基于 SIP 的组播接入控制

曹争 [1,2]　王剑 [1,2]

（1.东南大学计算机科学与工程系 江苏 南京 210096;
2.江苏省计算机网络技术重点实验室 江苏 南京 210096）

摘 要： 组播业务的实施离不开组播安全，而组播接入控制是组播安全中非常重要的一部分。本文提出了一种使用会话初始化协议（SIP）进行组播接入控制的方法，该方法利用 SIP 协议身份验证机制、S/MIME 加密与签名方法提供了组播用户身份验证、鉴权和安全通信。

关 键 字： 组播，接入控制，SIP

0. 引言

IP 组播可以有效节省网络带宽，在多媒体音频和视频会议应用方面具有得天独厚的优势，因此一经提出就受到广泛重视。经过几十年的发展，出现了多种组播路由选择协议，组管理协议经过了三个版本也日趋成熟。但是，除了一些试验性质的网络，IP 组播技术并没有在 Internet 上得到大量应用。究其原因，IP 组播技术在保持开放性的同时缺少必要的安全控制，用户可以随意地加入组播组和随意地向组播组发送信息，这使得 IP 组播很难在商业应用中有所作为。

因此，必须引入组播安全。组播安全可分为三个部分：1）组播分布树安全；2）端到端数据安全；3）子网内的组成员接入控制[3]。本文关注 3），即子网内的组成员接入控制。相对于主干网而言，子网更容易遭受安全威胁。通常主干网由网络运营商控制，用户基本上无法接入主干网从而危及网络安全；而子网位于网络的边缘，用户可以很容易地访问。在子网内控制用户的访问，将能够极大地提高组播应用的安全水平，同时核心网不必发生任何变化。本文提出了一种使用 SIP 协议来实现 IP 组播接入控制的方法。这种方法具有安全程度高、可扩展性好和易于实现的优点，可以很好地应用于商业组播网络。

1. 组播接入控制的现状

在子网中，主机用 IGMP 协议向组播路由器报告它们的 IP 组播组关系，组播路由器也可以主动发起组播组关系的查询。网络上的任意主机都可以通过发送 IGMP 报文给组播路由器加入组播组，路由器收到 IGMP 的加入组播组报文后，并不验证主机的身份而直接通过加入组播树将组播信息流引向请求主机。路由器也不保存加入组播组的主机信息。这种结构缺乏商业应用所需要的控制和计费特性而阻碍了组播技术的商业部署。

Thomas Hardjono 和 Brad Cain 提出了一种对 IGMP 消息进行验证的方法[3]：主机在发送 IGMP 消息前，必须从授权方获得一个访问令牌（Access-Token），同时授权方将令牌列表（Token-List）发布给组播路由器。这样，通过访问令牌中包含的信息，组播路由器能够验证主机的身份。这种方法的缺点是路由器要付出相当的代价来维护令牌列表。Tony Ballardie 和 Jon Crowcroft[4]提出的方法是使用授权服务器创建和维护组播证书。主机加入组播组前必须向 AS 请求验证，AS 使用保存的组播证书验证主机的合法性，验证通过则 AS 向主机颁发授权标签。然后主机向组播路由器发送附加了授权标签的 IGMP 加入消息，路由器将授权标签转发给 AS 验证，AS 回应路由器允许或拒绝该 IGMP 消息。这种方法的缺点是路由器收到的每个 IGMP 消息都要转发给 AS 验证，效率较低。Ghassan Chaddoud 和 Vijay Varadharajan[7]提出的安全 SSM 组播中的访问控制方法同上述方法类似，通过附加在 IGMP 消息中的鉴权信息并通过层次部署的控制器（Local Controller and Global Control）授权接入。Liu Guangyi、Mao Yanbin 和 Lin Xiaokang[6]提出的接入控制方法通过在网络边缘引入组播服务器（Multicast Service Center）控制用户和组播路由器。Jing Liu 和 Mingtian Zhou[5]提出的接入控制由子群安全控制器（同时也是密钥管理器）授权用户接入。

2. 基于 SIP 的接入控制方法

考虑商业应用对组播接入控制提出的要求，组播接入控制必须：1）可以制定组播接入控制策略；2）验证用户组播组关系，使只有合法用户才能使用组播服务；3）合法用户对组播服务的使用必须符合组播接入控制策略；4）提供必要的统计信息和计费依据。

本文提出了一种基于会话初始化协议（Session Initiation Protocol）的组播接入控制方法，能够很好地完成以上四点要求，对比上节所述的现有控制方法，本方法具有效率较高、交互报文少、对路由器要求较少、易于实现的优点。

2.1 SIP 与 SIP 安全机制概述[1][2][8]

会话初始化协议(SIP)在 RFC3261 中描述。SIP 是一个优秀的信令协议，使用 SIP 可以建立、调整和终止会话。SIP 协议是一种轻量协议，它使用能被终端设备轻易生成并分析的简单文本命令。 SIP 只使用 6 个指令管理呼叫控制信息，简单易行是

作者简介：曹争：硕士，副教授，研究方向是计算机网络体系结构，计算机网络管理等。王剑，男，1976 年生。硕士研究生，研究方向是计算机网络及应用。E-mail：jwang@njnet.edu.cn。

SIP 的一个重要优势。本质上 SIP 提供以下功能：名字翻译和用户定位；特征协商；呼叫参与者控制；呼叫特性改变。SIP 将建立会话和描述一个会话这两个功能分离开来，独立于会话类型和描述会话所使用的方法，这使得 SIP 有很大的适用范围。通过使用 SIP 位置服务器，SIP 可以很好地支持用户移动性。大部分 SIP 应用仅使用了 SIP 的核心协议，对一些有特殊需求的应用，SIP 还可以以一种模块化的方式扩展。SIP 的典型应用包括 IP 电话、移动游戏、在场显示与即时通信、视频与协同等。

作为一种用于 Internet 中的协议，SIP 具备的安全特性使用户能够保护他们的通信。SIP 可以使用基本验证方案和摘要验证方案，由于基本验证方案存在严重的缺陷，在 RFC3261 中已不推荐使用。摘要验证以质询/应答机制为基础，验证用户是否知道一个特定的口令，即事先共享的秘密。这种方法的优点是口令不通过网络传送。SIP 还可以使用 S/MIME 获得 SIP 消息及消息体的安全性，这是通过对消息加密及签名得到的。

2.2 接入控制模型

我们的组播接入控制方法将 IGMP 报文封装在 SIP 消息体中发送给安全控制服务器，使用了 SIP 的会话协商和安全机制。主机从发送 IGMP 消息加入组播组到离开组播组可以视为一个会话，使用 SIP 建立会话支持用户身份验证，并在建立会话的过程中交换加密/解密媒体的密钥。该方法使用基于 HTTP 的摘要验证机制，当要求验证的安全控制服务器收到一个 SIP INVITE 请求时，它向请求端发送一个质询，质询消息包含了 nonce，opaque 等。请求端使用 MD5 算法计算响应：response = MD5(nonce, username, password, realm)，并在下个 INVITE 消息中发给服务器。服务器通过同样的计算，就可验证请求端的身份。RFC3261 给出了一个 UAS 401Unauthorized 消息中 WWW-Authenticate 标题头的例子：

```
WWW-Authenticate: Digest
        realm="biloxi.com",
        qop="auth,auth-int",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

和 UAC 再次发起的 INVITE 消息中 Authorization 标题头的例子：

```
Authorization: Digest username="bob",
        realm="biloxi.com",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        uri="sip:bob@biloxi.com",
        qop=auth,
        nc=00000001,
        cnonce="0a4f113b",
        response="6629fae49393a05397450978507c4ef1",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

SIP HTTP 验证的细节请参考 RFC3261，这里从略。

组播接入控制系统引入组播控制服务器（MCS）完成控制功能，同时，MCS 也是 IGMP 代理。主机向 MCS 发送 SIP INVITE 消息加入组播组，INVITE 的消息体中包含了一个 IGMP 加入组消息。MCS 使用上面所述的 SIP HTTP 摘要验证机制验证主机的身份，若验证通过，则将 IGMP 消息经 IPSec 安全通道转发给路由器；否则，向主机返回 403 Forbidden 消息。除了 MCS，路由器不再从子网上接受 IGMP 消息。

MCS 在本地维护组播组的状态信息，包括活动的组播组以及加入组播组的主机列表。MCS 负责回答组播路由器的 IGMP 查询，当组播组的最后一台主机离开后，MCS 向路由器发送 IGMP 离开消息并删除组播组。MCS 将主机所有的组播活动都存入数据库中，例如用户名、主机地址、加入的组、开始时间、结束时间等，为统计计费提供依据。

系统使用 S/MIME 获得消息体的完整性和保密性。首先发送方使用接收者的公钥对消息体加密，使用 S/MIME 的 application/pkcs7-mime 类型；然后再用自己的私钥对加密后的内容签名，使用 S/MIME 的 multipart/signed 类型。接收方收到消息后，使用对方的公钥验证消息的完整性，然后用自己的私钥解密得到消息的明文。

2.2.1 主机加入与离开组播组过程

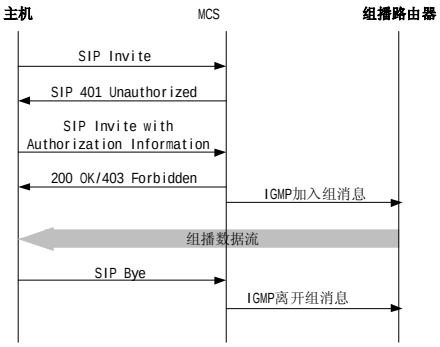

图 1 系统消息流

主机加入和离开组播组的流程如图 1 所示，图中各个步骤的含义如下：

1) 主机加入组播组的第一步是将 IGMP 加入消息放入 SIP INVITE 消息体部分发送给 MCS。MCS 的地址即可以通过手工配置得到，也可以通过 DNS，或者经由 SIP 代理服务器路由。SIP INVITE 消息中包括经加密和签名的 IGMP 消息体，消息的详细格式请参考 RFC3261。

2) MCS 向主机返回 401 Unauthorized 消息，要求对主机身份进行验证。401 消息的 WWW-Authenticate 标题头携带了验证的方法（Digest）和参数，格式见前文。

3) 主机计算 response，放入下一个 INVITE 请求的 Authorization 标题头中发送给 MCS。

4) MCS 用同样的方法计算 MD5 摘要值并与主机返回的值比较，若相同则通过验证。MCS 检查策略库，判断是否接受主机加入组播组；若接受主机，则 MCS 向主机返回 200 OK，这个消息的消息体部分包含了一个用于

解密组播数据的密钥，这个密钥同样使用 S/MIME 机制保证机密性和完整性。否则 MCS 发送 403 Forbidden 消息拒绝主机加入。

5） 通过预建立的 IPSec 安全通道，MCS 将 IGMP 加入消息发送给组播路由器。

6） 组播路由器加入组播树，用 MCS 创建的密钥加密组播数据流并向子网转发。主机用会话建立期间从 MCS 获得的密钥解密组播数据。

7） 主机向 MCS 发送 SIP BYE 消息结束会话，BYE 消息的消息体部分携带加密和签名的 IGMP 离开消息。

8） MCS 向组播路由器发送 IGMP 离开消息，组播路由器停止转发组播流。

2.2.2 MCS 与组播路由器的交互

MCS 充当子网的 IGMP 代理，接收子网上所有主机的 IGMP 消息并通过安全通道转发给路由器，转发方法如下：1) 收到 IGMP 加入组消息，MCS 查询本地数据库，若组已存在，则说明路由器已经开始向子网转发该组的组播数据流了，则不向路由器转发 IGMP 消息。若组不存在，则在本地数据库中添加组关系，并向路由器转发 IGMP 消息。2) 收到 IGMP 离开组消息，MCS 查询本地数据库，若是该组的最后一台主机，则向路由器转发 IGMP 消息并删除本地该组的所有信息；否则 MCS 只把该主机从本地数据库该组中删除，不向路由器转发。3) 收到路由器发出的组成员查询消息，MCS 检索本地数据库并回应路由器。

为了保护组播数据不被非授权的用户和已经离开组的用户访问，需要对子网的组播数据流加密。由于非对称加密算法效率较低，系统采用对称密钥加密算法 3DES。当第一个成员加入组播组时，MCS 随机生成一个加密该组组播数据的密钥。以后加入的成员只需要从 MCS 获得该密钥即可。MCS 同时控制组播密钥的变更，当有成员离开时或一个设定间隔后，重新生成该组的新的密钥并转发给路由器和已经加入组的成员。这种密钥管理方法的特点是组成员关系变化导致的密钥更新被限制在子网内。

2.3 系统实现与性能

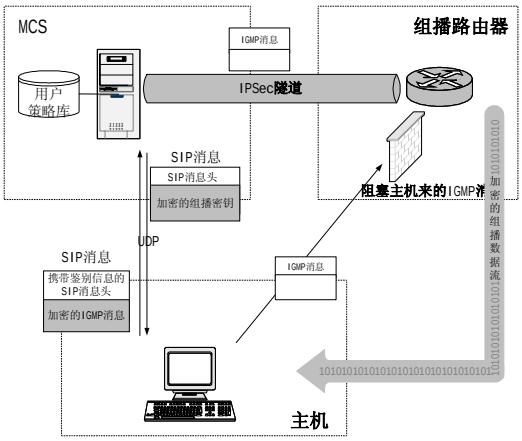

图 2 系统实现框架

2.3.1 主机端与 MCS

主机端和 MCS 需要实现标准的 SIP 客户端，以发起和接收 SIP 请求。GNU oSIP[1]提供了一个构造和解析 SIP 消息的 C 函数库，可用于快速实现 SIP 应用。主机端和 MCS 也需要进行加解密和签名操作，OpenSSL[2]对此提供了很好的支持。SIP 消息可以在 UDP 上传送，由 SIP 应用层保证消息的可靠传输。我们使用 oSIP 和 OpenSSL 开发了原型试验系统，MCS 服务器由一台配备 Intel Pentium 4 2.6G、512M 内存，运行 Redhat Linux 9 的 PC 充当，运行在其他 4 台 Pentium 4 PC 上的客户端模拟程序模拟大量主机加入请求以评测 MCS 的性能。服务器和客户机由 100MB 以太网连接。主机加入组播组与 MCS 之间需要交互 6 条消息，这些消息中最短的 253 个字节，最长 3132 字节，平均 837 字节（不包括 UDP 和 IP 报头长度）。MCS 响应一个主机加入请求的平均时间是 14 毫秒，其中加密与签名操作是其主要开销，完全可以满足一个中型网络的组播接入控制要求。对于大型网络，通过设置分域的多个 MCS 服务器，本系统也能很好的支持。

2.3.2 组播路由器

我们使用一台 Pentium 4 2.6G CPU、512M 内存，配置了 Redhat Linux 9 和 Zebra 路由软件的 PC 充当边界组播路由器。为评测该路由器的性能，我们在其上配置了 OSPF 路由协议、防火墙软件以及 IPSec。在其上测试 3DES 加密的平均速率为 14584KB/s，可以完全充盈 100MB 的以太网。为节约网络带宽，Internet 上的视频流多采用某种压缩编码例如 MPEG-4、H.261 等。对于 352×288、25 帧/s 的无闪烁视频，数据传输速率可以压缩在 64Kbps 之内。即使同时为数百个这样的组播组加密视频流，也不会影响路由器的正常工作。

对于 Internet 上正在运行的路由器，为阻止主机向路由器发送 IGMP 报文，路由器上需配置访问控制列表（ACL）。组播路由器通过 IPSec 接收从 MCS 来的 IGMP 消息和控制信息。另外，路由器需要支持 3DES 加密。现在的路由器处理器速度越来越高，为软件加密提供了条件，但考虑到性能与成本，更好的方案是路由器上添加专用的硬件完成加密运算。现在的接入路由器为了更好地完成防火墙、VPN 等功能，这样的硬件已经得到了广泛配置。因此，为实现本文描述的组播接入控制方法，这些路由器只需要在软件上稍作调整。

2.4 系统扩展性

本接入控制模型在网络边缘完成控制功能，核心网不需做任何修改。主机与 MCS 以及 MCS 与组播路由器之间交换的只是信令信息，这些信息都非常短而且主要在主机加入和离开组播组时发生，因此引入 MCS 增加的网络负担是有限的。在较大型的子网中，MCS 可以通过划分管理域的方法扩展，这样减少了每个 MCS 需要提供服务的范围。

系统在 IPv4 环境下进行了测试，由于 SIP 是应用层协议，

[1] http://www.gnu.org/software/osip/osip.html
[2] http://www.openssl.org

和传输协议无关，因此本系统可以方便地移植到 IPv6 网络环境下。将 SIP 消息体封装的内容改为 MLD（MLD 是 IPv6 下的组播接入控制协议，MLDv2 对应于 IPv4 下的 IGMPv3），由 IPv6 UDP 承载 SIP 报文，MCS 和主机端就可用于 IPv6 环境。IPv6 强制实施 IPSec，为本系统路由器端的实现提供了保证。

3．结束语

本文描述了一种使用 SIP 信令协议完成组播接入控制的方法，通过 SIP HTTP 的摘要验证机制，保证只有合法用户才能接入获得组播服务。从试验系统运行情况看，具有安全性高、运行稳定、扩展性好的优点，并能够轻松地移植到 IPv6 下运行。

参考文献

[1] Gonzalo Camarillo，“SIP 揭密”，人民邮电出版社，2003 年 6 月

[2] J. Rosenberg, H. Schulzrinne, G. Camarill, 等, “SIP: Session Initiation Protocol”, RFC3261, 2002 年 6 月

[3] Thomas Hardjono, Brad Cain, “Key Establishment for IGMP Authentication in IP Multicast”, IEEE ECUMN, CREF, Colmar, France, 2000

[4] A.Ballardie, J.Crowcroft, “Multicast-Specific Security Threads and Countermeasures”, Proc.ISOC Symp.Net.and Distirb.Sys.Sec.San Diego,CA,Feb,1995,pp.2-16

[5] Jing Liu, Mingtian Zhou, “Key Management and Access Control for Large Dynamic Multicast Group”，Proceedings of the 4th IEEE int’l Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS 2002)

[6] Liu Guangyi, Mao Yanbin, Lin Xiaokang，“A Novel Multicast Access Control Model”，IEEE 0-7803-7547-5，2002

[7] Ghassan Chaddoud，Vijay Varadharajan，“Efficient Secure Group Management for SSM”，IEEE 0-7803-8533-0，2004

[8] 张智江,张云勇，刘韵洁，“SIP 协议及其应用”，电子工业出版社，2005 年 1 月

Multicast access control based on SIP

CAO Zheng[1,2], WANG Jian[1,2]

(1.Department of Computer Science and Engineering, Southeast University, Nanjing, 210096, China;

2.Jiangsu Province Key Laboratory of Network Technology, Southeast University, Nanjing, 210096, China)

Abstract: Deployment of multicast service requires multicast security. Access control is one of the most important parts of multicast security. In this paper, we propose a way of access control based on SIP. By the mechanism of authorization and S/MIME supported by SIP, multicast users authenticating, authorizing, and secure communicating are acquired.

Keywords: multicast, access control, SIP