International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)

International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Secure Multiple Multicast in Wireless Network

J. Rini Angeline Vinshia (M.E)[1], Mr.Pugalenthi M.E., (Ph.D).[2]

M.E (C.S.E) – II year, St. Joseph's College of Engineering, Chennai, India
Professor – C.S.E. Department, St. Joseph's College of Engineering

[1]riniangeline90@gmail.com, [2]pugalsir@gmail.com

***Abstract*-With the emergence of diverse group based services,multiple multicast coexist in single network,user may subscribe to multiple group.However the existing froup key management,aiming to secure communication with a single group,are not suitable in multiple group because of inefficient keys,and much large rekeying overhead.In this paper,propose a new GKM for multiple multicast group,called master key encryption based multipl multiple group key management scheme(MKE-MGKM).This MKE_MGKM exploit asymmentric key that is master key and multiple slave keys,which are generated from proposed master key encryption(MKE)algoritm and is used for efficient distribution of group key.It alleviates rekeying overhead by using asymmentry of master and slave keys. That is even if one of the slave key is updated,the remaining one can be still unchanged by modifying the master key.Through numerical analysis and simulation it is dhown that MKE-KGKM can reduce storage overhead of key distribution centre by 75% and storage overhead of user by 85% and 60% of communication overhead,compared to the existing scheme.**

***Keywords*-Security, groupkey management, multicast, Chinese remainder theorem, master key encryption**

I. INTRODUCTION

Multicast is an efficient method in transmitting the data from single soure to several destination. Especially, in wireless network using a broadcast medium, a single transmission can be received by all nodes within a transmission range, which make it easy to implement the multicast. Therefore, multicast paves efficient way for multiple group communications, by which many group based application, such as charged video on demand or video conferencing, can be commercialized.

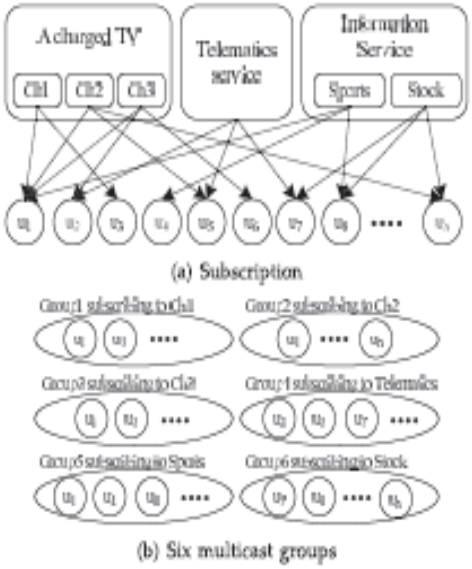
The broadcasting medium, however, makes the wireless network to various security attack since anyone can eavesdrop message transmitterd in the air.

To implement the multicast that is delivery of message to the member of the group, in wireless network, we need to have an access control mechanism for broadcasted message, which guarantees confidentiality, protects digital contents, and facilitate accurate accounting. Therefore, it is one of the key requirement for successful commercialisation of the multicast service in wireless networks.

The usual way to provide an access control mechanism for secure group communication is by using symmentric key, known as group key, shared only by group members. Messages, encrypted by a member having a group key, can be decrypted by the another group member having the same group key, which can guarantee secure group communication. Although this mechanism, using the shared group key,is an efficient way to guarantee security, it causes difficulties in maintaining efficient key management scheme since the user must be updated before leaving or joining, which is refered as rekeying. To reduce the key mangement overhead from rekeying, a tree based group key management (GKM) have been studied.

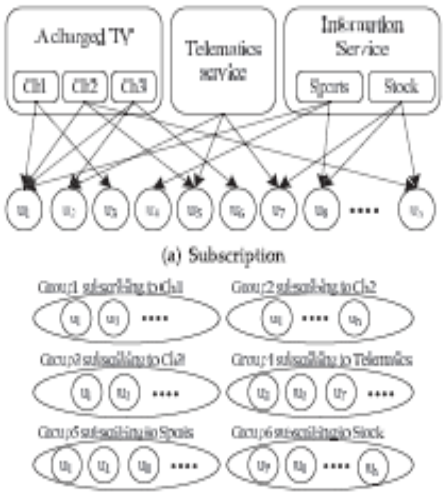
However the existing GKM still faces the limitation of rekeying as the no of multicast services increases. However, in the foreseeable future, multiple multicast group will exist in a single network due to the emergence of many group based application. In such a situation, service provider suffer from the key management overhead for supporting multiple multicast groups. For example, service provider may provide three different multicast in wireless network such as charged TV streaming, a telematics service and an information service. In this example, there will be three user groups for three services, each of which should be managed according to the membership record of the service provider. Moreover, if the subscription for the channel is either charged for each channel or content, the service provider must manage additional user group, for accurate accouting.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)



(a) Subscription

(b) Six multicast groups



(a) Subscription

(b) Six multicast groups

II. Overview

The usual way to provide access control mechanism for secure group communication is to employ symmentric key, known as group key, shared only by group members. Messages, encrypted by a member having the group key, can be decrypted by another group key having the same group key, which can guarantee secure group communication.

Although this mechanism, using the shared group key,is an efficient way to guarantee security, it causes difficulties in maintaining key management system since the group key must be updated according to the membership change such as user member leaving or joining refered as rekeying. However, the existing GKM still faces the limitation of group key as the no of multicast service increases.

A new group key management called multiple multicast group called master key encryption based multiple group key management (MKE-MGKM) is used in the proposed system.

The MKE-MGKM exploits asymmentric key that is master key and multiple slave key, which are generated from the proposed master key encryption algorithm,and is used for the efficient distribution of group key

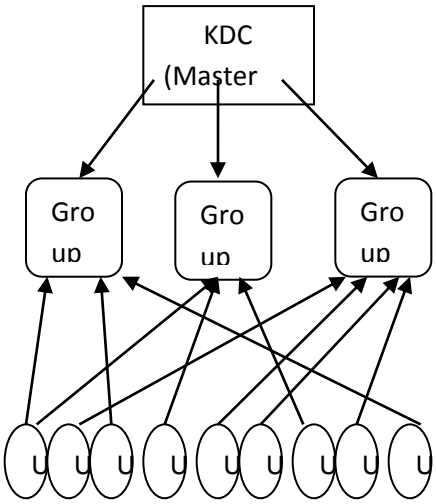
It alleviates the rekeying overhead by using asymmentry of master ans slave key, that is even if one of the slave key gets updated, the remaining ones will be still unchanged by modifying only the master key.

The Master key Management Algorithm created and updates the master key and multiple slave key.A message encrypted by master key can be decrypted by several slave key, and vice versa. The key feature of MKE is that one slave key can be revoked by updating master key with simple computation whereas the other key kept valid.This enable us to reduce the rekeying overhead.

The Rekey for presenting multiple group using the MKE-based key graph having master key and multiple slave key

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Proposed Architecture Diagram



III. RELATED WORK

Group Key Mangement Protocol: A Novel Taxonomy

Group Key Management is the important functional group for multicast services. The invention of internet leads to various services, combining voice, video and text over IP. Athough unicast is predominant sofar,for media services. Indeed, multicasting is useful for group oriented and in video conferencing, interactive group games, video on demand, TV over Internet, elearning, software updates and database replication. however lack of security cause lot of problem in multicasting.. These issue with certain ranges. In public broadcasting, while authentication is a fundamental requirement, confidentiality may not be.

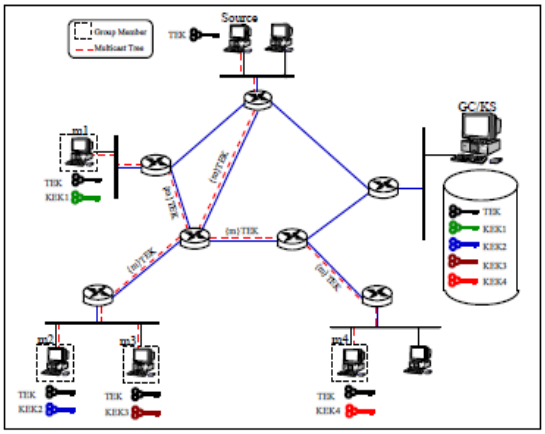
In the contrary case, both confidentiality and authentication are required in video conferencing application. In this paper focus on key store management over wired network:

Group Key Management.

The limition in research have caused lot of confusion in multicast, such as confidentiality, authentication, water marking and access control

Group Communication Confidentiality

The challenging feature for confidentiality. we select a source that sends data to set of receivers in multicast services. The Security is managed by two sessions: Group controller (GC) required for authentication, authorisation and acess control, key server required for distribution of keys. depending on key management architecture.



Simple scenario of Group Management

To ensure confidentiality of Group Management,the sender should share with all valid mambers, called traffic encryption key(TEK).To multicat a secret message, it should encrypt with symmentric key algorithm. upon receiving multicast encrypt message, each valid member can decrypt with TEk and recover the original one. To avoid leaving or rejected member from the group, continue to decrypt the secret message, the Ks must distribute TEK and distribute the valid members except the leaving one. This operation is called rekeying. The KS must distribute the Key Encryption Key(KEK) to all member. To rekey, a leave from the group, the KS generates a new TEK: TEK' sends to each member sends it to corresponding KEK. The leaving member doesn't know KEK' and cannot decrypt future multicast messages.

When a new member joins a group, it must be authenticated by the GC. After checking the access of group, they introduce rekey which avoids decrypting of messages using an old member who is not active.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Therefore KS generates a new TEK: new TEK' encrypts with a old TEK, and it multicast to the group. Henceall old member could recover the new key.so it sends to TEK' to decryt the message.

The encryption and distribution of key in rekeying is refered as Group Key Management. In this illustrative protocol, rekey induce a new key after leaving of a member(n) where n is the group members. It induce a storage of O(n) during the multicast services. Since each membership change needs an updation its highly dynamic, without using storage overhead. Proposed architecture in this literature, best storage performance.

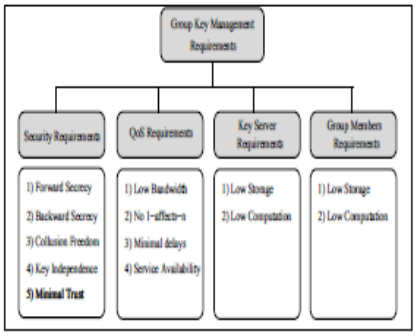
Group Key Management Requirement

Efficient Group must manage with the following requirement.These requirement from four point of view.

- Security
- Quality of service
- KS resource and
- Group member resource

It is represented in the following

Diagram



Group Key Management Requirement

Security Requirement

1. Forward Secrecy who left the group have no access of new grop. This ensures that group member leaving cannot decrypt using the od key and enter the future enhanced work. To assure forward secrecy, after leave a new TEK is the new solution.
2. Backward Secrecy ensures that new user must not have access over the old records. It ensures that data must not encrypt befor joining a group. To ensure the background ssecrecy, after join of new TEK is the ultimate solution.
3. Collusion Freedom ensures that any fraudulent user should use the traffic encryption key
4. Key Independence: a protocol is said to be key Independent,if a disclosyer does not compromise other key.
5. Minimal Trust: The key management must not trust any other entities.Otherwise,the deployment of key would not be easy

Quality Of Service Requirement

1. Low Banwidth Overhead: the rekey must not ensure a group of messages, especially for dynamic groups. Ideally, this should be independent of group size.
2. 1-affects-n:a protocol affects 1-affects-n since one group change will affect the number of group in a message.This affects the new group key member should be updated.

IV. Proposed System

In this paper, we propose a new group key management scheme for multiple multicast groups, called the master-key-encryption-based multiple group key management (MKE-MGKM) scheme.

The MKE-MGKM scheme exploits asymmetric keys, i.e., a master key and multiple slave keys, which are generated from the proposed master key encryption (MKE) algorithm, and is used for efficient distribution of the group key.

It alleviates the rekeying overhead by using the asymmetry of the master and slave keys, i.e., even if one of the slave keys is updated, the remaining ones can still be unchanged by modifying only the master key.

Modules:

1) User Enrollment
2) Master Key Management Algorithm
3) Rekeying at membership change

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

User Enrollment:

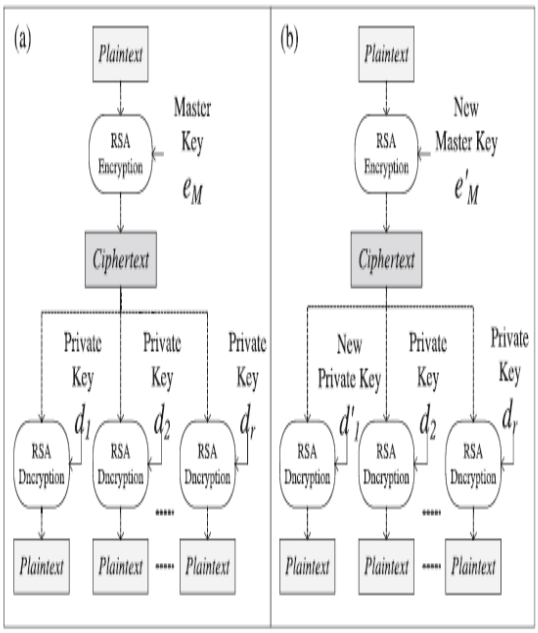
Each User should register their personal details and submit to the server, after submitting server provides the multiple services to access.

Master Key Management Algorithm:

Multicast Broadcast Services are provided in a network, First of all, the KDC generates a master key, and as many public-private key pairs as the number of Service Group (SGs), through the new proposed master key management algorithm. The number of SGs grows exponentially as the number of Data Group (DGs) increases.

Rekeying at membership change:

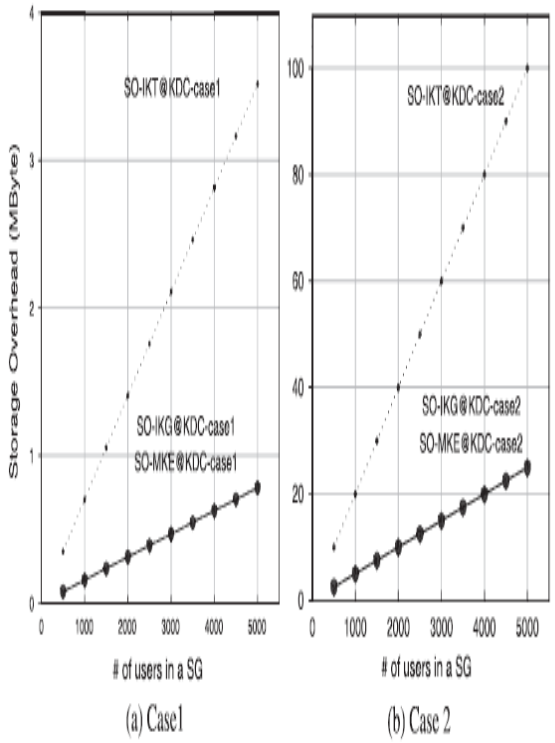
In order to describe the rekeying process of the MKE MGKM scheme, consider the case that a user changes membership. He has been subscribing to particular *MBS1*, but wants to subscribe to *MBS*2 instead of *MBS*3 while keeping *MBS*1. Therefore, the KDC should switch user's membership from *SG* to particular *SG*, which makes user lose the access privilege to *MBS*1 but gain access to *MBS*2. Since the data of *MBS*1 should not be visible to that user any more after he un-subscribed from *MBS*1. For the forward secrecy, the KDC should revoke all the keys. For the revocation, the KDC changes the old slave key to a new slave key and makes a new master key through the new proposed master key management algorithm.



(a)The Conceptual Diagram of MKE.(b)when d1 should be updated to d1',the other private places {d1…dr} are still valid without changes

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

SO at KDC for two cases



This case is applicable for hierrachial Service Set.

The Proposed Master Key Management For Algorithm

1.To determine p1…pr,q1…qr for safe prime no

2.For i=1…r

3.∅i=(p-1)*(q-1)

4.xi=(pi-1)/2

5.yi=(qi-1)/2

6.ei=(4*random)+1

7.di=ei^2(xi-1)(yi-1)-1mod(xi,yi)

8.end for

9.n=1

10.for i=1 to r

11.n=n*(xiyi)

12.end for

13.for i=1 to r

14.M[i]=n/(xiyi)

15.N[i]=M[i]^(xi-1)(yi-1)-1mod(xiyi)

16.end for

17.em=0

18.For i=0 to r

19.em=em+(ei*m[i]*n[i])mod n

20.end for

21.while(em mod4!=1)em=em+n

22.sleep

23.Interrupt(when jth key pair should be updated)

24.ej=4*random+1

25.di=ei^2(xi-1)(yi-1)-1mod 4xiyi

26.goto 17

V. CONCLUSION

In this paper, MGKM has been proposed for multiple group instead of hierrachial group. In contrast to other existing system of using symmentric keys, the MKE_MGKM exploit asymmentric keys, master key and multiple slave key, which are generatd from proposed master key generation. by using a set compromising master key and slave key, a TEK can efficiently distribute to multiple SGs. Therefore, number of rekeying efficiently reduced. Therefore keygraph of MKE-MGKM is much simpler than any other scheme, less memory is needed for storing the keys. Compared with other schemes, the MKE-MGKM can significantly reduce storage and Cos in the rekeying process, with acceptable compuatation overhead. It is expected MKE-MGKM is practical solution for various group application, especially those many SGs, especially TV charged services by channel basis.

REFERENCES

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

[2] Third Generation Partnership Project, "Multimedia Broadcast/Multicast Service; Stage 1 (Release 8)," Technical Specification 3GPP TS 22.146 v.8.3.0 (2007-06), June 2007.

[3] C.K. Wong, M.G. Gouda, and S.S. Lam, "Secure Group Communications Using key Graphs," ACM SIGCOMM Computer Comm. Rev., vol. 28, pp. 68-79, 1998.

[4] D.M. Wallner, E.J. Harder, and R.C. Agee, "Key Management for Multicast: Issues and Architectures," IETF RFC 2627, http://www.ietf.org/rfc/rfc2627.txt, June 1999.

[5] Y. Challal and H. Seba, "Group Key Management Protocols: A Novel Taxonomy," Int'l J. Information Technology, vol. 2, no. 1, pp. 105-118, 2005.