A Dynamic Layering Scheme of Multicast Key Management

YANG Fan¹, LI Xiao-ping¹, DONG Qing-kuan², LIU Yan-ming²

¹Department of mechanical and electronic engineering, XiDian Univ., Xi’an Shaanxi
²State Key Lab. of Integreted Services Networks; Xidian Univ., China, 710071
fly.f@163.com, {xpli, qkdong, ymliu}@xidian.edu.cn

Abstract

Group key management is a difficult task in implementing large and dynamic secure multicast. In this paper, a new scheme is proposed in the basis of in-depth analysis of the requirements of the secure multicast and group key management. The scheme is based on the multicast group security architecture and multicast security group key management architecture proposed by IETF. This scheme constructs group key based on pairings and distributes the group key using HSAH function polynomial, and manages group key making use of the dynamic layering GCKS. The scheme is better in security, lower in computation cost and communication cost. The analysis comparison proves that the scheme has strong scalability and efficiency.

1. Introduction

Multicast is an efficient paradigm to support group communications. This solves the scalability issues at the sender side and allows better utilization of network resources such as bandwidth and calculated load. However, multicast security problems are hampering the wider use of multicast. The issues include security of data processing, multicast key management and multicast security policies. Group key management mainly includes activities for the establishment and the maintenance of a group key. Since the group members may come and depart dynamically, the protocol should support a scalable group rekey operation for adapting to the changes.

Compared to unicast key management, some particularly problems in multicast key management including forward secrecy, backward secrecy, key independence and collusion freedom. The evaluation standard of a multicast key management scheme [1] includes the security, scalability, computation & communication cost.

There are many schemes about group key management [1–5]. But an appropriate scheme which suitable for large and dynamic secure multicast scheme has been seldom reported. In this paper, we propose a new dynamic layering scheme, which uses Group Security Association (GSA) to complete secure multicast and uses Group Controller and Key Server (GCKS) to complete group key management. This scheme constructs group key using pairings and distributes group key using Hash function and manages group key based on the dynamic layering GCKS. The scheme has strong security, efficiency and scalability.

This paper is organized as follows. Section 2 provides an overview of the work that has been done. Section 3 presents our proposed dynamic layering group key management scheme. Section 4 describes the performance analysis of our approach. follow by the conclusion is Section 5.
2. Related Work

Group key establishment and management method are both sides of the key management. The present schemes on group key management can be divided into three categories: centralized, distributed and contributed, and group key establishment protocols are based on generalizations of Diffie-Hellman key exchange or elliptic curve cryptography (ECC) and bilinear maps [1~5].

The multicast security group key management architecture proposed by IETF in RFC4046 [6], they define GSA and describes the key management protocols that help establish a GSA, and the group owner (GO) or the GCKS may define and enforce group membership, key management, data security, and other policies that may or may not be communicated to the entire membership.

3. Dynamic Layering Scheme

3.1 Dynamic layering scheme

Network Model This scheme uses multicast security (MSEC) group key management architecture proposed by IETF in RFC4046, and based on the following network model:

1) GCKS in this scheme responsible for access control and generation of group key and negotiate SA with multicast source, and it is also used to manage the group members. GCKS is a trusted manage entity who has authentication comes from the upper such as CA.

2) Each member which will come to the group has a unique authentication show that it is a legal member, and this authentication comes from CA.

3) Each group member who has access control by GCKS is secure, that is no information leakage by a legal member.

Dynamic Layering Scheme In our dynamic layering scheme, there may have two types of GCKS, the under actual GCKS and the upper virtual GCKS. The function of upper virtual GCKS is complete by a under actual GCKS, which is selected randomly by both parties of key negotiation. Each under actual GCKS manages a number-limited subgroup. There may or may not has upper virtual GCKS, which is defined by the network status. A balanced binary tree which composed of GCKS should be established according to the current network status under certain condition of the center GCKS exit. The network status is defined according to region or logic multicasts address or the two conditions mentioned above.

![Figure 1. Construct center GCKS](image1)

The upper virtual will exit or not according to the following condition: in a certain range such as in a province or a scale of wireless network or a network segment, there is a center GCKS can be established to manage the total multicast group and all members of the multicast group will have a same logic multicast address such as group ID. Otherwise, there will be no center GCKS.

According to our scheme, if a multicast group has 8 subgroups, on GCKS layer, there will be several possible situations as shown in Figure 1 and Figure 2.

![Figure 2. Partially construct upper GCKS](image2)

3.2 Construct and distribute group key

The construction and distribution may be roughly divided into two steps:

**Step 1:** GCKS construct subgroup key function
When a member is applying for a multicast group, he needs to negotiate with the very GCKS. Each member $M_i$ of the group generates a random integer $m_i \in \mathbb{Z}_q^*$ and forwards it to the GCKS, and the process is protected by registration SA [6]. The GCKS obtains $m_i$, and calculates the Hash function $H(r_s \parallel m_i)$ and constructs a subgroup distribution function $f(x) = (x - H(r_s \parallel m_i)) + k_{\text{group}} \mod q$ among which, $r_s$ is a random integer generates from GCKS. $r_s$ should be used to update the polynomial $f(x)$ when the group key rekeying for some members come or depart the multicast group. At the same time, GCKS multicast $r_s$ and $f(x)$ to all subgroup members, who use the new $r_s$ to calculate a $H(r_s \parallel m_i)$ for achieving a new group key.  

$k_{\text{group}}$ is the group which construct among GCKS layer.  

**Step 2 GCKS layer negotiate and construct group key**  

On GCKS layer, a balanced binary tree may construct based on network status. The construction and distribution of group key can be divided two conditions:

a. If a random GCKSi has no brother node, he can regard himself as his parent node to negotiate with the corresponding brother node. If a node has no brother node and he is a root node, he select a random integer $s_i \in (1, 2, \cdots, q-1)$ and calculates $k_{\text{group}} = H(s_i)$ as the group key.

b. If a random GCKSi has a brother node, he can start the authentication process with the brother node by a certificate which achieves from CA. After the completion of the authentication, the GCKSi selects a $s_i \in (1, 2, \cdots, q-1)$ and calculates the point multiplication $s_i P$. Then, he exchange $s_i P$ with his brother node to calculate a sharing key between them, and the computing paradigm is based on the scheme of [7], that is $k_{ij} = H(e^{s_i} (s_j Q_j, P_{\text{pub}})) e^{s_j} (Q_j, s_i P) = H(e^{s_i} (s_j Q_j, P_{\text{pub}})) e^{s_j} (Q_j, s_i P)$.

4. Analytical Comparison

**Security Analysis** In our scheme, each member needs to achieve an authentication such as CA authentication before he join a group. If he is joining a subgroup, another authentication is needed by GCKS once again to complete the access control of a member. As for the process of the construction and distribution of the group key, the security of our scheme is based on Bilinear Diffie-Hellman (BDH) problem in $\langle G_1, G_2, e^\cdot \rangle$. The difficult of an attacker gaining the group key in this scheme is equal to resolve the discrete logarithm (DL) problem.

**Key Independence** In the first step of our scheme, when a new member comes into the group, GCKS will construct a new polynomial $f(x)$ and a new group key $k'_{\text{group}}$, and he select a new $r_s'$. Obviously, the previous group key function has no information about the new member; therefore the new member can not achieve the previous group key, which is backward secrecy. And the forward secrecy can be deduced in the same way. And our scheme satisfies the key independence because it satisfies forward secrecy and backward secrecy.

**Collusion Freedom** Collusion attack defines that some fraudulent users who have much information about the multicast group by colluding to deduce the group key.
Obviously, in our scheme, the group key has no information of group member that is the information of group member can hardly affect the group key.

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Rounds</th>
<th>Messages Exchanged</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDH.3</td>
<td>$n+1$</td>
<td>$3(n-1)$</td>
</tr>
<tr>
<td>TGDH</td>
<td>$\lceil \log_2 n \rceil$</td>
<td>$n \lceil \log_2 n \rceil$</td>
</tr>
<tr>
<td>CGKA</td>
<td>$O(\log_2 n)$</td>
<td>$4n$</td>
</tr>
<tr>
<td>DLMKM</td>
<td>$\lceil \log_2 (2m+1) \rceil - 1$</td>
<td>$&lt; 2m$</td>
</tr>
</tbody>
</table>

Where, if $k > 10$, $m < n$

Table 2. Computation cost

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Scalar Mult.</th>
<th>Pairings</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDH.3</td>
<td>$5n-6$</td>
<td>-</td>
</tr>
<tr>
<td>TGDH</td>
<td>$n \lceil \log_2 n \rceil$</td>
<td>-</td>
</tr>
<tr>
<td>CGKA</td>
<td>$n$</td>
<td>$3n/2$</td>
</tr>
<tr>
<td>DLMKM</td>
<td>$n$</td>
<td>$&lt;m$</td>
</tr>
</tbody>
</table>

Efficiency analysis and comparison From the thought of our scheme, we can see that it can avoid the under GCKS failure as it limited the number of a subgroup. At the same time, both of the under GCKS can be used as the upper GCKS, which can avoid the single point of failure in maximum. And we can arbitrarily change the multicast scale by changing the number of GCKS. Therefore, this scheme has strong scalability.

As noted above, efficiency generally includes communication & computation cost. Here, we discuss the efficiency of our scheme in the condition of there in a center GCKS in a multicast group. Let $n$ is the number of the group member, the number of each subgroup is not more than $k$, then the number of subgroup is $m = \lceil \frac{n}{k} \rceil$. The number of rounds in this scheme equal to the negotiation number from under GCKS to the upper GCKS, which is equal to the depth of a balanced binary tree whose leaf node number is $m$, that is $\lceil \log_2 (2m+1) \rceil - 1$, and the number of messages exchanged approximately equal to the number of the total node of this tree, that is $2m$, thus the number of pairing computation is $m$. A comparison to other schemes [5] is presented in Tables 1 and 2.

5. Conclusion

We presented a new Dynamic Laying Multicast Key Management (DLMKM) scheme. The scheme constructed and distributed group key based on pairing and Hash function, which solved the multicast security problem. And it has high efficiency and strong scalability though the dynamic layering in GCKS layer. This scheme is quite suitable for a large and dynamic multicast environment.

6. References