Secure Group Key Management and Reducing Error Communication in Wireless Network - Survey

R. Mahaveerakannan[1]
Research Scholar,
Information Technology St. Peter's University,
Avadi, Chennai. [1]

Dr. Suresh Gnana Dhas[2]
Supervisor,
St. Peter's University,
Avadi, Chennai. [2]

***Abstract*:- Security is usually provided by encrypting the media packets sent from a user to other users with the help of a shared key called the session encryption key. The key is a threshold to visualize all media assessment as we have to manage like our property. In network, Key management is a critical issue for both wired and wireless communications. Key management is an essential cryptographic primitive upon which other security primitives are built based on network topology. Key management scheme in multicast network is achieving a secure group communication (SGC) between the group members. Key management scheme for hierarchical access control, which considers both ordered user relations and ordered data stream relations. The transactions reported, most have focused on addressing the issue of key management to SGC systems. Encryption can be used to protect messages exchange among group members, distributing the cryptographic keys becomes an issue. Here many authors have proposed their thoughts to solve the issues of key access on wireless network in several ways. We also propose secure group key management schemes for scalable secure multicast communications. We focuses on reducing the number of communication errors too.**

Keyword:* *Security, Key management, Group Key, Multicast, Encryption, Error Reduction.

INTRODUCTION:

Security is usually provided by encrypting the media packets sent from a user to other users with the help of a shared key called the encryption key. In existing systems a secure group communication, nodes share a single symmetric key (Neighborhood) for encrypting and decrypting messages. To perform encryption and decryption each node must have access to other nodes neighborhood key. At source, Neighborhood Key is encrypted with the public key of the receiver and transmitted to the destination node. At destination, neighbourhood key is decrypted with the node's own private key. The message specific key is encrypted with neighborhood key.

A key exchange and encryption mechanism is presented where each node shares secret key only with authenticated neighbors in the network. In the traditional techniques group key exchange mechanism, a new node joins or leaves. When a node (client) wants to join the group, the client and Group control (key server) mutually authenticate using an authentication protocol. The client is permitted to join the group, the key server provides it with the required keys. The keys sent to the client include the group key which is shared by all members of the group and auxiliary keys. The key server is also responsible for handling client removal and leaving event.

Since the key is exchanged only with neighborhood nodes, the time taken to exchange the key is reduced considerably as well as authentication is also increased.

Group Key management is a subcategory of cryptography. Cryptography concerns itself with securing information so that unauthorized individuals cannot access and understand the messages sent. In addition, many group communication applications require security services which are built atop secure group key management. Key Management is essential for proper and secure distribution, creation and revocation of the keys used to secure messages. Secure multicast group is associated with one or more trusted servers responsible for managing membership to the group called as key server.

Security scheme consists of RSA key exchange mechanism and a novel encryption mechanism to provide security. Keys are securely exchanged in a Key update message after encryption using the traditional RSA algorithm.

Secure network communication:

The key is a threshold to visualize all media assessment as we have to manage like our property. Multicast is a group communication that provides data delivery from a source to destination, also known as multicast group. The router automatically forwards the message to each receiver. Multicast protocols require the creation and maintenance of a structure for distribution of information to the group members.

Multicast group communication is very large and highly dynamical with frequent joins and leaves. The new member can joining request send to the group head and leaving request send to group head.

When user can leaving request to a secure group communication, every secret key that has been held by and other users is should be changed.

Issues in wireless network:

In network, Key management is a critical issue for both wired and wireless communications. In wireless network communication, the requested quality service level has to be guaranteed even though security services are in use in the network. And when the composition of the group is changing the group members and service providers want to be absolutely sure that members leaving the group cannot read the messages.

- Key distribution and key agreement over an insecure channel are risky and suffer from potential attacks
- Key integrity and ownership should be protected from key attacks.
- The key could be compromised or disposed after a certain period of usage.

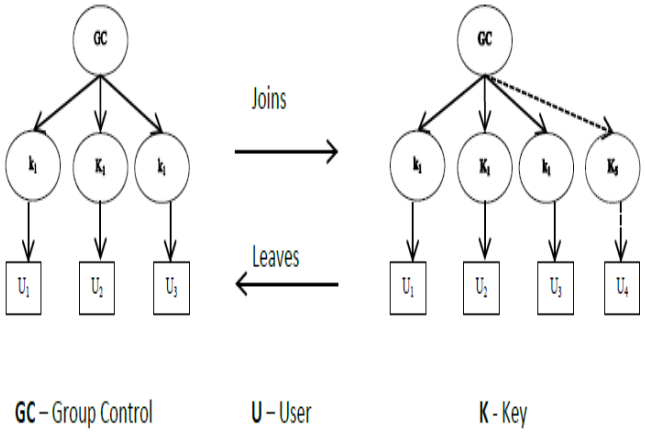
There are many approaches exist to provide the solution of group key management problems but mostly use the RSA and Deffi-Hellman approach to create and share the key between source and destination but these algorithms also increase the computing and communication overheads of system.

Key Management system in WN:

Key management is an essential cryptographic primitive upon which other security primitives are built based on network topology. In the cryptographic network security is used the primitive roots of prime number *p* and secret key *k*.

A group key management protocol is enables the creation and maintenance of a group key. In this approach, a group key distributor center, the first member joining the group for creating a group key request (*GKR*) including a traffic encryption key (*TEK*) and a key encryption key (KEK). A new member is interested to joining the group; the key distributor centers send a copy of *GKR* to the new member.

The Logical Key Hierarchy (LKH), is a tree based group key management scheme which utilizes the logical key tree. Key Distribution Center (KDC) is maintaining a key, when nodes join and leave the group. A GC (Group Control) which is the root of a key tree is used to encrypt all data traffic within a group. KEK (Key Encryption Keys), which is intermediate edges of a key tree are used to update the root GC and other KEK. The leaves of a key tree are IKs (Individual Keys) which are individually shared by each node and the GC. As a result, each node in a group possesses three kinds of keys: its own IK, KEKs (on the path to the root), and a root GC. Figure 1, the key tree update the procedures of both '*Node Join*' and '*Node Leave*' events.



Join and Leave the group

Node Join:

A Joining member associate with root node, a joining request from user u, group controller (GC) updating the key by creating a new node u and new key k. Encrypt it with the individual key and send the encrypted new group key to user u. The joining node should be updated to prevent the node from decrypting the previously exchanged messages within the group. The rekeying message generate for the existing member.

Node leave:

A member leave from group, a leave member request from user u, group controller updates the key by deleting the leave node for user and key for its individual key. Group controller generates a new group key k', are updated and encrypted with each of its respective nodes KEK.

For a joining request from new user, we provide that the group access control is performed by center using the access control list provided by the initiator of the secure group communication.

Individual key: when a new user sends a join request to Key Distributed center, KDC authenticate new user. If new user request is accept it will be granted with a new individual key that is shared between user and KDC.

Group key: it referrers to as root key. It is used to encrypt data and share between center and users.

Key encryption key: KEK means the path from group head (root) to leaf node (new user).

Secure group key Management (SGC):

Group key management schemes were developed for static wired networks with a small number of participants. Key management protocols for large and very large dynamic groups followed, to be used with, e.g., IP multicast. Secure multicast communication requires that the messages between group members are authenticated, encrypted and integrity of the security mechanisms. Most of the security mechanisms require the use of some kind of cryptographic keys that need to be shared between the communicating parties.

Key management scheme in multicast network is achieving a secure group communication (SGC) between the group members. Key management scheme for hierarchical access control, which considers both ordered user relations and ordered data stream relations.

The hierarchical group access control problem for group communication in this section. *SGC* is defined as the entire user, have access to a particular resource. From group access control points to use, a SGC is defined as a set of users , can access the exactly same set of resources.

The purpose of key management is to initialize system users within a domain.

- Generate, distribute and install keying material.
- Control the use of keying material.
- Update, revoke and destroy keying material.
- Store, backup/recover and archive keying material.

A group key management (GKM) protocol supports protected communication between members of a secure group. A secure group is a collection of members, who may be senders, receivers, or both receivers and senders to other members of the group.

Our proposed approach “Secure Group Communication is one option to reduce the computing and communication at source as well as destination.

CONCLUSION:

In this paper, we provide an efficient secure group communication and key management protocol. which is also scalable. We proposed the user, have hierarchical framework is known to have minimum number of rekey messages. Secure group communication is use, when new members are join the multicast group simultaneously; the Key Distribution Center creates a new key tree for the members and their individual keys. A generate new key tree is attached one node to many node using the network topology. We conclude reduce the group rekey over head simultaneous join/leave.

REFERENCES

[1] Jiang, B. &Hu, X., (2008) “A Survey of Group Key Management”, IEEE, International Conference on Computer Science and Software Engineering, Vol. 3, pp.994-1002.

[2] An Efficient LKH Tree Balancing Algorithm for Group Key Management Deuk -Whee Kwak, *Student Member, IEEE,* SeungJoo Lee, JongWon Kim, *Senior Member, IEEE,* and Eunjin Jung, *Student Member, IEEE.*

[3] C. K. Wong, M. Gouda, and S. S. Lam, “Secure group communications using key graphs,” *IEEE/ACM Trans. Networking*, vol. 8, pp. 16-30, Feb. 2000.