Review on Group Key Agreement Protocol

M. Swetha, L. Haritha

Abstract— Many applications in Dynamic Peer Group are becoming increasing popular nowadays. There is a need for security services to provide group-oriented communication privacy and data integrity. To provide this form of group communication privacy, it is important that members of the group can establish a common secret key for encrypting group communication data. A secure distributed group key agreement and authentication protocol is required to handle this issue. Instead of performing individual re-keying operations, an interval-based approach of re-keying is adopted in the proposed scheme. The proposed interval based algorithms considered in this paper are Batch algorithm and the Queue-batch algorithm. The interval-based approach provides re-keying efficiency for dynamic peer groups while preserving both distributed and contributory properties.Performance of these interval-based algorithms under different settings, such as different join and leave probabilities, is analyzed The Queue-batch algorithm performs the best among the interval-based algorithms

1. INTRODUCTION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password.

Secure and reliable group communication is an active area of research. Its popularity is caused by the growing importance of group-oriented and collaborative applications. The central research challenge is secure and efficient group key management. While centralized methods are often appropriate for key distribution in large multicast-style groups, many collaborative group settings require distributed key agreement techniques. Many applications in Dynamic Peer Group are becoming increasing popular nowadays. There is a need for security services to provide group-oriented communication privacy and data integrity. To provide this form of group communication privacy, it is important that members of the group can establish a common secret key for encrypting group communication data. A secure distributed group key agreement and authentication protocol is required to handle this issue.

Centralized protocols rely on a centralized key server to efficiently distribute the group key.

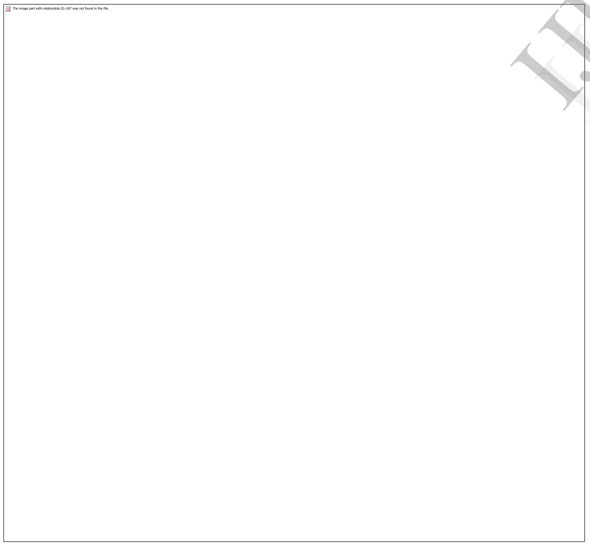
2. GROUP KEY ESTABLISHMENT

Two-Party Diffie-Hellman Extended To Groups protocol was intended to exchange a secret key over an insecure medium, and is based upon the difficulty of computing the discrete logarithm in a finite field. Linear

Group Diffie-Hellman for a group of n nodes arranged in a vector or list at indices 0 through n – 1 with an interconnection . Tree-Based Group Diffie-Hellman a group of n nodes arranged in a list or array representing the leaves of a binary tree, with an interconnection.

Fault-tolerant, scalable, and reliable communication services have become critical in modern computing. An important and popular trend is to convert traditional centralized services (e.g., file sharing, authentication, web, and mail) into distributed services spread across multiple systems and networks.

The tree-based group Diffie–Hellman protocol is used to establish the group key in a dynamic peer group. Each member maintains a set of keys, which are arranged in a hierarchical *binary tree*.


The image part with relationship ID rId7 was not found in the file.

A node ID *v* is assigned to every tree node. For a given node *v* a secret (or private) key KV and a blinded (or public) key BKV re associated. All arithmetic operations are performed in a cyclic group of prime order *p* with the generator. Therefore, the blinded key of node *v* can be generated by

Notations
V =which is anode id
K=private or secret key
B=public key

2.1 Tree Based Group Key in Dynamic Peers

Tree based group Diffie-Hellman is used to efficiently maintain the group key in a dynamic peer group with more than two members. Each member maintains a set of keys, which are arranged in a hierarchical binary tree. We assign a node ID to every tree node. For a given node, we associate a secret (or private) key and a blinded (or public) key. . Every member holds all the secret keys along its key path starting from its associated leaf node up to the root node. To provide both backward 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 performed whenever there is any group membership change (join of new member or leaving of existing member). Individual rekeying is performed after every single join or leave event. Before the group membership is changed, a special member called the sponsor is elected to be responsible for updating the keys held by the new member or departed member. Tree group key use the convention that the rightmost member under the sub tree rooted at the sibling of the join and leave nodes will take the sponsor role. The existence of a sponsor does not violate the decentralized requirement of the group key generation since the sponsor does not add extra contribution to the group key.

2.2 Interval Based Distributed Re-Keying

The group communication satisfies view synchrony that defines reliable and ordered message delivery under the same membership view. when a member broadcasts a message under a membership view, the message is delivered to same set of members viewed by the sender. Note that this view-synchrony property is essential not only for group key agreement, but also for reliable multipoint to- multipoint group communication in which every member can be a sender. Since the interval-based re-keying operations involve nodes lying on more than one key path, more than one sponsor may be elected. Also, a renewed node may be rekeyed by more than one sponsor. Therefore, it is assumed that the sponsors can coordinate with one another such that the blinded keys of all the renewed nodes are broadcast only.

2.3 Rebuild and Batch Algorithm

The Rebuild algorithm minimizes the resulting tree height so that the re-keying operations for each group member can be reduced. At the beginning of every re-keying interval, reconstruct the whole key tree with all existing members that remain 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 differ by at most one and those deeper leaf nodes are located at the leftmost positions. Rebuild is suitable for some cases, such as when the membership events are so frequent that we can directly reconstruct the whole key tree for simplicity, or when some members lose the re-keying information and the simplest way of recovery is to re-build the key tree. The Batch algorithm is based on the centralized 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 interval, we attach new group members to different leaf positions of the key tree in order to keep the key tree as balanced as possible.

2.4 Queue Batch Algorithm

Rebuild and batch re-keying approaches perform all rekeying steps at the beginning of every re-keying interval. These 4 results in high processing load during the update instance and thereby de-lay the start of the secure group communication. Thus a more effective algorithm Queue-batch algorithm is proposed to develop. It reduces the re-keying load by preprocessing the joining members during the idle re-keying interval. The Queue-batch algorithm is divided into two phases, namely the Queue-sub tree phase and the Queue merge phase. The first phase occurs whenever a new member joins the communication group during the rekeying interval. In this case, append this new member in a temporary key tree. The second phase occurs at the beginning of every re-keying interval and we merge the temporary tree (which contains all newly joining members) to the existing key tree.

3. CONCLUSION

This work provides a distributed collaborative key agreement protocols for dynamic peer groups. The key agreement setting is performed in which there is no centralized key server to maintain or distribute the group key.
TGDH protocol to achieve such distributive and collaborative key agreement.
Interval-based approach is used to reduce the re-keying complexity.
Queue-batch algorithm can significantly reduce both computation and

communication costs when there is highly frequent membership events.

M. Swetha working as Assistant professor in Jaya Prakash Narayan group of Institutions (JNTUH) , Mahabubnagar, Andrapradesh. Her areas of interest include Wireless networks, Information Security currently focusing on IP Networks

L.Haritha working as Associatae professor in Jaya Prakash narayan College of Engg(JNTUH) , Mahabubnagar, Andrapradesh. Her areas of interest include Wireless networks, Information Security currently focusing on IP Networks