Chapter I

INTRODUCTION

1.1 Mobile Ad hoc Networks (MANET)

1.2 Proposed Methodology

1.3 Performance Evaluations and Analysis of Results

1.4 Objective of the Thesis

1.5 Chapter Summary
I. INTRODUCTION

As the importance of computers in our daily life increases, it also sets new demands for connectivity. Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting the Internet, reading and sending E-mail messages, changing information in a meeting and so on. There are solutions to these needs, one being wireless local area network that is based on IEEE 802.11 [17] standard. However, there is increasing need for connectivity in situations where there is no base station (i.e. backbone connection) available (for example two or more PDAs need to be connected), there emerges Ad hoc networks.

In Latin, Ad hoc means "for this”, further meaning "for this purpose only”. This is a good and emblematic description of the idea why Ad hoc networks are needed. They can be set up anywhere without any need for external infrastructure (like wires or base stations). They are often mobile and termed as Mobile Ad hoc NETworks (MANET). MANET [37,56,57,62,and 73] is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

The popular IEEE 802.11 "Wi-Fi" protocol is capable of providing Ad hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile Ad hoc Networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet.

Mobile Ad hoc Networks can turn the dream of getting connected "anywhere at any time" into reality[44]. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, imagine a group of people with laptops, in a business meeting at a place where no
network services is present. In such a situation their machines can form an Ad hoc network. This is one of the many examples where these networks may possibly be the best ones to cater the needs of dynamic nature.

1.1 Mobile Ad hoc Networks (MANET)

In recent years, Mobile Ad hoc Network (MANET) has received much attention due to self-design, self-maintenance, self-organized and cooperative environments. In MANET, all the nodes are mobile nodes and the topology will change rapidly without any predefined infrastructure. Participating nodes can be laptops, palmtops, cell phones etc. Each device can act both as a host and a router to forward packets for other nodes. The structure of the MANET [37] shown in Figure 1.1.

![Figure 1.1. Structure of MANET](image)

Here, the mobile devices such as PDAs and laptops are used to route the data packets. In MANET, all the nodes actively discover the topology and the messages are transmitted to the destination over multiple-hop. It uses the wireless channel and asynchronous data transmission through the multiple-hop. The vital characteristics of MANETs are lack of infrastructure, dynamic topology, multi-hop communication and distributed coordination among all the nodes.
[3, 37, 84 and 85]. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or to deploy an infrastructure which is cost effective on a temporary basis.

Some applications of Ad hoc networks include students using laptop to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information about situation awareness in a battlefield, and emerging disaster relief after an earthquake or hurricane. Ad hoc networks are created, for example, when a group of people come together and use wireless communication for some computer based collaborative activities; this is also referred to as spontaneous networking [62]. The nodes are free to move randomly and organize themselves arbitrarily, thus the wireless network topology may change rapidly and unpredictably. Such a network may operate in standalone fashion as shown in Figure 1.2.

This wireless channel can be accessible for both legitimate users and malicious users. In such an environment, there is no guarantee that a route between the two nodes will be free for the malicious users, which will not abide by
the employed protocol. The malicious users can attempt to harm the normal network operations.

1.1.1 Constraints and Challenges in Ad hoc Networks

The principal constraints and challenges induced by the Ad hoc environment are as follows [84].

- **Autonomous**- No centralized administration entity is available to manage the operation of the different mobile nodes.

- **Dynamic topology**- Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

- **Device discovery**- Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate, automatic optimal route selection.

- **Bandwidth optimization**- Wireless links have significantly lower capacity than the wired links.

- **Limited resources**- Mobile nodes rely on battery power, which is a scarce resource. Storage capacity and power are severely limited.

- **Scalability**- Scalability can be broadly defined as, whether the network is able to provide an acceptable level of service, even in the presence of a large number of nodes.

- **Limited physical security**- Mobility implies higher security risks such as peer-to-peer network architecture or a shared wireless medium accessible to both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.
- **Infrastructure-less and self operated**- Self healing feature demands MANET should realign itself to blanket any node moving out of its range.

- **Poor Transmission Quality**- This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

- **Ad hoc addressing**- Challenges in standard addressing scheme to be implemented.

- **Network configuration**- The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links.

- **Topology maintenance**- Updating information of dynamic links among nodes in MANET.

Despite the many design constraints, Mobile Ad hoc Networks offer numerous advantages. First of all, this type of network is highly suited for use in situations where a fixed infrastructure is not available, not trusted, too expensive or unreliable. Because of their self-creating, self-organizing and self-administering capabilities, Ad hoc networks can be rapidly deployed with minimum user intervention.

There is no need for detailed planning of base station installation or wiring. Moreover, Ad hoc networks need not operate in a stand-alone fashion, but can be attached to the Internet, thereby integrating many different devices and making their services available to other users. Furthermore, capacity, range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity.
1.1.2 Applications of Mobile Ad hoc Networks

As a consequence, Mobile Ad hoc Networks are expected to become an important part of the future 4G architecture, which aims to provide pervasive computer environments that support users in accomplishing their tasks, accessing information and communicating anytime, anywhere and from any device.

An overview of present and future MANET applications with its possible scenarios and services are as follows [23].

- **Tactical networks**
  - Military communication and operations.
  - Automated battlefields.

- **Emergency services**
  - Search, rescue operations and disaster recovery.
  - Policing and fire fighting.
  - Supporting doctors and nurses in hospitals.

- **Commercial and civilian environments**
  - E-commerce: electronic payments anytime, anywhere.
  - Business: Dynamic database access, mobile offices.
  - Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks.
  - Sports stadiums, trade fairs, shopping malls.
  - Networks of visitors at airports.

- **Home and enterprise networking**
  - Home/office wireless networking.
• Conferences, meeting rooms.

• Personal area networks (PAN), Personal networks (PN).

• Education
  - Universities and campus settings.
  - Virtual classrooms.
  - Ad hoc communications during meetings or lectures.

• Entertainment
  - Multi-user games.
  - Wireless P2P networking.
  - Outdoor Internet access.
  - Robotic pets.
  - Theme parks.

• Sensor networks
  - Home applications: smart sensors and actuators embedded in consumer electronics.
  - Body area networks (BAN).
  - Data tracking of environmental conditions, animal movements, chemical/biological detection.

• Context aware services
  - Follow-on services: call-forwarding, mobile workspace.
  - Information services: location specific services, time dependent services.

• Coverage extension
Ad hoc networks have applications in two major fields: military and commercial environments as shown in Figure 1.3.

![Figure 1.3. Examples of Mobile Ad hoc Networks](image)

1.1.3 Communication in MANETs

As these Mobile Ad hoc Networks are increasingly being considered for more and more complex applications, the various Quality of Service (QoS) attributes[6,18 and 68], for these applications must also be satisfied as a set of pre-determined service requirements. In addition, due to the increasing use of the Ad hoc networks for military/police use, and commercial applications, it is being envisioned to be supported on these type of networks and necessary to communicate among groups securely[46].

Routing is one of the primary functions for communicating between two nodes that are not in direct range with each other. The routing protocols[71] plays a vital role to make some critical decisions such as the optimal route from the source to the destination, because the mobile nodes operate on battery power. In fact, Ad hoc networks have the capability of making communications even
between two nodes that are not in direct range with each other. It is even possible to exchange the packets between these nodes and forwarded by intermediate nodes.

The development of efficient routing protocols is a nontrivial and a challenging task because of the specific characteristics of a MANET environment:

- Due to node movements, the network topology may change randomly and rapidly at unpredicted times.
- The available bandwidth is limited and can vary due to fading, noise, interference, etc.
- Most mobile devices are battery powered; therefore energy consumption plays an important role.
- It is necessary to transfer the data with the minimal delay so as to consume less power.
- Quality of Service support is also needed reducing the packet drop ratio and increasing the key delivery ratio.

Unfortunately, most of the routing protocols suffer from a number of shortcomings:

i. Security problem in communications.

ii. Scalability problems with growing network size.

iii. Their performance is only optimal under certain network conditions such as mobility.

iv. Unreliability in drop of packets.

With the increasing number of applications to harness the advantages of Ad hoc Networks, more concerns arise for security issues in MANETs. Natures of
Ad hoc networks make them vulnerable to security attacks based on the following reasons.

- **Open medium**: Eavesdropping is easier than in wired network.
- **Dynamically changing network topology**: Mobile nodes come in and go out of network, thereby allowing any malicious node to join the network without being detected.
- Attacks from compromised entities or stolen devices.
- **Cooperative Algorithms**: The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of network security.
- **Lack of Centralized Monitoring**: Absence of any centralized infrastructure prohibits any monitoring agent in the system.

### 1.1.4 Security issues in MANETs

Security is hard in application areas, such as protecting trade secrets, confidential chat, Government use, pay-per-view and online auctions which need group communication[65]. In an open group membership, anyone can view or insert data into group and everyone gets same packets. There will be no individualization or customization. All the senders need not be members and thus it is not possible to have control over information that goes to the group.

Multicasting is a fundamental communication paradigm for group-oriented communications such as video conferencing, discussion forums, frequent stock updates, video on demand (VoD), pay per view programs, and advertising.

The combination of an Ad hoc environment with multicast services [21,39,40 and 45] induces new challenges towards the security infrastructure to enable acceptance and wide deployment of multicast communication. Indeed,
several sensitive applications based on multicast communications have to be secured within Ad hoc environments. For example military applications such as group communication in a battlefield and public security operations involving fire brigades and policemen have to be secured.

The characteristics of Mobile Ad hoc Networks, pose numerous challenges in achieving conventional security goals.

Security goals

To prevent attacks and eavesdropping, basic security services such as authentication, data integrity, group confidentiality and non repudiation are necessary for collaborative applications.[46]

- **Authentication**: Ensures that only authorized users are allowed to be assured of the others identity.

- **Data Integrity**: Ensures that the data has not been altered during transmission.

- **Group Confidentiality**: Ensures that transmitted information can only be accessed by the intended receivers of the group.

- **Non-repudiation**: Ensures that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data.

- **Availability**: Ensures that the intended network services are available to the intended parties when required.

Group confidentiality [20] is the most important service for military and disaster applications in Ad hoc environment. Group confidentiality requires that only valid users could decrypt the multicast data. These security services can be facilitated if group members share a common secret, which in turn makes
multicast key management [36,69 and 77] a fundamental challenge in designing secure multicast and reliable group communication systems.

To ensure group confidentiality during multicast session, most of these security services rely generally on encryption using Traffic Encryption Keys (TEKs) and re-encryption is using Key Encryption Keys (KEKs) [43]. The Key management includes creating, distributing and updating the keys then it constitutes a basic block for secure multicast communication applications.

1.1.5 Key Management Requirements

In a secure multicast communication, each member holds a key to encrypt and decrypt the multicast data. When a member joins and leaves a group, the key has to be updated and distributed to all group members in order to meet the multicast key management requirements. Efficient key management protocols should be taken into consideration for miscellaneous requirements. Figure 1.4 summarizes these requirements[20].

![Multicast Key Management Diagram]

**Figure 1.4 Multicast Key Management Requirements**
Security requirements:

i. **Forward secrecy**: In this case, users who have left the group should not have access to any future key. This ensures that a member cannot decrypt data after they leave the group.

ii. **Backward secrecy**: A new user who joins the session should not have access to any old key. This ensures that a member cannot decrypt data sent before they join the group.

iii. **Non-group confidentiality**: Users that are never part of the group should not have access to any key that can decrypt any multicast data sent to the group.

iv. **Collusion freedom**: Any set of fraudulent users should not be able to deduce the currently used key.

The process of updating the keys and distributing them to the group members is called rekeying operation. A critical problem with any rekey technique is scalability. The rekey process should be done after each membership change.

If the membership changes are frequent, key management will require a large number of key exchanges per unit time in order to maintain both forward and backward secretcies. The number of TEK update messages in the case of frequent join and leave operations affects several QoS characteristics as follows:

**Reliability:**

**Packet Drop Ratio**: The number of TEK update messages in the case of frequent join and leave operations induces high packet drop ratio and reduces key delivery ratio which makes it unreliable.
Quality of service requirements:

i. **“1 affects n”**: If a single membership changes in the group, it affects all the other group members. This happens typically when a single membership change occurs all group members commit to a new TEK.

ii. **Energy consumption**: This induces minimization in the number of transmissions in forwarding messages to all the group members.

iii. **End to end delay**: Many applications that are built over the multicast services are sensitive to average delay in key delivery. Therefore, any key distribution scheme should take this into consideration and hence minimize the impact of key distribution in the delay of key delivery.

iv. **Key Delivery Ratio**: This induces number of successful key transmission to all group members without any loss of packet during multicast key distribution.

Thus a QoS based secure multicast key distribution in mobile Ad hoc environment should focus on security, reliability and QoS characteristics.

To overcome these problems, several approaches propose a multicast group clustering [8,9,11 and 28]. Clustering is dividing the multicast group into several sub-groups. Local Controller (LC) manages each subgroup, which is responsible for local key management within the cluster.

Thus, after Join or Leave procedures, only members within the concerned cluster are affected by rekeying process, and the local dynamics of a cluster does not affect the other clusters of the group and hence it overcomes “1 affects n” phenomenon. Moreover, few solutions for multicast clustering such as dynamic clustering did consider the QoS requirements to achieve an efficient key distribution process in Ad hoc environments.
1.1.6 Existing Key Management Approaches

Key management approaches can be classified into three classes: centralized, distributed or decentralized. Figure 1.5 illustrates this classification.

![Diagram of Key Management Protocols]

Figure 1.5. Existing key management Approaches

In centralized approaches, a designated entity (e.g. the group leader or a key server) is responsible for calculation and distribution of the group key to all the participants. GKMP [33] achieves an excellent result for storage at the members. However, this result is achieved by providing no method for rekeying the group after a member has left, except re-creating the entire group which induces O(n) rekey message overhead where ‘n’ is the number of the remaining group members. Secure Lock [22] also achieves excellent results for storage and communication overheads on both, members and the key server. However, these results are achieved by increasing the computation overhead at the key server due to the Chinese Remainder calculations.

Distributed key agreement protocols do not rely on a group leader which has an advantage over those with a group leader because, without a leader, all
members are treated equally and if one or more members fail to complete the protocol, it will not affect the whole group. In the protocols with a group leader, a leader failure is fatal for creating the group key and the operation has to be restarted from scratch. The “1 affects n” phenomenon is not considered, because in distributed protocols all the members are contributors in the creation of the group key and hence all of them should commit to the new key whenever a membership change occurs in the group.

The decentralized approach divides the multicast group into subgroups or clusters, each sub-group is managed by an LC (Local Controller) responsible for security management of members and its subgroup. Two kinds of decentralized protocols are distinguished as static clustering and dynamic clustering.

In static clustering approach, the multicast group is initially divided into several subgroups. Each subgroup shares a local session key managed by LC. Example: IOLUS [55] belongs to the categories, which are more scalable than centralized protocol. Dynamic clustering approach aims to solve the “1 affects n” phenomenon. This approach starts a multicast session with centralized key management and divides the group dynamically. Example: AKMP [8], SAKM [19] belong to this approach and are dedicated to wired networks. Enhanced BAAL [11] and OMCT [12, 13,14,15] propose dynamic clustering scheme for multicast key distribution in Ad hoc networks.

OMCT (Optimized Multicast Cluster Tree) is a dynamic clustering scheme for multicast key distribution dedicated to operate in Ad hoc networks. This scheme optimizes energy consumption and latency for key delivery. Its main idea is to elect the local controllers of the created clusters. OMCT needs the geographical location information of all group members in the construction of the key distribution tree.
Once the clusters are created within the multicast group, the new LC becomes responsible for the local key management and distribution to their local members, and also for the maintenance of the strongly correlated cluster property. The election of local controllers is done according to the localization and GPS (Global Positioning System) information of the group members, which does not reflect the true connectivity between nodes.

Based on the literature reviewed, Optimized Multicast Cluster Tree (OMCT) is the efficient dynamic clustering approach for secure multicast distribution in Mobile Ad hoc Networks. To enhance its efficiency, it is necessary to overcome the above criteria, as OMCT needs geographical location information in the construction of key distribution tree by reflecting true connectivity between nodes.

To overcome the above limitations another method called Optimized Multicast Cluster Tree with Multipoint Relays (OMCT with MPR)[13] is introduced which uses the information of Optimized Link State Routing Protocol (OLSR) to elect the LCs of the created clusters. OMCT with MPRs assumes that routing control messages have been exchanged before the key distribution. It does not acknowledge the transmission and results in retransmission which consumes more energy and unreliable key distribution due to high packet drop ratio for Mobile Ad hoc Networks.

As the nodes are dynamic in nature, ensuring effective routing is one of the major challenge for MANET. Destination Sequenced Distance Vector (DSDV)[86] is a table driven proactive routing protocol designed for Mobile Ad hoc Networks. This protocol maintains routing table as a permanent storage. Routes are maintained through periodical and event trigger exchanges the routing table as the nodes join and leave. Route selection is based on optimization of distance vector. It avoids routing loops and each node has a unique sequence number which updates periodically. It is mainly used for intra cluster routing. It
allows fast reaction to topology changes. Improvement of DSDV (IDSDV) [49], improves the delivery ratio of Destination-sequenced Distance Vector (DSDV) routing protocol in Mobile Ad hoc Networks with high mobility. It uses message exchange scheme for its invalid route reconstruction and has multicast connectivity between nodes.

In Ad hoc networks, the nodes move to different location, thus creating a different network topology. Almost all well-known routing protocols are shown to perform poorly for a network where the topology is changing at random. With the realization of importance of node mobility in the routing process of Ad hoc networks, quite a lot amount of work has been done in mobility characterization of the mobile nodes. This mobility characterization research is attempting to quantify the randomness in the mobility of the nodes [52, 53]. Most of the research in this area of mobility characterization has however been towards mobility characterization of individual nodes [48].

The IMPORTANT framework [7] characterizes movement based on spatial dependence, relative speed, and other factors and illustrates how these metrics impact unicast routing performance. In [38], the authors have shown that the mobility model used can significantly impact the performance of Ad hoc routing protocols, including the packet delivery ratio, the control overhead and the data packet delay. In many multicast interactions, due to its frequent membership dynamism, it causes node failure, link failure, power failure. Node failure may cause faults in communication and delay in multicast transmission.

**Limitations of OMCT**

The major limitations of existing OMCT multicast key distribution approach is as follows.

- Needs geographical location information
• Election of local controllers is based on GPS

• Does not reflect true connectivity between nodes.

• It does not acknowledge the transmission
  
  o Results in retransmission
    ▪ Consumes more energy and delay
  
  o Results in unreliable key distribution
    ▪ High packet drop ratio

Moreover, few solutions for multicast clustering such as dynamic clustering did consider the QoS requirements to achieve an efficient key distribution process in Ad hoc environments.

The primary focus of this work are as follows

• To select a suitable environment for real time applications.

• To provide secure communication between the mobile nodes.

• To ensure efficient communication mechanism for group oriented applications.

• To select appropriate key management approaches.

• To achieve an efficient routing protocol to reduce overhead.

• To adapt with different mobility models.

• To tolerate the faults due to node failure.

1.2 Proposed Methodology

In order to assure secure multicast key distribution, a new approach of dynamic clustering scheme is proposed. The main objective of this approach is to divide the multicast group into clusters and to elect the local controllers for
efficient secure multicast key distribution in Mobile Ad hoc Networks. This approach also aims in improving the performance in terms of QoS characteristics as metrics. The methodology is proposed in order to assure reliable QoS based secure multicast key distribution for Mobile Ad hoc Networks. The specific contributions are structured in five phases.

1. **Phase I : Integration of OMCT with DSDV**
   - Makes easy election of LC
   - Improves key delivery ratio

2. **Phase II : Enhancement of OMCT with DSDV**
   - Reduces end to end delay
   - Consumes less energy

3. **Phase III : Cluster Based Multicast Tree with MDSDV**
   - Improves reliability
   - Reduces packet drop ratio

4. **Phase IV : Adaptability of CBMT with mobility aware MDSDV**
   - For various Mobility models

5. **Phase V : Efficient CBMT**
   - Fault tolerance

**1.2.1 Integration of OMCT with DSDV**

The main idea of this phase is to integrate OMCT clustering algorithm with DSDV routing protocol to elect the local controllers of the created clusters. The principle of this clustering scheme is to start with the group source, to collect its 1-hop neighbors by DSDV, and elect local controllers, which are group members
and which have child group members. The selected nodes will be elected as local controllers.

Thus this phase provides a simple, dynamic and scalable approach. It makes fast and easy election of the local controllers. It also increases the key delivery ratio in multicast transmission. For multicast clustering, main issues are energy consumption and end to end delay for multicast key distribution. The next phase deals with overcoming the issue of energy consumption and end to end delay during secure multicast key distribution.

1.2.2 Enhancement of OMCT with DSDV

The Integration of OMCT with DSDV approach is further enhanced by sending acknowledgement for each transmission using the DSDV routing protocol in order to reduce retransmission. Thus in this phase, it reduces the end to end delay and consumes less energy which makes this approach as energy efficient. Frequent membership dynamism induces high packet drop ratio and reduces key delivery ratio. This makes the approach unreliable. The next phase proposes a new version of OMCT as Cluster Based Multicast Tree (CBMT) to make the approach reliable.

1.2.3 Cluster Based Multicast Tree with MDSDV

Cluster based multicast tree (CBMT) with MDSDV algorithm is a new reliable version of OMCT with DSDV for secure multicast key distribution in Mobile Ad hoc Networks. It includes key tree engine and forms tree structure based on authentication. Multicast version of DSDV routing protocol is used to form multicast tree among the group members.

Thus this phase proposes a reliable dynamic clustering approach by reducing the packet drop ratio and increasing the key delivery ratio. In many multicast interactions, due to its frequent node mobility, new members can join
and current members can leave at a time. The moving behavior of each member in
the MANET should be realistic. The pattern of movement of members is classified
into different mobility models and each one has its own distinct features. It is a
crucial part in the performance of MANET. The next phase deals with adaptability
of the proposed approach with different mobility models.

1.2.4 Adaptability of CBMT with Mobility Aware MDSDV

The frequent mobility of members and limited communication resources
make routing in MANET very difficult. Mobility causes frequent topology
changes and may break existing paths. A routing protocol should quickly adapt to
the topology changes and efficiently search for new paths. To adapt to the above
scenario, Mobility Aware Multicast version of Destination Sequenced Distance
Vector routing protocol is used. It allows fast reaction to topology changes and is
specially designed for MANET.

This phase proposes the adaptability of CBMT with mobility aware
MDSDV under various mobility models in frequent membership dynamism with
varying number of nodes and speed of nodes. It presents the importance of
mobility patterns and illustrates the adaptability of CBMT with MDSDV for
different mobility models. More frequent membership dynamism causes node
failure, link failure, power failure which leads to time delay in multicast
transmission. The next phase deals with failure of nodes and proposes an efficient
approach for secure multicast communication.

1.2.5 Efficient CBMT

More frequent membership dynamism causes node failure, link failure and
power failure which leads to time delay in multicast transmission. Node fails due
to movement of node out of coverage area. Failure of node is easily identified by
reachability information of MDSDV. When an LC fails, it leads to clusterization.
Thus this phase proposes an efficient CBMT with Mobility aware MDSDV which tolerates the fault due to node failure.

The proposed approach is to achieve secure multicast communication for Mobile Ad hoc Networks. This approach uses Mobility Aware Multicast version of DSDV routing protocol to maintain routing table periodically. It forms multicast tree among the group members. Each node can determine their present physical location. It quickly adapts to the topology changes. It is used to discover alternate route for failure of existing route. It also sends acknowledgement for each transmission in order to reduce the retransmission. Thus the approach of CBMT using Mobility Aware MDSDV tends to have multicast connectivity between the nodes.

**Specific Advantages of Proposed Methodology:**

Some of the specific advantages of proposed methodology over the existing OMCT approach are as follows.

- Simple, dynamic and scalable approach
- Makes this approach energy efficient
- Reliable approach
- Adaptability of CBMT with MDSDV for different mobility models.
- Reduced end to end delay
- Less energy consumption
- Increased key delivery ratio
- Reduced Packet Drop ratio
- Failure of node is easily identified by reachability information of MDSDV
• Tolerates the Fault

1.3 Performance Evaluation and Analysis of Results

The performance of CBMT for multicast key distribution is evaluated in terms of QoS characteristics as metrics and simulated using NS2 version ns-allinone-2.33[79,87 and 88].

1.3.1 Performance Metrics

The QoS metrics are end to end delay in key distribution, energy consumption, key delivery ratio and packet drop ratio of multicast key distribution.

• **End to end Delay** The average latency or end to end delay of key transmission from the source to the receivers. This metric allows evaluating the average delay to forward a key from a LC to its cluster members.

• **Energy Consumption** is defined as the sum of units required to the key transmission throughout the duration of simulation.

• **Key Delivery Ratio** is defined as the number of received keys divided by number of sent keys. This metric allows evaluating the reliability of the protocol in terms of key delivery ratio in key transmission from the source to the group members.

• **Packet Drop Ratio** is obtained as dividing the number of packets received at the destination by the number of packets sent to destination. This metric allows in evaluating the reliability of the protocol in terms of packet Drop ratio in key transmission from the source to the group members.
1.3.2 Simulation Environment

The proposed CBMT using MDSDV is simulated under Linux Fedora, using the network simulator NS2 version ns-allinone-2.33[87,88]. This simulation environment is defined by the following parameters as shown in Table 1.1.

<table>
<thead>
<tr>
<th>TABLE 1.1. SIMULATION METRICS OF CBMT</th>
</tr>
</thead>
<tbody>
<tr>
<td>The density of group members</td>
</tr>
<tr>
<td>Network surface</td>
</tr>
<tr>
<td>The maximal speed</td>
</tr>
<tr>
<td>The pause time</td>
</tr>
<tr>
<td>The simulation duration</td>
</tr>
<tr>
<td>Physical/Mac layer</td>
</tr>
<tr>
<td>Mobility model</td>
</tr>
<tr>
<td>Routing protocol</td>
</tr>
</tbody>
</table>

The simulations are conducted and the performance is compared for CBMT and OMCT with varying density of cluster and network surface. This comparison is done in terms of end to end delay, energy consumption, key delivery ratio and packet drop ratio.

1.3.3 Analysis of Simulation Results

This section presents analysis of simulation results to compare the performance of proposed method CBMT with existing approach OMCT in varying density of nodes and network surface. The results of this simulation are presented in Table 1.2. in terms of QoS metrics as end to end delay, energy consumption, key delivery ratio and packet drop ratio.
### TABLE 1.2. SIMULATION RESULTS OF CBMT

<table>
<thead>
<tr>
<th>Surface</th>
<th>Nodes</th>
<th>End to end Delay (ms)</th>
<th>Energy (100 J)</th>
<th>Key Delivery Ratio (%)</th>
<th>Packet Drop Ratio (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CBMT</td>
<td>OMCT</td>
<td>CBMT</td>
<td>OMCT</td>
</tr>
<tr>
<td>1000</td>
<td>7</td>
<td>0.25</td>
<td>0.5</td>
<td>46</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>0.5</td>
<td>0.8</td>
<td>55</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>0.58</td>
<td>1.2</td>
<td>58</td>
<td>79</td>
</tr>
<tr>
<td>1500</td>
<td>7</td>
<td>0.2</td>
<td>0.3</td>
<td>47</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>0.4</td>
<td>0.64</td>
<td>50</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>0.6</td>
<td>0.89</td>
<td>58</td>
<td>86</td>
</tr>
<tr>
<td>2000</td>
<td>7</td>
<td>0.12</td>
<td>0.12</td>
<td>50</td>
<td>82</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>0.32</td>
<td>0.92</td>
<td>55</td>
<td>86</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>0.51</td>
<td>1.00</td>
<td>60</td>
<td>90</td>
</tr>
</tbody>
</table>

The Table 1.2. shows that the efficiency is improved by CBMT approach of multicast key distribution in terms of end to end delay in key distribution, energy consumption, key delivery ratio and packet drop ratio compared to the OMCT. The simulation results illustrate the comparison of CBMT with OMCT as shown in Figures 1.6a – 1.6d. Indeed, this approach of CBMT divides the multicast group with the effective connectivity between nodes. It allows fast reaction to topology changes.

The average delay of key delivery and the energy consumption are better with this approach of CBMT. This is due to the fact that it sends acknowledgement for each transmission in order to reduce the retransmission. Hence it reduces average end to end delay and energy consumption of multicast key distribution in CBMT compared to OMCT. It can be observed that CBMT gives better performance and achieves reliability in terms of key delivery ratio and
packet drop ratio compared to the OMCT algorithm under varying network conditions.

Figure 1.6a Average End to end Delay          Figure 1.6b Energy Consumption

Figure 1.6c Key Delivery Ratio   Figure 1.6d Packet Drop Ratio

Figure 1.6 CBMT vs OMCT
1.4 Objectives of the Thesis

This thesis proposes an efficient cluster-based multicast tree (CBMT) algorithm for secure multicast key distribution in Mobile Ad hoc Networks. Thus this new efficient CBMT approach is a dynamic clustering scheme with Mobility aware Multicast version of Destination Sequenced Distance Vector (MDSDV) routing protocol, which becomes easy to elect the local controllers of the clusters and updates periodically as the node joins and leaves the cluster.

The main objective of the thesis is to present a new approach of clustering algorithm for efficient multicast key distribution in mobile Ad hoc network by overcoming issues of multicast key management requirements. Extensive simulation results in NS2 shows the analysis of the efficient CBMT algorithm for multicast key distribution based on the performance of QoS characteristics. Hence, this proposed scheme overcomes “1 affects n” phenomenon, reduces average latency and energy consumption and achieves reliability, while exhibiting low packet drop ratio with high key delivery ratio, compared with the existing scheme under varying network conditions.

1.4.1 Organization of the Thesis

Organization of the thesis is structured as follows. Chapter 2 presents the related work of the existing approaches. The summary of different key management approaches are presented briefly with examples. Some of the well known routing protocols are discussed indicating the differences, advantages and disadvantages based on the desired routing properties of MANET. The previous enhancement of DSDV routing protocol are also discussed. The need for mobility pattern for dynamic network topology and its different mobility models for MANET are presented.
Chapter 3 explains the proposed methodology in five different phases. It introduces overall framework for secure multicast key distribution in MANET. The next coming chapters illustrates the significance of each phase of the proposed approach for secure multicast key distribution.

Chapter 4 integrates the existing OMCT clustering algorithm with DSDV routing protocol for easy election of local controllers. It presents the integrated algorithm of OMCT with DSDV. It improves key delivery ratio in multicast key distribution. Chapter 5 enhances the OMCT with DSDV as an energy efficient approach. It presents DSDV routing protocol based on energy efficiency. It consumes less energy and reduces end to end delay in multicast transmission.

Chapter 6 proposes a new clustering approach for secure multicast communication. An attempt is made to further reduce the energy and end to end delay and improve the reliability by reducing packet drop ratio and increasing key delivery ratio using an algorithm called Cluster Based Multicast Tree algorithm multicast key distribution. This algorithm uses MDSDV routing protocol for electing LCs.

Chapter 7 proposes the adaptability of CBMT with mobility aware MDSDV under various mobility models in frequent membership dynamism with varying number of nodes and speed of nodes. It presents the importance of mobility patterns and illustrates the adaptability of CBMT with MDSDV for different mobility models.

Chapter 8 further improves in efficiency as the number of node increases by using an approach of efficient Cluster Based Multicast Tree algorithm for secure multicast communication. The proposed approach further reduces the end to end delay and improves the fault tolerance as node increases for fault tolerant multicast communication. This algorithm uses Mobility aware Multicast version of DSDV routing protocol for electing LCs. The results are formed to be desirable and the
proposed method is efficient, reliable and more suitable for secure multicast communication dedicated to operate in MANET. Chapter 9 concludes the thesis with future directions.

1.5 Chapter Summary

Secure multicast communication is a significant requirement in emerging applications of Ad hoc environments like military or public emergency network applications. Membership dynamism is a major challenge based on QoS characteristics in providing complete security for Ad hoc networks. The most efficient Dynamic clustering algorithm OMCT address the critical problems like “1 affects n” phenomenon, energy and end to end delay issues of multicast key distribution. However the major QoS based challenges in Mobile Ad hoc Networks include high packet drop ratio which is not attempted in OMCT and hence it results in unreliable key distribution.

Therefore an attempt is made to further reduce the energy and end to end delay and improve the reliability by reducing packet drop ratio and increasing key delivery ratio using an algorithm called Cluster Based Multicast Tree algorithm for multicast key distribution. This algorithm uses Multicast version of DSDV routing protocol for electing LCs. The proposed CBMT is made to adapt with different mobility models for frequent membership dynamism. It is also made efficient by incorporating fault tolerance in the case of node failure by using the mobility aware multicast version DSDV.

The proposed efficient CBMT is tested and the entire experiments are conducted in a simulation environment using network simulator NS2. The results are formed to be desirable and the proposed method is efficient, reliable and more suitable for QoS based secure multicast key distribution dedicated to operate in Mobile Ad hoc Networks.