Adoptable Key Management Technique for Multicast and Broadcast Services

D.Nattiya and T.K.Thivakaran

[†]Department of Information Technology, Sri Venkateswara College of Engineering, Chennai, India
[††]Faculty of Information Technology, Sri Venkateswara College of Engineering, Chennai, India

Abstract
The popularity of group-oriented applications, secure and efficient communication among all group members has become a major issue. Another major issue is that to provide dynamic rekeying for all the users that join and leave the group. For the rekeying of the group key all members of the group should agree the rekeying of the key. When keys are distributed dynamically the content should be handled by an authenticated person and safe communication must be enhanced. In this paper we present a solution for dynamic rekeying by optimized rekey method to generate dynamic rekey for the users. This mechanism maintains the key server for frequent updating of key and calculating the key length to minimizing the storage cost as well as computational cost. The devices once found to be authenticated; they start communication by adopting various cryptographic techniques depending on the types of devices. The level may be classified based on the memory capacity and type of processor used. Elliptic curve cryptographic (ECC) schemes for high level devices, advanced encryption standard (AES) for intermediate level devices and hashing schemes with key harning for low level devices are implemented. Thus our proposed system reduces the number of rekeying and provides authenticated and secured group communication.

Key words:
Key management, multicast services, dynamic rekeying, anonymity, adoptability, security.

1. Introduction

With the new emerging applications like video-conferencing, multi-user games etc. getting into the life of an average computer user, a mode of communication called multicast has been used. The data should be delivered to multiple users and not to every end point alone. Hence, to fulfill the requirements where the communication is restricted to only a set of participants (a group), the multicast communication emerged in the computer communications arena. Group communication [1], [2], [3], [4] enabled by multicast techniques is of considerable interest today due to the growth of the internet and the widespread availability of high bandwidth connections. Members are generally allowed to join and leave groups, and access to multicast transmissions must be granted and revoked with minimal system overhead. Multicast provides efficient delivery of data from a source to multiple receivers. It reduces sender transmission overhead, network bandwidth requirements, and the latency observed by receivers. This makes multicast an ideal technology for applications based upon a group communications model. One way to implement secure multicast transmissions is through the use of message encryption and rekeying [5], [6], [7], [8]. The multicast host uses the session key for encrypting data packets by using cryptographic schemes [8] before sending them to the group. The data's are encrypted to protect it from outside eavesdropping. Many cryptographic schemes are applied for encryption and decryption. When a member is evicted from the group the session key must be changed in order to maintain message privacy. All remaining group members receive the new group key by secure transmission. The message must be indecipherable to the evicted member. This paper proposes technique like optimized batch algorithm to reduce the rekeys, and adoptable of cryptographic schemes is provided to encrypt/decrypt the content in a secured manner. Thus the proposed method results in well authenticated and secure group communication as well as reduced amount of rekeying results in reduction of key storage.

2. Related works

In recent years, many authors have investigated the multicast re-keying problem and have proposed some group key-management schemes. [3] Proposed that Group Multicast is used in many applications. The aim is to deliver multicasting content as secure and efficient as possible. Membership fluctuation needs to be dealt with in efficient way. That is, eviction/join of the users from/to the group. Exclusion

basis system is been implemented along with rekeying. But still the drawback of rekeying mechanism has not efficiently reduced. [4] have explained that in group-oriented applications like conferencing, chat groups and interactive gaming myriad messages are sent from one or more sources to multiple users. Multicasting is the optimum technique for such group oriented applications with effective network resource utilization. But maintaining security is a critical issue in group oriented protocols with frequent membership changes. Confidentiality can be achieved through changing the key material, known as rekeying every time a new member joins the group or existing member leaves from the group. Many techniques have been proposed earlier for this purpose. But the result concludes that the concept of reducing the rekeying is a challenging factor. [8] have explained development of Internet multicast techniques results in more and more multicast-based applications, such as pay-per view, video conferencing, real-time delivery of stock quotes, etc.. Anyone can join a multicast group to receive data from the data source or send data to the group. Therefore, cryptographic techniques have to be employed to prevent eavesdroppers or restrict the access of the multicast communications only to legitimate subscribers. But applying cryptographic schemes should be an adoptable technique based on the devices since each device has a varying feature. [9] Explain Key management is very crucial in a secure multicast system. The key storage of the group controller and group members, the communication cost and computation cost caused by joining/leaving members, are the determining factors for the performance of the key management system. A scheme is high-performed, if it has the optimal rekeying cost and the lower storage requirements. Multicasting using threshold based one way function was used to improve the rekeying parameters. But usage of threshold should be effective since it should not be a restricting factor for the members.

3. Proposed Work

The main design goal of this paper is minimizing the rekeying and improving the security of the users. The key is generated first to all the users, and then dynamic rekeying is introduced in key generation scenario. When the users are provided with the secured key they start to transfer the data. Secured communication is implemented by the anonymity manager and different cryptographic scheme is applied to the users based on their device types. In this framework the efficiency of the rekeying is improved by optimized batch algorithm. It is done by the implementation of optimized rekey mechanism. It is done by dividing the number of users in batches. When the group members are divided into batch, the rekeying could be done for the batch in which the members join/depart. The entire group has not needed to be rekeyed, only the divided batch that contains the member join/depart has to be rekeyed. So it could improve the efficiency of the rekeying mechanism. After distributing the keys to the members the communication part occurs. In this paper we propose the concept of adoptability of the cryptographic algorithm based on the types of devices for communication. Then encryption is done according to the type of users. A profile is created for the users. In this profile creation, separate profile is created for each user during the registration. The user profile consists of type of devices, type of processor used, and memory capacity of the devices. The devices may be a high level devices or intermediate devices or low level devices. For secure communication the low level devices are encrypted with hashing algorithm along with the key harning process. The intermediate devices are communicated with AES and the high level devices are communicated with Elliptic Curve Cryptographic algorithm. Thus the device adapts the various schemes and efficiently performs since each device captures their encryption method according to their capacity. Hence group communication is performed with secured factors.

4. Components of the proposed sytem

4.1 Key management

Key management for users in the communication networks is dependent upon the security of the keys, it is sometimes appropriate to devise a fairly complex mechanism to manage them. In group communication many individuals are involved, with a requirement for unique keys to be sent to each for encryption/decryption of transmitted data. In this case, a number of comprehensive and proven key management systems must be implemented.

4.1.1 Group creation and profile creation

Group creation is creating an environment in which the authorized users can communicate with other users in that particular group or domain. In order to establish a group communication a common group key is to be distributed to all the member of the group. The group key is to be changed when a member leaves or joins in the group. When group members are changes, new key information is transmitted to all users through re-keying messages. These re-keying messages must be delivered

reliability and in a timely manner. In profile creation, separate profile is created for each user during the registration. The user profile consists of type of devices, type of processor used, and memory capacity of the devices. The devices may be a high level devices or intermediate devices or low level devices. The devices classified based on the processor type and memory capacity.

4.1.2 Key generation

The key management scheme induces high storage of keys and high computation overhead at the key server or group members. Key management includes creating, distributing and updating the keys then it constitutes a basic block for secure multicast communication applications. Group confidentiality requires that only valid users could decrypt the multicast data. All members can perform access control and the generation of key is contributory. Key Management schemes [1] for mobile Broadcast and Multicast services are typically based on 4 layer architecture. In proposed method another layer is included where Multicast Session key is generated for secured communication.

1) The client performs mutual authentication with the server to establishment of unique session key (SK) between client and server.
2) The client sends a service to join a selected multicast broadcast group.
3) If the service request is validated and processed successfully, the Group management key is provided.
4) Multicast session key (MSK) is generated and used to protect a certain Multicast and Broadcasting Service session. It is also used to protect the distribution of traffic encryption key (TEK).
5) After receiving the MSK from the server, the client calculates granted number of TEKs and is prepared to deliver multicast broadcast contents.

4.1.3 Rekeying

In cryptography, rekeying refers to the process of changing the group key of an ongoing communication in order to accomplish forward and backward secrecy. The group is considerably divided into batches. Consider n batches in the group. Each batch can hold up to the members that are specified. This value could be varied, which is known as the threshold value. Each batch contains a threshold value which constraints a limited number of users. When rekeying is done the users is distributed with a new group key. But the process of rekeying should be efficiently handled because minimizing the rekeying only reduced the overhead in the system. In proposed system optimized batch algorithm is provided to reduce the rekey. When a user joins or leaves the batch rekeying is performed for that particular batch is known as optimized batch algorithm. By implementing a new key only to that batch the other members in the group are not disturbed. Since the efficiency of rekey is also enhanced. When we change the group key for all the users in group it involves a high amount of rekeying because for n number of users n number of rekeying should be done. But with this optimized method only limited users are provided with rekeying hence other users are not necessary to be rekeyed. We observe that the optimized batch Algorithm has identical rekeying costs compared to existing algorithms when the number of joining members and the number of departing members are comparable.

4.2 Adoptability of Cryptographic schemes

When the keys are distributed and dynamic rekeying is performed the client starts to communicate with other users in the group. The file or data transfer between the clients should be protected content. The client first registers their device types in the profile creation part. Based on the user registration in the profile, different cryptographic schemes are adopted based on their devices. These devices are classified based on their memory capacity and the processor type. High level devices are implemented with ECC, intermediate devices are provided with AES and the low level devices are provided with Hashing algorithm with harning process. The Intermediate level devices are not possible to use ECC. At the same time the low level devices are not possible for implements ECC and AES. The main reason is the device capacity. The memory of the low level processor could not support ECC and if AES is implemented the cost will be high. Likewise if hashing is implemented in intermediate or high level device then there is no efficient use of the processor since their capacity is high hence waste of resource utilization will be the result. By adopting these different techniques the devices could provide a secure communication based on their features. So it enables a better communicating scenario for each device.

Table.1 Device types

High Level	**Intermediate Level**	**Low Level**
Tablet	Smart Phones	Mobile Phones
Net book	PDA	

Table.2 Device Properties

Device Name	Memory	OS	Processor
Thinkpad X61 Tablet	Up to 4 GB DDR2	Vista Ultimate	Up to Intel Core 2 Duo Processor
Thinkpad X60 Tablet	Up to 4 GB DDR2	Genuine Windows XP Tablet PC Edition	Up to Intel Core 2 Duo Processor
Samsung Galaxy ACE Plus	512MiB RAM	Google Android 2.3.5	1000MHz
ZTE Tania (ZTE Spirit)	512 MB RAM	Microsoft Windows Phone 7.5	32bit Qualcomm Snapdragon MSM8255
Samsung SGH-i717 Galaxy Note LTE	1024MiB RAM	Google Android 2.3.7	32bit Qualcomm Snapdragon APQ8060, 1500MHz
Motorola DROID RAZR MAXX XT912 (Motorola Spyder)	1024MiB RAM	Google Android 2.3.5	32bit Texas Instruments OMAP 4430
Nokia 801T	256MiB RAM	Symbian OS Symbian^3 PR2 Anna Chinese	32bit ARM 1136JF-S, 680MHz
Verizon Samsung SCH-i815 Galaxy Tab 7.7 LTE	1024MiB RAM	Google Android 3.2	32bit ARM Cortex-A9 MPCore

4.2.1 High level devices

High level devices adopt ECC. It is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. It generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. ECC scheme is implemented for high level devices and a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys.

4.2.2 Imtermediate level devices

This Scheme is used for Intermediate level devices. Smart phones and PDAs are the examples of intermediate level devices. The intermediate level processors and memory capacity can be used. AES is based on a design principle known as a substitution-permutation network. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The blocksize has a maximum of 256 bits, but the keysize has no theoretical maximum. AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state).

4.2.3 Low level devices

This cryptographic hashing scheme is applied for low level devices. First one Key Seed is generated. Based on the key seed, the 2 way hash chain scheme is applied. This 2 way hash chaining scheme is weak for low level devices. To overcome this problem the harning process is applied. The user should obtain the value of hardened key Hk from a key K. It should not be possible for an outside attacker to determine Hk by exhaustive search. Hence there is a need for the Generation of the Strong Secret for a given key.

a) The user U selects a secret key k.
b) The Client system computes *s* = Hash (k), and repeats the process of applying hash function 'n' number of times.
c) Then it chooses a seed q.
d) It computes Hk = s *mod* q, where Hk is the Hardened Key of the user.

Thus harning process is used to overcome the inefficiency caused by the hashing algorithm.

5. Performance Evaluation

5.1 Experimental results

We observe that the optimized batch algorithm has an optimized rekeying costs compared to existing algorithms when the number of joining members and

the number of departing members are comparable. For the existing system the whole group is being rekeyed whenever the user joins or departs. So all the members have to change their group key associated.

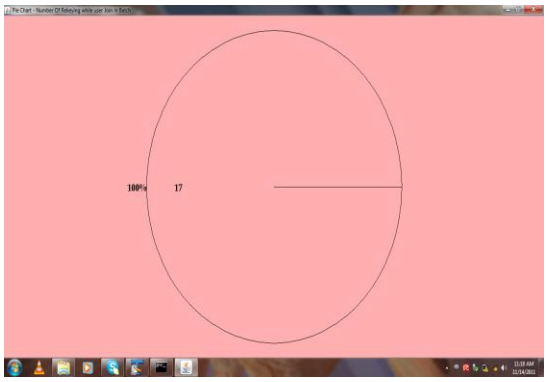

Fig.1 Rekeying for Existing system

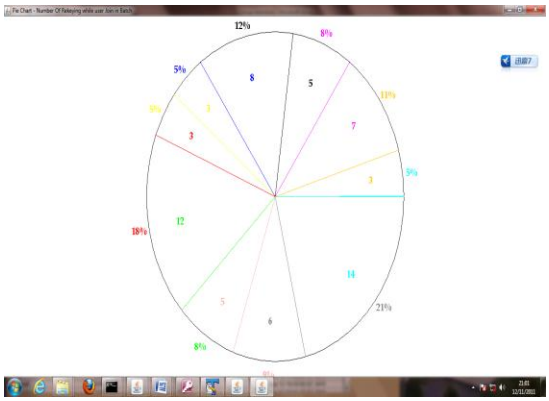

Fig.2 Rekey details for proposed system

Fig.1 shows the example rekeying computed for sixty six members. Here hundred percentage of rekeying is done since all the members have to update their key. But in the proposed system the group is divided based on optimized batch algorithm so the members associated with that particular batch is alone rekeyed so the rekeying factor is reduced to a great extent. Fig.2 shows the example of rekeying performed for the same members with optimized batch algorithm.

The next important factor is cost evaluation. The table. 3 displays examples for cost calculated for each type of device. The proposed system implements each type of device with a reasonable cost value. The cost depends on the message length and the device type algorithm used. Each algorithm has a specific cost predefined. The cost factor varies depending on the size of the message sent between the clients. Same types of files are transferred with different levels of devices and hence the computation cost is compared between them. The file sent in low level device cost high than the file sent in other two types. The file sent in intermediate type has a moderate cost and the file transferred in the high level device cost low. If the High level device uses AES or Hashing, the computation cost will high and the performance of the device is degraded. If the Intermediate level device uses Hashing, the computation cost will high and the performance of the device is degraded. If the high level device uses ECC, the computation cost is reduced and the performance of the device is improved. Likewise intermediate uses AES to reduce the cost.

Table.3 Cost of file transfer

Device	Size	Cost
High Level	1 Kb	1.056
Intermediate Level	1 Kb	2.456
Low Level	1 Kb	3.896

6. Conclusion

Overall, the solution to the problem to get better and faster key management scheme is achieved. To achieve this, the project proposes the optimized batch algorithm which reduces the rekey factor as well as reduces the overhead of the system. The parameters used must be dynamic and the changes must be unpredictable to intruders. Moreover the overall life cycle of key management is achieved. Due to the concept of adoptability introduced to different types of devices, security is enhanced. Since devices are separated on their memory and processor capacity each level could use the better algorithm depending on their property issues. Hence the cost is efficiently reduced.

References

[1] Sungoh Hwang, Seleznev, and Jae Yong Lee, “New Key Management Approach for Broadcast and Multicast Services”, IEEE Communications Letter, Vol.15, No.2, Feb 2011

[2] E.Munivel and J.Lokesh, “Design of Secure group Key Management Scheme for Multicast Networks using Number Theory”, IEEE Conference on

Communication System and Networks and Workshop, pp.124-130, Mar.2009.

[3] Elham Khabiri , Said Bettayeb 'Efficient Algorithms for Secure Multicast key Management', IEEE International Conference on Multicasting, pp 787-792, Nov 2006.

[4] Kumari V.V, NagaRaju, D.V., Soumya K. and Raju K.V.S.V.N, "Secure Group key Distribution Using Hybrid Cryptosystem", IEEE Second International conference on Machine Learning and Computing at Hawaii University, May 2010.

[5] Wee Hock Desmond Ng, Michael Howarth, Zhili Sun, and Haitham Cruickshank, 'Dynamic Balanced Key Tree Management for Secure Multicast Communications' IEEE Transactions on Computers, Vol.56,No.5,pp590-606, May 2007.

[6] Xu Yanyan, Xu Zhengquan and Yu Zhanwu, "A Scalable De-centralized Multicast Key Management Scheme", Proc.of the First International Conference on Innovative Computing, Information and Control, pp.463-467, Oct.2006.

[7] Shu-Quan Li and Yue-We, "A Survey on Key Management for Multicast", IEEE Conference on Information Tech. and Computer Science, pp.309-312, Aug.2010.

[8] Wu Tao, Zheng Xue-feng and Bai Li-zhen, "A new scalable key-management scheme for secure multicast", IEEE International Conference on Computer Science and Service System, pp.57-60, Aug.2011.

[9] Fucai Zhou, Jian, 'Multicast Key Management Scheme Based on TOFT', International Conference on High Performance Computing and Communications, pp. 1030-1038, Oct.2008.

[10] N.H Ayachit and Santosh L.Deshpande 'Evolutionary based secure key management Protocol' IEEE Conference on Computing communication and Networking technologies, July 2010.

[11] S.M.Cheng, W.R. Lai, P.Lin, and K.C.Chen, "Key management for UMTS MBMS", IEEE Trans. Wireless Commun., Vol.7, pp. 3619-3628, Nov 2007.

[12] K.Luther Martin, 'Key Management Infrastructure for Protecting Stored Data' IEEE Computer Society, vol.41, pp. 103-104, June 2008.

[13] Patrick P. Tsang, Apu Kapadia, "Nymble: Blocking Misbehaving Users in Anonymizing Networks", IEEETrans. On Dependable and Scalable Computing, Vol.8, No.2, pp 256-269, Jan 2011.

[14] Rahman R.H, Rahman M.L, 'An effcient group key agreement protocol for Ad-hoc networks', Internation Conference on Electrical and Computer Engineering, pp.478-483, Dec 2008.

[15] O.Rodeh and K.Birman, 'Optimized Group Communication System' ACM Transaction on Network and Distributed System Security, 2008.

[16] Sato.F, Tsang.S.Y, 'A push based key distribution and rekeying protocol for secure multicasting', International Conference on Parallel and Distributed Systems, pp.214-219, 2001.