CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

A Mobile ad hoc network (MANET) is a system of wireless mobile nodes that dynamically self-organize in random and momentary network topologies. A MANET is group of wireless networks consisting of a number of mobile nodes. Nodes in MANET connect and disconnect from the network dynamically. There is no permanent set of infrastructure and centralized administration in MANET. Nodes are organized and interconnected through wireless interface. The self-motivated nature of such type networks makes it extremely vulnerable to different link attacks. The essential needs for a protected networking are secure protocols, ensuring that the privacy, accessibility, authenticity and honesty of network. Many offered security solutions for wired networks are unproductive and useless for MANET environment. As the communication takes place in an open medium, the MANET communication is more susceptible to security attacks. In the occurrence of security protocol, the effects against different attacks are reduced. Therefore, the success of MANET communication greatly depends on the relationship of the participating mobile nodes.

A MANET is described by deficient in infrastructure, lack of centralized administration, recurrent mobility of nodes, network separation and wireless links. These characters indictate that the usual wire line security solutions are not directly applicable in MANET. Certainly, the properties
represent that the establishment of a public key infrastructure, is an unwieldy task in such networks.

Propagation of packet to the entire network is an essential process and includes broad applications in the MANET. The basic approach for transition is blind flooding, in which each node is compelled to retransmit the data whenever it obtains a packet for the first time. Blind flooding creates many repeated broadcasting. These repeated transmissions cause a serious trouble, referred as the transmission storm difficulty in which repeated packets leads to communication congestion and contention.

A MANET is a completely on-the-fly network utilized to maintain the idea of any time and any place transmission. MANET is an infrastructure-less network with a set of wireless mobile hosts to structure a temporary network without the support of any wired base stations. Each mobile node in such a network functions not only as a node but also as a router. The intrinsic restrictions of the MANET, such as insufficient resources and dynamic topologies, need a suitable routing protocol. The protocol design for such an environment requires straightforward, well-organized and robust structure. The methods that broadcast packets in the MANET are relatively unusual from that in the wired network, since a node transmits a packet, then all its neighbors receive that packet under the promiscuous receive mode.

Recent work on providing security comprises a fully-distributed Identification based Multiple secret Keys Management scheme (IMKM) facilitating an efficient key method. It involves an interaction of ID-based multiple secret and threshold cryptography. IMKM eliminates public key distribution using certificate authentication. In addition IMKM provides efficient key update and key revocation schemes. The nodes are clustered and needs a Cluster Heads (CHs) to participate in key construction. The updated cluster head shares the keys on establishing a threshold sharing of the master
secret key. Multiple secret keys scheme is able to withstand cryptanalysis and periodically updates share keys of CHs with a predefined time interval. The scheme does not require the exchange or signing of any additional messages. At last, the method supports improved performance by reducing computation and communication overheads. Efficient group key agreement provides authentication without authenticating signatures and needs only one round.

1.2 STATEMENT OF THE PROBLEM

Ensuring secure communication in ad hoc network is extremely challenging due to dynamic nature of the ad hoc network. The difficulty in MANET communication is that the data broadcast is insecure due to lack of centralized management. MANET is a division of ad hoc network working in wireless infrastructure-less environment in the way of self-configuring communication with the mobile devices. Each node or mobile device in a MANET is independent to each other moving without self-control in any route resulting in insecure communication. The independent behavior of node flow changed the interaction link to other devices or nodes frequently. The absence of fixed infrastructure in shared wireless medium results in node mobility and limited resources of mobile devices. Due to the limited resource in communication, the bandwidth is restricted. Additionally, error-prone communication links by key management is difficult to implement in ad hoc networks.

The information is broadcast with a secure private key. Group Key Agreement (GKA) protocol is the common protocol generally used in secure transmission. GKA protocol permits two or more parties to agree on common group key and exchange information over insecure channel. GKA provides mutual key authentication among parties involved in the communication.
The limitation of GKA protocol for transmission is its overcoming nature with the establishment of Authenticated Group Key Agreement (AGKAP) protocol applications in cooperative, distributed and self organized ad hoc networks. Design of secure and well-organized protocol for group key agreement gains much concentration as an important research area. The group key management protocol is also less efficient in the transmission of packets. Major researches are needed to be handled in the key management issues for securing MANET using clusters.

1.3 SECURITY IN MANET

Wireless Mesh Networks (WMNs) are noted as a standard choice for Internet Service Providers (ISPs) in broadcasting the information over wireless access. The WMNs are estimated to integrate the characteristics of self-organization, self-healing, and self-configuration for high consistency and scalability. In addition to the numerous advantages, the WMNs require security guarantees due to its open medium, shared architecture and inconsistent topology.

A MANET is an independent set of mobile nodes which communicate over moderately bandwidth restricted wireless links. MANET varies from predictable wireless networks, such as cellular networks and IEEE 802.11, an infrastructure mode networks as self-organizing. The infrastructure networks are self-containing i.e., the nodes communicates openly with each other lacking reliance on centralized infrastructures such as base stations. Additionally, MANET is self organizing and adaptive in the way of structuring and de-structuring on-the-fly without the need for any system administration.

These exclusive characters make MANET popular for situations which will need fast network use, such as search and rescue operations. The
decentralized property of MANET, specifically the deficiency of centralized entities offers a better application work nature. The avoidance of single point of disappointments makes these network models also perfect for military and commercial applications that require high level of robustness. But some challenging security issues are to be concentrated before MANET is set for extensive commercial or military deployment.

One of the major security issues in MANET is trust management. Trust is usually recognized and handled in wired and other wireless networks using centralized entities like Centralized Authority (CA) or Key Distribution Center (KDC). The lack of centralized entities in MANET creates trust management security issue as a challenging task. The inaccessibility of trusted authorities also builds crisis to achieve essential functions such as the revocation of distribution centre. Another attractive MANET security difficulty is the issue of false accusation in the existence of malicious nodes. The false accusation tries to prove the valid node as malicious node resulting in removal of legitimate node from the network. The malicious node causes several communication difficulties such as gap of opportunity problem.

In MANET, certification systems play a vital role to attain network security. Controlling the issue of certificate cancellation in wired network is simple compared to the MANET. In wired network when the certificate of a malicious node get canceled then the certificate authorities append the information about the cancelled node into the Certificate Revocation Lists (CRLs). Otherwise, they transmit the CRLs to each and every node present in the network or either saves them on an open repositories. But the certificate revocation is a difficult task in MANET and also this usual method of certificate revocation is not valuable for MANET due to lack of centralized repositories and trusted authorities. A method is required for MANET to
cancel the certificate of malicious nodes after detecting the first misbehavior of nodes.

The wireless technology makes MANET more susceptible to security attacks and due to this the established security methods does not offer a novel solution to MANET. A new protocol needs to be urbanized to overcome the disadvantage in the traditional security methods such as distribution centre. Symmetric key cryptography method requires trusted third party and vital repositories to preserve information about the node whose certificate is get cancelled. But these standard security methods fail in providing the preferred security in the case of wireless networks such as MANET. In other words, the capacity of the standard security approaches is only restricted to the wired networks and to some extent in the wireless networks because the number of security problems is less in wireless networks compared to wired networks.

1.3.1 Attacks in MANET

A MANET is an infrastructure-less category network containing number of mobile nodes with wireless network boundary. In order to establish communication among nodes, the nodes enthusiastically launch paths among one another. The character and outline of such networks make it interesting to several types of attackers. The section discusses different types of attacks on various layers under protocol stack. Various types of attacker try different approaches to drop off the network performance and throughput. The main attention is on routing and security issues related with mobile ad hoc networks which are necessary in order to offer secure communication. On the basis of the character of attacks on communication, the attacks against MANET are classified into two types, namely, active and passive attacks. Also the
attackers against a network are classified into two groups namely, insider and outsider. An outside attacker is not a legal user of the network but an insider attacker is a certified node and a component of the routing mechanism on MANET.

1.3.1.1 Vulnerabilities of MANETs

A MANET is vulnerable to different attacks not only from exterior but also from within the network itself. Ad hoc networks are essentially subjected to several vulnerability issues as follows:

**Dynamic Topology:** In MANET, nodes connect and disconnect from the network dynamically and travel independently. Due to such type character, there is no permanent set of topology mechanism in MANET. The node with insufficient physical security becomes malicious node and minimizes the network performance.

**Wireless Links:** As the nodes in such networks are interrelated through wireless interface that makes it extremely vulnerable to link attacks. The bandwidths of wireless networks are not as much of wired networks and offers less bandwidth. The less restricted bandwidth draws many attackers to stop normal communication among nodes.

**Cooperativeness:** In MANET, all routing protocols believe that nodes offer secure communication. But some nodes become malicious nodes which interrupt the network process by modifying routing information.

**Lack of clear line of defense:** There is no clear line of protection mechanism available in the MANET. Attacks come from any directions. Attackers attack the network either within the network or outside the network.
**Limited resources**: The MANET includes various collections of devices such as laptops, computers, and mobile phones and so on. All of such devices consist of different storage capacity, processing speed and computational cost. This attracts the attackers to concentrate on new attacks.

1.3.1.2 **Attackers**

There are various types of attackers present in MANET. They attempt to minimize the performance of network. The various attackers are categorized as shown in Figure 1.1.

![Figure 1.1 Classifications of Attackers](image-url)

**Figure 1.1 Classifications of Attackers**
Figure 1.1 describes the classification of attackers in MANET into five major types in two levels. The first level of attack arises on the fundamental means of the ad hoc network such as routing like emission, location and quantity. The second level of attacks attempts to break the security methods engaged in the network such as motivations and mobility.

### 1.3.1.3 Active and passive attacks

A MANET is more vulnerable to passive attacks. A passive attack does not change the data transmitted within the network. But it comprises the unauthorized listening to the network traffic or gathers data from it. Passive attacker does not interrupt the process of a routing protocol but tries to find the significant data from routed traffic.

Identification of such type of attacks is complex since the process of network itself does not get affected. In order to conquer this type of attacks dominant encryption algorithms are required to encrypt the data being broadcast. The attack against the MANET is kept on increasing due to its open medium and independent nature. In addition to passive attack, another attack that plays against secure communication is active attack.

Active attacks are very harsh attacks on the network that stop message flow between the nodes. But active attacks are of inside or outside type. Active outside attacks are handled by outside basis that do not belong to the network. Inside attacks are from malicious nodes which are part of the network. Internal attacks are more rigorous and inflexible to detect than external attacks. These attacks make unauthorized access to network that supports the attacker to make changes such as alteration of packets, denial of service and congestion.
Figure 1.2 describes the active and passive attacks in MANET. The passive attacker listens to the data broadcasted in the network. The active attacker acts as transmitter and changes the data transmitted to the receiver. Detecting the active attacks is more difficult compared to passive attacks. The nature of MANET formulates them vulnerable to many new attacks. The attacks in different layers of the network protocol stack are described in Table 1.1.
Table 1.1 Attacks on Protocols

<table>
<thead>
<tr>
<th>Layer</th>
<th>Types of Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Malicious code, Data corruption, Viruses and Worms</td>
</tr>
<tr>
<td>Transport</td>
<td>Session hijacking attack and SYN flooding attack</td>
</tr>
<tr>
<td>Network</td>
<td>Blackhole, Wormhole, Grayhole, Link spoofing, Rushing attack, Replay attack, Sybil attack, Resource consumption attack and Link withholding attack</td>
</tr>
<tr>
<td>Data Link</td>
<td>Selfish Misbehavor, Malicious Behavior, Traffic Analysis</td>
</tr>
<tr>
<td>Physical</td>
<td>Eavesdropping, Jamming and Active interference</td>
</tr>
</tbody>
</table>

The attacks on physical layer are hardware related and require support from hardware origins. These attacks are straightforward to perform as compared to other attacks. They do not need the entire knowledge of technology. Some of the attacks detected at physical layer comprise eavesdropping, intrusion and congestion.

1.3.1.4 Attacks at physical layer

Eavesdropping is an interception and interpretation of messages and discussions by unintended receivers. As the transmission takes place on wireless medium, the message is easily interrupted with receiver tuned to appropriate frequency. The major intention of such attacks is to take the confidential information that is kept covered during the transmission. The information includes private key, public key, place or passwords of the nodes. Classified data is eavesdropped by tapping transmission paths, and wireless links are easier to trace.
Figure 1.3 describes the attacker attacking on transmission between source and destination. Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. An active interference is a denial of service attack which stops the wireless communication channel or alters communications. Old messages are repeated to reinitiate the data information.

1.3.1.5 Attacks at network layer

The network layer protocols allow the MANET nodes to be linked with another through hop-by-hop. In MANET, every distinct node takes choice of route to transmit the packet. So, it is very simple for malicious node to attack on such network. The essential thought behind network layer attacks is to add itself in the active path from source to destination or to take up network traffic. In such attacks, the attackers build routing loops to form harsh congestion. Various type of attacks are detected which are initiated by malicious node. Figure 1.4 describes the routing attacks by the malicious nodes.
The malicious node X takes main data by locating itself between source A and destination D as shown in Figure 1.4. X also distracts the data packets swapped between A and D, resulting in significant end to end delay between A and D. The malicious node X interrupts the route path discovery process by constructing routing loops and overflow of routing tables.

In Blackhole Attack, malicious node maintains finest path to the node packet to be interrupted. On getting the request the malicious node forwards a false respond with extremely short route. In wormhole attack, malicious node obtains data packet at one location in the network and channels them to another malicious node. Rushing Attacks are essentially against the on-demand routing protocols. These types of attacks threaten the path discovery process.
1.3.1.6 Attacks at transport layer

Attacker in Session Hijacking acquires the benefit to develop the insecure session after its initial setup. In this attack, the attacker spoofs the injured party node’s IP address, discovers the right sequence number i.e. estimated by the target and then initiates various DoS attacks. In Session Hijacking, the malicious node attempts to gather secure data like passwords, secret keys, logon names and other information from nodes. Session Hijacking attacks are also known as address attack and affect the transmission protocol like Transmission Control Protocol (TCP).

Figure 1.5 Session Hijacking

Figure 1.5 describes the Session Hijacking. The TCP-acknowledgement (ACK) tempest trouble arises when malicious node initiates a TCP session hijacking attack. The attacker X adds session data, and node 1 forwards acknowledgement packet to node 2. Packet does not hold any sequence number that node 2 is expecting. The attack is seen when node 2 receives the packet and tries to resynchronize the TCP session with node 1.
This process is repeated over and over that leads to ACK tempest. Application layer protocols are also vulnerable to many DoS attacks.

1.3.1.7 Attacks at data link layer

Selfish misbehavior of node straightforwardly changes the self-performance of nodes and does not obstruct the action of the network. The main objective of malicious node is to interrupt regular operation of routing protocol. The collision of such attack is enlarged when the communication takes place between adjacent nodes.

The significant attack at data link layer is the DoS attack. These types of threats created a malicious action with the support of node co-operation that forms harsh security risks. In the presence of node cooperation, it is very complex to identify the cooperation routing. The cooperation route emerges like a usual route but guides to rigorous problems. For example, node cooperation involves in the communication but drops some packets resulting in degradation of service quality being offered by network. A detailed overview of DoS attack is described in the following section.

1.3.2 Denial of Service Attack

A DoS attack is an occurrence that reduces or removes a network's power to perform its expected function. The hardware failures, software errors, resource collapses, environmental constraints, or any complex communications between these factors cause DoS. The DoS attacks on the link layer and network layer are summarized below:

1.3.2.1 DoS attacks on the link layer

IEEE 802.11 Medium Access Control (MAC) protocol is used as the link layer protocol for MANET. IEEE 802.11 MAC is vulnerable to DoS
attacks and utilizes its binary exponential back-off scheme. Because a successful broadcast results in a smaller conflict window, a constantly broadcasting node always confine the channel and causes other nodes to back off continually. A customized back-off scheme solves DoS attack by offering the back-off timer from the receiver end. Additionally, the Network Allocation Vector (NAV) field in the Request to Send/Clear to Send (RTS/CTS) frames represents another vulnerability to DoS attacks. Since a malicious node is conscious of the time interval of the current transmission in its neighborhood, it forwards few bits to interrupt the current link-layer frames with an insignificant energy cost.

1.3.2.2 DoS attacks on the network layer

DoS attacks on network layer normally categorized into three, namely, resource deficiency, routing interference and forwarding denial.

In a resource deficiency attack, malicious nodes add additional control or data packets into the network. For example, a malicious node keeps forwarding different messages to its adjacent node. Since the sequence numbers or fake target address is changed each time, an attacker's neighbors are unable to distinguish the messages as fake ones or new requests. If the malicious node forwards these fake messages at a high speed, its neighbors spends much resources, like bandwidth, CPU sequences and battery power, to face fake messages.

A typical example of this attack is Blackhole in which an attacker initiating the Blackhole Attack could direct all packets to some destination and then discard them. Another type of routing interruption attack is so called wormhole. To begin the wormhole attack, two malicious nodes N1 and N2 cooperate with each other via a private network connection, such that N1 forwards the packets received from other nodes directly to N2 through the
wormhole. N2 rebroadcast the received packets to another area of the network.

1.3.3 Channel Aware Detection

The WMN is a multi-hop network which depends on mesh routers to send the packets to the destination. A successful association among routers is the basis for a trustworthy network. Cryptography solutions are utilized to defend the mesh routers from most of the routing protocol attacks like selective forwarding, Gray hole, Blackhole and Wormhole Attacks. But, if the routers are liberal, the attacker is allowed to access the public/private keys of the liberal routers and then crack through the cryptographic system. Therefore, to attain absolute security in a network, it is ideal to use cryptographic solutions as a first line of protection and non-cryptographic solutions as a second line of protection.

Most of the existing studies on selective forwarding attacks concentrate on attack detection under the statement of an error-free wireless channel. An additional realistic and demand scenario that packet falling is due to Grayhole Attacks or normal loss events such as medium access crash or worst channel quality. Specifically, a Channel Aware Detection (CAD) algorithm is developed to effectively detecting the selective forwarding attackers by sorting out the standard channel losses.

The CAD algorithm is based on two measures, namely, channel evaluation and traffic monitoring. The measure of channel evaluation is to approximate the normal loss rate due to worst channel quality or medium access crash. The measure of traffic monitoring is to monitor the definite loss rate. CAD involves four-fold contributions:
Channel evaluation is incorporated with traffic monitoring to attain channel-aware detection of Grayhole Attack. The Grayhole detection effectively detects selective forwarding misbehavior unseen in the usual loss events due to worst channel quality or medium access crash.

In CAD, upstream and downstream traffic monitoring is integrated to obtain a flexible detection method. In addition to Grayhole Attack, the CAD also identifies restricted transmit-power attack, on-off attack and dreadful opening attack.

The CAD algorithm is inefficient when multiple malicious nodes act in collision. The CAD is unable to provide useful information about the authenticated and unauthenticated nodes in the network. The more unauthenticated nodes involved in the communication, instead of authenticated node, lead to unsecure communication. Additionally, the unauthenticated nodes are not prevented to involve in the network communication.

1.4 NODE CLUSTERING IN MANET

Cluster-based routing is a solution to address node’s diversity and to control the quantity of routing information that broadcasts inside the network. The purpose of clustering is to collect the network nodes into a number of coinciding clusters. Clustering makes promising ranked routing in which routes are traced between clusters instead of nodes. This increases the routes duration, thus reducing the amount of routing control overhead. In the cluster formation, the node coordinating the cluster activities is called as cluster head (CH).

For a clustered network, the network is grouped into clusters with one cluster head per cluster. Essentially, the clustered network transfers a
thick network to a thin one that involves cluster heads and some gateways. The broadcast protocol uses a separation of nodes, called forward node set, to communicate a broadcast packet in a clustered network. Only a cluster head determines its forward node set to envelop other cluster heads within its neighborhood and within the exposure area. A non-cluster head node immediately communicates the broadcast packet if it is chosen as a forward node. The forward node set is determined by cluster heads. All the cluster heads in the network are connected to each other. Consequently, a broadcast packet is delivered to the total network ultimately. Cluster heads are chosen through a selection process. A cluster head straightforwardly connects to all the nodes in the cluster. Other members in the cluster are non-cluster head nodes. The clustered network is produced by the lowest-ID cluster algorithm.

Figure 1.6 shows the effect of applying clustering in a network with 10 nodes. The cluster formation involves the connection of nodes into clusters groups. The node 2 acts as attacker in interrupting the communication. Other
nodes are protected to deliver the packets. The pure clustered network does not sustain position of maintenance. But it will be possible to localize if a little different cluster structure strategy is applied. Once a cluster is shaped, a non-cluster head node, which are newly entered in the cluster challenges the current cluster head.

Figure 1.7 describes the cluster graph and adjacent cluster graph of the sample network as shown in Figure 1.6. If a cluster head travels into an existing cluster, the cluster head that has the higher ID will stop its role of cluster head. If a cluster head travels out of a cluster, the left non-cluster head nodes in this cluster will compute their new clusters. A node that has cluster head adjacent obtains the neighboring cluster head with the lowest ID as its new cluster head and connects in that cluster. For nodes with no cluster head adjacent, the cluster formation procedure is applied among those nodes to structure new clusters. Thus, the clusters mobility is adaptive and alters a cluster, controlled in a limited area. Thus, transmission of packet in a clustered MANET using the forward node set is able to efficiently convey the packet.

Figure 1.7 explicates the cluster graph formed in a cluster. Each cluster has its own nodes with its edges. In this the vertices refers the nodes and the edges refers the connection between the nodes. The cluster graph in Figure 1.7(a) is with good quality and dense, because all the nodes are close to each other. The cluster graph in Figure 1.7(b) is almost similar to Figure 1.7(a) with same number of nodes and edges; whereas most of the vertices are outside the cluster. The cluster graph in Figure 1.7(c) has very few connections with other nodes but lacks in internal density and hence it is not a good cluster.
1.5 PURPOSE OF THE STUDY

Security is the main challenge faced in protecting wireless communications especially in MANET. The security test reveals that many techniques provide strong privacy protection but wormhole attacks are difficult to prevent. These existing techniques support a secure shared key based on-demand for packet data but offers an unsecure communication.

In MANET topology, crisis occurs mainly due to the attacks that affect the network. A dynamic method is required to employ topology control algorithms in MANET to avoid topology problems. Network topology among MANET varies due to mobility and thus, it unable to maintain the network connectivity.

The cryptographic protocols concentrates on providing secure communication but also affected by diverse attacks. The attacks present in the networks and the root of that attack is also avoided. But the drawback is that the attacks on encrypted protocol are unavoidable. For the attacks like Blackhole, Grayhole, Wormhole and Rushing attack, no algorithms is launched still now and above all attack problems are still faced by MANET.

The possible solution to attacks is by performing node clustering and deriving cluster heads. Cluster heads are combined and used to avoid
attacks but at the same time a key security is required to solve the attacks. The data transmission through the cluster nodes is efficient regarding energy but the congestion at the cluster heads raises. Key security along with clustering is necessary to avoid loss of packets or prevention from attacks.

A fully-distributed identification based multiple secrets key management for a secure communication using a protocol of group key management is proposed. But the disadvantages in IMKM are bandwidth usage is limited for a secure communication and consumes several rounds to recognize the secure channel. But the main drawback is that the communication between the nodes and the clustering processes are inefficient.

Misbehavior of nodes also causes problems in MANET. Routing misbehavior is also a difficult problem in providing security during transmission as the nodes drops the packets before transmitting. The packet dropping problem is avoided by using reputation based method which mainly avoid when an attacker resets a poor reputation by rejoining the system with a new identity (whitewashing attacks). The existence of delay problems keeps on increasing due to addition of nodes resulting in inefficient packet delivery to destination node in given period of time.

Nodes in the networks are scattered reducing the efficiency in communication. Cluster-based routing is a resolution to solve nodes diversity and to control the amount of routing information that propagates inside the MANET. The nodes in the network are clustered for secure ad hoc communication. A secure key model is provided for ad hoc network with efficient node clustering based on reputation and ranking model. An improvement in the reliability of the network is required to provide a fast transmission. The reputation technique is necessary to find the unauthenticated nodes involved in the communication.
In addition, the reputation and ranking models are employed to detect the misbehavior, and selfish nodes within the network communication. Determination of unauthenticated nodes is essential to avoid the adversary acts performing in MANET. The nodes co-operation is necessary to perform clustering and in recognizing cluster head. The cluster head formation helps in ranking.

A secure transmission between the source and destination plays a vital role in the MANET communication. To provide the security in communication, a key is incorporated with the information. To decide the secret keys in authenticating group, an authenticated group key agreement protocol is essential. There are several security issues generated by the selfish nodes in MANET and to improve the cooperativeness among the mobile nodes in MANET, it is necessary to ensure the node cooperation among the nodes.

1.6 ORGANIZATION OF THE THESIS

Chapter 1 provides a brief discussion on the security of MANET with infrastructure-less network with different attacks on each layer of the network, and clustering of nodes by providing efficient node cooperation between the nodes. Additionally the performance and organization of nodes within the network is deeply discussed.

Chapter 2 reviews the previous research work on MANET security, infrastructure-less network that is relevant for the present thesis. In addition, reviews related to node clustering in infrastructure-less environment for secure communication, a secure key model for efficient node clustering based on reputation and ranking, a hybrid approaches for node co-operation based clustering in MANET using the closeness between the nodes are also interpreted from the research works.
Chapter 3 provides an overview of various security related issues while constructing the network. A secure key model (SKM) with reputation and ranking system is proposed as a first research work. This model dynamically evaluates the authentication of neighboring nodes and selects the trusty nodes in the cluster to support efficient transmission of data. The nodes are clustered based on the reputation table. The model provides secure successful communication between the nodes in the network without any loss of data. The design of node clustering proves the usefulness and feasibility of secure key model approach.

Chapter 4 presents a detailed description of a secure communication framework between the nodes in the network without any loss of data and the needs for node cooperation based clustering in MANET. The second research work namely hybrid approach for node cooperation based clustering (HANCC) is efficiently designed for enhancing a secure communication over MANET by improving the node cooperation among nodes by monitoring the behavior and activity of nodes along with the weightage of node cooperation. The work evaluates the performance results of the secure communication framework for hybrid approach using node cooperation based clustering.

Chapter 5 describes a mechanism to avoid the misbehavior nodes from replacing the security associations with unidentified nodes. The third research work ENCS is designed for enhancing cooperation of nodes and secures communication by adopting the closeness technique.

Chapter 6 focuses on end-to-end route awareness and represents the end-to-end route quality in terms of path lifetimes. The fourth research work Routing Aware Packet Reserving (RAPR) framework is developed in MANET that takes into account both the clogging state and the end-to-end throughput maintenance. RAPR is complimentary system to packet reserve
that utilizes only local routing information. RAPR framework local routing information contains the node clustering, cooperation and high security level, which provides the maximal throughput among the contending flows. Finally, Chapter 7 provides the concluding remarks and suggestions for future work.