Optimization Techniques For Military Multicast Key Management

Thorsten Aurisch

Date: 2009/12/08
Speaker: Jhang Hon-Bin
Outline

- Introduction
- Proposed Scheme
- Performance evaluation
- Conclusions
Introduction

Multicast is a very efficient and scalable technique for group communication.

1. Multicast group mapping
2. Source authentication
3. Group access
4. Confidentiality
Proposed Scheme

The key agreement part forces every member to calculate the tree by means of an iterative Diffie Hellman group key exchange.

The key distribution mode a group controller constructs the key tree and spreads the group key in a secure way.
Proposed Scheme

From the software design point of view both modes can base on the c++ class KeyTree{}

The derivate classes AgreeKeyTree{} and DistKeyTree{} implement the special mode functionality needed for key update.

In order to provide an easy accessible interface to the cryptographic library the classes are derived a second time.
The principle of the algorithm is encrypting the exchanged data with the auxiliary keys of the tree to securely communicate with a subset of the group.

The selected auxiliary key is only known by the subset of the group.
Proposed Scheme

Within groups working with the key agreement algorithm a transaction manager (TM) exists for the observation of the next key operation.

A three way handshake is used to transmit the new user’s individual blind key BK(u8) to the current TM and authenticate the user.

A new node is added to the key tree storing the user’s individual blind key.

The tree path from the user to the root become invalid.

Figure 4. key agreement: protocol and key tree for u₈ joining the group
1. Within a group of 140 users batched rekeying with 10% maximum fluctuation rate for the mode **key distribution** is investigated.
2. By means of batched rekeying a significant efficiency can be obtained when the number of leaves is about the same size as the number of joins.
3. The improvement depends on the group size. Within large groups the efficiency is also larger.

1. Within a group of 40 users and 20% maximum fluctuation rate, the obtained improvements are in principal comparable to the improvement within the **key distribution** mode.
2. The increased efficiency is much higher because of the saved transmissions of the total tree during the membership operation.
3. Processing J join and L leaves in a batch reduces the number of update messages within key distribution to one.
Performance evaluation

1. Join request inter arrival time = 7.5 minutes
2. Average membership duration = 4.3 hour
3. The obtained improvement of key distribution is smoothing the rekeying frequency.
4. The system saves 18% and 24% of the update keys using a collection period of 120s and 240s.
1. The same investigation is done for the mode key agreement.

2. Collecting the requests 120s and 240s saves 51 and 61% of the transmitted keys.
Performance evaluation

1. The investigation results of using the probabilistic tree construction and key distribution within a group of 200 users.

2. The polygon display gives a compressed representation of the key tree.

3. Group key update efficiency is improved by decreasing of the tree entropy.

4. It causes a depletion of the balance within the tree.
Conclusions

- The usage of key trees simplifies the implementation of both modes.

- Utilizing information of military groups increases the efficiency of the key update procedure.

- The increased efficiency is obtained by means of batched rekeying and probabilistic key tree construction.

- The usage of key trees produces an optimization for both modes of operation.