一种新型的组播密钥管理方案

殷鹏鹏[1,2]　曹争[1,2]　陆正军[1,3]

（东南大学计算机科学与工程学院，江苏南京 210096）[1]
（江苏省计算机网络技术重点实验室，江苏南京 210096）[2]
（计算机网络和信息集成教育部重点实验室，江苏南京 210096）[3]

摘　要: 本文提出了一种引入二层设备控制技术辅助组播密钥管理的方案。该方案包括了一套完整的组播密钥管理机制，由组播认证、安全组播转发树的维护、组密钥的分发和更新组成，以二层控制的方式降低了传统的密钥管理方案在组成员离开时的密钥更新操作的复杂度，保障了组密钥分发和更新过程的安全性和高效性，具备了较优越的计算开销、通信开销和可接受的存储开销。

关键词: 组播，密钥管理，二层控制

A Novel Key Management Scheme for Multicast

YIN Peng-Peng[1,2]　CAO Zheng[1,2]　LU Zheng-Jun[1,3]

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

【Key words】 multicast, key management, layer 2 control

1 引言

对组播报文加密传输是实现安全组播的一种方法。组播密钥管理为参与组播的成员生成、分发和更新组密钥。组密钥作为所有组成员都知道的密钥，被用来对组播报文进行加密和解密操作。相比单播的密钥管理，组播密钥管理存在特有的问题[1] [2]，如前向加密、后向加密和同谋破解。

目前，对于组播密钥管理的研究主要集中在三个方向：

（1）集中式控制：存在一个节点负责全组的密钥生成、分发和更新。典型方案是简单密钥分发中心 SKDC、逻辑密钥树 LKH[3]和单向函数树 OFT[4]。

（2）分布式协商：参与通信的节点是对等的，通过某种密钥协商算法生成组密钥。典型方案是 TGDH（Tree-based Group Diffie-Hellman）和 Cliques。

（3）分层式管理：将参与组播的成员进行分组，每个小组存在一个控制节点，这些控制节点组成了密钥管理的层次 I，小组内部的密钥管理属于层次 II。典型方案是 Iolus。

这些研究成果各有优劣，更多的只是以方案、协议或框架的形式存在，很少有在实际应用中付诸实现的。在此基础上对组播密钥管理方法进一步研究和完善很有意义。

2 项目背景

本文提出的组播密钥管理方法是大规模组播控制项目的重要组成部分，包括一套完整的管理方案，由组播认证、安全组播转发树的维护、组成员初始化触发的密钥分发和周期性的密钥更新组成。

基金项目： 本文受国家科技支撑计划项目“新一代可信任互联网安全和网络服务”(2008BAH37B04)，江苏省科技支撑计划项目“新一代互联网大规模组播关键技术的研究与试验”(SBE200800789)资助。

作者简介： 殷鹏鹏(1985-)，男，硕士生，研究方向为计算机网络及应用，安全组播技术；曹争，男，副教授，研究方向为计算机网络体系结构；陆正军，男，硕士生，研究方向为计算机网络及应用。

E-mail： njngypp@gmail.com

项目以会话初始化协议 SIP 为信令，对用户的组播权限进行认证；通过简单网络管理协议 SNMP 或远程登录协议 Telnet 接口对接入交换机进行访问控制列表 ACL 配置，实现了组播侦听者发现协议 MLD 的报文过滤功能，结合交换机的 MLD Snooping 机制，为每个特定的组维护了一棵安全的组播转发树。在此基础上，本方法提出了一套密钥分发和更新机制，实现了组密钥分发和更新过程的安全性和高效性，以二层控制的方式降低了组成员离开时的密钥更新操作的复杂度。

本文提出的组播密钥管理方法采用集中式控制的技术，使用环境如图 1 所示，包括客户端系统、二层交换机和组播控制服务器 MCS。其中，MCS 起多重作用：(1) 作为 SNMP 管理站，定期采集各个接入交换机的 MAC 表，根据用户上报的 MAC 地址定位其所在的接入交换机，利用 SNMP 或 Telnet 接口进行 ACL 的远程配置；(2) 作为认证服务器，与客户端系统交互以验证用户身份；(3) 作为密钥服务器，在组成员初始化和定时器超时情况下进行组密钥的分发和更新。

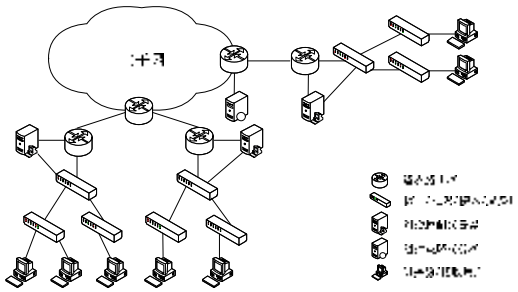

图 1　使用环境图

3 组播密钥管理相关流程

本文提出的组播密钥管理方法的流程包括组播认证流程、安全组播转发树的维护流程、组成员初始化触发的密钥分发流程和周期性的密钥更新流程，如图 2 所示。实际应用中，组成员关系变动中的加入情况对应用户通过认证获得相应组的访问权限；离开情况对应用户退出认证失去相应组的访问权限，以及在通过认证后，退出认证前的使用中，失去其中部分组的访问权限。

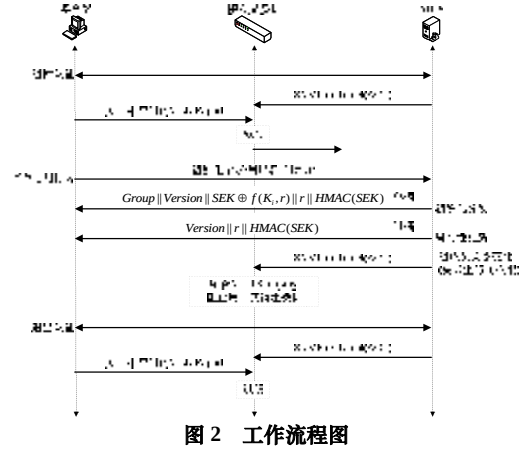

图 2　工作流程图

3.1 组播认证

用户组播认证时，以用户名和密码为输入；MCS 用随机数对用户名的密码信息进行单向函数计算，与用户使用该随机数计算的结果进行对比，若相同，反馈认证通过的消息。

3.2 安全组播转发树的维护

结合接入交换机的 ACL 和所有交换机的 MLD Snooping 机制，本文提出的组播密钥管理方案为每个安全组维护了一棵安全的组播转发树，这棵树工作在二层上，与组播路由协议中的内容分发树属于不同层次，并不对其造成任何影响，旨在保障组播组的数据与组密钥的安全分发，通过流量控制保证只有合法成员才能以组播方式获取数据，彻底杜绝非法流量的产生。

(1) 预先在各接入交换机配置 ACL 过滤关于特定组播地址（段）的 MLD 成员关系报告报文，保证非组播用户无法以组播形式接收特定组播组的数据。

(2) 用户组播认证时上报 MAC 地址，MCS 根据 MAC 地址定位用户所连接的接入交换机，建立关联，并结合用户具备权限的组地址，远程配置 ACL，放行用户关于这些组的 MLD 成员关系报告报文，保证这些组的用户能够以组播形式接收这些组播组的数据；若定位失败，即时发起 MAC 表采集过程，重新进行定位和配置操作。

(3) 用户退出组播认证，MCS 根据用户名和接入交换机的关联找到用户所连接的接入交换机，并结合用户具备权限的组地址，远程配置 ACL，过滤用户关于这些组的 MLD 成员关系报告报文，保证非组播用户无法以组播形式接收这些组播组的数据。

(4) 通过认证后，用户在退出认证前试图获得其它组播组的访问权限时，需要重新进行组播认证，认证通过后可自动获得这些组的访问权限。

(5) 通过认证后，用户在退出认证前，若失去其当前拥有的部分或全部组的访问权限，MCS 相应的接入交换机进行 ACL 配置。这时，由于 MLD Snooping 机制中，MLD 查询器定期向本地网段内的所有主机发送 MLD 普遍组查询报文，以查询该网段有哪些 IPv6 组播组的成员，该非法成员响应的关于该安全组的 MLD 成员关系报告报文会被交换机上的 ACL 过滤，使得 MLD 查询器没有从相应端口收到该成员响应该特定组查询的 MLD 成员关系报告报文，表示该端口下已没有该 IPv6 组播组的成员，则在其老化时间超时后，将其从该安全组所对应转发表项的出端口列表中删除，从而使该非法成员离开了该安全组的组播转发树，无法再以组播方式获得该组的数据。

3.3 初始化密钥分发

(1) 用户在通过组播认证后接收组播数据前，

会向 MCS 发送密钥初始化请求，包括用户名和组地址；MCS 结合用户的身份密钥，向用户以单播方式发送组密钥信息，报文格式如下：

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

从左到右依次是：组地址、组密钥版本号、组密钥密文信息、随机数和组密钥摘要。

（2）用户收到单播报文后，利用身份密钥 K_i 和收到的 r 计算出 $f(K_i, r)$，并通过异或操作还原出 SEK：$((SEK \oplus f(K_i, r)) \oplus f(K_i, r) = SEK$。

3.4 周期性的密钥更新

（1）每隔一段时间，MCS 用一个随机数与当前使用的组密钥一起做单向函数运算，将所得的值作为更新后的组密钥，同时通过该组的安全组播转发树，向所有组成员以组播方式发送这个随机数，报文格式如下：

$Version$	r	$HMAC(SEK)$

从左到右依次是：组密钥版本号、随机数和组密钥摘要。

（2）用户收到组播报文后，利用当前使用的组密钥 SEK_{old} 和收到的随机数计算出更新后的组密钥 SEK_{new}：$SEK_{new} = f(SEK_{old}, r)$。

4 实验与分析

本文提出的组播密钥管理方案为每个安全组形成了一棵安全的组播转发树，利用二层控制解决了前向加密和后向加密问题，组成员关系变动仅仅触发相应的二层控制操作，无需进行密钥更新；同时，方案中周期性的密钥更新也与传统方案不同，并非为了降低服务器的计算开销和密钥更新的通信开销，仅仅是为了保持组密钥的时效性而进行的操作。因此，在与其他方案的开销比较中，本方案将对接入交换机的二层控制开销纳入总开销中。

单个组成员加入组播组（获得该组的访问权限）时，本文提出的组播密钥管理方案需要在用户通过认证后，对该用户所连接的接入交换机远程配置ACL，放行用户关于该组的MLD成员关系报告报文；并在用户通过认证后，退出认证前的使用中，向该成员以单播方式发送该组当前使用的组密钥。值得注意的是，用户认证时可能无法从现有MAC表中查询到其所连接的接入交换机IP地址和端口号，这是需要即时发起利用SNMP采集MAC表的过程，由于接入交换机数量较多，可根据用户的IP地址查询全局IP地址分配表，定位用户IP地址对应的汇聚交换机端口，采集该端口下各接入交换机的MAC表即可，以降低采集的开销，这也是整个组播密钥管理方案的性能瓶颈。

单个组成员退出组播组（失去该组的访问权限）时，本文提出的组播密钥管理方案与同属于集中式控制方式的SKDC、LKH和OFT方案在存储开销、计算开销和通信开销方面的比较如下。

4.1 计算开销

本文提出的方法中，密钥分发和更新采用基于单向函数的摘要算法，代替了传统密钥管理方案中的加密、解密操作，明显降低了密钥服务器和组成员的计算开销。在一台双核 CPU1.8MHz 的 PC 机上的实验表明，对于固定长度的数据内容，用 3DES 进行加密计算需要 140us，而用 SHA_1 进行摘要计算仅需要 30us。

此外，LKH 和 OFT 需要在密钥服务器上为每个组实时维护一棵动态变化的密钥分发树，维护开销较大；本文方法中，由网络设备（接入交换机的 ACL 和各二层交换机的 MLD Snooping 机制）为每个安全组维护了一棵安全的组播转发树，密钥服务器无需关注转发树的维护，计算开销大大降低。

4.2 存储开销

本文提出的方法中，密钥服务器存储组密钥和所有用户的身份密钥，用户端存储组密钥和自己的身份密钥，与 SKDC 方案一样，达到了最小的密钥存储量。以一个密钥占用 16 字节空间为例，本文提出的方法与 SKDC、LKH 和 OFT 在不同组规模下服务端的存储开销如图 3 所示。

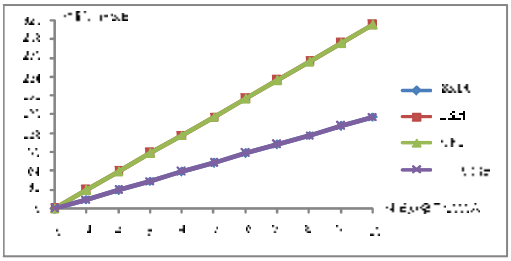

图 3　本文方法与 SKDC、LKH 和 OFT 的存储开销比较

另外，二层控制所需的存储开销包括用户名与用户 IP 地址、接入交换机 IP 地址、端口号的关联，SNMP 采集的 MAC 表和网管提供的 IP 地址分配表等，加上这些开销，本文方法的存储开销会高于其他方案，但由于所需存储空间在 20M 字节左右，且大多以数据库表或文件形式存放在硬盘中，需要常驻内存的并不多，所以本文方法的存储开销在实际应用中是可以接受的。

4.3 通信开销

本文提出的组播密钥管理方案中，对接入交换机的远程配置，如采用 Telnet 接口，由于是基于 TCP 协议的命令行配置，交互流程虽然稳定，但次数较多，开销颇高；若采用 SNMP 接口远程配置，则只需一次命令下发，关于 ACL 的 MIB 库属于私有，但不同厂家都有所涉及，虽然实现方式不同，功能大都能满足，如本文方法目前使用 SNMP 配置的就是 H3C 的 H3C Compatible Style Private MIB 中的 h3c-acl.mib。

本文提出的组播密钥管理方案中，组成员初始化时的密钥分发采用以单播方式，加上使用 SNMP 接口的 ACL 远程配置，即便可能出现需要即时采集 MAC 表的情况，也可采用多种方式对其开销进行优化；同时，相比传统密钥管理方案中组成员离开需进行 次通信，本文方法中，由于接入交换机的 MLD 报文过滤功能和各二层交换机的 MLD Snooping 机制为每个安全组维护了一棵安全的组播转发树，非法用户将无法以组播方式接收这些组的数据和密钥更新报文，组成员关系变动时只需采用 SNMP 接口为该组进行一次 ACL 的远程配置，即可与传统方案对组密钥进行更新一样，实现该组的前向加密和后向加密的需求，通信开销和管理复杂度都明显降低。通过分析，单个组成员离开（失去组的访问权限）时，本文方法与 LKH 和 OFT 方案在不同组规模下的通信开销如图 4 所示。

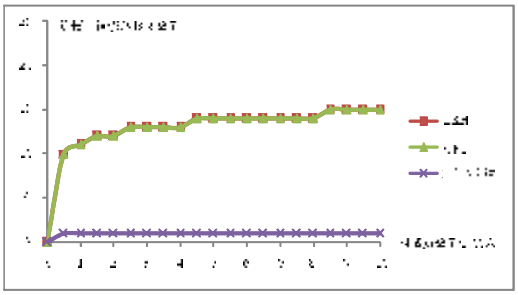

图 4　单个组成员离开（失去组的访问权限）时，本文方法与 LKH、OFT 的通信开销比较

4.4 通用性和扩展性

现有的可控组播方案大多用于类似 IPTV 的视频直播和视频会议中，如华为提出的可控组播方案，就在用户所连接的接入交换机上截获用户的 MLD 成员关系报告报文进行本地或远程组播认证，但这种方法需要对接入交换机的实现进行修改，并依赖于二层接入认证方法（如 802.1X），虽然已经商用，但仍存在一定缺陷。

在用户位置与组播组访问权限的变化相对频繁的环境中，不能简单地将接入认证与组播认证进行绑定，形成紧耦合，本文提出的组播密钥管理方案将组播认证从接入交换机中剥离，通过配置 ACL 对用户的 MLD 成员关系报告报文进行过滤，对接入交换机的实现不做修改，同时，组播认证将独立于接入认证的方式，不同的接入认证方式也不会对组播认证产生影响，具备了通用性。

同时，本文提出的组播密钥管理方案所涉及到的 SNMP 管理、Telnet 接口、ACL 配置和 MLD Snooping 机制均为当前的标准技术，主流厂商如 Cisco、H3C 的设备均支持，易于实现和部署，加密转发模块采用 OpenSSL 源码库，也提供了相应的接口，可以按照实际应用需求，选择不同的加密算法，具备了通用性和扩展性。

5 结论

本文提出的组播密钥管理方法是一种引入二层设备控制技术辅助组播密钥管理的方案，适用于 IPTV[5]、视频直播等典型应用。未来的工作中，结合实际运行情况，对用户接入交换机的定位操作可以在性能上做进一步的优化。

参考文献

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

[4] 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.

[5] 张鹏, 张兴明, 林林 等. IPTV 组播源控制的设计与实现[J]. 计算机工程, 第 35 卷 第 6 期,: 90-93. 2009 年 3 月.