IFERP
connecting engineers... developing research

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 5, May 2015

Centralized Group Key Management Scheme for Secure Multicast Communication using ElGamal

Shishira M.C [1], Vipin K.M [2]
[1][2]Department of Computer Science, Calicut University, India
[1]shishirac8@gmail.com, [2]vipinkm06d@gmail.com

Abstract- **Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the key generation, exchange, storage, use, and replacement of keys. Several schemes have been proposed to make key management efficient and usable. This paper proposes a centralized group key management with minimal computation complexity to support dynamic secure multicast communication. In this scheme, a Chinese remainder theorem-based group key management scheme that drastically reduces computation complexity of the key server. The computation complexity of key server is reduced to O (1) in this proposed algorithm. Moreover, the computation complexity of group member is also minimized by performing one modulo division operation when a user join or leave operation is performed in a multicast group. The keys generated in the network are securely exchanged with the help of ElGamal algorithm. This paper solves the most security problem by user registration and verification phases in the multicast network. The security of ElGamal is based on the discrete logarithm problem. To encrypt and respectively decrypt a message, a discrete power is executed. An attacker that seeks to decrypt an intercepted message may try to recover the private key. To this end a logarithm needs to be computed. No actual method exists for this, given certain requirements on the initial group are met. Under these circumstances, the encryption is secure.**

Keyterms: **Group Key Management, Multicast, Chinese Remainder Theorem (Crt), Elgamal**

I. INTRODUCTION

Multicasting refers to the transmission of a message from one sender to multiple receivers or from multiple senders to multiple receivers. If the same message is to be sent to different destinations, multicast is preferred to multiple unicast. The advantage of multicast is that, it enables the desired applications to service many users without overloading a network and resources in the server. One of the most important issues in multicast security is the group key management. Security key management is a big deal in-group communication. The goal of group key management is to set up and maintain a shared secret key among the group members. It serves as a cornerstone for other dynamic multi group communication security. There are several approaches to group key management in multicasting groups. One approach relies on a single entity (called a key server) to generate keys and distribute them to the group is referred to as centralized group key distribution. Another approach – called decentralized group key distribution – involves dynamically selecting a group member to generate and distribute keys to other group members.

In the centralized scheme, group center (GC) or key server (KS) is responsible for interacting with the group members and also to control them. Groups can be classified into static and dynamic groups. In static groups, membership of the group is predetermined and does not change during the communication. Therefore, the static approach distributes an unchanged group key (GK) to the members of the group when they join or leave from the multicast group. Moreover, they do not provide necessary solutions for changing the GK when the group membership changes which is not providing forward/backward secrecy. When a new member joins into the service, it is the responsibility of the KS to prevent new members from having access to previous data. This provides backward secrecy, in a secure multimedia communication. Similarly, when an existing group member leaves from any group, he or she should not have further access to the multicast communication which provides forward secrecy. The backward and forward secrecy can be achieved only through the use of dynamic GK management schemes. In order to provide forward and backward secrecy, the keys are frequently updated whenever a member joins or leaves the multicast service.

LITERATURE SURVEY

There are many works that are present in the literature on centralized GK management schemes. In most of the existing centralized key management schemes, different types of group users obtain a new distributed multicast GK which is used for encrypting and decrypting multimedia data for every session update. However, most of these schemes consume more key computation time and memory, and in addition most existing schemes take more broadcast messages.

2.1Chinese Remaindering Group key Protocol:

The first protocol is the base Chinese Remaindering Group Key (CRGK) protocol [3], which with a group of n users requires the key server to do O (n) XORs, additions, multiplications, and Extended Euclidean Algorithm computations and broadcast 1 re-key message; each individual user is required to do only 1 modulo arithmetic and 1 XOR operation for each group key update. By shifting more computing load onto the key server we

optimize the number of re-key broadcast messages, user-side key computation, and number of key storages.

2.2 Fast Chinese Remaindering Group Key (FCRGK) protocol:

The second protocol is the Fast Chinese Remaindering Group Key (FCRGK) protocol l[3], which only requires the key server to do O(n) XORs, additions, and multiplications most of the times with no change to the number of re-key messages and user computation per group key update. One special attraction for our FCRGK protocol is that it allows most of the re-keying computation to be done preemptively, which means when a user-join or user-leave event happens the response time for the key server to send out the new group key can be very short.

2.3 Centralized key distribution protocol using the greatest common divisor method

In [2] Vijayakumar et al. proposed a greatest common divisor-based key distribution protocol that focuses on two dimensions. The first dimension deals with the reduction of computation complexity and second dimension aims at reducing the amount of information stored in the GC and group members while performing the update operation in the key content. The computation cost of GC is O (3 + G) and the user has to perform 1 mod, 1 multiplication and 1 multiplicative inverse operations. Moreover, the storage complexity of GC is ((n × k) +2k 1) where k is the number of clusters and user's storage complexity is three keys.

II. EXISTING TECHNIQUE

In this section, existing CRTGKM algorithm [1] which is based on the CRT. This section is divided into two subsections. The first Section 2.1 gives an overview of CRT and second Section 2.2 explains about our proposed CRTGKM algorithm which is based on CRT.

2.1 Chinese remainder theorem

Let k1, k2, k3… k_n be pairwise relative prime positive numbers, and let a1, a2, a3… a_n be positive integers. Then, CRT states that the pair of congruence

$$X \equiv a1 \bmod k1$$
$$X \equiv a2 \bmod k_2$$
$$.$$
$$.$$
$$X \equiv a_n \bmod k_n$$

has a unique solution mod $M = \prod_{i=1}^{n} (k_i)$. To compute the unique solution, the KS can compute the value as:

$$X = \sum_{i=1}^{n} a_i \beta_i \gamma_i \pmod{M} \qquad (1)$$

where $\beta_i = M/k_i$ and $\beta_i \gamma_i \equiv 1 \bmod k_i$

2.2 CRTGKM algorithm

The proposed CRTGKM algorithm works in three phases. The first phase is the Key Server Initialization phase, where a multiplicative group is created at KS. In the second phase called the user, the users are sending join requests to the KS and obtain all the necessary keys for participation through secure channel. The final phase of this protocol is known as user leaves phase that deals with updating of GK when a user is left from the dynamic multicast group in order to provide forward secrecy.

2.2.1 Key Server Initialization Phase:

After the key server communicates a private key, picked randomly from a pairwise relatively prime integer pool, to each initial group user securely, the key server will pick an initial group key K randomly and build the following congruence system for this group with n initial users. Initially, the KS selects large prime numbers a and b, where a > b and b ≤ [a/4]. The value 'a' helps for defining a multiplicative group z_a^* and 'b' is used to fix a threshold value to select the GK values. Initially, the KS selects secret keys or private keys k_i from the multiplicative group z_a^* for 'n' number of users which will be given to users as they join into the multicast group. In the CRT-based scheme, we require that all the private keys selected from z_a^* are pairwise relatively prime positive integers. Moreover, all the private keys should be much larger than the GK which is selected within the threshold value fixed by 'b'. Next, KS executes the following steps in the KS initialization phase.

1) Compute $M = \prod_{i=1}^{n} (k_i)$.

2) Compute $x_i = M / k_i$
where i = 1, 2, 3, …,n. (2)

3) Compute y_i such that $x_i * yi \equiv 1 \bmod k_i$ (3)

4) Multiply all users x_i and y_i values and store them in the variables $var_i = x_i * y_i$ (4)

5) Compute the value $\mu = \sum_i^n var_i$ (5)

2.2.2 User initial join:

After the initial group has been set up, if a new user wants to join the group then it will first go through the same authentication process as other group users do. If the joining new user is granted the access to the group communication, it will be assigned a new key. In this phase when a new user 'i' is authorized to join the dynamic multicast group for the first time, the KS sends a secret key k_i using a secure unicast which is known only to the user u_i and KS. Next, KS computes the GK in the following way and broadcast it to the users of the multicast group.

(1) Initially, KS selects a random element k_g as a new GK within the range b.

(b) Multiply the newly generated GK with the value μ (computed in KS initialization phase) and the value is stored in the variable $\gamma = k_g \ * \ \mu$. (6)

(c) The KS broadcast a single message γ to the multicast group members. On receiving γ value from the KS, an authorized user u_i of the current group can obtain the new GK k_g by doing only one mod operation as shown in 7

$\gamma \bmod k_i = k_g$ (7)

The k_g obtained in this way must be equal to the kg generated in step (a) of user initial join phase. When 'i' reaches to n, KS executes KS initial set up phase to compute M, var_i and μ for 'm' number of users where $m = n \times \delta$. The value δ is a constant value which may take values < 5 depending on the dynamic nature of the multicast group.

2.2.3 User leave:

Group key updating when a member leaves usually requires more efforts in most other group key management protocol since we cannot use the old group key to encrypt the new group key. However in our protocol group key updating for member leave are also very simple. When a new user joins the service, it is easy to communicate the new GK with the help of the old GK. Since the old GK is not known to the new user, the newly joining user cannot view the past communications. This provides backward secrecy. User leave operation is completely different from user join operation. In user leave operation, when a user leaves the group, the following steps will execute in KS.

(1) Subtract var_i from μ, $\mu ' = \mu - var_i$ (8)

(2) Next, KS must select a new GK and it should be multiplied r by μ′ to form the rekeying message as shown below $\gamma' = k_g' * \ \mu'$ (9)

(3) The updated GK value will be sent as a broadcast message to all the existing group members.The existing members of the multicast group can obtain the updated GK value k_g' by doing only one mod operation as shown in (7).

III. PROPOSED KEY MANAGEMENT SCHEME

A secure Key management scheme is developed using Elgamal algorithm for key exchange purpose during information sharing on a public network. The proposed system provides a secure platform for encrypting and decrypting user's key. This key could be used by a symmetric algorithm for file encryption and decryption. The system is found capable of securing user's key from illegal access by an unauthorized person.

3.1 Elgamal Algorithm

In 1985, T. Elgamal introduced Elgamal asymmetric encryption algorithm (Benoit, Pascal & David, 2006). This algorithm provides an alternative to RSA algorithm for public key encryption. In public key cryptosystem, the encryption key is published and the decryption key is kept private. The various stages involved in Elgamal encryption are as follows:

Stage 1: Public key generation and Transmission

For Bob to communicate with Alice, she generates her private and transmits her public keys. To do this she chooses the following parameters

i. large prime number q

ii. a primitive element r

iii Then generates a random number X_A such that $1<X_A<q-1$.

iv. $Y_A= r^{XA} \bmod q$ where X_A is the private key and (Y_A,q,r) is the public key. Bob then transmits CRT key to Alice.

Stage 2: Message Encryption and Transmission

For Alice to send encrypted message to Bob, he does the following

i. Bob generates a random number k such that $1\leq k\leq q-1$ and selects the message M, such that $0\leq M\leq q-1$.

ii. Generates K as $K= (Y_A)^k \bmod q$ and two cipher texts:

$C_1= r^k \bmod q$

$C_{2=}(KM) \bmod q$.

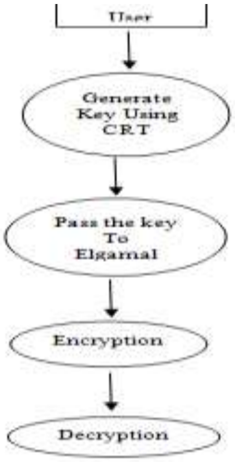
And sends C_1 and C_2 to Alice.

iii. Alice now send encrypted message (C_1, C_2) to Bob.

Stage 3: Message Decryption

i. Bob needs to decrypt Alice's cipher text (C_1, C_2)

ii Alice decerypts the message as $k= C_1^{X_A} \bmod q$ and $M=(K^{-1} C_2) \bmod q$.



IV. SECURITY ANALYSIS

The security of our protocol is based on the assumption is that an adversary might be a group member sometime and KS keeps all users private key as secret and each user will keep their private as secret.. Moreover, the set of m values are randomly picked from an unlimited large pool of pairwise relatively prime positive integers, hence knowing one number gains little knowledge about the others except that the other numbers do not contain the same factors.

4.1 Forward Secrecy

Forward Secrecy is about preventing evicted users to continue accessing future group communications. When a member leaves the group, he or she may try to derive the GK by using any attacking methods. In the proposed algorithm, it is infeasible for an adversary to compute the current GK after the leave for the same reasons that was explained for the backward secrecy technique. Since when a user ui leaves from the group, KS subtracts his or her share value such as multiplication of xi and yi which is stored in var_i from μ value to produce μ′. This updated μ′ is multiplied by the newly generated GK value k′g to form the rekeying message γ′. Therefore a user who had already left from the service cannot find the new GK in a feasible way since his or her personal keying information is not included.

4.2 Backward Secrecy

Backward Secrecy is about preventing new users from accessing previous group communications. In order to access the previous communication, an adversary needs to make the previous GK. Moreover, if the adversary becomes a group member, it may try to derive the previous GK which is not permitted. In the proposed protocol, when the newly updated GK is communicated to old group members, an adversary needs to find any one of the group users private key. Moreover, the private keys are randomly selected from a large set of positive integers with respect to
the multiplicative group. This property makes the situation infeasible for the adversary to compute any other users secret key. Consequently, the adversary cannot access the communication sent before join, which means the proposed approach supports the initial security requirement.

4.3 Collusion Attack

Collusion attack on group key protocol is about a set of previous group users working together to try to gain access to the new group key. For our protocol, if the pool of positive integers is only pairwise relatively primes then the collusion of previous users may gain some information about the KS values of current users. Since the value of var_i subtracted from μ after the leaving operation is performed in a multicast group, any number of previous users collusion will not be used to gain information about the congruence system and to derive the updated GK k′g as long as the pairwise relatively prime numbers are large.

CONCLUSION

Elgamal system is a public key cryptosystem that is based on discrete logarithm problem. CRT based group key management protocol which is very scalable for large size dynamically changing group .In this paper, a network based key exchange cryptosystem was developed using Elgamal algorithm to make the key more secured. This paper proposes a new solution to reduce the computation complexity without increasing the storage complexity for providing secure multimedia multicast through effective GK management technique which is based on CRT. Elgamal algorithm used both public and private key, the private key is generated by CRT. The algorithm gives a different cipher text each time encryption is performed. However, the disadvantages of Elgamal algorithm include slow in speed, message expansion by a factor of two during encryption, semantically insecure and require randomness during operation.

References

[1] VijayaKumar, P., Bose, S., Kannan, A.: ‘Chinese Remainder Theorem based centralized group key management for secure multicast communication’, doi: 10.1049/iet-ifs.2012.0352,ISSN **1751-8709**

[2] VijayaKumar, P., Bose, S., Kannan, A.: ‘Centralized key distribution protocol using the greatest common divisor method’, Comput. Math. Appl., 65, (9), pp. **1360–1368**

[3] Zheng, X.L., Huang, C.T., Matthews, M.: ‘Chinese remainder theorem based group key management’. Association for Computing Machinery Proc. 45th Annual Southeast regional Conf. (ACMSE-07), Winston-Salem, North Carolina, USA, 2007, pp. **266–271**

[4] VijayaKumar, P., Bose, S., Kannan, A.: ‘Rotation based secure multicast key management for batch rekeying operations’, Netw. Sci., 2012, 1, (1–4), pp. **39–47**

[5] Wallner, D.M., Harder, E.J., Agee, R.C.: ‘Key management for multicast: issues and architectures’, Internet Draft Report, Filename: draft-wallner-key-arch-01.txt, 1998

[6] Zhou, J., Ou, Y.-H.: ‘Key tree and chinese remainder theorem based group key distribution scheme’, J. Chin. Inst. Eng., 2009, 32, (7), pp. **967–974**.