组播服务用户控制机制综述

梅飞　龚俭

东南大学计算机科学与工程系 南京 210096

摘要： 随着组播服务逐步的商业化运行，对其可控制和可管理的要求越来越高。文章对组播服务的开放性所带来的问题进行分类，并详细阐述和讨论了组播服务用户控制机制。

关键字：组播　组播安全　群组控制

Survey of User Control about Multicast Services

Mei Fei　　Gong Jian

Computer Science and Engineering Dep, Southeast University，NanJing，210096

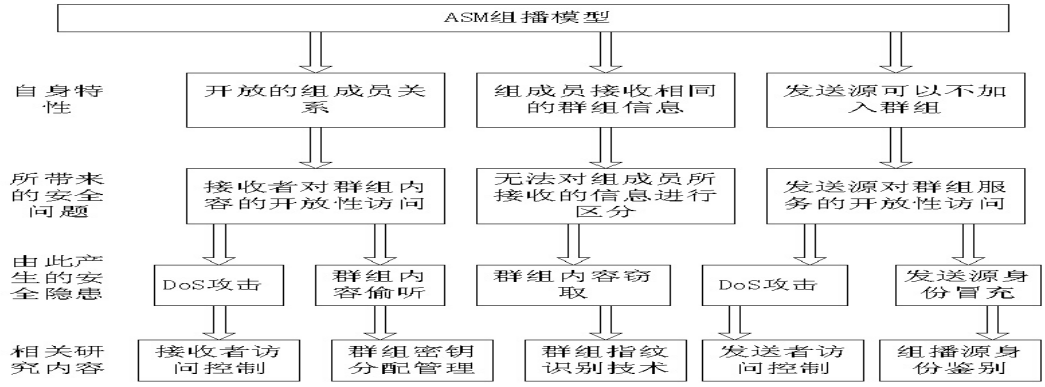
Abstract: With the commercial development of multicast, the demands of controllable about multicast services is a concern. The problems which are brought by the open character of multicast model are classified ,and the solutions of multicast group users control are expatiated and discussed in this paper.

Key words: multicast　multicast security　　multicast control

1．前言

组播技术以其支持大规模的一对多和多对多通信的特点，成为目前网络通信领域研究的热点。大量相关研究工作都集中在组播传输的可靠性、可管理性、扩展性、QoS 和易于部属等方面。然而随着上述研究工作的深入和组播技术在商业化网络中的逐步应用，组播模型固有的特性所带来的安全问题变得越来越突出。组播技术的特性表现在：a）开放的组成员关系，用户可以任意的加入或离开群组，群组所有者无法获得群组成员的信息；b）所有的组成员都能够接收到发往本群组的信息，组成员无法区分组内信息的来源；c）任何群组成员都可以向群组发送信息，甚至支持非群组成员的发送。组播开放性的通信方式带来了很多的安全问题，例如群组内容的窃取、组内信息的伪造、DoS 攻击等等。因此为了使组播应用能够从网络边缘扩展到整个 Internet，确保组播通信安全是首先要解决的问题。关于群组可控制性问题的研究有两个分支：a）通过重新设计组播模型来达到安全和可管理的目的。研究内容包括提出了 SSM 模型（指定源组播）和 Host-End 模型（端系统组播）。前者只允许某一个特定的组播源向群组发送信息；后者采用基于主机的应用层组播，不需要网络设备的支持，既达到了群组通信管理的目的，又可以穿越不支持组播的网络。b）在现有的 ASM 模型（任意源组播）基础上进行群组的可控制性研究。本文讨论的研究内容均基于 ASM 模型（任意组播），不涉及对其他组播模型的讨论。【1】

ASM 组播模型开放性所带来的安全问题和相关的研究成果如下图所示：



梅飞，男，硕士研究生，主要研究方向为网络管理，可控组播；龚俭，教授，博导，CERNET 华东北地区网络中心主任，主要研究方向包括网络安全，网络管理，网络体系结构等。

根据图示，下文将展开进行详细的介绍和论述。

2．组成员关系的开放性

2.1 问题提出

从组播设计的初衷来看，开放的组成员关系确实带来了很大的便利，包括轻量级的用户加入操作、组播源不需要维护所以接收者的信息、以及组成员加入的匿名性等。然而当组播应用到商业化环境中，这种便利就成为了致命的安全隐患。任何网络用户均可以使用 IGMP 协议加入任何群组，从而可以偷听群组内容、窃取组播服务、甚至进行服务失效攻击（这种攻击的破坏性表现在恶意的用户加入大量的群组，从而占用线路的带宽，或者进行频繁的加入/离开群组的操作，加重路由器的负担）。

从目前的研究来看，为了保证群组通信在合法用户（已授权用户）之间进行，有效的方法有两类：a)采用加密技术，对群组内容进行加密。加密/解密技术可以沿袭单播中的成熟技术，但由于群组多点通信的特性，方案的难点在于如何进行高效的密钥分配和密钥更新，因此研究的重点在于***群组密钥管理***；b）***群组接收者访问控制***。由于采用加密技术会增加端系统的计算负担，不适合高速的多媒体组播应用，因此可以考虑对群组接收者进行访问控制。在用户加入群组的同时，进行用户身份检查，允许合法用户的加入，拒绝非法用户的请求，从而保证组成员的合法性。本方案需要群组授权机制和安全组播路由协议的支持。

2.2 群组密钥管理

在单播通信中，发送方和接受方可以通过共享密钥来提供通信信息的保密。而在组播环境中，使用群组密钥对组内信息进行加密，需要将对称密钥分发给群组内的所有成员，并且在组成员关系动态变化的情况下，对群组密钥的管理就变得非常复杂，需要及时更新群组密钥，以保证离开群组的用户不能利用旧密钥解密新的群组信息，同样需要保证新加入的组成员不能利用当前的密钥去解密旧的群组信息。因此，群组密钥管理的核心在于如何设计高效的密钥更新算法。

IETF 制订了一个标准的群组密钥管理体系结构，在此框架下针对不同群组特性和不同组播应用来设计相应的群组密钥管理协议。其中定义，群组密钥管理协议将为组播应用提供一个安全的“组”。一个安全的“组”的成员之间可以安全的交换数据，组外的用户不能访问组内的信息；同时允许合法的组成员更新加密状态。此结构中定义了两个基本组成协议：注册协议和密钥更新协议。前者提供 GCKS （Group Control/Key Server）和正在加入的组成员之间的双向单播交互，进行相互身份认证。在注册协议中，往往也需要包含退出注册协议，退出注册可以使用单向或双向验证机制。后者用来在 GCKS 和群组用户之间传递密钥和各种 SA 信息，其需要保证所有的组成员都能接收到更新密钥；保证组成员及时获得更新密钥信息；当密钥过期和更新信息丢失时，用户联系 GCKS 重新进行同步；避免组成员合作破解密钥，保证信息的可靠性传输。 目前已经设计出的群组密钥管理协议有：MIKEY（Multimedia Internet Keying，服务于运行在 RTP 协议上的实时组播应用的群组密钥管理协议）、GSAKMP(Group Secure Association Key Management Protocol，一个通用的群组密钥管理协议)、GDOI（Group Domain of Interpretation，架构在 ISAKMP 基础上的群组密钥管理协议）。

在目前已有的密钥管理协议中，基本的密钥分配和管理方法有以下几种。

a)手工配置方法：组成员事先获得密钥列表，并按预定的时间周期或按 GCKS 的要求切换到新的密钥。这种方法的优点是简单易实现，但密钥管理开销大，不灵活。如果在线的成员总是合法的，则这种方法可以适应成员动态进入或退出的情形。

b)N 对密钥方法：GCKS 首先询问希望参加会话的成员，并将它们置在一张表内。然后 GCKS 根据表中的成员顺序依次逐节点进行 SA 建立协商，如果协商成功，则与这个成员建立 KEK(Key-Encrypting Key) ；协商不成功则淘汰这个成员。在与第一个成员协商成功后，GCKS 生成公用的 TEK(Traffic-Encrypting Key)，并用该成员的 KEK 加密后送给该成员。然后 GCKS 每协商成功一个成员，就将 TEK 用其 KEK 加密送给它，最终协商完成后形成该组的 KEK 表。当组成员关系变化时或按安全管理的需要，GCKS 进行 TEK 的密钥更新。这种方法也比较简单直观，但密钥管理的信息交换量太大，因此可扩展性不好。

c)补充变量方法：各成员的 KEK 和组的 TEK 的建立方法与 N 对密钥建立方法一样，但同时 GCKS 为每个成员建立一个补充变量。在进行密钥传递时，每个成员收到 N 个值，其中一个是自己的 KEK，另外 N－1 个值是其它成员的补充变量（即每个成员都不知道自己的补充变量）。于是，成员 J 离开该群时，GCKS 通知其它成员切换 TEK，这时新的 TEK 从原 TEK 与成员 J 的补充变量中生成，这可以实现对 J 的后向访问控制。与上一个方法相比，密钥更新信息可以用明文方式由群成员一起帮着传递，交换速度大为加快。这种方法的缺点是每个成员的密钥信息存储量加大；另外更重要的是两个退出的成员通过相互交换信息可以自行生成当前正在使用的 TEK。

d)子群组方法：对于规模较大的群组，往往一个成员的变化（加入或退出），会影响到所有的成员，特别在变化较为频繁的时候，这样密钥更新效率会很低。因此可以使用子群组的方式来消除这个问题。使用具有层次结构的子群组来构成一个安全的群组，这些子群组构成一个安全分发树的结构，每个子群组之间相互独立，这样每个子群组就具有自己的密钥资源，而不再具有全局的密钥资源。这样当一个用户加入或离开时，只会影响到自己所在的子群组，而不会影响整个群组。在这种方式中，将有两个不同的管理实体——GSC（Group Security Controller）和 GSI（Group Security Intermediary），GSC 管理最高层的子群组（根部），而 GSI 管理每个子群组，类似于 GSC 的 proxy 或者父亲 GSI 的 proxy 的功能。GSI 将加入其上一层 GSI 所管理的子群组或者 GSC 所管理的根部子群组，他们在子群组之间起连接的作用，并且中转各个子群组之间的群组信息，从而达到整个群组的通信。

e)分级树方法：这种方法使用一个辅助密钥树来帮助实现 TEK 的更新，在时间和空间上都达到对数级的优化。所有组成员均位于树中的叶节点，GCKS 知道所有的中间节点密钥和叶节点成员的 KEK，而成员只知道自己的 KEK 和到此树根节点沿途路径上的中间节点密钥。当 GCKS 给某个成员分发 KEK 和 TEK 时，将使用通往该成员路径上的中间密钥进行加密，并转发给该成员。如果某个成员从组中退出，则其到根沿途对应的中间节点密钥要修改，并要通知相关成员。这种方法比用各个成员的 KEK 分别加密并分别传送的方法在传输次数和传输时间上要节约很多。如果想进一步减少传输次数，还可以将对每个密钥的修改用一次传输报告给所有有关成员。当然这样做的结果是传输的信息量增加了。分级树方法与组播转发树的结构最为贴近，因此还可以变形为分布式树结构和共享树结构。【2】

2.3 群组接收者访问控制

在目前的组播路由机制中，任何主机均可以使用 IGMP 协议来加入任何群组，并且通知组播路由器向其所在子网转发相关群组的内容。这很容易带来群组内容的偷听和服务的窃取。当然可以使用上文介绍的方法，在发送端加密组播报文，然后将密钥发送给合法用户，这样即使非法用户获取群组内的信息，也不能获得真正的服务。然而即使这样，也不能阻止非法的用户接收组内信息，并进行报文分析和解密工作。同时，会出现 DOS 攻击，恶意的用户会通过加入大量的群组，来非法占用线路带宽和加重组播路由器负担。因此，需要一种机制（例如安全的 IGMP），对主机的群组加入机制进行管理，也就是需要进行群组接收者的访问控制。目前已有研究成果如下：

a）Hardjono and Cain 提出的方法：通过使用密钥来进行 IGMP 的验证和对群组成员的授权。授权服务器提供访问 Token（令牌）给组成员，同时提供类似于路由器 ACL（访问控制列表）的 Token 给路由器。主机发送的请求中包含了访问 Token，路由器根据 ACL Token 进行请求的验证。

b）Ballardie and Crowcroft 提出的方法：首先，主机从授权服务器处获得一个授权标记，将此标记附在 IGMP 请求中发送给路由器，路由器将此请求转发给授权服务器进行验证，根据授权服务器的回应来进行授权。

c)Gothic：这是一个全面的授权机制。该方案中分析认为要完成群组接收者的访问控制功能，需要有以下组成部分的支持：a）群组策略的描述。其中包括某个主机请求描述群组策略、对请求主机的身份鉴别以及群组策略的描述规范。群组策略用来描述主机加入群组的访问权限，群组的所有者被允许描述群组策略。B）访问请求功能。其中包括某个主机通知系统其想成为某个群组的成员。C）访问控制功能。其中包括接收主机的请求、

验证主机的身份、对主机进行授权，授权需要以群组策略的内容为依据。其主要通过两个系统来实现：***群组策略管理系统***和***群组成员授权系统***。前者实现群组策略的描述功能，群组的所有者提供合法用户的名单以及相关的安全策略给 ACS（access control server）,其中 ACS 根据群组的规模，可以为一个单独的 server，也可以是分布式的 server cluster。后者实现主机的访问请求和访问控制功能，设计的目标要减少路由器的计算负担，以及减少主机和路由器的交互信息。【3】

2.4 相关讨论

在组播服务用户控制机制中，对接收者的控制是最急需解决的问题。综合***密钥管理***和***群组成员授权***这两种技术能够达到更好的效果。在主干网络中使用群组成员授权，可以有效的对组播流量进行管理；而在边缘网络，特别是在共享的信道上，组播报文是以广播的方式传输，因此有必要采用加密的方式进行控制。并且在此基础上，组播用户管理和组播计费等相关问题都能够迎刃而解了。

3 群组发送者的任意性

3.1 问题提出

在 ASM 模型中，任何群组成员均可向群组地址发送信息，信息将传送到群组内所有成员，并且网络用户可以在非显式加入群组的情况下，向群组发送信息。这就意味者任何主机均可以影响群组通信，由此带来两个需要解决的问题：a)群组接收者需要验证自己所收到的信息是否为合法的组播源所发送的，因此需要***组播源身份鉴别***；b）需要限制非授权组播源向群组发送信息，因为这会带来服务失效攻击。因此需要***群组发送者访问控制***。

3.2 组播源身份鉴别。

组播源身份鉴别要满足真实性、完整性、不可抵赖性、高效性、抵制同谋、低延迟性、健壮性。目前主要有两大类的方法：***基于散列（hash）***和***基于 MAC（Message Authentication Code）***。

1. 基于散列的方法。采用基于数字签名的方法，每个发送源对其所发送的报文进行数字签名，然而，为了进行大规模群组通信和减轻计算负担的需要，不可能对每个报文都进行签名。由此研究出一系列的方法。
   a) 报文链方法。这是一个高效的流媒体报文的签名方法。只对第一个报文进行数字签名，维护此报文与后续报文的联系。流媒体中的数据包被分割放置在不同的链中，并且每个链中的单个报文都维护着下一个报文在链中的散列值。这样，只需要对链中的第一个报文进行签名即可。当然，这种方式只适用于有限的流，并且预先要知道流中的所有报文。
   b) 树链方法。这种技术将流媒体分割成块，块中的每个报文用树型结构来组织。树中的叶子节点为一个报文的摘要，每个父节点为其两个子节点的摘要，根节点为整个数据块的摘要，并且对其进行签名。接收者根据所接收的数据块，重新构造相同的树型结构，计算每个节点的摘要，最后和经过签名的根节点进行比较。
   c) 针对突发报文丢失的方法。这种技术主要为了保证在突发报文丢失的情况下，鉴别技术的健壮性。其将报文的数字签名复制到流中的多个报文中，并且对流的最后一个报文进行签名，从而达到对突发流量的兼容。
   d) 混和签名方法。这种技术采用基于公钥的数字签名技术。其离线产生 K-time 的密钥对，进行单向的鉴别。信息被在线的私钥加密，然后使用公钥进行验证。
2. 基于 MAC 的方法。这类方法采用 MAC 的方式，从而达到提高效率的目的。
   a) 高效的 MAC 方法。发送者拥有一堆 MAC 密钥，每个群组用户拥有其中的一个子集 MAC 密钥。发送的信息将使用每个密钥进行 MAC，接收者使用其拥有的 MAC 密钥子集来进行验证。选择合适的子集大小可以有效的防止群组用户同谋伪造信息。
   b) TESLA。使用对称加密技术，但是其要求发送者和接收者之间具有松散的时钟同步，从而通过

时间滞后的密钥公布来提供异步的鉴别机制。其大大减轻了计算代价，并且由于密钥链中的密钥支持由后继的密钥计算出来，因此当出现密钥丢失时，接收者可以先缓存报文，等接收到后继的密钥后，解出先前所丢失的密钥，再进行缓存报文的数据鉴别。TESLA 协议可以根据不同的需求，应用在网络层或应用层。【4】

3.3 群组发送者访问控制

由于群组的发送者并不使用 IGMP 协议来加入群组，所以对发送者的访问控制和对接收者的访问控制被分成了两个不同的领域来研究。最近 IETF 的相关讨论的结果还是遵循这样的思想。相关研究成果如下：

1．Crowcroft 在他文章中提出一种检测和阻止非法组播流量传输的模型。模型中要求所有的组播报文中均要包含一个时间标记和一个授权标记。一旦发现了从某个新的组播源发送的组播报文，路由器会将此报文的一个 copy 发送给授权服务器验证，同时要验证授权标记和时间标记。如果验证失败，路由器将会主动向其所在组播树的上游路由器发送 alert 消息，以保证组播树中的所有路由器均阻止此报文的传输。【5】

2．SSM 模型的提出和应用。有人认为，SSM 模型本身固有的组播源和群组地址绑定的机制已经提供了源访问控制。目前 SSM 模型已经得到广泛的认可，并开始商业化运行。【6】

3.4 相关讨论

对于组播源的鉴别，需要根据不同的组播服务和群组特性灵活的选择不同的方法来实现。对于群组发送者访问控制，SSM 模型虽然提供了一定的源访问控制，但是其控制力度还是相当低的，需要一些相关方法的辅助，例如路由器级的防火墙，允许合法的组播源流量进入主干网络，阻断非法组播流量的传输，但是这样的控制方法在以二层设备架构的网络里很难发挥作用。这方面的研究工作目前还在讨论中。

4. 组内信息的不可区分性

4.1 问题提出

加密技术仅仅能保证非合法用户对内容的解读，而不能防止某些用户对所获得信息的复制和传播。而采用***Water-marking***(水印技术)可以防止这种现象的出现。所谓 Water-marking 就是将一些标识信息嵌入到报文中，这些信息不能被接收者所删除，却能够被适当的机构所提取和验证。这些标识信息的内容往往是和接收者相关的，这样一旦发现网络上有未经授权的报文的传输，只需要读取相关标识信息，就可以知道是由那个接收者所传播的。这种和接收者相关的 Water-marking 也叫做 F***inger-printing***。在组播的环境中，传统的 Finger-printing 技术不能应用，因为发送方无法获得所有接收者的信息，并且所有的接收者收到的都是相同的报文。这也就是所谓的组内信息的不可区分性，这样在群组信息被复制和传播时，很难确定到底是由哪个群组成员进行的。所以需要重新考虑组播环境下的 Finger-printing 技术。

4.2 水印技术

根据 Water-marking 作用在不同的位置，可以分为 4 类区分机制。a)基于客户端的 marking。采用某些 client 端的软件对内容进行 marking。b）基于应用层的 marking。在应用层加入逻辑参数来对不同的用户投递不同版本的组内消息。c）基于网络层的 marking。通过网络层的中间设备进行计算来保证对不同的用户投递不同的版本内容。d）基于覆盖的 marking。在组播转发树中采用中间设备来保证对不同的用户投递不同的版本内容。由于水印技术需要较大的计算量，因此需要在效率和安全之间进行权衡。【7】

4.3 相关讨论

水印技术并不是群组用户控制中最迫切需要解决的问题，并且在单播通信中，此技术也没有被广泛的使用。因此关于组播的水印技术理论的探讨比较多，实际的、高效的机制比较少。

5．总结

从目前的研究情况来看，要能够实现商业化的组播服务，需要有一套完善的群组用户控制机制。此控制机制需要根据不同的组播服务和群组特性，灵活的采用不同的方案来支持。

【参考文献】

【1】A.Ballardie and J.Crowcroft, “Multicast-Specific Security Threats and Countermeasures,”, Proc.ISOC Symp.Net and Distib.Sys.Sec.San Diego,CA,Feb.1995,pp.2-16

【2】T.Hardjono,Brian Weis,”The Multicast Security Architecture”,draft-ietf-msec-arch-01.txt

【3】P.Q.Judge and M.H.Ammar,”Gothic:Group Access Control Architecture for Secure Multicast and Anycast”,IEEE INFOCOM,July 2002.

【4】Perrig,Canetti,Whillock,”TESLA:Multicast Source Authentication Transform Specification”, draft-ietf-msec-tesla-spec-00.txt

【5】A.Perrig et aL,”Efficient and Secure Source Authentication for Multicast”,Net and Distrib.Sys.Sec.Symp,Feb,2001

【6】Supratik,Leonard,”An Overview of Source-Specific Multicast(SSM)”,draft-ietf-ssm-overview-05.txt

【7】I.Brown,C,Perkins,and J.Crowcroft,”Watercasting:Distributed Water-marking of Multicast Media”,Networked Group Commun,”99,Pisa,Italy,Nov.1999.pp 286-300