IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 1 (May. - Jun. 2013), PP 36-40
www.iosrjournals.org

A Novel High Order Tree for Securing Key Management for Multicast Services

M.Latha[1] , Mrs.S.Nalini[2] ,
1.M.E (CSE), Department of Computer science & Engg,University College of Engineering,BIT Campus, Trichy,
2.Asst. Professor, Department of Computer Applications, University College of Engineering,BIT Campus Trichy

Abstract: *With the emergence of diverse group-based services, multiple multicast groups are likely to co-exist in a single network,and users may subscribe to multiple groups simultaneously. However, the existing group key management (GKM) schemes, aiming to secure communication within a single group, are not suitable in multiple multicast group environments because of inefficient use of keys, and much larger rekeying overheads. 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. Through numerical analysis and simulations, it is shown that the MKE-MGKM scheme can reduce the storage overhead of a key distribution center (KDC) by 75% and the storage overhead of a user by up to 85%, and 60% of the communication overhead at most, compared to the existing schemes.*

Index Terms: *Security, group Key Management, multicast, chinese remainder theorem, master key encryption*

I. INTRODUCTION

Objective of the project

The multicast group can be identified with the class D IP address so that the members can enter or leave the group with the management of Internet group management protocol. The trusted model gives a scope between the entities in a multicast security system. For secure group communication in the multicast network, a group key shared by all group members is required. This group key should be updated when there are membership changes in the group, such as when a new member joins or a current member leaves. Along with these considerations, we take the help relatively prime numbers and their enhancements that play a vital role in the construction of keys that enhances the strength for the security. Multicast cryptosystems are preferably for sending the messages to a specific group of members in the multicast group.

Unicast is for one recipient to transfer the message and 'Broadcast' is to send the message to all the members in the network. Multicast applications have a vital role in enlarging and inflating of the Internet. The Internet has experienced explosive growth in last two decades. The number of the Internet users, hosts and networks triples approximately every two years. Also Internet traffic is doubling every three months partly because of the increased users, but also because of the introduction of new multicast applications in the real world such as video conferencing, games, atm applications etc.. Broad casting such as www, multimedia conference and e-commerce, VOD (Video on Demand), Internet broadcasting and video conferencing require a flexible multicasting capability. Multicast is a relatively new form of communications where a single packet is transmitted to more than one receivers. The Internet does not manage the multicast group membership tightly. A multicast message is sent from a source to a group of destination hosts. A source sends a packet to a multicast group specifying as the multicast group address. The packet is automatically duplicated at intermediate routers and any hosts that joined the group can receive a copy of the packet. Because a host can receive transmitted data of any multicast groups, secure communications is more important in multicasting than in unicasting.

II. Multicast

In computer networking, multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source. Copies are automatically created in other network elements, such as routers, but only when the topology of the network requires it.

Multicast is most commonly implemented in IP multicast, which is often employed in Internet Protocol (IP) applications of streaming media and Internet television. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for data grams sent to a multicast destination address.

2.2.GroupKey Management in Multicast Security

Multicast technology is used for distributing data to a group of participants by conserving bandwidth more efficiently than traditional unicast mechanism. This is done by replicating IP streams in the router at the same time thus achieving better delivery to multiple users. This would mean conservation of computational resources of the sender and bandwidth efficiency in the network. A group membership can be performed using the Internet Group Multicast Protocol (IGMP) protocol. It provides admission control operation such as "join" and "leave". Some examples of applications that take advantage of multicast technology are video conferencing, digital broadcasting, software distribution and electronic learning

2.3. A Group Key Management Approach For Multicast Cryptosystems

Multicast cryptosystems are preferably for sending the messages to a specific group of members in the multicast group. Unicast is for one recipient to transfer the message and ‘Broadcast’ is to send the message to all the members in the network. Multicast applications have a vital role in enlarging and inflating of the Internet. The Internet has experienced explosive growth in last two decades. The number of the Internet users, hosts and networks triples approximately every two years. Also Internet traffic is doubling every three months partly because of the increased users, but also because of the introduction of new multicast applications in the real world such as video conferencing, games, ATM applications etc. broad casting such as www, multimedia conference and e-commerce, VOD (Video on Demand), Internet broadcasting and video conferencing require a flexible multicasting capability.

Multicast is a relatively new form of communications where a single packet is transmitted to more than one receivers. The Internet does not manage the multicast group membership tightly. A multicast message is sent from a source to a group of destination hosts. A source sends a packet to a multicast group specifying as the multicast group address. The packet is automatically duplicated at intermediate routers and any hosts that joined the group can receive a copy of the packet. Because a host can receive transmitted data of any multicast groups, secure communications is more important in multicasting than in unicasting.

The security in the multicast communication in the large groups is the major obstacles for effectively controlling access to the transmitting data. The IP Multicast itself does not provide any specific mechanisms to control the intruders in the group communication. Group key management is mainly addresses upon the trust model developed by Group Key Management Protocol (GKMP). There are several group key management protocols that are proposed, this paper will however elaborate mainly on Group key management which has a sound scalability when compared with other central key management systems. This paper emphases protocol which provides a scope for the dynamic group operations like join the group, leave the group, merge without the need of central mechanisms. An important component for protecting group secrecy is re-keying. With the combination of strong public and private key algorithms this would become a better serve to the multicast security.

Multicast routing protocols provide resilience against collaborating malicious nodes. PGKMP is a complete multipath protocol, in the sense that it provides the maximum security in the network when compared to the existing protocols like LKH etc. The security of PGKMP is mainly based on neighborhood authentication of the nodes, as well as on security associations, while the use of public key cryptography is minimized. The PGKMP protocol can be integrated on top of existing on-demand routing protocols such as LKH. A key reason for this good performance is the fact that PGKMP operates entirely on-demand with no periodic activity of any kind required within the network. PGKMP finds disjoint paths only, so the route discovery cost will be less as compared to LKH where all possible paths exist and a key server has to be maintained. Also due to the double encryption scheme provided to the protocol, the network is more secured. There is a scope to further decrease the overheads and increase more security with this Protocol (PGKMP) and a positive hope for the enhancement of this protocol.

III. Existing System

The existing GKM schemes still face the limitation of rekeying performance as the number of multicast services increases. However, in the foreseeable future, multiple multicast groups will co-exist in a single network due to the emergence of many group-based applications. In such a situation, it is likely that the service provider may suffer from considerable key management overhead for supporting multiple multicast groups. In existing system if the user wants to access from different server the user have to login each time for different server hence the key management process become too tedious to handle if the server number increases tremendously Once the master key has been change the entire configuration has to be configured to access the service.

Disadvantages

- Rekeying management is too difficult to handle.
- If any changes in the network configuration mean the entire key system has to be modified.
- Group key management has limitation in managing the key.

IV. Proposed System

A new multiple group key management (MGKM) scheme, named the master-key-encryption based MGKM (MKE-MGKM) scheme,which can reduce the rekeying overhead from managing multiple group keys. The key idea of the MKE-MGKM is to employ an asymmetric encryption scheme, called the master key encryption (MKE), to enhance the rekeying performance by alleviating the rekeying overhead. Compared with the MGKM schemes expanding the existing GKM schemes, the MKE-MGKM scheme can reduce the storage overhead of a key distribution center (KDC) by 75%. Hence this has been implemented for multicast service like video streaming and downloading to avoid the pirated movies and to avoid unauthorized users to view and download the videos in video service websites.

Advantages

- Efficient key management process.
- No limitation in rekeying process.
- Storage resource has been reduced.
- Used in third-party data storage system.

V. Problem Definition

The existing GKM schemes targeted to a single multicast group are not directly applicable to the multiple multicast service environments. If each multicast group is managed by its own GKM scheme according to the existing GKM schemes, more independent multicast groups would be required. In this case, when a user subscribing to the multiple multicast services stops subscribing to all the services, all these multicast groups independently initiate the rekeying procedure, which may result in much more rekeying overhead. To alleviate the problem of unauthorized video watching and recording from sites.

VI. Experimental Results

MODULE DESCRIPTION

1. Multicast Service Module
2. Traffic Encryption key Generation
3. MKE based MGKM algorithm
4. Rekey Management.
5. Video layer coding

6.1. Multicast Service module

In order to implement the multicast, i.e., the delivery of data only to the members of a group, in wireless networks, we need to an access control mechanism for the broadcasted messages, which guarantees confidentiality, protects digital contents, and facilitates accurate accounting.

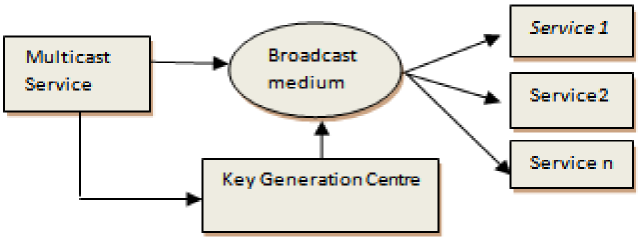

FIG.6.1

6.2. Traffic Encryption key Generation

All these keys comprise a logical key tree, where the TEK is the root node, an IK is a leaf node, and the KEKs are the rest of the nodes in the key tree. It can significantly reduce the amount of rekeying overhead which is a logarithmic function of a group size.

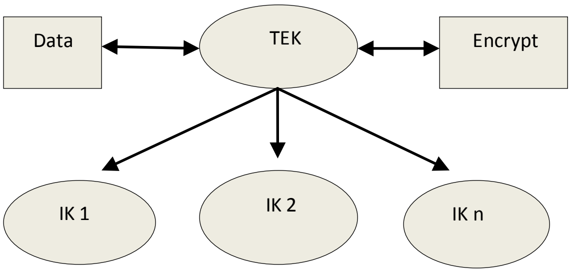

FIG.6.2

6.3. MKE based MGKM algorithm

The key idea of the MKE-MGKM is to employ an asymmetric encryption scheme, called the master key encryption (MKE), to enhance the rekeying performance.

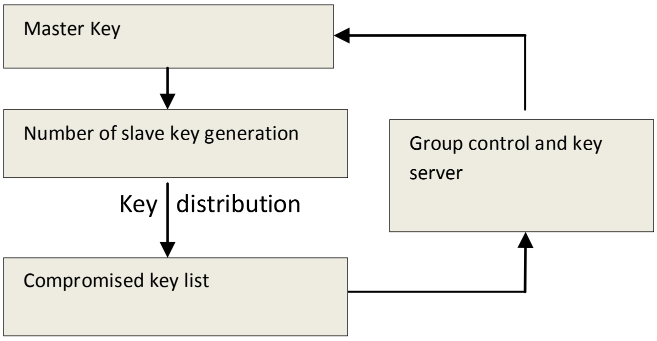

FIG.6.3

6.4. Rekey Management

A rekeying mechanism for multiple groups by introducing a MKE-based key graph having the master and slave keys. Rekeying can significantly increase due to the number of multiple groups.

6.5.Video layer coding

To deliver high quality video services, it becomes vital to consider the heterogeneous wireless infrastructure and multi-radio capability of mobile devices.

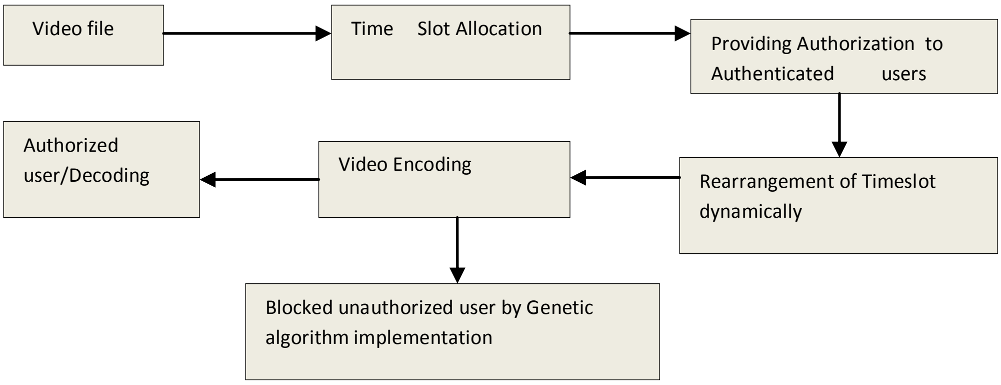
Video file
Time Slot Allocation
Providing Authorization to Authenticated users
Authorized user/Decoding
Video Encoding
Rearrangement of Timeslot dynamically
Blocked unauthorized user by Genetic algorithm implementation

FIG.6.4

VII. Conclusion And Future Work

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 can significantly reduce the storage and communication overheads in the rekeying process, with acceptable computational overhead. It is expected that the MKEMGKM 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.

In future the concept can be applied for video broadcasting service to avoid unauthorized users to view and access the video.

References

[1] Lawrence Horte "Introduction to data multicasting", 2008

[2] Zhang, J, Varadharajan, V and Mu, Y," A novel dynamic key management scheme for secure multicasting," ICON2003. The 11th IEEE International Conference on Network

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

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

[5] Y. Challal and H. Seba, "Group key management protocols: A 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 Transactions on 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*. IEEE Computer Society, 2005, pp. 336–343. [Online].Available:http://doi.ieeecomputersociety.org/10.1109/LCN.2005.61

[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 Comments 2627, 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 Acta Mathematica 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.