KEY MANAGEMENT FOR MULTIPLE MULTICAST CLUSTERS IN WIRELESS NETWORK

[1]D.Prabhakaran, [2]C.Ramkumar
[1,2]Assistant Professor, Department of CSE, Sasurie College of Engineering, Tirupur, India
[1]prabha619@gmail.com, [2]c.ramkumar84@gmail.com

Abstract:The advancement of several multiple multicast clusters and aggregation-based services are likely to mesh in a single network, and users may contribute to multiple clusters all together. The objective of Group Key Management is to secure a single group of element and due to ineffective use of keys it is not suitable for securing multicast group element. We propose a new GKM technique for multiple multicast teams, referred to as the master-key-encryption-based multiple cluster key management (MKE-MGKM) technique. The MKE-MGKM technique make advantage of asymmetric keys, i.e., a base key and multiple derived keys, which are generated from the projected base key encryption (MKE) algorithm and distribution of the cluster key is made effective. By using the imbalance of the base and derived keys used for effective distribution of the cluster key, it relieves the rekeying overhead. Also, it relieves the rekeying overhead by using the asymmetry of the base and derived keys.

Keyword: Master key encryption, multiple cluster key management, Asymmetric key, Key hierarchy.

1. INTRODUCTION

In the wireless network used one of the well-organized multicast methods. Multicast method used for transmitting data's from sender to the several destinations. Each and every transaction rates of efficiency should be received by sender. The multicast wireless network is increased the efficiency of group communication. These methods are called multicast service or multimedia broad cast. The broadcasting medium, however, makes the wireless network prone to numerous security attacks since anyone can simply snoop on messages transmitted within the air. To implement the multicast, i.e., the delivery of information solely to the members of a gaggle, in wireless networks, Access control mechanism for the broadcast method confidently to produce a accurate result. So it is successful optimal key management in wireless network. The way to produce an access control mechanism for secure group communication using symmetric key or group key. Group key only share a group members. Messages are converted to encrypted format and transmit to group members they are used group key and decrypt the message. This can provide secure group communication in wireless network. In this group key communication have some of the difficulties to provide an efficient for secure communication. Group key should be updated in the particular interval time when the members are leaving and joining in the communication.

Since the existing group key management schemes have some of the limitation for using rekeying in multicast service. In future the group of multicast network used in single network key management also support multicast group. Examples IEEE802.11 supports different multicast services eg., charged TV ,telematics service and information services.

In these services can be managed by several membership record of the service provided. if the subscription to a service is charged for either each channel (Ch1, Ch2, and Ch3) or content(sports and stock), the service supplier ought to manage the extra user teams (e.g., channel-based or content-based groups) for correct accounting like Fig. As a result, the management overhead stemming from rekeying will considerably increase owing to the amount of such teams. we ability a brand new multiple group key management (MGKM) theme, named the master-key-encryption-based MGKM (MKE-MGKM) scheme, which may scale back the rekeying overhead from managing multiple cluster keys. The key plan of the MKEMGKM is to use AN uneven encoding theme, called the passe-partout encoding (MKE), to reinforce the rekeying performance by assuaging the rekeying overhead.

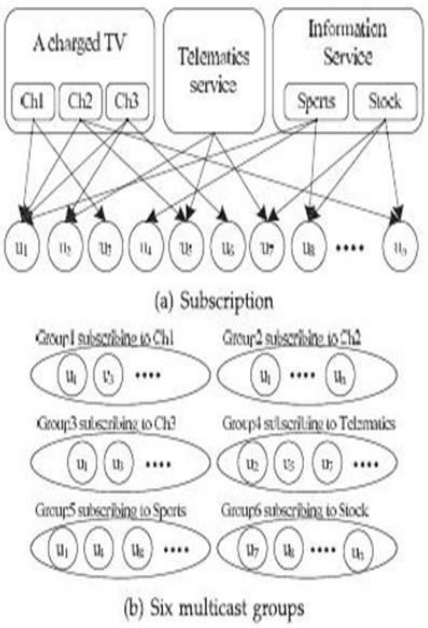

Figure 1: Multiple groups in a Wireless Networks the Main Contribution:

- We present a master key management algorithmic rule that makes and updates a master key and multiple slave keys. A message encrypted by the master key will be decrypted by every of various slave keys, and contrariwise.
- We present a rekeying mechanism for multiple teams by introducing a MKE-based key graph having the master and slave keys.

2. RELATED WORKS

The KDC (Key Distribution Center) provide a new group key to all group members to invalidate old group key.so members should not allow leaving and joining to access in future message. This is called as forward or backward secrecy.

In a multicast group multiple members have shared a group key to encrypt/decrypt messages among them. Once the member leaves, the old group key should be revoked and updated with a new group key. This rekeying process may cause a lot of key management overhead. Since the existing members do not have any shared secret keys except for the old group key

To solve these problem provide a new data structure called Logical Key Hierarchy (LKH). Group members shares Key Encryption Key (KEK), Traffic Encryption Key (TEK), Individual Key (IK). These keys comprise Logical Key Trees, TEK is root node, IK is leaf node. The rekeying overhead is a logarithmic function of a group size. These tree based approach are one way function key and one way key derivation.

In the existing GKM scheme only used for single multicast group it cannot able to use multicast service in network. Multiple users can be access to multiple multicast groups. Each and every multicast groups can be access own group key management. All multicast groups independently used the rekeying procedure.

3. MOTIVATION OF OUR APPROACH

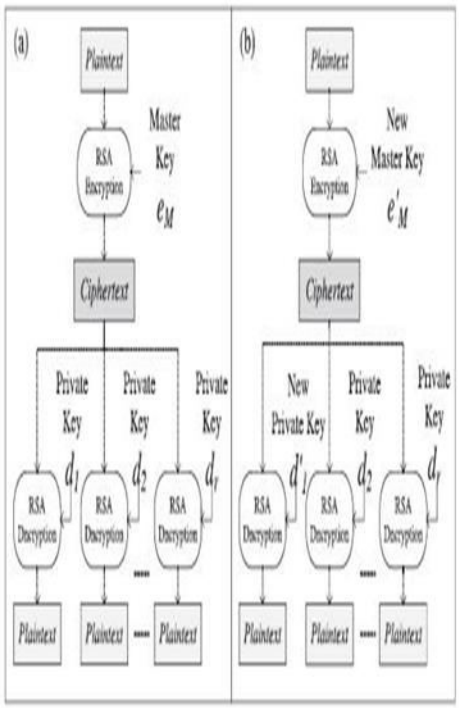

Figure 2: The Conceptual diagram of MKE

The existing HAC (Hierarchical access control) schemes can reduce the rekeying performance of the data structure is called hierarchical logical key tree. These schemes, KEK used to distribute TEK in efficient manner; KEK hierarchical key trees improve the rekeying originator from leaving user in symmetric TEK. These Schemes can include another rekeying method in KEK also include a symmetric key. The single multicast group manages rekeying in TEK. The multiple multicast group due to consider several TEK and KEK can updated in multiple multicast group. Duplicate part of multiple multicast groups to be

reduced in hierarchical IKG. It should not achieve a high rekeying performance in generic multicast environment in multicast services.

Motivation to consider MGKM use of asymmetric key. It has share a common key. This key symmetry means removed and provides rekey.

The MKE decrypt a cipher text each and every different key get the same plaintext, even one different key are repealed.

4. PROPOSED APPROACH FOR MGKM

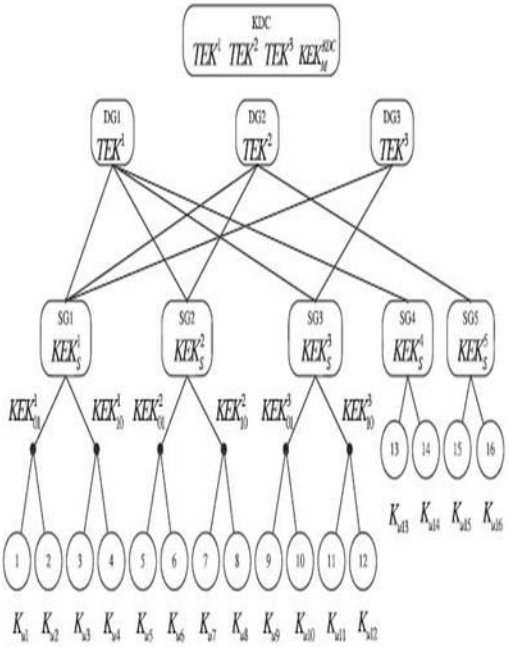

Figure 3:An MKE-based key graph after the initial setup

In MBS is used for DG-Oriented encryption for ensure low cost. Each and every encrypted data in TEK for all user corresponding DG share. Example Consider a broadcasting station providing 3 channels, every of that is for drama, sports, and news, severally. The three channels is thought to be 3 MBSs if the content of every of the channels is encrypted and distributed severally. A user will subscribe as several channels as desired, and hence, there is at the most 3 DGs and seven SGs during this case.

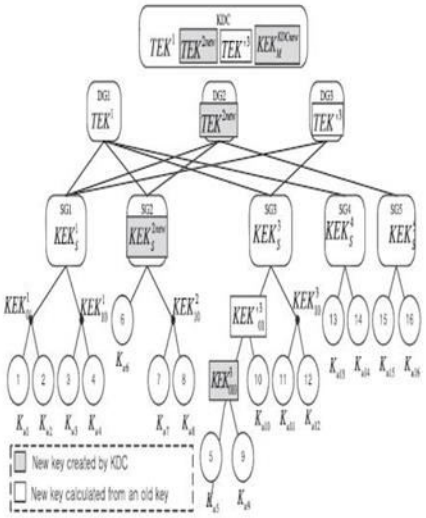

Figure 4:An updated MKE-based key graph after rekeying

Step 1: Initial setup

- Generating a master key and slave keys.
- Constructing SG key tree.
- Constructing an MKE based key graph.

Step 2: Rekeying at membership change

- Revoking the old keys and generating a new master key.
- Rekeying the new slave key and the KEKs inside the SG.
- Broadcasting a new TEK encrypted with the new master

The KDC generates a master key, and as several public-private key pairs because the number of SGs, through the new projected master key management formula. the quantity of SGs grows exponentially because the variety of DGs will increase. For example, allow us to think about twenty DGs as 20 TV channels broadcasted by a supplier. If the provider uses all the potential mixtures of channels.

This constructs as several SG key trees because the variety of SGs. The leaf nodes of each SG key tree square measure the IKs of all users within the SG. This paper focuses on a way to manage multiple group keys, instead of a way to generate AN economical key tree structure in an exceedingly cluster. Though there's no

restriction on constructing the SG key trees, it is assumed that a binary tree structure is employed, to demonstrate the performance of the MGKM them.

The KDC finishes the initial setup by distributing the corresponding TEKs to the users in every SG in step with the capability matrix. Since the initial distribution of the TEKs would be done just one occasion, it is not considered here however the TEKs square measure sent to the users of each SG at the initial setup; this may be done by using the user's IK or every SG's KEKs.

The analysis of MKE-MGKM scheme is reducing in terms of storage capacity in key information. These schemes employs in asymmetric encryption compare to symmetric it has provided more computational cost.
The storage overhead can be considered by memory capacity to maintaining the keys, It has direct access able to the number of keys to produce key sizes are same.

5.CONCLUSION

An MGKM schemes has been enhance the performance of multiple group key used to hierarchy of the user or the data streams, other existing schemes used only symmetric keys, MKE-MGKM schemes used for asymmetric keys. It should be specify master key and multiple slave keys, It has generate by proposed master key algorithms. TEK can be produce efficient way of transaction. The number of rekeying message can be reduced for using MKE-MGKM schems.in these key management of MKE-MGKM schemes simpler to other schemes. It has access less memory used for storing the keys compared to other schemes. MKE-MGKM schemes can be used for many practical solutions for various group applications. It has required TV streaming service charged on a channel 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.
[6] S. McGrew, "Key Establishment in Large Dynamic Groups Using One-Way Function Trees," IEEE Trans. Software Eng., vol. 29, no. 5,pp. 444-458, May 2003.
[7] J.-C. Lin, F. Lai, and H.-C. Lee, "Efficient Group Key Management Protocol with One- Way Key Derivation," Proc. IEEE Conf. Local Computer Networks, pp. 336-343, http://doi.ieeecomputersociety.org/10.1109/LCN.2005.61, 2005.
[8] Y. Sun and K.J.R. Liu, "Hierarchical Group Access Control for Secure Multicast Communications,"IEEE/ACMTrans. Networking,vol. 15, no. 6, pp. 1514-1526, Dec. 2007.
[9] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," Proc. IEEE GLOBECOM, pp. 2067-2071, 2004.
[10] D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast: Issues andArchitectures," IETF RFC 2627, 1999.
[11] R.L. Rivest, A. Shamir, and L. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.
[12] K. Koyama, "A Master Key for the RSA Public-Key Cryptosystem," IEICE Trans. Information and Systems, pp. 163-170, 1982.