CHAPTER 1
INTRODUCTION

Wireless communication has shown its numerous advantages over wired communication since Guglielmo Marconi successfully transmitted signals across the English Channel for the first time in 1898. In recent years various wireless communication networks have been developed, such as cellular networks [TRA2002], Wireless LANs (WLAN) [IEE1997], Bluetooth networks [JHA2000], Ultra-Wideband (UWB) Networks [SRO2004], Mobile Ad Hoc Networks (MANETs) [CSI2004] and WiMax [IEE2004]. Among these, Cellular networks, Bluetooth networks and WLANs are the most widely used. However, Cellular networks and WLANs are centralized networks, which mean that costly infrastructure and centralized administration are required. Using Bluetooth technology, hosts can connect to each other in an ad hoc fashion, but this technology is only targeted at low power short-range wire replacement. Therefore, a distributed, self-organized and multi-hop network a Wireless Mobile Ad Hoc Network is a different type of network that has obtained tremendous attention in recent years.

A MANET is a distributed network that does not require centralized control, and every host works not only as a source and a sink but also as a router. This type of dynamic network is especially useful for military communications or emergency search-and-rescue operations, where an infrastructure cannot be supported. Furthermore, the simplicity of building an ad hoc network enables sharing data in a meeting or in inhospitable terrain conveniently. At the same time, the rapid development of coding technologies, such as MPEG-4 [TSI1997] and H.264 [TWI2003], makes low data rate video over wireless feasible. Enabling such multimedia, military applications as video and audio communication in MANETs requires Secure Quality of Service (QoS) support. To provide a support for QoS parameters and fool proof security protocol for ad hoc routing is a very challenging task due its unique characteristics. In this thesis, the over all objectives of the research work is to design a Secure and QoS Enabled Communication Support to soft real-time application areas such as military, multimedia and voice telephony.

1.1 CELLULAR NETWORKS VS MOBILE AD HOC NETWORKS

Cellular network is based on the cellular architecture in which a large area to be covered is divided in to several cells, each having a fixed base station. Each cell consists of several Mobile
Chapter 1: Introduction

Terminals (MT) which communicate to other mobile terminals in a same cell through the base station as shown in Figure 1.1.

![Figure 1.1 A Cellular network](image)

1.1.1 Mobile Ad hoc Networks

Mobile Ad hoc Networks (MANETs) are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. As shown in Figure 1.2, there are no base stations and every node must co-operate in forwarding packets in the network. Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes. The comparison between cellular networks and ad hoc wireless networks are summarized in Table 1.1.

![Figure 1.2 A Mobile Ad hoc Network](image)

---

2
Chapter 1: Introduction

### TABLE 1.1 Comparison Between Cellular Networks and Ad hoc Wireless Networks

<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>Single-hop wireless links</td>
<td>Multi-hop wireless links</td>
</tr>
<tr>
<td>Guaranteed bandwidth (design 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>Seamless connectivity (low call drops during handoffs)</td>
<td>Frequent path breaks due to mobility</td>
</tr>
<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 achieve time synchronization</td>
<td>Time synchronization is difficult and consumes bandwidth</td>
</tr>
<tr>
<td>Easier to employ bandwidth reservation</td>
<td>Bandwidth reservation requires complex medium access control protocols</td>
</tr>
<tr>
<td>Application domains include mainly civilian and commercial sectors</td>
<td>Application domains include battlefields, emergency search and rescue operations, and collaborative computing</td>
</tr>
<tr>
<td>High cost of network maintenance (backup power source, staffing, etc.)</td>
<td>Self-organization and maintenance properties are built into the network</td>
</tr>
<tr>
<td>Mobile hosts are of relatively low complexity</td>
<td>Mobile hosts require more intelligence (should have a transceiver as well as routing / switching, capability)</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 third 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>

### 1.2 MANETs FEATURES THAT IMPACT SECURITY AND QoS

- **Resource Reservation and Bandwidth Constraints:** The provisioning of QoS defined by parameters such as bandwidth, delay, buffer space, stale route information and processing power. The inherent mobility of nodes in MANETs makes QoS a difficult task.

- **Denial of Service Attack:** The Denial of Service (DoS) attack does not allow authorized user to access the service. DoS attack launched by IP Spoofing and TCP SYN consumes bandwidth that impact QoS in MANET.
Chapter 1: Introduction

- **Infrastructure-less**: Central servers, specialized hardware and fixed routers are necessarily absent. The lack of such infrastructure precludes the deployment of centralized host relationships. Instead, nodes uphold an egalitarian relationship that is, any security solution should rely on a distributed cooperative scheme instead of a centralized scheme.

- **Wireless Link Use**: Wireless link usage renders ad hoc networks susceptible to attacks. Unlike wired networks, in which an adversary must gain physical access to the network’s wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad hoc network can come from all directions and target any node. Hence, ad hoc networks will not have a clear line of defense and every node must be prepared to defend against threats. Moreover, the MAC protocols used in ad hoc networks, such IEEE 802.11 rely on trusted cooperation in a neighborhood to ensure channel access, which leads to high vulnerability.

- **Lack of Central Authority**: Because of the lack of central routers and gateways, hosts are themselves routers [CAR2005]. Thus, packets follow multi hop routes and pass through different mobile nodes before arriving at their final destination. Due to the possible untrustworthiness of such nodes or no any central authority, this feature presents a serious vulnerability.

- **Lack of Association**: Since the networks are dynamic in nature, a node can join or leave the networks at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join the network quite easily and carry out attack [CKT2002].

- **Node Movement Autonomy**: Mobile nodes are generally autonomous units that are capable of roaming independently. This means that tracking down a particular mobile node in a large-scale ad hoc network cannot be done easily.

- **Amorphous**: Node mobility and wireless connectivity allow nodes to enter and leave the network spontaneously, to form and break links unintentionally. Therefore, the network topology has no fixed form regarding both its size and shape, i.e., it changes frequently. Any security solution must take this feature into account.

- **Power Limitation**: Ad hoc enabled mobile hosts are small and lightweight, and they are often supplied with limited power resources, such as small batteries. This limitation
Chapter 1: Introduction

does vulnerability, namely, attackers may target some node’s batteries to disconnect them, which may lead to a network partition. This is called an energy starvation attack or sleep deprivation torture attack. This feature also represents a challenging constraint when designing security solutions for MANETs.

- **Memory and Computation Power Limitation:** Ad hoc enabled mobile nodes have limited storage devices and weak computational capabilities. Consequently, high complexity security solutions, such as symmetric or asymmetric data encryption, are difficult to implement.

1.3 APPLICATIONS OF AD HOC WIRELESS NETWORKS

Ad hoc wireless networks, due to their quick and economically less demanding deployment, find applications in several areas. Some of these include: military applications, collaborative and distributed computing, emergency operations, wireless mesh networks and wireless sensor networks.

- **Military Applications:** Ad hoc wireless networks can be very useful in establishing communication among a group of soldiers for tactical operations [ZJH2002]. Setting up a fixed infrastructure for communication among a group of soldiers in enemy territories or in inhospitable terrains may not be possible. In such environments, ad hoc wireless networks provide the required communication mechanism quickly. Another application in this area can be the coordination of military objects moving at high speeds such as fleets of airplanes or warships. Such applications require quick and reliable communication. Secure communication is of prime importance as eavesdropping or other security threats can compromise the purpose of communication or the safety of personnel involved in these tactical operations.

- **Collaborative and Distributed Computing:** Another domain in which the ad hoc wireless networks find applications is collaborative computing. The requirement of a temporary communication infrastructure for quick communication with minimal configuration among a group of people in a conference or gathering necessitates the formation of an ad hoc wireless network. In such cases, the formation of an ad hoc wireless network with the necessary support for reliable and soft real-time multicast routing can serve the purpose.
Chapter 1: Introduction

- **Emergency Operations:** Ad hoc wireless networks are very useful in emergency operations such as search and rescue, crowd control and commando operations. The major factors that favor ad hoc wireless networks for such tasks are self-configuration of the system with minimal overhead. In environments where the conventional infrastructure-based communication facilities are destroyed due to a war or due to natural calamities such as earthquakes, immediate deployment of ad hoc wireless networks would be a good solution for coordinating rescue activities.

- **Wireless Mesh Networks:** Wireless mesh networks are ad hoc wireless networks that are formed to provide an alternate communication infrastructure for mobile or fixed nodes / users, without the spectrum reuse constraints and the requirements of network planning of cellular networks. The mesh topology of wireless mesh networks provides many alternate paths for a data transfer session between a source and destination, resulting in quick reconfiguration of the path when the existing path fails due to node failures. Wireless mesh networks provide very high availability compared to the existing cellular architecture, where the presence of a fixed base station that covers a much larger area involves the risk of a single point of failure.

- **Wireless Sensor Networks:** Sensor networks are a special category of ad hoc wireless networks that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain. Recent advances in wireless communication technology and research in ad hoc wireless networks have made smart sensing a reality. Sensor nodes are tiny devices that have the capability of sensing physical parameters, detecting border intrusion, sensing the temperature of a furnace to prevent it rising beyond a threshold, and measuring the stress on critical structures or machinery is example of the sensing activities [IFA2002].

1.4 **ISSUES IN AD HOC WIRELESS NETWORK**

The major issues that affect the design, deployment and performance of an ad hoc wireless system are as follows:

- **Medium Access Scheme:** The primary responsibility of a Medium Access Control (MAC) protocol in ad hoc wireless networks is the distributed arbitration for the shared channel for transmission of packets. The performance of any wireless network hinges on
Chapter 1: Introduction

the MAC protocol, more so for ad hoc wireless networks. The major issues to be considered in designing a MAC protocol for ad hoc wireless networks are distributed operation, synchronization, hidden terminals, exposed terminals, access delay, fairness, real-time traffic support and resource reservation.

- **Routing:** The responsibilities of a routing protocol include exchanging the route information; finding a feasible path to a destination based on criteria such as hop length, minimum power required, lifetime of the wireless link, gathering information about the path breaks, mending the broken paths expending minimum processing power and bandwidth. The major challenges that a routing protocol faces are mobility, bandwidth constraint, error-prone and shared channel, location-dependent contention, computing power, battery power and buffer storage also limit the capability of a routing protocol.

- **Multicasting:** It plays an important role in the typical applications of ad hoc wireless networks, namely, emergency search-and-rescue operations and military communication. The major issues in designing multicast routing protocols are robustness, efficiency, control overhead, QoS support, efficient group management, scalability and security.

- **Quality of Service Provisioning:** The goal of QoS provisioning is to achieve a more deterministic network behaviors, so that information carried by the network can be better delivered and network resources can be better utilized. The first step toward a QoS-aware routing protocol is to have the routing use QoS parameters for finding a path. The parameters that can be considered for routing decisions are network throughput, packet delivery ratio, reliability, delay, jitter, packet loss rate, bit error rate and path loss.

- **Security:** The security of communication in ad hoc wireless networks is very important, especially in military applications. The lack of any central coordination and shared wireless medium makes them more vulnerable to attacks than wired networks. The major security threats that exist in ad hoc wireless networks are Denial of service, Resource consumption, Buffer overflow, Host impersonation and Information disclosure.

- **Scalability:** Scalability of a routing protocol is its ability to support the continuous increase in the network parameters (such as mobility rate, traffic rate and network size) without degrading network performance. Scalability has a direct relation with routing overhead, which in turn has a direct relation with varying network parameters. First, these relations must be understood and analyzed properly. Second, the responsible routing
strategies for these relations must be devised carefully to achieve better network performance. Therefore, scalability is an important issue for routing protocols in MANETs.

- **Transport Layer Protocols:** The main objectives of the transport layer protocols include setting up and maintaining end-to-end connections, reliable end-to-end delivery of data packets, flow control and congestion control. There exist simple connectionless transport layer protocols (e.g. UDP) which neither perform flow control and congestion control nor provide reliable data transfer. Such unreliable connectionless transport layer protocols do not take into account the current network status such as congestion at the intermediate links, the rate of collision, or other similar factors affecting the network throughput. This behavior of the transport layer protocols increases the connection of the already-choked wireless links. The major performance degradation faced by a reliable connection-oriented transport layer protocol such as Transmission Control Protocol (TCP) in an ad hoc wireless network arises due to frequent path breaks, presence of stale routing information, high channel error rate and frequent network partitions.

- **Energy Management:** It is defined as the process of managing the sources and consumers of energy in a node or in the network as a whole for enhancing the lifetime of the network. Shaping the energy discharge pattern of a node’s battery to enhance the battery life; finding routes that result in minimum total energy consumption in the network; using distributed scheduling schemes to improve battery life; and handling the processor and interface devices to minimize power consumption are some of the functions of energy management.

### 1.5 SECURITY IN MOBILE AD HOC NETWORKS

Wireless mobile ad hoc nature of MANET brings new security challenges to network design. Mobile ad hoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats. In this section, we explore the various security requirements (goals) for wireless ad hoc network and the classification of security threats.

#### 1.5.1 Security Goals

To secure an ad hoc network, a security protocol must satisfy the following attributes: confidentiality, integrity, availability, authenticity and non-repudiation [LZH1999] [MOP2008].
Chapter 1: Introduction

- **Confidentiality:** Ensures that classified information in the network is never disclosed to unauthorized entities. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.

- **Integrity:** It guarantees that a message being transferred between nodes is never altered or corrupted. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

- **Availability:** It implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system. Availability of a network can be tempered for example by dropping off packets and by resource depletion attacks.

- **Authenticity:** It is a network service to determine a user’s identity. Without authentication, an attacker can impersonate any node, and in this way, one by one node, it can gain control over the entire network.

Finally, non-repudiation ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

1.5.2 Security Attacks on Ad hoc Routing Protocols

The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as shown in Figure 1.3.

- **Passive Attacks:** A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it.

- **Active Attacks:** An active attack attempts to alter or destroy the data being exchanged in the network thereby disrupting the normal functioning of the network.

- **External Attacks:** These attacks are carried out by nodes that do not belong to the network.

- **Internal Attacks:** These attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks.
Chapter 1: Introduction

1.6 DEFINITION OF QoS

In the originally used network model, traffic is transmitted only with best-effort. It means that there is no quality guarantee for each transmission. When the real-time traffic is transmitted in the network, the QoS becomes demanding. In addition, because of the limitation of network resources especially in wireless networks, real time traffic need to be given higher priority to ensure that it reaches the destination on time [SHA 2006].

For the transmission of non-real time data, timing is not a critical issue. As a result, the non-real time network could work well without guarantee of timely delivery of data. The applications of non real time data transmissions are Telnet, FTP, E-mail and web browsing. For real time transmission like telephone, video conference, streaming video and audio, the basic requirement is to transmit packets to the destination on time need QoS provisioning. QoS parameters for different applications are shown in Table 1.2.

<table>
<thead>
<tr>
<th>Applications</th>
<th>QoS Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military</td>
<td>Security</td>
</tr>
<tr>
<td>Defense</td>
<td>Trust</td>
</tr>
<tr>
<td>Multimedia</td>
<td>Packet delivery ratio, End to End delay, Routing overhead, Throughput, Jitter, Bandwidth and Packet delay variation</td>
</tr>
<tr>
<td>Emergency search-and-rescue operation</td>
<td>Availability</td>
</tr>
<tr>
<td>Conference communication</td>
<td>Battery life</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

1.6.1 QoS in Different Layers

- **QoS in Physical Layer**: Take care of changes in transmission quality.
- **QoS in Data Link Layer**: Take care of the variable bit error rate.
- **QoS in Network Layer**: Take care of the change in bandwidth and delay.
- **QoS in Transportation Layer**: Take care of the delay and packet loss due to transmission errors.
- **QoS in Application Layer**: Take care of frequent disconnections and reconnections

1.6.2 Classification of QoS Metrics

The QoS metrics can be classified into three categories as described in Figure 1.4. These are additive metrics, concave metrics and multiplicative metrics.

![Figure 1.4 Classification of Different QoS Metrics](image)

- **Additive Metrics**: It is defined as sum of the value of the metric on all links along the path.
  Delay and jitter are additive metrics.
- **Concave Metric**: It means the minimum metric value over a path. Bandwidth and Data rate are concave metrics.
Chapter 1: Introduction

- **Multiplicative Metric**: It represents the product of the metric values on all links over a path. Link outage probability, reliability are multiplicative metrics.

1.6.3 Classifications of QoS Approaches

The QoS approach classification is shown in Figure 1.5.

I) **Based on the Interaction between the Routing Protocol and the QoS Provisioning Mechanism.**

- Coupled QoS approach, the routing protocol and the QoS provisioning mechanism closely interact with each other for delivering QoS guarantees. If the routing protocol changes, it may fail to ensure QoS guarantees [CSI2004].
- Decoupled approach, the QoS provisioning mechanism does not depend on any specific routing protocol to ensure QoS guarantees.

II) **Based on the Interaction between the Network and the MAC Layers**

- Independent QoS approach, the network layer is not dependent on the MAC layer for QoS provisioning.
Chapter 1: Introduction

- Dependent QoS approach requires the MAC layer to assist the routing protocol for QoS provisioning.

III) Based on the Routing Information Update Mechanism.
- Table-driven approach, each node in the network maintains a routing table which aids in forwarding packets.
- On-demand approach, no such tables are maintained at the nodes, and hence the source node has to discover the route on the fly.
- Hybrid approach incorporates features of both the table-driven and the on-demand approaches.

1.7 SIMULATION TOOLS
Simulation is the process of testing a designed model on a platform which imitates the real environment. It provides the opportunity to create, modify and study the behavior of proposed design. It helps the user to predict its strengths and weakness before implementing the model in real environment. Some of the popular simulators used to simulate the ad hoc networks are:

- NS2 (Network Simulator 2)
- OPNET

1.7.1 Introduction to NS2
NS2 is an object oriented, discrete event driven network simulator [KFA2002]. It is written in C++ and OTcl (Tcl (Tool command language) script language with object-oriented extensions developed at MIT (Massachusetts Institute of Technology). In order to reduce the processing time, the basic network component objects are written using C++. Each object has a matching OTcl object through an OTcl linkage NS provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless networks. NS can run under both UNIX and Windows operating systems.

Random Waypoint mobility (RWP) model is a mobility model which defines node movement pattern that is widely used to evaluate the performance of MANET protocols. In RWP node’s speed, direction and destination are chosen randomly once parameters are set. It produces large amounts of relative nodes movement because of which network topology changes. NS2 offers setdest command to generate waypoint mobility. Continuous Bit Rate traffic (CBR) connections are used. Source generates 512-byte long UDP packets. Source and destination pairs
are chosen randomly. NS2 provides `cbrgen.tcl` tool to generate traffic pattern file. Figure 1.6 shows the simulation flow/run.

First, the user has to program with OTcl script language to initiate an event scheduler, set up the network topology using the network objects and tell traffic sources when to start and stop transmitting packets through the event scheduler. OTcl script is executed by NS2. The simulation results from running this script in NS2 include one or more text-based output files and an input to a graphical simulation display tool called Network Animator (NAM). Text-based files record the activities taking place in the network. It can be analyzed by other tools such as Gwak and Gnuplot to calculate and draw the results such as delay and jitter in the form of figures or tables.

NAM is an animation tool for viewing network simulation traces and real-world packet traces. It has a graphical interface which can present information such as the number of packets drops at each link. The main window of NAM is depicted in Figure 1.7.
Chapter 1: Introduction

1.7.2 OPNET-Network Simulator

OPNET is network modeling software that predicts performance of networking protocols and networks through simulation. Simulation allows us to reproduce the unfavorable conditions of networks in a controllable and repeatable lab setting. Key benefits of OPNET are as follows:

- **Speed**: OPNET can support real-time and faster than real-time simulation speed, which enables software-in-the-loop, network emulation, hardware-in-the-loop, and human-in-the-loop exercises.

- **Scalability**: OPNET supports thousands of nodes. It can also take advantage of parallel computing architectures to support more network nodes and faster modeling. Speed and scalability are not mutually exclusive with OPNET.

- **Model Fidelity**: OPNET offers highly detailed models for all aspects of networking. This ensures accurate modeling results and enables detailed analysis of protocol and network performance.

- **Extensibility**: OPNET connects to other hardware and software applications, such as OTB, real networks, and STK, greatly enhancing the value of the network model.
Chapter 1: Introduction

1.8 RESEARCH OBJECTIVE

The overall objective of the research work is to provide a Secure and QoS Enabled Communication Support in MANETs for soft real-time application areas such as military, multimedia and voice telephony etc. The research work gives an overview of routing layer solutions for ad hoc networks and describes how Security and QoS can be added to ad hoc networks especially in the network layer. Figure 1.8 gives pictorial representation of the work carried out in this thesis. In this thesis, we have used NS2 and OPNET simulator to analyze QoS parameters on routing protocols for Scalability, Voice over Internet Protocol, On-demand Link-state Mutipath Support over MANETs. An efficient generic search algorithm, a model for Cache Coherence handling and Trust Conscious Secure routing for reactive protocols has been proposed. Our research contributes as follow:

- Overview of ad hoc networks, its features that impact QoS and security, QoS approaches classification and descriptions of the MANETs routing protocols which are used during research work are discussed. In literature survey, different issues such as scalability, QoS provisioning, cache handling to provide cache coherence, VoIP support over MANETs, Trust based routing and QoS provisioning in term of bandwidth and security are investigated.

- The impact of scalability on various QoS parameters for MANETs routing protocols is analyzed by varying number of nodes, packet size, time interval between packets and mobility rates. The performance metrics comprises of QoS parameters such as packet delivery ratio, end to end delay, routing overhead, throughput and jitter.

- An efficient generic search algorithm on associative cache memory organization to speedup searching of single/multiple paths for destination, if exist, in intermediate mobile node cache with a complexity O(n)(where n is number of bits required to represent the searched field) is proposed. To handle the Stale Cache problem, we have also proposed an optimized cache coherence handling scheme for on-demand routing protocol (DSR).

- The various QoS parameters on different routing protocols for the voice transmission support over Hybrid MANETs have been analyzed using OPNET simulator.
Chapter 1: Introduction

- Trust reflects expectations on the honesty, integrity, ability, availability and quality of service. The proposed Trust Conscious approach dynamically increases the trust (in term of security) between the nodes and provides secure routing.

- The goal of the proposed Secure QoS Enabled On-demand Link-state Multipath routing protocol is to provide QoS provisioning in term of bandwidth and security. The protocol search single/multiples path that collectively satisfy the required bandwidth. The above said protocol also provides security provisioning during en-route process to foil the spoofing, modification, fabrication, routing loops and denial of service attacks.

Figure 1.8 Pictorial Representation of the Work Carried Out in this Thesis
1.9 THESIS ORGANIZATION

The rest of thesis is organized as follow:

**Chapter 2:** Descriptions of the MANETs routing protocols covered during research work are summarized.

**Chapter 3:** In ‘Literature Survey’ various problem areas of mobile ad hoc network are studied. This chapter starts with a brief description of problem areas of MANETs such as scalability, secure routing, voice transmission and cache handling are discussed.

**Chapter 4:** Forms the crux of this thesis and discusses the simulation carried out to analyze the impact of scalability on various QoS parameters for MANETs routing protocols.

**Chapter 5:** Describes a search algorithm and a scheme to handle the cache coherence problem on DSR protocol.

**Chapter 6:** Highlights the performance of different routing protocols during voice transmission over Hybrid MANETs.

**Chapter 7:** Describes an approach to dynamically increase the trust (in term of security) between the nodes and provides secure routing.

**Chapter 8:** Overall working of proposed Secure QoS Enabled On-demand Link-state Multipath Routing protocol to provide QoS provisioning in term of bandwidth and security has been discussed.

**Chapter 9:** We summarize the research work and give an outline of the broader impact of the thesis and provide further scope of research.