Efficient and Scalable Group Key Management in Wireless Networks

Yiling Wang
Monash University, Australia

Phu Dung Le
Monash University, Australia

INTRODUCTION

Multicast is an efficient paradigm to support group communications, as it reduces the traffic by simultaneously delivering a single stream of information to multiple receivers on a large scale. Along with widespread deployment of wireless networks and fast improving capabilities of mobile devices, it is reasonable to believe that the integration of wireless and multicast will result in enormous benefits. Before users can enjoy the flexibility and efficiency of wireless multicast, security must be achieved. The core issue of wireless multicast security is access control, which means that only authorized users can participate in the group communications. Access control can be achieved by encrypting the communication data with a cryptographic key, known as group key. Group key is shared by all the registered users, so that only authorized members can gain access to the group communication contents. Several group key management approaches (Challal & Seba, 2005; Sherman & McGrew, 2003; Kostas, Kiwior, Rajappan, & Dalal, 2003; Wong, Gouda, & Lam, 2000; Wallner, Harder, & Agee, 1999; Harney & Muckenhirn, 1997; Steiner, Tsudik, & Waidner, 1996; Mittra, 1997; Hardjono, Cain, & Monga, 2000; Kim, Perrig, & Tsudik, 2004; Perrig, Song, & Tygar, 2001) have been proposed in the literature, most of them directed towards wired networks. Although some approaches can be employed in the wireless environment, they cannot achieve the same efficiency as in the wired networks. The complexity of group key management in wireless networks cannot be confined only to the limitation of wireless networks such as higher data error rate and limited bandwidth, but also from the properties of wireless devices, such as insufficient computation power, limited power supply, and inadequate storage space.

BACKGROUND

Over the last decade, a large number of group key management approaches have been proposed. Among them, the most prominent is the logical key hierarchy (LKH) (Wong et al., 2000; Wallner et al., 1999). In LKH, a key tree is formed comprising group and other auxiliary keys (key encryption key, KEK) that are used to distribute the group key to the users. Figure 1 depicts a typical LKH key tree. In the LKH key tree, users are associated with the leaf nodes, and each user must store a set of keys along the path from leaf node up to the root. When membership changes such as join or departure, the rekeying procedure is invoked to update the keys along the path, thereby ensuring security. This update affects all the members in the tree. LKH algorithm has some drawbacks which prevent its application in the wireless environment:

- **1-Affects-n:** As mentioned above, one membership change affects all the group members. But some changes are unnecessary to the members, especially in cellular networks, because the users in the cell are not only logical neighbors in the key tree but also physical (Sun, Trappe, & Liu, 2002).
- **Storage Inefficiency:** In the LKH algorithm, users have to store a set of keys. As the size of group increases, so does the number of keys stored by each user. This results in storage inefficiency of the lightweight mobile devices due to the limitation of storage space.

Figure1. Typical LKH key tree

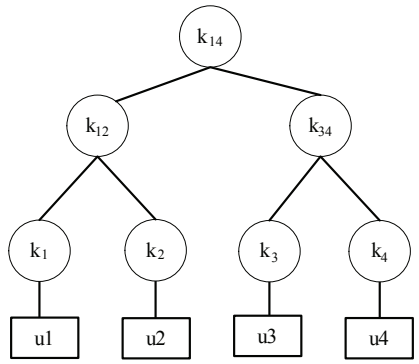
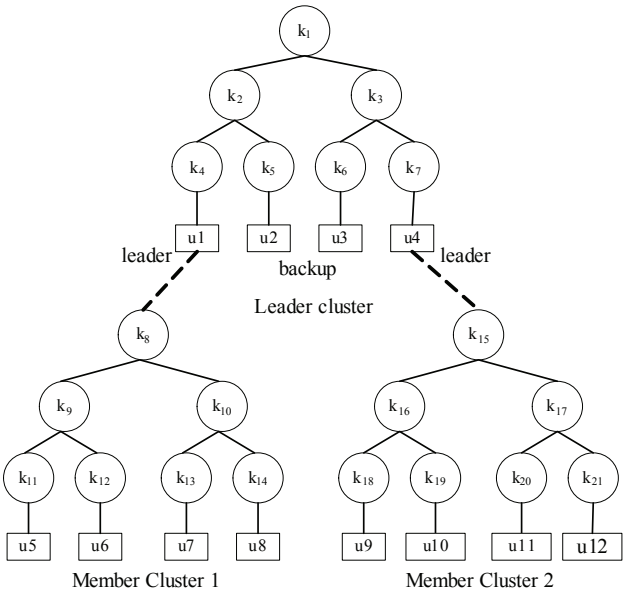


Figure 2. Group key management structure



Group Key Management Algorithm

Group key management algorithm is a 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:

- bs: base station
- BS: a set of the base stations
- {x}k: message x is encrypted by the key k
- A → B {message}: A sends message to B via unicast
- A⇒B {message}: A sends message to B via broadcast or multicast

The Proposed Logical Key Structure

In each cell of wireless network, the base station is responsible for managing the group key. In our proposed work the base station categorizes the authorized members into several clusters to form a two-level key management structure. Figure 2 depicts this logical structure within the cell. The group key management area is divided into smaller areas called clusters. Each cluster has its own cluster key for communication. The members of the leader cluster are assigned as leaders of the lower level member cluster—that is, one leader for one member cluster. The leader is responsible for distributing the rekeying messages to the lower level cluster users, thereby reducing the communication and computation overhead of the key server. The leftover users in the leader cluster serve as leadership backups.

The steps to build our proposed logical key management structure are as follows:

- **Step 1:** The base station groups users into several clusters based on the cluster policy, which defines the size of clusters and the ratio of leaders and backups. One cluster is assigned as the leader cluster, and others are member clusters.
- **Step 2:** Separate key trees are built for each cluster. The members in the leader cluster are assigned as leaders of member clusters—that is, one leader for one member cluster.
- **Step 3:** The base station assigns a local multicast address to each cluster for cluster communications.

The Proposed Group Key Management Algorithm

There are three main operations in the wireless group key management (multiple subgroups): member join, member leaving, and handoff. The rekeying procedures of these operations occur independently in each wireless cell. We illustrate our algorithm in each of these operations in the following subsections.

Member Join

When a user wants to join a group, backward secrecy must be maintained to prevent the new member from accessing the previous group communication details. The join procedure starts with the group join request sent by the user to the group key server (GKS).

u → GKS: {join request}

After authentication, GKS updates the group key and distributes to the base stations.

GKS ⇒ BS: {new group key}

There are two types of join: leader cluster join and member cluster join. The base station assigns the new member into a cluster according to the cluster policy, where leader cluster is given priority over member clusters. When the cluster is decided, the base station invokes the join procedure to rekey the cluster key tree. For example, in Figure 2, if u2 wants to join the group, then the rekeying procedure is invoked at the leader cluster. The base station needs to send the following two messages: