CHAPTER 1

INTRODUCTION

Communication is sharing of information by means of signals, speech, visuals or information. In order to share any information, minimum two entities are needed. Among that, one may be transmitter and another one may be receiver. It is fulfilled only if the receiver receives the information sent by the transmitter. It can be established across various distances in time and space. It has been broadly categorized into two major areas of wired and wireless communications. In communication networks, a node is a connection point, a redistribution point or a communication endpoint. The definition of a node depends on the network. The communication could be established between a set of nodes also.

Nowadays, usage of computers is tremendous. In all areas, for all applications we are in need of computers. Due to efficient communication between computers, technical revolution resulted and thus internet comes into use. Individual computers are capable of gathering, processing, storing and distributing information, under the direction of humans.

There are three main areas where benefits can be expected if one computer is able to communicate with others:

(i) It can get information that is stored in other computers;

(ii) It can get other computers to do specialized work for it and

(iii) It can facilitate user interaction.
There are two main problems associated with communication:

(i) Co-ordination between computers based on the nature of communications and

(ii) Establishing the required communications using available physical communication media.

The processes of coordination and establishment of physical media, require a lot of human being managerial skill, which make communications being possible.

Wireless networks have allowed organizations to become more mobile. A wireless network consists of nodes that communicate by exchanging packets via radio waves. These packets can take one of two forms. A unicast packet contains information that is addressed to a specific node, while a multicast packet distributes the information to a group of nodes. The MAC protocol simply determines when a node is allowed to transmit its packets, and typically controls all access to the physical layer. The specific functions associated with a MAC protocol vary according to the system requirements and application.

The architecture determines how the structure of the network is realized, and where the network intelligence resides. Centralized network architecture features a specialized node, i.e., the base station that coordinates and controls all transmissions within its coverage area, or cell. Cell boundaries are defined by the ability of nodes to receive transmissions, from the base station. To increase network coverage, several base stations are interconnected, by land lines, which eventually tie into an existing network, such as the public switched telephone network (PSTN) or a local area network (LAN). Thus each base station also plays the role of an intermediary between the wired and wireless domains.
Communication from a base station to node takes place on a downlink channel, while the opposite occurs on an uplink channel. Only the base station has access to a downlink channel, while the nodes share the uplink channels. In most cases, at least one of these uplink channels is specifically assigned to collect control information from the nodes. The base station grants access to the uplink channels in response to service requests received on the control channel. Thus the nodes simply follow the instruction of the base station. The concentration of intelligence at the base station leads to a greatly simplified node design that is both compact and energy efficient. The centralized control also yields high performance of the network such as sufficient allocation of bandwidth, minimum delay and high throughput. In a simplified manner, we can state that QoS improves for the network and results with bandwidth management since the base station can collect the requirements and prioritize channel access accordingly. Moreover, multicast packet transmission is greatly simplified since each node maintains a single link to the base station. On the other hand, the deployment of a centralized wireless network is a difficult and slow process. The installation of new base stations requires precise placement and system configuration along with the added cost installing new landlines to tie them into the existing system. The centralized system also presents a single point of failure, i.e., no base station equals no service. These disadvantages are overcome by adhoc wireless network.

The primary ad hoc network architecture is the absence of any predefined structure. Service coverage and network connectivity is defined solely by node proximity and the prevailing RF propagation characteristics. Ad hoc nodes directly communicate with one another in a peer-to-peer fashion. To facilitate communication between distant nodes, each ad hoc node also acts as a router, storing and forwarding packets on behalf of other nodes. The result is a generalized wireless network that can be rapidly deployed and
dynamically reconfigured to provide on-demand networking solutions. An ad hoc architecture is also more robust in that the failure of one node is less likely to disrupt network services.

Organizations are now using a combination of both wired and wireless networks. To setup a network, central administrator must ensure that the nodes in the network must have a Network Interface Card, commonly referred to as a NIC. NIC gives its identification in that network. A NIC is a device that locates a computer or other device in a network. For computers, the NIC is usually installed in an expansion slot and has a chip that handles the physical and data-link layers of network communications.

Wireless networking takes into consideration about range, mobility and several types of hardware components like cable modem, router, hub and switch. These hardware components are needed to establish a wireless network. The difference between a hub and a switch is that a switch filters the data that passes through it and a hub does not. Information can be transmitted by modulation techniques also.

Wireless networks have become increasingly popular in the past few decades. The network can be deployed by using RF signal to communicate among computers and other network devices as shown in the Figure 1.1. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networks.

An ad-hoc or peer-to-peer wireless network consists of a number of nodes, each equipped with a wireless networking interface card. Each node can communicate directly with all of the other wireless enabled nodes. They can share files, but may not be able to access wired LAN resources, unless
one of the computers acts as a bridge to the wired LAN using special software such as Oregon Library Resource Sharing Program.

![Diagram of wireless network](image1.png)

**Figure 1.1 Model for wireless network**

An infrastructure wireless network consists of an access point or a base station. In this type of network, the access point acts like a hub. Hub provides connectivity for the wireless nodes. It can connect or bridge the wireless LAN to a wired LAN. It allows wireless node access to LAN resources, such as file servers or existing Internet Connectivity is shown as in Figure 1.2.

![Diagram of wired and wireless network combinations](image2.png)

**Figure 1.2 Combinations of wired and wireless networks**
There are four basic types of transmission standards for wireless networking. These are proposed by the Institute of Electrical and Electronic Engineers (IEEE). These standards define all aspects of radio frequency wireless networking. They have established four transmission standards; 802.11, 802.11a, 802.11b, 802.11g.

802.11a and 802.11b standards specify lowest range of 1 or 2 Mbps. They specify use of 57.8 and 65 Mbps respectively for high speed communication. Both specify operating frequency of 2.4 GHz. 802.11a operates at 5 GHz frequency and can transmit up to 54 Mbps. 802.11g operates at 2.4 GHz frequency and can transmit at up to 54 Mbps. Actual transmission speeds vary, depending on factors like allotted bandwidth, Number of MIMO channels used, OFDM techniques within the network and any interference in the radio transmissions.

Wireless networks are reliable. During the signal transmission, if the signal is disturbed, it will reduce the radio coverage range and the quality of the signal. Interference is also one kind of disturbance, which caused by other devices, while operating on the same radio frequency. It is very hard to control the addition of new devices on the same frequency. we have used Log Distance Path Loss model which is given by $p_r(d) = K/d^2$, in which the value of K varies with environments. The important factor is received power decays as the square power of distance. The effect of extraneous radio signal on that node will predominate. So, in our AEERG protocol interference can be reduced by considering small radio coverage range.

Interference is the important reason for reducing the wireless range in our experiments. Results are not affected due to dense deployed network for our experiments. Range of 250m radio coverage is taken in all our experiments to avoid interference.
Many wireless networks can increase the range of the signal by using many different types of hardware devices. A wireless extender can be used to relay the radio frequency from one point to another without losing signal strength. Even though this device extends the range of a wireless signal it has some drawbacks. One drawback is that it extends the signal, but the transmission speed is lowered.

There are many benefits with a wireless network. The most important one is the option to expand current wired network to other areas of organization where it would otherwise not be cost effective or practical to do so. An organization can also install a wireless network without physically disrupting the current workplace or wired network. Wireless networks are far easier to move than a wired network and adding users to an existing wireless network is easy. Organizations opt for a wireless network in conference rooms, lobbies and offices where adding to the existing wired network may be too expensive to do so. The important fact in these networks is that it eliminates installation of expensive cables and associated maintenance costs. This kind of network is referred as Wireless Local Area Network (WLAN). Use of MANETs and their applications are essential at the places where necessary infrastructure is not available. This network usage is getting increased nowadays due to low cost and easy implementation procedure. Wireless ad hoc networks and wireless sensor networks are the two broad categories of wireless networks. Both fields have now become the most vibrant and active fields of communication and networking research.

Wireless ad hoc network allows all wireless devices, within radio range of each other, to communicate without the use of any central access point and administration. These devices can have their communication within the radio coverage area. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental
conditions such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Wireless sensor network has been deployed by means of a large number of small radio coverage nodes. The nodes sense various parameters and report them to their neighbor sensor nodes. Placing sensor nodes is very easy in hostile environments or over large geographical areas since they are not having mobility. The issues of increasing the life time of sensors and replacement of sensors are the important focus in research area of WSN.

1.1 MOBILE AD HOC NETWORKS (MANET)

Mobile Ad-hoc networks (Jochen Schiller 2003) are self-organizing and self-configuring multihop wireless networks. The topology of a MANET changes dynamically due to mobility of the nodes. Nodes in these networks utilize random access technique to access wireless channel. Random access is a widely used technique for coordinating the access of large numbers of intermittent transmitters in a single shared communication channel. Each transmitter (node) sharing the channel transmits data packets at random times. In most random channels the transmitters rely on some protocol (such as repetition) to handle the case of packets lost due to interference by other packets. A random channel may also just provide a best effort delivery mechanism and leave it to the receiver to deal with lost packets. The basic concept is whenever a node wants to communicate, immediately, it will access the channel. If the channel is free, node will communicate through them. Otherwise, if the channel is busy, node has to wait for a random amount of waiting time for free channel. Thus, the nodes are cooperating in a friendly manner to engage themselves in a multihop forwarding of communication. The nodes in the network not only act as hosts but also as routers that route data to/from various nodes in network. Mobile Ad hoc networks consist of collection of wireless nodes that can exchange information dynamically among themselves without pre-existing fixed infrastructure. From a source
node, a packet may have to be forwarded by a sequence of nodes to reach its destination. Finding the shortest path to reach the destination is called as routing. Protocols are developed for routing in MANETs. But, because of highly dynamic nature of the nodes, performance of routing protocols is an important issue.

In addition to this, routing protocols face many challenges like limited battery backup, limited processing capability and limited memory resources of the nodes (as stated by Chen et al (2002)). Other than efficient routing, efficient utilization of battery power and security are also the major concern for routing protocols. In mobile ad-hoc networks as proposed by Mads Darø Kristensen & Niels (2008), since there is no infrastructure support, a routing procedure is always needed. Routing is used to find a path so as to forward the packets appropriately between the source and the destination. Similar procedure is needed even when a destination node might be out of range of a source node. Within a cell, a base station can reach all mobile nodes through broadcast mode in common wireless networks. In broadcast mode, there is no need for routing. In case of ad-hoc networks routing, each node must be able to forward data for other nodes. This creates routing overhead and some additional problems along with the problems of dynamic topology change stated by Aminu Mohammed et al (2009) - which results in unpredictable changes in connectivity and more energy consumption due to data forwarding in the network.

1.2 CHARACTERISTICS OF MOBILE AD-HOC NETWORKS

1. Dynamic topologies

Nodes are free to move arbitrarily. Thus the network topology may change randomly and may primarily consist of bidirectional wireless links. In some cases, where the transmission power of two mobile nodes is very much
different, even though bidirectional links exist, a unidirectional link may be used (Brent Peacock 2007).

2. **Bandwidth-constrained and variable capacity links**

   Wireless links continue to have significantly lower channel capacity than infrastructure networks. The realized throughput of wireless communications is computed after accounting for the effects of multiple access, fading, noise, interference conditions etc. The Log Distance Path Loss Model is used in all our experiments. One effect of relatively low to moderate link capacities is that congestion is typically the norm, rather than the exception. In this work, inter node interference (INI) - simultaneous transmission by nodes has been considered as interference. This work has been experimented with a MAC protocol independent model for INI in inter-working multi-hop wireless networks.

3. **Energy-constrained operation**

   Some or all of the nodes in an ad hoc network rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design optimization criteria may be energy conservation Maleki et al (2002).

4. **Limited physical security**

   Mobile wireless networks are generally more prone to security threats than wired networks Loay Abusalah et al (2009). The increased possibility of eavesdropping, spoofing and denial-of-service-type attacks should be carefully considered.
To reduce security threats Yang et al (2004) analyzed many existing link security techniques with their proposed technique. These techniques are applied within wireless networks to improve their security levels. As a side benefit, the decentralized nature of ad hoc network control provides an additional robustness against the single point of failure of more centralized approaches. In addition, scalability also is the serious limitation of ad hoc networks.

1.3 ROUTING

Routing in a MANET finds the shortest path between two nodes so as to enable communication in a fast, reliable and secure manner. Routing depends on many factors, including modeling of the topology, selection of routers and initiation of request.

MANETs, by nature, are highly dynamic networks with scarce channels. The low resource availability in these networks necessitates efficient utilization; hence the motivation for optimal routing in MANETs. Also the highly dynamic nature of these networks places many restrictions on any routing protocol. For an example, a routing protocol which is designed for a network which consists of large number of nodes is not suitable for another network comprising smaller number of nodes. There are three major goals (as stated by Royer et al (1999)) when selecting a routing protocol:

(1) Provide the maximum possible reliability by selecting alternative routes if node connectivity fails due to the mobility of the nodes.

(2) Route network traffic through paths of least cost in the network (paths with minimum number of intermediate nodes).
(3) Configure all nodes in a network to perform routing mechanism. This will end up with some routes having best possible response time and throughput. This is especially important for interactive sessions between user applications.

In ad hoc network, each node is expected to serve as a router and each router is indistinguishable from another in the sense that all routers execute same routing algorithm to compute routing paths through the entire network. As the number of nodes becomes larger, the overhead in computing, storing, and communicating the router table information could become prohibitive Lijuan Cao (2007).

1.3.1 Need for Routing

Routing is the process in which a route from a source to a destination node is identified and is achieved either by computing all routes before and pre-storing them or computing them when needed. Ad hoc network routing typically has the following requirements:

(1) Route computation must be distributed, because centralized routing in a dynamic network is impossible, even for fairly small networks.

(2) Database is created in every node about its neighbors and number of hops needed to reach that neighbors and the shortest path to reach that neighbor node. Based on that, if routing has been performed, it leads to enormous state transmission overhead when the network topology changes.

(3) Positively few numbers of nodes must be involved in route computation and packet transmission. Those nodes are involved in monitoring and updating the network status to
other nodes in the network. Minimum processing overhead is the goal to achieve so as to enable every host must have quick access to the routes on demand.

(4) Larger number of nodes must care only about the packet route which leads to reach their destination. It must not be involved in frequent topology updates of isolated network that have no traffic.

(5) Stale routes must be detected. Detection is possible by sensing either large response time or more cost. Once it has been found, it should be eliminated quickly.

(6) Broadcasts must be avoided as far as possible because broadcasts are not reliable in ad hoc networks.

(7) If the node stabilizes, then routes must converge to the optimal routes.

(8) It is desirable to have a backup route when the primary route has become broken and is to be re-computed.

In ad hoc networks, one of the major challenges in designing a routing protocol is that a node needs to know at least the information how to reach the destination through its neighbors for determining a packet route Zayene & Tabbane (2009). On the other hand, in an ad hoc network, the network topology can change very frequently. Furthermore, as the number of network nodes becomes large, the potential number of destinations also becomes large, requiring large and frequent exchange of data among the network nodes. Thus the amount of update traffic can be high.
1.4 CLASSIFICATION OF ROUTING PROTOCOLS IN MANET’s

Many routing protocols have been proposed to solve the dynamic routing problem in ad hoc networks. In general, there are three classes of routing protocols for ad hoc networks, proactive routing, reactive routing and hybrid routing. Classification of routing protocols in MANET’s can be done in many ways, but most of these are done depending on routing strategy and network structure as shown as in Figure 1.3. According to the routing strategy the routing protocols can be categorized as Table-driven and source initiated protocols. Table-driven routing protocols are also called as proactive routing protocols Xie et al (2007). On-demand source initiated routing protocols are also called as reactive routing protocols Yuval Shavitt & Amir Shay (2005). Hybrid routing protocol is the combination of both proactive and reactive protocol features. Royer et al (2001) have given many protocols existed under these categories; among them, few protocols are considered here.

![Figure 1.3 Classification of routing protocols in MANETs](image-url)
Ad hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are reactive protocols and AODV is taken for experimentation. Destination Sequenced Distance Vector (DSDV) and Wireless Routing Protocol (WRP) are proactive protocols. Zone Routing Protocols is a Hybrid Routing protocol.

1.4.1 Table-Driven Routing Protocols

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information. They respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. The proactive protocols are not suitable for large networks, as they need to maintain node entries for each and every node of the network, in the routing table of every node. This cause more overhead in the routing table leading to consumption of more bandwidth is studied by performance evaluation given by Awan & Al-Begain (2006). Some of the protocols are described as follows.

1.4.1.1 Destination-Sequenced Distance-Vector Routing

The Destination-Sequenced Distance-Vector Routing protocol (DSDV) is a table-driven algorithm (proactive) based on the classical Bellman-Ford routing mechanism. The improvements made to the Bellman-Ford algorithm avoid ‘from’ loops in routing tables. Every mobile node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded.
Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain table consistency. To help alleviate the potentially large amount of network traffic, route updates can be generated. Route updates can employ two possible types of packets. The first is known as a full dump. This type of packet carries all available routing information and could require multiple Network Protocol Data Units (NPDUs).

During periods of slow movement, these packets are transmitted infrequently. Smaller incremental packets are used to relay only changes in previous information, since the last full dump. Each of these broadcasts should fit into a standard-size NPDU, thereby decreasing the amount of traffic generated. The mobile nodes maintain an additional table where they can store the data sent by the incremental routing information packets. New route broadcasts contain the following fields: address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination and a new sequence number unique to the broadcast. The route labeled with the most recent sequence number, is always used. In the event that two updates have the same sequence number, the route with the smaller metric is used in order to optimize (shorten) the path. Mobiles also keep track of the settling time of routes (Mikki 2009), or the weighted average time that routes to a destination will fluctuate before the route with the best metric is received. By delaying the broadcast of a routing update by the length of the settling time, mobiles can reduce network traffic and optimize routes by eliminating those broadcasts that would occur if a better route was discovered in the very near future (Gupta 2010).
1.4.1.2 The Wireless Routing Protocol

Murthy et al (1996) have stated that the Wireless Routing Protocol (WRP) is a table-based protocol with the goal of maintaining routing information among all nodes in the network. Each node in the network is responsible for maintaining four tables:

- Distance table
- Routing table
- Link-cost table
- Message retransmission list (MRL) table

Each entry of the MRL contains the sequence number of the update message, a retransmission counter, an acknowledgment flag vector with one entry per neighbor, and a list of updates sent in the update message. The MRL records which updates in an update message need to be retransmitted and which neighbors should acknowledge the retransmission. Mobiles inform each other of link changes through the use of update messages. An update message is sent only between neighboring nodes and contains a list of updates (the destination, the distance to the destination, and the predecessor of the destination), as well as a list of responses indicating which mobiles should acknowledge (ACK) the update.

Mobiles send update messages after processing updates from neighbors or detecting a change in a link to a neighbor. In the event of the loss of a link between two nodes, the nodes send update messages to their neighbors. The neighbors then modify their distance table entries and check for new possible paths through other nodes. Jayakumar & Gopinath (2008) have proposed a method in which information about any new paths are relayed back to the original nodes so that they can update their tables.
accordingly. Nodes learn of the existence of their neighbors from the receipt of acknowledgments and other messages. If a node is not sending messages, it must send a *hello* message within a specified time period to ensure connectivity. Otherwise, the lack of messages from the node indicates the failure of that link; this may cause a false alarm.

When a mobile node receives a *hello* message from a new node, that new node is added to the mobile nodes’ routing table. Then, the mobile node sends the new node a copy of its routing table information. Part of WRP discussed about a new way to avoid the loop. This WRP, routing nodes communicate the distance and second-to-last hop information for each destination in the wireless networks. WRP belongs to the class of path-finding algorithms. It avoids the self loop problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. This ultimately (although not instantaneously) eliminates looping situations and provides faster route convergence when a link failure event occurs.

1.4.2 **Source-Initiated On-Demand Routing**

A different approach from table-driven routing is source-initiated on-demand (reactive) routing Corson & Macker (1999). This type of 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 when all possible route permutations have been examined. Once a route has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired. The route discovery usually occurs by flooding the network with route request packets.
1.4.2.1 Ad Hoc On-Demand Distance Vector Routing

Royer et al (2000) used the Ad Hoc On-Demand Distance Vector (AODV) routing protocol. It builds on the DSDV algorithm as explained previously. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes, as in the DSDV algorithm. AODV is classified as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a “fresh enough” route to the destination is located. Figure 1.4a illustrates the propagation of the broadcast RREQs across the network. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information Safa (2007).

Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node’s IP address, uniquely identifies an RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ. It is shown in Figure 1.4b.
During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh route requirement, the destination or an intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor. That neighbor node is the one from which it first received the RREQ (Figure 1.4). As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. RREP is forwarded along the path which is established by the RREQ. AODV only supports the use of symmetric links. Routes are maintained as follows: If a source node moves away (isolated from radio frequency propagation), it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its
upstream neighbor notices the move by absence of radio frequency signals and propagates a link failure notification message (an RREP with infinite metric (cost or distance) to each of its active upstream neighbors to inform them of the erasure of that part of the route. These nodes in turn propagate the link failure notification to their upstream neighbors, and so on until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired.

An additional aspect of the protocol is the use of hello messages, which are periodic local broadcasts by a node to inform each mobile node of other nodes in its neighborhood. Hello messages can be used to maintain the local connectivity of a node. However, the use of hello messages is not required if the path has been established by means of RREQ and RREP messages. Nodes listen for retransmission of data packets to ensure that the next hop is still within reach. If such a retransmission is not heard, the node may use any one of a number of techniques, including the reception of hello messages, to determine whether the next hop is within communication range. The hello messages may list the other nodes from which a mobile has heard, thereby yielding greater knowledge of network connectivity.

1.4.2.2 Dynamic Source Routing

The Dynamic Source Routing (DSR) protocol is also an on-demand routing protocol. It is based on the concept of source routing as used in Bai & Singhal (2006). Mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware. Entries in the route cache are continually updated as new routes are learned.

The protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache to determine whether it has a
predetermined route to the destination. If it has an unexpired route to the destination, it will use that route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This route request contains the address of the destination, along with the source node’s address and a unique identification number.

Each node receiving the packet checks whether it knows of a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links. To limit the number of route requests propagated on the outgoing links of a node, a node forwards the route request only once. If the node’s address does not already appear in the route record, it includes its address and forward the packet.

A route reply is generated when the route request reaches either the destination itself, or an intermediate node which contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken.

If the node generating the ‘route reply’ in the destination, it places the route record contained in the route request into the route reply. If the responding node is an intermediate node, it will append its cached route to the route record and then generate the route reply. To return the route reply, the responding node must have a route to the initiator. If it has a route to the initiator in its route cache, it may use that route. Otherwise, if symmetric links are supported, the node may reverse the route in the route record. If symmetric links are not supported, the node may initiate its own route discovery and piggyback the route reply on the new route request.
Route maintenance is accomplished through the use of route error packets and acknowledgments. *Route error* packets are generated at a node when the data link layer encounters a fatal transmission problem. When a route error packet is received, the hop in error is removed from the node’s route cache and all routes containing the hop are truncated at that point. In addition to route error messages, acknowledgments are used to verify the correct operation of the route links. Such acknowledgments include passive acknowledgments, where a node is able to observe the next hop forwarding the packet along the route.

### 1.4.3 Hybrid Routing Protocol

Hybrid routing protocols combine the table-driven and source-initiated on-demand approaches in one. So, Hybrid protocol reduces the drawback of each protocol. A proper proactive multicast routing approach and a proper reactive multicast routing approach are deployed at different hierarchical levels. Moreover, these protocols maintain the topology inside a zone with a certain radius (Intra-Zone) using the Table-driven approach, and outside this zone (Inter-Zone) using the Source-Initiated On-Demand approach.

#### 1.4.3.1 Zone Routing Protocol

Haas et al (2002) have proposed the Zone Routing Protocol (ZRP) as an example of hybrid routing protocol. In ZRP, a node proactively maintains routes to destinations within a local neighborhood, which is referred to as a routing zone. A node routing zone is defined as a collection of nodes whose minimum distance in hops from the node in question is no greater than a parameter referred to as zone radius. Neighbor discovery is implemented through a MAC level Neighbor Discovery Protocol (NDP). The ZRP maintains routing zones through a proactive component called the Intra zone Routing Protocol (IARP). The Inter-zone Routing Protocol (IERP) is used for acquiring routes that are beyond the routing zone. The main
drawback of this approach is that a node outside the zone may wait a considerable time to join a multicast group.

The zone routing protocol (ZRP) and zone-based hierarchical link state (ZHLS) routing protocol provide a compromise on the total number of nodes and the frequency of topology change. Furthermore, these protocols can provide a better trade-off between communication overhead and delay, but this trade-off is subject to the size of a zone and the dynamics of a zone. Thus, the hybrid approach is an appropriate candidate for routing in a large network.

1.5 APPLICATIONS OF MANETs

In military communications use of MANETs is highly beneficial and also confidential. Also, in battlefield, the message is communicated in a fast manner to carry out the necessary actions throughout the coverage area. In emergency situations where hurricane, Storm and flood will affect the existing infrastructure, these networks will come into rescue. In business environments, in order to instant access to the company’s database for an emergency meeting, these networks configure the secure and authenticated link.

Information regarding individual node behavior can be used for identifying selfish behavior in the network. Also, an approximation of arriving and departing traffic load at each node is important in the context of quality of service, load balancing, and congestion control. Furthermore, the network topology picture can provide valuable information to network management in detecting preferred routes and bottlenecks, discovering network partitioning, and in detecting faults. Das et al (2000) compared the robustness with respect to mobility, rapid changes in the network topology and node connectivity. Wireless network traffic is highly diverse and each traffic type has unique requirements in terms of bandwidth, delay, packet loss and availability Wang et al (2000). With the exponential growth of Internet during the last few years, IP networks now support not only typical services
like ftp and email, but also real-time services and video streaming application. Zhu & Corson (2002) have stated that the traffic characteristics of these applications require a certain Quality of Service (QoS) from the network in terms of bandwidth and delay requirements. The biggest problems in a network are related to the allocation of network resources: as buffers and link bandwidth among different users. A limited amount of resources has to be shared among many different competing traffic flows in an efficient way in order to maximize the performance and the use of the network resources. If resources are available, packets are handled according to their classification. Traffic shaping functions are used to reduce the congestion by controlling the volume of traffic entering in the networks and the rate at which packets are sent. For achieving these queuing techniques are used, where queues are managed in a way to ensure each queue gets the level of services required for its class.

A number of queue disciplines are available as listed in Chen et al (1999). Some of these are: First-In-First-Out (FIFO), Priority Queuing (PQ), Fair Queuing (FQ), Weighted Fair Queuing (WFQ) and Class Based Queuing (CBQ). A comparison between queuing disciplines has been carried out in our research. Advantages and disadvantages of different queuing discipline with area of applicability are also listed. Much research has been done on “weighted fair queuing” algorithms for achieving the desired bandwidth allocation on a wired link. We proposed modified weighted fair queuing (m-WFQ). With m-WFQ, the bandwidth received by a flow in a shared link is in proportion to the flow’s weight on order to avoid the overload problem. Since Wireless LANs have been considered as just another type of technology used in the communications, it is desirable that the architecture for bandwidth allocation follows the same principles in the wireless network as in the wired Internet, assuring compatibility among the wireless and the wired parts. The challenge in Wireless LAN is that we do not have all packets in a centralized queue, like in wired links, but we have them distributed in the wireless hosts. Therefore, we need to design a new MAC mechanism for Wireless LAN
capable of providing the desired scheduling. When network congestion is experienced, packets in excess must be discarded. Packet discard cannot be avoided but can be controlled. Techniques for handling packet discard are performed such as Tail Drop and Random Early Detection.

The original contributions in this research work are

Energy efficient routing protocol using sleep-awake schedule is developed for MANETs. By adaptive algorithm, sleep-awake schedule is varied to achieve maximum throughput and minimum energy consumption. Constant Bit Rate traffic is used in military and other strategic communications.

(ii) Development of Mathematical model for AEERG Routing protocol
A mathematical model is developed for energy estimation in sleep – awake scheduled nodes in MANETs. For the same network, throughput calculations have been done. Finally, mathematical model results are compared with simulation results. The comparison shows that simulation results are very close to theoretical results.

(iii) Quality of Service (QoS) analysis in AEERG Routing protocol
First-in-First-Out, Random Early Detection, Priority queue and Weighted Fair Queueing is used in AEERG protocol and QoS parameters such as end-to-end delay, throughput and energy consumption are analyzed.

(iv) Implementation of modified Weighted Fair Queuing in AEERG Routing protocol.
Modified Weighted Fair Queuing is implemented in AEERG protocol in order to improve the QoS. m-WFQ is suitable for application where same information is to be communicated to two or more different applications with minimum delay. This queue results in better QoS compared to other queueing disciplines especially in military and other strategic communications.

The thesis outline is as follows:

In the second chapter of thesis, essence of gossip routing is stated. Conventional gossip protocols with their algorithms are explained. All the energy conservation techniques are discussed.

In the third chapter of thesis, basic concepts for all fundamental technical concepts are explained. The energy saving algorithms and their mechanisms are explained. The transport protocols operations such as UDP and TCP are explained. Various queuing disciplines are discussed such as First in First Out (FIFO), Random Early Detection (RED) and Priority Queuing (PQ) methods are applied for the gossip routing algorithm.

In the fourth chapter of thesis, proposed protocol with adaptive technique in AODV gossip routing protocol is introduced. Applications with scenarios are given at the end of this chapter. The adaptive technique consists of Remote activated switch. It is placed in the physical layer. With RAS, RF signal is used to change the node’s state. Thus we implemented adaptive technique for the communication of packets. Simulation is carried out to analyze the performance metrics like Packet delivery Ratio, Consumption of Energy, Routing overhead. Mathematical model of proposed protocol is developed. It is theoretically shown that minimum number of paths conserves energy with better reliability by using the adaptive technique. With this, for
the proposed routing protocol, User Datagram Protocol (UDP) and Transport Control protocol (TCP) is applied to carry the packets. Analyses are made for performance comparison of the parameters end to end delay, throughput and energy conservation. Results are obtained for proposed protocol, GSP and AODV.

In the fifth chapter, Quality of Service is analyzed for the proposed protocol. Modified Weighted Fair Queuing (WFQ) is implemented for the proposed protocol. Performances of Modified WFQ with WFQ is done and proved that the implemented M-WFQ gives better results. The M-WFQ is compared with other queuing disciplines and it has been proved that QoS has been improved with WFQ.

In the sixth chapter of thesis, the results of AEERG protocol with GSP, GAF and AODV are analyzed for Energy consumption and for reliability. Results proved that the proposed Adaptive Energy Efficient Reliable Gossip Routing Protocol achieved reliability with energy reduction by proposed routing protocol. Transport protocols of UDP and TCP are applied in AEERG and performance has been analyzed. The results showed that TCP transport routing protocol is better for good packet delivery ratio and UDP transport protocol is better for average end-to-end delay. So it has been concluded that for proposed routing protocol, choice of selection of transport protocol depends upon the application. FIFO, RED, PQ and WFQ queueing are applied to AEERG. Quality of service for AEERG is analyzed. But, in order to further improve the QoS for AEERG, modified WFQ is implemented in AEERG and its performance is compared with above queueing techniques. The results are compared with GSP and AODV. Results show that m-WFQ implemented AEERG gives better performance compared to the other two routing protocols.