Secure Decentralized Group Key Management through Progressive Approach

S. Sandosh
Lecturer
Department of Information, Technology,
Manakula Vinayagar Institute of Technology,
India.

V.Akila
Assistant Professor
Department of Computer Science,
Pondicherry Engineering College,
India.

S. Uthayashangar
Lecturer
Department of Information Technology
Manakula Vinayagar Institute of Technology, India.

ABSTRACT

Multicast routing protocols are widely used as efficient communication methods for Group-oriented applications. Decentralized system is preferred to improve bandwidth economization. However, security with the key management for such protocols re-mains a significant problem. In this paper, a secure group key agreement over decentralized systems is proposed. The proposed system is based on the use of progressive approach which is a step by step improvement process. The main advantage of our proposed system is the periodic Authentication of group key members.

Index Terms— Multicast, Cryptography, Group Key Management, RMTP, Progressive Approach.

1. INTRODUCTION

Many applications, such as digital media distribution Pay-per view, teleconferencing, multiparty video games, military application and cooperation in a network and software updates, use multicast services. However, an increasing number of such applications require secure multicast services in order to control the Group Members (GM) in a secure way.

Group Key Management (GKM) helps to achieve security in multicasting information over group-oriented environments. In order to multicast information among a certain group securely, a Group Key (GK) should be shared among all members in this group. Every information packages should be encrypted with the shared Group Key (GK) before they are transmitted. Only the authorized users who have the shared common Group Key (GK) can decrypt the package and get the information.

The unauthorized users perhaps received the encrypted packages; they can't get the information without the Group Key (GK). So the communications among these members in the group are secure *[1]*. But there are some problems need to be addressed in Group Key Management (GKM). The members in group may be changed frequently. Any time when a new member joined, a new Group Key (GK) should be generated and distributed to all group members (GM), include the new joined member. This re-keying (generation and distribution of new key) process helps to maintain Forward Security and Backward Security *[1]*.

2. MULTICAST

Transmission of messages to the selected group of recipients. A simple example of multicasting is sending an E-mail to a mailing list.

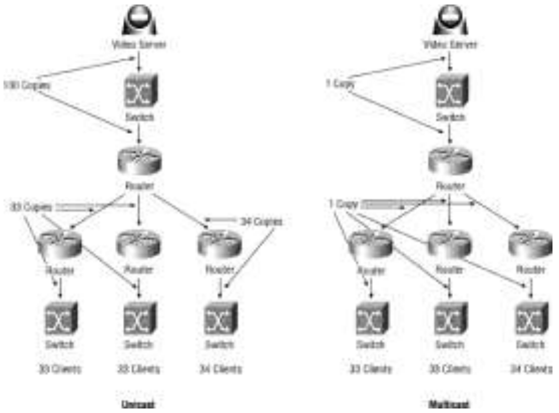

Figure 1. Unicast/Multicast

Teleconferencing and videoconferencing also uses multicasting. Multicast addressing is a network technology for the delivery of information to a group of destination simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the multiple destinations split.

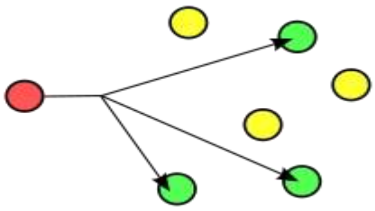

Figure 2. Multicast

Group Key Management (GKM) is the foundation stone of Multicast security. In Group Key Management (GKM), shared secret key among the Group Members (GM) in order to access confidential information improves security.

3. GROUP KEY MANAGEMENT

In a Group-Oriented system there is Group Server (GS), who allows the agents in the group to access data. Initially when any user wants to join the group, the user should request the Group Server (GS) that he is interested in joining the group. Then the Group Server (GS) asks for the one time authentication from the new user which is the Username and Password. After this process the Group Server (GS) introduces two keys to the new agent which is called the Group Key (GS) and the Individual Key(IK). The Group Key (GK) is used to decrypt the confidential information shared among the group members.

All the members in the group have the same Group Key (GK). The Individual Key is used to request the Group Server (GS) that the particular user is interested in leaving the group. The Individual Key (IK) is unique and it differs from other members in the group. Each Group Server (GS) generates and distributes the Group Key (GK). Then the Group Server (GS) encrypts the confidential information with the Group Key (GK) and send it to the agents. The agents decrypt the message with the shared Group Key (GK).

If any member leaves the group re-keying (generation and distribution of new Group Key (GK) will be done by the Group Key Server (GKS).When a user leaves the group, the Group Key Server (GKS) generates a new Group Key(GK) and wait till the new user enters the group. Other users in the group continue to work with the old group key (GK).

When a new user enters the group the Group Key Server (GKS) distributes the new Group Key (GK) to the entire users including the new one *[1]*.

3.1 Forward Security

Any new member who joins the group is restricted to get the former Group Key (GK) so that he can decrypt the former package which he has not been authorized to know.

3.2 Backward Security

If any member has left the group, he has no rights to know the information packages shared in the group any more.

4. DECENTRALIZED GROUP KEY MANAGEMENT

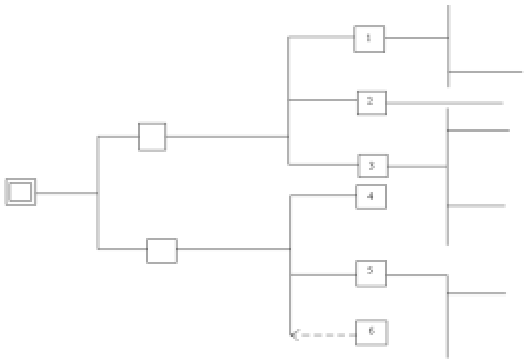

Figure 3. Decentralized Network

The drawback in multicasting is high Bandwidth requirement, but reduces **latency.**

In order to improve bandwidth economization, decentralized system is preferred.

In decentralized group key management protocols, the group is divided into several subgroups, there is a group key (GK) shared among all group members and every subgroup have a subgroup key among them. There is a group key server (GKS) which serves for all the members in group and every subgroup has a subgroup key sever (SGK) which manages the members with the subgroup key.

One of the decentralized group key management protocol is **Reliable Multicast Transfer Protocol. (RMTP)**

5. RMTP

Reliable **M**ulticast Transfer **P**rotocol provides sequenced, lossless delivery of bulk data from one sender to a group of receivers. RMTP achieves reliability by using a packet-based selective repeat retransmission scheme, in which each acknowledgment (ACK) packet carries a sequence number and a bitmap.

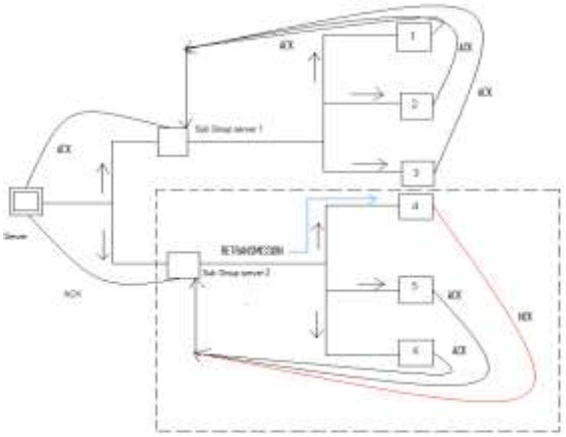

Figure 4. RMTP

Reliable **M**ulticast Transfer **P**rotocol is a computer network protocol that provides a reliable sequence of packets to multiple recipients simultaneously, making it suitable for applications like multi-receiver file transfer or streaming media *[3]*.

It does not guarantee the delivery of a message stream. Messages may be dropped, delivered multiple times, or delivered out of order. A Reliable Multicast Transfer Protocol adds the ability for receivers to detect loss of packets and take corrective action. In addition, lost packets are recovered by selective repeat retransmissions, leading to improved throughput *[3]*.

Even though multicasting information over decentralized environment with secure group key management using RMTP, helps to maintain security and to achieve throughput, there are still some problems need to be addressed.

Multicast protocols would be subject to attack by an **active intruder** compared to a unicast protocols. There are inherently more opportunities for interception of traffic, would typically make it easier for an intruder to pose as another legitimate principal.

6. PROPOSED WORK

The important problem need to be addressed here is Authentication. Because multicast protocols are easily attacked by active intruders and interception is possible. In order to prevent intruders and maintaining security, a step by step continuous improvement called **Progressive Approach** is implemented.

6.1 Progressive Approach

A multicast protocol is easily subject to attack by an intruder compared to unicast protocol and there are inherently more opportunities for interception.

In Existing System, the Group Key Server (GKS) asks for one time authentication (Username and Password) then it generates a new Group Key (GS) and Individual Key (IK) to the Users in the group. After the one time authentication the Group Key Server (GKS) does not worry about whether the confidential information reaches the authorized destination or user. Hence the intruder receives the encrypted messages from the Group Key Server (GKS). If any of the users leave or joins the group re-keying will be done by the Group Key Server (GKS) and the intruder will get the new key then he starts decrypting the confidential information which he has not been authorized to read.

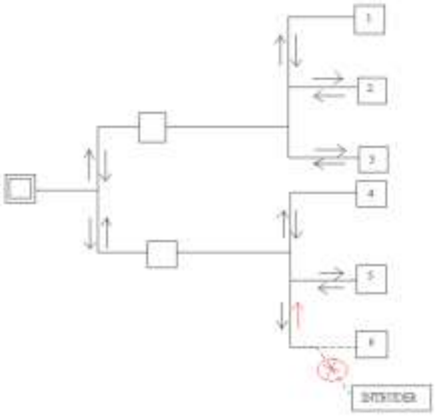

Figure 5. Intruder

To avoid intruders into the Group, accessing the confidential information, periodic authentication is required *[2]*. It is the role of the Group Server (GS) keep tracking the information send by the Group Server (GS) only reaches the legitimate user. Hash strategy is used to confirm that the users in the Group are original or legitimate user *[4]*.

Once the one time authentication (requesting the Username and Password) is done the Group Server (GS) generates and distributes new Group Key (GS) to all the members of the Group and an individual key for the new user. The Group Key (GK) is used to decrypt the confidential encrypted messages by all the members and the individual key is used to inform the Group Server (GS) when the member is interested in leaving the Group.

In the proposed work, a tiny bit of plain text other than encrypted confidential Group message is sent to all the members in the Group at regular intervals of time. Each member in the Group receives the tiny bit plain text and calculates hash for that value with the unique Individual Key and sends the result of hashing back to the server. Then the Group Server (GS) also calculates hash for that plain text separately in the Server side and compares the results with the received value from each member.

Any intruder who enters the communication link between the member and the Group Server (GS) may get the group key if any one of the member joins or leaves the Group but the intruder is not possible to get the unique individual key.

Only legitimate group member who is having the unique individual key can provide the expected results of hashing to the server [4]. After receiving the result of hashing from each member the server compares the result.

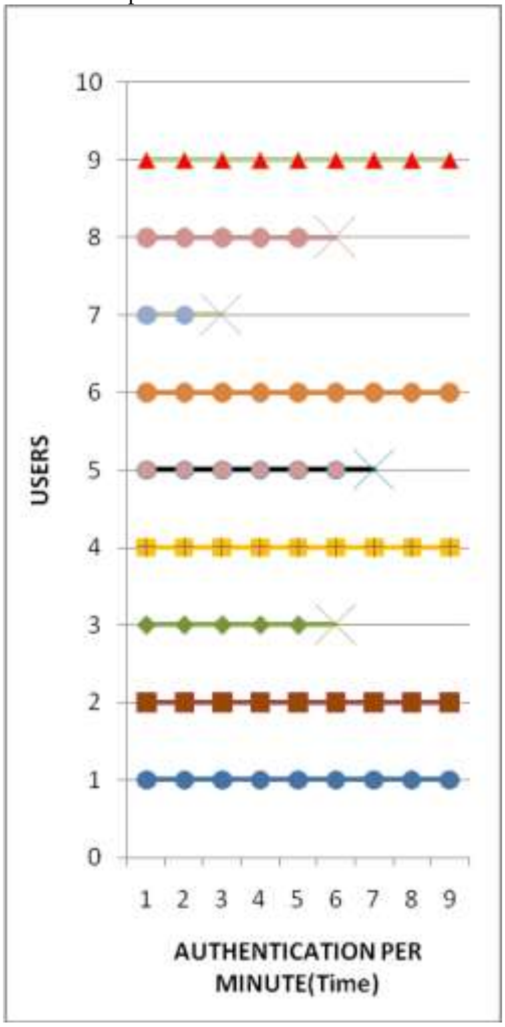

Figure 6. Progressive Approach

If match is found the communication continues, if no match is found the server stops the communication and the communications stops.

If the result received by the server is identified as wrong, the server comes to know some unauthorized person is trying to access the information then it stops the communications with the particular group member (GM) *[3]*.

7. CONCLUSION

Sharing confidential information among the Group Members (GM) in a secure way is more critical. After the one-time authentication, the new Group Member (GM) enters the group and starts sharing the confidential information by Encrypting and Decrypting the messages with the help of the Group Key (GK) provided. Skipjack- an efficient Encryption Algorithm helps to maintain the information more secure among the Group Members (GM). During the process of sharing of the encrypted information among the members, it is not assured that the information reaches only the legitimate Group Members (GM).

After the one-time Authentication (Username and Password) it is possible for the Intruders to enter the group and receives the confidential information but, the Intruder cannot decrypt the encrypted information without the group key.

In Group Key Management (GKM), if any member joins or leaves the group rekeying (generation and distribution of new group key) is done. Hence the Intruder easily receives the Group Key (GK) and decrypts the confidential information. Once the new member joins the group, the Group Members (GM) shares the information without worrying about whether the confidential message reaches the legitimate Group Members (GM) or not.

With the proposed system, Periodic Authentication is introduced and maintained till the Group Member (GM) quits the group. If any Intruder has entered the group, the intruder cannot perform the Authentication Verification process with the Group Server (GS) successfully. If the Authentication Verification Process fails, the communication between the Group Server (GS) with the intruder is terminated. Hence, the confidential information among the Group Members (GM) becomes more secure through Periodic Authentication.

8. REFERENCES

[1]. *Bibo Jiang and Xiulin Hu, Wuhan,*“A Survey of Group Key Management,”CSSE 1282,VOL:12, IEEE Nov 2008 .

[2]. *Feng Zhu, Wei Zhu, Matt W. Mutka*, “Private and Secure Service Discovery via Progressive and Probabilistic Exposure” VOL. 18, NO. 11, IEEE November 2008.

[3]. *C. Kenneth Miller,* The Internet Protocol Journal - Volume 1, No. 2 “Reliable Multicast Protocols and Applications”, September 1998 *StarBurst Communications.*

[4].*E. Michail, A.P. Kakarountas, A. Milidonis,* “Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 Hash function”©2004 IEEE.

[5]. *Raul Monroy and Graham Steel*, “Faulty Group Protocols Version 1.0”, February 2007.

[6]. M. Winslett, T. Yu, K.E. Seamons, A. Hess, J. Jacobson, R. Jarvis, B.Smith, and L. Yu, “Negotiating Trust on the Web,” IEEE Internet Computing, pp. 30-37,IEEE Dec 2002.

[7]. F. Zhu, M. Mutka, and L. Ni, “Service Discovery in Pervasive Computing Environments,” Pervasive Computing, vol. 4, pp. 81-90, IEEE Oct 2005.

[8].F. Zhu, M. Mutka, and L. Ni, “A Private, Secure and User-CentricInformation Exposure Model for Service Discovery Protocols,”. Mobile Computing, vol. 5, pp. 418-429, IEEE 2006.