Secure Group Based Biometric Authentication Approach for Mobile Ad hoc Networks

Developed by

Muhammad Tallal Chaudhry

(544-FBAS/MSCS/F09)

Supervised by

Prof. Dr. Muhammad Sher

MSCS-F09

Department of Computer Science

& Software Engineering

Faculty of Basic & Applied Sciences

International Islamic University, Islamabad.

PAKISTAN

(2012)

International Islamic University, Islamabad
Faculty of Basic & Applied Sciences
Department of Computer Science & Software Engineering

Dated: 27-06-2012

Final Approval

It is certified that we have read the Thesis titled "**Secure Group Based Biometric Authentication Approach for Mobile Ad hoc Networks**" submitted by Muhammad Tallal Chaudhry Reg. No. 544-FBAS/MSCS/F09. It is our judgment that this dissertation is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the degree of **Master of Science in Computer Science (MSCS)**.

Project Committee

External Examiner

Dr. Mujahid Alam,
Principal Scientific,
PAEC, Islamabad.

M. Alam

Internal Examiner

Dr. Tariq Abdullah,
Lecturer,
Department of Computer Science
& Software Engineering,
IIU, Islamabad.

27/6/12

Supervisor

Prof. Dr. Muhammad Sher,
Chairman,
Department of Computer Science
& Software Engineering,
IIU, Islamabad.

27.6.12

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِيْمِ

In the name of Allah (SWT) the most benificient and the most merciful.

A dissertation submitted to the
Department of Computer Science,
International Islamic University, Islamabad
As a partial fulfillment of the requirements
For the award of the degree of
Master of Science in Computer Science (MSCS)

Dedicated...

To a Person who is
"The Rehmat" for all the Universe,
and
To my Parents and my Supervisor
and
To whom I love and respect.

DECLARATION

I hereby declare and affirm that this thesis neither as whole nor as a part thereof has been copied out from any source. It is further declare that I have completed this dissertation on the basis of my personal efforts, made under the science guidance of my supervisor. If any part of thesis report as proven to be copied out or found to be reproduction of some other I shall stand by the consequences. No portion of the work presented in this report has been submitted in support of an application for other degree or qualification of this or any other university of learning.

(Muhammad Tallal Chaudhry)
544-FBAS/MSCS/F09

ACKNOWLEDGEMENT

(In the name of Allah, the Most Gracious and the Most Merciful)

All praise and glory to Almighty Allah (Subhanahu Wa Ta'ala) who gave me the courage and patience to carry out this work. Peace and blessings of Allah be upon His last Prophet Muhammad (peace be upon him), said: "Allah makes the way to Jannah easy for him who treads the path in search of knowledge."

First and foremost, I would like to thank my supervisor **Prof. Dr. Muhammad Sher** for accepting, supporting and allowing me to take the liberty to follow my research interests as well as for continuous guidance, valuable advice, immense effort, and thoughtful discussions throughout my research.

I would like to thank my Family, specially my parents for their love, understanding, prayers and financial support. Their prayers and encouragement always help me to take the right steps in life.

I would like to give special thanks to all my colleagues and friends for their friendship, barter ideas, motivation social and moral support throughout my academic carrier.

Muhammad Tallal Chaudhry

ABSTRACT

Ad hoc network is a temporary association of mobile nodes which don't depend upon any fixed infrastructure. In Mobile Adhoc Networks (MANETs) nodes are mobile and every node may change its location from one network to another. Due to mobility of nodes security is a big issue in it. It is important to provide security and to maximize the lifetime of network. The main drawback during node mobility is that, when a soldier (node) moves out of one group and it joins other group then it can be easily attacked by the attacker. Our purpose is to overcome that problem. What happens if an attacker killed the soldier and if it takes the mobile device (in which soldier certificate is stored) of that soldier then how to authenticate it before joining the other group. For this purpose, we propose that Certification Authority (CA) embeds a certificate that includes the soldier id, nonce number, login id, password and its image in each soldier allocated mobile device. CA sends the same information (certificate) to soldier affiliated GR and GR further sends this information to the GR of targeted group for communication and mobility. Before joining the new group, the GR of targeted group takes image again of this new soldier and matches the login, password and image with the stored existing original information for authentication and authorization. Another issue during node mobility is if a node leaves one group then its correlated information is cleared only from its affiliated GR. But the neighboring nodes still contains the information of this leaving node in their neighbors list and hence will be contacted in future elections. It will cause an overhead to locate that which nodes have left the group and increases the communication overhead. Therefore, we have proposed a backlog clearance algorithm that clears the backlog information of the leaving node from their neighboring nodes lists by using DSR (Dynamic Source Routing) approach after GR receives the node attachment reply from the GR of targeted group. This reduces the communication cost and overhead. Our proposed approach is suitable for disaster situation like WAR. We propose a reliable and secure group based biometric authentication approach (image recognition) for node mobility in MANETs. In addition; node joining, node migration and node leaving algorithms are used for our proposed approach. Simulation for this evaluation is based on Network Simulator (NS-2) by using the Fedora 14 operating system. The experimental results have been explained by graphs. Thus, this scheme updates the neighboring lists as well as provided secure authentication and protection from the compromised nodes.

Keywords: *Mobile Ad hoc Networks, Certification Authority (CA), Group Representative (GR), Node Mobility, Dynamic Source Routing, Biometric Authentication Approach, Compromised Nodes, Soldier, Attacker, Certificate, Neighboring Nodes, Backlog Clearance, Image Recognition.*

Table of Contents

List of Figures

List of Table

Acronyms

BAA	Biometric Authentication Approach
BCA	Backlog Clearance Algorithm
CA	Certification Authority
Cert	Certificate
CH	Cluster Head
DSDV	Destination Sequenced Distance Vectoring
DSR	Dynamic Source Routing
E_K	Encrypted Key
GR	Group Representative
IMG	Image
MANET	Mobile Ad hoc Network
NA	Network Administrator
NAR	Node Attachment Reply
NJA	Node Joining Algorithm
NLA	Node Leaving Algorithm
NMA	Node Migration Algorithm
OTCL	Object Tool Command Language
RREP	Route Reply
RREQ	Route Request
TCL	Tool Command Language
TTL	Time to Live
TTP	Trusted Third Party

Symbols and Notations

=	Equality
→	Assigns
||	And
EK_{NG}	Asymmetric Key Encryption
ID_N	Node Id
IMG_N	Node Image
IMG_C	Image given by CA
IMG_G	Image given by GR
IMG_J	New Image taken by node
R	Nonce
login	Login Id
pwd	Password
REQ	Request
REP	Reply
N	Node
$Cert_N$	Certificate of Node
Req_clear	Node clear request
Node_mig_request	Node migration request
Node_leave_request	Node leaving request

Chapter 1
Introduction

1. INTRODUCTION

An Ad hoc network is a two-way mixture of mobile nodes without any fixed centralized access point. Every node in the ad hoc network acts as router and each node forwards the message from its one neighbor node to other nodes until the messages reaches to the destination node. These types of network are so much expensive but broadly used in military environment like battlefield scenarios and even used in home and personal area networking applications (as shown in *figure.1-1*). The "Ad hoc Networks" are easily deployed and they don't need any backbone infrastructure support [9]. But the "Mobile Ad hoc Networks" (MANETs) are infrastructure less wireless network in which mobile nodes are connected with each other through wireless channel and they are capable of moving at their own desire. In "Ad hoc Wireless Networks", there is a base station and if any node wants to communicate with other node then it sends a request message to the base station and then base station forwards this message to that specific node. In the next section we will explain the MANET functionality along with its architecture and applications.

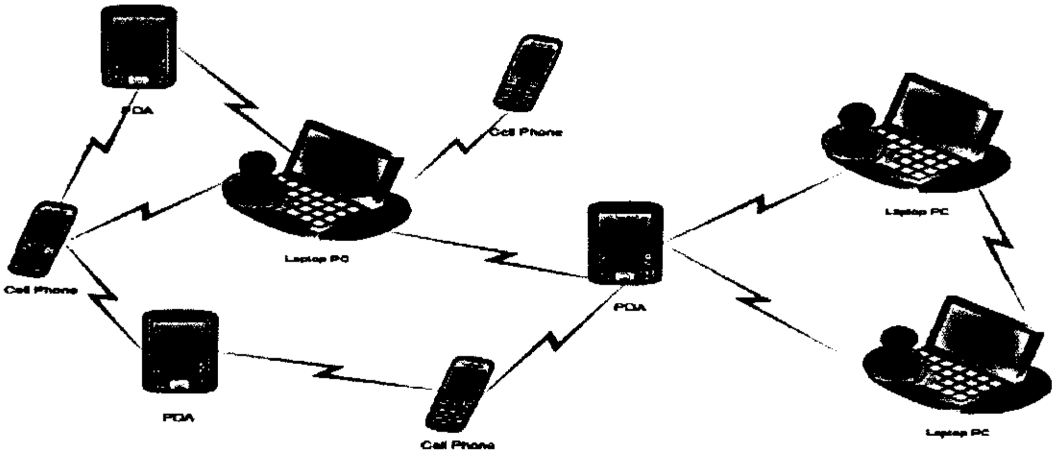


Figure 1-1: Ad hoc Network [9]

1.1 Mobile Ad hoc Networks (MANET)

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes which don't depend on fixed infrastructure. Basically it consists of temporary network topologies. The nodes are capable of moving freely, independently in any direction and change their locations in unpredictable and random manner. MANET is a wireless network and not a wired network that's why in MANET nodes are mobile and they must be able to generate packets and messages even if the communication range among nodes is raze.

A mobile ad hoc network (MANET) is a temporary system of mobile nodes connected by wireless links forming a diminutive and live network (as shown in *figure.1-2*) and it is available even when internet access is unavailable [9]. The nodes in MANET normally work on such batteries devices that have minute power and these nodes can function both as routers and hosts. A MANET can be a private (standalone) network or it can be connected to exterior networks (i.e. wireless internet). The idea of mobile ad hoc networks is to support strong and efficient applications/operations. "Mobile IP" functionality is used to support routing between mobile nodes. Basically, mobile IP shows the current location of the nodes when it joins the new group after leaving the present group.

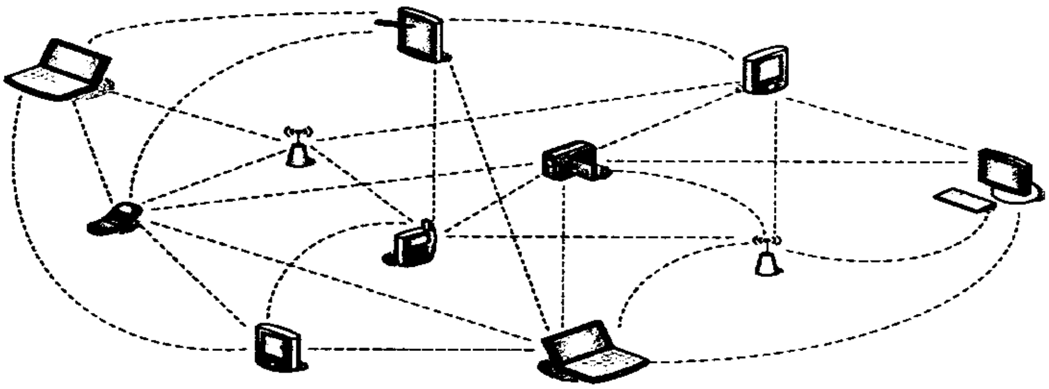


Figure 1-2: A Mobile Ad hoc Network (MANET) [9]

'Internet' means worldwide internet that we access globally but 'internet' means small pair of computers that connected with each other through LAN etc. Security plays an important role in wireless mobile ad hoc networks. If we send a data packet over an insecure channel i.e. internet we must fulfill four (04) aspects of security that includes; confidentiality, integrity, authentication, authorization and data integrity [9] as shown in *figure.1-3*. There are numbers of encryption algorithms generally categorized as Symmetric and Asymmetric encryption algorithms. Symmetric encryption techniques are less efficient as compared to Asymmetric encryption techniques because asymmetric encryption is used for authentication and the secret key doesn't need to be shared.

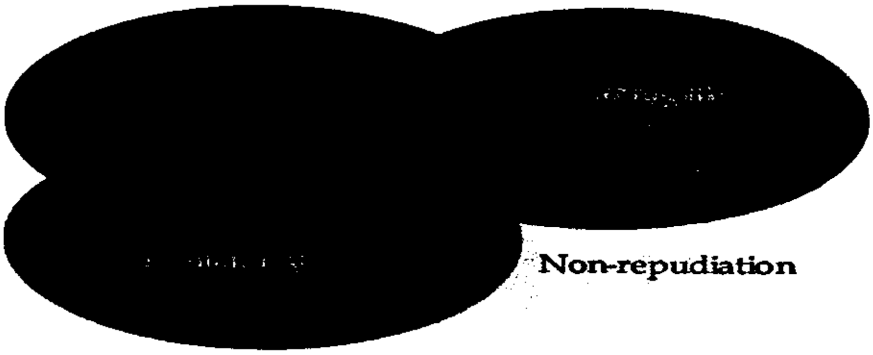


Figure 1-3: The four fundamental requirements for a secure network [9]

1.2 Applications of MANET

Workstations in mobile ad hoc networks can function not only as base-stations (source nodes are used for sending the data packets and destination nodes are used for receiving this information) but also acts as intermediate system (forwarding data packets from one node to other nodes). Therefore, in a cluster it is achievable that two nodes communicate with each other even when they are outside of their communication (transmission) ranges. This happens because intermediate (neighboring) nodes [8] can work as routers and forward data packets from one neighbor to other till it reaches to the destination. That's why mobile ad hoc network sometimes called *"multi hop mobile ad hoc network"*. MANET usage/application areas are in Military conflicts, Sensor networks, Human-induced Disasters, Emergency medical situations etc.

1.3 Security Issues and Challenges in MANETs

Mobile Ad hoc Networks (MANETs) are wireless networks thus they are more susceptible to attack by the attacker anytime as compared to wired network. The security issues and challenges in MANETs [8].

These are because of the following reasons mentioned below:

1.3.1 Open Medium

Due to their open (wider) medium, eavesdropping attack is much easier in it than in wired network.

1.3.2 Dynamically Changing Network Topology

In MANETs, mobile nodes are freely to leave the present group and join the new group at own will so nodes are changing their network/group location time to time (rapidly). That's why even compromise nodes can easily join the new network without being detected.

1.3.3 Cooperative Algorithms

The routing algorithms used in MANET require shared understanding (trust) between nodes which tumble the fundamental principles of network security.

1.3.4 Lack of Centralized Monitoring

A monitoring agent eliminates the absence of a centralized communications in the network.

1.3.5 Lack of Clear Line of Defense

If we need to research on network security the basic requirement we need to deploy layered security mechanism because security is a process that provides secure way and preventing the compromised nodes to join the system.

1.4 Mobile Ad hoc Network Routing Protocols

Reviews of some prominent routing protocols for mobile ad hoc networks [8] as shown in *figure. 1-4* are listed below in detail:

1.4.1 Ad hoc On Demand Distance Vector Routing (AODV)

In AODV, when a node wants to transmit data packet to destination node then it selects a route by generating a route request (RREQ) packet which includes the sequence number of the destination node. When the request packet reaches to the chosen destination then this node generates a route reply (RREP) packet which is sent back to that source node followed by the same path. The reply packet/message contains the current sequence number as well as the number of hops to the destination.

1.4.2 Dynamic Source Routing (DSR)

DSR is a major routing protocol that uses a concept of source routing. Each node maintains a route cache (routing table) in which it lists overall routes to the destination and the entry of its neighboring nodes. Basically, DSR is used for route discovery and route maintenance. It allows nodes to maintain and discover single or multiple route(s) to the destination.

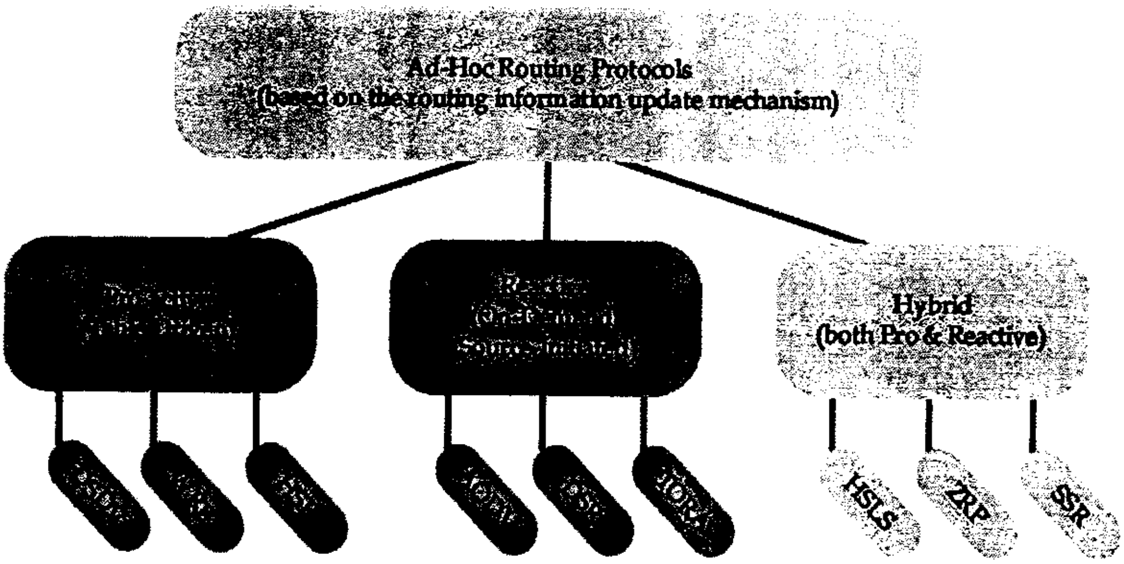


Figure 1-4: Mobile Ad hoc Network Routing Protocols [8]

1.5 Biometric Authentication Mechanisms

The biometric authentication [8] is an electronic identification of the physical and unique characteristics of the user (individual). The biometric technologies can easily be structured and deployed in mobile ad hoc networks. The most important biometric authentication approaches includes:

- Image recognition
- Finger prints
- Retinal scans
- Voice prints
- Signature verifications

In all of above mentioned schemes, we used image recognition scheme for our proposed secure group based biometric authentication approach.

1.6 Problem Identification

During Node Mobility, when a soldier moves out of one group and joins the other group then it may possible that an attacker attacks on the soldier and killed the soldier. Furthermore, if the attacker takes mobile device (in which soldier's certificate is stored) of the soldier then by using this mobile device an attacker can easily joins other group without its proper authentication and authorization.

Another issue in Node Mobility is if a node leaves one group then its correlated information is cleared only from its affiliated GR. But the neighboring nodes still contains the information of this node in their neighbors list and hence will be contacted in future elections. It will cause an overhead to locate the nodes which have left the group.

1.7 Objectives of Study

The main objective is to extend the security of Mobile Ad hoc Networks (MANETs) by preclusion from compromised nodes to join the group. To increase the life time of MANET we provide strong and efficient authentication by using secure group based biometric authentication approach (image recognition). By using this proposed approach, we can authenticate a soldier (node) that wants to join a new group. Furthermore, our proposed approach reduces the communication overhead by clearing the backlog information of leaving node with the help of backlog clearance algorithm. Thus, this scheme updating the neighboring lists as well as provides security (authentication and authorization) and protection from compromised nodes.

1.8 Research Assumptions

Assumptions in our proposed research work are as follows:

- Network Administrator is not compromised by the attacker because it is a powerful entity.

- The mobile agent is a program segment that collects information about trustworthy nodes in a group and information about nodes whose certificates are expired.

1.9 Scope of Study

The simulation of secure group based biometric authentication approach (image recognition) during node mobility and communication have been developed on Fedora 14 operating system by using Network Simulator version 2 (NS-2). So results are on the basis of simulation not on actual experimental work.

1.10 Proposed Algorithms and Simulation Scenarios

Our proposed secure group based biometric authentication approach (image recognition) during node mobility and communication consists of following algorithms and simulation scenarios.

1.10.1 Proposed Algorithms

- Backlog Clearance Algorithm
- Node Joining Algorithm
- Node Migration Algorithm
- Node Leaving Algorithm

1.10.2 Simulation Scenarios

- Node Deployment Strategy
- Node Joining Strategy using Biometric Authentication
- Node Leaving Strategy and Backlog Clearance Testing
- Node Migration

1.11 Thesis Organization

Chapter 2 provides a background and related work of the research areas (Literature Review).

Chapter 3 gives an overview of problem identification/formulation, proposed solution and proposed algorithms used in our proposed scheme.

Chapter 4 present details of the simulation results and analysis obtained by applying algorithm techniques on MANET test systems. Conclusion drawn from these results is also presented using secure biometric authentication approach (image recognition) during node mobility and explained in the form of graphs.

Chapter 5 gives a conclusion. It also gives some points about limitations of proposed approach and future work.

Chapter 2
Literature Review

2. LITERATURE REVIEW

In this chapter the related work establishes where our proposal stands in comparison to the existing work. In the literature review different schemes have been proposed. These schemes are listed below in detail:

Tseng, Y et al **[20]**, have explained mobile IP functionality in ad hoc network. In this scenario there was no concept of fixed gateway (TTP) and every node moves from one place to another. This concept is based on *"Single Node Mobility"*. Each gateway has two interfaces. One interface is connected to wireless and other is connected to wire-line. Gateways are fixed and they are responsible for connecting MANETs with internet. To support mobile Internet Protocol (IP) functionality each gateway serves as a foreign agent in the local MANET. When a node moves from one group and joined other group then the new group acts as a foreign agent for it. The former group is its home network. It asks for registration request from the foreign agent. The foreign agent sent this registration request to its home agent. Home agent authenticated this node and sent registration reply to foreign agent. After authentication/validation of the node from home agent, the node in foreign agent was assigned a Care of Address (CoA). Now any data for this node will come through it.

Advantages and Limitations

1. There was no concept of fixed gateway and authentication of group representatives (GRs) as well as nodes was assumed by any reliable Trusted Third Party (TTP).
2. Individual CoA was assigned to every node in the network and thus every node has to register individually in the new network.
3. This individual registration process consumed more network bandwidth.
4. Number of messages was increased and every node sent messages to register itself in the new network.
5. Delay occurred in registering nodes in the previous network.
6. No concept of single entity registration on behalf of the whole group.
7. When the node left the present group and joined the new group then its current location can easily be identified by using CoA.
8. Lack of security architecture in this scheme and any node as well as GR was attacked easily by the attacker.

Critical Comments/Findings

This paper deals with the concept of single node mobility. Our proposed research is based on single node mobility scenario too. In this paper, there is no authentication mechanism when nodes are moving from one group to another that's why even a compromise node can join the new group easily.

Irshad, E et al **[13]**, have proposed a group registration with group mobility scheme to overcome the approach of individual entity registration. A new concept of fixed gateway (fixed node) in the network was introduced, in which the fixed gateway is the overall controller of MANET. The fixed gateway kept the mobility location of all the nodes in the network and responsible for validation of former group when registration request was send by any of the group representative. Every group has a group representative (GR) which is the controller/organizer of the group. Only GR was assigned an individual Care of Address (CoA), IP of all other nodes in the group remained same. Mobile IP functionality is used to support mobility in MANET and it basically allows a mobile node to acquire CoA.

Advantages

1. The number of messages for registration was reduced.
2. Registration time for registration of nodes was reduced.
3. Delay of registering the nodes in a new group was reduced.
4. Only one node registration (i.e. GR) was required in a new group.
5. Network Bandwidth was greatly optimized.
6. Routing table updates in a MANET was reduced.

Limitations

1. No model was given for authentication/authorization of nodes, even if a single node was out of cluster range during mobility then adversary can easily attacked/killed the node and joined other network easily without its proper authentication and authorization due to security (validation) assumption in this whole technique.
2. Single point of failure (i.e. cluster head), if a cluster head in a group was compromised then whole group becomes compromised and if a single node is compromised by the attacker then it can easily injected false messages in the route and generated unwanted traffic due to lack of security measures.
3. No way of generation of secure public and private keys (Symmetric & Asymmetric keys).
4. Without authentication & authorization of GR and nodes, even a node in one group can send data packet (information) to node of other group.

5. Before a node joins other group, first its authentication will be performed and then a CoA will be assigned to that node after its complete authentication and authorization.

Critical Comments/Findings

This paper deals with the concept of group registration. The scheme only deals with performance evaluation of MANET and doesn't provide security that's why mobility & communication channel is insecure. Further, it is assumed that each group representative (GR) of a group is authenticated by the fixed gateway which is the Trusted Third Party (TTP).

Vincent, A and PushpaLakshmi, R [3], proposed the concept of composite key management approach in which a network was hierarchically structured into clusters on the basis of node's trust value and only that cluster head (CH) was elected for the group that has maximum trust value after the election. The network was divided in the form of clusters. The node with maximum trust value was selected as cluster head (CH). Private Key Generation (PKG) serving node was used to generate the public and private keys for the nodes. Nodes moves from one cluster to another and the entire communication was made through Inter-Intra cluster communication strategy.

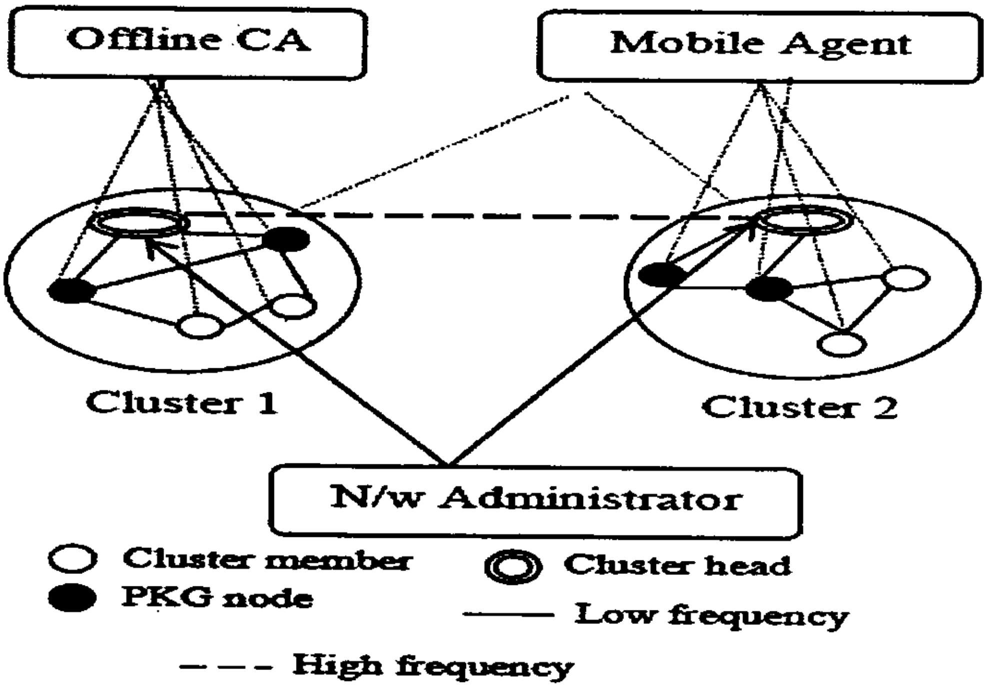


Figure 2-1: Network Model of composite key management scheme [3]

According to *figure.2-1*, Network Administrator (NA) elected CH after an election. The offline CA assigned node id and nonce number for the new node that wants to join the network. The PKG nodes were combined by the CH for obtaining the whole key for the node. The NA originally allocated the private key for CHs. The mobile agent was a program segment that collected information about how many trustworthy nodes in the network and has information about nodes whose certificates was expired. Low level frequency was used for communication between cluster member nodes and high level frequency was used for cluster heads transmission.

Node Joining and Node Leaving

Offline CA assigned node id and nonce number for the new node that wants to join the group. Firstly, this new node registered the information about its public key with CH. New node can contact CH directly or contact through their neighboring nodes. For message communication, the message included node id and nonce number R. Basically the nonce/random number (R) was used for the authenticity of data packets (messages) that was being sent. Actually when a node leaves the present cluster, then Cluster Head (CH) removes this left node correlated information only from its own list. So the node that left the cluster can't receives the generated messages by the cluster head.

Key Establishment Algorithm

```
Procedure KEY_ESTAB ($ID_N$)

Begin

1.  GR→ PKG: $E_{PKG1}$ (REQ ($ID_N||R'$))
            ……. $E_{PKGk}$ (REQ ($ID_N||R'$))
2.  PKG→ GR: $EK_{PG}$ ($S_{P1}||R'$))…. $EK_{PG}$ ($S_{PK}||R'$))
3.  GR computes private key
            $S_N = S_{PKG1} + S_{PKG2} + …… + S_{PKGk}$
4.  GR→N: $EK_{GN}$ ($S_N||R||KNO$))
            where KNO=Unique number ||Time of expiry

End KEY_ESTAB
```

Step 1: GR send the request message to the PKG nodes PKG_1, PKG_2,..., PKG_K. The message is encrypted using PKG's public key. R′ represents the random number used by the PKG nodes for authentication.

Step 2: PKG nodes send the GR's public key encrypted key shares to GR.

Step 3: GR works as key combiner and it generates the whole key S_N.

Step 4: GR sends the generated secret key to the node and this is encrypted using nodes public key. KNO is generated using unique number and expiry time of the key.

Advantages and Limitations

1. Each node has self allocated public key which was known simply to cluster head.
2. The public key of the node was generated based on node's identity (id) and this node id was assigned by CA.
3. No need to store public keys in Cluster Head (CH).
4. Cluster nodes don't broadcast their public keys to all its neighbor nodes, which saving network bandwidth and storage space.
5. Public key of CH changes occasionally and each CH computed its new public key based on the trust value and its earlier (older) public key.
6. Key renewal process can be done easily using timestamp in the key numbers.
7. The essential problem in this scheme is when a node moves out of one cluster and it moves to other cluster then it may possible that an attacker attacks on the node and killed the node, further if the attacker takes mobile device of the node then by using this mobile device attacker can easily joins other cluster without its proper (successful) authentication and authorization.

Critical Comments/Findings

In this paper, the authentication was made only on the basis of nonce number R which can be attacked easily by the attacker anytime during node mobility and communication. So the authentication process used in this scheme was much weaker and node may be compromised before it joins the new group. The other issue in this scheme is if a node leaves one cluster then its correlated information was cleared only from its affiliated cluster head (CH). But the neighboring nodes still contains the information of this node in their neighbors list and hence will be contacted in future elections. It causes an overhead to locate that which nodes have left the group and increases the communication overhead.

Kadri, B et al **[15]**, proposed a secured weight based algorithm for clustering to compute trust value under the supervision of cluster size variation. This algorithm also called secured clustering algorithm (SCA), basically this algorithm included some major security requirements by using the node trust value. The trust value defines that how deeply every node was trusted by its neighboring nodes if it was placed in a one (same) cluster/group. Furthermore, by using the nodes certificate as an identifier they avoid several possible attacks occurred (i.e. spoofing attacks).

Advantages and Limitations

1. Certificates were used as an identifier for avoiding spoofing attacks.
2. This approach overcomes the problem of election of power efficient cluster head (CH) because SCA elected strong and power efficient cluster heads according to their weights which was computed by combining the set of parameters (i.e. stability, battery power, degree and the maximum value etc).

Critical Comments/Findings

This scheme used an efficient flooding scheme for sending beacons within the specified cluster range to avoid overhead which was occurred due to flooding.

Chen, R et al **[16]**, proposed a reliable and trustworthy region based protocol for group key management in a group communication for mobile ad hoc networks (MANETs). For openness and self-motivation, Authors proposed two-level hierarchical key design to securely plan the distribution of keys. In Addition for key generation, a key protocol named Contributory Key Agreement (CKA) protocol has been proposed to avoid the use of key generation by using centralized key server (KDC). Moreover, to minimize the communication cost of overall network an optimum regional size was used.

Advantages

1. The given region (area) can be of any size and nodes can move from one region to other at their own desires.
2. Contributory Key Agreement (CKA) protocol was used for key generation without using a centralized key server.
3. Passive attacker can't discover any group key because of using the secure MAC for group key secrecy. Basically a passive attacker inserting his own data into the data stream and playback of data from another connection.
4. Network communication cost was reduced by this approach.

Limitations

1. Group partitioning and merging model was not involved in this scheme. That's why this scheme doesn't provide a better reflection for group mobility behavior as well as it was not capable for various mobility models.

Critical Comments/Findings

This scheme only deals with outsider (external) attacks which were injected by the adversary/attacker and there was no method available for preventing with insider attacks (i.e. resource consumption, node isolation, route disruption, route invasion). Trusted Third Party (TTP) was assumed for authentication of all mobile nodes due to which attacker attacked on any node and compromised that node due to lack of security infrastructure.

Saju, P and Samuel, P [2], have proposed a scalable method of crypto-graphic key management (SMOCK) that deals with the node compromised attacks. But this approach has some main drawbacks such as when number of nodes was increased than over reliant on centralized server as well as key pairs were increased. To deal with these cons, Authors presented a superior hierarchical key management approach by using a secure and proficient clustering technique. Every cluster head (CH) preserved the public key of its neighbor nodes and distributed the keys only during node communication and mobility with other group. Moreover, the adaptive weight cluster (AWC) approach was used to achieve a power efficient and strong cluster head (CH).

Advantages

1. The need of storing public keys of the neighbor nodes was diminished thus minimizing the storage overhead of each node.
2. Only the cluster head (CH) contains the public keys of the nodes and provides the copy of it to all its neighboring nodes thus each node contained the public keys of its member nodes only in the same cluster. So overhead on centralized server was reduced.
3. Each node has storing public keys of all neighbor's nodes in the cluster which increased the storage overhead and consumed more bandwidth thus this method was diminished and just need to store the public keys of cluster members in same cluster.
4. In the same cluster every node knows the public key of its member nodes and if a node needs to communicate with other node within a cluster, it acquires the public key of this specific node then it sent the encrypted message through it.
5. Proposed technique was convenient spirit against node capture attacks.
6. This scheme provide higher delivery ratio which reduce overhead and delay.

Limitations

1. No authentication was done for cluster head and member nodes, and if intruder attacks on member nodes then it can easily injected false messages during inter-intra cluster communication.
2. Due to centralized approach, single point of failure may be occurred i.e. cluster head.

Critical Comments/Findings

In this scheme if the cluster head is compromised by the intruder then all the nodes within the cluster becomes compromised. No Trusted Third Party (TTP) is used for generation of public and private keys and the keys were generated through insecure channel and distributed among the nodes which can be attacked easily by the intruder any time.

Renuka, A and Shet, K **[10]**, proposed a group key management scheme that use a symmetric key for group based communication within the cluster (Intra cluster communication) by using public key cryptography (PKC). Initially the group key was generated by the cluster heads (CHs) and transfer via a secure channel to other nodes. Basically a secure channel is a way of transferring data that is opposed to overhearing and tampering. Asymmetric key encryption was used to encrypt the group keys if and only if the membership changes were occurred. For the authentication of public keys, authors used hash trees in this scheme. CH is basically responsible for key generation and inter-intra group communication. Mainly this scheme uses the combination of private & public keys cryptography. There was no trusted third party to achieve the process of authentication during node mobility. Cluster head generates a group key and transmitted it to all neighboring nodes within a same group without the proper authentication and authorization of these mobile nodes.

Advantages

1. Minimized the computational cost of authentication by using hash trees.
2. Reduced the communication costs of re-keying messages every time membership changes occur.
3. Used the combination of public and private key cryptography that makes it more secure.

Limitations

1. Group key was generated by the cluster head and delivered to all member nodes but if the cluster head was compromised by the adversary then whole group becomes compromised due to lack of secrecy (authentication).

2. Cluster head generated a group key and distributed it to all member nodes without authentication and authorization of these mobile nodes.

Critical Comments/Findings

In this paper, there is no Key Distribution Center (KDC) to perform the service of authentication and authorization. Further, it is assumed that all of the incoming members of the MANET carry a valid certificate issued by an offline certification authority binding the node id with its public key.

Xiao, Q **[19]**, proposed a battlefield scenario in which several mobile devices were developed for military applications. Peer to peer network provided structural design for mobile communication in group based network. Hence, there was no need for a fixed infrastructure and nodes (users) that can energetically route their desired information in any network location at any time. Retinal (Iris) scan was precise, accurate and less in cost as compared to others biometric technologies. Signature identification was less secure as compared to other biometric technologies. Image and fingerprint techniques were accurate and adequate for user authentication process. Images can be used to authenticate the new user that want to join the group because in same group the neighboring nodes should be familiar with each other.

Advantages and Limitations

1. Each group leader (cluster head) has allocated a biometric pattern/template that includes one of the following(s) biometric technologies (fingerprint authentication, image recognition, retinal scan and signature verification).
2. The group key was used to provide secure communication within the group whereas the coalition key was used to encrypt messages that were sent between the groups.
3. Voice recognition created problems in rough environments such as battlefields.

Critical Comments/Findings

In this paper a biometric authentication model is used to validate the identity of the user by using biometric authentication techniques in mobile ad hoc networks. By using this technique, biometric templates of authorized users are stored in the database along with their identities. Further, a centralized server is used to carry out the biometric authentication. All nodes that want to join the network have to send their identities (i.e. group id and personal id) through their specified access points.

Deodhar, A and Gujarathi, R **[18]**, proposed a two way detection mechanism that decided whether there was an intrusion detection system between the member nodes. In mobile ad hoc networks (MANETs) nodes normally have a partial battery power so if the threat level was low then it was not possible to make each and every node in a MANET that act as a monitoring node. Even their neighboring nodes can arbitrarily elect a monitoring node such as the cluster head. The key disadvantage in cluster based approach was the single point of failure which is the cluster head (CH). If the cluster head was compromised then the whole group becomes compromised and it can easily generate attacks and erroneous data packets. Basically, this scheme provided security and protection in case if the cluster head was compromised by the attacker.

Advantages and Limitations

1. The cluster backup eliminated the single point of failure (i.e. CH) and improves the fault tolerance for the network.
2. Weighted election algorithm (WEA) allows the election of efficient and powerful master and backup.

Critical Comments/Findings

In this paper the concept of a cluster backup is introduced that is a replica (copy) of the Cluster Head (CH). If a cluster head is compromised then there is another possibility to make cluster backup as a cluster head. Moreover, this elected cluster head (CH) performed signature detection mechanism on all their neighboring nodes.

Huang, D and Medhi, D **[14]**, proposed a secure group key based approach for mobile ad hoc networks (MANETs). Basically the group key management approach intends to improve the accessibility and mount-ability of hefty mobile ad hoc networks. They have developed a roaming protocol that provided a secure group transmission between two different groups without involving any new keys. Therefore, nodes in two different groups communicated with one another efficiently by using the concept of secure tunneling.

Critical Comments/Findings

This paper presented the concept of tunneling. In MANETs, different groups were made. When a node moves out from one group range and it joins the other group range then this moving node developed a secure tunnel from its source (home) group to the destination (foreign) group. The critical comment about this scheme is that even if cluster head (group manager) becomes compromised then this scheme offers uninterrupted group communication between member nodes.

Berndt, L **[21]**, has proposed an ad hoc on-demand distance vector (AODV) routing protocol that forwarding messages from one network to another. It transmit data packets form one neighbor node to other nodes until the message/data packet reaches to the destination node. The nodes that directly communicate were considered as intermediate (neighbors) nodes. When any node wants to send message to any other node then it generates a route request (RREQ) message. This RREQ message contains some valid information about that node (i.e. the source, the destination and the sequence number). The sequence number was used as unique id or as time stamp. It basically tells the freshness of stored information. Node that contains eminent sequence numbers indicates fresh route. Therefore, neighboring nodes can easily identify that which node contained more perfect and precise information.

Critical Comments/Findings

In this paper, Berndt has proposed the concept of AODV protocol which selects the optimum (shortest) route for message or packet delivery from source to destination. In AODV, the route error message (RERR) permits to removes such routes that contains the awful (poor) nodes in the group.

Burg, A **[22]**, explained variety of attacks in an ad hoc network. In this paper author describes various attacks that can occurs during node mobility and communication.
These attacks are described in more detail under separate headings.

Impersonation attacks: sometimes called as spoofing attacks. In these attacks the attacker understood the identity of each node in the system.

Sinkhole attacks: in sinkhole attacks an attacker node tries to compromise all its neighboring nodes and magnetized the data packets towards it. Sinkhole attacks spread haziness in ad hoc network routing algorithms.

Wormhole attacks: in this type of attacks, one compromised node used some route to request messages to some other compromised nodes at different locations that were so far to the original network. A wormhole attacks itself were not injurious because it takes less time for data packets to reaches the destination node.

Sleep deprivation attacks: were overwhelming to ad hoc networks having nodes that contained not enough resources.

Sybil attacks: basically in sybil attacks an attacker node was not merely mimic (copy) the single node but it was assumed the characteristics of numerous nodes in the network.

Critical Comments/Findings

All of these above mentioned attacks can occurred during node mobility and communication. But in our proposed approach, we encountered/tackle with Man-In-The-

Middle attack. In Man-In-The-Middle attack, there is an attacker within the route if any node moves from present group and joins other group then this attacker can easily kill this moving node and take out all necessary information from this node and joins the new group. Man-In-The-Middle attack is basically the type of attack where attackers interrupt into an existing connection to capture the exchanged data and insert false information.

Lein, H and Jian, R **[1]**, have been proposed a narrative design for the key establishment and for user authentication by establishing the key concept of Generalized Digital Certificates (GDC). To support key agreement and user authentication process the design of GDC is used. Basically in GDC, a user didn't have a pair of public-private keys and even GDC didn't utilize public key of users. To provide authenticity of users the certificates was used for public key namely as "public-key digital certificates" that were mainly used for public key infrastructure (PKI). Mostly, the public key digital certificates were not used for user authentication purpose.

Critical Comments/Findings

In this paper the key concept of Generalized Digital Certificates (GDC) is introduced. Basically a GDC consists of public information of users which contains the driver license of users in digital format and the user birth certificate in digital form. It further requires a digital signature which is signed by a trustworthy certification authority (CA). That's why this approach is used for both discrete logarithm (DL) and integer factoring (IF) supported procedures that can attain secure authentication and obscured key development for the users.

Mukherjee, S et al **[4]**, proposed a secret message communication/transmission between nodes in a cluster based hierarchical wireless sensor networks (WSNs). During node mobility and establishment of an authentication prototype, it was important to verify that the new node that going to join the cluster is an attacker node (compromised node) or not. Based on simulation analysis and experimental results it clarifies that during redistribution process if a node moves from one CH to another then the messages communication were increased with respect to their figure of mobile nodes. After perfect analysis, the results show that the detecting efficiency for the proposed authentication model was .9 → 1 whereas the threshold rate was .02. The message conduction increased during key redistribution process if number of node moves from present CH and joins other CH.

Critical Comments/Findings

Basically this scheme works when the member nodes change their locations and moves from the present cluster head (CH) and joins other CH time to time (rapidly). The method totally depends upon key redistribution process. The new model of watch dog have been introduced in this paper, in this scheme the cluster heads (CHs) is fully responsible and acted as a watch dog and detects the activities of compromised nodes that wants to join the new group.

Yong, L and Zygmunt, J **[17]**, proposed the protected (secure) communication in mobile ad hoc networks (MANETs) that was a big problem due to large amount of nodes in the groups can repeatedly change their positions from one location to other. Typically, this group authentication approach was based on two factors of performance, first one was the overall cost and other was the trustworthiness. The established approach attained successful authentication when the size of one group consists of 10 → 12 nodes approximately per random group.

Critical Comments/Findings

In this approach, the problem of proficient authentication for users is discussed. Basically this proposed approach used the idea of certification authority (CA) that developed arbitrary (randomized) groups for distributing the authentication information between nodes. The main purpose behind this approach is the affluent authentication of groups and the basic purpose of CA is to generate certificates for the member nodes.

Virendra, S and Gaurav, S **[5]**, have been proposed a routing protocol for transmission among network nodes and the successful route was established for data packets delivery. If the whole forwarded packets received successfully by the destination node then it means that the proposed routing protocol is still energetic, alive and not attacked by the adversary. Moreover, the authors developed a routing protocol namely as secure node AODV (SNAODV). It provided a facility for destination nodes to ensure the validity of data packets before receiving it. The key advantage by using this technique was that no data packets were loss during its mobility and transmission. Moreover, this approach increased network throughput by comparing it with SAODV and AODV schemes.

Critical Comments/Findings

Basically in this scheme a single node is fully responsible for sending information in the form of data packets. But if the adversary attacked on that data packet and becomes the packet compromised then subsequently for this purpose a new secure routing protocol is introduced by the authors for efficient transmission and furtive delivery of data packets from home network to foreign network.

Gopalakrishnan, B et al **[11]**, proposed a Transitive Signature Scheme (TSS) for the authentication of mobile nodes by using a routing protocol namely ad hoc on demand distance vector (AODV). The mobile nodes were vivacious, active and self motivated so each and every node can join the new group and leave the present group at own desire. These operations were performed on a particular instance of time instead of performing single rekeying actions.

Critical Comments/Findings

For secure group communication a two way (joint) group key protocol is proposed. The approach guarantees that the performance is completely secured for the data transmission among group members and their neighboring nodes. The experimental results explained that the proposed approach provided better benefits all over different approaches with respect to delay, time, throughput, communication overhead and cost.

Shanthi, N and Ganesan, L **[12]**, proposed a secure hash algorithm-1 (SHA-1) for the routing protocol namely multicast ad hoc on demand distance vector (MAODV). Basically, nodes in the mobile ad hoc networks (MANETs) play the essential function (role) of routers as well as workstations. Furthermore, the routing paths in MANETs are wireless and not fixed as compared to wired networks. In Addition, the SHA-1 algorithm was applied in MANETs for the process of secure communication by using MAODV protocol.

Critical Comments/Findings

The main purpose of this research paper is to discover a sheltered and resourceful transmission in mobile ad hoc networks. Hence, there exists large number of problems in MANETs such as tunneling attacks. In these attacks, huge loss of data packets during node mobility and communication but there is no better approach (solution available) to overcome these types of attacks till yet.

Nagaprasad, S et al **[6]**, explained the idea of multicast routing protocols in mobile ad hoc networks (MANETs). The three key approaches for performance factors were average end to end delay and overhead, packet delivery ratio, and losses of data packet. The simulation was done through ns2 simulator and the results have been explained that DSR approach was much efficient and high-class as compared to DSDV approach. In DSDV if we work on large amount of nodes then the DSDV performance were listless and enervated. Further in DSDV, each and every node maintained a routing table (in which its neighbor node entry is saved) which caused an additional overhead over the network. Multicasting is used to transmit a single message to a select group of receivers. A simple example of multicasting is sending an email message to a mailing list.

Critical Comments/Findings

The key concept of this paper is the relative study of MANETs routing protocols. Moreover, it creates the comparison of DSR and DSDV routing approaches by using the performance features. At the end the accuracy, performance and velocity of DSR is superior as compared to DSDV.

Sumon, K et al [7], explained group based communication structure in mobile ad hoc networks (MANETs). Basically, this paper presented vast study of MANET routing protocols i.e. broadcasting (BCAST) and dynamic source routing (DSR) protocols. Initially, DSR approach was used to indicate the unicast routing approach while BCAST was used to signify the broadcasting protocol. Their performance comparisons were based on two techniques namely random way point mobility structure and shadowing path-loss method. For unicast routing algorithm, N×M unicast relations were maintained if there were N senders and M receivers in the overall network. This caused crucial overhead and increased high load over the network. The simulation was done by using ns2 simulator and the results explained that the broadcast protocol (BCAST) was energetic and robust even in hefty communication environments.

Critical Comments/Findings

This paper basically compares the performance of BCAST and DSR approaches over a group based transmission in MANETs. BCAST is information based enhanced neighbor broadcasting approach due to which delay in active routine is reduced. Furthermore, the transmission overhead and chances of packets dropped is also reduced.

Summary

Mobile Ad hoc Network (MANET) was developed without any prior infrastructure that's why security is always a big issue in it. The above mentioned papers provide different authentication schemes for node mobility. Each paper has its own advantages and limitations but our major focus is to prevent the node becomes compromised by the attacker and to provide power efficient method of authentication for the nodes during their mobility and communication.

Chapter 3

Problem Identification And Proposed Solution

3. PROBLEM DEFINITION AND PROPOSED SCHEME

Mobility is an important aspect of Mobile Ad hoc Networks (MANETs). Due to mobility of nodes from single location to multiple locations security is a big issue in it. It is extremely essential to provide security and to prevent unauthorized access to join the network without its proper authentication and authorization.

Mobile Ad hoc Network (MANET) is developed without any prior infrastructure so if we don't imposed any security feature over MANET then without security an attacker node may join the group easily. Further if the attacker attacks on one node during mobility and become that node compromised then it means that the whole group becomes compromised due to the entrance of that compromised node in a group. Moreover, these compromised nodes easily generate false messages and make the network busy all the time due to lack of security infrastructure.

For this purpose, initially the authentication scenario will be observed for a node who wants to join the new group. After its successful authentication from other side this node allowed to join the group and to access the resources of the network. Therefore, we are using the power efficient authentication mechanism that blocks the entrance of compromised nodes in a group.

3.1 Problem Identification

During Node Mobility, when a node moves out of one group and joins the other group then it may possible that an attacker attacks on the node and killed the node. Furthermore, if the attacker takes mobile device (in which node's certificate is stored) of the node then by using this mobile device an attacker can easily joins other group without its proper authentication and authorization.

Another issue in Node Mobility is if a node leaves one group then its correlated information is cleared only from its affiliated GR. But the neighboring nodes still contains the information of this node in their neighbors list and hence will be contacted in future elections. It will cause an overhead to locate that which nodes have left the group and increases the communication overhead.

3.2 Problem Scenario

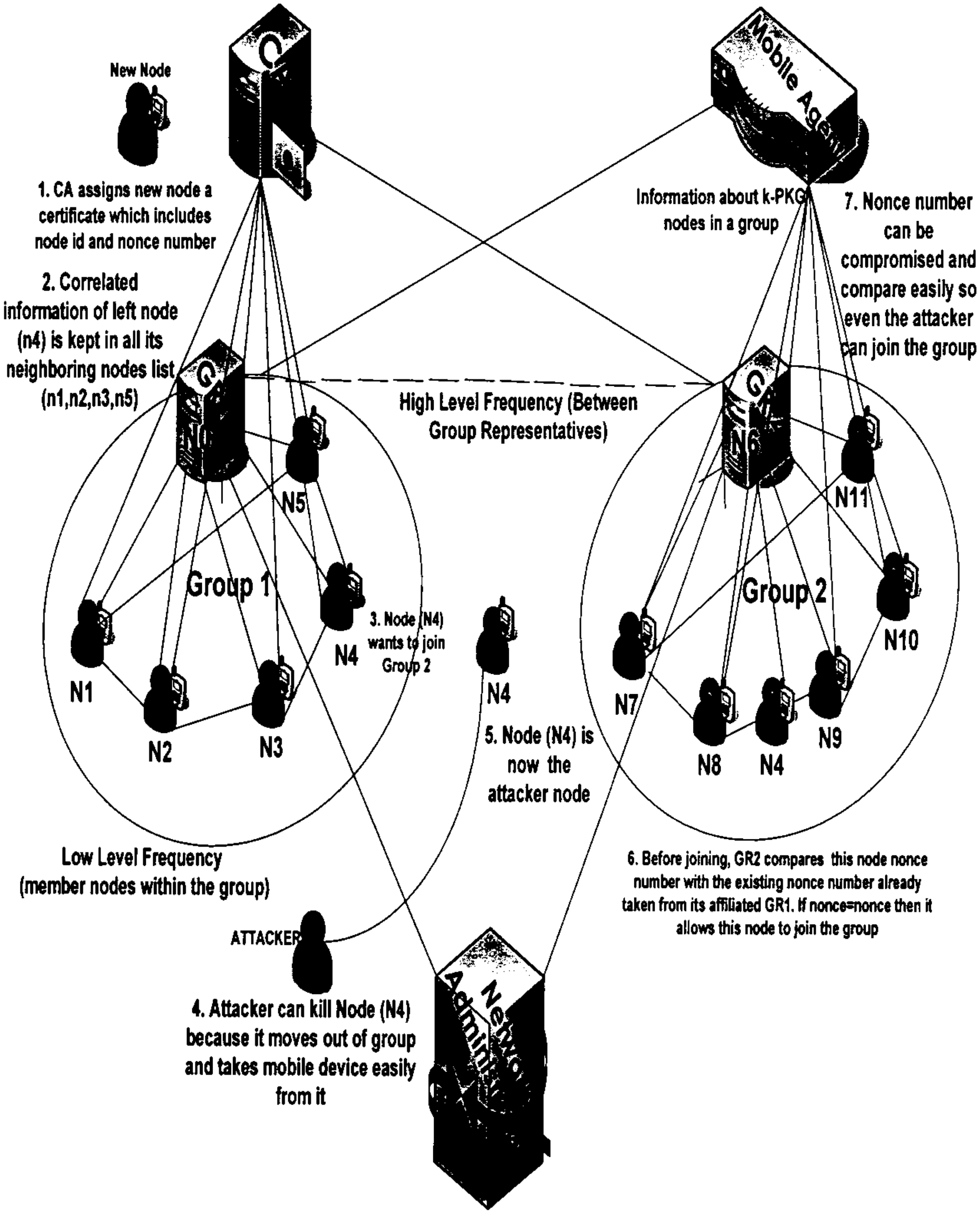

New Node
CA
1. CA assigns new node a certificate which includes node id and nonce number
2. Correlated information of left node (n4) is kept in all its neighboring nodes list (n1,n2,n3,n5)
Mobile Agent
Information about k-PKG nodes in a group
7. Nonce number can be compromised and compare easily so even the attacker can join the group
GR1
N6
GR2
N6
High Level Frequency (Between Group Representatives)
N5
Group 1
N1
N2
N3
N4
3. Node (N4) wants to join Group 2
N4
5. Node (N4) is now the attacker node
Group 2
N11
N10
N7
N8
N4
N9
Low Level Frequency (member nodes within the group)
6. Before joining, GR2 compares this node nonce number with the existing nonce number already taken from its affiliated GR1. If nonce=nonce then it allows this node to join the group
ATTACKER
4. Attacker can kill Node (N4) because it moves out of group and takes mobile device easily from it
Network Administrator

Figure 3-1: Problem Scenario of Node Mobility in MANETs

According to *figure.3-1*, each node (node) has a self assigned public key which is known only to GR. Each new node allocates a mobile device in which Certification Authority (CA) embedded this node certificate which includes node id and its nonce number. All of this information is certified in node allocated mobile device. At the time of joining, GR compares this nonce number with the existing nonce number which GR has already given to him. If the information matches successfully (nonce=nonce) then the GR allows a new node to join the group otherwise not. Mobile agent is a program segment that collects information about PKG (trustworthy nodes) in a group and information about the nodes whose certificates are expired. Incase if any node certificate is expired then it will be issued again by certification authority. Symmetric encryption is used between group representatives as well as used between group member nodes.

The key problem in the scheme is that if a node leaves the present group and joins other group then it may possible that an attacker attacks on the node and killed this nodes further if the attacker takes mobile device of this node in which its security credentials are stored then by using this mobile device attacker can join other group successfully. At the time of joining, the GR of the targeted group compares this node nonce number with the information he already taken from its affiliated GR. If the nonce number compares successfully with the stored nonce number then it allows this node to join the group otherwise not. The reason behind this whole process is that authentication in the above scenario is totally based on the nonce/random number which can be easily compromised by the attacker anytime during node mobility and communication thus the authentication used in this scheme is much weaker and not strong enough because even compromised nodes can join the group.

Another problem in the above mentioned scenario is if a node leaves one group and joins other group then its information is cleared only from its affiliated GR but the correlated information is stored still in its attached neighboring nodes lists and hence this left node will be called for future elections. Only concern GR knows that which node has left the group but neighboring nodes don't know about that leaving node. This will caused a communication overhead because the entry of this left node is available in its neighboring nodes lists so each time these neighboring nodes generate messages for communication with this left node and with no reply from his side these nodes will generate message again and again after some interval of time. Furthermore, due to the unnecessary generation of messages caused higher load/overhead on the network and all time channel is busy.

3.3 Proposed Solution

The secure biometric authentication approach (image recognition) is proposed for node mobility to overcome the authentication and authorization problem of a compromised soldier (attacker) having a mobile device and wants to join the other group. At the time of joining, the GR of targeted group takes this soldier image again and compares this soldier certificate information (login id, password, image) with the original stored information he already taken from its affiliated GR. If this soldier new information (login, password, image) matches correctly with the existing stored information (login, password, image) then the GR authenticates this soldier and allow the soldier to join the group otherwise GR doesn't allow him to join his group.

To reduce communication cost and overhead in node mobility scheme a backlog clearance algorithm by using dynamic source routing (DSR) approach will be used to remove leaving node entry from their neighboring node lists. Hence the backlog of leaving node will be cleared when the GR receives the node attachment reply from the GR of targeted group.

As a result, by using our proposed scheme updates the neighboring lists as well as provides security (secure authentication and authorization) and diminished the entrance of compromised nodes to join the group.

3.4 Proposed Scenario

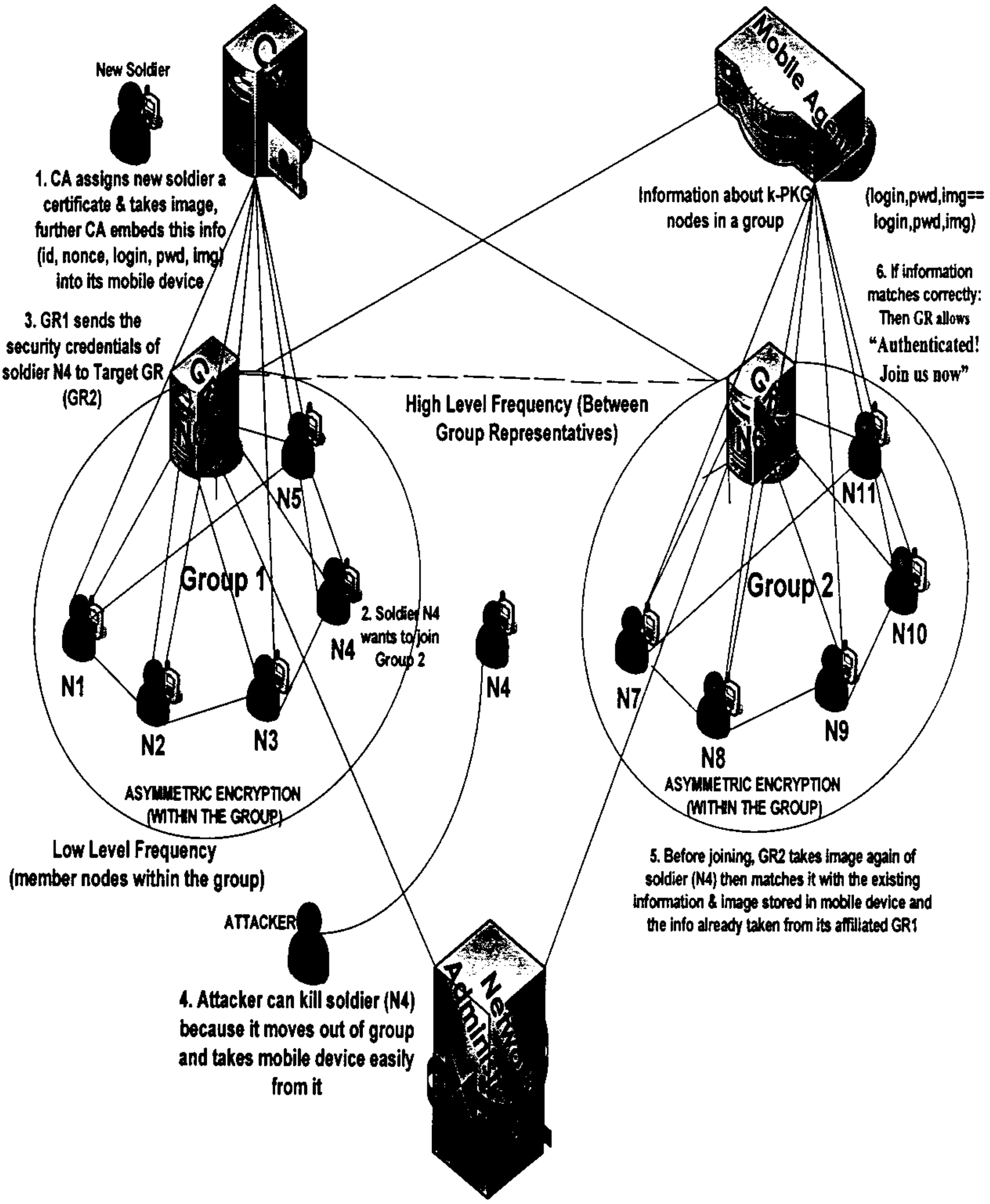

CA
New Soldier
1. CA assigns new soldier a certificate & takes image, further CA embeds this info (id, nonce, login, pwd, img) into its mobile device
3. GR1 sends the security credentials of soldier N4 to Target GR (GR2)
Mobile Agent
Information about k-PKG nodes in a group
(login,pwd,img== login,pwd,img)
6. If information matches correctly: Then GR allows "Authenticated! Join us now"
High Level Frequency (Between Group Representatives)
N5
Group 1
N1
N2
N3
N4
2. Soldier N4 wants to join Group 2
N4
Group 2
N6
N11
N10
N7
N8
N9
ASYMMETRIC ENCRYPTION (WITHIN THE GROUP)
ASYMMETRIC ENCRYPTION (WITHIN THE GROUP)
Low Level Frequency (member nodes within the group)
ATTACKER
4. Attacker can kill soldier (N4) because it moves out of group and takes mobile device easily from it
5. Before joining, GR2 takes image again of soldier (N4) then matches it with the existing information & image stored in mobile device and the info already taken from its affiliated GR1
Network Administrator

Figure 3-2: Node Mobility in Mobile Ad hoc Networks

According to *figure.3-2*, each node (soldier) has a self assigned public key which is known only to GR. Each new soldier allocates a mobile device in which Certification Authority (CA) embedded this soldier certificate which includes soldier id, nonce number, login id, password, and its image. All of this information is endorsed in soldier allocated mobile device in encrypted format. Each time CA assigns a certificate (id, nonce, login, password and image) to each new soldier that wants to join the group; in addition, CA stores/embeds this whole information (soldier's certificate) into soldier allocated mobile device. Further, CA sends this soldier information to its affiliated Group Representative (GR) for authentication and authorization purpose. At the time of joining, GR takes image again of this soldier and matches it with the existing information which CA has already given to him. If the information matches successfully then the GR allows a new node (soldier) to join the group otherwise not. Asymmetric encryption is used between group representatives as well as used between group member nodes.

If a soldier wants to move from one group and joins other group, First, its affiliated GR sends the registration request (RREQ) message + security credentials about that soldier (who wants to move) to the GR of targeted group. After receiving the message and security credentials of this soldier, Target GR sends a registration reply (RREP) message to affiliated GR of that soldier. Soldier moves from one group and join other group. In case, if a soldier is attacked by attacker before it joins the new group and attacker takes mobile device of that soldier then with the help of this mobile device an attacker can easily joins other group without its authentication and authorization. For this purpose, before a soldier joins the new group, GR of targeted group takes image of that soldier (who wants to join the group) and match this new image with its existing mobile device information (certificate is stored by CA), further Target GR matches the same information (login, password and image) which he has already taken from its affiliated GR. If the information matches correctly (login, password, image == login, password, image) then GR authenticates the soldier to join the group otherwise GR doesn't allow him to join the group.

When a node (soldier) leaves one group and joins other group then its related information is cleared only from its affiliated GR but the correlated information is stored still in its neighboring nodes lists which caused the communication overhead and hence this left node will be called for future elections. Only concern GR knows that which node has left the group but neighboring nodes don't know about that leaving node. For this purpose, to reduce communication cost and overhead a backlog clearance algorithm by using dynamic source routing (DSR) approach will be used to remove leaving node entry from the neighboring nodes lists. Hence, the backlog of leaving node will clear when the GR receives the node attachment reply from the GR of targeted group.

3.5 Proposed Algorithms

The algorithms for backlog clearance, node joining, node migration and node leaving by using secure biometric authentication approach (image recognition) for the proposed scheme is listed below in detail.

3.5.1 Backlog Clearance Algorithm

```
Procedure CLEAR_LOGINFO_GR ($ID_N$)        // backlog clearance from GR

Begin
        for i: = 1 to n do                 where n = no. of group members
        GR→N: $E_{K_{GN}}$ {$ID_{GR}$, R, req_clear}
        end for
                a. Remove the trust value of this node.
                b. Discard the routing paths via this node.
                c. Remove its nonce value R.
                d. Remove its certificate Cert.
                e. Remove its public key.

End CLEAR_LOGINFO_GR

Procedure CLEAR_LOGINFO_NODE ($ID_N$)      // backlog clearance from Neighbors

Begin
                a. Remove the trust value of this node.
                b. Discard the routing paths via this node.

End CLEAR_LOGINFO_NODE
```

Steps:

In Backlog Clearance Algorithm, Group Representatives (GRs) calls the **CLEAR_LOGINFO_GR (ID_N)** procedure to clear the backlog information of the migrated/left node after getting a node attachment reply from GR of targeted group.

The following information of left node will be removed by the GR.

1- The trust value of the left node is removed.

2- All routing paths via this node are removed and then source routing will be done again which selects the next shortest path.

3- The node nonce value and certificate will also be removed.

All neighboring nodes call the **CLEAR_LOGINFO_NODE (ID_N)** procedure for removing the left node entry. The neighboring nodes clear the following information.

1- Trust value of the left node is removed by every neighbor node.

2- All routing paths via this node are removed and then source routing will be done again which selects the next shortest path.

3.5.2 Node Joining Algorithm

Each node (soldier) has allocated a separate mobile device (mentioned in figure 3-2) that is physically connected with the Certification Authority (CA). CA assigns certificate (node id, nonce number, login id, password and image) for the new node that wants to join the group. This whole information embeds into soldier allocated mobile device further CA sends the same information to the node affiliated group representative (GR) for authentication and authorization purpose. We used the concept of image hashing for the purpose of node authentication.

The algorithm for node joining using secure biometric authentication approach (image recognition) is as follows:

1. $CA \rightarrow GR_i$: EK_{CG} (REQ ($ID_N||R||login||PU_N||pwd||H(IMG_N)$, $Cert_N$))

2. $GR_i \rightarrow CA$: EK_{GC} (REP ($ID_N||R$))

3. $N \rightarrow GR_i$: EK_{NG} (REQ ($ID_N||R||login||pwd||PU_N||H(IMG_N)$))

4. if ($login||pwd||H(IMG_N)$) equals ($login||pwd||H(IMG_C)$) equals ($login||pwd||H(IMG_{GR})$)

    4.a $GR_i \rightarrow N$: EPU_N (REP_AUTHENTICATED)

```
    else
            4.b    $GR_i \rightarrow N: E_{PU_N}$ (REP_NOT_AUTHENTICATED)
    end if
5.  $GR_i$: KEY_ESTAB ($ID_N$)
```

Step 1: Certification Authority *CA* sends the node id ID_N, nonce value *R*, login id *login*, password *pwd* and public key PU_N of the node to group representative (GR). Further, CA binds all of this information into a certificate $Cert_N$ that includes hash of image of the node $H(IMG_N)$ encrypted using *KCG* which is public key established between certification authority and group representative.

Step 2: *GR* sends reply message to *CA* that the information of node (ID_N, *R*) is received successfully. Basically the nonce value *R* avoids from replay attack.

Step 3: Node *N* sends authentication request message encrypted using public key of *GR* to group representative. The message includes node id ID_N, nonce value *R*, login id *login*, password *pwd*, public key PU_N and hash of image of the node image $H(IMG_N)$.

Step 4: Before the node *N* joins the group, GR_i compares this node information (*login*, *pwd*, $H(IMG_N)$ with the information he already taken from the CA (*login*, *pwd*, $H(IMG_N)$. Further, GR_i takes image of this node *N* and calculates its hash value and matches it with the stored information. Where IMG_C is the image given by CA, IMG_N is the image of node and IMG_{GR} is the new image taken again of the node by GR. If the information matches successfully then the GR_i sends encrypted message to authenticate the node *N* to join the group otherwise GR_i doesn't allow the node *N* to join the group.

Step 5: GR_i calls the KEY_ESTAB function for the node N.

3.5.3 Node Migration Algorithm

Members may leave the present group and moving into another group instead of leaving the group. In this scenario which is called migration, it is not necessary to update the group key because the node is still a valid member of the group. In node migration two different scenarios will be observed. In the first scenario, node will move if network administrator (NA) will order him. In second scenario, a node will move at own desire.

The node migration algorithm for these two scenarios using secure biometric authentication approach (image recognition) is as follows:

Scenario # 1:

- **Network Administrator (NA) orders the node to move from present group and join other group**

Network Administrator (NA) orders any node to move from the present group and joins other group. NA asks to the node affiliated group representative (GR) then the GR further asks the specific node to rove from the present group and joins other group.

For example:

When a posting order generated from the head quarters on demand then the soldier will be transferred from present group and join the new group.

Scenario # 2:

- **Node wants to move from the present group at own desire**

If a node wants to move from the present group then it reports to its group representative (GR). The GR allows the node to move from the present group and joins other group.

For example:

Without any posting orders, any soldier in group sends a request message to its affiliated GR that he wants to leave the present group at his own will.

Scenario # 1: Network Administrator (NA) orders the node to move from present group and join other group

The node migration algorithm for scenario # 1 is as follows:

<table>
<tr><th>SENDER</th><th>RECIEVER</th></tr>
<tr><td>1. NA→GR$_i$: EK$_{NG}$ (REQ (ID$_N$||R||node_mig_req))</td><td></td></tr>
<tr><td>2. GR$_i$→N: EK$_{GN}$ (REQ (ID$_N$||R||node_mig_req))</td><td></td></tr>
<tr><td>3. N→GR$_i$: EK$_{NGi}$ (REP (ID$_N$||R)</td><td></td></tr>
<tr><td>4. GR$_i$→GR$_j$: EK$_{GiGj}$ (REQ (ID$_N$||R||login||pwd|| H(IMG$_N$), Cert$_N$)</td><td>5. GR$_j$→GR$_i$: EK$_{GjGi}$ (REP (ID$_N$||R)</td></tr>
<tr><td></td><td>6. N→GR$_j$: (REQ (ID$_N$||R||login|| pwd|| H(IMG$_N$)))</td></tr>
<tr><td></td><td>7. if (login||pwd||H(IMG$_C$)) equals (login||pwd||H(IMG$_N$)) equals (login||pwd||H(IMG$_{GR}$))
{
GR$_j$→N:
EPU$_N$ (REP_AUTHENTICATED)
else
GR$_j$→N:EPU$_N$
(REP_NOT_AUTHENTICATED)
}</td></tr>
<tr><td></td><td>8. GR$_j$: KEY_ESTAB (ID$_N$)</td></tr>
<tr><td>10. GR$_i$: CLEAR_LOGINFO_GR (ID$_N$)</td><td>9. GR$_j$→GR$_i$: EK$_{GjGi}$
(REP (“NODE_JOIN_REPLY”))</td></tr>
<tr><td>11. GR$_i$: CLEAR_LOGINFO_NODE (ID$_N$)</td><td></td></tr>
</table>

Step 1: Network Administrator *NA* sends a migration request message to the node affiliated group representative *GR$_i$* encrypted using *KNG* which is public key established between the network administrator and group representative.

Step 2: *GR_i* further forwards this migration request message to the specific node *N.*

Step 3: Node *N* sends a reply message to its affiliated *GR_i.*

Step 4: GR_i sends the node information/security credentials to GR_j. The information includes node ID *ID_N,* nonce value *R,* login id *login,* password *pwd,* hash of image of the node *$H(IMG_N)$* and its certificate $Cert_{N.}$

Step 5: GR_j sends a reply message to GR_i that the information is received successfully.

Step 6: In addition, a node *N* also sends a authentication request message which includes *(ID_N, R, login, pwd, $H(IMG_N)$)* to $GR_{j.}$

Step 7: Before the node *N* joins the group, *GR_j* compares this node information *(login, pwd, $H(IMG_N)$* with the information he already taken from its affiliated group representative *GR_i (login, pwd, $H(IMG_N)$*. Further, GR_j takes image of this node *N* and calculates its hash value and matches it with the stored information. Where *IMG_C* is the image taken from its group representative *GR_i, IMG_N* is the image of node and *IMG_{GR}* is the new image taken again of this node. If the information matches successfully then the GR_j sends encrypted message to authenticate the node *N* to join the group otherwise GR_j doesn't allow the node *N* to join the group.

Step 8: *GR_j* calls the KEY_ESTAB function for the node *N.*

Step 9: GR_j sends a reply message to GR_i that your node has joined our group.

Step 10: After receiving the node attachment reply message from GR_j, GR_i calls the CLEAR_LOGINFO_GR function to clear this node information from its own member list.

Step 11: Further GR_i calls the CLEAR_LOGINFO_NODE function to clear this node information from all its neighboring nodes lists.

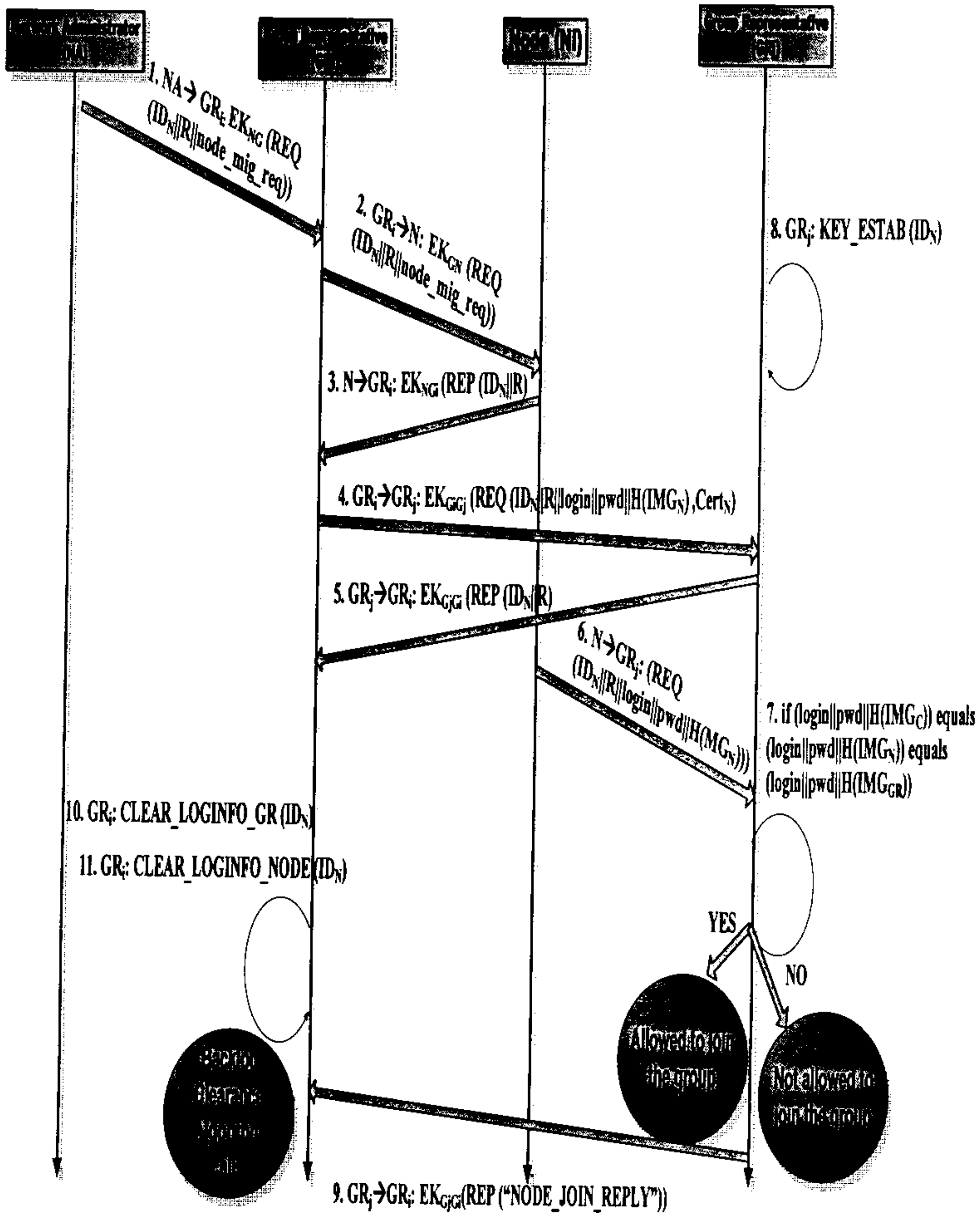

Administrator
Representative
Node (ND)
Representative
1. NA → GR_i: EK_{NG} (REQ (ID_N||R||node_mig_req))
2. GR_i → N: EK_{GN} (REQ (ID_N||R||node_mig_req))
3. N → GR_i: EK_{NG} (REP (ID_N||R)
4. GR_i → GR_j: EK_{GiGj} (REQ (ID_N||R||login||pwd||H(IMG_N),$Cert_N$)
5. GR_j → GR_i: EK_{GjGi} (REP (ID_N||R)
6. N → GR_j: (REQ (ID_N||R||login||pwd||H(IMG_N)))
7. if (login||pwd||H(IMG_C)) equals (login||pwd||H(IMG_N)) equals (login||pwd||H(IMG_{GR}))
8. GR_j: KEY_ESTAB (ID_N)
YES
NO
Allowed to join the group
Not allowed to join the group
9. GR_j → GR_i: EK_{GjGi}(REP ("NODE_JOIN_REPLY"))
10. GR_i: CLEAR_LOGINFO_GR (ID_N)
11. GR_i: CLEAR_LOGINFO_NODE (ID_N)

Figure 3-3: Hierarchical Structure of NA orders the node to move from present group

Scenario # 2: Node wants to move from the present group at own desire

The node migration algorithm for scenario # 2 is as follows:

<table>
<tr><th>SENDER</th><th>RECIEVER</th></tr>
<tr><td><b>1.</b> $N \rightarrow GR_i$: EK_{NG} (REQ (ID_N||R||node_mig_req))
<b>2.</b> $GR_i \rightarrow N$: EK_{GN} (REP (ID_N||R))
<b>3.</b> $GR_i \rightarrow GR_j$: EK_{GiGj} (REQ (ID_N||R||login||pwd|| H(IMG_N), $Cert_N$)</td><td></td></tr>
<tr><td></td><td><b>4.</b> $GR_j \rightarrow GR_i$: EK_{GjGi} (REP (ID_N||R)
<b>5.</b> $N \rightarrow GR_j$: (REQ (ID_N||R||login|| pwd|| H(IMG_N)))
<b>6.</b> if (login||pwd||H(IMG_C)) equals (login||pwd||H(IMG_N)) equals (login||pwd||H(IMG_{GR}))
{
$GR_j \rightarrow N$:
EPU_N (REP_AUTHENTICATED)
else
$GR_j \rightarrow N$:EPU_N (REP_NOT_AUTHENTICATED)
}
<b>7.</b> GR_j: KEY_ESTAB (ID_N)
<b>8.</b> $GR_j \rightarrow GR_i$: EK_{GjGi} (REP ("NODE_JOIN_REPLY"))</td></tr>
<tr><td><b>9.</b> GR_i: CLEAR_LOGINFO_GR (ID_N)
<b>10.</b> GR_i: CLEAR_LOGINFO_NODE (ID_N)</td><td></td></tr>
</table>

Step 1: Node *N* sends a migration request message to its affiliated group representative *GR_i* encrypted using *KNG* which is public key established between the node and group representative.

Step 2: GR_i sends a reply message to node *N*.

Step 3: GR_i sends the node information/security credentials to GR_j. The information includes node ID ID_N, nonce value *R*, login id *login*, password *pwd*, hash of image of node IMG_N and its certificate $Cert_N$.

Step 4: GR_j sends a reply message to GR_i that the information is received successfully.

Step 5: In addition, a node *N* also sends a join request message which includes $(ID_N$, *R*, *login*, *pwd*, $H(IMG_N))$ to GR_j.

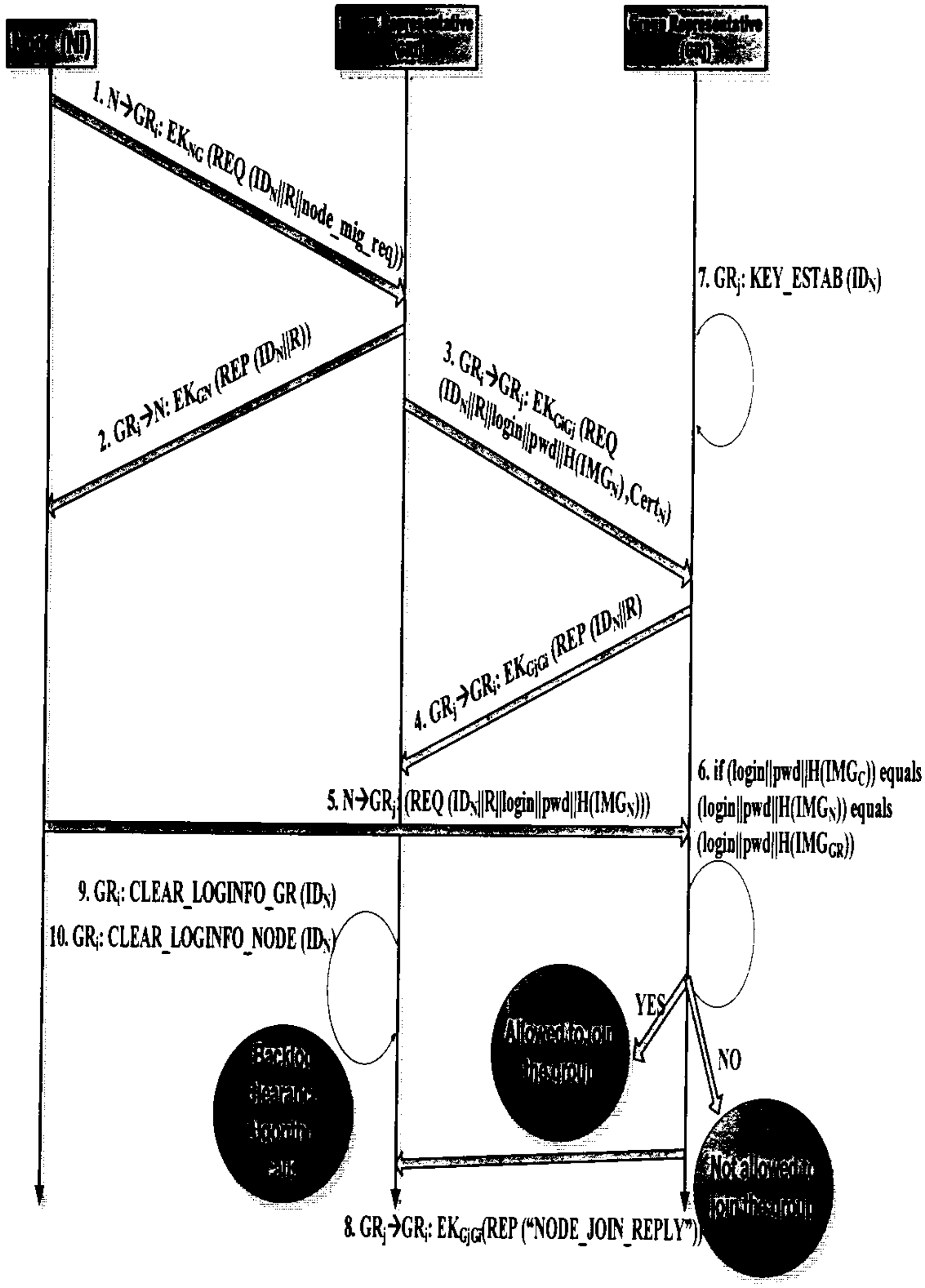
Step 6: Before the node *N* joins the group, GR_j compares this node information (*login*, *pwd*, $H(IMG_N)$ with the information he already taken from its affiliated group representative GR_i (*login*, *pwd*, $H(IMG_N)$. Further, GR_j takes image of this node *N* and calculates its hash value and matches it with the stored information. Where IMG_C is the image taken from its group representative GR_i, IMG_N is the image of node and IMG_{GR} is the new image taken again of this node. If the information matches successfully then the GR_j sends encrypted message to authenticate the node *N* to join the group otherwise GR_j doesn't allow the node *N* to join the group.

Step 7: GR_j calls the KEY_ESTAB function for the node *N*.

Step 8: GR_j sends a reply message to GR_i that your node has joined our group.

Step 9: After receiving the node attachment reply message from GR_j, GR_i calls the CLEAR_LOGINFO_GR function to clear this node information from its own member list.

Step 10: Further GR_i calls the CLEAR_LOGINFO_NODE function to clear this node information from all its neighboring nodes lists.



(NI)
Representative
Group Representative
1. N→GR_i: EK_{NG} (REQ (ID_N||R||node_mig_req))
2. GR_i→N: EK_{GN} (REP (ID_N||R))
3. GR_i→GR_j: EK_{GiGj} (REQ (ID_N||R||login||pwd||H(IMG_N),$Cert_N$)
4. GR_j→GR_i: EK_{GjGi} (REP (ID_N||R)
5. N→GR_j (REQ (ID_N||R||login||pwd||H(IMG_N)))
6. if (login||pwd||H(IMG_C)) equals (login||pwd||H(IMG_N)) equals (login||pwd||H(IMG_{GR}))
7. GR_j: KEY_ESTAB (ID_N)
YES
NO
Allowed to join the group
Not allowed to join the group
8. GR_j→GR_i: EK_{GjGi}(REP ("NODE_JOIN_REPLY"))
9. GR_i: CLEAR_LOGINFO_GR (ID_N)
10. GR_i: CLEAR_LOGINFO_NODE (ID_N)
Back to clearance Algorithm

Figure 3-4: Hierarchical Structure of node move from present group at own desire

3.5.4 Node Leaving Algorithm

If a node wants to leave the present group then two different scenarios will be observed. In the first scenario, node will leave the group if network administrator will order him. In second scenario, a node will leave the group at own desire. After a node leaves the group, this node information will be cleared from its affiliated GR and all its neighboring nodes lists.

The node leaving algorithm for these two scenarios using secure biometric authentication approach (image recognition) is as follows:

- **Scenario # 1: Network Administrator (NA) orders the node to leave the present group**

Network Administrator (NA) orders any node to leave from the present group. For this purpose, NA asks to the node affiliated group representative (GR) then the GR further asks the specific node to leave the group.

The node leaving algorithm for Scenario # 1 is as follows:

1. $NA \rightarrow GR_i$: EK_{NG} (REQ (ID_N||R||node_leave_req))
2. $GR_i \rightarrow N$: EK_{GN} (REQ (ID_N||R||node_leave_req))
3. $N \rightarrow GR_i$: EK_{NG} (REP (ID_N||R||LEAVE_REPLY)
4. GR_i: CLEAR_LOGINFO_GR (ID_N)
5. GR_i: CLEAR_LOGINFO_NODE (ID_N)

Step 1: Network Administrator *NA* sends a leaving request message (node_leave_req) to the node affiliated group representative GR_i encrypted using *KNG* which is public key established between the network administrator and group representative.

Step 2: GR_i further forwards this leaving request message to specific node *N*.

Step 3: Node *N* sends a reply message to its affiliated GR_i.

Step 4: GR_i calls the CLEAR_LOGINFO_GR function to clear this left node *N* information from its own member list.

Step 5: Further GR_i calls the CLEAR_LOGINFO_NODE function to clear this left node *N* information from all its neighboring nodes lists.

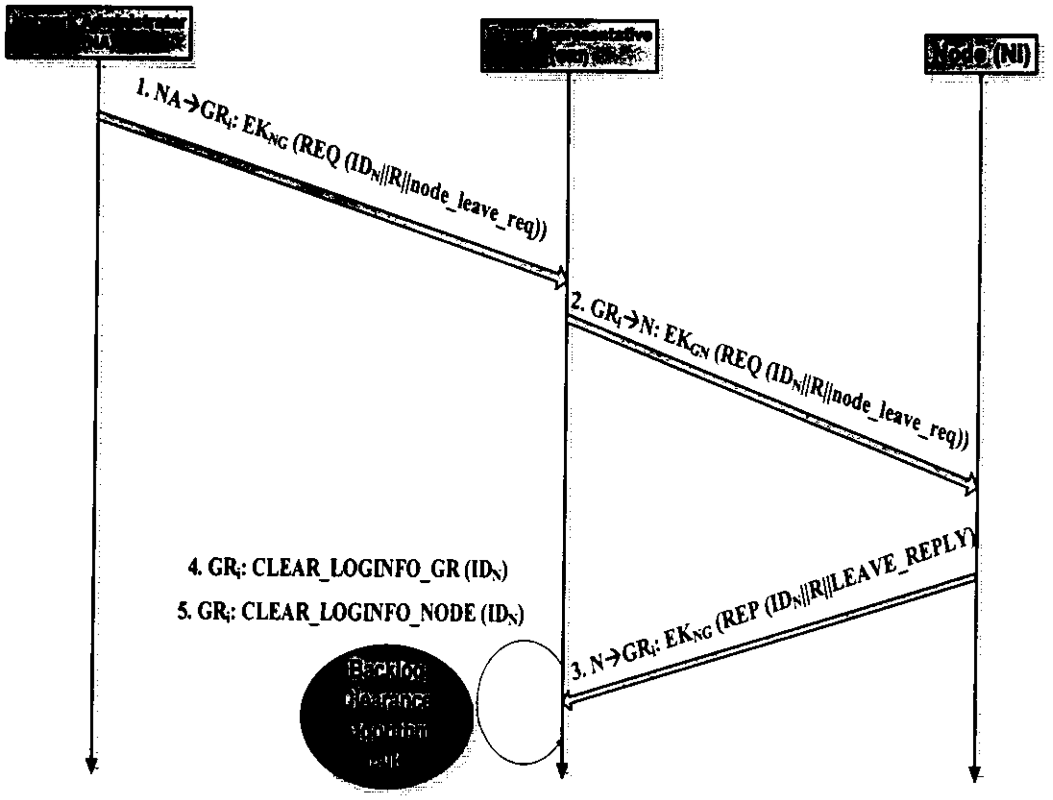

Node (NI)
1. NA→GRi: EKNG (REQ (IDN||R||node_leave_req))
2. GRi→N: EKGN (REQ (IDN||R||node_leave_req))
3. N→GRi: EKNG (REP (IDN||R||LEAVE_REPLY))
4. GRi: CLEAR_LOGINFO_GR (IDN)
5. GRi: CLEAR_LOGINFO_NODE (IDN)

Figure 3-5: Hierarchical Structure of NA orders node to leave the present group

- **<u>Scenario # 2</u>: Node wants to leave the present group at own desire**

If a node wants to leave the present group then it reports to its group representative (GR). The GR allows the node to leave from the present group.

The node leaving algorithm for Scenario # 2 is as follows:

1. N→GR$_i$: EK$_{NG}$ (REQ (ID$_N$||R||node_leave_req))
2. GR$_i$→N: EK$_{GN}$ (REP (ID$_N$||R||LEAVE_REPLY))
3. GR$_i$: CLEAR_LOGINFO_GR (ID$_N$)
4. GR$_i$: CLEAR_LOGINFO_NODE (ID$_N$)

Step 1: Node *N* sends a node leaving request (node_leave_req) to its affiliated group representative *GR$_i$* encrypted using *KNG* which is public key established between the node and group representative.

Step 2: GR$_i$ sends a reply message to node *N*.

Step 3: GR$_i$ calls the CLEAR_LOGINFO_GR function to clear this left node *N* information from its own member list.

Step 4: Further GR$_i$ calls the CLEAR_LOGINFO_NODE function to clear this left node *N* information from all its neighboring nodes lists.

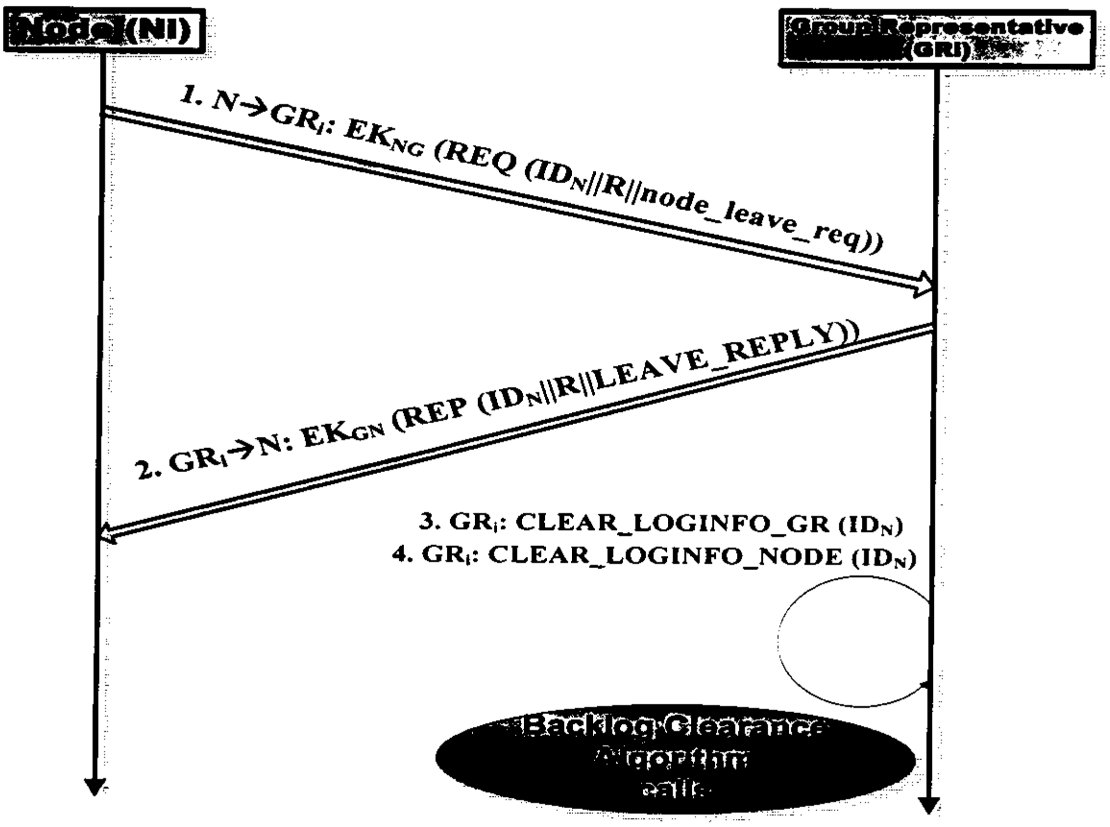

Node (NI)
Group Representative (GRI)
1. N→GR$_i$: EK$_{NG}$ (REQ (ID$_N$||R||node_leave_req))
2. GR$_i$→N: EK$_{GN}$ (REP (ID$_N$||R||LEAVE_REPLY))
3. GR$_i$: CLEAR_LOGINFO_GR (ID$_N$)
4. GR$_i$: CLEAR_LOGINFO_NODE (ID$_N$)
Backlog Clearance Algorithm calls

Figure 3-6: Hierarchical Structure of node leaves present group at own desire

Chapter 4

Simulation Results And Analysis

4. SIMULATION RESULTS AND ANALYSIS

In this chapter the simulation details of this research work has been discussed and explained by graphs.

4.1 Network Simulator (NS-2)

The secure group based biometric authentication approach (image recognition) during node mobility and communication is entirely simulated in Network Simulator version 2 (NS-2). NS 2 is available with Fedora 14 operating system.

4.2 TCL Class

The TCL (Tool Command Language) class reviews the authentic instance of OTCL (Object Tool Command Language) interpreter and provides the proper way to communicate with that interpreter [23]. Basically, this class presents some key methods for the following operations.

1. Attain an indication to the Tcl occurrence.
2. Cited OTcl proceedings and events throughout the interpreter.
3. Improve consequences (results) to the interpreter.
4. Give detail of error conditions and then depart in a homogeneous manner.
5. Acquire immediate (instant) access to the interpreter.
6. Explore and seek out the *TclObjects*.

4.3 NS-2 Objectives

The goals/objectives [23] of Network simulator (NS-2) includes:

1. Protocol plan and procedures etc.
2. Protocol association.
3. Innovative structural designs are also supported.
4. To provide mutual surroundings.
5. Liberally disseminated and open foundation etc.
6. Enlarge assurance in outcome (results).

4.4 Simulation Parameters

Simulation of the work has been implemented on Network Simulator (NS-2) by using Fedora 14 operating system. In simulation two (02) groups have been proposed. The network consists of 13 nodes. Both groups contain six (06) nodes each in which first node of each group stated as group representative (GR). The thirteenth node is known as certification authority (CA). The scenario dimension is 1000*1000 (meters). The traffic type is constant bit rate (CBR) and the overall simulation time is 35 seconds.

Following parameters are chosen for simulation:

Parameters	Value
Simulation area	NS 2
Number of groups	02
No of GRs	02
Number of nodes	13
Simulation duration	35 seconds
Routing protocol	DSR
Scenario dimension	1000m × 1000m
Traffic type	CBR
Node velocity	4500 mps
MAC	802_11
Message port	42
Message size	100

Table 4-1: Simulation Setup

4.5 Proposed Simulation Procedure

A simulation procedure consists of different phases. These phases are categorized below in detail:

4.5.1 Node Deployment

According to our simulation in *figure.4-1*, two (02) groups have been proposed in node deployment strategy. Each group contained six (06) nodes. First group contains nodes namely Node 0,1,2,3,4,5 and second group contains nodes namely Node 6,7,8,9,10,11. In the first group, Node 0 is stated as Cluster Head (CH1) and the remaining 05 nodes (n1, n2, n3, n4, n5) are the normal nodes of that group. In the second group, Node 6 is stated as Cluster Head (CH2) and the remaining 05 nodes (n7, n8, n9, n10, n11) are the normal nodes of that group. In addition; Node 12 is represented as Certification Authority (CA).

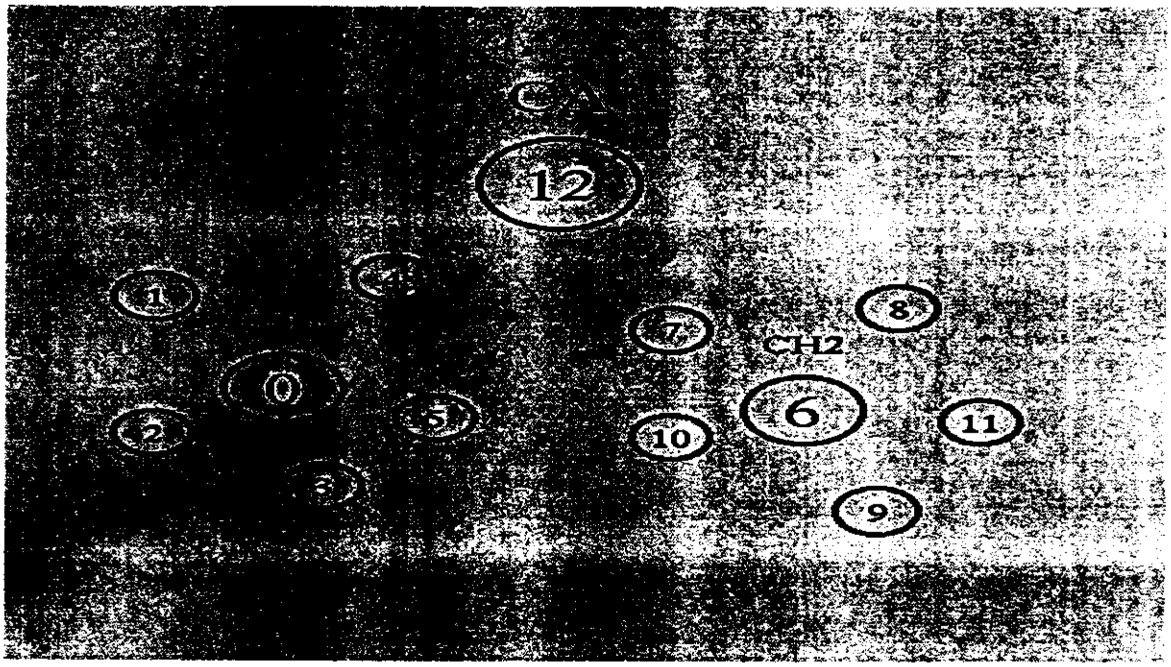


Figure 4-1: Node Deployment Strategy

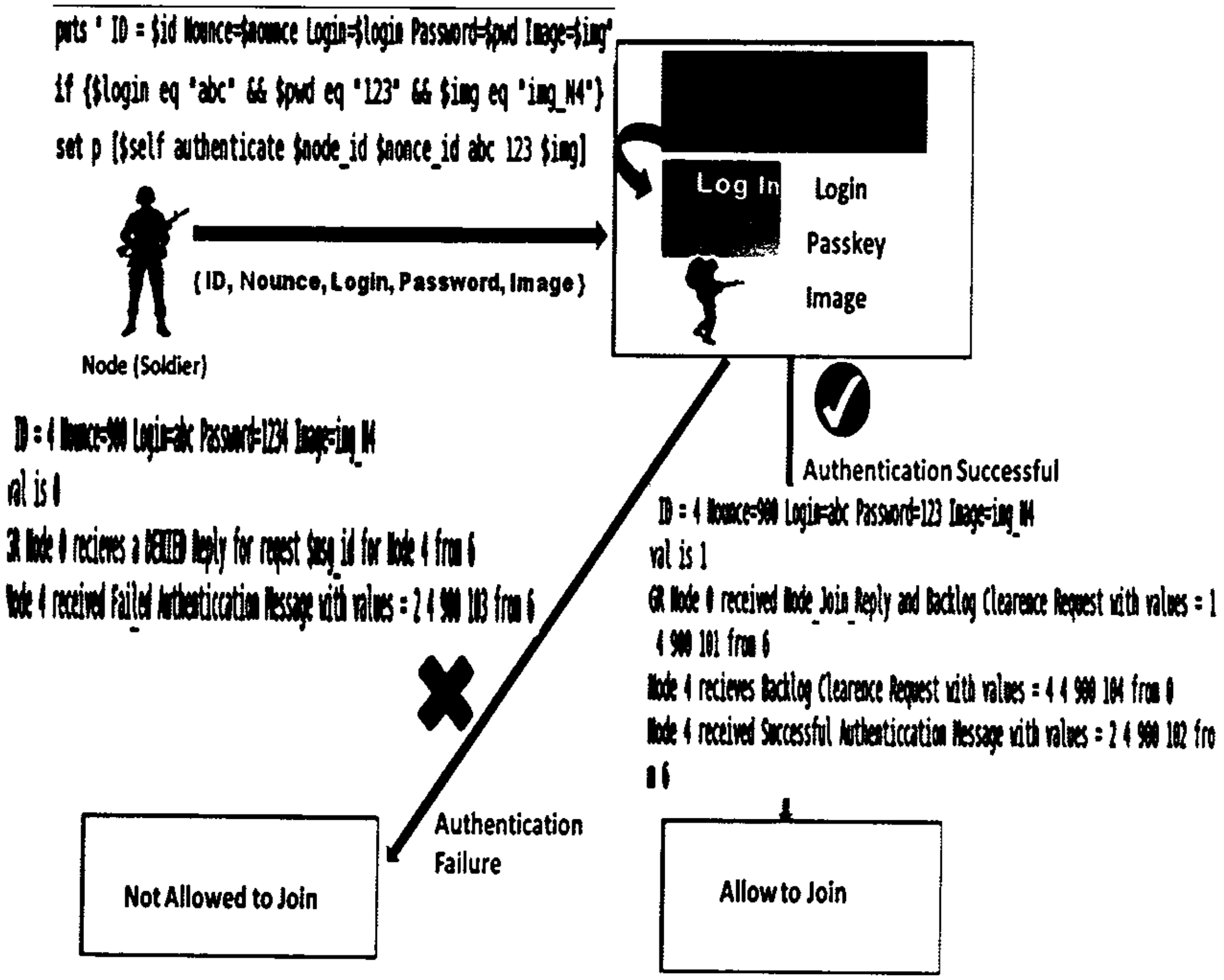
4.5.2 Node Joining Strategy using Biometric Authentication

In node joining scheme *figure.4-2*, a new node will be added in the group and its authentication scenario will be observed. If a node in one group wants to move from the present group and join other group then the authentication of this leaving node will be done by using biometric authentication approach before it joins the new group.

For this purpose, Certification Authority (CA) assigns a certificate to a new node that wants to join the group. The certificate contains node id, nonce value, login, password and image of the node who wants to join the group. Furthermore, CA sends this information to node affiliated GR for mobility and communication. If any node wants to leave present group and joins new group then it sends a request message to its affiliated GR. Further this GR forwards all of its security credentials to GR of targeted group. After receiving a reply message from targeted GR to the node affiliated GR the specific node move from present group and joins new group. Before the node joins the new group the targeted GR compares the node information with the information he already taken from its affiliated GR. If the login, passkey and image of the node compares with the stored node login, passkey and image then it means the node is not compromised and it authenticates the node to join his group and sends a node attachment reply message to the

GR of targeted group that your node has join our group after its successful authentication. But if the login, passkey and image of the node is not authenticated then the target GR doesn't allow this node to join the group.

The underneath simulation shows that how our proposed secure biometric authentication approach works:



```
puts " ID = $id Nounce=$nounce Login=$login Password=$pwd Image=$img"
if {$login eq "abc" && $pwd eq "123" && $img eq "img_N4"}
set p [$self authenticate $node_id $nonce_id abc 123 $img]
```

```
ID = 4 Nounce=900 Login=abc Password=1234 Image=img_N4
val is 0
GR Node 0 recieves a [illegible] Reply for request $msg_id for Node 4 from 6
Node 4 received Failed Authenticcation Message with values : 2 4 900 103 from 6
```

```
ID = 4 Nounce=900 Login=abc Password=123 Image=img_N4
val is 1
GR Node 0 received Node_Join_Reply and Backlog Clearence Request with values : 1
 4 900 101 from 6
Node 4 recieves Backlog Clearence Request with values : 4 4 900 104 from 0
Node 4 received Successful Authenticcation Message with values : 2 4 900 102 fro
m 6
```

Figure 4-2: Node Joining Strategy using secure biometric authentication

4.5.3 Node Leaving Strategy and Backlog Clearance Testing

In node leaving scenario *figure.4-3*, if any node wants to leave from the present group and joins other group then this node sends the request message to its affiliated GR. Further the GR forwards this message to the targeted GR and waits until it getting a reply message from the GR of targeted group. When this node joins new group and leaves the present group then the targeted GR sends a node attachment reply message to that node affiliated GR. After receiving the node attachment reply from the GR of targeted group the backlog information of this left node is cleared from its affiliated GR as well as its all neighboring nodes lists. Moreover, by using Dynamic Source Routing (DSR) approach in backlog clearance algorithm we tested the backlog information of the leaving node to make it cleared from its neighboring nodes lists.

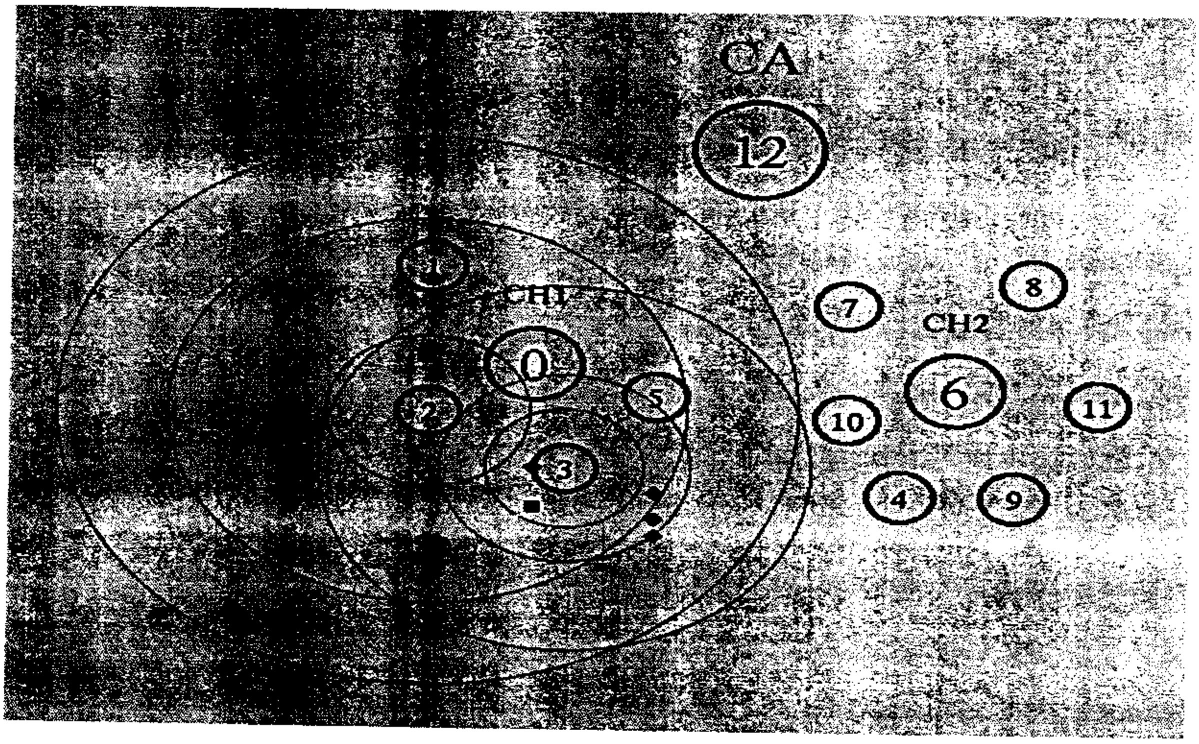


Figure 4-3: Node Leaving Strategy using DSR approach

According to the above figure, after the leaving node (n4) has joined the new group then the target GR (GR 6) sends the add request message to its neighbor nodes (n7,n8,n9,n10, n11) to add the entry of this new node (n4) in their member lists.

Further the previous GR (GR 0) sends a backlog clearance message to its neighboring nodes (n1, n2, n3, n5) to remove the entry of the left node (n4) in their member lists. Afterwards, if neighboring nodes (n1, n2, n3, n5) wants to sends the message to the left node (n4) then by using DSR approach the message will be generated but dropped at same time so the left node (n4) cannot receive the messages generated by its previous group member nodes (n1, n2, n3, n5) by introducing the concept of DSR approach in biometric authentication approach for mobile ad hoc networks.

4.6 Implementation of Proposed TCL Scenarios

Our proposed implementation scenarios in NS-2 comprises of several steps. These development phases are as follows:

Step No. 1 (Starting the simulation)

```
# create simulator
        set ns [new Simulator]
```

Step No. 2 (Creating topography)

```
# size of the topography (Area is 1000m x 1000m)
        set val(x)          1000
        set val(y)          1000
```

Step No. 3 (Define ns/nam traces)

```
# open the trace file (.tr)
        set f [open MoveOwnDesire.tr w]
        $ns trace-all $f

# open the nam file (.nam)
        set nf [open MoveOwnDesire.nam w]
        $ns namtrace-all-wireless $nf $val(x) $val(y)
```

Step No. 4 (Create GOD)

- GOD means General Options Directors
- Stores minimum amount of hops from one node to other
- set god [create-god <no of mnodes>]

```
# Create God

create-god $num_nodes

$ns color 0 green
$ns color 1 black
$ns color 2 blue
$ns color 3 red
$ns color 4 brown
$ns color 5 yellow
$ns color 6 purple
```

Step No. 5 (Configuring nodes)

```
set chan_1_ [new $val(chan)]

$ns node-config -adhocRouting $val(rp) \

            -llType $val(ll) \
            -macType $val(mac) \
            -ifqType $val(ifq) \
            -ifqLen $val(ifqlen) \
            -antType $val(ant) \
            -propType $val(prop) \
            -phyType $val(netif) \
            -topoInstance $topo \
            -agentTrace ON \
            -routerTrace ON \
            -macTrace ON \
            -movementTrace OFF \
            -channel $chan_1_ \
            -energyModel $opt(engmodel) \
           -initialEnergy $opt(initeng) \
           -txPower  $opt(txPower) \
           -rxPower  $opt(rxPower) \
           -idlePower  $opt(idlePower)
```

Step No. 6 (Creating nodes)

```
# defining heads labels

 $ns at 0.0 "$n(0) label CH1"
 $ns at 0.0 "$n(6) label CH2"
 $ns at 0.0 "$n(12) label CA"

# create a bunch of nodes for Group 1

  set n(0) [$ns node]
  $n(0) color "blue"        // node color
  $n(0) set X_ 150.0       // position or location
  $n(0) set Y_ 200.0
  $n(0) set Z_ 0.0
```

```
    $ns initial_node_pos $n(0) 60
    puts "Node 0 created as GH1"

  # create a bunch of nodes for Group 2

    set n($group_size) [$ns node]
    $n($group_size) color "blue"
    $n($group_size) set X_ 340.0
    $n($group_size) set Y_ 200.0
    $n($group_size) set Z_ 0.0
    $ns initial_node_pos $n($group_size) 60
    puts "\n Node $group_size created as GH2 "

  # create a node 12 as CA

    set n(12) [$ns node]
    $n(12) color "green"
    $n(12) set X_ 250.0
    $n(12) set Y_ 450.0
    $n(12) set Z_ 0.0
    $ns initial_node_pos $n(12) 80
    puts "\n Node 12 created as CA"
```

Step No. 7 (Define node movements and traffic model)

```
# Define node movement model
source <movement-scenario-files>
# Define traffic model
source <traffic-scenario-files>
```

Step No. 8 (Creating node movements)

```
for {set i 1} {$i < $group_size} {incr i} {
   set n($i) [$ns node]
   $n($i) color "black" }
   set v_x [expr fmod ((([expr [$rng integer
$twidth]])*(50*$group_size)*($i/$group_size%2) + 50*($i%($group_size/2))),90.0)]
   set v_y [expr fmod ((100*floor($i/$group_size) +
100*(($i%$group_size)>=($group_size/2))*([expr [$rng integer $twidth]])),90.0)]
   if {[expr $i % 4] == 0} {
```

```
$n($i) set X_ [expr (170.0+$v_x)]
$n($i) set Y_ [expr (220.0+$v_y)]
} elseif {[expr $i % 4] == 1} {
$n($i) set X_ [expr (130.0-$v_x)]
$n($i) set Y_ [expr (220.0+$v_y)]
} elseif {[expr $i % 4] == 2} {
$n($i) set X_ [expr (130.0-$v_x)]
$n($i) set Y_ [expr (180.0-$v_y)]
} elseif {[expr $i % 4] == 3} {
$n($i) set X_ [expr (170.0+$v_x)]
$n($i) set Y_ [expr (180.0-$v_y)]}
```

<u>Step No. 9</u> (Scheduling an event)

```
$ns at 0.07 "$n(4)  setdest 320.0 150.0 4500.0"
```

<u>Step No. 10</u> (Terminating a Tcl scenario)

```
        $ns at 0.35 "finish"
```

<u>Step No. 11</u> (Finish procedure)

```
proc finish {} {
     global ns f nf val NamAnimationSpeed  mswindows
     $ns flush-trace
     close $f
     close $nf

# puts "running nam..."
     exec nam -r $NamAnimationSpeed MoveOwnDesire.nam &
     exit 0
```

<u>Step No. 12</u> (Run the simulation)

The simulation starts with the final command in the TCL script:

```
        $ns run
```

4.7 Simulation Results

Simulation mechanism, simulation assumptions and simulation results have been discussed here and explained by graphs. These results show the efficiency of suggested solution and objectives of research are attained. To simulate the proposed solution we used Network Simulator version 2 (NS-2) and operating system is Fedora version 14. Results are deeply observed then compare these with the existing solutions and found it more result oriented in terms of communication overhead, successful rate of authentication and detection of compromised nodes.

4.7.1 Performance Parameters

The following metrics of performance are considered as follows:

1. Number of compromised nodes vs. Successful rate of authentication (%)
2. Nodes vs. Number of messages sent by neighboring nodes

4.7.2 Results of Simulation

In the graph *figure.4-4,* we proposed the concept of "**Secure Biometric Authentication Approach (image recognition)**" for detection of compromised nodes in mobile ad hoc network, if a group consists of 10 nodes and out of these 10 nodes, node (nl) becomes compromised then our proposed system is too efficient to detect this compromised node (nl) on the basis of our secure biometric authentication model and the successful rate of authentication to detect this compromised node (nl) is 100 % by our proposed system. Furthermore, this successful authentication rate (100 %) is same in case of any of the remaining nodes are compromised i.e. n2, n3, n4, n5, n6, n7, n8, n9, n10 respectively. This proposed system provides 100% authentication to successfully detect the compromised node in the network. As our proposed authentication process is based on three parameters (node login id, password and node image). So the successful rate of authentication to detect the compromised nodes in the network is efficient and higher in our proposed scheme. Moreover, if the information matches correctly with the information already stored by the targeted GR then the GR allows the node to join the group otherwise not.

The "**composite key management approach**" is used for authentication of compromised nodes. If a group consists of 10 nodes and out of these 10 nodes, node (nl) becomes compromised then this approach is not so much efficient to detect this compromised node (nl) on the basis of composite key management approach and the successful rate of authentication to detect this compromised node (n1) is 35 % by the system. Furthermore, this authentication rate (35 %) is same in case of any of the remaining nodes are compromised i.e. n2, n3, n4, n5, n6, n7, n8, n9, n10 respectively. This scheme provides 35% authentication to detect the compromised node in the network. In this scheme the authentication process is done only on the basis of nonce/random number. So the successful rate of authentication to detect the compromised nodes in the network is less efficient and even the compromised nodes can join the group easily without its proposer authentication and authorization in this scheme. In addition, if the random number (R) matches successfully with the random number (R') already stored by the targeted GR then the GR allows the node to join the group otherwise not.

By comparing the both schemes in *figure.4-4*, shows that the composite key management approach is less efficient and not enough stronger for authentication purpose because it provides authentication on the basis of only nonce number which can be compromised by the attacker easily during node mobility and communication. But our proposed secure biometric authentication approach provides authentication on the basis of node (login id, password and image).

As a result, if the compromised node wants to join the group then on the basis of login id, password and image the attacker will unable to join the new group. Let say, if the attacker knows about the login id then if the password and image will not match with the already stored information kept by the targeted GR the attacker will powerless to join the group and our proposed system will easily detect this node as the malicious/attacker node. That's why the successful rate for authentication is higher 100% by using our proposed secure biometric authentication approach and the authentication rate is less 35 % in composite key management scheme.

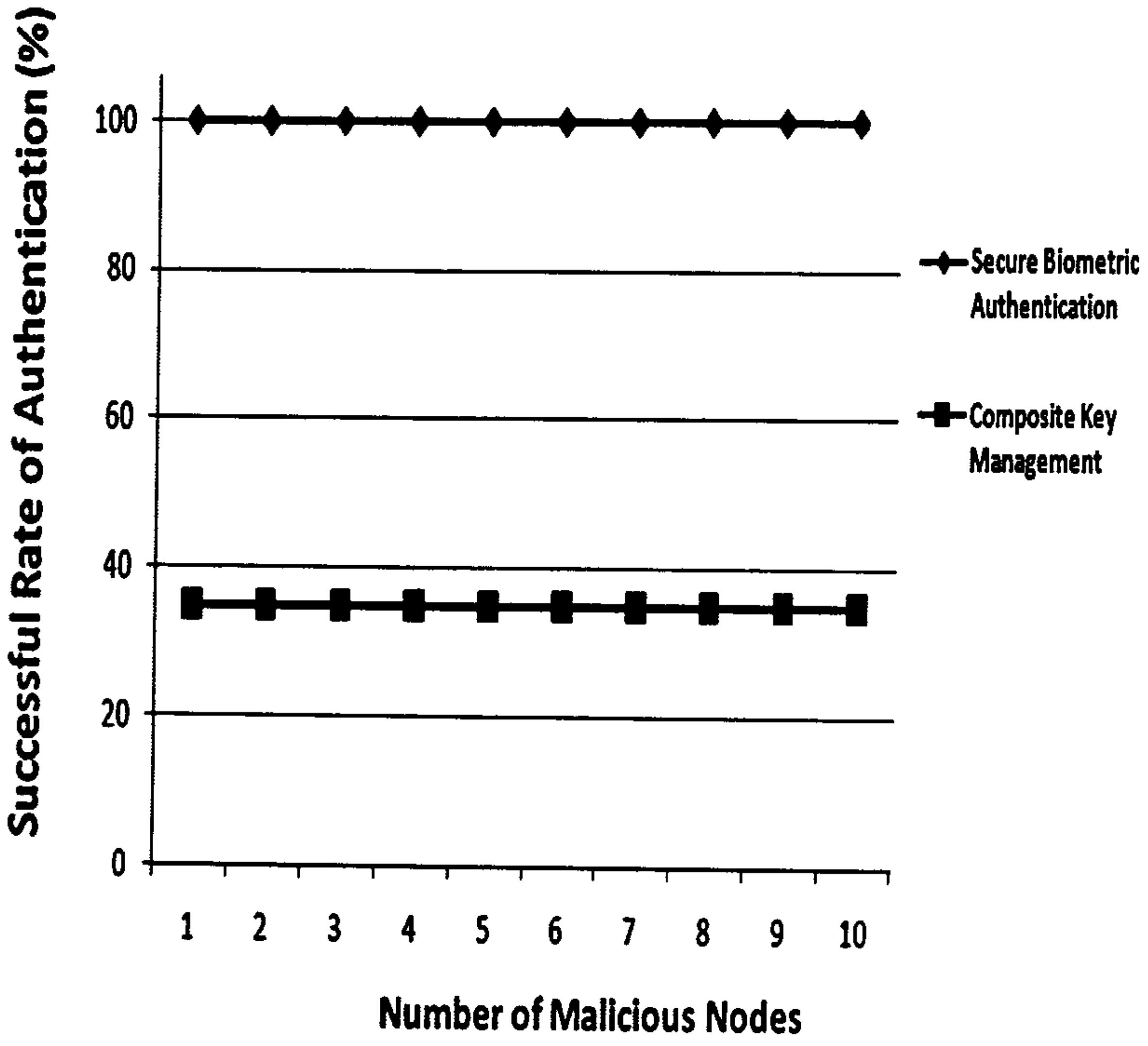


Figure 4-4: Secure Biometric Authentication Approach vs. Composite Key Management

In the graph *figure.4-5,* **Backlog Clearance Algorithm** by using **Dynamic Source Routing (DSR) approach** is used for reducing the communication overhead. If a group consists of 5 nodes and out of these 05 nodes, node (n4) has left the group and joined other group then after getting a node attachment reply from targeted GR the information of this left node (n4) is deleted from all its neighbor nodes lists (n1,n2,n3,n5) respectively. So in our proposed scheme, among of these remaining neighbors nodes if these nodes (n1,n2,n3,n5) sends a message to the left node then these messages will be generated but dropped at same time so the left node (n4) cannot receive the messages generated by its previous neighbors nodes (n1,n2,n3,n5) by using backlog clearance algorithm. The scheme effectively reduces the communication overhead and cost and only four (04) messages will be generated by the neighbor's nodes and at a same time these messages will be dropped and cannot be sent to the left node (n4) and next time no message will be generated. Furthermore, the number of generated message (N=4) will remain same in case if any other node (n1, n2, n3, n5) has left the group.

In the **cluster based composite key management approach** is used for mobile ad hoc networks. In this scheme, if a group consists of 5 nodes and out of these 05 nodes, node (n4) has left the group then its correlated information is cleared only from its affiliated GR but the neighboring nodes still contains the information of this leaving node (n4) in their neighbors list and hence will be contacted in future elections. It will cause an overhead to locate that which nodes have left the group and increases the communication overhead. The scheme increases the communication overhead and cost because their neighbor's node contains the information of the leaving node (n4) and these nodes generating messages to contact with node (n4) time by time. Every node (n1, n2, n3, n5) generates four (04) messages each and in case of no reply these four nodes generates again 4 messages for node (n4) and so on until no reply from node (n4). So the total number of messages is 32 for the node 4 means that thirty two messages will be generated if node 4 has left the group. These messages sends up to the maximum TTL (time to live) value and after reaching the maximum value its stop generating. These unnecessary messages will increase a large amount of overhead and all the time channel/network is busy. Moreover, the number of generated messages N=4 remains same if any other node (n1, n2, n3, n5) has left the group.

By comparing the both schemes in *figure.4-5,* shows that the cluster based composite key management approach is not much efficient because it caused too much overhead over the network due to unnecessary generation of messages by the neighbors nodes and all time channel is busy due to lot of messages are generated for the node who has left the group and there is no proper mechanism in this scheme to remove the entry of the left node from their neighboring nodes lists and to stop the production of needless messages. But our proposed backlog clearance scheme by using DSR approach is used for the reduction of communication overhead in mobile ad hoc networks. When a node has joined the group after its successful authentication the targeted GR sends a node attachment reply message to the node affiliated GR that your node has joined our group and on the basis of this message the GR sends a backlog clearance message to all its neighboring nodes (n1, n2, n3, n5) that removes the entry of the left node (n4) from their neighbors lists.

As a result, our proposed DSR approach effectively reduces the communication overhead and cost and only first time message will be generated but dropped at same time so the node (n4) that has left the group is unable to receive messages generated by their member nodes because node (n4) entry is deleted from their neighbors nodes list as well as from its affiliated GR list.

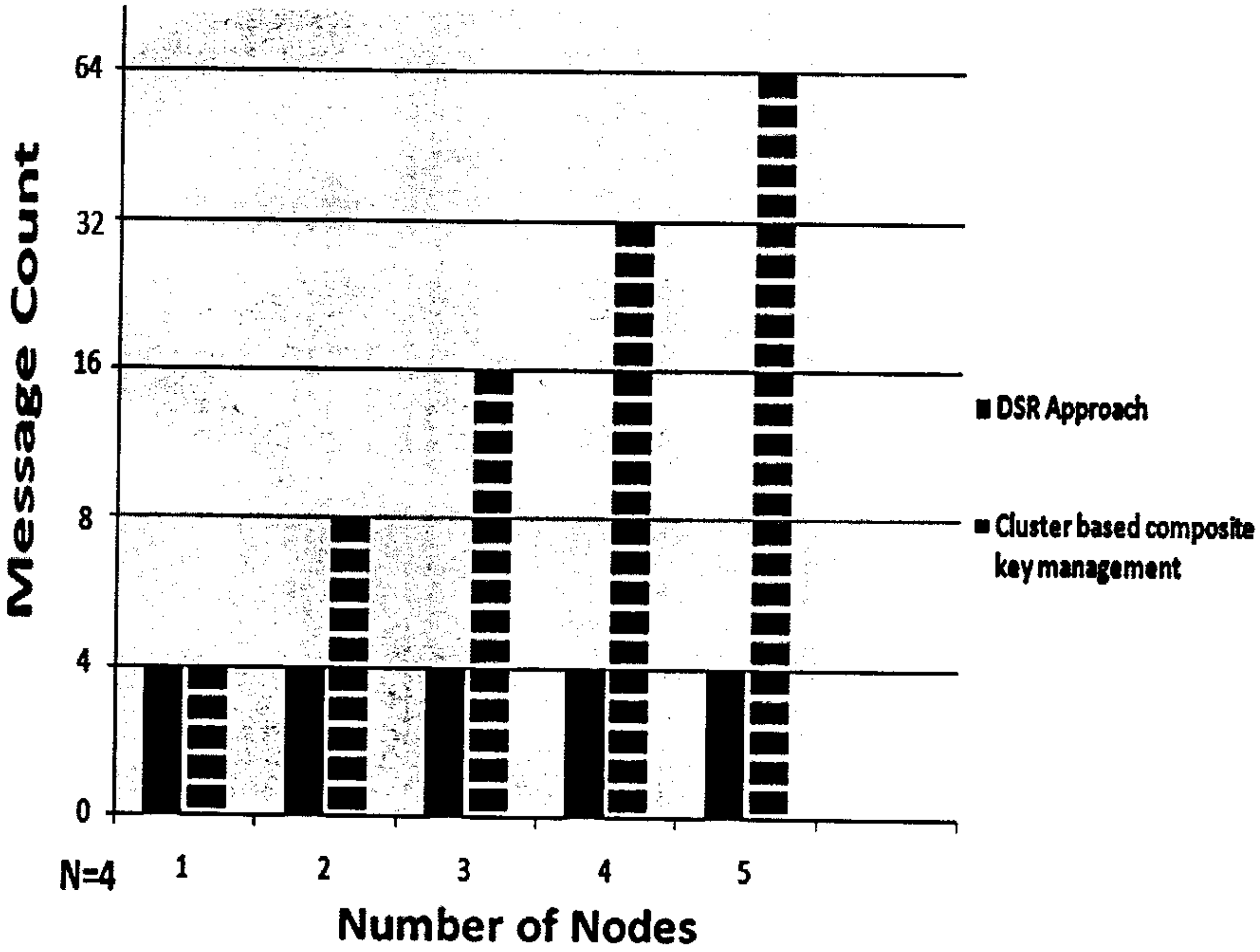


Figure 4-5: DSR Authentication Approach vs. Cluster Based Composite Key Management

Chapter 5

Conclusion And Future Work

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

A Mobile Ad hoc Network (MANET) consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices) which are free to move about randomly. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in separation, or may have gateways to and interface with a fixed network. Basically it is typically visualized to operate as a "stub" network connecting to a fixed internetwork.

Mobile Ad hoc Network (MANET) nodes are equipped with wireless senders and receivers using antennas which may be omni-directional (broadcast) and highly-directional (point-to-point) communication. At a given point in time, depending on the node positions and their sender and receiver coverage patterns, a wireless connectivity in the form of a random, multi hop and ad hoc network exists between the nodes. This ad hoc topology may change with time as the nodes move and change their location from one place to another rapidly.

Our main objective is to extend the security of Mobile Ad hoc Networks (MANETs) by preclusion from compromised nodes to join the network/group. To increase the life- time of MANET we provided strong and efficient authentication by using secure group based biometric authentication approach. By using this proposed approach, we can authenticate a soldier (node) that wants to join a new group on the basis of soldier login id, passkey and its image. If the attacker attacks on the soldier during node mobility and become the soldier compromised then it will pass the authentication process to join the new group. If these three security credentials (login, passkey, and image) of the solider match with the original information that is already stored by GR of targeted group then it allows the soldier to join the group otherwise if one of the parameter is incorrect (not compare) then our proposed system detect that node as malicious node and doesn't allow that node to join the new group. So our proposed secure biometric authentication approach diminished the entrance of compromised nodes in a group.

Furthermore, our proposed approach reduces the communication overhead by clearing the back log information of leaving node by using Dynamic Source Routing (DSR) protocol approach. So if any node leaves the group then the entry of this left node is deleted from its affiliated GR as well as its neighbor's nodes list. Thus, this scheme updating the neighboring lists as well as provides security (authentication and authorization) and protection from compromised nodes.

5.2 Limitations and Future Work

Perfection is elusive. Our proposed scheme deals with single node mobility scenario. The computational overhead is increased little bit but it is occasional and not regular. In future, we are looking forward to extend the direction of our current work in large Mobile Ad hoc Networks (MANETs). We will work on group mobility scenario which can further decrease the overall communication cost. If the whole group along with group representative (GR) and all its neighbors nodes wants to move and join other group then it authentication scenario will be observed. Further, we will work on cluster backup which is the replica of cluster head so if the cluster head is compromised then there is another possibility to make cluster backup as a cluster head. This technique hopefully reduces the entrance of compromised nodes in the network. Moreover, we will work on large group based mobility scenarios instead of single node mobility. We need some how to modify this current scheme to overcome the problem of group mobility development.

References

References

[1] Lein Harn and Jian Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications," *International Journal of IEEE Transactions on Wireless Communications.*, vol.10, no.7, July 2011.

[2] Saju P. and Samuel P, "A Distributed Hierarchical Key Management Scheme for Mobile Ad hoc Networks," *Proceeding of the International Conference on Information, Networking and Automation ICINA.*, 2010.

[3] Dr. A.Vincent Antony Kumar and R.PushpaLakshmi, "Cluster Based Composite Key Management in Mobile Ad Hoc Networks," *International Journal of Computer Applications.*, 4(7): 30–35, July 2010.

[4] Saswati Mukherjee, Matangini Chattopadhyay, Samiran Chattopadhyay, Amrita Saha, "A Key Re-Distribution and Authentication Based Technique for Secured Communication in Clustered Wireless Sensor Networks with Node Mobility," *International Journal of Computer Networks & Communications (IJCNC).*, vol.2, no.6, November 2010.

[5] Virendra Singh Kushwah & Gaurav Sharma, "Implementation of New Routing Protocol for Node Security in a Mobile Ad Hoc Network," *International Journal of Computer Science and Security (IJCSS).*, vol.4, no.6, 2010.

[6] Nagaprasad, S., VinayaBabu, A., Madhukar,K., Sujatha,B., AnandKumar,B., Veena,N., and Sunitha.J, "Multicast Routing Protocols in Ad hoc Mobile Networks," *(IJCSE) International Journal on Computer Science and Engineering.*, vol. 02, no. 08, pp. 2745-2748, 2010.

[7] Sumon Kumar Debnath, Foez Ahmad, and Nayeema Islam, "Performance Evaluation of Unicast and Broadcast Mobile Ad hoc Networks Routing Protocols,"

(IJCSIS) International Journal of Computer Science and Information Security., vol. 7, no. 1, 2010.

[8] Gupta, N and Gupta, R, "Routing Protocols in Mobile Ad-Hoc Networks: An Overview," *Proceedings of International Conference on Emerging Trends in Robotics and Communication Technologies (INTERACT).*, Bhopal, India, pp. 3-5 Dec 2010.

[9] Saleh Ali K.Al-Omari, Putra Sumari, "An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications," *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks.*, vol.2, no.1, pp. 87-110, March 2010.

[10] Renuka A. and K.C.Shet, "Cluster Based Group Key Management in Mobile Ad hoc. Networks," Dept. of Computer Science & Engineering, Manipal University (India), *International Journal of Computer Science and Network Security (IJCSNS).*, vol.9, no.4, April 2009.

[11] B. Gopalakrishnan, T.V.P Sundararajan and Dr. A.Shanmugam, "AGPM: An Authenticated Secure Group Communication Protocol for MANETs," *International Journal of Recent Trends in Engineering.*, vol.1, no. 1, May 2009.

[12] N.Shanthi and L.Ganesan, "Security in Multicast Mobile Ad-Hoc Networks," *International Journal of Computer Science and Network Security (IJCSNS).*, vol.8, no.7, July 2008.

[13] Irshad, E., Noshairwain, W., Usman, M., Irshad, A., Gilani, M, "Group Mobility in Mobile Ad hoc Networks," *IADIS Proceeding of the International Conference WWW/Internet Germany.*, 13-15, Oct 2008.

[14] Huang, D. and D. Medhi, "A Secure Group Key Management Scheme for Hierarchical Mobile Ad-hoc Networks," *International Journal of Science Direct Ad hoc Networks.*, vol.6, no .4: pp. 577-560, 2008.

[15] B. Kadri, A. Mhamed, and M. Feham, "Secured Clustering Algorithm for Mobile Ad Hoc Networks," *International Journal of Computer Science and Network Security.*, vol.7, no.3, pp. 27-34, 2007.

[16] I.R. Chen, J.H. Cho and D.C. Wang, "Performance Characteristics of Region-based Group Key Management in Mobile Ad Hoc Networks," *Proceedings of the 1st IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, Taiwan., pp. 411-419, June 2006.

[17] Yong Lee and Zygmunt J. Haas, "Authentication in very Large Ad Hoc Networks using Randomized Groups," *Proceedings of 16th International Symposium on Personal, Indoor and Mobile Radio Communications.*, IEEE: 1989-1993, vol.3, 2005.

[18] Deodhar, A., Gujarathi, R, "A Cluster Based Intrusion Detection System for Mobile Ad Hoc Networks," *Technical Report.*, Virginia Polytechnic Institute & State University, 2005.

[19] Xiao, Q, "A Biometric Authentication Approach for High Security Ad-hoc Networks," *Proceedings from the Fifth Annual IEEE Information Assurance Workshop.*, June 2004.

[20] Tseng, Y., Shen, C., Chen, W, "Integrating Mobile IP with Ad hoc Networks," *IEEE Computer.*, pp. 48-55, 2003.

[21] Berndt, L. K. A, "Quick Guide to AODV Routing," *National Institute of Standard and Technology (USDC).*, pp. 7, 2003.

[22] Burg, A, "Ad hoc Network Specific Attacks," *Proceedings on Ad hoc Networking: Concepts, Applications and Security.*, Technische Universitat Munchen, pp. 12, 2003.

Webography

Webography

[23] http://www.isi.edu/nsnam/ns/