IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Novel Group Key Management Service for Sharing Data through Wireless Network that Ensures Better Security

A. Subashini

Assistant Professor, Computer Applications, Faculty of Science and Humanities, SRM University, Chennai, Tamilnadu

Abstract: In the fast growing wireless network and mobile technology, we have experienced several group based services. Group key management is an essential building function for secure multicast architecture. The existing GKM-Group Key Management Services accomplish to establish the communication within a single group and it may not fit into multiple multicast group circumstances because of inadequate use of keys. The rekeying overheads are occurred in GKM approach. In the suggested approach, the Master Key Encryption based MGKM Scheme will reduce the releasing overheads from managing multiple group key. The Key Distribution Center will generate the master key and multiple slave keys will be generated depending upon the group added or removed. This will increase the data security, where the authorized user can access data and unauthorized user may not able to access the data.

Keywords: Group Key Management, Key Distribution Center, Master Key Encryption-Multiple Group Key Management, Group Controller.

I. INTRODUCTION

Multicast is one of the method to transfer the data from single source to multiple groups. Simply the transmission range will accept a single source received by all nodes. Open source transmission (Broadcasting medium) will be accessed by anyone and there will not be security when the message is transmitted through air. The regular method is to titan the security control for group communication by providing identical key. It is known as group key. It should be used only by the number of the group. All data can be encrypted and decrypted through this group key which will ensure secured communication for data transfer from one group to another group. But the challenges here are to maintain the efficient key management. Since the group members should update the key information before leaving or joining the group which will trigger rekeying concept. To reduce this rekeying overhead a tree based GKM should be revisited. Anyway the current GKM still has constraint of rekeying as the number of multiple services increases.
In a dynamic multicast group, GC will issue a session key. With this key, the GC is a secure multicast channel to allow the authorized group members. The GC reissues a new session key when the group membership changes. The rekeying procedure will ensure the security of the new session that of the previous earlier sessions. That is the new member can't receive the communication of previous sessions and also old members who left the group can't access the new session. So that both forward and backward secrecy of group communications are maintained.

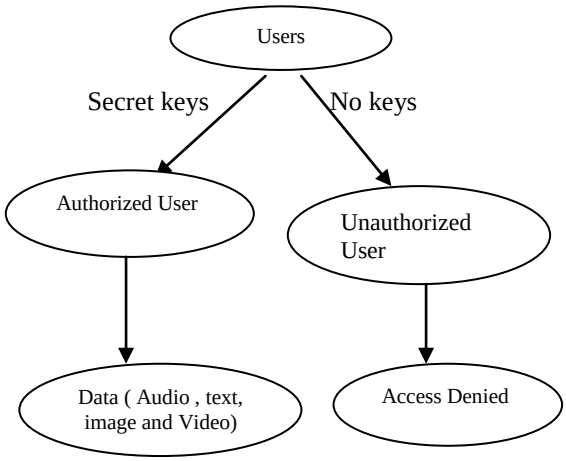
II. GROUP KEY MANAGEMENT SCHEME

A Key Distribution Center (KDC) is a system that will provide keys to the users in a network. It will share private information. Each time a connection is provided between two computers in a network, they send request to the KDC to generate a secret key which will be used by users for validation.
A Key Distribution Center is in the form of symmetric encryption that will provide access of two or more systems in a network by generating a token to establish a secure connection over that data can be either shared or transferred. It is the main server which is connected before proper communication takes place. It is used in smaller networks where the connection requests do not upset the system. It is used instead of key encoding because the secret key is created each time a connection is established, that reduces the possibilities of attack.
Group key management is very critical functional group in multicast services. When we send data to set of receivers in multicast services, data security is managed by two ways. Group Controller needs authentication access, key server required, distribution of keys depending on the key management structure. Group controller should authenticate when a new member joins in a group.
The members can leave any group and rejoin to that group at any interval. Rekeying facilities will be provided for them instantly. An authorized user can convert plaintext to cipher text and cipher text to plain text. An unauthorized user cannot access the text. He/she should have the keys to access the data. Data may be in different format.

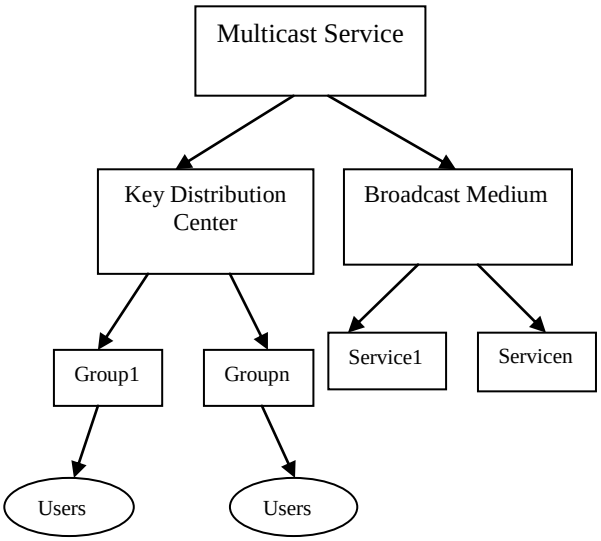
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017



Types of Users



The Overall Structure of Multicast Service

III.PROPOSED SYSTEM

In this paper, we investigate the differences between securing multicast communication and security unicast communication. These differences create scalability issues for many applications. We say that these issues are fundamentally different in terms of managing keys. Furthermore, we show how these differences create scalability problems for many typical applications.
In this paper, we propose a new group key management technique for various groups known as Multiple Group Key Management Scheme. The single and multimove across a wireless network was managing for MGKM protocol. It will minimize rekeying transmission overheads. In this scheme, a master key and multiple slave keys are created from the Master key Encryption algorithm. This scheme is used for providing a group key to the users. This will reduce the rekeying problem by updating the asymmetry of the master and slave keys. That is one of the slave keys is updated, the other keys can be unchanged by changing the master key. The steps to encrypt and decrypt data are:

- The files should be selected and uploaded into the server.
- Create the cluster formation of subscribers are developed and for each subscriber within the cluster a separate IP address is created.
- For each cluster a domain key is dynamically created in a random way.
- Keys are randomly created for each cluster.
- The resultant file will be in encrypted format.
- To decrypt the file with the help of area key and domain key should be given.

IJARCCE

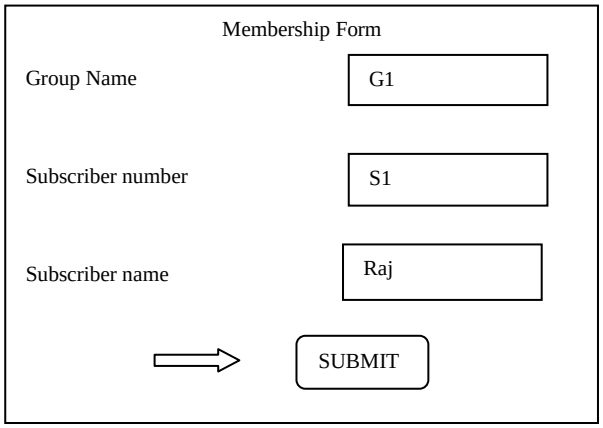
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

This system contains three modules: Registration form of Users, Key Methods and Rekeying Process

A. Registration form of Users

Each user must register their information and register through server. Then server will provide the multiple services to use. Each user has to fill group name, subscriber number and subscriber name to create a group.



Group Creation

B. Key Methods

Group key management is concerned with creating and updating private keys. It is the basic technique to secure group communication. Key Management facilitate the data confidentiality and access control by ensuring that the keys used to encrypt group communications to share only authorized members. These members can access group communication. For authentication purpose shared group key can be used. The messages should be sent from an authenticated group member. To prevent these issues, the following two security methods are essential for the group key distribution in a secure multicast communication.

Forward Secrecy: when a member left a group, he/she cannot decrypt encrypted messages transmitted after leaving.
Backward Secrecy: when a member joins in a new group, he/she cannot decrypt encrypted messages before joining.
The process for forward and backward secrecy requires reproducing of the group key. This is known as rekeying.

KDC must generate a master key and many slave keys through this proposed system. The number of service group increases as the number of data group increases.

C. Rekeying process

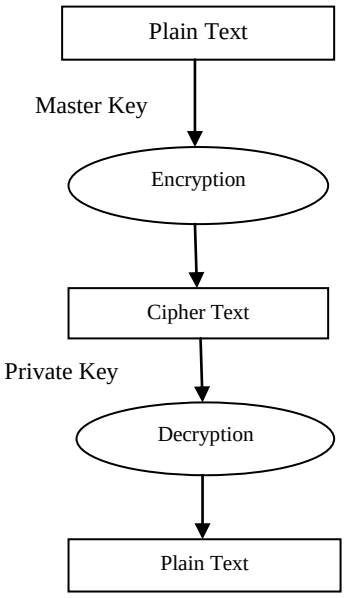


Diagram to convert plain text to cipher text and vice versa (Using Master key and Private Key)

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

Rekeying is split into centralized, decentralized and contributory schemes in Group Key Management protocols. The domain key distributor is also known as the centralized server. Consider the case that a member updates membership. He/she has been subscribing to system1, but wants to access to s2 while having system1. The KDC must switch user's membership from one service group to another service group. Data of system1 might not be visible to that user after he/she un-subscribed from system1. For forward method, the KDC must revoke all the keys. For revoking all the keys, the KDC updates the old slave key to a new slave key to make a new master key through the new proposed master key management method.

IV. CONCLUSION

In this paper, Multiple Group Key Management technique has been proposed for multiple groups for accessing data. In an existing system symmetric keys are generated for members to access data. In proposed system asymmetric keys, master key and slave key are generated by using a set compromising master key and slave key. So number of rekeying is reduced. Therefore graph of this proposed system is simpler than any other system, less memory is enough to store the keys. This scheme can reduce storage and rekeying process. This scheme makes the computation complexity greatly reduced.

REFERENCES

[1] C.K. Wong, M.G. Gouda, and .S. Lam (1998), "Secure group communications using key graphs", ACM SIGCOMM Computer Comm. Rev., Vol. 28,pp.68-79,1998.
[2] S. Rafach and D. Hutchison (2003), "A survey of key management for secure group communication", ACM Computing. Surveys, vol.35,pp.309-329.
[3] Y. Challal and H. Seba (2005), "Group Key Management Protocols: A Novel Taxonomy," International Journal of Information Technology, Vol. 2, No. 1, pp. 105-118.
[4] Zhang.Q and Wang.Y(2004), "A centralized key management scheme for hierarchical access control", in IEEE Globecom. IEEE Communication Society, pp. 2067-2071.
[5] D.M. Wallner, E.J. Harder and R.C. Agee (1999), "Key Management for Multicast Issues and Architectures", IETF RFC 2627, http://www.ietf.org/rfc/rfc2627.txt.
[6] Qiong Zhang, Yuke Wang and Jason P. Jue (2008),"A Key Management Scheme for Hierarchical Access Control in Group Communication", in International Journal of network security, Vol.7. No.3, PP.323-334.
[7] T.T Mapoka(2013), "Group key management protocols for secure mobile multicast communication: A comprehensive survey",Int. J. Comput Appl., vol.84, pp.28-38.
[8] T.Ballardie(1996), "Scalable Multicast Key Distribution", RFC 1949.