LeaSel: A Highly Secure Scalable Multicast Model

ELIJAH BLESSING.R, RHYMEND UTHARIARAJ.V
Ramanujan computing Centre,
Anna University,
Chennai 600025,
INDIA

Abstract: Multicast is an internet service that provides efficient delivery of data from a single source to multiple recipients. The emerging multicast applications like teleconferencing, distributed interactive simulation, online network games, online education etc require secure techniques for group member authentication, group membership control, key generation and distribution and data transfer. And they are controlled and monitored by one or more dedicated controllers. When these controllers are attacked and compromised, the whole of the multicast service is affected and interrupted. In this paper, the security level of different multicast models viz. centralized model, distributed subgroup model, and the recently proposed LeaSel model are examined and analyzed. The mathematical and experimental results show that it is very difficult to break the LeaSel model thereby proving that LeaSel is highly secure when compared to other approaches.

Keywords: Multicasting, Security, Centralized, Distributed Subgroup, LeaSel, Confidentiality.

1 Introduction
Most network applications make use of unicasting technique to deliver packets to the clients. On the other hand, many emerging applications like teleconferencing, distributed interactive simulation, online network games[12] make use of multicasting technique. Instead of sending multiple copies of the data, one per client, multicast allows the sender to send one copy of the data to the group’s address. Thus it reduces sender transmission overhead and proves to be an efficient internet service. In multicast, the data is secured by encrypting it with the group key, which is shared by all the members of the group.

The recently proposed LeaSel model[2] consists of two entities that manage and control the groups and subgroups. They are controller and deputy controller. The deputy controller decides the rank of all the members in the subgroup and maintains a rank list. The member that ranks first will be designated as a leader and will be authorized to perform key generation and distribution. Moreover only the deputy controller knows the leader and it is hidden from all other members of the subgroup.

The computational complexity analysis of multicast models [3] has proved the fact that, LeaSel is an efficient model for scalable secure multicasting[3]. In this paper, the security level of different multicast models viz. centralized model, distributed subgroup model and the recently proposed LeaSel multicast model is analyzed and examined both mathematically and experimentally. The analysis proves that LeaSel model is very difficult to attack and hence hacking the whole multicast service is all the more difficult.

The remainder of the paper is organized as follows. The section 2 presents the multicast objectives and security problems. The section 3 gives a review of secure multicast models. The section 4 introduces the LeaSel multicast model. In section 5, the security aspects of the multicast models is evaluated and analyzed mathematically. The
section 6 discusses the experimental results. Finally section 7 concludes.

2 Multicast objectives and Security problems
With widespread use of the internet, multicast communications should be secured. For communications to be secure, the data is encrypted with the group key. Whenever an authorized member joins the group or leaves the group or expelled from the group, the encryption key should be updated. The reason behind updating the encryption key is two fold: i) to prevent the leaving or expelled group member accessing the future communications. This property is termed as forward confidentiality [4] and ii) to prevent a joining member accessing the past communications. This property is termed as backward confidentiality[4]. Thus when a member joins or leaves the group, a new group key need to be generated and distributed securely[1].

Moreover, the essential components for secure multicast include group membership control, secure key generation, distribution and secure data transfer. In the literature [7],[8],[5],[9],[1],[10],[6],[15],[11],[13] a dedicated controller or few controllers perform these components of secure multicast. The controllers and key generation/distribution unit are a crucial point of failure. The group privacy is dependent on the successful functioning of the group controller and key generation and distribution unit. The entire group will be affected if there is a problem with the controller or key generation and distribution unit. The problem may be caused by mechanical malfunction or a malicious individual that hacks the controller and forces the disruption of the service. When the controller or key generation and distribution unit is not working, the group becomes vulnerable because the keys, which are the base for the group privacy, are not being generated and distributed. Hence the group key generation and distribution unit should be protected and hidden from the members of the group.

3 Review of secure multicast models
Several different available multicast models can be grouped into two main classes viz. centralized approaches and distributed subgroup approaches.

3.1 Centralized approaches
In the centralized approach [1],[6],[8],[5],[9],[10], there is only one entity controlling the whole group. This dedicated central controller does not rely on any auxiliary entity to perform access control and key distribution but with one managing entity the central server is a crucial point of failure.

For example in Group Key Management Protocol (GKMP) [5], the group controller GC creates the group key packet (GKP) that contains a group traffic encryption key (GTEK) and a group key encryption key (GKEK). When there is a security breach at GC, the entire group is affected. The group key management architecture proposed by Dunigan and Cao [8] is similar to GKMP and presents same limitation of GKMP. Walner et al proposed the use of hierarchical binary tree (HBT)[6]. In this approach, there is a group controller that maintains a tree of keys. The nodes of the tree hold KEKs. Here the size of the rekeying message is considerably larger and if there is a problem with GC, this approach fails. The One way function tree [9],[10] proposed by McGrew and Sherman is an improvement to HBT approach. This approach reduces the size of the rekeying message but offers no solution when the group controller fails or being hacked. Finally Wong et al [1] extended the binary tree to k-ary tree but didn’t solve the problem of entire group getting affected if the malicious individual hacks the controller. In all these proposals, the entire group will get affected if there is a security breach or any problem at the controller.
3.2 Distributed subgroup approaches

In the distributed subgroup approach [4],[11],[15], the large group is split into small subgroups. Different dedicated subgroup controllers are used to manage each subgroup minimizing the problem of concentrated work. This approach scales well for large groups but each dedicated controller is vulnerable to attack.

For example in the Iolus framework [4], Suvo Mittra proposes a framework with a hierarchy of Group Security Agents(GSA). The GSA splits the large group into small subgroups. Independent keys are used for each subgroup. The framework affects the data path. Setia et al proposes Kronos[11], in which a new group key is generated after a certain period of time, without considering whether any member has joined, left or been expelled from the group (i.e., independent of group membership change). Kronos compromises the multicast objectives because it generates the new key based on the previous one. If one key is disclosed then it compromises all following keys. Ballardie[15], proposes a scheme to use the trees built by the Core Based Tree (CBT) multicast routing protocol to deliver keys to a multicast group. There is no solution for forward confidentiality. In all these proposals each dedicated controller is vulnerable to attack.

4 LeaSel - An Efficient multicast model

In LeaSel [2], the multicast group is divided into subgroups based on administratively scoped IP multicast. Each subgroup has its own multicast group with its own multicast address. Packets addressed to administratively scoped multicast addresses do not cross those administrative boundaries. LeaSel [2] introduces two entities that manage, control groups and subgroups. They are deputy controller DC, one per subgroup and the controller CR. The Controller and the deputy controllers are special trusted servers. The deputy controller manages each of their subgroups, and the controller manages all deputy controllers. There are three different keys viz. individual member key k, group key GK and subgroup key SK. The group key GK is shared between controller and deputy controller and subgroup key SK is shared between the deputy controller and the members of the subgroup.

The controller distributes the individual member key k to the authorized member through a secure channel. The controller prepares the game group access control list (GACL). Based on the administrative scoped regions, the controller also prepares game subgroup access control list (SACL) and distributes it to the deputy controller. The controller generates group key GK and shares it with deputy controller. When a member desires to join the group, it sends a JOIN message to the deputy controller. The deputy controller first verifies its subgroup access control list to decide whether to approve or deny the request. Assuming the request is approved, it stores this member detail in its database. Likewise many members join different deputy controllers. Each deputy controller collects all the approved details of the members of its subgroup and prepares a rank list. The deputy controller designates the first rank holder as the leader of its subgroup and authorizes it to perform the key generation and distribution operation and triggers KGM application. KGM is a software that generates keys, stores them and communicates to all the members of that subgroup. The leader generates a subgroup key SK that is shared by all its members and distributes it to them encrypting with the individual keys [k₁...kₙ]. Thus in LeaSel there is no dedicated controller that performs key generation and distribution but it is distributed to leaders of the group and it is hidden from all the members of the group. The model has been evaluated [2],[12] for parameters viz. encryption cost, rekey distribution cost, encryption complexity, message distribution complexity [3]. It is found that for every membership event, the processing cost is independent of group size[3], and the computational complexity is
minimum[3], thereby proving that the model is scalable and efficient.

5 Mathematical analysis of security in multicast models

In this section, we mathematically evaluate the security level of the LeaSel multicast model with other models. The analysis is based on the difficulty to break the model by malicious attackers. On an average, if the malicious attacker takes more number of attempts to successfully break the multicast service then the model is said to be highly secure i.e., more difficult to break, better is the model. In this analysis, the approaches [1],[6],[8],[5],[9],[10], that has only one controller to control the whole group is denoted as ‘centralized’ and the approaches [4],[11],[15] which splits the large group into small group and has different subgroup controllers are denoted as ‘Distributed’. The recently proposed approach is denoted as ‘LeaSel’. The mathematical analysis of the model proves that attacking the whole group for our model is very difficult compared to other models and thus proves that LeaSel model is highly secure.

Let \( N \) be the total number of members in the multicast group \( MG \) and \( C \) be the number of subgroups. Let \( n \) be the number of malicious attackers. Let there be at least one attacker in the group and in the subgroups. Every malicious attacker possesses ‘breaking software’ to attack the group. Let \( S \) be the number of ‘breaking software’.

**Definition:**

a) Fully armed malicious attacker: At least one software is capable of breaking the system or the subgroup.
b) Partially armed malicious attacker: No software is capable of breaking the system.

Let \( T_a \) be total number of fully armed malicious attacker in the system and \( T_{a'} \) be the total number of partially armed malicious attacker in the system. Let \( a \) be the number of fully armed malicious attacker in each subgroup and \( a' \) be the number of partially armed malicious attacker in each subgroup. In all the following cases, it is assumed that i) Every malicious attacker are not fully armed with breaking software. ii) Every \( a \) has equal number of breaking software denoted by \( S_a \) and every \( a' \) has equal number of breaking software denoted by \( S_{a'} \).

If the number of attempts to successfully break the service is given by \( B \), then

**Case 1:**
Assumption:
1) \( N \) and \( n \) are equally distributed within subgroups.

Centralized:
\[
1 \leq B \leq \left( S_{a'} \cdot T_{a'} \right) + \left[ T_a \cdot \left( S_a - 1 \right) \right] + 1 \quad (1)
\]
Distributed:
\[
C \leq B \leq C((S_{a'} \cdot a') + (a \cdot (S_a - 1)) + 1) \quad (2)
\]
LeaSel:
\[
C \leq B \leq (S_{a'} \cdot N \cdot a') + (a \cdot S_a \cdot N) - C + 1 \quad (3)
\]

**Case 2:**
Assumption:
1) \( N \) are unequally distributed among subgroups. Let \( N_1, N_2, \ldots, N_C \) are number of members in subgroups \( MSG_1, MSG_2, \ldots, MSG_C \) respectively.
2) \( n \) are equally distributed and \( a, a' \) are equal in all groups.

Centralized:
\[
1 \leq B \leq \left( S_{a'} \cdot T_{a'} \right) + \left[ T_a \cdot \left( S_a - 1 \right) \right] + 1 \quad (4)
\]
Distributed:
\[
C \leq B \leq C((S_{a'} \cdot a') + (a \cdot (S_a - 1)) + 1) \quad (5)
\]
LeaSel:
\[
C \leq B \leq ((S_{a'} \cdot a') \sum N_i + ((S_a - 1) \cdot a) \sum N_i)
\]
\[
+ a (\sum N_i - C) + C \quad \text{for all } i = 1 \text{ to } C \quad (6)
\]

**Case 3:**
Assumption:
1) \( N \) is equally distributed
2) \( n \) is equally distributed but \( a \) is different in each subgroup and \( a' \) is different in each subgroup such that \( a + a' = n \).

Centralized:
\[1 \leq B \leq (S_a \cdot T_a) + [T_a \cdot (S_a - 1)] + 1 \quad (7)\]

Distributed:
\[C \leq B \leq (S_a \cdot \sum a_i^\prime) + (S_a - 1) \sum a_i + C \quad (8)\]

LeaSel:
\[C \leq B \leq (S_a \cdot N/C) \sum a_i^\prime + ((S_a - 1) \cdot N/C) \sum a_i + C \quad (9)\]

\[i=1 \quad i=1\]

Case 4:
Assumption:
1) \( N \) are unequally distributed among subgroups. Let \( N_1, N_2, \ldots, N_C \) are number of members in subgroups MSG\(_1\), MSG\(_2\), \ldots, MSG\(_C\), respectively.
2) \( n \) is equally distributed but \( a \) is different in each subgroup and \( a' \) is different in each subgroup such that \( a + a' = n \).

Centralized:
\[1 \leq B \leq (S_a \cdot T_a) + [T_a \cdot (S_a - 1)] + 1 \quad (10)\]

Distributed:
\[C \leq B \leq (S_a \cdot \sum a_i^\prime) + (S_a - 1) \sum a_i + C \quad (11)\]

LeaSel:
\[C \leq B \leq (S_a \cdot \sum a_i^\prime N_i) + (S_a - 1) \sum a_i N_i \]
\[C \leq B \leq (\sum a_i N_i - \sum a_i) + C \quad (12)\]

The careful examination of the equations prove that in LeaSel model, the maximum number of attempts to break the multicast model depends on the total number of members in the group \( N \), which is not the case in other approaches. Hence LeaSel model is very difficult to attack and therefore highly secure.

6 Experimental Results and Discussion
The test bed has been setup and the secure multicast model is implemented in JAVA.

The group is divided equally into five subgroups and the Deputy Controller controlled each subgroup.

About 10% of the members were manually designated as malicious attackers and the searching and breaking algorithms were loaded. All the malicious attackers try to break the whole multicast service. For different number of members in the group say 1000, 2000, 3000 etc, the experiment is run 10,000 times and the mean number of attempts to successfully break the group is determined for LeaSel as well as for centralized approaches and it is shown in Fig. 1.

![Fig. 1. Mean number of attacks Vs Number of members, with C = 5 and 10 % malicious attackers a) LeaSel b) Centralized approaches.](image)
thereby proving the fact that LeaSel model is highly secure.

7. Conclusion
In this paper, different multicast models including LeaSel multicast model is evaluated and analyzed both mathematically and experimentally. The mathematical equations shows that the maximum number of attempts to break the multicast model depends on the total number of members in the group N. Thus for group with large number of members in the multicast group, the LeaSel model is highly secure. The experimental results also prove this fact. Thus LeaSel model is highly secure.

References: