Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2002-2007 | ISSN:2251-6727

Secure Key Refurbishing Using Queue Batch Algorithms in Multicast Group Communication

[1]Somasundaram K, [2]Karthikeyan A

[1]Assistant Professor, Department of Information Science and Engineering, Bannari Amman Institute of Technology Sathyamangalam, Erode - 638401., Tamil Nadu, India.

[2]Assistant Professor, Department of Computer Science and Engineering, Panimalar Engineering College Chennai 600123, Tamil Nadu, India

(Received: 07 October 2023 Revised: 12 November Accepted: 06 December)

KEYWORDS
Authentication, peer groups allocation, group key management, re-keying, multicast group communication

ABSTRACT:
In a group-oriented communication here is a need for privacy and data integrity. The group members can find a shared key for encrypting data. A protected distributed group key agreement and authentication protocol is implemented by means of interval-based approach of renewing the keys with batch and queue-batch algorithm.Presentationof these interval-based algorithms under different settings, such as unlike joins and leave probabilities, is analyzed. The Queue-batch algorithm accomplishes the best among the interval-based algorithms. Distributed group key arrangement protocol is different from traditional national group key management protocols. This planned scheme provides rekeying efficiency.

I.INTRODUCTION

Distributed group key arrangement protocol is different from outdated centralized group key management protocols. Centralized protocols trust on a centralized key server to professionally distribute the group key. An excellent body of work on national key distribution protocols exists. In those approaches, cluster members are arranged in a rational key hierarchy known as a *key tree*. Using the tree topology, it is easy to allocate the group key to members whenever there is any modification in the group membership (e.g., a new member joins or an existing member leaves the group).

In the distributed key agreement protocols we consider, however, there is no unified key server available. This arrangement is acceptable in many situations—e.g., in peer-to-peer or ad hoc networks wherever centralized resources are not eagerly available. Moreover, an benefit of distributed protocols over the national protocols is the increase in system reliability, because the group key is

generated in a common and contributory fashion and there is no single-point-of-failure.

In the special case of a announcement group having only two members, these associates can create a group key using the Diffie–Hellman key exchange protocol [6]. In the protocol, associates and use a cyclic group of prime order with the generator. They can produce their secret exponents. Member can figure its public key and send it to receiver. Since both associates know their own exponent, they can each raise the other party's public key to the advocate and produce a common group key. Using the common group key, and can scramble their data to prevent eavesdropping by intruders.

To prevent a new user from reading past communications (backward confidentiality) and a deceased user from reading future communications (forward confidentiality) [6], the re-keying, which means reintroducing the keys associated with the nodes of the key tree, is performed. In this paper, we suggest, based on the tree-based group Diffie–Hellman protocol [11], several group key arrangement protocols for a dynamic communication group in which members are positioned in a distributed fashion and can join and leave the group at any time.

II.RELATED WORKS

Diffie–Hellman [6] planned the first two-party single-round key agreement protocol. Joux proposed a single-round three-party key agreement protocol that uses bilinear pairings. Burmester and Desmedt [5] had planned a multiparty two-round key agreement (BD) protocol using a ring structure of participants. The BD

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2002-2007 | ISSN:2251-6727

protocol makes the active opponent control over the conduit of all these protocols. These protocols assume only a passive adversary and validate their security on purely heuristic models.
Burmester and Desmedt demonstrated that their ring structure-based group key agreement protocol is secure against a passive opponent in standard model under decision Diffie–Hellman (DDH) assumption. Several variations of Diffie–Hellman protocol and Joux [11] protocol have been proposed to incorporate authentication and a trial-and-error method has been adopted to provide informal security.

To accomplish secure group communication and re-keys at each join or leave event. Li et al. [13] and Yang et al. [13], then apply the periodic re-keying concept in Kronos [16] to the key tree setting. All the key-tree-based approaches [16] require a national key server for key generation. Burmester and Desmedt [5] propose a computation-efficient protocol at the cost of high communication overhead. Steiner et al. [3] propose Cliques, in which every member introduces its key module into the result caused by its preceding member and permits the new result to its following member.

Cliques are well-organized in re-keying for leave or partition events, but imposes a high capability on the last member in the chain. Kim et al. [10] propose TGDH, which organizes keys in a tree structure. The setting of TGDH is similar to that of the One-Way Function Tree (OFT) scheme [16] excluding that TGDH uses Diffie–Hellman instead of one-way functions for the group key generation. Kim et al. [10] also recommend a variant of TGDH called STR which reduces the communication overhead by trading off the computation complexity. All the above arrangements are decentralized and hence avoid the single-point-of-failure problem in the centralized case, though they introduce high message traffic due to distributed communication. A orientation [11] considers re-keying at single join, single leave, merge, or partition events. Our work considers a more wide-ranging case that consists of a batch of join and leave events. Comparison between the national and regionalized re-keying is studied by Amir et al. [1]. In particular, Amir et al. [1] suggest a national key distribution scheme based on Cliques [3] and compare the routine of both schemes. In distinction, our work compares the centralized and decentralized key management schemes modified from a key tree setting. Rather than accentuate the re-keying efficiency, [3] focus on the security issues and develop valid group key agreement schemes based on the Burmester-Desmedt model, Cliques, and TGDH, respectively.

Tree based group Diffie-Hellman is used to proficiently maintain the group key in a dynamic peer group with more than two members. Each member maintains a set of keys, which are settled in a hierarchical binary tree. We allocate a node ID to every tree node. For a given node, we subordinate a secret (or private) key and a blinded (or public) key. All arithmetic operations are accomplished in a cyclic group of prime order with the originator. Each leaf node in the tree resembles to the individual secret and blinded keys of a group member. Every associate holds all the secret keys along its key path starting from its connected leaf node up to the root node. Therefore, the undisclosed key held by the root node is shared by all the members and is watched as the group key. The secret key of a non leaf node can be produced by the undisclosed key of one child node of and the blinded key of another child node. The secret key at a leaf node is selected by its corresponding group participant through a secure pseudo random number originator. Since the blinded keys are widely known, every member can calculate the keys along its key path to the root node based on its separate secret key.

To provide both regressive confidentiality (i.e., joined members cannot access previous communication data) and forward confidentiality (i.e., left members cannot access future communication data), re-keying, is accomplished whenever there is any group membership change (join of new member or leaving of existing member). Individual re-keying is completed after every single join or leave event. Before the group membership is transformed, a special member called the sponsoris elected to be answerable for updating the keys carried by the latest member or departed member. Tree group key utilize the conference that the rightmost member under the sub tree rooted at the sibling of the enter and leave nodes will take the sponsor role. The survival of a sponsor does not violate the reorganized requirement of the group key generation while the sponsor does not add extra contribution to the group key.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2002-2007 | ISSN:2251-6727

Interval based distributed re-keying algorithms significantly lower the computation and communication expenditures of maintaining the group key. The interval-based approach provides re-keying efficiency for dynamic peer groups while preserving both distributed (i.e., no centralized key server is involved) and contributory (i.e., each member contributes to the resulting group key) properties. Interval-based re-keying maintains the re-setting frequency regardless of the dynamics of enter and leave events, with a tradeoff of declining both backward and forward confidentialities as a result of delaying the update of the group key. The interval-based algorithms are created based on the following hypotheses

The group communication fulfills point of view synchronization that defines consistent and ordered message dispensing under the same membership view. Naturally, when a member broadcasts a message under a membership view, the message is sent to same set of members viewed by the sender. Note that this view-synchrony property is important not only for group key agreement, but also for consistent multipoint-to-multipoint group communication in which every single member can be a sender. Since the interval-based re-keying processes consist of nodes lying on more than one key path, more than one sponsor may be nominated. Also, a new node may be re-keyed by more than one sponsor. Therefore, it is understood that the sponsors can organize with one another such that the blinded keys of all the improved nodes are broadcast only. An interval-based re-keying is utilized in order to eradicate the difficulties of individual re-keying such as incompetence and out-of-sync problem.Interval-based re-keying retains the re-keying frequency irrespective of the dynamics of enter and quit events, with a tradeoff of declining both backward and forward confidentialities as a result of postponing the update of the group. Interval-based re-keying is done through the methodologies Rebuild algorithm, the Batchalgorithm, and the Queue-batch algorithm.

The Rebuild algorithm reduces the resulting tree height so that the re-keying functions for each group member can be red uced. At the opening of every re-keying interval, recreate the whole key tree with all existing members that persist in the communication group, together with the newly joining members. The resulting tree is a left-complete tree, in which the depths of the leaf nodes vary by at most one and those deeper leaf nodes are located at the leftmost positions. Rebuild is appropriate for some cases, such as when the membership events are so repeated that we can directly reconstruct the whole key tree for simplicity, or when some members miss the re-keying information and the easiest way of recovery is to re-build the key tree.The Batch algorithm is based on the central approach, which is now applied to a distributed system without a centralized key server. Given the numbers of joins and leaves within a re-keying period, we attach new group members to different leaf positions of the key tree in order to stay the key tree as neutral as possible.

Rebuild and batch re-keying approaches play all re-keying steps at the starting of every re-keying interval. This results in high processing capacity during the update instance and thereby de-lays the beginning of the protected group communication. Thus a more successful algorithm Queue-batch algorithm is proposed to develop. It decreases the re-keying load by pre-processing the joining members during the idle re-keying interval. The Queue-batch algorithm is divided into two segments, namely the Queue-sub tree phase and the Queue-merge phase. The first stage occurs every time a new member joins the communication group during the re-keying interval. In this case, attach this new member in a short-term key tree. The second phase occurs at the opening of every re-keying interval and we merge the temporary tree (which contains all newly joining members) to the existing key tree.

Pseudo-code of the Queue sub tree phase
Queue-sub tree ($")

```
1.  if (a new member joins){
2.    if ($"==NULL)/*no new member in $"*/
3.        else{
4.     find the insertion node;
6.     add the new member to $";
7.     elect the rightmost member under the sub tree
       rooted at the sibling of the joining node to be
       the sponsor;
8.     If (sponsor)/* sponsor's responsibility*/
9.          re-key renewed nodes and broadcast new
            blinded keys;
10.   }
11.}
```

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2002-2007 | ISSN:2251-6727

Pseudo-code of the Queue merge phase

Queue-merge (T,$",M[l], Q)

1. If (Q==0){
2. add $" to either the shallowest node (which need to be the leaf node) of T such that the merge will not increase the resulting tree height, or the root node of T if the merge to any location will increase the resulting tree height;
3. } else {
4. add $" to the highest leave position of the key tree T;
5. remove remaining Q-1 leaving leaf nodes and promote their siblings;
6. }
7. elect members to be sponsors if they are the rightmost members of the sub tree model rooted at the sibling nodes of the departed leaf nodes in T, or they are the rightmost member of $";
8. if(sponsor)
9. re-key renewed nodes and broadcast new blinded keys;

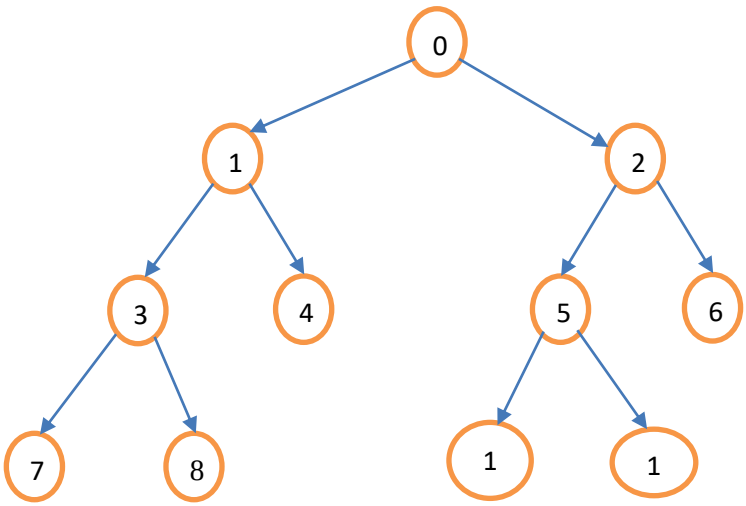

Fig. 1: Queue sub tree phase

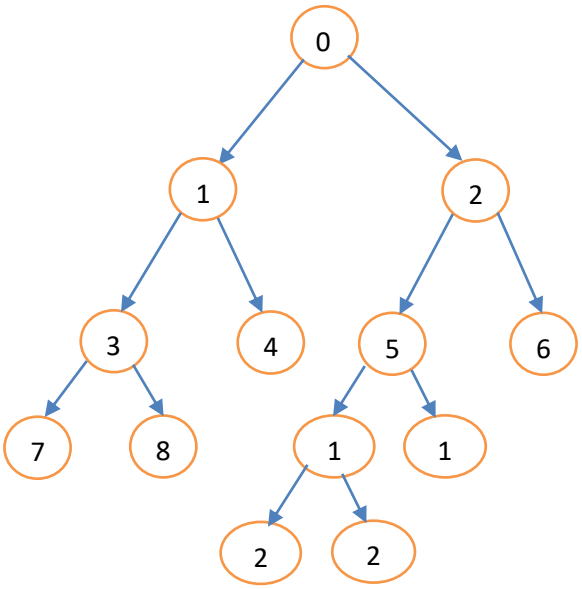

Fig. 2: Queue merge phase

III.PERFORMANCE EVALUATION ON SECURED GROUP KEY MANAGEMENT:

To indicate the latency of generating the latest group key for data privacy, we calculate the performance of the interval-based algorithms in two aspects: mathematical analysis and simulation-based experiments. The mathematical analysis considers the difficulty of the algorithms under the assumption that the key tree is completely stable. Using simulations, we then study their performance in a more general setting. We also compare the performance of our interval-based algorithms and a centralized key distribution methodology.

The analysis of the three proposed algorithm are based on two performance measures i.e., number of exponentiation operations and the number of renewed nodes. The number of exponentiation operation gives a measure of the computation load in terms of node density to communication group's packets drop . The number of new nodes is said to be new if it is a non leaf node and its associated keys are new. These metric measures the communication cost since the new blinded keys of the new nodes have to be transmitted to the whole group.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2002-2007 | ISSN:2251-6727

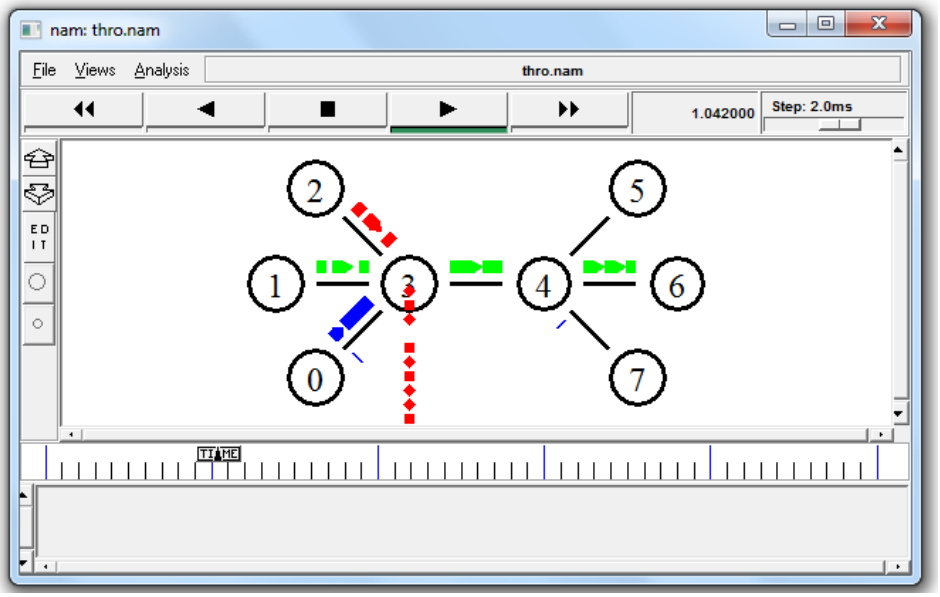

Fig. 3: Secure Key Refurbishing Using Queue Batch Algorithms In Multicast Group Communication

IV.CONCLUSION:

The anticipated model of this work provides a distributed cooperative key agreement protocols for dynamic peer groups. The key arrangement setting is performed in which there is no national key server to maintain or dispense the group key. We show that one can use the TGDH protocol to achieve such distributive and concerted key agreement. To condense the re-keying complexity, we recommend to use an interval-based approach to carry out re-keying for many joins and leave requests at the same time, with a interchange between security and performance. In particular, suggestion showed that the Queue-batch algorithm can menacingly reduce both computation and announcement costs when there is highly frequent membership events. The proposal also discourses both authentication and employment for the interval-based key arrangement algorithms.

ACKNOWLEDGEMENT

This paper is based on research conducted by emerging technology key distribution .I am grateful for a number of friends and colleagues in encourages me to start a work, I thanks to our management of Panimalar Engineering College and Department of Computer Science and Engineeering for academic support and friend. Finally I would like to thanks for all kept me going process.

REFERENCES

[1] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, “Secure group communication using robust contributory key agreement,” IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468–480, May 2004.

[2] Y. Amir and J. Stanton, The Spread Wide Area Group Communication System. Johns Hopkins Univ., Baltimore, MD, CNDS-98-4, 1998.

[3] G. Ateniese, M. Steiner, and G. Tsudik, “Authenticated group key agreement and friends,” in Proc. 5th ACM Conf. Computer and Communication Security, Nov. 1998, pp. 17–26.

[4] S. Blake-Wilson and A. Menezes, “Authenticated Diffie-Hellman key agreement protocols,” in Proc. 5th Annu. Workshop on Selected Areas in Cryptography (SAC’98), 1998, vol. LNCS 1556, pp. 339–361.

[5] M. Burmester and Y. Desmedt, “A secure and efficient conference key distribution system,” in Proc. Advances in Cryptology—EUROCRYPT’ 94, 1995, vol. LNCS 950, pp. 275–286.

[6] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, 1976.

[7] A. Fekete, N. Lynch, and A. Shvartsman, “Specifying and using a partionable group communication service,” in Proc. 16th ACM Symp.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2002-2007 | ISSN:2251-6727

Principles of Distributed Computing (PODC), Aug. 1997, pp.53–62.

[8] C. G. Günther, "An identity-based key exchange protocol," in Proc. Advances in Cryptology—EUROCRYPT'89, 1989, vol. LNCS 434, pp. 29–37.

[9] M. Just and S. Vaudenay, "Authenticated multi-party key agreement," in Proc. Advances in Cryptology—ASIACRYPT'96, 1996, vol. LNCS 1163, pp. 36–49

[10] Y. Kim, A. Perrig, and G. Tsudik, "Communication-efficient group key agreement," in Proc. 17th IFIP Int. Information Security Conf. (SEC'01), Nov. 2001, pp. 229–244.

[11] ——, "Tree-based group key agreement," ACM Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60–96, Feb. 2004.

[12] P. P. C. Lee, "Distributed and collaborative key agreement protocols with authentication and implementation for dynamic peer groups," M.Phil. Thesis. The Chinese University of Hong Kong, Jun. 2003.

[13] X. S. Li, Y. R. Yang, M. G. Gouda, and S. S. Lam, "Batch re-keying for secure group communications," in Proc. 10th Int. World Wide Web Conf. (WWW10), Orlando, FL, May 2001, pp. 525–534.

[14] A. Perrig, "Efficient collaborative key management protocols for secure autonomous group communication," in Int. Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), Jul. 1999, pp.192–202.

[15] S. Setia, S. Koussin, and S. Jajodia, "Kronos: a scalable group re-keying approach for secure multicast," in Proc. IEEE Symp. Security and Privacy, May 2000, pp. 215–228.

[16] A. T. Sherman and D. A. 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.