Secure Group Communications in Wireless Networks

Yiling Wang
Monash University, Australia

Phu Dung Le
Monash University, Australia

INTRODUCTION

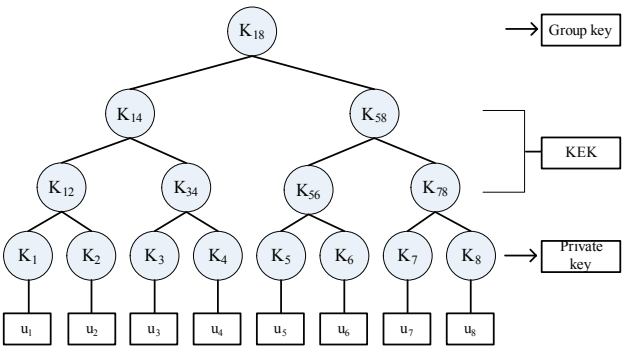
After a decade of exponential growth, wireless technologies have profoundly impacted people's lifestyles. Wireless networks provide users with greater flexibility and benefit by anytime and anywhere services (Pahlavan & Krishnamurthy, 2002). At the same time, rapid developments in multicast have led to the emergence of many multicast applications, such as stock quoting, multimedia conferencing and network gaming. Therefore it is reasonable to believe that the integration of wireless and multicast will benefit mobile users. Before the customers can enjoy the efficiency and convenience of wireless multicasts, access control must be employed to guarantee that only legitimate users can utilize the multicast services.

BACKGROUND

Access control can be achieved by employing a cryptographic key shared by all group members, which is applied to encrypt the multicast contents. Many group key management approaches (Sherman & McGrew, 2002; Perrig, Song, & Tygar, 2001; Amir, Kim, NitaRotaru, Schultz, Stanton, & Tsudik, 2004; Harney & Muckenhirn, 1997; Steiner, Tsudik, & Waidner, 1996; Mittra, 1997; Banerjee & Bhattacharjee, 2002; Kostas, Kiwior, Rajappan, & Dalal, 2003) have been proposed and most of them are directed toward the wired network. Although the research work done in the wired environment can be applied in wireless networks, the efficiency and security are not the same as that in wired networks. The reason results from not only the limitations of wireless networks, such as high communication error rate and limited bandwidth, but also the properties of light-weight mobile devices, such as limited computational power, insufficient power supply, great mobility and storage limitation.

In order to reduce the communication, computation and storage costs, hierarchical structure (tree structure) is widely applied in the group key management approaches. These schemes utilize all the keys, that is, group key and supporting keys, to construct a balanced key tree.

Figure 1. A typical key management tree



Each node of the tree holds a key. The root node of the tree represents the group key. Each leaf node corresponds to a group member, and possesses a private key associated with the member. The intermediate nodes hold key encryption keys (KEK), which are the auxiliary keys used for the distribution of the group key and other KEKs. Each member needs to store a set of keys in the path from its node to the root of the tree. When a member joins or leaves, the key distributor center (KDC) generates a set of new keys from the leaf node associated with the member to the root, and multicasts this set of keys to all the other group members. For example, as shown in Figure 1, for user 3 joining or leaving, key $k_{34,}$ $k_{14,}$ and k_{18} need to be updated.

For user 3 joining:

$KDC \rightarrow u_3: \{k_{34,} k_{14,} k_{18}\}_{k3}$

$KDC \rightarrow u_4: \{k_{34,} k_{14,} k_{18}\}_{k4}$

$KDC \Rightarrow (u_1,u_2): \{k_{14,} k_{18}\}_{k12}$

$KDC \Rightarrow (u_5,u_6,u_7,u_8): \{k_{18}\}_{k58}$

For user3 leaving:

$KDC \rightarrow u_4: \{k_{34,} k_{14,} k_{18}\}_{k4}$

$KDC \Rightarrow (u_1,u_2): \{k_{14,} k_{18}\}_{k12}$

$KDC \Rightarrow (u_5,u_6,u_7,u_8): \{k_{18}\}_{k58}$

GROUP KEY MANAGEMENT ALGORITHM

Group key management algorithm is core part of multicast security. It maintains the logical key structure and performs the procedures to assign, distribute and update the group key and other KEKs.

Notation

In this section, we depict the notations that we will use in the following sections:

- u: user
- bs: base station
- n: the number of members in the subgroup
- n_c: the number of the cluster in the subgroup
- n_s: the number of subgroups
- m: the number of users in the cluster
- j: the number of multiple subgroups which user joins and leaves simultaneously
- α: degree of the balance tree
- d: the height of the balance tree ($d = \log_\alpha n$)
- k: the encyption key
- BS = $\{s_1, s_2, s_3, ..., s_n\}$: the set of the base stations
- $\{x\}k$: message x encrypted by the key k
- A → B: {x}: A sends message x to B via unicast
- A => B: {x}: A sends message x to B via broadcast or multicast

The Proposed Logical Key Structure

Generally, a large multicast group is comprised of several smaller subgroups. Each member not only joins the group communications but also participates in one or some subgroup communications. Nevertheless the current proposed key tree cannot reflect such a group organization structure. Meanwhile a separate key tree must be constructed for each subgroup. To improve the performance of group key management under such scenario, we propose a new logical group keying structure shown in Figure 2.

From Figure 2, we can see that the proposed structure is a multi-tier model. The root node instigates the group communication session, and holds the group key. Each subgroup represents a multicast session and is associated with two keys: subgroup key and subgroup KEK (key encryption key). Users in the subgroup are divided into several clusters. Each cluster has its own cluster key to distribute other keys in the cluster. In the user level, each user shares a secret key with base station.

It is a common scenario that a user subscribes multiple subgroups simultaneously. To improve the efficiency, we introduce a new concept: super-subgroup, which is a virtual container to accommodate users who participate in multiple subgroups simultaneously. Each super-subgroup is a combination of several subgroups. For example, as shown in Figure 2, super-subgroup (A_B) is a super-subgroup combining subgroup A and B, where users 9 to 11 participate in the subgroup A and B concurrently. Super-subgroup can be a combination of any subgroups. According to the theory of permutation and combination, for a group having n_s subgroups, the total number of super-subgroups is

$$\sum_{i=2}^{ns} c_n^i .$$

Figure 2. Logical key management structure