and 54 Megabits per second (Mbps) as compared to the wired LAN which operates at 100 to 1000 Mbps. This means that any activity that need high bandwidth, are better done on wired network than on wireless.

Wide Area Network: Wireless wide area network (WWAN) cover geographically larger area than local area network. The wide area networks almost consist of one or two local area networks. Examples of WWAN are satellite systems, paging networks, 2G and 3G mobile Cellular.

1.3 AD HOC NETWORKS

Ad hoc networks have no infrastructure where the nodes are free to join and leave the network. The nodes are connected with each other through a wireless link. A node can serve as a router to forward the data to the neighboring nodes. Therefore this kind of network is also known as infrastructure less networks. These networks have no centralized administration. Ad hoc networks have the capability to handle any malfunctioning of nodes or any changes that it experience due to topology changes. Whenever a node in the network is down or leaves the network, its link between other nodes are broken. The affected nodes in the network simply request for new routes and new links are established ad hoc network can be categorized in to static ad hoc network (SANET) (Jeffrey.E.Wieselthier et al 2001) and mobile ad hoc network (MANET).
1.3.1 Static Ad hoc Networks

In static ad hoc networks the geographic location of the nodes or the stations are fixed. There is no mobility among the nodes in the networks, thus they are known as static ad hoc networks.

1.3.2 Mobile Ad hoc Networks

Mobile ad hoc network is an autonomous system, where nodes/stations are connected to each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes can join or leave at any point of time. This property of the nodes makes the mobile ad hoc networks unpredictable from the view-point of scalability and topology.

Figure 1.1 Mobile ad hoc Networks
1.4 HISTORY OF MOBILE AD HOC NETWORKS

The whole life-cycle of ad hoc networks can be categorized into first, second, and third generation ad hoc network systems. The Present ad hoc networks systems are considered as the third generation.

The first generation of wireless ad hoc networks dates back to 1972. At the time, they are called PRNET (Packet Radio Networks) (Huang and Tseng 2003). In conjunction with ALOHA and CSMA (Carrier Sense Multiple Access), approaches for medium access control and a kind of distance-vector routing, PRNET are used to offer different networking capabilities in a combat environment.

The second generation (Murthy and Manoj 2005) of Ad hoc networks emerged in 1980s, when the ad-hoc network systems are further enhanced and implemented as a part of SURAN (Survivable Adaptive Radio Networks) (Freebersyser and Leinerr 2001) program. This provides a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

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 a collection of mobile nodes was proposed at several research conferences.

The IEEE 802.11 subcommittee had adopted the term "ad-hoc networks" and the research community had started to look into the possibility of deploying ad-hoc networks in other areas of application.
GloMo (Global Mobile Information Systems) (Leiner et al 1996) and the NTDR (Near-term Digital Radio) (Ruppe et al 1997) are results of these efforts. GloMo was designed to provide an office environment with ethernet-type multimedia connectivity anywhere and anytime in handheld devices.

NTDR is the only "real" non-prototypical ad-hoc network that is in use today. It uses clustering and link-state routing, and is self-organized into a two-tier ad hoc network. Development of different channel access approaches are now in the CSMA/CA and TDMA molds, and several other routing and topology control mechanisms are some of the other inventions of that time.

Later on, in mid-1990s, within the Internet Engineering Task Force (IETF), the mobile ad hoc Network working group was formed to standardize routing protocols for ad-hoc networks. The development of routing within the working group and the larger community resulted in the invention of reactive and proactive routing protocols.

Soon after, the IEEE 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable for building mobile ad-hoc networks prototypes out of notebooks and 802.11 PCMCIA (Personal Computer Memory Card Proceedings of the Association cards). Wireless local area products (IEEE 802.11, Hiperlan) (Arndt Kadelka and Arno masella 2001) provide in-building wireless access, however, they are usually deployed as access links. The packet relaying is performed by traditional bridges or routers. Bluetooth is a low cost technology for short range communication, its market is targeted towards PCs, phones, appliances, watches, etc. It allows multiple nodes to get connect to each other in a multi-hop arrangement.
Efforts are on to standardize different existing schemes for different network controls in a single framework that could be taken as a standard for all the applications which uses ad hoc networks as its networking technology. Wireless devices are getting smaller, cheaper, and more advanced. As these devices become more ubiquitous, organizations are looking for inexpensive ways to keep these devices connected. Building an ad-hoc network could make this happen.

Wireless ad hoc networks can broadly be classified into three categories:

- Mobile ad hoc networks (MANETs)
- Wireless Sensor Networks
- Wireless Mesh Networks.

Each one of these has significance for different application areas, each of these differs in the capacity and capabilities of nodes that participate in the network, the purpose of the network and the communication protocols employed. The focus of this thesis is MANETs, from this point onwards, the words MANETs and wireless ad hoc networks will be used interchangeably.

1.5 CHARACTERISTICS OF MANETS

When a node wants to communicate with another node, the destination node must lie within the radio range of the source node that wants to initiate the communication. The intermediate nodes within the network aids in routing the packets from the source node to the destination node. These networks are fully self organized, having the capability to work anywhere without any infrastructure. Nodes are autonomous and play the role of router and host at the same time. MANET is self governing, where there is no
centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other. The network can be set up anywhere without any geographical restrictions. One of the limitations of the MANET is the limited energy resources of the nodes.

The characteristics of an ad hoc network can be divided into five main areas:

1) **Dynamic Topology.** Ad hoc network is an infrastructure-less mobile network, which means that the mobile nodes are free to move. In addition, a change in the radio frequency, change in the environment, and disturbance from different signals, will affect the network topology.

2) **Bandwidth is limited:** Compared with wired infrastructure network, the usable bandwidth is much lower in an Ad hoc network. This is because communication among mobile nodes uses radio frequency waves, and the strength of the waves will fade during transmission.

3) **Limited Power Supply:** Since the power supply to mobile nodes comes from the battery, the performance of the network deteriorates as the power consumption of the mobile nodes increases.

4) **Multi-hop Communication:** Based on the limited transmission range of wireless network, the source node and the destination node are usually not on the same radio frequency range. Thus, multi-hop communication is used in ad hoc network for long distance data transmission between the source and the destination nodes.
5) **Lower Security:** Since the communication among the mobile nodes in an ad hoc network is wireless, data packets are easily attacked by snooping, resending, modification and falsification. It will affect the overall network performance.

From the above, it is clear that a reasonable routing protocol must take into consideration the features mentioned.

### 1.6 APPLICATIONS OF MANETS

The properties of MANET make it much favourable that would bring many benefits. There are many research areas in MANET which are under study now. One of the most important areas where MANETs are applied is emergency services such as disaster recovery and relief activities, where traditional wired network is already destroyed. There are many other application areas such as entertainment, education and commercial where MANETs are playing their role for connecting people.

An ad hoc network is a wireless technology which supports various applications, such as:

1) **Mobile meeting:** In an outdoor environment, all ad hoc network users can work together on one project by using a temporary network. In an office environment, users can use PDA to download email or update their duty schedule on the internet through an Ad hoc network.

2) **Home and personal networks:** Create a Small Office Home Office (SOHO) environment to work from home. ad hoc network users can also control the home electric appliances such as the TV set, air-conditioner, etc, by using personal wireless devices.
3) **Emergency search and rescue**: Establish an ad hoc network to help emergency search and rescue workers communicate with each other in an infrastructure-less environment and in other emergency environment situations.

4) **Sensor network**: Sensor devices can work in some dangerous situations, like gas leak. People provide information on accidents by using the sensor devices in an ad hoc network. They do not need to enter dangerous sites.

5) **Military wireless communications**: In the battlefield, frequent communication is necessary among soldiers and vehicles. This kind of communication network is a typical ad hoc network. Ad hoc network was used during the 2nd Iraq War.

An example of ad hoc network application in the military context is shown below:

Self-Healing Minefield system (SHM) had been developed by a US government agency, DAPRA, from 2000 to 2003 (Rider 2002). In this system, the intelligent mobile antitank landmines are used to counter the enemy. These landmines are embedded with the modules for wireless communication and self-organization, which literally create an ad hoc network in the battlefield. SHM can change the topology of the minefield, automatically, after an enemy attack. These antitank landmines will self-detonate when the network cannot be reestablished. Thus, the SHM can provide a highly effective military obstacle in a war. This system uses Frequency Hop Spread Spectrum (FHSS) model to communicate, in an 83MHz bandwidth and 2.4GHz wave frequency.
1.7 SECURITY IN MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of the network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, dynamic topology, lack of central monitoring and management, absence of cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

Recently in the past few years security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However mobile ad hoc networking is still in need of further discussions and development in terms of security (Biswas and Ali 2007). With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network, the mobile ad hoc network is different. The routing protocols designed majorly for internet is different from the mobile ad hoc networks (MANET). Traditional routing table is basically made for the hosts which are connected through wires to a non-dynamic backbone (Pegueno and Rivera 2006). Due to which it is not possible to support ad hoc networks.

Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks (Lu et al 2009).

Major vulnerabilities faced by MANETs include selfishness, dynamic nature, severe resource restriction and open network medium.
Despite the above said issues, there are attacks which can be categorized in to passive, active, internal and external attacks.

MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication (Paolo Santi 2005). Mobile nodes present within the range of wireless link can overhear and participate in the network.

1.7.1 Flaws in MANETS

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main authority that keeps tracking of the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and are discussed as below.

1) **Non secure boundaries:** MANET is vulnerable to different kind of attacks due to non secure boundary. The nature of MANET, nodes have the freedom to join and leave the network. Node can join a network automatically if the network is in the radio range of that node, thus it can communicate with other nodes in the network. Due to non secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. The links are compromised and open to various attacks. Attacks on the link interfere between the nodes and
then invading the link, destroying the link after performing malicious behavior.

There is no protection against attacks like firewalls or access control, which may expose the vulnerability of MANET to attacks. Spoofing of node’s identity, data tampering, confidential information leakage and impersonating node are the results of such attacks when security is compromised (Parsons and Ebinger 2009).

2) **Compromised Node:** Some of the attacks get access inside the network to get control over the nodes in the network. Some attacks use unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous (Roy et al 2009). Due to this autonomous factor it becomes difficult for mobile nodes to prevent malicious activity during communication. Ad hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. Impact of threats from internal nodes in the network is more dangerous than threats from External ones.

3) **No Central Management:** MANET is a self-configurable network, which consists of mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets (Shanti et al 2009). MANET works without any preexisting infrastructure. This lack of centralized management makes MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly
dynamic and for large scale ad hoc network is very difficult due to no central management. When there is a central entity monitoring the network by applying proper security and authentication can decide which node should join the network by filtering the attacking nodes. The node connect with each other on the basis of blind mutual trust on each other, a central entity can manage this by applying a filter on the nodes to find out the suspicious one, and let the other nodes know which node is suspicious.

4) **Problem of Scalability**: In traditional networks, where the network is build and machines are connected to each other with the help of wires. The scalability of the network is designed at the initial phase of the network design and is not expected to change during the usage.

The case is quite opposite in MANETs because the nodes are mobile. The scale of the MANETs keeps changing due to the mobility nature of nodes. It is too hard to predict the numbers of nodes that will participate in the MANETs. The nodes are free to move in and out of the ad hoc network which makes them very much scalable and shrinkable. The protocols and services of MANET should be designed in such a way to accommodate above said issues.

### 1.8 Classification of Attacks

The attacks can be categorized on the basis of the source which originates the attacks i.e. internal or external, and on the behavior of attack i.e. passive or active attack. This classification is important because the attacker can exploit the network either as internal or external and as active or passive.
1.8.1 External and Internal Attack

**External attack:** External attackers mainly exist outside the networks they want to get access to the network and once they get access they start sending bogus packets and perform denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated.

**Internal Attack:** In internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access to the network as a new node either by compromising a current node or by malicious impersonation. Impact of the internal attack is more severe than that of external attacks.

![Figure 1.2 External and Internal Attacks in MANETs](image)

1.8.2 Active and Passive Attack

The attacker disrupts the performance of the network by stealing the important information and by destroying the data during exchange (Wei et al 2007).
Active attacks: They may be an internal or an external attack. To degrade the performance of network the active attack acts as an internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to inject bogus packets or perform denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the messages.

Passive Attack: Attackers in passive type do not disrupt the normal operations of the network (Wei et al 2007). In this type of attack, the attacker listens to the network in order to get information about it. Further it monitors the network to understand how the nodes are communicating with each other, and to know how are they located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily inject attacks in to the network.

![Figure 1.3 Active and Passive Attacks in MANETs](image)

1.9 ROUTING PROTOCOLS IN MANETS

The highly dynamic natures of the mobile nodes create frequent and unpredictable network topology changes. This topology change increases the routing complexity among the mobile nodes within the network. Therefore the traditional routing algorithms do not guarantee effective routing
in MANET. Routing in a MANET depends on many factors like topology, selection of routers, and location of request initiator and specific underlying characteristics that could serve as a heuristic in finding the path quickly and efficiently. This makes the routing area perhaps the most active research area within the MANET domain. Especially over the last few years, numerous routing protocols and algorithms have been proposed and their performance under various network environments and traffic conditions are closely studied and compared.

1.9.1 Classification of MANET Routing Protocols

MANET routing protocols are mainly categorized into three:

1. Topology based approach
2. Location based approach
3. Power/energy aware approach

1.9.2 Topology based approach

Topology based approach uses the knowledge of instantaneous connectivity of the network which emphasis on the state of the network links. In this approach the associated routing protocols are again classified into three categories, based on the time at which the routes are discovered and updated.

1. Proactive Routing Protocol (Table Driven)
2. Reactive Routing Protocol (On-Demand)
3. Hybrid Routing Protocol

**Proactive Routing Protocols**: Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating route updates at fixed time intervals.
These protocols are sometimes referred as table-driven protocols since the routing information is maintained in tables. The proactive routing approaches designed for ad hoc networks are derived from the traditional routing protocols. The primary characteristic of proactive approaches is that each node in the network maintains a route to every other node in the network at all times. Route creation and maintenance is accomplished through some combination of periodic and event-triggered routing updates. Periodic updates consist of routing information exchanges between nodes at set time intervals. The updates occur at specific intervals, regardless of the mobility and traffic characteristics of the network. Event-triggered updates, on the other hand, are transmitted whenever some event, such as a link addition or removal, occurs. The mobility rate directly impacts the frequency of event-triggered updates because link changes are more likely to occur as mobility increases. Proactive approaches have the advantage that routes are available the moment they are needed. Because each node consistently maintains an up-to-date route to every other node in the network, a source can simply check its routing table when it has data packets to be routed to some destination and begin packet transmission. However, the primary disadvantage of these protocols is that the control overhead can be significant in large networks or in networks with rapidly moving nodes. Further, the amount of routing state maintained at each node scales as $O(n)$, where $n$ is the number of nodes in the network. Proactive protocols tend to perform well in networks where there is a significant number of data sessions within the network. In these networks, the overhead of maintaining each of the paths is justified because many of these paths are utilized. Proactive routing protocol includes Destination-Sequenced Distance-Vector (DSDV) protocol, Wireless Routing Protocol (WRP) (Garcia Luna Aceves 1996), Optimized Link State Routing Protocol (OLSR) and Fisheye State Routing (FSR) (Guangyu Pei et al 2000).
In DSDV (Perkins and Bhagwat 1994) every node in the network maintains a routing table in which all the possible destinations within the network as well as the number of hops to reach each destination are recorded. Each route entry is marked with a sequence number. Nodes periodically transmit routing table updates throughout the network in order to maintain table consistency. Route updates contain the address of some node, the number of hops to reach the destination, the destination sequence number as well as a sequence number that uniquely identifies the update.

OLSR (Clauson and Jacquet 2003) is an optimization over the classical link state protocol. The key idea is to reduce duplicate broadcast packets in the same region. This is achieved with the use of multipoint relay nodes. Each node selects a minimal set of multipoint relay nodes from among its one-hop neighbors. The goal behind the MPR principle is to achieve efficient flooding. When a node wants to flood a message it sends the message only to the nodes in MPR, which in turn send the message to their MRP nodes and so on.

A node retransmits a message if it has not received the message before, and the node is selected as multipoint relay by the node from which the message is received. WRP is another loop-free proactive protocol whereby four tables are used to maintain distance, link cost, routes, and message retransmission information. General route updates are sent among neighboring nodes with distance and second-to-last hop information for each destination, resulting in faster convergence. The FSR protocol is also an optimization over Link State algorithm using the fisheye technique. In essence, FSR will propagate link state information to other nodes in the network based on how far away the nodes are. The protocol will propagate link state information more frequently with nodes that are in a closer scope as opposed to ones that are further away. This means that a route will be less
accurate the further away the node is, but once the message gets closer to the destination, the accuracy increases.

**Reactive Routing Protocol:** Reactive routing techniques, also called on-demand routing, take a very different approach to routing than proactive protocols. A large percentage of the overhead from proactive protocols stems from the need for every node to maintain a route to every other node at all times. In a wired network, where connectivity patterns change relatively infrequently and resources are abundant, maintaining full connectivity graphs is a worthwhile expense. The benefit is that when a route is needed, it is immediately available. In an ad hoc network, however, link connectivity can change frequently and control overhead is costly. Because of these reasons, reactive routing approaches take a departure from traditional Internet routing approaches by not continuously maintaining a route between all pairs of network nodes. Instead, routes are discovered when they are actually needed. When a source node needs to send data packets to some destination, it checks its route table to determine whether it has a route. If no route exists, it performs a route discovery procedure to find a path to the destination. Hence, route discovery becomes on-demand. If two nodes never need to talk to each other, then they do not need to utilize their resources maintaining a path between each other. The route discovery typically consists of the network wide flooding of a request message. To reduce overhead, the search area may be reduced by a number of optimizations.

The benefit of this approach is that signaling overhead is likely to be reduced compared to proactive approaches, particularly in networks with low to moderate traffic loads. When the number of data sessions in the network becomes high, then the overhead generated by the route discoveries approaches, and may even surpass, that of the proactive approaches. The drawback to reactive approaches is the introduction of route acquisition
latency. That is, when a route is needed by a source node, there is some finite latency while the route is discovered. In contrast, with a proactive approach, routes are typically available at the moment they are needed. Hence, there is no delay to begin the data session. Reactive type routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is maintained by some form of route maintenance procedure until either the destination becomes inaccessible along every path or until the route is no longer desired. Reactive routing protocol includes Dynamic Source Routing (DSR) protocol, ad hoc On-demand Distance Vector (AODV) protocol (Perkins and Royer 1999), Temporally Ordered Routing Algorithm (TORA) (Park and Corson 1997).

TORA (Park and Corson 1997) is source-initiated on-demand routing protocol, built on the concept of link reversal of Directed Acyclic Graph (ACG). In addition to being loop-free and bandwidth-efficient, TORA has the property of being highly adaptive and quick in route repair during link failure, while providing multiple routes for any desired source/destination pair. These features make it especially suitable for large and highly dynamic mobile ad hoc environments with dense populations of nodes. The limitation in TORA’s applicability comes from its reliance on synchronized clocks. If a node does not have a GPS positioning system or some other external time source, or if the time source fails, the algorithm cannot be used.

**Hybrid Routing Protocols:** Hybrid protocols (Donbing et al 2008) seek to combine the proactive and reactive approaches. An example of such a protocol is the Zone Routing Protocol (ZRP) (Haas 1997). ZRP divides the topology into zones and seek to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols. ZRP is totally modular, meaning that any routing protocol can be used within
and between zones. The size of the zones is defined by a parameter $r$ describing the radius in hops. Intra-zone routing is done by a proactive protocol since these protocols keep an up to date view of the zone topology, which results in no initial delay when communicating with nodes within the zone. Inter-zone routing is done by a reactive protocol. This eliminates the need for nodes to keep a proactive fresh state of the entire network.

1.9.3 Location Based Approach

Location based routing uses the geographic position of nodes to make routing decision. Location information can be obtained through GPS or some other mechanism. One of geographical-based routing protocols is Location-Aided Routing (LAR) (Young and Vaidya 1998). The central point of LAR is the limited flooding of routing request packets in a small group of nodes which belong to a request zone. To construct the request zone, the expected zone of the destination needs to be obtained first. The procedure of route discovery in LAR is: The source puts the location information of itself and the destination in the routing request packet. Then routing request packet is broadcast within the request zone. In other words, the nodes within the request zone forward the message, others discard the message. On receipt of the route request packet, the destination sends back a route reply packet which contains its current location; If LAR fails to find the route to the destination due to estimation error or other reasons, the routing protocol resorts to flooding of routing message throughout the MANET.

1.9.4 Power/Energy Aware Approach

COMPOW proposed by Narayanaswamy et al (2003) is based on a very simple idea. Each node proactively maintains multiple routing tables, one for each of the power levels available on the wireless card. Routing table $RT_i$, corresponding to the $i_{th}$ power level, is built and maintained by exchanging hello messages at power level $P_i$. Thus, the number of entries in
RT$_i$ of node u corresponds to the number of nodes reachable from u using power level P$_i$. Clearly, the number of entries in RT$_{\text{max}}$ (the routing table that corresponds to the maximum power introduction to MANET routing level) gives the total number of network nodes. The optimal power level is then defined as the minimum level i such that the number of entries in RT$_i$ equals the number of entries in RT$_{\text{max}}$. Once the optimal power level i is chosen, table RT$_i$ is set as the master routing table, which is used to route packets between nodes. The CLUSTERPOW (Vikas Kawadia and Kumar 2003) protocol displays many similarities with the simpler COMPOW protocol. As in COMPOW, every node in the network maintains separate routing tables, one for each power level. Routing table RT$_i$, referring to power level P$_i$, is maintained by exchanging hello messages at power level P$_i$. When node u has to send a message to node v, it calculates the minimum power level needed to reach node v: it is the minimum level P$_i$ such that RT$_i$ contains an entry for node v. Then, the packet is sent using this minimum power level. This process of calculating the minimum power level needed to reach the destination is repeated at each intermediate node in the route from the source to the destination (Paolo Santi 2005).

1.10 Dynamic Source Routing (DSR) Protocol

Dynamic Source Routing (DSR) was developed at Carnegie Mellon University (Johnson and Maltz 1996). It is a direct descendant of the source routing scheme used in bridged LANs. This protocol is designed to restrict the bandwidth consumption by control packets as it eliminates the periodic table-update by the control packets. As compared with other on-demand routing protocols, it is a beacon-less and therefore does not require periodic hello packet (beacon) transmission, usually used by a node to inform its presence to the neighbors. The basic approach of this protocol is briefly described as under:
The sender of a packet determines the complete sequence of nodes through which the node has to travel. The sender of the packet explicitly mentions the list of all nodes in the packet’s header, identifying each forwarding ‘hop’ by the address of the next node to which to transmit the packet on its way to destination host. In this protocol the nodes don’t need to exchange the Routing table information periodically and thus reduces the bandwidth overhead in the network. Each Mobile node participating in the protocol maintains a routing cache, which contains the list of routes that the node has learnt. Whenever the node finds a new route it adds the new route in its routing cache. Each mobile node also maintains a sequence counter ‘request id’ to uniquely identify the requests generated by a mobile host. The pair < source address, request id > uniquely identifies any request in the ad hoc network. The protocol does not need transmissions between hosts to work in bi-direction. The main phases in the protocol are – route discovery phase and route maintenance phase.

1.10.1 Route Discovery Phase

Route discovery allows any host to dynamically discover the route to any destination in the ad hoc network. In DSR, a source initiates a route discovery process when the source wants to send a packet to a destination to which it doesn’t have a valid route. The Source, if it has the valid route in its routing cache then uses it otherwise sends a route request packet by broadcasting it to the neighbors. The route request packet contains the source address, request- id and a route record in which the sequence of hops traversed by the request packet before reaching the destination are noted down. A node upon getting a Route request packet does the following:

It checks to see if it has the pair <initiators address, request id> in its list of recently seen requests if so discards the packet.
1. Otherwise, if this host’s address is already present in the route record of the request packet then it discards the packet. This eliminates the looping problem.

2. Otherwise, if the destination and the source are looking for matches with its address then it sends the route reply packet to the initiator containing the list of nodes the request packet has traversed before it reaches the destination.

3. Otherwise, it appends its own address to the route request packet and rebroadcasts it. The route request travels through the network until it reaches the destination node.

Any node forwards the route reply packet by using a route in its route cache if it has one for the source node or by using the node reverses the route in the reply packet and sends it to the source node.

Path 1:

Figure 1.4  Propagation of the Route Request (Also Known as Route Establishment)
Figure 1.5  Propagation of the Route Reply Containing the Route Entry from the Destination ‘D’. To Source ‘S’ in a DSR

1.10.2  Route Maintenance Phase

Route maintenance is a procedure of monitoring the correct route in use. The host that uses the route does this maintenance. Since the nodes do not exchange any routing information in this protocol the route maintenance procedure monitors the operation of the route and informs the source of any errors. Any host if it detects that its neighboring node, which is the next hop for a route, is not working then the node sends an error packet containing its address and the address of the hop not working. A node upon receiving the route error packet removes the hop in error from its routing cache. Acknowledgements are used to verify the correct operation of the route. The route maintenance can be provided by using either hop-to-hop or by using end-to-end acknowledgements. In case of hop-to-hop acknowledgements the hop in error is indicated in the route error packet. But in case of end-to-end acknowledgements the source node assumes that the last hop of the route to the destination is error.
1.11 MOTIVATION

With recent advances in mobile technology and mobile devices, mobile computing has become an important part of our life. People are using wireless networks for their day-to-day work, to make a phone call or to download news or to see and listen or only listen to their favorite song from various multimedia servers with the help of various devices such as mobile phones, PDAs or a laptop. More services may be offered in the near future (Agrawal and Zeng 2005). The desire to get connected anytime, anywhere, anyhow has led to the development of wireless networks, opening new vista of research in pervasive and ubiquitous computing (Anderson et al 2000). This emerging field of mobile and nomadic computing (Chlamtac and Redi 1998) requires a high secure routing protocol for effectively managing the communication among the peers.

Wireless networks (Murthy and Manoj 2005), in general, refer to the use of infrared or radio frequency signals to share information and resources between devices. Due to basic difference in the physical layer
ISO/OSI model (Tenenbaum 2003), the wireless devices and networks show distinct characteristics from their wireline counterparts, such as (Stefano et al 2004):

1. Higher interference results in lower reliability.
2. Low bandwidth and much slower data transfer rate.
3. Highly variable network conditions.
4. Limited computing and energy resources.
5. Device size limitation
6. Weaker security.

In spite of the above limitations the wireless networks are immensely popular because of its benefits. Some of the benefits are listed as below:

- **Access to more than one technology** - Users can use more than one access technology to service various parts of their network and during the migration phase of their networks, when upgrading occurs on a scheduled basis. It enables a fully comprehensive access technology portfolio to work with existing technologies.

- **Minimal cost** - The inherent nature of wireless is that it doesn’t require wires or lines to accommodate the data/voice/video pipeline. Although paying fees for access to elevated areas such as masts, towers, and building tops is not unusual but the associated logistics, and contractual agreements are often minimal as compared to the costs of trenching a cable.
- **Reduced time to revenue** - Companies can generate revenue in less time through the deployment of wireless solutions than with comparable access technologies because a wireless system can be assembled and brought online in a very short span of time.

- **Provides broadband access extension** - Wireless commonly competes and complements existing broadband access. Wireless technologies play a key role in extending the reach of cable, fiber, and Digital Subscriber Link (DSL) markets, and it does so quickly and reliably.

Based upon the criterion of network formation and architecture, the wireless networks can be subdivided into two classes, infrastructured and infrastructure less networks (Chlamtac et al 2003). These are defined as follows:

- Infrastructured networks have fixed and wired gateways. They have fixed base stations connected to other base stations through wires. The transmission range of a base constitutes a cell. A “hand-off” occurs as mobile host travels out of range of one station and into the range of another and thus, the mobile host is able to continue communication seamlessly throughout the network, represented in Figure 1.7. The cellular networks fall under this category.

- Infrastructureless networks, do not have fixed routers and all nodes are capable of moving and can be connected dynamically in an arbitrary manner. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other, represented in Figure 1.8. Mobile ad hoc Networks (MANETs) falls under this category.
The basic principle behind ad hoc networking is the multi-hop relaying (Murthy and Manoj 2005), which traces its root back to 500 B.C. Darius I (522-486 B.C.), the king of Persia, devised an innovative communication system that was used to send messages and news from his capital to the remote provinces of his empire by means of a line of shouting men positioned on the tall structures. The system was faster than normal method of sending the message/news through a messenger. The use of ad hoc voice communication was used in many tribal societies with a string of repeaters of drums, trumpets or horns. In recent times, it was the Department of Defense (DoD), in 1972, initiated a new program on Packet Radio Networks (PRNET) (Ephremides et al 1987) with the intention to create technologies for the battlefield that did not employ the previously deployed infrastructure but are highly survivable. Table 1.1 summarizes the major milestones in the development of MANET (Bdale Garbee 1987) (Frank 1998) (Ivanhowitt et al 2006)
Table 1.1 Mobile ad hoc Network Applications

<table>
<thead>
<tr>
<th>Applications</th>
<th>Descriptions/Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor networks</td>
<td>Collection of embedded sensor devices which are used to collect real-time data to automate everyday functions. E.g., remote sensors for weather, earth activities and sensors for manufacturing equipment. They can have 1000–100,000 nodes, each node collects sample data, and forwards it to centralized host for further processing.</td>
</tr>
<tr>
<td>Emergency Services</td>
<td>Search-and-rescue operations as well as disaster recovery, e.g., early retrieval and transmission of patient data (record, status, diagnosis) from/to the hospital, replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire, etc.</td>
</tr>
<tr>
<td>Tactical Networks</td>
<td>Military communication and operations, Automated Battlefields.</td>
</tr>
<tr>
<td>Educational</td>
<td>To set up virtual classrooms or conference rooms and to set up ad hoc communication during conferences, meetings, or lectures.</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Multiuse games, Robotic pets, Outdoor Internet access.</td>
</tr>
<tr>
<td>Location-aware Services</td>
<td>Follow-on services: automatic call forwarding, transmission of the actual workspace to the current location. Information services: Push, e.g., advertise location-specific service, like- gas stations, Pull, e.g., location-dependent travel guide, Services (printer, fax, phone) availability information etc.</td>
</tr>
<tr>
<td>Home and Enterprise</td>
<td>Home/office wireless networking (WLAN), e.g., shared whiteboard networking application. Use of PDA to print from anywhere, trade shows like Personal Area Network (PAN) and Body Area Network (BAN).</td>
</tr>
</tbody>
</table>

The benefits of ad hoc networks appeal to applications like conferences, meetings, disaster relief, rescue missions, and battlefield operation (Toh 2002). Such scenarios typically lack a central administration or wired infrastructure (Toh 1996). Some of the application areas (Tapaswi and Ramesh Joshi 2004) are listed in Table 1.1.
Apart from the above applications the MANETs are found to be useful for realizing the tetherless computing and opportunistic mobile computing (Stefano et al 2004).

A MANET can also be defined as a distributed infrastructureless network (Corson and Maker 1999) and mainly relies on individual security solutions from each mobile node and therefore centralized security control is hard to implement (Buchegger and Boudec 2002). Securing a MANET is a severe problem because of the conjunction of several factors:

- **Vulnerabilities**: the lack of physical security and the ease of eavesdropping and spoofing leaves much desired gap between the security in wireless communication and the security in standard wireline communication.

- **Lack of a priori trust**: A MANET consists of set of nodes, which are not part of any organization, therefore the classical security paradigm based on preestablished trust among the parties are not applicable.

- **Lack of infrastructure**: security solutions comprising of dedicated secure components with predefined roles (such as trusted third party and key servers) cannot be used in this environment.

- **Requirement for cooperation**: due to lack of dedicated components, such as - routers and servers, the basic network functions and services need to be carried out by a set of ordinary nodes in a distributed fashion. Thus, the routing is affected by the presence of malicious node or the absence of cooperation among the nodes.
1.12 PROBLEM STATEMENT

The high dynamic nature of MANETs results in frequent and unpredictable changes in the network topology, which adds to the difficulty and complexity for routing among the mobile nodes within the network. Thus, establishing communication among mobile nodes is a great challenge in itself. The applications associated with the field of MANETs, make them an important part of the next generation wireless networks.

In this research work, focus has been put on the strategy to address the security issues because MANETs are generally more vulnerable to information and security threats than fixed-wired networks. The use of open and shared broadcast channels means the nodes with inadequate physical protection are prone to security threats.

Further, emphasis has been given on the routing mechanism and the security area which has not been addressed adequately in existing research. Thus, the issue of designing and developing an efficient and secure routing protocol is still wide open.

The main objective of the present work can be stated as – “to design and develop a secured dynamic source routing protocol for MANETs”. In order to handle the above problem, the following outline is proposed:

1. Evaluation and analysis of existing dynamic source routing protocol under the threat of different types of attacks such as packet dropping attack, selective packet dropping attack, blackhole attacks, cooperative blackhole attacks and greyhole attack are observed through the relevant simulation. The assessment and study of different metrics helps in better understanding of the basic characteristics and functioning of
the standard dynamic source routing protocol under the above said scenario. The results yield the fact that as the number of malicious nodes increases the performance of the protocol gets degraded.

2. Design and development of the proposed routing protocol - based upon the association between the neighboring nodes as pavement for improving an existing dynamic source routing protocol. The new protocol is proposed after proper verification and validation through simulations. The proposed protocol is validated against different RFCs proposed by IETF and the verification is done by taking various performance metrics such as – packet delivery ratio, throughput, average latency, route overhead, byte overhead and total number of drops during the simulation period.

1.13 ORGANISATION OF THESIS

Based on the objectives stated above, the work carried out is presented in the thesis as given below:

In Chapter 1, a brief introduction to wireless networks and history of Mobile ad hoc Networks and its different types are discussed. The characteristics, Security features of the MANET are also presented in the same section.

A brief introduction to ad hoc routing protocols namely proactive, reactive and hybrid Protocols and detailed description about DSR protocol are given in Chapter 1. Then network security requirements, issues and challenges in security provisioning for ad hoc networks are also presented.
Chapter 2 describes a review of relevant literature carried out for use of trust in MANET routing protocols. Then a survey on various characteristics, levels, attributes and classification of trust are discussed. Later the issues in incorporating trust in to MANETS are elaborated in detail.

A brief introduction to proposed association based dynamic source routing protocol. Then different association estimator technique used for identifying the different attacks and the proposed routing mechanism are discussed. Details regarding the simulation setup are also provided in chapter 3.

Chapter 4 discusses the packet dropping attack in detail and proposes the procedures to prevent Packet dropping attacks and the simulation results have also been presented.

In chapter 5 the impact of selective packet dropping attack is studied and methods to mitigate the above attack are also discussed along with appropriate results.

A new secure routing protocol for MANET for preventing blackhole attack is proposed and the simulation results have also been presented in Chapter 6.

Proposed methodologies to encounter cooperative blackhole attack in MANET are discussed in the chapter 7 along with their relevant results.

A new procedure for prevention of greyhole attack is proposed and the simulation analysis is presented in Chapter 8.

Chapter 9 summarizes the work done and present the major contributions made in this thesis. It also suggests the scope for further work that could be carried out in continuation of this research.