CHAPTER 5

DYNAMIC GROUP KEY MANAGEMENT SCHEME

5.1 Objective

Security of a network is an important factor in its construction. In the traditional wired networks and infrastructural wireless networks, central servers are available to provide security services for the users inside the network system. A network has to achieve security requirements in terms of authentication, non-repudiation, confidentiality, integrity and availability. The major factor in the implementation of the secured model is the key management system. The main goal of key management system is to manage the keys used by the members of the group and to protect from the unauthorized modifications, and disclosure.

There are many key management systems, in which group key optimal methodology is one of the important method. The purpose of the group key management system is to secure communication among group of nodes in MANET. The main purpose of this group key management system is to generate and distribute common secret for all group members. Various
group management schemes have been proposed and are in use (Abbas et al., 2013).

This Group key management involves creating and distributing the public key (Group Key) for all group members. A group is managed and organized by the Group Leader. Group Leader keeps track of group members and identifies node failure or leaving node and disseminates the information to other group members. In this research work, a key management scheme which ensures both forward and backward secrecy with less communication is proposed. The proposed work improved throughput, Reduced Network delay and computational cost.

Virtual infrastructure achieves reliable transmission in MANET. It is affected also by the security vulnerabilities on the routing protocols. Black hole attack is the major problem that affects the virtual infrastructure. It is a severe attack that can be easily employed against routing in mobile ad hoc networks. A black hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets.

Hence, in this proposed research work, in addition to the group key management, an algorithmic approach is used for analysing and improving the security of AODV. The aim of the research work is to ensure the security against black hole attack. The proposed solution is capable of detecting black hole node(s) in the MANET at the beginning and a solution to discover a safe route detects cooperative black hole attack.
5.2 Security Requirements

Wireless Network must be capable of keeping the information they are collecting private from eavesdropping. Use of encryption and cryptographic authentication costs both power and network bandwidth. This impacts application performance by decreasing the number of samples than can be extracted from a given network and the expected network lifetime. Effective Sample Rate It is the sample rate that wireless data can be taken at each individual wireless and communicated to a collection point in a data collection network. In-network processing can increase the effective sample rate.

The design requirements of the security model of the wireless network and wireless nodes are discussed in this section. The design requirements of the wireless networks are,

- **Security Vulnerabilities:** It is always advantageous to have the ability to deploy a network over a larger physical area. Multi-hop communication techniques can extend the coverage of the network; but increase the power consumption of the nodes, which may decrease the network lifetime. Additionally, they require a minimal node density, which may increase the deployment cost.

- **Energy efficiency / system lifetime:** The wireless nodes are battery operated, rendering energy a very scarce resource that must be wisely managed in order to extend the lifetime of the network.
• **Cost and ease of deployment:** For system deployments to be successful, the wireless nodes must configure themselves for any possible physical node placement. In the long term, the total cost of ownership for a system may have more to do with the maintenance cost than the initial deployment cost.

• **Response Time/Latency:** Many wireless applications require delay-guaranteed service. Protocols must ensure that sensed data are delivered to the user within a certain delay. The ability to have low response time conflicts with many of the techniques used to increase network lifetime.

• **Accuracy:** Obtaining accurate information is the primary objective; accuracy can be improved through joint detection and estimation.

• **Fault tolerance:** Robustness to wireless and link failures must be achieved through redundancy and collaborative processing and communication.

• **Scalability:** As a wireless network may contain thousands of nodes, scalability is a critical factor that guarantees that the network performance does not significantly degrade as the network size increases.

• **Transport capacity/throughput:** As most wireless data must be delivered to a single base station or fusion center, a critical area in the wireless network exists, whose wireless nodes must relay the
data generated by virtually all nodes in the network. Apparently, this area has a paramount influence on system lifetime, packet end-to-end delay, and scalability.

5.3 **Security Attacks**

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. For a large-scale wireless network, it is impractical to monitor and protect each individual wireless from physical or logical attack. Attackers may devise different types of security threats to make the WN system unstable. Here in this section, is presented a layer-based classification of WN security threats and also based on the capability of the attacker and defenses proposed in the literature.

5.3.1 **Outside and Inside Attacker**

Outside attacks are attacks from node which is not belongs to a WN; inside attacks occur when legitimate nodes of a WN behave in unintended or unauthorized ways. To overcome these attacks, require robustness against outsider attacks, resilience to insider attacks, graceful degradation with respect to node compromise and realistic levels of security.

5.3.2 **Passive versus Active attacks**

Passive attacks include eavesdropping on or monitoring packets exchanged within a WN; active attacks involve some modifications of the data steam or the creation of a false stream.
5.3.3 Attacks on Information in Transit

In a wireless network, wireless node monitors the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be attacked to provide wrong information to the base stations or sinks. The attacks are

- ** Interruption**- Communication link in wireless networks becomes lost or unavailable. This operation threatens service availability. The main purpose is to launch denial-of-service (DoS) attacks. From the layer-specific perspective, this is aimed at all layers.

- **Interception**- Wireless network has been compromised by an adversary where the attacker gains unauthorized access to wireless node or data in it. An Example of this type of attacks is node capture attacks. This threatens message confidentiality. The main purpose is to eavesdrop on the information carried in the messages. From the layer-specific perspective, this operation is usually aimed at the application layer.

- **Modification**- An unauthorized party not only accesses the data but also tampers with it. This threatens message integrity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer, because of the richer semantics of these layers.
• **Fabrication**: An adversary injects false data and compromises the trustworthiness of information. This threatens message authenticity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This operation can also facilitate DoS attacks, by flooding the network.

• **Replaying existing messages**: This operation threatens message freshness. The main purpose of this operation is to confuse or mislead the parties involved in the communication protocol that is not time-aware.

5.3.4 **Host-Based Attacks**

• **User compromise**: This involves compromising the users of a WN, e.g. by misleading the users into revealing information such as passwords or keys about the wireless nodes.

• **Hardware compromise**: This involves tampering with the hardware to extract the program code, data and keys stored within a wireless node. The attacker might also attempt to load its program in the compromised node.

• **Software compromise**: This involves breaking the software running on the wireless nodes. Chances are that the operating system and/or the applications running in a wireless node are vulnerable to popular exploits such as buffer overflows.
5.3.5 **Network-Based Attacks**

It has two orthogonal perspectives: layer-specific compromises and protocol-specific compromises. This includes all the attacks on information in transit. Apart from that, it also includes deviating from protocol; When the attacker is, or becomes an insider of the network, and the attacker’s purpose is not to threaten the service availability, message confidentiality, integrity and authenticity of the network, but to gain an unfair advantage for itself in the usage of the network, the attacker manifests selfish behavior that deviates from the intended functioning of the protocol.

5.3.6 **Physical Layer Attack**

- **Jamming** - This is one of the DoS Attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high-energy signal. Jamming attacks in WN are classified as four models, which are 1) Constant - corrupts packets as they are transmitted, 2) Deceptive - sends a constant stream of bytes into the network to make it look like legitimate traffic, 3) Random- randomly alternates between sleep and jamming to save energy, and 4) Reactive - transmits a jam signal when it senses traffic.

In order to defend against this attack, use spread-spectrum techniques for radio communication. Handling jamming over the Medium Access Control (MAC) layer requires Admission Control Mechanisms. Network layer deals with it, by mapping the jammed area in the network and routing around the area. Algorithms that combine statistically analyzing the received signal strength
indicator values, the average time required to sense an idle channel (carrier sense time), and the packet delivery ratio techniques can reliably identify all four types of jamming.

- **Radio interference attack** – This is one in which the adversary either produces large amounts of interference intermittently or persistently. To handle this issue, use of symmetric key algorithms in which the disclosure of the keys is delayed by some time interval.

- **Tampering or destruction** - Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. One defense to this attack involves tamper-proofing the node’s physical package. The self-destruction and fault tolerant protocols are briefly discussed below:

  - Self - Destruction (tamper-proofing packages): whenever somebody accesses the wireless nodes physically, they vaporize their memory contents and this prevents any leakage of information.

  - Fault Tolerant Protocols: the protocols designed for a WN should be resilient to this type of attacks.
5.3.7 Data Link Layer Attacks

- **Continuous Channel Access (Exhaustion):** A malicious node disrupts the MAC protocol, by continuously requesting or transmitting over the channel. This eventually leads to a starvation for other nodes in the network with respect to channel access. One of the countermeasures to such an attack is Rate Limiting to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions. A second technique is the use of time-division multiplexing where each node is allotted a time slot in which it can transmit.

- **Collision:** This is very much similar to the continuous channel attack. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change is likely to occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid. A typical defense against collisions is the use of error-correcting codes.

- **Unfairness:** Repeated application of these exhaustion or collision based MAC layer attacks or an abusive use of cooperative MAC layer priority mechanisms, can lead into unfairness. This kind of attack is a partial DoS attack, but results in marginal performance degradation.
• **Interrogation:** Exploits the two-way Request-To-Send / Clear To Send (RTS/CTS) handshake that many MAC protocols use to mitigate the hidden-node problem. An attacker can exhaust a node’s resources by repeatedly sending RTS messages to elicit CTS responses from a targeted neighbor node. To put a defense against such type of attacks a node can limit itself in accepting connections from same identity or use Anti replay protection and strong link-layer authentication.

• **Sybil Attack:** This type of attack is very much prominent in the Link Layer. The first type of link layer sybil attack is data aggregation in which single malicious node is act as different sybil nodes and then this negative reinforcements to make the aggregate message a false one. Second type is voting.

Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here the sybil attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and of course it depends on the number of identities the attacker owns.

5.3.8 **Network Layer Attacks**

• **Sinkhole:** Depending on the routing algorithm technique, a sinkhole attack tries to attract almost all the traffic towards the compromised node, creating a metaphorical sinkhole with the adversary at the center. Geo-routing protocols are known as one of the routing protocol classes that are resistant to sinkhole attacks.
Because, geo-routing protocol topology is constructed using only localized information, and traffic, which is naturally routed through the physical location of the sink node.

- **Hello Flood:** This attack exploits hello packets that are required in many protocols to announce nodes to their neighbors. A node receiving such packets may assume that it is in the radio range of the sender. A laptop-class adversary can send this kind of packet to all wireless nodes in the network so that they believe the compromised node belongs to their neighbors. This causes a large number of nodes sending packets to this imaginary neighbor. Authentication is the key solution to such attacks. Such attacks can easily be avoided by verify bi-directionality of a link before taking action based on the information received over that link.

- **Node Capture:** It is observed and analyzed that even a single node capture is sufficient for an attacker to take over the entire network. Good solution to this problem would definitely constitute an important work in WN.

- **Selective Forwarding/ Black Hole Attack (Neglect and Greed):** WN are usually multi-hop networks and hence based on the assumption that the participating nodes will forward the messages faithfully. Malicious or attacking nodes can however refuse to route certain messages and drop them. If they drop all the packets through them, then it is called a Black Hole Attack. However if they selectively forward the packets, then it is called selective forwarding. To overcome this, Multi path routing can be used in
combination with random selection of paths to destination, or braided paths can be used which represent paths which have no common link or which do not have two consecutive common nodes, or use implicit acknowledgments, which ensure that packets are forwarded as they were sent.

- **Sybil Attack**: In this attack, a single node presents multiple identities to all other nodes in the WN. This may mislead other nodes and hence routes believed to be disjoint with respect to node can have the same adversary node. A countermeasure to sybil Attack is by using a unique shared symmetric key for each node with the base station.

- **Wormhole Attacks**: An adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. This is usually done with the coordination of two adversary nodes, where the nodes try to understate their distance from each other, by broadcasting packets along an out-of-bound channel available only to the attacker. To overcome this, the traffic is routed to the base station along a path, which is always geographically shortest or use very tight time synchronization among the nodes, which is infeasible in practical environments.

- **Spoofed, Altered, or Replayed Routing Information**: The most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information
in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency. A countermeasure against spoofing and alteration is to append a MAC after the message. Efficient encryption and authentication techniques can defend spoofing attacks.

- **Acknowledgment Spoofing:** Routing algorithms used in wireless networks sometimes requires acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes. The most obvious solution to this problem would be authentication via encryption of all sent packets and also packet headers.

- **Internet Smurf Attack:** In this type of attack the adversary can flood the victim node's network link. The attacker forges the victim's address and broadcasts echoes in the network and also routes all the replies to the victim node. This way the attacker can flood the network link of the victim. If it gets observed that a node's network link is getting flooded without any useful information then the victim node can be scheduled into a sleep mode for some time to overcome this.

- **Homing:** uses the traffic pattern analysis to identify and target nodes that have special responsibilities, such as cluster heads or
cryptographic-key managers. An attacker then achieves DoS by jamming or destroying these key network nodes. Header encryption is a common prevention technique. Using “dummy packets” throughout the network to equalize traffic volume and thus prevent traffic analysis. Unfortunately, this wastes significant wireless node energy, so use it only when preventing traffic analysis is of utmost importance.

5.3.9 Transport Layer Attack

- **Flooding** - An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes. A solution proposed for this problem is the requirement that each connecting client demonstrate its commitment to the connection by solving a puzzle. As a defense against this class of attack, a limit can be put on the number of connections from a particular node

- **De-synchronization Attacks**: In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence, these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in the network in an endless synchronization-recovery protocol. A possible solution to this type of attack is to require authentication of all packets including control fields communicated
between hosts. Header or full packet authentication can defeat such an attack.

5.3.10 Application Layer Attacks

- **Overwhelm attack:** An attacker may attempt to overwhelm network nodes with wireless stimuli, causing the network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy. We can mitigate this attack by carefully tuning wireless so that only the specifically desired stimulus, such as vehicular movement, as opposed to any movement, triggers them. Rate-limiting and efficient data-aggregation algorithms can also reduce these attacks’ effects.

- **Path-based DoS attack:** It involves injecting spurious or replayed packets into the network at leaf nodes. This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station. Combining packet authentication and anti-replay protection prevents these attacks.

- **Deluge (reprogram) attack:** Network-programming system allows remotely reprogram nodes in deployed networks. If the reprogramming process insecure, an intruder can hijack this process and take control of large portions of a network. It can use authentication streams to secure the reprogramming process.
5.4 Survey on Secured MANET

Many researchers in the literature deal with virtual infrastructure concept based the battery power and signal strength. Prior work uses a simple group key management approach. The basic idea of this scheme is that a multicast tree is formed in MANET for efficient dissemination of messages including keys. It basically uses the same multicast tree structure and defines new group key agreement protocols.

Two multicast trees are constructed and maintained in parallel to achieve fault tolerance. Group members take turns as group coordinators to compute and multicast the blinded keys to all members through the active tree links. Each group member computes the group key locally by collecting the necessary keys from the group coordinator. The operation can be made in rounds and the coordinator is selected. Construction and maintenance of double multicast tree demand additional memory requirement and require additional computation on construction and maintenance. It also increases the work burden of the node which is acting as Group Leader.

Only group members who know the current group key are can recover the original message. The DH protocol can be extended to a generalized version of n-party DH. Research efforts have been put into the design of a group key management protocol for improving the scalability, reliability, and security. Furthermore, group key management also needs to address the security issue related to membership changes. The modification of the membership requires refreshment of the group key. This can be done either by periodic rekeying or updating right after a member change.
Group key management protocols can be classified into three categories: centralized, decentralized, and distributed. In the distributed method, group members themselves contribute to the formation of a group key and are equally responsible for the rekeying and distribution of group keys. Key management protocol is a critical component for securing group communications.

However, group key management for large and dynamic groups in MANETs is a difficult problem because of the restrictions on available resources and unpredictable mobility.

Group members take turns acting as group coordinators to compute and distribute intermediate key materials to group members. So, the duty of group maintenance and the burdens of computation, storage, and energy consumption are balanced among all mobile nodes. The intermediate keys are delivered through the tree links for efficiency. Each group member computes the group key locally without maintaining a logic key tree. Another important factor is to improve the performance of the overall system to achieve less end-to-end and network delay by using Secured Group Key Management Scheme.

A secure key management method in group structured MANET, where a group leader is responsible to generate, maintain and revoke the key of group members. Shifting the ownership of the group leader from one node to another node. By the time it transfers many secret info including key & function to generate key. Each time transferring this information increases overhead in network.
5.5 Proposed Dynamic Group Key Management Scheme (DGKMS)

A novel mutual authentication and key management protocol is proposed, which satisfies most of the security requirements like mutual authentication, confidentiality, integrity for one hop communication in MANET. In the proposed work, there is no pre key distribution and key storage for making protected data transmission in vulnerable wireless link. Common secret key is generated only between the communicating peers on the fly to provide secure communication simultaneously, while performing authentication.

There are three scenarios in the proposed work, which are given below:

Case 1 : Time Triggered Protocol (TTP) is completely reachable by every node of the MANET.

Case 2 : TTP is not reachable by some of the nodes of the MANET.

Case 3 : TTP is not reachable by any of the node of the MANET.

This authentication and key agreement protocol is based on authority based MANET. Every node gets a certified token from the TTP after successful verification of its credentials. All nodes are properly set up with certified tokens before network formation. TTP can be a mobile node in the MANET or it can be a separate entity, apart from MANET and its presence is
not compulsory in the active phase of the network. Each node is hard coded, which is unique in nature and immutable.

There are two phases involved in the proposed work, which are 1) Bootstrap phase, 2) Authentication and key management phase. The bootstrap phase is a pre-authentication phase. TTP verifies the credential information of the particular node to examine its genuineness. On successful verification TTP generates and distributes token to that particular node.

The authentication and key management phase is executed when a node in MANET needs to communicate with other nodes which are one hop distance. This approach is scalable, requires reasonable computational complexity and less communicational overhead. This authentication and key management (agreement) protocol is scalable, which requires reasonable computational complexity and less communicational overhead.

5.5.1 **Secured Group Key Management Scheme**

This Secured Group Key Management Scheme generates and distributes group key, thus reducing the burden of generating and verifying blinded key for each group members. In addition, it performs periodic rekeying and periodic group leader changes. The proposed Key Management technique is propagation of speeds of request and statistical profiling; they do not require network-wide synchronized clocks, do not impose any additional control packet overhead, and need only simple computations by the group leader and group member of connections.
The technique is based on reducing the computational burden and memory requirement of the node acting as a group leader. It implements the techniques in a widely studied secured group key management system and evaluated their effectiveness. Once the group is formed, a group leader is elected and it generates and distributes group key for that group and intimates its group members to generate private keys.

The methodology implemented for Rekey on Member Join is shown below:

- Node n broadcast a “Hi” message to all its neighbouring nodes.
  
  `Send_msg(“Hi”)`.

- If the message received by a neighbour node which is not the Group Leader (GL) then: Forward the message to its neighbour node.

- If the message is received by a neighbour node which is the present group leader then:

  a) GL request for some basic confidential information to the new node.

  b) Verify the information and authenticate the new node.

  c) Provide the group_id and let permission to the new node to generate private key_id.

  d) Broadcast information about the new member to the group members.
The methodology for Re-key on Member Leave is described below:

- The node that leaves the group has to send a leave notice to the group leader.

- Send leave (“Leaving!!”). If the group leader wants to leave the network then it must have to perform handoff.

- If the message received by a neighbour node which is not the GL then forward the message to its neighbour node.

- If the message is received by a neighbour node which is the present group leader then:
  
a) Broadcast the node leaving information to all the member of the group (i.e.,) if node A leave then group leader will broadcast the message as “Node A doesn’t belongs to the group anymore”.

  b) Generates a new group key for the group and notifies the group member to rekey their private keys.

The methodology for the Periodic rekeying is explained in the below: It assumes n-party DH algorithm for key generation. It uses the algorithm to generate key.

\[ k = m^e \mod n \] (5.1)
Where, \( k \) is the key, \( n \) is a prime number, \( m \) is a random number chosen by the node and \( e \) is primitive root of the prime number.

The methodology for the Periodic Group Leader Change is briefed below:

It is assumed that the node that acts as the GL should maintain a timer for certain sec/min/hrs.

- When the timer reaches the grace period then: GL will broadcast a message leadership change(“request for leadership change”);

- The node that is a valid member of the group and which provides a fast response to the request will be the new group leader.

- Perform handoff.

- Broadcast message about the new GL to the group member.

- Performs rekeying operation.

Every time the group leader verifies the request sent by the member of the group for group leader change request, the group leader verifies the information of each of the node. The node that doesn’t send any response is considered as the non-existing node and the group leader will broadcast the non-existing node information to its group members.
5.5.2 System Architecture of DGKMS

The responsibilities of the system are partitioned in such a way that each subsystem performs its own functions and when they are integrated together, they represent the complete functionality of the system. The first module takes the responsibility group formation and selecting the Group Leader.

The next immediate module is responsible for generating the Group key. It deals with DH algorithm implementation and in turn makes use of Message Digest 5 (MD5) for key generation. Whenever a Group leader is chosen the information has to be broadcast along with the group key. The next module deals with interval-based rekeying among the group members. It also performs rekeying on ever membership change. When a new node tries to join in a network the intermediate nodes are responsible for forwarding the packets from the new node to the Group Leader of the existing group.

Each node generates its join request; the requests are verified to ensure security. If the request is appropriate, new node is authenticated and included in the group. Then the group leader will generate a broadcast message that includes: information about new node, new group key and rekeying notice for all the group members. Node leaving operation works in the same way as like the operations that involves when a node joins except that the node must have to generate a leaving notice to the group leader.

The system performs interval-based Group Leader change operation to share the work burden of all the nodes among the network. This is done to maintain the security of the network. It is hard to predict the mobility
of a wireless node. So a node can act as a group leader only for a certain period of time.

When a group leader change operation is performed the node performs handoff. The new node that has been selected as a new group leader performs rekeying to protect the information about the group. Once the handoff and rekeying is done new group leader ID is passed to all the nodes in the network.

![Figure 5.1 Basic Information Flow in GKMS](image)

The basic information flow diagram is shown above. It describes the functionality of the starting of modules. It contains four states namely: Generate and distribution of group by GL, verify and authenticate node while joining and leaving, periodic rekeying and periodic group leader change.

5.5.3 **Algorithms**

Algorithm-A: node_join()
• Create a node, n.

• Node n broadcast a “Hi” message to all its neighboring nodes. Send_msg(“Hi”)

• if the message is received by a neighbor node which is the present group leader then:
  
  a. GL request for some basic confidential information to the new node.
  
  b. Verify the information and authenticate the new node.
  
  c. Provide the group_id and let permission to the new node to generate private key_id.

• If the message received by a neighbor node which is not the GL, then Forward the message to its neighbor node.

Algorithm-B: node_leave()

• The node that leaves the group has to send a leave notice to the group leader. Send leave (“Leavind!!”). If the GL wants to leave the network it has to elect new leader and performs handoff.

• if the message is received by a neighbour node which is the present group leader then:
a. Broadcast the node leaving information to all the member of the group (i.e.,) if node A leave then GL will broadcast the message as “Node A doesn’t belongs to the group anymore”.

b. Invoke group_rekey() algorithm.

- If the message received by a neighbour node which is not the group leader (GL) then: Forward the message to its neighbour node.

**Algorithm-C: GL_Change()**

Assumption: The node that acts as the GL must have to maintain a timer for certain sec/min/hrs.

- When the timer reaches the grace period then: Group Leader will broadcast a message leadership_change(“request for leadership change”);

- Group Leader verifies which node have send response and which node doesn’t send any response. Nodes which dint respond are considered as the non-member node and is identified.

- The node that is a valid member of the group and which provides a fast response to the request will be the new group leader.

  a) Perform handoff.
b) Broadcast message about the new GL to the group member.

- Invoke group_rekey().

**Algorithm-D: rekey()**

Assumption: either can use MD5/ data encryption standard algorithm.

- Invoke n-party DH (MD5) algorithm.

- Broadcast the new key generated to the group. Broadcast(groupke, ki).

- Along with the key, send intimation to the group member to generate a new key.

- Return.

5.6 Result and Performance Analysis

The proposed DGKMS in this thesis is compared with the traditional Target Authority (TA) Model and Recent Mobile Agent (MA) model. The Reliability and scalability are major research issues in the design of networking protocol.

Hence, the proposed work has analysed the reliability and scalability of proposed work and compared with TA and MA. The reliability is
computed based on the simulation data and result. The number of nodes is varied and number of attacker node also varied for performance comparison.

The simulation data is shown in Table 5.1. The reliability when 10% of attacker node, 20% of attacker node, and 30% of attacker node are shown in Figure 5.1, 5.2 and 5.3.

**Table 5.1 Simulation Environment**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>10 unit time</td>
</tr>
<tr>
<td>No of Nodes</td>
<td>100, 200, 300, 500 and 1000</td>
</tr>
<tr>
<td>Attacker Nodes</td>
<td>10%, 20% and 30% on total number of nodes</td>
</tr>
<tr>
<td>Reliability</td>
<td>In term of Packet Delivery Ratio (PDR)</td>
</tr>
<tr>
<td>Scalability</td>
<td>Model supports &gt; 75% PDR</td>
</tr>
</tbody>
</table>
Figure 5.2 Reliability When 10% of Attacker Node

Figure 5.3 Reliability When 20% of Attacker Node
Figure 5.4 Reliability When 30% of Attacker Node

The reliability of the methodologies is computed based on packet delivery ratio. The packet delivery ratio is total number of effectively delivered packets and total number of data packets transmitted. The packet delivery ratio is computed by increasing number of nodes and increasing number of attacker nodes. The numbers of attacker node are defined as 10%, 20% and 30% of the total number of nodes. The number of nodes are varies from 100 nodes, 200 nodes, 300 nodes, 500 nodes and 1000 nodes.

5.7 Conclusion

The scalability is observed from the above data, in which the system has 70% and above packet delivery ratio only accepted as scalable system. Hence, when 10% attacker nodes are inserted the TA supports up to 300 Nodes, whereas MA supports up to 500 Nodes and proposed DGKMS support 1000 Nodes.
When attacker nodes are increases to 20% of number of nodes, the TA supports up to 300 Nodes only, whereas MA supports up to 500 Nodes and proposed DGKMS support even for 1000Nodes. Similarly, the TA supports only 100 Nodes, the MA supports up to 200 Nodes when 30% of attacker nodes are inserted. The proposed system always supports above 80% packet delivery ratio. Hence, the proposed system proves better scalability than the existing systems.