Chapter 1

Introduction

1.1 GENERAL

The current computing scenario, with abundant mobile hosts using wireless networking, requires their integration with the existing conventional network facilities such as internet for effective application of the network services. Often the mobile users need to communicate instantly in contexts, where fixed infrastructure is unavailable or economically non-viable to install or requires lot of time for installation. Typical situations requiring expediency in communication include, a group of students participating in teleconference, transfer or sharing of files among business associates while on the move, or rescue team negotiating natural disasters or combating soldiers in hostile territories. In such circumstances, a cluster of mobile hosts can be integrated to wireless network interfaces to form a provisional network without depending on any established infrastructure or centralized control. Such a temporary network is termed as Mobile Ad hoc Network (MANET). (Charles Perkins et al., 1999) opine a MANET to be a conglomeration of individual mobile nodes competent to mutually communicate without seeking assistance from any conventional network infrastructure.

1.2 ORIGINS OF MANET

MANETs function on the primary principle of multi-hop relaying with the other nodes assisting message transmission, when the target node is inaccessible directly. The origins of multi-hop communication can be traced to early times of civilization. Persian King, Darius I (533-486 B.C.) was believed to have used a sort of multi-hop transmission by strategically placing messengers at elevated places at regular distances, which relayed the messages by loudly shouting. The immediate neighbor picked up the message for further transmission without moving from his place. This innovative multi-hop transmission was believed to be
23 times more effective than the conventional methods in transmitting the messages across the length and breadth of the empire. As an extension of this, a ‘Packet Radio’ project was launched by DARPA (Defense Advanced Research Project Agency) in 1970, for use in battle front, enhancing the scope of the concept of packet switching, to the sphere of radio network broadcast.

1.3 EVOLUTION OF MANET

MANETs could be perceived, as several individual nodes integrated into an ad hoc network, devoid of support or assistance from any centralized infrastructure. Such networks are ideally suited for network contexts of either lost infrastructure or where installation and deployment of right infrastructure could be very expensive or not possible. The ad hoc network systems could be broadly classified into three generations. PRNET (Packet Radio Networks) marks the first generation, dating back to 1972, functioning in combination with ALOHA (Areal Location of Hazardous Atmospheres) and CSMA (Carrier Sense Multiple Access), adopting the methods of medium access control and a sort of distance-vector routing. The second generation emerged in 1980 with further expansion and deployment of ad hoc networks as a component of SURAN (Survivable Adaptive Radio Networks) program. This enabled the networks to switch packets in mobile network ambience without infrastructure, enhancing the performance of radios, shaping them to be much smaller in size, economic and resistant to various electronic attacks. With the evolution of note book computers, the decade of 1990 launched ad hoc networks on commercial perspective marking the third generation, realizing the dire need of the concept of mobile nodes being integrated.

1.4 SAILENT FEATURES OF MANET

The current times have been witnessing a growing popularity and concentrated focus on the evolution and evaluation of wireless networks devoid of infrastructure. MANET can be classified among such networks independent of either the base stations or any requirement of wired points for accession or intercommunication. This non-dependence on infrastructure differentiates it from the other static networks. Broadly, MANET can be understood as conglomeration of several independent mobile nodes intercommunicating without any rooted
foundation or base. Direct communication is possible among the neighboring nodes only. Hence, any internal communication among the remote nodes depends on multiple-hops. The prime aspects of difference between MANETs and the networks based on infrastructure are listed out by (Khalili et al., 2003) as:

- **Absence of Fixed Topology:** MANET’s topology is highly volatile and dynamic because of the mobile nature of the individual nodes, where the nodes freely and frequently move in and out of the range of one another.

- **Energy Constraints:** In general all the mobile devices rely on battery power which could be exhausted over a period of time. There is a provision for some devices to slip into sleep mode as energy saving measure. The performance of the devices in sleep may not be optimal. They may possibly be unreachable, or cannot efficiently negotiate the network traffic or may not be able to revert to standard mode with latency. The mobile devices usually utilize the spread spectrum communications requiring signal reception and decoding, which consume a lot of energy. In addition, the computational processes are complex and prove expensive in terms of energy. As a result, power can be quickly exhausted in MANETs.

- **Processor Limitations:** The processors in most of the mobile devices are moderate and slow in order to accommodate factors of cost and portability, since faster processors are expensive and larger in size. Hence, complex computational processes may involve more operational time in MANETs.

- **Constraints of Storage and Other Resources:** Due to compulsions of cost and portability condition in most of the mobile devices to opt for moderate storage capabilities. On the other hand, several bandwidth constraints are imposed even by some wireless technologies.
• **Transient Availability and Connectivity:** In order to conserve power, several nodes may remain unavailable at times. In such phases of time, they become inaccessible to the other nodes.

• **Every Node as a Router:** A fixed node in the network cannot reach the out-of-range nodes directly. Such nodes can only be accessed by the process of the other nodes forwarding the packets.

• **Sharing of Physical Medium:** The transmission medium in MANETs remains accessible to all the devices within the range, unlike as in the wired networks, where accession is restricted.

• **Absence of centralized Management:** A centralized management in MANETs is not always available as the very nature of the network is ad hoc and it can be established anytime at any place.

Due to the constraints of the absence of any fixed infrastructure and the availability of very limited resources, it becomes complex to adopt diverse protocols or different technologies into MANET from other networks based on fixed infrastructure.

### 1.5 MANET APPLICATIONS

Ever enhancing utilization of portable devices, constantly growing range of applications and explosive strides in wireless communication propelled ad hoc networking into lime light in the modern times. In instances of existing infrastructure being either too expensive or inconvenient for utilization, mobile Ad hoc networks come in handy with their ease in application from almost anywhere. Ad hoc networking is flexible and permits connectivity between the devices and the network, or adds or removes the devices with reference to the network as easily. The range of MANET applications are vast and versatile from applications of greater magnitude, highly dynamic and mobile networks to moderate static networks, which have inherent constraints of power sources. Besides, in case of legacy applications which shift from the conventional infrastructure environment to MANET’s ad hoc environment, several new services are generated which are compatible to the new environment (Lee et al., 2007). Some of the typical applications are Military Battlefield, Emergency or

1.6 MANET CHALLENGES

MANETs are vulnerable to several security challenges ranging from simple and passive eavesdropping to more active direct interference, exposing their susceptibility to attacks both internal and external or threats of Denial of Service (DoS) due to their wireless nature, limited computing capabilities and consumption of power. It is difficult to effectively deploy security mechanisms in the absence of any responsible Centralized Authority (CA) or a Trusted Third Party (TTP). Besides, a malicious attacker could launch attacks on the network through a compromised trusted node. The following are some of the major issues affecting an ad hoc wireless network system in its design, development, deployment and performance:

**Medium Access Scheme:** In the context of the absence of any centralized control in ad hoc networks, the major responsibility of Medium Access Control Protocol (MACP). (Chlamatac et al., 2003) is the distributed arbitration in packet transmission for channels shared.

**Routing:** Packet routing between any two nodes can become a major issue and a challenging task in the ad hoc network, due to its frequently changing and volatile topography. Reactive routing becomes the basis for several protocols instead of proactive routing. Communication routes between the nodes are accomplished potentially more through multiple hops than a single hop, which makes it further complex. Hence there is a dire requirement of new protocols for routing.

**Multicasting:** Periodic restructuring of the links of the nodes is required in ad hoc networks, since they need data and voice communication from a single point to multi-point or from multi-point to multi-point. In general, the multicast protocols depend on the precondition that the routers are static. After the formation of the multicast tree, there will be no movement of the tree nodes. But the scenario is different in MANET (Frodigh et al., 2000) and environment. Consequently, multicast routing is
another major challenge to be addressed as the multicast tree is no more static due to the random movement of the nodes within the network.

**Security and Reliability:** Besides the general inherent vulnerabilities associated with wireless connections, MANET has its unique security issues, including nasty neighbor relaying packets. The aspect of distributed operation needs diverse authentication schemes and key management. In addition, reliability problems also crop up due to the characteristics of wireless link, such as limited range of wireless transmission, the wireless medium’s nature of broadcast, (e.g. hidden/exposed terminal problem) packet losses induced by mobility and errors in the transmission of data. Challenges of such types obviously demand a gross requirement for evolving solutions of security and reliability in order to accomplish broad protection, as well as network performance at desired levels (Dahill et al., 2001; Zhou and Haas, 1999).

**Energy Management:** The dual functioning of the nodes of MANET both as the host and the routers require more energy. Since just small batteries with inadequate lifetime of energy provide power to the network nodes, the management of energy turns to be another challenge requiring necessary consideration and apt remedial measures (Li et al., 2006).

**TCP Performance:** As the Transmission Control Protocol (TCP) cannot differentiate between the congestion occurrence in the network and mobility, there is a requirement of additional modifications and enhancement, so that proper performance levels of the transport protocol can be ensured, with the end-to-end throughput of communication remaining unaffected (Zhu et al., 2005).

In spite of the several attractive features embedded in MANETs and the exponential growth of their applications, they still face numerous challenges as evident from the above illustrations. Each single challenge referred to, has immense potential for individual consideration and research focus requiring thorough probe and analysis.

1.7 MANET SECURITY CRITERIA

In spite of the enhanced applications of MANETs, they are still required to be adequately secured at least in three major areas, namely services, attacks and
mechanisms pertaining to security. In order to implement the basic functionalities of network services, possible security threats and challenges must be anticipated and required blocks of structure to encounter, resist and alleviate the effects of the security breaches must be developed in the very design and architecture of the networks. The ultimate security objectives of MANET should be to provide robust fundamental security services such as authentication, confidentiality, integrity, non-repudiation and availability to all the mobile users (Murthy and Mano 2004; Stallings 2003). Authentication, understands the specific identity of the partner in communication. Confidentiality is prohibiting the unauthorized users to access secure information. Integrity assures no unwarranted content modifications during data transmission. Non-repudiation is the source or destination of the message not denying having sent the message. Availability is uninterrupted provision of all the normal network services, even while under attacks. The network security solutions must furnish comprehensive security and protection covering the entire stack of protocols to accomplish these objectives. Since a single mechanism cannot provide all these security services for the MANETs, they could be obtained through a combination with certain MANET applications, such as recovery after disaster and military etc., (Luo and Fang, 2003). Considered security services are further illustrated below:

**Authentication:** In a network environment Authentication is a fundamental requisite to confirm that the peers at both the ends are not impersonators but genuine. Authentication ensures that the authorized individuals alone can either access or supply the data. User authentication techniques are indispensable for the efficient operation of MANETs. Authentication failures could lead to a rival gaining unauthorized access to sensitive data and important resources disguised as a genuine node and subsequently interfering with the operations and functions of the other nodes in the network (Zhou and Haas 1999).

**Confidentiality:** Confidentiality ensures that the contents of the transmitting message remain inaccessible to unauthorized entities, such as the intermediate nodes. The messages must be readable and understood only by the authorized parties. Fundamentally, the data is protected from passive attacks. Information of sensitive nature, such as that of military need dis
Crest handling and requires confidentiality. Any leakage of such information during transmission to the adversaries could be catastrophic and may result in dire consequences. Information regarding routing and forwarding of packets also must be kept confidential in order to prevent the adversaries from taking advantage of locating or identifying the intended targets in the battle front. Any acknowledged method of encryption with appropriate key management system can procure and ensure confidentiality.

**Integrity**: Integrity ensures permission exclusively to the authorized parties only for making any modifications in the messages or information. It further guarantees that any unauthorized entities cannot alter, corrupt or retransmit the message being transmitted. This integrity can be very critical, while handling the data related to military or banking or equipment controls such as planes or trains, where any slightest modification could result in dire consequences. Both modification of stream of messages and denial of service are addressed here.

**Non-Repudiation**: Non-repudiation averts either the receiver or the sender from refuting a message that has been transmitted. Thus, when a message is transmitted, it is possible for the receiver to establish the fact that the alleged sender has transmitted that specific message. Similarly, after relaying a message, the sender can ascertain that the alleged receiver has received the message. Non-repudiation is specifically valuable in instances of identifying and isolating the compromised nodes. When node B transmits an erroneous message to node A, non-repudiation makes it possible for node A to use this message to accuse B and persuade the other nodes about node B being compromised. This is vital, specifically in instances of disagreement in certain situations. This can be procured through the processes such as obtaining digital signatures, which can easily co-relate the data relayed or received to the actual signed entity.

**Availability**: A node must be in a position to provide all the essential services at all times, whenever they are required, irrespective of any contingencies or attacks. Besides, the idea of availability of a network denotes that a need-based accessibility to all network services must be ensured in all circumstances, including the instances of break-in.
The availability may have certain limitations or may be reduced or even lost due to diverse attacks. It is possible to counter certain categories of attacks adopting automated countermeasures comprising of encryption or authentication, while some other categories need a deliberate action to counter them and to recover from the consequent losses and to restore the normal availability of all the service aspects of a network system. Hence, the objective of availability is to ensure the survivability of the services of a network despite diverse attacks. For instance, at the physical layer or the control layer of media access, hostile entities could introduce jamming in order to disrupt communication through physical channel, while at network layer, the routing protocol or network service continuity could be interfered and adversely affected. Further, in higher levels, it is possible for the adversary to cause deterioration of high-level services including services of authentication and key management (Zhou and Haas 1999).

1.8 MANET SECURITY ATTACKS

Depending on the nature of attacks, a broad two-fold classification of the attacks in MANET can be made, as active attacks and passive attacks (Yi and Kravets, 2004). An active attack disrupts MANET’s standard functionalities through the means of interruption, alteration and fabrication of information, while a passive attack does not disrupt network’s communication operations but stealthily obtains access to the data exchanged or transmitted in the network.

Table 1.1 demonstrates a broad categorization and lists out the possible security attacks encountered by MANETs. Based on the targeted domain of attack, yet another categorization of these attacks can be made as internal or external attacks. (Kozhat and Tassiula 2004). The magnitude of severity and consequent damage is comparatively higher through internal attacks than the external attacks, since the insider has the privilege of both the knowledge of secret and valuable information and the required accession rights.

Another approach to the nomenclature of attacks is, on the basis of protocol stacks of network. Table 1.2 displays a categorization of security attacks on the basis of protocol stack. It is possible to launch attacks at different or multiple layers. Some security attacks adopt the approach of stealth (Perkins et al., 2002), in an attempt to
hide their activities from the detection of either an automated Intrusion Detection System (IDS) or a closely monitoring individual. This approach of stealth cannot be used by other security attacks such as DoS.

**Table 1.1 Classifications of Security Attacks**

<table>
<thead>
<tr>
<th>Category</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive Attacks</td>
<td>Eavesdropping, Traffic analysis, Monitoring</td>
</tr>
<tr>
<td>Active Attacks</td>
<td>Jamming, Spoofing, Modification, Replying, DoS</td>
</tr>
</tbody>
</table>

**Table 1.2 Security Attacks on Protocol Stacks**

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td>Repudiation, Data corruption</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Session hijacking, SYN flooding</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Wormhole, Black hole, Byzantine, Flooding, Resource Consumption, Location Disclosure</td>
</tr>
<tr>
<td>Data link Layer</td>
<td>Traffic analysis, Monitoring, Disruption MAC (802.11)</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>Jamming, Interceptions, Eavesdropping</td>
</tr>
<tr>
<td>Multi-layer attacks</td>
<td>DoS, Impersonation, Replay, Man-in-the-middle</td>
</tr>
</tbody>
</table>

1.8.1 PHYSICAL LAYER ATTACKS

Most of the wireless communication systems extensively use Radio Frequency (RF) spectrum. It is easy to eavesdrop or intercept RF spectrum and to inject fake messages into the networks by attuning the receivers to the appropriate frequency (Karygiannis and Owens, 2002). Abundant avenues are open to interfere or jam radio signals leading to corruption or even loss of messages. An attacker in possession of powerful transmission mechanism can generate a stronger signal to subvert and crush the targeted signal and cause disruption in communications, using usually random pulse and noise signal jamming procedures.
1.8.2 LINK LAYER ATTACKS

The architecture of MANET is open and adopts peer-to-peer multipoint design. The link layer protocols specifically maintain single-hop connectivity among the participating neighboring nodes. This connectivity is further extended to the different other network nodes by the protocols of the network layer. Link layer may be the primary target of the attackers in an attempt to disrupt the harmonious cooperation existing in inter-layer protocols.

Traffic Monitoring and Analysis: The attackers may resort to the method of monitoring and analyzing the traffic to understand the parties involved in communication and various functionalities, thus extracting information for further onslaughts. (Borisov et al., 2011). Since these attacks are not directed exclusively towards the MANETs, there is a potential threat to diverse wireless networks including WLAN, cellular networks and satellite networks which suffer from these vulnerabilities. However, the focus of the study is not on such types of security attacks on this layer in MANETs.

Disruption on MACP and Back-off Mechanism: Wireless Medium Access Control Protocol (MACP) must ensure right coordination among the nodes through a common medium of transmission. IEEE 802.11 protocol in specific is allotted to WLANs, since radio-channel control cannot be maintained employing a token-passing bus MAC protocol. The IEEE 802.11 MACP employs the mechanisms of dispersed contention resolution in order to share the wireless channel. For contention resolution, two algorithms are proposed by the IEEE 802.11 work group.

A well-coordinated and cooperative inter-node behavior is the basic presumption of the wireless MACPs at present. Obviously, it is not mandatory for the selfish or malicious nodes to follow these standard protocols of operation. A malicious or selfish node, at link layer, could cause interruption among MACPs, which are based either on contention or reservation. It is possible for a deliberate malicious neighbor of the receiver or the sender, not to follow the accepted specifications of the protocols intentionally.
1.8.3 NETWORK LAYER ATTACKS

The protocols of the network layer expand the connectivity from the adjacent one-hop nodes to the other participating nodes in the MANET. Mutual cooperative responses among the participating network nodes are the prime requisites for establishing potential wireless multi-hop connectivity among the mobile hosts. The focus of several researchers and extensive studies has been on identifying a wide range of attacks encountered by the network layer. The attackers can intercept and intrude into the network traffic, in between the source and the target, absorb portion of it and take a control over the traffic flow of the network, in the process of their malicious attacks on the routing protocols.

The following are some of the possibilities: forwarding of the traffic packets to a non-optimal path or causing considerable delay or transmitting to a path that does not exist and consequently getting lost.

**Attacks at the Route Discovery Phase:** Some malicious attacks target the maintenance or discovery phase by violating the specifications of the standard routing protocols. Some simple instances of routing attacks aiming at the route discovery phase can be hello-flooding, attacks of routing message flooding, flooding of Route Request packets (RREQ), flooding of acknowledgements, overflow of routing table, routing loop and routing cache poisoning (Hu and Perrig, 2004).

**Attacks at the Route Maintenance Phase:** Some attacks affect the phase of route maintenance through transmitting dubious control messages, such as error messages suggesting broken link, necessitating expensive operations for repairing and route maintenance. For example, Ad-hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) employ several procedures for maintenance of path in order to recover and restore broken paths in the context of moving nodes. The upstream node related to the broken link, on detecting any movement of intermediate or destination node along the dynamic path, sends out a message of route error to all its active neighbors in the upstream. Further, the node invalidates this particular route for the specific target in its routing register. This
could be greatly advantageous to the attackers for launching malicious onslaughts through dispatching error messages of false route.

**Attacks on Specific Routing Protocols:** Some attacks specifically target particular protocols of routing. For instance, in DSR, the focus of the attacker may be on the modification of the source route as has been registered in the packets of RREQ or Route Reply (RREP). The nature of attack may involve modification of the list by deletion of an existing node or addition of a new node or rearranging the order of nodes. The other variation of the attack may be in the form of the attacker announcing a route with much smaller metric of distance than the actual one, or publicize the updates of routing with larger number of sequence and thereby invalidating all updates of routing existing in the other nodes.

1.8.4 OTHER ADVANCED ATTACKS

Several researchers in recent times have identified very subtle and more advanced routing attacks. The wormhole, black hole (or sinkhole) and Byzantine are some prominent ones among them, which are detailed hereunder:

**Wormhole Attack:** This is a malicious practice of the attacker seizing the packets at some specific location and tunneling them to another network location. When such tunneling of the control messages of routing occurs, there could be a disruption in the routing procedures. Such a tunnel existing between the accomplice attackers is generally termed as ‘wormhole’ (Ilyas, 2003). Wormhole attacks pose very serious threats to the protocols of routing in MANETs.

**Black hole Attack:** There are two major characteristics attributed to the black hole attack. The nasty node, intending to intercept the packets, may explore the routing protocols of the mobile ad hoc networks, such as AODV, to announce its possession of a valid route to the target node, though the route may be a fake one. Alternatively, the attacker may just consume such packets thus intercepted, without further transmitting those (Sanjay et al., 2003).

**Byzantine Attack:** Byzantine attacks are instances of the functioning of either a single compromised intermediary node or a cluster of such nodes, as accomplices
in launching attacks. The attacks usually include the creation of routing loop, packet transmission through an intentionally chosen non-optimal route or selective packet dropping, ultimately disrupting and degrading the services of routing (Ming et al., 2009).

**Rushing Attack:** In the Rushing attack (Hu et al., 2003) two accomplice attackers adopt the procedure of tunnel and form a wormhole. If there is a quick route of transmission in existence between either ends of the wormhole, such as the attackers sharing a dedicated channel, the tunneled packets disseminate much faster in comparison with the packets traversing through a standard route of multi-hop.

**Resource Consumption Attack:** In this category of attack, also understood as sleep deprivation attack, a compromised node or an aggressive attacker attempts to exhaust the life of battery through spurious requests for route discovery in excess, or through onward transmission of unnecessary packets in the direction of victim node.

1.8.5 TRANSPORT LAYER ATTACKS

Some major protocols in Transport layer in MANET are establishing end-to-end connection, flow control and congestion for clearance of end-to-end connection. The mobile node is just as vulnerable as the Internet’s TCP protocol to the typical synchronous (SYN) attacks of flooding or attack of session hijacking. But MANET records a higher rate of error in comparison with the wired networks. Since the TCP is not endowed with any mechanism to identify, whether the occurrence of loss is due to congestion or random errors or some malevolent attacks, the TCP on discovering the losses, correspondingly reduces its congestion window size, degrading the performance of the network considerably (Hsieh and Sivakumar, 2002).

**SYN Flooding Attack:** The SYN flooding attack is primarily a Denial of Service attack. Here, the attacker initiates a huge number of semi-opened connections of TCP with a victim node, without duly completing the process of opening the connection fully through the required handshake. As per the standard protocols, the victim node may store these semi-opened connections in a standard sized register awaiting the acknowledgement of a three-way handshake, marking the culmination of the transaction. In the meantime, the buffer could be overflowing with all these pending
semi-open connections disabling the victim node from receiving any fresh, even legitimate instances of opening a connection (Siris and Papagalou, 2006)

**Session Hijacking:** Session hijacking is an intelligent mode of attack, taking advantage of the general practices of security. Protection to sessions is provided in several instances in the form of furnished credentials, at the setup time and usually, not thereafter, exposing them to vicious attacks. The session hijackings attackers in the TCP spoof the IP address of the victim confirm the precise number of sequence as expected by at the target node and then launch DoS attacks of the session. It is a classic example of where the malicious attacker in the guise of a victim node, continues the session with the target, where the unsuspecting target becomes exposed and vulnerable.

1.8.6 APPLICATION LAYER ATTACKS

A majority of the Application layer threats are attacks of mobile viruses, worms or repudiation.

**Virus and Worm Attacks:** The user information contained in the application layer usually can support several protocols such as FTP, HTTP and SMTP. Malicious code, in the form of viruses and worms, can affect the operating systems and vulnerable applications.

**Repudiation Attack:** Installation of firewalls at the level of network layer, can keep the packets in or out. Encryption of the entire end-to-end range of connections at the level of transport layer can offer some protection. But the issues of either non-repudiation or authentication cannot be addressed in general, by these solutions. Repudiation concerns an outright denial of involvement in the process of communications either in part or whole. For instance, a selfish person may reject having conducted a credit card purchase operation or refuse any bank transaction online. These are prototypical instances of attacks of repudiation involving commercial systems.
1.8.7 MULTI-LAYER ATTACK

It is possible to launch certain security attacks from multiple layers in contrast to attacking a particular layer. Some instances of multi-layer attacks include attacks of DoS, impersonation and man-in-the-middle.

**Denial of Service:** Attacks of DoS can be initiated from multiple layers. For instance, an attacker can resort to jamming of the signals at the physical layer disrupting all the normal processes of communication. Malicious nodes can adopt capture-effect to occupy channels at the link layer, taking advantage of MACP’s binary exponential method and preventing channel access to the other nodes. The processes of routing at the network layer can be intercepted adopting packet modification of routing control, selective packet dropping, overflow of table or poisoning. Similarly, attacks of SYN flooding or hijacking of sessions and malicious programs can result in DoS, affecting the transport and application layers.

**Impersonation Attacks:** For most of the attackers, attacks of impersonation are the curtain raisers for launching several other serious and much sophisticated attacks. A malicious node for example, can herald an attack by means of modifying its addresses of Medium Access Control (MAC) or Internet protocol (IP).

**Man-in-the-middle Attacks:** In this category of attack, an attacker is stationed between receiver and the sender indulging in sniffing inter-change of information between them. In some situations, the attacker impersonates the sender in order to communicate with the receiver or responds to the sender disguised as the receiver. These result in severe breeches in MANET’s security.

1.9 RESEARCH MOTIVATION

Certain MANET applications such as the military battlefield heavily rely on Group communication, where frequent inter-communication is a primary requirement more among the neighboring nodes than the distant isolated nodes. Due to the quantity of involved nodes, there is a need for structured mechanism for furnishing scalability and maintain the entire network to ensure equal communication opportunities to all the nodes and orderly message transmission process. Providing security services in instances of group communication, specifically in adverse
ambience, is challenging. The offered solutions of security must be fortified against internal and external attacks and effectively resist them with similar vigor. Robust authentication mechanism, with appropriate key management strategies conducive to group communication environment, could block any unauthorized entry of an external node into the MANET. In addition, MANETs are susceptible to numerous internal attacks such as routing attacks, totally jeopardizing the entire system of group communication. The gravity of the attacks, for instance of the severe black hole attack, is all the more serious, since the victims remain ignorant of the fact that they are under attack and the network resources remain inaccessible to both the sender and the receiver. Only a very robust and reliable service of group communication, capable of handling larger networks, can negotiate all these MANET security issues and ensure proper availability of the network resources to all the nodes, even under conditions of attack.

1.10 PROBLEM STATEMENT

This research study focuses on the design features of dependable and secure mobile ad hoc networks. As several of the multi-hop wireless environments have inherent resource constraints of processing, energy and bandwidth, envisaging and creating apt mechanisms for detection of threats and adequate measures to counter various threats become more challenging tasks than they are in the corresponding wired networks. Our believe is that the current trends in technology can address and alleviate some of the issues pertaining to the constraints of resources, such as processing capabilities and memory in the near future, whereas the constraints of bandwidth and energy may stay for a little longer for obtaining suitable solutions.

This investigative and analytical study traces the origin and evolution of the MANETs, discusses their salient features of absence of infrastructure and centralized control and issues related to security, authentication and vulnerability to internal and external attacks. In this context, the work already done in this field and the existing schemes, their efficacy and limitations are studied and analyzed in order to evolve a meaningful and robust scheme capable of negotiating the inherent limitations and challenges in MANETs.
The study provides insights to develop a dependable ambience for group communication ambience and appropriate framework for identifying and preventing various black hole and wormhole attacks, using rigid graphs and the method of identifying trusted nodes for an efficient network performance during transmission. Further, a secure system of communication is envisioned to establish right authentications after due identification of the node ID through the method of voting in order to detect and isolate the intruder. A secure and trusted routing is selected computing the trust ID of the node by maintaining a log of destination, source, port, sequence numbers and subsequent hops in the look-up table. The method of Erlang distribution is considered in its various variations and integrated with Markov modulated processes to identify the occurrence of congestion in the network traffic and to evolve an appropriate framework for effective packet distribution, also considering the inter-departure time of the packets. The objective of this research work is to assist in the design and development of a robust architecture for the MANETs addressing several of their deficiencies and set-backs and make MANET applications strong, secure, reliable and efficient.

1.1 ORGANIZATION OF THE THESIS

Chapter 1 traces the origins and evolution of the MANET, defining certain salient features it encompasses such as its lack of fixed infrastructure or centralized control and vulnerability to threats, its applications and challenges including security and authentication. The possible threats to MANETs such as black hole and wormhole and the multi-layered attacks are also discussed leading to the problem statement and the requirement to develop a robust technology for effective implementation in MANETs, and to construct solutions to several MANET limitations.

Chapter 2 provides a general survey of literature on the available schemes of security at present, dealing with internal and external attacks as well as on congestion and trusted transmission. It also proposes a novel scheme of security in comparison with certain other schemes in existence at present.

Chapter 3 proposes a dependable environment of group communication for diverse nodes present in MANET after a thorough study and survey of the constraints and
advantages of the available schemes of security in the context of wormhole attack. It also evolves a dependable framework for identifying and preventing the attacks of wormhole employing rigid graphs and also detecting the trusted neighbors in order to enhance the performance of transmission. In addition, a comparative analysis with the proposed scheme is provided.

Chapter 4 puts forth a secure system of communication within the MANET subsequent to intense investigations about the constraints and advantages of the available security schemes to counter black hole attacks. It also attempts to evolve a framework for the identification of the black hole on the basis of the ID of the node and quality of the link in rule-set. Intruder is identified through a method of voting. A comparative assessment of the proposed scheme is also attempted.

Chapter 5 attempts to furnish a trusted route for the purpose of communication. Trust route is selected in accordance with the trust value of the nodes after a careful consideration and computation of the trust ID of the individual nodes in the network. Every node maintains all the relevant information regarding IP addresses of source and destination, port and sequence numbers and the subsequent hop address in the look-up table.

Chapter 6 addresses the issue of developing an appropriate framework in ad hoc mobile networks in order to evade occurrence of congestion. In source node congestion can be avoided by employing the method of Erlang distribution, where packet distribution is done on the basis of inter departure time, while in trusted node use of Markov modulated process can avoid congestion.

Chapter 7 provides a conclusion of the current study, emphasizing the valuable contributions in the area of study and opening up the possible avenues for further research in future.