International Journal of Power Control Signal and Computation(IJPCSC)
Vol3. No1. Jan-Mar 2012 ISSN: 0976-268X
www.ijcns.com

A secure key transfer in decentralized secure group communication

T.Sangeetha[1], V.Jeyakrishnan[2], A.Srisakthi[3], R.B.Dravidaapriya[4], K.Rajakumari[5]
[1,3,4] PG Student ,SNS College of Technology, Coimbatore, India
E-Mail :sangimusic@gmail.com
[2,5]Assistant professor , SNS College of Technology, Coimbatore, India
E-Mail : jeyan.krishnan@gmail.com

Abstract

In this paper , we mainly focus storage, computation, communication cost for secure dynamic multicast key distribution. Efficient key distribution is an important problem in secure group communication. Members in the groups are dynamic. They required new key update by using some encryption algorithm during the time of member join and revoked from the group. The previous work is focus on the basis of complete key graph algorithm, hierarchical key management algorithm follow the secure key distribution in the centralized method. We propose new protocol framework is secure group overlay multicast (SeGrOM) that follow decentralized method apply the protocol in hierarchical structure forms hybrid key management algorithm. Instead of using conventional encryption algorithm, the MDS code is used. Easily combined with the hierarchical structure provide low and balanced communication cost, storage cost, computation complexity for secure dynamic multicast key distribution.

Key words- secure multicast, hierarchical key management, MDS code, erasure decoding , key distribution, cost estimation.

1. INTRODUCTION

Group communication refers to either point-to-multipoint or multipoint-to-multipoint communications via some underlying networking infrastructures. The some of the real time applications like network gaming, conferencing are group oriented. They required key to communicate with each other. Key is a variable value that is applied using algorithm or encode, decode method is used send the message in the group communication. There are three types of keys used are group key, shared key, individual key. Group key is shared by all the user used to encrypt data transmitted to the group[2],[3] . Individual key is used for only one user also called unique key or pair wise key. Shared key used to communicate.

Members in the groups are dynamic can be handled under three methods.

- Centralized key management
- Distributed key management
- Decentralized key distribution

In first method, there is an single central group controller employed for controlling the whole group .The problem is the single point of failure. some examples logical key hierarchy , one-way function tree . In the second method, there is no group controller all the members in the group collaborate to perform the key generation [11]. Examples octopus protocol , PFMH tree. In the third method the management of a large group divided into the subgroup managers, mainly used to minimize the problem in the single manager [8] .Examples Iolus, kronos etc. We go with the first and third method to manage the large members in the group.

Key management is an cryptographic system design that related to generation, exchange, use and replacement of keys. Here group controller act as the key server to generate the new keys when new member join in the group or existing member revoked from the group.

A. Client Join

Client want to join the group, the client and server mutually authenticate share with server a key called individual key. When the user admitted to the group the group controller regenerate all the three keys and unicast to particular joining user and multicast to remaining rest of the user in the group. The cost of rekeying due to the joining user is small.

B. Client Revoked

When the one or more users revoked or forcefully removed from the group the group controller regenerate all the three keys and encrypted with the individual key then multicast to the remaining members in the group. The cost for revoking user from the secure group is an expensive operation.

Multicast [2],[7] is an efficient means of distributing the data than the unicast to reduce network traffic multicasting is divided into two categories are dynamic and the static group. In the dynamic group, the group controller sets up the system and the user in the group can form subgroup. In the static group system only a fixed group controller has the ability to form the subgroup. Data privacy can be achieved by a shared group key and shared key. Two types of the secrecy maintained are forward and the backward secrecy. The forward secrecy the old member who excluded from group cannot access the future communication. The

backward secrecy is the new member in the group cannot access the past communicated data.

The some of the fundamental attributes in the secure group communication are types of group management, scalability, overheads, trust relationship, resilience etc. This paper is mainly concentrating the overheads. In general, three types of overheads are incurred by all network operations: storage, communications and processing. For storage overheads, a group controller and a group member may require different amounts of memory to store group information such as session and group keys, list of group members, cryptography materials and Service-related .To process overheads, each group operation requires computation which can be measured in terms of the number of processing steps, processing duration and complexity bound.

The earlier works follow the basic structure. It cannot adopt the large group member. In order to overcome the problem they follow hierarchical structure come under centralized method. The group controller needs to interrupt the group communication during the rekeying. The efficient distribution of the new group key for multiple membership changes is a critical problem in secure group communication. We enhance the decentralized method , MDS code to overcome the problem. The main contribution of this paper are :

- We propose new protocol framework(**SeGrOM**) for secure group communication, that employ decentralized group membership, accommodate dynamic group changes and reduce communication overhead.
- Protocols combine with hierarchical structure forms hybrid key management algorithm.
- Instead of encryption algorithm, enhance MDS code, a class of error control codes to distribute multicast key dynamically.

2. HYBRID KEY MANAGEMENT ALGORITHM

A. Hierarchical Structure

It consist of basic structure. Where each R_i, $1 < i < d$, further consists of the basic structure $<R_i,u_{i1},u_{i2}, \ldots , u_{id}>$. The parameter d is the number of elements in a basic structure and can be considered as the degree of the hierarchy. Each level in structure maintained different shared key. R denote the root node. U denote user.

This follow the degree concept d=2,3,4…If d=2 root node contain two child. Then each child node maintains two node. The same procedure is followed to d=3,4..When one or more users revocate from structure at a time. The time required for rekeying.

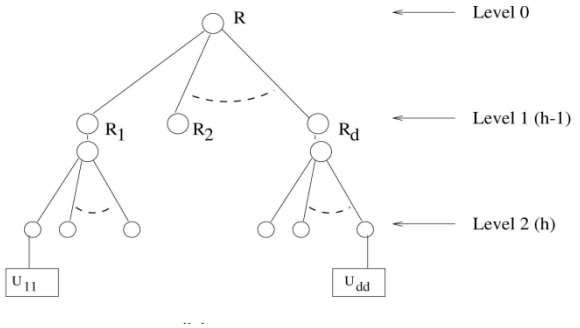

Figure.1 Hierarchical structure

The upper bound for rekeying cost is calculated by the formula $\min\{(h-p)r+d^{p-1})\}$.The storage cost by $2^{d-1}(dN-1/d-1)$.The rekeying cost is calculated number of encryptions performed and messages transmitted by the group controller. The computation cost be measured by the number of computation operations that the group controller and group members need to distribute and extract the key. Storage cost determined by number of key stored by the members in the group.

The problem in existing system the single group controller maintains the whole thing during the time of join/leave in the group. Moreover, as the group controller needs to interrupt the group communication during the rekeying, the resulting delay can be unreasonable for many applications. Thus, efficient distribution of the new group key for multiple membership changes is a critical problem in centralized secure group communication.

B. SeGrOM Framework and Protocol

SeGrOM uses hierarchical structure follows two protocols as a global data delivery protocol and local data delivery protocol forms .It supports three different variants are the security, communication cost and the storage ,computation cost .Local data protocol establish communication with the members in same access router .Each member in the group contain equal rights to become head member by using simple leader election algorithm .It maintain local data key .Head member handle join and the leave .Two head members connected by the link contain link key followed by the Diffie-Hellman key exchange .

During member join and revoked the group key ,link key ,local key maintained by the head member could be send by MDS code is described below .The flow of regenerated key as followed by the algorithm 1

Input: Packet m regenerated keys to be sent

1 s(source node) sends m to its local head member h_s;

2 h_s sends m to local receivers via the local protocol at a_s;

3 h_s forwards m to h_r via the global protocol;

4 h_r sends m to its local receivers via the local protocol at a_r.

The algorithm2 for Global data delivery with SeGrOM-Group

Packet m to be sent from h_s to any h_r

1 h_s encode m with group key K_g, result is m_e;

2 h_s sends m_e to h_r;

3 h_r decode m_e with group key K_g, result is m

These two algorithm combine with the hierarchical structure forms the hybrid key management algorithm .It maintain the certificate revocation list that include the name of the revoked members.

C. Maximum Distance Separable (MDS)

MDS consists of three phases:

1) The initialization of the GC 2) The join of a new member 3) The re-keying procedure whenever a group member leaves.

It is an class of error control code follows Galois field GF(q) be a finite field with q elements .The E(m)=c ,where m is the original message block, c is its code word block .If a decoding function D(c)=m is called an (n,k) MDS code. The process of recovering the k message symbols is called erasure decoding. The Reed-Solomon (RS) codes are a class of widely used MDS codes.

First have to initialize the group controller makes both the MDS code and the one-way hash function H. Whenever a new member i is authorized to join the multicast group for the first time, the GC sends it a pair (j_i,s_i), where s_i is a random element domain F, and j_i is a positive integer .The member join or revoked rekeying process held by the following procedure

D. Rekeying

The GC executes the rekeying process in the following steps:

1. The GC randomly chooses a fresh element r in F, which has not been used to generate previous keys.
2. The GC constructs an element c_{ji} in GF(q) : $c_j = H(s_i + r)$, where + is a simple combining operation in F.
3. Using an efficient erasure decoding algorithm for C, the GC can easily calculate the n corresponding message Symbols m_1m_2 ……..m_n.
4. The GC sets the new session key k to be the first message symbol m_1
5. The GC multicasts r and m_2……m_n.

The following steps to obtain the new session key:

1. Calculate $c_j = H(s_i + r)$ with its seed key (j_i,s_i)
2. Decode the first message symbol m1 from the (n – 1) message symbols m_2……m_n, together with its code word symbol c_j .
3. Recover the new session key k .This key recovery process, as shown in finishes the whole rekeying procedure.

The effort that an attacker makes to deduce a session key depends on the parameters of the scheme, namely, the size of finite field GF(2m), the size t of member i's seed key component s_i, and the size of a random number r .They couldn't find the correct message. The communication cost is determined by nl.The storage cost determine by $\lceil \log_2 L \rceil + t$ for group member and group controller follows $n(\lceil \log_2 L \rceil + t)$.

The erasure decoding operations for an MDS code only need $O(n^2)$ arithmetic operations if standard erasure decoding algorithms are used. Fast decoding algorithms only need O(nlogn) operations. The MDS code is chosen, both encoding and decoding only need $O(mn^2)$ binary exclusive OR operations. This scheme reduces the communication complexity of rekeying operations to O(logn), whereas each member needs to store O(logn) keys, and the GC needs to store O(nlogn) keys, where n is the multicast group size.

The advantage of the enhanced achieve data confidentiality in decentralized method equal to the centralized method .The protocol provide good performance and also small overhead than centralized. The wireless broadcast can be leveraged to reduce bandwidth consumption ,computation overhead and latency . Static routers provide a decentralized and more stable structure .It easily accommodate the dynamic member changes. It reduce the storage , computation ,communication cost due to MDS code .

3. KEY GENERATION AND DISTRIBUTED FRAMEWORK

A. Private Key

The Private Key is generated using MDS code. The GC sends his number of group members to the KGC (Key Generation Center). The keys are generated by the KGC and submitted to the GC.

B. Session Key

In session key generation, initially sixteen decimal digits are generated by using random number generation method .Then each decimal digit is splited and compared with pre determined binary format. In DES algorithm the 64 bits session key is considered as a message file and generated user's private key is considered as a key file. DES algorithm encrypts the session key by using user's private key and transmitted to the appropriate users.

C. Join Request

A Network node issues a request to GC to join the group. The GC checks whether the request is from an authenticated member or not. If yes the GC accepts the request. Then the node communicates its session key through some secure channel

D. Generate keys

From the new position onwards the GC generates the new key(s) along the path to root. The new

keys are used to replace the old keys of the auxiliary nodes. Update tree structure Old keys are replaced by their corresponding new keys. Hence forth newly generated keys are used for future communication. This operation provides backward secrecy i.e. it prevents the newly joined member from accessing the previously communicated data.

E. Distribute keys

A packet is constructed, which consists of newly generated key(s). This packet is encrypted using the old key known by a member or sub-group of members.

F. User-oriented re-keying

In the user-oriented re keying, the GC constructs each re keying message. Rekey message contains the encrypted form of session key. So that they contain exactly all the messages that some user or a group of users need.

G. Leave Request

The member issues a request to leave the group

H. Process Request

The GC checks whether the request is from an existing member, if so the GC accepts the request

I. Find leave position

The GC traverses the tree structure and finds the leaving position of the member. The GC then deletes the member details and removes the node from tree structure

4. IMPLEMENTATION AND RESULTS

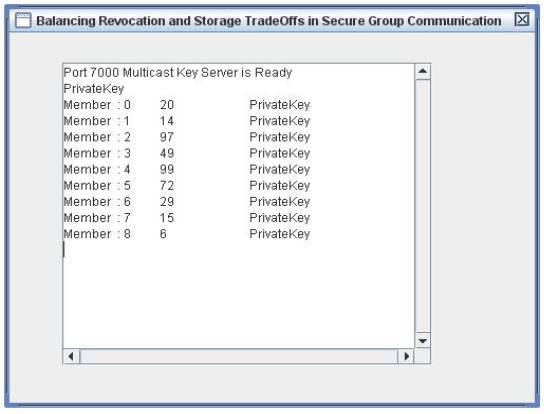

Figure.2 Initial member join

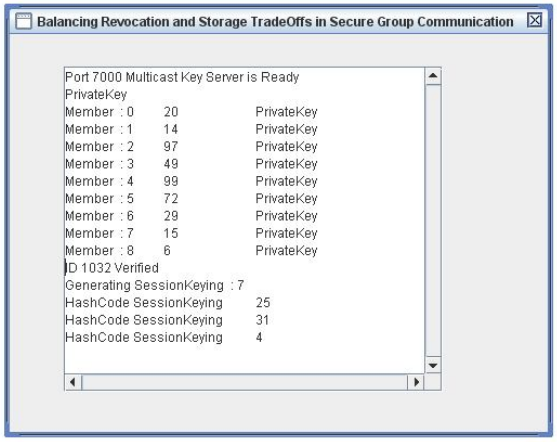

Figure.3 Regenerated key after member join

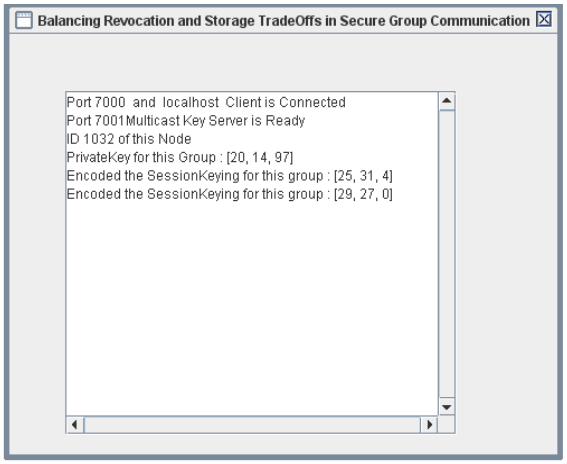

Figure.4 Regenerated key distributed to member

5. CONCLUSION & FUTURE WORK

Secure group overlay multicast that employs decentralized group membership to efficiently accommodate dynamic group changes and reduce communication overhead. The Generated keys distributed using MDS code. Our algorithm reduce the cost of rekeying by 50-90 As these tasks result in increased overhead at the end nodes, reducing control traffic is an important problem for overlay multicast. Our algorithms reduce the overhead at the end nodes by reducing the number of group key update messages sent by the group controller. These benefits are also desirable in wireless systems which are constrained in battery power for long days. Thus, in heterogeneous systems which compose of wired and wireless systems, our algorithms can be used to improve battery longevity of wireless systems by reducing the amount of traffic they need to transmit forward.

In future work can be followed by the load balancing and fault tolerant

6. REFERENCES

1. Bezawada Bruhadeshwar and Sandeep S.Kulkarni(2011)"Balancing Revocation and Storage Trade-Offs in Secure Group Communication" IEEE Transactions On Dependable And Secure Computing, VOL. 8, NO. 1
2. Chung Kei Wong ,Mohamed Gouda ,Simon S. Lam (2000) "Secure Group Communications Using Key Graphs," IEEE/ACM Trans. Networking, vol. 8,no. 1, pp. 16-30
3. Hanjin Lee, Hyunsoo Yoon , Junbeom Hur , Seungjae Shin (2009) "Bandwidth Efficient Key Distribution for Secure Multicast in Dynamic Wireless Mesh Networks", WCNC 2009 proceedings
4. Liaho xu , Cheng Huang (2008) "Computation-Efficient Multicast Key Distribution" IEEE Transaction on Parallel and Distributed System VOL 19,NO 5
5. Mittra.S(1997) "Iolus: A Framework for Scalable Secure Multicasting" Proc. ACM SIGCOMM '97, pp. 277-28
6. Mohamed M. Nasreldin Rasslan, Yasser H. Dakroury, and Heba K. Aslan (2009),"A New Secure Multicast Key Distribution Protocol Using Combinatorial Boolean Approach" ,International Journal of Network Security, Vol.8, No.1, PP.75–89
7. Rakesh Chandra gangwar(2008) "secure and efficient decentralized group key establishment protocol for robust group", journal of theoretical and applied information technology
8. Sasikala Devi.S, Dr. Antony Selvadoss Thanamani (2010) "An optimized approach for multicast rekeying using MDS code on PFMH tree " IEEE International Conference on Computational Intelligence and Computing Research , VOL 2
9. Harney.HandMuckenhirn.C,(1997)"Group Key Management Protocol (GKMP) Specification," RFC 2093.
10. Lein Harn and Changlu Lin,(2010) "Authenticated Group Key Transfer Protocol Based on Secret Sharing", IEEE transactions on computers, vol. 59, no. 6
11. Alwyn R. Pais ,Shankar Joshi "A new probabilistic rekeying method for secure multicast groups"