Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Secure Group Communication and Applications

A. Revathi*
Assistant Professor
PERI Institute of Technology,
Chennai, India

Dr. Paul Rodrigues
Principal
DMI College of Enginering,
Chennai, India

Abstract— Multicast communication is an efficient method of disseminating data to a group of beneficiaries over an open access network. Secure distribution of information to authorized recipients is an important prerequisite for group applications with commercial potential. An ever-increasing number of Internet applications, such as content and software distribution, distance learning, multimedia streaming, teleconferencing, and collaborative workspaces, need efficient and secure multicast communication. However, efficiency and security are competing requirements and balancing them to meet the application needs is still an open issue. A scalable group communication model ensures that whenever group membership changes the confidentiality of the group is to be maintained. This paper addresses the growth of secure group communications over a decade.

Keywords— Secure Group communication, Session Key, Rekeying, Multicast

I. INTRODUCTION

There has been a growing demand in the past few years for security in collaborative environments deployed for emergency services, as well as many applications including military, business, government and research organization. Examples of such collaborative applications include tele/videoconferencing, white-boards, distributed simulations, stock quote system, Pay TV, and cloud groups. All these applications depend on a framework called as secure group communication. Group communications employs IP multicasting in order to deliver the data to n receivers using a single message. Though the communication overhead is greatly reduced compared with unicasting , the security requirements becomes a big challenge. A primary method of limiting the accesses to the group data is by encrypting the contents intended for the group with a common key called as session key or group key. Since the encryption algorithm is open to all, the security relies entirely on the selected group key.

Furthermore the group key should be renewed for every change in group membership. This process is coined as Group Rekeying. The rekey policy of each group is unique but it should ensure the following security requirements.

1. Forward Secrecy
2. Backward Secrecy
3. Collision Resistance

The remainder of the article is organized as follows. The different requirements and services of a security system of a group communication is analyzed in section II. The various parameters which measures the performance of the group communication services are discussed in Section III. Section IV discusses about the diverse framework used for group communicationand the various group rekeying policies. At the end the challenges and application of group communication are summarized.

II. SECURITY REQUIREMENTS OF SGC

Secure Group communication (SGC) expects the following as the basic security needs for any applications.

1. Group Authentication – It deals with identifying the members as legitimate members and non group members. The basic authentication policy for any group framework is to allow only the legitimate members of the group to access the current group data and able to authenticate the source for the data.
2. Group Admittance Management : It specifies the level of access and permissions for group resources to each members of the with the help of access control list.
3. Group Secrecy: The most important security requirements for any group are group secrecy which ensures the communication inside the group is only by the group members in a confidential manner. The messages intended for the group is encrypted with a secret key known as group key. The group key is known to only members of the group.
4. Group Survivability: It ensures that the members of the group can bale to access any group data in the presence of an attacker.

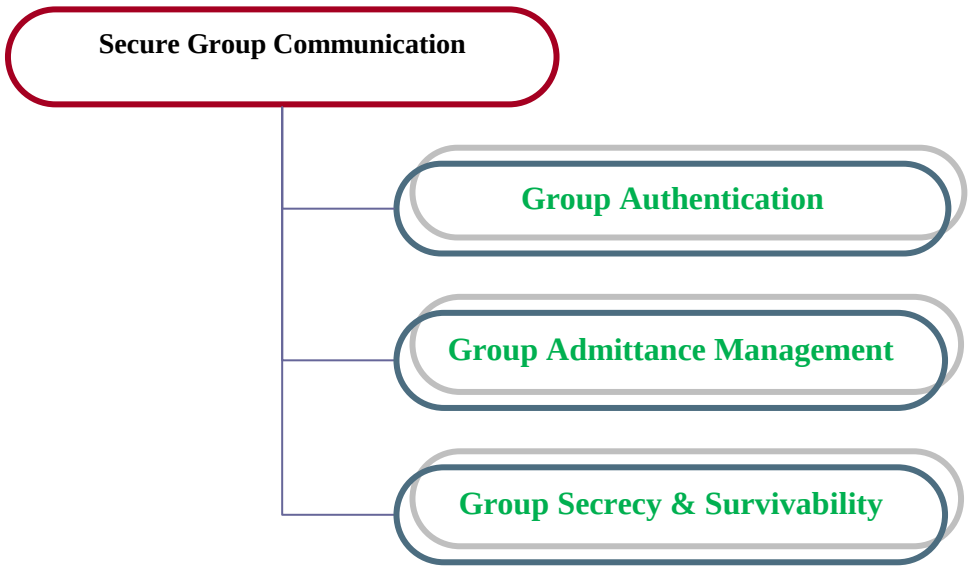

Fig 1.1. Requirements for Secure Group Communication

III. PERFORMANCE MEASURES OF SGC

This section illustrates the fundamental attributes of secure group communication and lists out the performance measurement indicators for any secure group communication.

1. Type of Group: Generally the group can be open group or closed group. The open group does not provide any admission control and the closed group allows only the authorized members of the group. For any type of group the group management framework is divided into three different ways

    a. Centralized Group Management Architecture
    b. Distributed Group Management Architecture
    c. Decentralized Group Management Architecture
2. Types of Overhead : All types of group communication network incurs three different types of overhead

    a. Storage Overhead: Amount of memory required to store the list of group members and the group key and other cryptographic materials by the members and the controller of the group.
    b. Communication Overhead: The overhead involved in communicating the new session key and other cryptographic material in order to ensure group confidentiality.
    c. Computation Overhead: It deals the process overhead involved in maintaining group secrecy.
3. Scalability: Group size should affect the performance of the group . The group should be scalable enough.
4. Resilience: It deals with the types of security threat model built to survive from any attacks. Generally the security threat model may be based on the types of attacks.
5. Most famous attacks are network based attacks and service based attacks. Attacks explores the vulnerabilities of the network.

IV. GROUP COMMUNICATION FRAMEWORK

The security of the group communication mainly resides on the group key or session key. Since the group membership is dynamic it is essential to change the group key for each member join and leave. The process of changing the group key is coined as Rekeying. The rekeying algorithm should meet the following requirements:

1. Forward Secrecy: It assures that a submissive challenger who knows a contiguous subset of old session keys cannot ascertain any subsequent session key.
2. Backward Secrecy: It ensures that a submissive challenger cannot ascertain former session key by knowing only the present session key.
3. Perfect forward Secrecy: Ensures that a compromise of a long-term key seed that generates the present short-term key(s) cannot deprive the secrecy of other previous short-term keys which have been generated by the compromised long-term key.
4. Collusion resistance: Unfeasibility for any two or more former group members who have been expelled, to gain access to future group keys even if they collude and put their keying material jointly.

Based on the rekeying policy the secure group communication framework is classified into

    a. Centralized Group Key Management Architecture
    b. Distributed Group Key Management Architecture
    c. Decentralized Group Key Management Architecture

A. ***Centralized Group Key Management Architecture:***

In this architecture only one entity controls the entire group called as Group Controller (GC). Since it is an independent unit it does not wait for any other to generate and communicate the new key. But it suffers with a major problem of "1 affects n". If the GC fails then the total group function abruptly stops. The overall performance depends only on the group controller. And also the scalability is a major issue. The efficiency of the protocols under this are measured by size of the rekeying messages. The various benchmark protocols under this are

1. GKMP (Group Key Management Protocol)
2. LKH (Logical Key Hierarchy)
3. OFT (One-way Function Tree)
4. OFCT (One-way Function Chain Tree)
5. FT (Flat Table)
6. ELK (Efficient Large group Key)

B. ***Decentralized Group Key Management Architecture***

The whole is subdivided into various subgroups and each subgroup is controlled by a central entity in the subgroup. Different controllers used are to avoid the problem of single point of failure. It supports the graceful degradation. In addition to the standard performance measures the following are also used in this category.

a. Decentralized Controller
b. No of Subgroups
c. Rekey Policy in a subgroup

The various benchmark protocols under this are

1. SMKD (Scalable Multicast Key distribution)
2. Iolus
3. DEP (dual Encryption Protocol)
4. CS (Cipher Sequences)
5. Marks
6. Kronos
7. IGKMP (Intra-domain Group Key Management)
8. Hydra

C. ***Distributed Group Key Management Architecture***:

It follows the principle of no group controller. The Group key is generated in a contributory fashion by all the members of the group or any one member of the group. It is fault tolerant. But the computation time increases linearly with the group member. It is very important to ensure the integrity of the rekey messages. In addition to the standard performance measures the following are also used in this category.

a. Processing during setup
b. Number of rounds
c. Number of Rekey Messages

D. ***Group Rekeying Algorithms***

The process of changing the group key for members join and leave is termed as group rekeying. Group Rekeying can be classified into

1. Immediate Rekeying
2. Batch Rekeying
3. Exposure Oriented Rekeying

Immediate Rekeying: Algorithms which ensures that for each change in group membership the rekeying mechanism is executed. This is suitable for application like military communication

For large and dynamic groups implementing ideal forward and backward secrecy may be infeasible because of the increased cost of rekeying. The standard approach is to amortize the rekeying cost over multiple join / leave. With this idea Batch and Exposure oriented rekeying algorithms are proposed.

Batch Rekeying Algorithm: Individual rekeying is inefficient due to overhead involved in computing and communicating the new key for every change in membership. It also induces the problem called as "Out of sync" problem. Batch rekeying algorithms can be ideal solution for application where forward and backward secrecy can be relaxed for while.

Exposure Oriented Rekeying: In this rekeying, the total number of join and leave is collected when it crosses the limit defines as threshold value the rekeying algorithm is executed.

V. CONCLUSIONS

In this paper a detailed survey is presented in the area of secure group communication. First the security requirements are discussed. The difference performance measurements indicators are explained. The classification of group key management algorithms and the benchmark algorithms are compared for each category. The different rekeying policies and the application where these rekeying algorithms can be employed are also discussed

REFERENCES

[1] S.Rafeli and David Hutchison, "A survey of Key Management for Secure Group communication" ACM computing Surveys, vol.35, No.3 (2003), pp. 309-329.

[2] Vasanthi. A and Dr.T. Purusothaman, "Optimizing Batch Rekeying Interval For Secure Group communication Based on Queuing Model", Journal of Computer Science, 10(2) 2014, pp. 325-329.

[3] Sakarindr P and Ansari N, "Survey of Security Services on Group Communication", IET Iform.Security, Vol 4 2010, pp. 258-272,

[4] E.L. Hahne, A.K. Choudhary, Dynamic queue length thresholds for multiple loss priorities, IEEE/ACM Transactions on Networking, vol.10, (3) (2002) 368-380.

[5] Simon T Jones 2006, 'IPTV Delivery Architecture', ITU-T IPTV Global Technical workshop, Korea.

[6] Inshil Doh, Jiyoung Lim & Min Young Chung 2012, 'Group Ley Management for Secure Mobile IPTV Service', Proceedings of the Sixth International conference on Innovative Mobile and Internet Services in Ubiquitous Computing IMIS, pp. 352-357.

