Implementation of Security Services in LMA based Multicast Key Management Scheme for Proxy Mobile Ipv6 Networks

R. Jesuraj
PG student,Department of CSE,
GCE Tirunelveli.

D.Shalini Punithavathani,
HOD,Department of CSE,
GCE Tirunelveli.

ABSTRACT
Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to support mobile nodes (MNs) for IP with mobility, without requiring the participation of MNs in any mobility-related signaling. Network based mobility management protocol is more advanced from the host based mobility protocol .Recently, multicast issues in PMIPv6 networks have generated a great deal of interest among researchers, and several multicast schemes had been proposed. However, these schemes do not take security issues into account. Most of the group communications use multicast communication because if the information is sent once by the sender, it will be received by all the users. Main problem in multicast group communication is its security. In order to improve the security, various keys are given to the users. Using the keys the users can encrypt their messages and send secretly. The proposed scheme follows the security mechanism and also indirectly implement the LKH concept.the main advantage of proposed system is its security, Individual key and key encryption key generated by the secure cryptosystem. The proposed system implement the L-MKMS concept with high security

Keywords
Proxy Mobile IPv6 (PMIPv6); Multicast; key management; cryptography

1. INTRODUCTION

IP mobility support mechanisms, for example Mobile IPv4 [1] or Mobile IPv6 are terminal based, meaning that terminals are aware of their mobility and have to do operations in order to be able to maintain their on-going communication sessions. The reason is a very basic design choice adopted in IP, both in IPv4 [2] and in IPv6 [3], namely that addresses have two roles: they are used as locators and identifiers at the same time. [6]IP addresses are *locators* that specify, by means of the routing system, how to reach the node (more properly, the *network interface*) that is using a specific destination address. The routing system keeps information about how to reach different sets of addresses that have a common network prefix, thus improving scalability of the system itself. However, IP addresses are also *identifiers* used by upper-layer protocols (for example, the*Transmission Control Protocol* [TCP]) to identify the endpoints of a communication channel. Additionally, names of nodes are translated by the *Domain Name System* (DNS) to IP addresses (which, in that way, play the role of node identifiers The solution for the handover process presented in this report is based on a network controlled layer 3 mobility protocol. It is based on Proxy Mobile IPv6 (PMIPv6), the network controlled version of MIPv6, and is aimed at reducing the handover latency.

The main objective was to develop a solution to provide, using functionality residing only in the network, mobility support to terminals moving and changing their point of attachment within a particular area (the Localized Mobility Domain, LMD). In this solution, terminals only perform the standard IP operations (e.g., Neighbour Discovery) without any particular functionality related to mobility at the IP layer. The base solution that has been developed by the Net LMM WG is the Proxy Mobile IPv6 protocol (PMIPv6) [1]. This protocol is based on the Mobile IPv6 protocol [2] but relocating the mobility related functionality of the terminal to network node.

2. PRELIMINARIES

2.1 Host based IP level mobility protocols

This section describes the IPv6 mobility protocols that currently exist. First, host based
protocols are described. With these, the MN takes care of his own mobility management. In the second part, network based protocols are described, in which the network is the coordinator of the handover.MIPv6: MN communicates with CN via HA

2.1.1 Hierarchical mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) [24] was designed to reduce the amount of signaling needed between MN, CN and HA. It does this by separating global and local mobility. A Mobility Anchor Point (MAP) is introduced into the network. This MAP can exist at any level in a hierarchical network of routers. A MAP can span multiple subnets. A MN sends BU messages to the MAP, instead of to the home agent. The MN does not need to contact all CN's; all traffic is redirected after the one BU message is received by the MAP. The MN has two care-of addresses in the HMIPv6 domain: the Local CoA (LCoA) and the Regional CoA (RCoA). The RCoA is used for communication with CN's and stays the same while connected to the same MAP. The LCoA (or on-link CoA) is used to communicate with the MAP. Whenever the MN moves to a different link in the domain of the MAP it obtains a new LCoA and has to register this address with the MAP. After a successful registration to the MAP by a MN, a bi-directional tunnel is set up. Packets sent by the MN have the LCoA as source in the outer (tunnel) header and the RCoA as source of the inner header. The MAP receives these packets from the MN, removes the outer header and forwards the packet towards the CN with the RCoA as the source address

2.1.2 Fast mobile IPv6

Fast Mobile IPv6 (FMIPv6) [5] tries to decrease the handover latency that is experienced when a MN moves from one access link to another. After the MN is 'IP-capable' on the new link, e.g. has a layer 2 connection and has a valid IP address, it can send a binding update to 28 the home agent and correspondent nodes. Packets only start arriving at the new CoA after a successful registration with home agent. FMIP can work with both MN and network-initiated handovers. In the first mode, the MN can make use of layer 2 scanning

techniques to identify other access point within its reach. While still connected to its current access router, it can already get information like other access routers L2 and IP address. This is done by sending a Router Solicitation for Proxy Advertisement (RtSolPr) message to its current access router, asking information about a certain access point identified by AP-ID. The reply to this is a Proxy Router Advertisement (PrRtAdv) message. With these messages it is also possible to already form a prospective new CoA (NCoA) that can be used when the MN moves to the new AR. This way, the latency due to the prefix discovery when connecting to a new AR can be eliminated.
Proposed system follows the network based mobility management protocol that is nothing but PMIPv6

2.2 Network based protocol

2.2.1 Proxy mobile IPv6
Proxy Mobile IPv6 [1] tries to offer mobility to IPv6 hosts that do not have Mobile IPv6 in their stack. This is done by extending Mobile IPv6 signaling and also by reusing the home agent via a proxy mobility agent. With this approach it is not necessary for the MN to be part of layer 3 mobility signaling. The proxy mobility agent takes care of the MN's mobility management. This protocol can be used in networks that have both Mobile IPv6 enabled and non-Mobile IPv6 enabled nodes. The mobility entities in the network track the movements of the MN, initiate the mobility signaling and set up the required routing state. The major functional entities of PMIPv6 are MAGs, Local Mobility Anchors (LMAs), and MNs.

2.2.2 Mobile Node
A MN is an IP host whose mobility is managed by the network. An MN can be an IPv4-only node, IPv6-only node, or a dual-stack node, which is a node with IPv4 and IPv6 protocol stacks. An MN is not required to participate
In any IP mobility-related signaling for achieving mobility for an IP address or for a prefix that is obtained in the PMIP domain

2.2.3 Mobile Access Gateway
A MAG performs mobility-related signalling on behalf of the MNs attached to its access links. MAG is the access router for the MN; that is, the first-hop router in the localized mobility management infrastructure

A MAG performs the following functions:

- Obtains an IP address from an LMA and assigns it to an MN
- Retains the IP address of an MN when the MN roams across MAGs
- Tunnels traffic from a MN to LMA

2.2.4 Local Mobility Anchor

LMA is the home agent for an MN in a PMIPv6 domain. It is the topological anchor point for MN home network prefixes and manages the binding state of an MN. An LMA has the functional capabilities of a home in Mobile IPv6 base specification (RFC 3775) along with the capabilities required for supporting the PMIPv6 protocol
Components of a Proxy Mobile IP Network
Five devices participate in proxy Mobile IP:

- A visiting client device. The visiting client device is any device such as a personal digital assistant or a laptop that can associate to a wireless access point. It does not need any special Mobile IP client software.
- An access point with proxy Mobile IP enabled.The access point proxies on behalf of the visiting client device, performing all Mobile IP functions for the device. The access point uses a subnet map to keep track of home agent information. The access point also gets updates about new home agents from the authoritative access point.
- An authoritative access point on your network supporting proxy Mobile IP. The authoritative access point uses a subnet map to collect and distribute home agent information stored in the subnet map to all the other access points for all visiting client devices.
- A home agent. The home agent is a router on the visiting client's home network that serves as the anchor point for communication with the access point and the visiting client. The home agent tunnels packets
from a correspondent node on the Internet to the visiting client device by way of a tunnel to a foreign agent.
- A foreign agent. The foreign agent is a router on your network that serves as the point of attachment for the visiting client device when it is on your network, delivering packets from the home agent to the visiting client.

3 .SECURITIES

As with Mobile IPv6 signaling, PMIPv6 signaling is very sensitive to security threats, because it changes routing states of nodes in the network on behalf of the Mobile Nodes. PMIPv6 specification recommends using IP Security (IPsec) to protect the signaling exchanges between the MAGs and the LMA. A security association is needed between MAGs and the LMA, but how it is created is not defined. Two cases are possible: The network elements (LMA and MAGs) belong to the same operator.The elements belong to different operators with an agreement for roaming support.In both scenarios, creating the security association is an affordable problem.

3.1 Secure Multicast Groups

First, we provide a brief background of multicast technology and potential network security threats and issues. Second, we explore the application of existing and proposed security techniques for multicast networking, including key distribution, dynamic key management, and reliability issues. Multicast sessions may be described in terms of their membership. In general, a session is defined as either public or private. Both types are defined by the level of session access Control required receiving or transmitting data within the multicast group

3.1.1 Public sessions

Public sessions are typically encountered on the Internet Multicast Backbone (MBONE) and are supported by the dynamic nature of multicast communications (i.e., knowledge of the multicast address is often the only requirement for membership). Eavesdropping can quickly become a problem because of the potentially broad scope of a session. Session confidentiality can be provided through encryption.

3.1.2 Private Session

In order create a private session, access to the required session cryptographic key material should be restricted through a registration and authentication process. Only authorized users

should be able to gain access to group key material and subsequently participate in the session. In this paper, we define a secure multicast session as a private session with encryption of data content

3.2 Key Distribution Architectures

In applying a keying solution for secure multicast applications, it is desirable to maintain protocol features that preserve multicast efficiency and scale well for large one-to many or many-to-many data sessions. The ideal key distribution efficiency in a multicast environment can be represented in asymptotic O-notation as O(1). In such a scenario, a centralized server may transmit only a single keying message to the entire group to perform a group rekey. Every group member can extract the required key material from this one message. In contrast, the efficiency of using unicast techniques, without hierarchy, to distribute a group key separately to each group member is O(n). Note, in most cases, it may be more practical to perform the initial keying of participants in a unicast fashion during a registration/authentication process (this may be done out-of-band with secure e-mail, etc.).

Keying functions may be either centralized or distributed throughout the architecture. In a centralized architecture, keying functions are restricted to a single trusted authority. In some cases, this may be the initiator of a session or another entity assigned by the initiator to handle these vital functions. For scalability and robustness purposes, keying and registration functions may be distributed to other trusted entities. "One-to-many" type applications may benefit from a strictly centralized architecture. Alternatively, distributed architectures may prove more scalable since processing, messaging, and storage requirements are distributed across the network.

3.2.1 ***Existing System Key Distribution Architectures***

3.2.1.1 *Manual keying*

Manual keying methods are often not appropriate for dynamic multicast sessions in which membership is not defined prior to the start of the session. However, in some military environments with a well-structured manual key distribution architecture already in place, this solution may be the easiest to implement**.**

3.2.1.2 *Pairwise keying*

Pairwise keying techniques similar to those presented in [3] typically provide linear efficiency for initial keying and rekey operations. By consolidating all rekey messages into a single multicast message, the efficiency of session rekeying can be dramatically improved. However, for n participants this technique increases the overall size of the rekey message to n. Storage requirements for pairwise techniques are minimal at participant sites but requires n keys to be stored with the key distributor. This method can be made more scalable if keying and registration functions are distributed to other trusted entities

3.2.1.3 *hierarchical trees*

The hierarchical trees method presented in [3] provides linear initial keying performance and improved logarithmic rekey performance. The size 1 of any rekey message is no greater than (k-1)d. Key storage requirements at each participant site are d+1 keys while the initiator must store all key encryption keys (KEKs) and the group traffic encryption keys (GTEKs). The solution is more scalable than pairwise techniques because of the logarithmic rekey performance.

3.2.1.4 secure lock

The secure lock method described in [3] has linear initial keying performance and an impressive constant rekey performance. The size of the rekey message is also constant providing the best rekey performance of all methods reviewed. The drawbacks of this method include the computation time for the lock and the fact that the technique is inherently centralized and may not scale well to large groups

3.3 Security Services

In order to counter the common threats to multicast communications, we can apply several of the fundamental security services, including authentication, integrity, and confidentiality as defined in . A secure multicast session may use all or a combination of these services to achieve the desired security level. The amount or type of service required is dictated by the specific security policy defined for the session.

3.3.1 Authentication

Authentication services provide assurance of a participating host identity. Authentication mechanisms can be Applied to several aspects of multicast communications. Foremost, authentication is an essential part in providing access control to keying material. If the group employs cryptographic techniques such as encryption for confidentiality, then authentication measures may additionally provide a means to restricted access to the keys used to secure group communications

3.3.2 Integrity

Integrity services provide assurance that multicast traffic is not altered during transmission. Integrity is not inherent to IP datagram traffic payloads and is usually reserved for transport layer protocols (e.g., TCP). The lack of weakness of integrity services in IP can lead to spoofing attacks [7]. Strong integrity mechanisms can be applied indirectly at the network layer with security protocols such as the Encapsulating Security Payload (ESP) and AH [3,4]. In some applications where corrupted data can easily be detected, this service is not vital. However, in other applications including key management protocols, integrity services are essential means of countering spoofing attacks.

3.3.3 Confidentiality

Confidentiality services are essential in creating a private multicast session. Although encryption is typically used to provide this service, a weaker form of confidentiality may be achieved by limiting data distribution of routed session IP datagrams through time-to-live (ttl) settings

The typical security services (e.g., confidentiality, integrity, authentication) can be applied to traffic to counter these threats: – Security at the network layer using IPSEC mechanisms. – Security at the application layer for true end-to-end security**.**

3.4 Key Management Issues For Multicast

As introduced previously, through the use of encryption and digital signatures, we can achieve desired levels of Confidentiality, integrity, and authentication for a network multicast session. Assuming the use of strong security mechanisms that cannot be easily defeated by frivolous cryptanalytic attacks, we can focus our security concerns on protecting the key material. Therefore, we focus our security concerns and the rest of our technical discussion around key

management, key distribution, and access control for key material. With this in mind, a secure multicast session is defined by its Class D IP address or addresses and the required keying material. The size, type (e.g., asymmetric vs. symmetric), and number of keys required to secure a multicast session is determined by the encryption mechanism, the employed security policies, and the keying architecture. For private multicast sessions , access to these keys must be restricted in order to maintain the security of the overall session. Therefore, during the session registration process, it is necessary to require strong authentication mechanisms to establish the identity of potential participants prior to distributing key material. When these personal attributes are bound to a signed digital certificate, the certificate's digital signature and its relationship in a certificate hierarchy [20] may verify the identity of a participant and their assigned permissions.

In wireless multicasting, cryptography is normally employed to ensure that communications are secure. Specifically, a group key shared by all members of the multicast group is used to encrypt and decrypt the communication content. As a result, key management is a major research issue in the secure wireless multicast.new proposed system fully concentrate on the security related functionality and also it must satisfy the security services. Each and every dynamic member must follow the security requirements.

3.4.1 Security Requirements

The multicast key must be renewed when a mobile node joins, departs, and hands off a multicast group. The multicast key management scheme must satisfy the forward and backward secrecy requirement.

1**)** Forward secrecy:

The multicast key must be changed to ensure that a departing member cannot decrypt data

transmissions after he/she has left the multicast group.

2) Backward secrecy:

The multicast key must be changed to ensure that a new member cannot decrypt data transmitted before he/she joined the multicast group

.

4. PROPOSED SYSTEM

New proposed MAG-based and LMA-based multicast mechanisms[4] for PMIPv6 networks, as shown in Fig. 1. Consequently, the key distribution center (KDC) is responsible for generating, distributing, and updating the multicast key. The service provider (SP) obtains the multicast key from the KDC and can deliver the encrypted multimedia content to MNs via MAG-based or LMA-based

multicast methods. The objectives of MAG-based and LMA-based multicast mechanisms are to reduce handoff latency and end-to-end transmission delay and thereby improve the quality-of-service (QoS). In existing system Unfortunately, these multicast mechanisms do not take the security issue into account, even though many group communication services require a secure mechanism to protect the privacy of valid users.so in proposed system concentrate on the security related functions .

LKH scheme[5] satisfies the forward and backward secrecy, reduces the number of rekey messages, and encryption operations, it suffers from the "one affects all"[8]problem , where one member (i.e., a joining or departing member) affects all the other group members.so in proposed system indirectly follows the LKH scheme.

In general, several multicast security issues can be

addressed through participant registration and access to

multicast session keys. In many scenarios, initial participant keying is best performed out-of-band of the actual multicast data session. Subsequent key distribution can then occur within the multicast session.

Proposed key distribution centre must maintain the three kind of keys which is used for maintain the security services. key management tree architecture which is composed of key nodes and member nodes. The key node means a key in the key tree and the member node means an MN in the multicast group.

4.1 Key Nodes

Group key (GK),

key encryption keys (KEKS), and

Individual keys (IKS).

4.1. 1 Group key (GK)

The root node is the *GK* to guarantee secure communications among the group member.group key provide the authority to all leaf node.

4.1.2 Individual keys (IK)

Individual keys are nothing but unique key , which is used for individual node authentication. Individual key is used for authentication purpose.

4.1.3 key encryption keys (KEK)

The internal nodes are *KEKs* to

encrypt the updated messages sent to valid MNs. This key used for secure message transmission.And also existing system used less secure cryptosystem. But the proposed system using new secure cryptosystem algorithm for generate the KEK, compare to existing system it will give the best security services.

4.2 L-MKMS

The proposed L-MKMS scheme adopts a two-level key management architecture, as shown in below figure. The entire wireless network is divided into several LMDs, and the LMA manages the MAGs within its domain. Under the LMA-based multicast method, the MN does not rejoin the group when it moves around the same LMD because it joins the multicast group through the LMA. Therefore, we implement a "Handoff Operation"[3] in L-MKMS when the MN moves around different MAGs in the same LMD. The handoff operation is the main difference between the

L-MKMS scheme and the M-MKMS scheme. Moreover, in the L-MKMS method, the LMA acts as a key node and a member node at the same time

1) Multicast Data Transmission

In Fig. 1, the SP encrypts the multicast data with the *GK*

and sends to the LMA, which decrypts data with its *GK*. The LMA then encrypts the data with *Domain-GK*, and multicasts it to all members via the MAG-LMA tunnel. Note that the role of *Domain-GK* is similar to *GK* but it belongs to the domain in the serving range of the LMD. In addition, the relation between *GK* and *Domain-GK* is independent. Finally, the recipients use the *Domain-GK* to decrypt and obtain the data.

2) Join Operation

When an MN joins a group, backward secrecy must be ensured so that the new member cannot decrypt the multicast data sent before he joined. There are two possible scenarios when an MN wants to join a multicast group: (i) the LMA is not a member of the multicast group; or (ii) the LMA is already a member. Note that the LMA does not change the *Domain-GK* when the MN hands off to a different MAG in the same serving range of the LMD. The steps of the join operation are as follows.

Step 1: {*mn*}→ {*lma*}: When an MN wants to join a multicast group, it sends a group join message to the current LMA via the MAG-LMA tunnel.
Step 2: On receipt of the join message, the LMA checks whether it is a multicast member of the group that the MN wants to join. If it is not a member, it joins the multicast group through the LKH scheme (i.e., it satisfies the backward secrecy) and obtains the *GK*. Then, the KDC broadcasts the new *GK* to all LMAs. Otherwise, the LMA performs Step 3.
Step 3: {*lma*}→{*MN*}: The LMA generates the new *Domain-GK* via the LKH scheme for the join of the MN and broadcasts the new *Domain-GK* to all MNs belonging to its domain. Note that all *Domain-KEKs* on the key path from the new member's parent to the root are compromised and should be changed.
Step 4: {*lma*}{*mn*}: The LMA encrypts the new *Domain-GK* with the new member's *Domain-IK* and sends it to the new member.
3) Leave Operation
When a member leaves the group, forward secrecy must be guaranteed to prevent the departing member decrypting subsequent data transmissions. There are also two possible scenarios when an MN leaves the multicast group: (i) there are no other multicast members in the LMA; or (ii) some multicast members are still located in the LMA. The steps of the leave operation are as follows.
Step 1: {*mn*}→{*lma*}: When an MN decides to leave the multicast group, it sends a group leave message to the current LMA.
Step 2: On receipt of the message, the LMA checks whether there are any other members in its group. To ensure forward secrecy, the LMA updates the key tree if there are no other members in its group, and the KDC broadcasts the new *GK* to all LMAs. Otherwise, the LMA performs Step 3.
Step 3: {*lma*}→{*MN*}: The LMA generates a new *Domain-GK*, encrypts this new *Domain-GK* with each member's *Domain-IK*, and broadcasts it to each member. Note that this broadcast message contains multiple encrypted keys. The new *Domain-GK* received by each member is encrypted with his/her *Domain-IK*.
4) Handoff Operation
The MN does not rejoin the multicast group and change the *Domain-GK* when it moves around the same LMD. However, it still needs to be authenticated when it hands off. The steps of the handoff operation are as follows.
Step 1: {*magnew*}→{*magold*}: The new MAG sends an authentication request to the old MAG.
Step 2: {*magold*}→{*magnew*}: On receipt of the request message, the old MAG sends the MN's authentication information to the new MAG, which then verifies the MN.
Step 3: If the MN's authentication request is successful, the LMA builds a bi-directional tunnel between the MAG and the LMA, encrypts the multicast data via the *Domain-GK*, and transmits it to the MN. Otherwise, the MAG asks the LMA to generate a new *Domain-GK* to guarantee backward and the forward secrecy. Note that, the authentication process is out of scope of this work, and any PKI authentication mechanisms can be applied to here.
Proposed algorithm is nothing but

4.3 A New Variant Of Subset-Sum Cryptosystem Over RSA

4.3.1 Introduction

In this section we introduce a new approach for public key cryptosystem. Modified Subset Sum
(MSS) is an asymmetric-key cryptosystem in which two keys are required: a public key and a private key. Furthermore, unlike RSA[7], it is one-way, the public key is used only for encryption, and the
private key is used only for decryption.

Modified algorithm consist of three steps-
Step 1) Key Generation Process
Step 2) Encryption of Message
Step 3) Decryption of Message

4.3.2 Key Generation Process

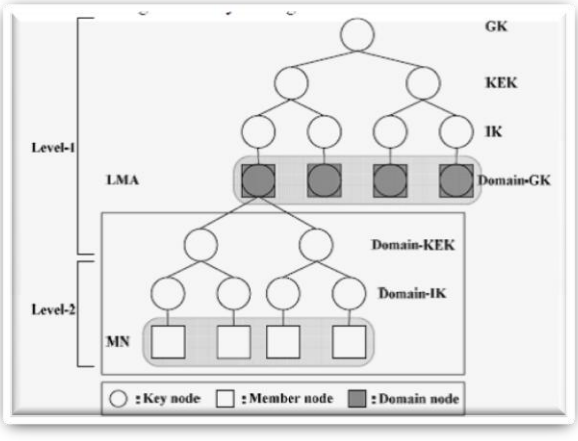
1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product m = p x q is of the required bit length, e.g. 1024 bits. (From Big Integer library function of Java)
2. Compute m = p x q and ϕ = (p-1) x (q-1).
3. Choose an integer *e*, satisfying 1 < e < ϕ, such that gcd (e, ϕ) = 1.
4. Compute the secret exponent *d*, 1 < d < ϕ, such that e x d $\equiv_\phi$ 1 (mod ϕ).
5. Choose a super increasing set A = (a1, ...,an)
6. Choose an integer M with M > SUMi=1...n(ai). M is called the modulus.
7. Choose a multiplier W such that gcd(M, W) = 1 and 1 <= W < M This choice of W
guarantees an inverse element
U:UW = 1 (mod M)
8. To get the components bi of the public key B, perform b_i = ai*W mod M, I = 1 ... n
The superincreasing property of A is concealed by modular multiplication.
The public key is (B, n, e) and the private key is (A, M, W, n, d). Keep all the values d, p, q and ϕ secret.Public key is published for every one and private key must be kept secret. Then by using these keys encryption and decryption are performed

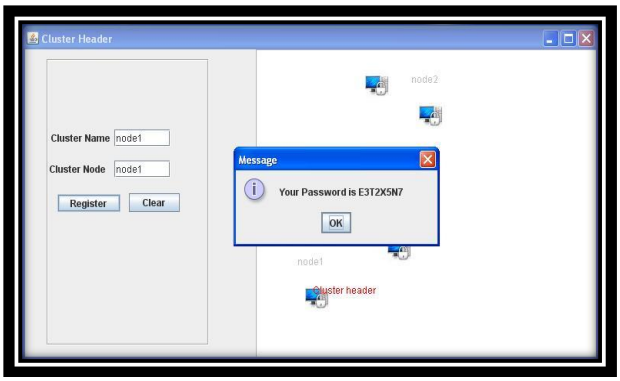
4.3.3 Encryption of Message

Sender A does the following: -
1. The length of a message to be encrypted is fixed by the parameter n prior to encryption; a possibly larger message p has to be divided into n-bit groups.
2. Let p = (p1, p2... pn) the message to be encrypted.
- The ciphertext c is obtained by computing
  c = b1p1 + b2p2 + ... + bnpn
- Computes the cipher text c1 = ce mod n.
- Sends the cipher text c1 to B.

4.3.4 Decryption of Message

Recipient B does the following: -
1. Uses private key and first compute $m_1 = c_1^d \bmod n$.
2. First compute c' = Um_1 mod M = w^{-1} mod M
3. Now solve (A, c'). Because A is superincreasing, (A, c') is easily solvable. Let X = (x1... xn) be the resulting vector and $p_i = x_i$ and p = (p1... pn) is the plaintext.





The above screen shows , how the group key will be generated for secure communication

The above screen shows how the cluster node secretly communicate with the individual key.

4.4 Security analysis of SSRPKC cryptosystem

4.4.1 Mathematical attacks

If RSA which is based on single modulus, is broken in time x and Subset sum based algorithms is broken in time y then the time required to break SSRPKC algorithm is x*y. So the security of SSRPKC algorithm is increased as compare to RSA algorithm and it shows that the SSRPKC algorithm is more secure for *Mathematical attacks* [4].

4.4.2 *Brute force attack*

As in SSRPKC double decryption is performed and unlike RSA that is not only based on private key but also based on the subset sum problem so one can't break SSRPKC only guessing the private key only. So it shows that SSRPKC algorithm is more secure as compare to RSA for Brute force attack[4].

4.4.3 Factorization attack

As the SSRPKC cryptosystem uses dual modulus, so for breaking this one have to factor both the modulus. That's why our cryptosystem provides the far better security against the factorization methods [4].and attacks on RSA cryptosystem

5 .CONCLUSION AND FUTURE WORK

The proposed cryptosystem more secure than the existing system, because it indirectly follows the LKH architecture and also it provide the security services with authentication. while generate the individual key for each node ,it will take some time so reduce the time complexity by the way of improve the QoS[2]. In this paper, we propose two multicast key management schemes (L-MKMS) for secure group communications based on LMA multicast methods in PMIPv6 networks.and also it uses new cryptosystem for secure group communication.The schemes satisfy the forward and the backward secrecy requirement, and mitigate the "one affects all" problem in the LKH scheme with lower communication cost. In the future, we will investigate an adaptive key management scheme that can adjust itself to the network environment and the characteristics of the user

6 .REFERENCES

[1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil,"Proxy Mobile IPv6," *RFC 5213*, August 2008

[2] J. Guan, Y. Qin, S. Gao, and H. Zhang, "The Performance Analysis of Multicast in Proxy Mobile IPv6," *IEEE ICCTA*, pp. 719-723, October2009.

[3] D.Wallner, E. Harder, and R. Agee, "Key Management for Multicast:Issues and Architecture," *RFC 2627*, June 1999. [6] Ralph C. Merkle, Martin E. Hellman. "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Transactions on Information Theory, vol. IT-24, 1978, pp. 525-530.

[4] RSA Laboratory (2009), "RSA algorithm time complexity", Retrieved fromhttp://www.rsa.com/rsalabs/node.asp?id=2215 (4 April 2011).

[5] Y. Sun, W. Trappe, and K. J. R. Liu, "An Efficient Key Management Scheme for Secure Wireless Multicast," *IEEE ICC*, pp. 1236-1240, August 2002.

[6] D. H. Kwon, W. J. Kim, Y. S. Kim, W. S. Im, Y.J. Suh, "Design and Implementation of an Efficient Multicast Support Scheme for FMIPv6," *IEEE INFOCOM*, pp. 1-12, April 2006.

[7] R. Vida and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," *RFC 3810*, June 2004.

[8] P. Wang, Y. Cai, J. Huang and X. Xu, "A hierarchical multicast protocol in mobile ipv6 networks," *Science Direct, Computer Communications* 30, 2006, pp. 144-152.