Approximation Algorithms for Key Management in Secure Multicast

Agnes Chan[1], Rajmohan Rajaraman[1], Zhifeng Sun[1], and Feng Zhu[2]

[1] Northeastern University, Boston, MA 02115, USA
[2] Cisco Systems, San Jose, CA, USA

Abstract. Many data dissemination and publish-subscribe systems that guarantee the privacy and authenticity of the participants rely on symmetric key cryptography. An important problem in such a system is to maintain the shared group key as the group membership changes. We consider the problem of determining a key hierarchy that minimizes the average communication cost of an update, given update frequencies of the group members and an edge-weighted undirected graph that captures routing costs. We first present a polynomial-time approximation scheme for minimizing the average number of multicast messages needed for an update. We next show that when routing costs are considered, the problem is NP-hard even when the underlying routing network is a tree network or even when every group member has the same update frequency. Our main result is a polynomial time constant-factor approximation algorithm for the general case where the routing network is an arbitrary weighted graph and group members have nonuniform update frequencies.

1 Introduction

A number of data dissemination and publish-subscribe systems, such as interactive gaming, stock data distribution, and video conferencing, need to guarantee the privacy and authenticity of the participants. Many such systems rely on symmetric key cryptography, whereby all legitimate group members share a common key, henceforth referred to as the *group key*, for group communication. An important problem in such a system is to maintain the shared group key as the group membership changes. The main security requirement is *confidentiality*: only valid users should have access to the multicast data. In particular this means that any user should have access to the data only during the time periods that the user is a member of the group.

There have been several proposals for multicast key distribution for the Internet and ad hoc wireless networks [2,7,8,18,24]. A simple solution proposed in early Internet RFCs is to assign each user a *user key*; when there is a change in the membership, a new group key is selected and separately unicast to each of the users using their respective user keys [8,7]. A major drawback of such a key management scheme is its prohibitively high update cost in scenarios where member updates are frequent.

H.Q. Ngo (Ed.): COCOON 2009, LNCS 5609, pp. 148–157, 2009.

The focus of this paper is on a natural key management approach that uses a hierarchy of auxiliary keys to update the shared group key and maintain the desired security properties. Variations of this approach, commonly referred to as the *Key Graph* or the *Logical Key Hierarchy* scheme, were proposed by several independent groups of researchers [2,4,21,23,24]. The main idea is to have a single group key for data communication, and have a group controller (a special server) distribute auxiliary subgroup keys to the group members according to a key hierarchy. The leaves of the key hierarchy are the group members and every node of the tree (including the leaves) has an associated *auxiliary* key. The key associated with the root is the shared group key. Each member stores auxiliary keys corresponding to all the nodes in the path to the root in the hierarchy. When an update occurs, say at member u, then all the keys along the path from u to the root are rekeyed from the bottom up (that is, new auxiliary keys are selected for every node on the path). If a key at node v is rekeyed, the new key value is multicast to all the members in the subtree rooted at v using the keys associated with the children of v in the hierarchy.[1] It is not hard to see that the above key hierarchy approach, suitably implemented, yields an exponential reduction in the number of multicast messages needed on a member update, as compared to the scheme involving one auxiliary key per user.

The effectiveness of a particular key hierarchy depends on several factors including the organization of the members in the hierarchy, the routing costs in the underlying network that connects the members and the group controller, and the frequency with which individual members join or leave the group. Past research has focused on either the security properties of the key hierarchy scheme [3] or concentrated on minimizing either the total number of auxiliary keys updated or the total number of multicast messages [22], not taking into account the routing costs in the underlying communication network.

1.1 Our Contributions

In this paper, we consider the problem of designing key hierarchies that minimize the average update cost, given an arbitrary underlying routing network and given arbitrary update frequencies of the members, which we refer henceforth to as weights. Let S denote the set of all group members. For each member v, we are given a weight w_v representing the update probability at v (e.g., a join/leave action at v). Let G denote an edge-weighted undirected routing network that connects the group members with a group controller r. The cost of any multicast from r to any subset of S is determined by G. The cost of a given key hierarchy is then given by the weighted average, over the members v, of the sum of the costs of the multicasts performed when an update occurs at v. A formal problem definition is given in Section 2.

[1] We emphasize here that auxiliary keys in the key hierarchy are only used for maintaining the group key. Data communication within the group is conducted using the group key.