CHAPTER 1

INTRODUCTION TO WIRELESS NETWORK AND ROUTING PROTOCOLS

1.1 INTRODUCTION

Wireless technology is a radical paradigm change which enables communication between devices from any location without connected cables, using radio waves to maintain communication channels. The rapid technological advances and innovations in the past few decades have drastically reduced the size and energy requirements of the wireless devices. The advances in access to wireless broadband internet and multimedia content have increased popularity of wireless communication.

There are principally three different types of wireless networks – Wireless Wide Area Networks (WWAN), Wireless Local Area Networks (WLAN) and Wireless Personal Area Networks (WPAN). WWAN is wireless connectivity, created through the signals using cellular tower technology, normally offered and maintained by specific mobile phone (cellular) service providers. WWANs are infrastructure based networks, covering large geographical areas. WLAN are wireless networks that use radio waves but usually have a wired infrastructure as backbone, with one or more wireless access points connecting to the wired network. The range of a WLAN varies from a single room to an entire campus. WPAN is short-range networks with a range of about 30 feet.
“Communication anytime and anywhere” is made possible with the development of wireless transmissions and portable computing devices. Users on the move can still remain connected with the rest of the world. This is called mobile computing or nomadic computing by Archarys et al (1996). Single hop connectivity to the wired network is commonly used in nomadic computing applications. This is the usual cellular network model where base stations or access points support the wireless communication; communications between two mobile hosts completely rely on the wired backbone and the fixed base stations.

However, during natural disasters or radio shadows, the wired infrastructure may not be available for use by mobile hosts. Cost and performance factors of building fixed access points may not be feasible as in wilderness areas. Also when temporary networks are required in festival grounds, or outdoor meetings it is not feasible to erect wired infrastructure. In emergency search-and-rescue or military maneuvers, a temporary communication network needs to be set up immediately. A Mobile Ad hoc Network (MANET) by Lin et al (1999) can be used in such situations. A MANET consists of a set of mobile hosts operating without any support from established wired infrastructure like base stations or access points. Wireless links formed by the mobile hosts through its antennas provide communication channels. The mobile host may not be able to communicate directly with other mobile units in the network due to radio power limitation and channel utilization. Thus, a multi hop setting is used, where the data packets sent by the source units reaches the destination unit by the data being relayed through intermediate mobile units. Thus, each mobile host in a MANET serves as a router too.
1.2 INFRASTRUCTURE AND INFRASTRUCTURELESS NETWORK

Wireless mobile networks based on the cellular concept depends on infrastructure support of base stations, which acts as access points to the mobile devices to route messages to and from mobile nodes in specified transmission area. WLAN, Global System for Mobile Communications (GSM), Wireless local loop (WLL) are wireless networks based on this concept. Whereas MANET does not require any pre-existing fixed network infrastructure; centralized message passing device is not required for communicating between mobile nodes. MANET does not rely on any devices other than two or more mobile nodes to cooperate to form a network; mobile nodes are self-configuring, form their own network and transfer data packets to and from each other.

Comparison between cellular network and ad hoc wireless network by Toh (2002) is given in table 1.1.

Table 1.1 Comparison of Cellular network and Ad hoc wireless network

<table>
<thead>
<tr>
<th>Cellular Networks</th>
<th>Ad Hoc Wireless Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed infrastructure-based</td>
<td>Infrastructure less</td>
</tr>
<tr>
<td>Guaranteed bandwidth (designed for voice traffic)</td>
<td>Shared radio channel (more suitable for best-effort data traffic)</td>
</tr>
<tr>
<td>Centralized routing</td>
<td>Distributed routing</td>
</tr>
<tr>
<td>Circuit-switched (evolving toward packet switching)</td>
<td>Packet-switched (evolving toward emulation of circuit switching)</td>
</tr>
<tr>
<td>Application domains mainly include civilian and commercial sectors</td>
<td>Application domains include battlefields, emergency search and rescue operations, and collaborative computing</td>
</tr>
</tbody>
</table>
Table 1.1 (Continued)

<table>
<thead>
<tr>
<th>Cellular Networks</th>
<th>Ad Hoc Wireless Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>High cost and time of deployment</td>
<td>Quick and cost-effective deployment</td>
</tr>
<tr>
<td>Reuse of frequency spectrum through geographical channel reuse</td>
<td>Dynamic frequency reuse based on carrier sense mechanism</td>
</tr>
<tr>
<td>Easier to employ bandwidth reservation</td>
<td>Bandwidth reservation requires complex medium access control protocols</td>
</tr>
<tr>
<td>Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio</td>
<td>Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths</td>
</tr>
<tr>
<td>Widely deployed and currently in the fourth generation of evolution</td>
<td>Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense</td>
</tr>
</tbody>
</table>

1.3 AD HOC NETWORKS

An ad hoc wireless network consists of a set of mobile hosts operating without the aid of an established infrastructure. MANET is infrastructure less networks of mobile nodes linked with wireless connectivity by Freebersyser et al (2001) which are dynamic in nature, to transfer data. The mobile hosts are free to move randomly and arrange themselves arbitrarily; so the network’s topology keeps changing quickly. Figure 1.1 shows a MANET consisting of several home-computing devices. Ad hoc networks are the key to the evolution of wireless networks. Although military tactical communication is still considered the primary application for ad hoc networks, commercial
interest in this type of networks continues to grow. Applications such as rescue missions in times of natural disasters, law enforcement operations, commercial and educational use, and sensor networks are just a few possible commercial examples.

![Figure 1.1 Mobile Ad Hoc network](image)

In MANET, topology is highly dynamic and random. In addition, the distribution of nodes and, eventually, their capability of self-organizing play an important role. The main characteristics can be summarized as follows:

- The topology is highly dynamic and frequent changes in the topology leads to the difficulty in fault detection and management.

- MANETs have significantly lower capacity and reliability than its wired counterparts.

- Security is limited as it is unprotected by outside signals.

- MANETs are affected by higher loss rates, and can experience higher delays than fixed networks due to the wireless transmission.
MANET nodes rely on batteries or other exhaustible power supplies for their energy. This limits the processing power; this in turn limits services and applications supported by each node.

Ad hoc wireless networks inherit the traditional problems of wireless and mobile communications, such as bandwidth optimization, power control, and transmission quality enhancement. In addition, the multihop nature and the lack of fixed infrastructure generate new research problems such as discovery, and maintenance, as well as ad hoc addressing and self-routing.

1.4 ROUTING PROTOCOLS

The routing of the data packets in an ad-hoc network is complex due to the dynamic nature of the network. Nodes in an ad hoc network can move freely in and out of the network, that is, new nodes get included into the network and existing nodes move out of the network at any given time. This frequent change in topology of the network makes it difficult to maintain the correct routes. It is of critical importance that communication among the nodes is maintained. Routing protocols for efficient route establishment is widely researched in literature by Perkins (2000) and Belding-Royer et al (2003). Ad hoc routing protocols must operate in networks with not only highly dynamic topologies but, also where routing algorithms run on resource-constrained devices. Various routing protocols and algorithms have been proposed, and their performance under different network and traffic conditions have been studied and compared. The design considerations for an ideal routing protocol which deals with the limited energy resources and copes with dynamic topologies are:
- Simplicity and ease of implementation
- Routes should be loop free and multiple routes should be available
- Minimal control overhead
- Bandwidth, power and computing efficiency
- Scalability
- Security and reliability, satisfying Quality Of Service (QoS) requirements

Routing protocols can also be classified as unicast, geocast, multicast and broadcast forwarding Belding-Royer and Toh, CK (1999). Unicast forwarding is widely used in ad hoc networks, where one source node transfers data packets to one destination node. In multicast routing protocol, a node sends data packets to multiple destinations’ nodes. Nodes are included and excluded as desired in multicast forwarding. Geocast forwarding is a special type of multicast routing with a difference that the data packets are delivered to nodes present in the specific geographical area. In broadcast forwarding, the data packets are transmitted to all the neighbors located within one-hop from the source. This section presents various types of routing protocols.

1.4.1 Unicast Routing

Unicast routing protocols establish and maintain routes between a pair of nodes, such that the messages are delivered reliably and in time. The classical Internet link-state and distance-vector routing protocols are unicast routing protocols by Stevens (1994) but direct use of these in MANET is
infeasible by Toh (2002) due to the frequent link changes in ad hoc environment.

MANET routing protocols are usually subdivided into two major categories, proactive routing protocols and reactive on-demand routing protocols. Proactive routing protocols are based on the legacy of Internet distance-vector and link-state protocols. The routing information between pair of nodes is updated at fixed time intervals by propagation as the routing information is maintained in tables. These protocols are also referred to as Table-Driven protocols. Reactive on demand routing protocols establish the route to a destination only when there is a demand for it. The source node initiates the route discovery process, and once a route has been established, it is maintained until either the destination becomes inaccessible or until the route is no longer used, or expired by Belding-Royer et al (2003).

1.4.1.1 Proactive routing protocols (Table driven)

The proactive routing protocol constantly maintains the routes of each node to all other network nodes. The route creation and maintenance are performed through both periodic messages. Some of the proactive protocols are:

- Destination-Sequence Distance-Vector (DSDV)
- Optimized Link State Routing (OLSR)
- Topology Dissemination Based on Reverse-Path Forwarding (TBRPF).

DSDV protocol by Perkins and Bhagwat (1994) is a distance-vector protocol adapted to suit MANET. The shortest path route based on the number of hops is maintained in a routing table by each node to different destination
nodes. Destination sequence number is used to avoid loops in routing. The sequence number is incremented in accordance to the changes in the neighborhood of the node. This number is compared when multiple routes are available to a destination node; the route with the highest number is selected as it will be based on most-recent information.

CGSR and WRP are also based on the distance vector protocol as DSDV. CGSR is similar to DSDV, with clustering to increase the protocol scalability by Chiang et al (1997). The performance in CGSR is improved by using priority token scheduling, gateway code scheduling, and path reservation. WRP is another loop-free proactive protocol, which uses four tables for maintaining distance, link cost, routes and message retransmission information by Murthy and Garcia-Luna-Aceves, JJ (1996). The distance and the second-to-last hop information are used to avoid loops in the route. The main disadvantage of the entire distance vector shortest path based proactive routing protocols like DSDV, CGSR and WRP is the degree of complexity faced during link failures and additions.

OLSR protocol by Jacquet et al (1998) is an optimization of legacy link-state protocols adapted for MANET. Optimization is achieved by multipoint relay. Each node recognizes its multipoint relay, and when a message is flooded to all points on retransmission of the same it will identify its two hop neighbors. Moreover, when exchanging link-state routing information, a node lists only the connections to those neighbors who have selected it as its Multi-Point Relay selector (MPR) set. The protocol selects bi-directional links for routing, hence avoiding packet transfer over unidirectional links.

Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) by Bellur et al (2001) is similar to OLSR that employs a different overhead reduction technique. Shortest path tree is computed by each node to
all the other nodes but only part of the tree is propagated to the neighbors in an attempt to optimize bandwidth by Belding-Royer (2003). FSR, LANMAR is also based on link-state information. The FSR uses the fisheye technique. The FSR protocol by Pei et al (2000) will propagate link state information more frequently to 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. LANMAR by Pei et al (2000) builds on top of FSR and achieves hierarchical routing by partitioning the network nodes into different mobility groups; a landmark node is elected within each group to keep track of which logical subnet a node belongs to, and facilitates inter-group routing.

1.4.1.2 Reactive routing protocol (On Demand)

Reactive routing protocol establishes a route from source node to destination nodes only when required. This reduces the overhead in the network. Commonly used reactive routing protocols include:

- Dynamic Source Routing (DSR)
- Ad hoc On Demand Distance Vector (AODV)
- Temporally Ordered Routing Algorithm (TORA)
- Associatively Based Routing (ABR)
- Signal Stability Routing (SSR).

DSR is a loop-free, source based, on demand routing protocol by Johnson and Maltz (1996). In DSR, each node maintains a route collection which contains the source routes learned by the node. If the destination node route is not available in the route cache of the source node, then the route
discovery process is started. The entries in the route collection are constantly updated and new routes learnt are included.

AODV is a reactive improvement of the DSDV protocol. AODV creates routes on demand thus reducing the number of broadcasts by Perkins and Royer (1999). Similar to DSR, route discovery is initiated on-demand. The route request is then forwarded by the source to the neighbors, and so on, until either the destination or an intermediate node with a fresh route to the destination, are located. AODV requires less control overhead and memory requirements when compared to DSR as AODV packets contain only the destination address and not the full routing path information. Disadvantage of AODV is that it only works with symmetric links. In general, AODV works well in small to medium-size networks with moderate mobility.

TORA is built on the concept of link reversal of the Directed Acyclic Graph (DAG) by Park and Corson (1997). In addition to being loop-free and bandwidth efficient, TORA has the advantage of being highly adaptive and quick in route repair during link failure and also provides multiple routes for any desired source/destination pair. These properties make it especially suitable for large, highly dynamic, mobile ad hoc environments with dense node's populations. The limitation in TORA's applicability is that the algorithm fails if the nodes do not have a GPS positioning system or have synchronized clocks.

ABR protocol uses a new routing metric termed degree of association stability in selecting routes. The route thus selected has longer life, more stable and hence requires fewer updates. The periodic beaconing used to establish the association stability metrics, which may result in additional energy consumption is a disadvantage. Signal Stability Algorithm (SSA) by Dube, et al (1997) is basically an ABR protocol which also uses signal strength of the link while route selection.
In general, on-demand reactive protocols are more efficient than proactive routing protocols. Proactive protocols update routes to keep information current and also maintain multiple routes that might never be needed, which adds to routing overheads. Proactive routing protocols provide better quality of service than on-demand protocols as current routing information is available due to updating; this reduces the end-to-end delay. In on-demand protocols, the source node has to wait for the route to be discovered before communication can happen; this delay is a big constraint for real-time communication. Reactive protocols are more scalable. Proactive protocols are suitable for small scale static networks, while reactive protocols, such as DSR and AODV can normally work well in medium-size networks with moderate mobility by Belding-Royer (2003).

1.4.1.3 Hybrid routing protocols

Hybrid routing protocols combines reactive path setup with the proactive path probing, maintenance and improvement. The limitation of both reactive and proactive routing protocols is that both rely on a unipath route for each data session. Thus link break in active route, results in route discovery process. The route discovery process involves flooding, which gives rise to latency and additional overheads. Hybrid routing protocols use a mix of both proactive and reactive routing techniques to combine the virtues of both and overcome their failings. In practice, many algorithms like AntHocNet, Hybrid Ad Hoc Routing Protocol (HARP), Zone Routing Protocol (ZRP) are hybrid algorithms by Liu et al (2005) using both proactive and reactive components. In ZRP and HARP, nodes maintain routing information of nodes within its zone and its neighboring zones. Routing information within the zone is achieved by proactive techniques and use reactive techniques for information between zones. Thus no delay in the transmission is experienced within the zone, while a route discovery and route maintenance are required for every
other destination. AntHocNet (Caro 2004) is a hybrid algorithm based on the framework of Ant Colony Optimization (ACO). In ACO, the paths are set up as required at the start of the session. The paths are setup using reactive techniques, where ant agents called reactive forward ants is used. During a session, the paths are explored, maintained using proactive techniques, where ant agents called proactive forward ants is used. Link failures are handled by local repair or by warning preceding nodes in the route.

1.4.2 Multicasting Routing

Multicasting in the internet is a communication service which helps support multi-point applications. In ad hoc networks, multicast services are achieved through multicast packets. Multicast services in MANET are important due to the bandwidth and energy savings achieved by Chlamtac and Weinstein (1987). MANET multicast research started by adapting the existing approaches used in internet to ad hoc networks. Two main techniques by adapting internet approaches are used for multicast routing in fixed wireless networks:

- Group-shared tree
- Source-specific tree

In multicast routing, multicast trees are constructed interconnecting all the nodes in the multicast group. All the nodes in the tree path receive data packets. A single tree is constructed for the whole group in a group-shared tree whereas in source specific approach each source has a tree connecting all the receivers in it. Different multicast protocols for ad hoc networks based on trees are Multicast AODV (MAODV) by Royer and Perkins (1999) and AMRIS by Wu and Tay (1999). Both protocols are an on-demand, and
construct a shared delivery tree to support multiple senders and receivers within a multicast session.

The dynamic nature of MANET causes large overheads for the maintenance of the multicast routing trees. To avoid the overheads, a different approach based on meshes is used. Meshes support more connectivity than trees, thus avoiding drawbacks of multicast trees, e.g., intermittent connectivity, traffic concentration, or frequent tree reconfiguration. The major disadvantage of mesh technique is that it tends to form routing loops and on flooding high overhead is incurred in large networks (Madruga and Aceves 2001). Representative mesh-based multicast routing protocols include:

- Core-Assisted Mesh Protocol (CAMP)
- On-demand Multicast Routing Protocol (ODMRP)

Routing meshes are built to distribute multicast packets within groups. The ODMRP by Lee et al (2001) uses flooding to build the mesh, while CAMP uses one or more core nodes to assist in building the mesh. To avoid the significant delay in route recovery caused by link failures, another tree, which does not include the failed link, is immediately utilized.

1.5 FACTORS AFFECTING ROUTING

The following is a summary of the major challenges to provide QoS in MANETs.

- Unreliable Wireless Channel

The wireless channel is prone to bit errors due to interference from other transmissions, thermal noise, shadowing, and multipath fading effects by
Saunders (2001). This makes it impossible to provide high packet delivery ratio or link longevity guarantees.

- **Node Mobility**

  The nodes in a MANET may move completely independently and randomly as far as the communications protocols are concerned. This means that topology information has a limited lifetime and must be updated frequently to allow data packets to be routed to their destinations. Again, this invalidates any hard packet delivery ratio or link stability guarantees. Furthermore, a QoS state which is link- or node position dependent must be updated with a frequency that increases with node mobility.

  An important general assumption must also be stated here: for any routing protocol to be able to function properly, the rate of topology change must not be greater than the rate of state information propagation. Otherwise, the routing information will always be stale and routing will be inefficient or could even fail completely. This applies equally to QoS state and QoS route information. A network that satisfies this condition is said to be combinatorially stable Chakrabarti et al (2001).

- **Lack of Centralized Control**

  The major advantage of an ad hoc network is that it may be set up spontaneously, without planning, and its members can change dynamically. This makes it difficult to provide any form of centralized control. As such, communications protocols which utilize only locally available state and operate in a completely distributed manner are preferred (Perkins 2001). This generally increases an algorithm’s overhead and complexity, as QoS state information must be disseminated efficiently.
Channel Contention

In order to discover network topology, nodes in a MANET must communicate on a common channel. However, this introduces the problems of interference and channel contention. For peer-to-peer data communications these can be avoided in various ways. One way is to attempt global clock synchronization and use a TDMA-based system where each node may transmit at a predefined time. This is difficult to achieve due to the lack of a central controller, node mobility, the complexity, and overhead involved (Yang and Kravets 2005). Other ways are to use a different frequency band or spreading code for each transmitter. This requires a distributed channel selection mechanism as well as the dissemination of channel information. However data communications take place, without a central controller, some setup, new neighbor discovery and control operations must take place on a common contended channel. Indeed, avoiding the aforementioned complications, much MANET research, as well as the currently most popular wireless ad hoc networking technology (802.11x) is based on fully-contended access to a common channel, that is, with Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA).

However, CSMA/CA greatly complicates the calculation of potential throughput and packet delay, compared to Time-Division Multiple Access (TDMA) based approaches. This is because nodes must also take into account the traffic at all nodes within their carrier sensing range. Furthermore, the possibility of collisions also arises. Collisions waste channel capacity, as well as node battery energy, increase delay, and can degrade the packet delivery ratio.

Finally, the well-understood hidden node by Klienrock and Tobagi (1975) and exposed node by Shukla et al (2003) problems are a further consequence of channel contention. These problems are even more
pronounced when the nodes may interfere with transmissions outside of their transmission range by Yang et al (2003) and Chen et al (2005), since receivers are able to detect a signal at a much greater distance than that at which they can decode its information.

- **Limited Device Resources**

  Mobile devices have less computational power, less memory, and a limited (battery) power supply, compared to devices such as desktop computers typically employed in wired networks. This factor has a major impact on the provision of QoS assurances, since low memory capacity limits the amount of QoS state that can be stored, necessitating more frequent updates, which incur greater overhead. Additionally, QoS routing generally incurs a greater overhead than best-effort routing in the first place, due to the extra information being disseminated. These factors lead to a higher drain on mobile nodes’ limited battery power supply. Finally, within the pool of QoS routing problems, many are NP-complete by Chakrabarti and Mishra (2001), and thus complicated heuristics are required for solving them, which may place an undue strain on mobile nodes’ less-powerful processors.

1.6 **METRICS EMPLOYED FOR ROUTE SELECTION**

- **Network Layer Metrics**

  Achievable throughput or residual capacity (bits/sec) - The achievable data throughput of a path or node or residual capacity is often termed “available bandwidth” in the literature; it is preferred to reserve the use of the word “bandwidth” for quantifying the size of frequency bands in Hz.

  End-to-end delay(s) - the measured end-to-end delay on a path by Chen and Nahrstedt (1999).
Node buffer space - the number of packets in a node’s transmission buffer plays a major part in determining the amount of delay a packet traveling through that node will suffer by Sheng et al (2003).

Delay jitter(s) or variance - the measured delay jitter on a path.

Packet Loss Ratio (PLR) (percent) - the percentage of total packets sent, which is not received by the transport or higher layer agent at the packet’s final destination node.


Route lifetime(s) - the statistically calculated expected lifetime of a route, can depend on node mobility as well as node battery charges by Rubin and Liu (2003).

- Link and MAC Layer Metrics

MAC delay – the time which is taken to transmit a packet between two nodes in a contention-based MAC, including the total time deferred, and the time to acknowledge the data (Fan 2004). This provides a good indication of the amount of traffic at the relevant nodes.

Link reliability or frame delivery ratio – the statistically calculated chance (percentage) of a packet or frame being transmitted over a link and correctly decoded at the receiver by Misra and Banerjee (2002) and Barolli et al (2003).

Link stability(s) – the predicted lifetime of a link by Rubin and Liu (2003)

Node relative mobility/stability – can be measured as the ratio of the number of neighbors that change over a fixed period to the number that remain
the same by Nikaein et al (2001). For example, if all of the node’s neighbors are the same over a fixed period, that node is completely stable in that period, relative to its neighbors. This is listed as a link-layer metric, since neighbor discovery is usually performed at that layer.

- **Physical Layer Metrics**

  Signal-to-Interference Ratio (SIR) – although a physical layer metric, the received SIR at a destination node can be used as a routing metric that shows link quality, via cross-layer communication by Kim et al (2004).

  Bit Error Rate (BER) – closely related to SIR, this value determines the level of error correction and/or number of retransmissions required over a “link” and has a major impact on the link’s reliability metric and on energy consumption. From another perspective, the BER is a consequence of the SIR between two nodes Wisitpongphan et al (2005).

  QoS metrics such as the above can be classified as either additive, concave, or multiplicative metrics, based on their mathematical properties (Reddy 2004). Additive metrics are defined as over path P, of length n, where $L_i(m)$ is the value of the metric m over link $L_i$ and $L_i \in P$.

  \[
  \sum_{i=1}^{n} L_i(m) \tag{1.1}
  \]

  The value of a concave metric $C_m$ is defined as the minimum value of that metric over a path, that is, $C_m = \min(L_i(m))$. Finally, a multiplicative metric $M_m$ is calculated by taking the product of the values along a path,
Thus, end-to-end delay for example, is an additive metric, since it is cumulative over the whole path. Available channel capacity is a concave metric, since interest is only on the bottleneck: the minimum value on the path. Finally, path reliability is a multiplicative metric, since the reliabilities of each link in the path must be multiplied together to compute the chance of delivering the packet via a given route (assuming that the MAC layer retransmissions have been considered in the reliability value, or that there are no retransmissions for example, for broadcast packets).

1.7 METRICS USED FOR EVALUATION IN AD HOC NETWORK

The following are some of the important metrics, which certifies the performance of the protocols:

- Packet delivery ratio (PDR): The ratio of the number of packets originated by the “application layer” of Constant Bit Rate (CBR) sources to the number of packets received by the CBR at the destination.

- Routing overhead: The number of extra routing packets “transmitted” per data packet to “delivered” at the destination node is called the routing overhead.

- Path optimality: The difference between the number of hops a packet takes to reach its destination and the length of the shortest path that physically exists through the network when the packet is originated.
• Throughput: Average number of messages successfully transmitted per unit time. The metric throughput points to the average number of messages successfully transmitted per unit time. It is also the function of the other factors like congestion, collision and packet loss, etc.

• End-to-end delay: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times.

• Connection Success Ratio (CSR): It is the ratio of successfully established connections to the number of connections attempted in a scenario.

• Normalized Effective Throughput (NET): Effective throughput is measured as the ratio of data bits (UDP data) received at the destination to the total time during which connection between source and destination was functional. An average of this throughput per network scenario is then normalized with respect to MAC throughput as well as routing throughput to calculate the normalized effective throughput. It reflects how effectively the network resources are used.

• Route Acquisition Time: It is the time required to establish a route when requested in an on-demand routing protocol.

Some ratios that are used as a measure of the efficiency of a protocol are:

• Average number of data bits transmitted/data bit delivered: This is the measure of the bit efficiency of delivering data
within the network. Indirectly, it also gives the average hop count taken by data packets.

- **Average number of control bits transmitted/data bit delivered:** This ratio gives the bit efficiency of the protocol in expending control overhead to delivery data, anything that is not data is control overhead and should be counted in the control portion of the algorithm.

- **Average number of control and data packets transmitted/data packet delivered:** This measures a protocol’s channel access efficiency, as the cost of channel access is high in contention-based link layers.

**Metrics related to the network are:**

- **Network size:** The number of nodes in a network.

- **Network connectivity:** The average number of neighbors of a node.

- **Topological rate of change:** The speed with which the network’s topology is changing.

- **Link capacity:** Effective link speed after losses due to multiple accesses, coding, etc.

- **Traffic patterns:** The effectiveness of a protocol in adapting to non-uniform traffic patterns.

### 1.8 OPNET SIMULATION SOFTWARE

Constructing an ad hoc network test bed for a project is infeasible and costly. Also protocol scalability, speeds of network are difficult to evaluate using test bed. Thus simulation is used to study the network behavior
under various parameters. Simulation is preferred over analytic model of the network as simulation offers more flexibility and has the ability to model network details. The factors taken into consideration during simulation are: number of nodes in simulated area, movement of users in simulated area, node mobility model and so on by Bononi et al (2004).

Network environment and performance metrics are defined to establish a repeatable simulation environment. The ad hoc network architecture and protocols under different network scenario and constraints is studied using simulation models. Simulations help in the selection of routing protocol by comparing the metrics of various protocols in a systematic way. OPNET by Cavin et al (2002), NS-2, Glomosim are some of the popularly used network simulators. The simulators contain libraries of predefined models of most communication models. OPNET provides with a graphical interface during model development stage and during simulations. The OPNET provides advanced simulation environment for testing and debugging of different protocols. Collision detection modules, radio propagation and MAC protocol can be studied too.

1.9 OBJECTIVE OF THE THESIS

The main objective of this research is to decrease the network overheads without affecting the QoS of the network in highly dynamic ad hoc networks. Highly dynamic and dense network have to maintain acceptable level of service in delivering data packets and limiting the network control overheads. This capability is closely related to, as how quickly the network protocol control overhead is managed as a function of increased link changes. Dynamically limiting the routing control overheads based on the network
topology improves the throughput of the network. The following are some of the contributions of this thesis:

- Propose an improved AODV based on Link quality. Investigate the performance of the proposed protocol and compare it with AODV.

- Propose a novel routing algorithm, Varying Overhead Ad hoc On Demand Distance Vector (VO-AODV), which is an extension of AODV routing protocol to decrease network overheads.

- Propose an optimization techniques based on Ant Colony Optimization (ACO) to improve the packet delivery ratio of the proposed routing protocol.

- Propose a hybrid optimization technique based on ACO and Tabu search.

1.10 THEESIS ORGANIZATION

The organization of the rest of the thesis is as follows:

Chapter 2 presents a survey of related works.

Chapter 3 consists of the effects of link quality in wireless network and investigations conducted with the proposed L_{qm}-AODV for varying pause time and also discussed about the proposed routing algorithm Varying Overhead Ad hoc On Demand distance Vector (VO-AODV) routing protocol. The simulation results and conclusions of the proposed routing protocol are given.
Chapter 4 deals with the optimization of the VOO-AODV with Ant Colony Optimization.

Chapter 5 presents the hybrid optimization based on ACO and Tabu search for improving the routing performance.

Chapter 6 concludes the thesis and elaborates on the direction of future investigations.

1.11 SUMMARY

A MANET consists of a set of mobile hosts operating without any support from established wired infrastructure like base stations or access points. Wireless links formed by the mobile hosts through its antennas provide communication channels. The routing of the data packets in an ad-hoc network is complex due to the dynamic nature of the network. The different types of routing protocol, i.e., proactive, on-demand and hybrid routing protocol, used in wireless network is discussed. Factors affecting the routing are detailed. Route selection in wireless network decides the efficiency of the network. The metrics used for evaluation during routing is discussed. Further, the metrics used for evaluating the performance of the network is also studied in detail. In this chapter, introduction to MANET and routing with various aspects related to MANET is explained in detail.