"A Survey On A Low Cost Multi Group Multicast Key Distribution Scheme In Wirless Network"

Prasanna G
M Tech Student
Dept of CSE
VTU,East West Institute of Technology
Bangalore, India

Guruprasad
M Tech Student
Dept of CSE
VTU, EWIT
Bangalore, India

Dr Arun Biradar
HOD
Dept of CSE
VTU, EWIT
Bangalore, India

Abstract

The group key management is a key management system in which same key is assigned to all member of the subscribed group. In this group key management same key is used for both encryption and decryption. The group key management provides the better security because of same key is used for both encryption and decryption process and it has greater key overhead due to group member changed, some times the group member leaving or new member joining to the group. To over come this problem we are use the master key encryption based multiple group key management scheme. This scheme based on the asymmetric key (i.e,different key is used for encryption and decryption).It is efficient method for key distribution to multiple multicast group and reduces the communication overhead, storage overhead and it can be established in single netw reduces the key overhead.

Keywords-Security,group key manageme ork. The multiple group key management scheme nt,multicast chinese remainder theorem,master key encrption.

1.INTRODUCTION

Multicast is most important in wireless network, multicast is the process of delivery of data from single point to multi point in a single transmission can received by all node within limited transmission range. The group key management has high security because of all member of subscribed group use the same key for both encryption and decryption and in this management access control mechanism is adopted. In this system group key (shared key) is updated according to the new member joining or subscribed member is leaving the group this is refers to rekeying. To over come this problem we are use tree based master key encryption management system. In group key management provides the confidentiality, authenticity and integrity of messages delivered between group members.

We are present a new multiple group key management scheme is called as master key encryption multiple group key management scheme(MKE MGKM) it has a master and multiple slave in this system message is encrypted by master and decrypted by each of individual slave key. Master key encryption generates a master key and slave key according to membership changed. In this method changes the key of member and there is no change of remaining members keys, and also presents graph for tree, it is a non cyclic graph with two types nodes and they are **u** node that reprints the users and **k** nodes reprints keys. In MKE MGKM maintain forward and backward security , forward security means that leaves member cannot the learn the new group key and backward security means that newly added member cannot learn previous group key.OFT maintains the perfect forward and backward security or secrecy[6].

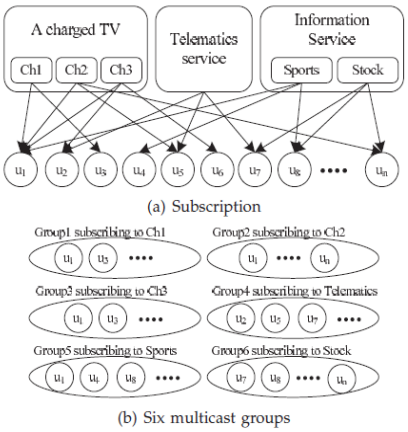

Fig. 1. An example of multiple groups in a wireless network

The above figure shows the multiple groups in wireless network, the user1 and user2 subscribed the ch1service of A charged TV and user1 and user5 they are subscribed ch2 services of A charged TV and user2 also subscribed ch3 service of A charged TV. In multiple group system same user subscribed several channel and who they are subscribed the same channel and they are combined together and all the group member has group key or shared key and both encryption and decryption is done by a group key or shared key, the shared

key is same for all group members. suppose that whenever one member of the group is leaves the group or any new comer join to the group that is major problem in the this system. After member leaves the group that group shared key should be changed because of in order to maintain the forward secrecy and another major problem is suppose that new comer joining to the group at that time also change group key in order to maintain the backward secrecy. In both case more rekeying overhead and storage overhead and communication overhead of users to maintain the multiple group system and over come those problem by introducing the master key encryption based multiple group key management scheme. In this scheme creates and updates a master key and multiple slave key and message is encrypted by master key can be decrypted by each different slave key and vice versa. The key feature of the master key encryption is that one of slave keys can be revoked by regenerating the master key through a simple computation and the other slave keys can be kept valid. This enables us to reduce the rekeying overhead.

2 RELATED WORK

In group key management system rekeying overhead high communication overhead and storage overhead are the main drawbacks of existing GKM. And rekeying overhead procedure as follows, In multicast group, several user subscribes the different services same services combine into group and generates the key for that group members, In this system group key is symmetric key and this key is used for both encryption and decryption. Suppose any one of the subscribed member leaves or new member joining to the group we are provides the new key for all group members. Suppose we are does not provide new key,the leaves member of the group is able to get the all services without the payment and new member joing to the group also generate the key for new member with new key for all reaming member of that group. Key Generating for the group member after the membership changes that requires more memory space for rekey storage and also occurred communication overhead.

To improve the high level of security in group key management , group shared key be changed after every join and leaves to group so that former group member has no access to current communication and a new member has no ac cess to previous communication. The large groups whose members join and leave frequently pose a scalability and security by using forward and backward secrecy. The existing group key management method is applicable to only single multicast group and it is not applicable to multiple multicast service system.

To overcome the drawback of existing system and maintain the backward and forward secrecy by using master based algorithm called as multiple multicast group key management system. In this method we are use logical data strucrure, the logical data structure is level of key system and logical total 3 levels

1. key encryption key.

2. Traffic encryption key.

3. Individual key.

In this tree structure traffic encryption key is a root node and individual key is a leaf node and key encryption key is a rest of node in tree strucutre and it has the path from leaf node to root node. In a network each user subscribed one or more services among a total of M multicast services and multicast broadcast services denoted by MBS1, MBS2……..In this model two types user group they are data group and service group, The data group contains the all the users who subscribed to MBSN and service group contains a set of usera who subscribe to same set of MBS and data group is denoted by (DG1, DG2……..DGm) and service group is represented by SG1, SG2……

2.1 HIERARCHICAL ACCESS CONTROL

Network application are most important to world they are teleconference,information services this application are based on the group communication and securing the group communication is very important for maintain confidentiality ,authenticity and integrity of message delivered between the group .we present the three strategies for securely distributing rekey message after join/leave and specify protocol for joing and leaving secure group.First network are based upon the client server paradigm and make use of point to point message delivery and every to point to multipoint communication can represented as a set of point to point communication.The server and client communication mutually authenticate each other using a authentication protocol and a symmetric key is created and shared by them to be used for pairwise confidential communication this proceduer can be extend to a group as fallows.

Let there be a trusted server which is given membership information to up access control,when a client wants to join the group,the client and server mutually authenticate using an authentication protocol, having authenticated using an authentication and accepted into the group each member shares with the server a key to be called the member individual key for group communication,the server distributes to each member group key to be shared by all members of group.The group contains n member and distributing group key securely to all member the n message encrypted with individual key,all mesage may be sent seperately via unicast altenatively the n message may be sent as a combined message to all group member via multicast,The q cost proportional to group size n,consequently the group key should be changed frequently,To achieve a high level of security,the group key should be changed after eve changed after every join and leave so that a former group member has no access to current communicationand new member has no access to previous communication.Let there be a trusted server that creates a new group key after evry join and leave.After every join, the new group key can be sent via unicast to the new member and encrypted with its individual key and via multicast to existing group member encrypted with prevoius group key ,changing theer group key securely after a join is too much work,previous group key can no longer.

To solve above problem we are use the hierchical access control, most existing group key management are designed for single level access control ,the hirarchicared by all access control is provides the hirarchical group access control for multiple group key management.In this method the group access control is make by encrypting the content using an encryption key known as session key that is shared by all logitimate group members and group membership will most likely be dynamic with users joining and leaving .The group communication group key and cannot decrypt the group key management scheme that do not allows unauthorized entitiess do not accees the group communication.The existing key management address the access control issues in one multicast session.

The hierarchical group access control provides the access control an on thd updating keys with dynamic member ship and it allows all grol is mainly focusoup members are same level of access privilege,The users who possess the decrypting data key have the full access to the content and users who do not have the decryption keys cannot interpret thedata,some group application contains multiple related data streams and group member have different access privileges.The multimedia applications distributing data in multi coding format. Receivers can receives the normal format and extra information needed to archive HDTV resolution and multicast program containg several related services[8].

The group member subscribed to different data streams or possibility multiple of them,it is necessary to develop an access control mechanism that support multi level access privielege which is referred to as the hierachical group access control.In hierarchical access control is mainly focus on the centralized multi key management scheme and into divided this system key management protocol is divided into two category.They are (1)centralizepedent and (2)contributory.In centralized key ma nagement relies on a centralized server this is known as key distribution center which creates and distributes encryption keys. In the contributory of key management there is no use KDC and group member contribute independent keying matrix and all participatent in group key establishment.The key management schemes are designed for a single multicast session,where all group members have same privilege for group application containing multiple related data streams and member with various access privilege,directly applying the existing scheme can lead to inefficient solutions.In centralized key management protocols have logical tree structure is used for maintain materials and coordinate key generation and this protocol is scalable in the terms of communcation, computation and storage overhead.The KDC maintains a key tree,where each node on the tree corresponds to a user's privacy key,group key or KEK and rekeying overhead for user joining and leaving.The Rekeying overhead at KDC is (2log(n)) is reduced to log(n) by using one way function tree.Hierarchical access control can be achieved in either centralized or contierarchributory mehod[8].

2.2 Centralized multi group key management scheme

One way to solve the hierarchical access control problem is to using existing tree based key management scheme, this scheme use a logical tree structure to maintain keying materials. In this method each node of the key tree is associated with a key and the root of the key tree is associated with the session key (Sk),Ks, which is used to encrypt the multicast content and each users associated with the user's private key Ui which is only known by this user and KDC.The intermediate node are associated with key encrypted key and this key is used for protecting the session key and other KEKs.The key distribution center knows all keys on the key tree, each users knows his private key ,the session key and set of KEK,on the path from himself to the root of the key tree. Each key has the secret materials that is the content of the key and a key selector that is used to distinguish the key, when a users leaves to be updated in order to maintain forward secrecy, when a user join the service the KDC chooses a leaf position on the key tree to put the joining users, the KDC updates the key along the path from the new leaf to the root by generating the new keys from the old key using a one way function [8].

2.3Contributory multi group key management scheme.

The tree based scheme for contributory is applying to two party DH protocol amongest two subgroup of users,the user in the first subgroup who share a common subgroup key Kiand users in the second subgroup, who share a common subgroup key Kj and users in two subgroup compute a new key these two subgroups can be combined into a large subgroup that share the common key Kij.The key tree for contributory is same as the centralized tree structure.The intermediate keys and the group key are generated from bottom to up.In this method users are grouped into pairs and perform two party DH and two users from a subgroup,each pair of subgroup perform DH and combined into a larger subroupgroup with shared key,finally all users are merged into a one group that share the group key[8][9]. All the above problem is overcomes by using master key encryption based multiple group key management scheme.

CONCLUSION

In this paper, a multiple group key management scheme has been proposed, that can enhance the management performance of multiple group keys regardless of the hierarchy of the users or the data streams. In contrast to other existing schemes using only symmetric keys, the MKE-MGKM scheme exploits asymmetric keys, i.e. a master key and multiple slave keys, which are generated from the proposed master key generation

algorithm. By using a set comprising a master key and slave keys, a TEK can be efficiently distributed to multiple SGs. Therefore, the number of rekeying messages can be dramatically reduced. Also, since the key graph of the MKE-MGKM scheme is much simpler than that of other schemes, less memory is needed for storing the keys. Compared with other schemes, the MKE-MGKM scheme significantly reduce the storage and communication overheads in the rekeying process, with acceptable computational overhead. It is expected that the MKEM GKM scheme can be a practical solution for various group applications, especially for those requiring many service groups, such as TV streaming services charged on a channel by channel basis.

REFERENCES

[1] *IEEE Std 802.16-2004, Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, IEEE, ´ Edition 2004.

[2] 3GPP, "3GPP TS 22.146 v.8.3.0 (2007-06) 3rd generation partnership project; technical specification group services and system aspects; multimedia broadcast/multicast service; stage 1 (release8)," June 2007.

[3] C. K. Wong, M. G. Gouda, and S. S. Lam, "Secure group communications using key graphs," 1998.

[4] D. M. Waller, E. J. Harder, and R. C. Agee, "Key management for multicast: Issues and architectures," Internet Engineering Task Force, Internet Request for Comment RFC 2627, June 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2627.

[5] Y. Challal and H. Seba, "Group key management protocols: Novel taxonomy," *International Journal of Information Technology*,vol. 2, no. 1, pp. 105–118, 2005.

[6] Sherman and McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEETSE: IEEE Transaction son Software Engineering*, vol. 29, 2003.

[7] J.-C. Lin, F. Lai, and H.-C.Lee, "Efficient group key management protocol with one-way key derivation," in *LCN*.

[8] Y. Sun and K. J. R. Liu, "Hierarchical group access control for secure multicast communications," *IEEE/ACM Trans. Netw*,vol. 15, no. 6, pp. 1514–1526, 2007.

[9] Q. Zhang and Y. Wang, "A centralized key management scheme for hierarchical access control," in *IEEE Globecom*. IEEE Communication Society, 2004, pp. 2067–2071.

[10] D. WALLNER, E. HARDER, and R. AGEE, "Key management for multicast: Issues and architectures," IETF, Request for Comments2627, 1999.

[11] R. L. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[12] K. Koyama, "A master key for the RSA public-key cryptosystem,"*Systems-Comput.-Controls*, vol. 13, no. 1, pp. 63–70 (1983), 1982.

[13] A. Kondracki, "The chinese remainder theorem," *Formalized Mathematics*,vol. 6, no. **4**, pp. 573–577, 1997.

[14] L.R. YU and L. B. LUO, "The Generalization of the Chinese Remainder Theorem," *Springer ActaMathematica Sinica*, vol. 18, no. 3, pp. 531–538, 2002.

[15] X. Zou, B. Ramamurthy, and S. S. Magliveras, "Chinese remainder theorem based hierarchical access control for secure group communication," *Lecture Notes in Computer Science*, vol. 2229, pp.381–385, 2001.

[16] X. Zheng, C.-T. Huang, and M. M. Matthews, "Chinese remainder theorem based group key management," in *ACM Southeast Regional Conference*, D. John and S. N. Kerr, Eds. ACM, 2007, pp.266–271.

[17] G. Caronni, M. Waldvogel, D. Sun, N. Weiler, and B. Plattner,"The VersaKey framework: Versatile group key management,"*IEEE Journal on Selected Areas in Communications*, vol. 17, no. 9,pp. 1614–1631, Sept. 1999.

[18] Y. Kim, A. Perrig, and G. Tsudik, "Simple and fault-tolerant key agreement for dynamic collaborative groups," in *SIGSAC: 7thACM Conference on Computer and Communications Security*. ACMSIGSAC, 2000.

[19] H. Lu, "A novel high-order tree for secure multicast key management,"*IEEE Transactions on Computers*, vol. 54, 2005.