A Key Management Scheme for Multicast Based on Layer 2 Control

CAO Zheng[1,2] YIN Pengpeng[1,2] LU Zhengjun[1,3]

(School of Computer Science and Engineering, Southeast University, Nanjing, 210096, China) [1]
(Key Laboratory of Computer Network Technology, Jiangsu Province, Nanjing, 210096, China) [2]
(Key Laboratory of Computer Network and Information Integration, Ministry of Education, Nanjing, 210096, China) [3]

Abstract This paper presents a key management scheme for multicast based on layer 2 control, which includes multicast authentication, secure multicast forwarding tree management, key distribution when users are initialized and periodical key updating. This scheme offers a set of methods for key distribution and updating with MLD snooping mechanism and MLD report filtering on access switches. This method reduces the complexity of the key updating problem when members leave the group by layer 2 control and guarantees the efficiency and security of key management. Compared with other schemes, this scheme performs better on computation cost and communication cost than them and has acceptable storage cost.

Keywords multicast, key management, layer 2 control, secure forwarding tree.

PERFACE

As a group communication model for multi-point transmission and cooperative application, multicast has a broad application prospect on multimedia conference, VOD (Video On Demand), network game and CSCW (Computer Supported Cooperative Work). Multicast senders only need to send data once, and the data will be duplicated and forwarded by network elements, such as routers and switches, to all receivers. Multicast reduces the processing overhead of the senders and the transmission overhead on the network so as to enable efficient large-scale content distribution. Good scalability benefits from the open model which includes: any user can receive the data from any group, and any user can send the data to any group. However, the application of multicast is restricted by security problems. Because of lacking efficient control of multicast senders and receivers, multicast can not guarantee the rights of legal users.

Data encryption transmission is a method to implement secure multicast. Key management for multicast generates, distributes and updates a group key for all group members. As known by all group members, the key is used to encrypt and decrypt the data from the group. Compared with key management for unicast, key management for multicast has some specific problems[1] [2]:

(1) Forward confidentiality. To ensure the members who have left a group can not use the known group key to obtain subsequent data.

(2) Backward confidentiality. To ensure the members who have joined a group can not use the known group key to obtain foregoing data.

Besides, resisting conspiracy attack, the differences among communication entities, scalability, reliability and robustness also should be considered in key management for multicast.

BACKGROUND

There are three main research directions on multicast key management at present:

(1) Centralized control. There is a node, always called root or group controller, to generate, distribute and update the group key for the whole group. Centralized control can be divided into flat form and hierarchical form. Flat centralized control uses a star structure, and the typical representatives are SKDC (Simple Key Distribution Center) and GKMP [3][4] (Group Key Management Protocol). Hierarchical centralized control uses a tree structure or a graph structure, and the typical representatives are LKH[5] (Logical Key Hierarchy) and OFT[6] (One-way Function Tree).

(2) Distributed coordination. All nodes participate in the communication equally, and they use some algorithms, such as Diffie-Hellman, to generate a group key. The typical representatives are TGDH[7] (Tree-based Group Diffie-Hellman) and Cliques[8].

(3) Hierarchical management. All nodes are divided into several subgroups. There is a control node on each subgroup, and all of them compose the first level of key management. All nodes in subgroups compose the second level of key management. Different levels can choose centralized

Project: This paper is supported by National Key Technology R&D Program “New Generation Trusty Internet Security and Service” (2008BAH37B04) and Jiangsu Key Technology R&D Program “The Research and Experiment on Key Technology of Large-scale Multicast on New Generation Internet” (SBE200800789).

Authors: Cao Zheng, male, associate professor, researching on compute network. Yin Pengpeng, male, master, researching on compute network. Lu Zhengjun, male, master, researching on compute network.

control or distributed coordination independently. The typical representatives are Iolus[9] and GDOI[10] (ISAKMP Domain Of Interpretation for Group Key Management).

These research achievements have different characteristics. Most of them exist in the form of schemes, protocols and frameworks, but few of them were implemented and used in applications. Take the security lock technology as an example, it ingeniously packages SKDC and once became a research hotspot, but the weakness of its scalability restricts its practical value and prospect.

DESIGN

This paper presents a complete set of key management scheme based on layer 2 control， which includes multicast authentication, secure multicast forwarding tree management, key distribution when users are initialized and periodical key updating. This scheme takes SIP [11] (Session Initiation Protocol) as the bearer for multicast authentication, and offers a method of ACL on access switches to implement MLD (Multicast Listener Discovery) report filtering so as to enable fine control on switch ports by SNMP[12][13][14] (Simple Network Management Protocol) or Telnet interface. Meanwhile, this scheme also offers a set of methods for key distribution and updating with MLD snooping[15] mechanism and MLD report filtering on access switches to reduce the cost for key updating when members leave the group by a secure multicast forwarding tree on layer 2.

In this scheme, the behavior of traditional “join” means: a user gets the access authority for the groups which he can join by multicast authentication; when a user gets the access authority for some other groups, he needs to restart multicast authentication to get the authority for them. The behavior of traditional “leave” includes: (1) a user loses the access authority for the groups by exiting authentication; (2) a user loses the access authority for some groups in use between passing the authentication and exiting it.

In this scheme, a user communicates with the authentication server to start an authentication process when he wants to use multicast service and quit the authentication when he doesn’t. Then, the authentication server notifies the control server to configure ACL remotely on the access switch which is connecting with the user. ACL implements MLD report filtering, which combines with MLD Snooping mechanism to maintain a secure multicast forwarding tree. When a user passes the authentication, ACL permits MLD report from the user to the groups he can join. When a user quits the authentication, ACL denies MLD report from the user to these groups. Between passing the authentication and exiting it, if the user loses the access authority for some groups, ACL will also be configured to deny MLD report from the user to these groups. When MLD querier sends the specific group query periodically in MLD snooping mechanism, the MLD report from the user to these groups will be filtered by ACL which results in MLD snooping mechanism will remove this user from the port on access switch for these groups, and that also means the user is removed from the secure multicast forwarding trees of these groups. Because of these secure multicast forwarding trees, the user who loses the access authority for some groups will not be able to obtain the data from these groups by sending MLD report. Meanwhile, if the group key is updated by multicast, the user who loses the access authority for the group also will not be able to obtain it. So the cost for key updating problem when members leave is reduced by a method of layer 2 control, which is the most important characteristics of this scheme and different from other traditional key management schemes for multicast.

Secure multicast forwarding trees works on layer 2 by ACL and MLD snooping mechanism on switches. A secure multicast forwarding tree is for a specific group which guarantees the specific needs of forward confidentiality, backward confidentiality and so on. So key management for multicast itself becomes similar to key management for unicast, and key distribution and updating become more efficient than other schemes. When a user passes the authentication and has a usage behavior for a group, he will send a request to the key server which will return the current group key to the user by unicast. Once the membership changes, which can be said some users get or lose the access authority for the group, ACL will be configured remotely on access switch and the key server does not need to send the updated key to all members immediately for forward confidentiality because layer 2 control has done it. Considering the timeliness for group key, the key server only needs to update it periodically by multicast.

The network topology of this scheme can be seen as figure 1. The architecture of this scheme includes the client system, layer 2 switches and MCS (Multicast Control Server). The project runs on CERNET2 which is a pure IPv6 network. And the application will be deployed in Fudan University firstly and then it will be promoted to other universities. In figure 1, “SH” means Shanghai, “NJ” means Nanjing, “FD” means Fudan University, “SEU” means Southeast University and “NJU” means Nanjing University.

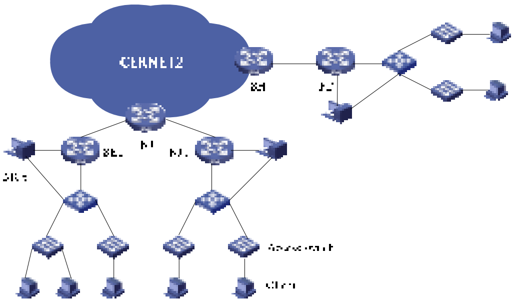

Figure 1. The network topology of this scheme.

Among them, MCS plays a pivotal role:

(1) As a SNMP manager, MCS collects the MAC table on each access switch periodically, locates the specific access switch according to the MAC address which is report by the authenticated user and configures layer 2 ACL remotely on the access switch by SNMP or Telnet interface.

(2) As an authentication server, MCS communicates with the users to provide authentication service.

(3) As a key server, MCS distributes the group key when a user is initialized and updates it periodically.

The access switches, according to the configuration from MCS, permits MLD report from the legal user to the specific group and denies MLD report from the illegal user by ACL, which implements MLD report filtering. Meanwhile, combined with MLD snooping mechanism, all layer 2 switches maintain a dynamic secure multicast forwarding tree for the traffic of layer 2 multicast.

As is shown in figure 2, the working flow is described as follows:

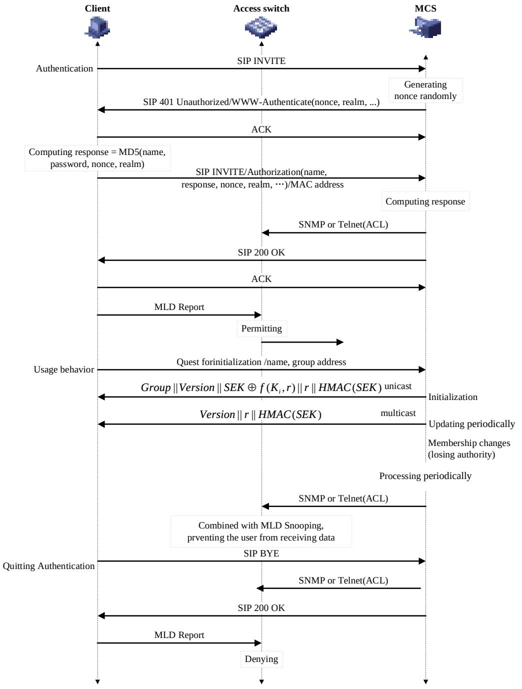
Client
Access switch
MCS
Authentication
SIP INVITE
Generating nonce randomly
SIP 401 Unauthorized/WWW-Authenticate(nonce, realm, ...)
ACK
Computing response = MD5(name, password, nonce, realm)
SIP INVITE/Authorization(name, response, nonce, realm, ⋯)/MAC address
Computing response
SNMP or Telnet(ACL)
SIP 200 OK
ACK
MLD Report
Permitting
Usage behavior
Quest forinitialization /name, group address
$Group \| Version \| SEK \oplus f(K_i, r) \| r \| HMAC(SEK)$ unicast
Initialization
$Version \| r \| HMAC(SEK)$ multicast
Updating periodically
Membership changes (losing authority)
Processing periodically
SNMP or Telnet(ACL)
Combined with MLD Snooping, prventing the user from receiving data
Quitting Authentication
SIP BYE
SNMP or Telnet(ACL)
SIP 200 OK
MLD Report
Denying

Figure 2. The working flow of this scheme.

(1) Default configuration. All access switches is configured default ACL to deny all MLD reports about specific groups in advance. Without passing the authentication, any user can not get the data from these groups by multicast. Each user shares a private key with MCS in advance. All users share a one-way function with MCS.

(2) Multicast authentication. The authentication process takes SIP as the bearer, which is triggered when a user has a demand on a specific group. The user inputs name and password. The client system sends a SIP INVITE message to MCS and starts an authentication process. After receiving the INVITE message, MCS returns 401 Unauthorized message as a challenge, whose WWW-Authenticate title carries the authentication algorithm (MD5), a random number “nonce” based on timestamp, the scope argument “realm” and so on. The client system returns an ACK and computes the response according to name, password, nonce and realm by MD5. Then the client system sends a SIP INVITE message including the response, name, nonce and realm in the Authorization title and the user’s MAC address in the message body. After receiving the INVITE message and confirming the nonce, MCS confirms queries the password according to the name, and then it computes the response by itself. If the computed response is equal to the received one, the user passes the authentication, and MCS sends a SIP 200 OK message to the user. The client system also returns an ACK.

(3) Layer 2 control for a user’s successful authentication. After a user passes the authentication, MCS records the reported MAC address and locates the access switch which is connecting with the user according to the MAC address by querying it in a collected MAC table for all access switches to configure ACL remotely on it by SNMP or Telnet interface. The MLD report from the user to the groups he can join will be permitted. If the MAC address querying fails, MCS will collect the MAC table on each access switch immediately. To reduce the cost of collecting and optimizing the performance, MCS can choose only a part of access switches according to a caching mechanism or the IP address information of the user.

(4) Key distribution. After a user passes the authentication and has a usage behavior for a group, he will send a request for initialization to MCS. MSC sends the current group key to the user by unicast. The message format is as follow:

$Group$	$Version$	$SEK \oplus f(K_i, r)$	r	$HMAC(SEK)$

From left to right, there are the group address, the group key version, the group key information, a random number and the digest of the group key. Among them, the group key information is the result of XOR operation between the group key and the result of one-way function between the user's private key and the random number. The digest algorithm is HMAC. After receiving the message, the user computes the result of one-way function between his private key and the received random number. Then he can recover the group key by XOR operation according to the result and the received group key information. The process is as follow:

$$((SEK \oplus f(K_i, r)) \oplus f(K_i, r) = SEK .$$

If the message is wiretapped by an illegal user, he will not be able to obtain the group key because of lacking the private key.

(5) Key updating. MCS sends the updated group key to all group members by multicast periodically. The message format is as follow:

Version	*r*	*HMAC*(*SEK*)

From left to right, there are the group key version, a random number and the digest of the group key. The updated key is the result of one-way function between the current group key and the random number. After receiving the message, the user can recover the updated group key by one-way function between the current group key and the received random number. The process is as follow:

$$SEK_{new} = f(SEK_{old}, r) .$$

If the message is wiretapped by an illegal user, he will not be able to obtain the group key because of lacking the old group key.

(6) Layer 2 control when a user loses the authority for some groups between passing the authentication and exiting it. Once the user has passed the authentication, the information of access switch which he connects to is already recorded, so MCS will configure ACL remotely on it by SNMP or Telnet interface. The MLD report from the user who loses the authority to these groups will be denied, which combines with MLD snooping mechanism to guarantee the user can not get the data from the group any more. If the user does not start the authentication, he will lose the authority automatically on his next authentication.

(7) Layer 2 control for a use's quitting authentication. When a user quits the authentication, the client system will send a SIP BYE message to MCS. MCS returns a SIP 200 OK message, and configures ACL remotely on the access switch which the user connects to by SNMP or Telnet interface. The MLD report from the user to the groups he can join after authentication will be denied.

IMPLEMENTATION

In our network for experiment, we take one route and two layer 3 switches for routers which run OSPF, OSPFv3 and PIM-SM for connection. Meanwhile, we bring sources to our network by VLAN technology and only bring traffic of specific groups to MCS1 and MCS2 for decryption (using by source key) and encryption (using by group key) by configuring policy route on R1 and R2. The topology can be seen as figure 3.

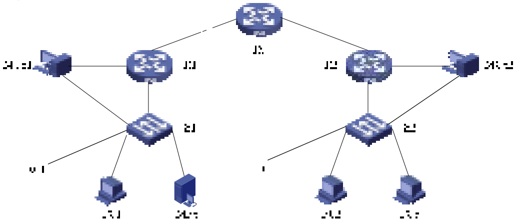

Figure 3. The network topology of experiment.

Figure 4 shows the implementation of project.

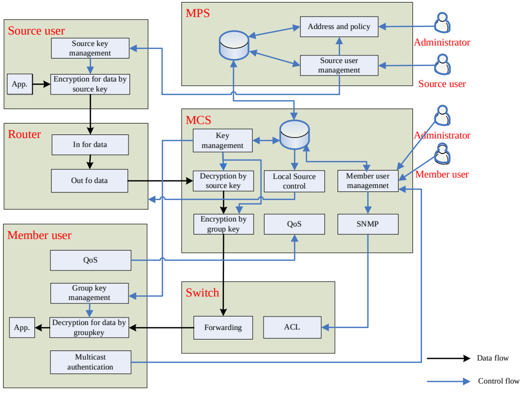

Figure 4. The implementation of project.

We take MCS for example. MCS includes three main modules: multicast authentication, layer 2 control and data forwarding. Figure 5 points the interactions among them.

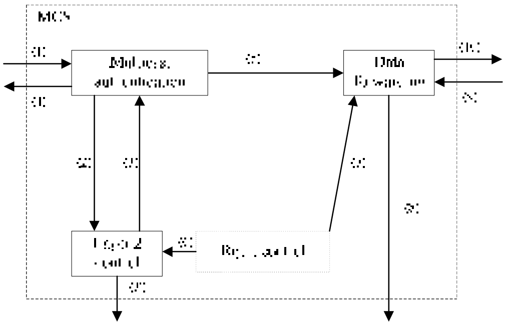

Figure 5. The implementation of MCS

(1) Joining flag, user name, password, user's MAC address.

Leaving flag, user name.

(2) Joining flag, group addresses, user's IP address, user's MAC address, communication identity.

Leaving flag, user name, communication identity.

(3) “OK” string.

(3’) (to access switches) ACL.

(4) Authentication success.

Exiting success.

(5) Joining flag, group addresses.

Leaving flag, group addresses.

(6) User name, group addresses.

(7) Group addresses.

(8) Group data, group key.

(9) User name, group address.

(10) Group key.

Multicast authentication module takes SIP as bearer and offers service to local member users by multithread technology. Layer 2 control module configures ACL on access switches to permit MLD report from legal users to specific groups and deny MLD report from illegal users to specific groups by SNMP or Telnet interface and multithread technology according the notifications from multicast authentication module and right control module. Data forwarding module processes and forwards the data from specific groups and manages group keys according to the result of multicast authentication by multithread technology. Different thread of different modules communicates with others by communication identity based on UNIX domain sockets.

It is worthwhile to mention that this scheme takes NET-SNMP to implement SNMP operation and collects the MIB “dot1dTpFdbTable” on all access switches. The command is as follows:

```
snmpwalk –c njnet –v 2c
udp6:[2001:da8:1001:270::2] .1.3.6.1.2.1.17.7.
1.2.2
```

“2001:da8:1001:270::2” is the address of access switch. And the result is as follows:

```
SNMPv2-SMI::mib-2.17.7.1.2.2.1.2.2.0.7.233.16
.95.141 = INTEGER: 8
SNMPv2-SMI::mib-2.17.7.1.2.2.1.2.2.0.35.137.8
2.102.209 = INTEGER: 1
…
```

The 48 bits before “=” are MAC address, and the number after it is port. The results shows MAC address “0007-e910-5f8d” is from port “8”, and MAC address “0023-8952-66d1” is from port “1”.

ANALYSIS

This scheme builds a secure forwarding tree for each specific group, which meets the forward confidentiality and backward confidentiality by layer 2 control. The change of membership only triggers layer 2 control, instead of key updating in traditional schemes. As a result, when comparing this scheme with other schemes, we take the cost of layer 2 control into account.

When a member joins a group, this scheme needs one ACL configuration message in multicast authentication and one key distribution message by unicast according the quest from the user. It is worthwhile to mention that the MAC querying for locating access switch may fails and MCS needs to collect the MAC table immediately. The number of access switches may be huge and we can limit the range to the port of aggregation switches by querying user’s IP address in a global IP table which is planned in advance.

Take a member’s leaving as an example, the compassion on storage cost, computation cost and communication cost among SKDC, LKH, OFT and this scheme can be seen as table 1. The symbols are explained as table 2.

Table 1. The compassion among different schemes.

	SKDC	LKH	OFT	This scheme
[illegible]	$N+1$	$\frac{dN-1}{d-1}$	$\frac{dN-1}{d-1}$	$N+1$
[illegible]	2	$\log_d N+1$	$\log_d N+1$	2
Computation cost	C_R+C_E	$(C_R+2C_E)\log_d N$	$C_R+(2C_F+C_E$ $+C_{XOR})(\log_d N-1)$	$C_R+C_F+C_{ACL}$
[illegible]	$N-1$	$2\log_d N-1$	$\log_d N+1$	0
[illegible]	$N-1$	$\log_d N$	$\log_d N$	1

Table 2. The symbols interpretation.

N	The member number of the group	d	The tree's degree of LKH and OFT
C_R	The cost of generating a random [illegible]	C_E	The cost of encryption
C_F	The cost of one-way function	C_{XOR}	The cost of XOR operation
C_{ACL}	The cost of ACL operation [illegible]		

(1) Computation cost. Different from other schemes, this scheme takes one-way function instead of encryption to obviously reduce the computation cost. As an experiment on a computer which has dual-core processor with 1.8GHz shows, for a fixed message, the encryption with 3DES takes about 140 us while the digest with SHA_1 taking 30us.

In LKH and OFT, the key server needs to maintain a dynamic key tree for every group and trace the change of membership. However, in this scheme, ACL and MLD snooping maintain a secure forwarding tree in layer 2 which reduce the cost of the key server largely.

(2) Storage cost. In this scheme, the server only stores N+1 keys, and the client only stores 2 keys. Figure 6 shows the change of the storage cost according to different group scale among different schemes when a key takes 16 bytes. Comparing with LKH or OFT based on a binary tree which stores 2N-1 keys in the server and logN+1 keys in the client, this scheme has the optimal storage cost as the same with SKDC.

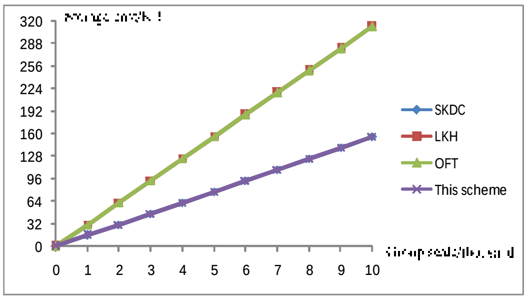

Figure 6. The storage cost according to different group scale among different schemes.

When we take the cost of layer 2 control into account, this scheme needs other storage cost, such as the connection among user name, user's IP address, access switch's IP address and the port, the MAC table, global IP table and so on. However, these spaces only need about 20M bytes and the cost is acceptable.

(3) Communication cost. Figure 7 shows the change of the communication cost (taking the number of messages as a parameter) according to different group scale among different schemes. When a member leaves the group, SKDC has a communication complexity of O (n), and LKH or OFT has a communication complexity of O (log n), but the communication complexity of this scheme is O (1). In this scheme, the server only needs to configure ACL remotely on the access switch once. The user who loses the authority will not be able to get the updated key and the data from the group by multicast.

This scheme takes SNMP or Telnet interface to configure ACL. Telnet needs several interactions because it uses TCP. However, SNMP performs better than Telnet because it has fewer messages than Telnet. At present, this scheme takes h3c-acl.mib in H3C Compatible Style Private MIB for SNMP configuration.

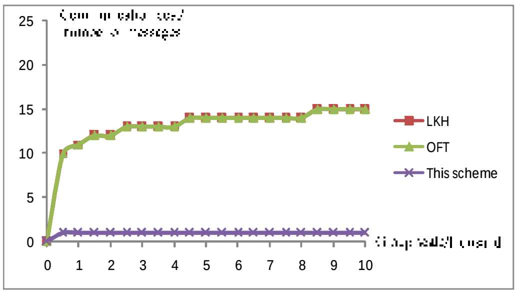

Figure 7. The communication cost according to different group scale among different schemes.

(4) Scalability. The present controllable scheme intercepts MLD report on access switches for multicast authentication which need to be bind with layer 2 access authentication, such as 802.1X. However, we can not bind the access authentication and multicast authentication simply in dynamic environment. This scheme separates multicast authentication from access authentication and does not need to change the implementation of access switches. Meanwhile, ACL, MLD snooping, SNMP and Telnet are supported by most main equipment manufacturers such as Cisco, Juniper and H3C at present. Combined with the optimal computation cost and communication cost and the accptable storage cost, this scheme is easier to be implemented and extended and more suitable for the large-scale secure multicast application than other schemes.

(5) Improvement. The bottleneck of this scheme is the collection of MAC table on access switches when MAC address querying fails for locating specific access switch. We take an experiment for collecting 1, 10, 100, 500 and 1000 access switches' MAC table by order, the time is 2 .857s, 26.600s, 239.792s, 1350.443s and 2820.362s. Once the number is above 100, the time begins to be unacceptable. To improve the performance, this scheme takes three methods: First, taking multithread technology for collecting; Second, limiting the range for collocating by a global IP table which can help us to locate the port of aggregation switches according to user's IP address; Third, taking cache technology to record some possible access switches for each user. By these methods, we can limit the time to 30s and make it acceptable.

CONCLUSION

The application of multicast is restricted by the security problem. Data encryption transmission is a method to implement secure multicast. This paper presents a novel multicast key management scheme based on layer 2 control. Combined with ACL configuration on access switches, this scheme optimizes the computation cost and the communication cost greatly while guaranteeing the specific needs of forward confidentiality and backward confidentiality in key management for multicast.

When a user passes the authentication successfully, ACL will permit MLD report from the user to the groups he can join. After a user exits the authentication, ACL will deny MLD report from the user to these groups. Combined with MLD snooping mechanism, the user who has exited the authentication or lose the authority for some groups will not be able to obtain the key and the data from these groups by multicast because of the secure multicast forwarding tree.

Finally, this paper analyzes the performance of the scheme and the scalability for practical application. The next work is to optimize the cost of ACL operation so as to further improve the performance of this scheme on some large-scale applications, such as live video service on campus network by multicast.

REFERENCES

[1] Xu MW, Dong XH, Xu K. A survey of research on key management for multicast[J]. Journal of Software, 2004, 15(1): 141~150.

[2] Zhu WT, Xiong JP, Li JS, et al. A study of the key distribution in secure multicast[J]. Journal of Software, 2003, 14(12): 2052~2059.

[3] H. Harney, C. Muckenhirn. Group Key Management Protocol (GKMP) specification[R]. RFC2093, 1997.

[4] H. Harney, C. Muckenhirn.. Group Key Management Protocol (GKMP) architecture[R]. RFC2094, 1997.

[5] D. Wallner, E. Harder, R. Agee. Key Management for Multicast: Issues and Architectures[R]. RFC2627, 1999.

[6] D. Balenson, D. McGrew, A. Sherman, Key management for large dynamic groups: one-way function trees and amortized initialization[S]. Draft-balenson-groupkeymgmtoft-00.txt, February 1999.

[7] Lee PPC, Lui JCS, Yau DKY. Distributed collaborative key agreement protocols for dynamic peer groups[J]. In: Proc. of the ICNP. 2002. 53~62.

[8] M. Setiner, G. Taudik, M. Waidnet. Cliques: a new approach to group key agreement[S]. Technical Report, RZ 2984, IBM Research, 1997.

[9] S. Mittra. Iolus: a framework for scalable secure multicasting[J]. Proc. of ACM SIGCOMM, Cannes, France, 1997.

[10] M. Baugher, R. Canetti, L. Dondeti, et al. Multicast Security (MSEC) Group Key Management Architecture[R]. RFC4046, 2005.

[11] J. Rosenberg, H. Schulzrinne, G. Camarillo et al. SIP: Session Initiation Protocol. RFC3261, 2002.

[12] J. Case, M. Fedor, M. Schoffstall, et al. A Simple Network Management Protocol (SNMP).
RFC1157, 1990.

[13] J. Case, K. McCloghrie, M. Rose, et al. Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). RFC1905, 1996.

[14] D. Harrington, R. Presuhn, B. Wijnen. An Architecture for Describing SNMP Management Frameworks. RFC2571, 1999.

[15] M. Christensen, K. Kimball, F. Solensky. Considerations for Internet Group Management Protocol (IGMP)and Multicast Listener Discovery (MLD) Snooping Switches. RFC4541, 2006.