组播通信的访问控制和密钥管理

戴琼海,覃毅力,张 莹
(清华大学自动化系,北京 100084)

摘 要: IP 组播是一种高效的多目标传输机制.随着网络的发展,组播在网络的应用占据着越来越重要的地位,其应用不断扩展,技术日益成熟.目前,组播作为一个崭新的学术研究领域,在组播路由算法、流量控制、可靠传输等方面的研究已有很多成果,而对于组播安全问题的研究特别是组播通信密钥的研究还很不成熟.本文通过研究组播通信安全进行深入的研究,对比各种密钥管理方法,研究了可扩展的密钥管理方法.该密钥管理体系采用分层管理结构,采用子管理中心对各个子域进行管理,不仅可以高效地处理组播组成员动态加入和退出,同时,大大减少了密钥管理中心的负担.使该方法可以应用于大型、动态的组播系统.此外,该方法根据现有的网络和组播系统的要求,提出了控制中心由计算机组进行统一调度管理,避免了单点故障的问题,增加了系统的鲁棒性.

关键词: 组播; 组播安全; 密钥管理; 访问控制
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2002) 12A-2020-04

Access Control and Group Key Management of IP Multicast

DAI Qiong-hai, QIN Yi-li, ZHANG Ying
(*Dept. of Automation, Tsinghua University, Beijing* 100084, *China*)

Abstract: IP multicast is an efficient multi-agent transport protocol. With the development of network, multicast will be more and more important. Applications of multicast will be used in many areas. As a fresh new thriving academic field, the main research is focused on multicast routing, the flow control, the congestion control and reliable multicast. But there are few results referred to multicast security especially to group key management. In this paper, it will submit a scheme of group key management for large dynamic multicast system. This scheme adopts hierarchical architecture, includes a control-center (main key management center: KMC) which is composed of a cluster of computers, and some sub key management center (SKMC) which manages its sub-domain. The scheme can efficiently handle the joining and leaving of group members and avoid one-point failure. It also enhances the robustness of the manage system.

Key words: multicast; multicast security; key management; access control

1 引言

IP 组播是一种高效的多目标传输机制,和单播系统比较,它可以节约占用的带宽,缓解服务器以及网络的负载,同时提高了系统的性能.组播特有的优点使它在网络的应用占居着越来越重要的地位,其应用主要有:网上会议、网上视频广播、白板、远程教育等.目前,IP 组播的研究主要集中在 IP 组播的流量控制、可靠性传输以及安全性的问题上.流量控制和可靠性传输都已经有不少的研究成果.而对于组播安全性的研究,由于 IP 组播系统的特殊性,目前还没有一个统一的解决方法,还需要进行更深入的研究.

组播的安全包括数据的完整性、源验证、访问控制等.数据的保密性和完整性等问题可以采用密码算法诸如对称密码算法、非对称密码算法进行解决.可是,如何授予用户访问控制的权利、解决用户密钥的安全性,这是一个非常重要的问题.根据 Kerckhoff 假设:除了密钥之外,攻击者知道所有有关加密和解密的详细过程.Kerckhoff 假设表明加密算法的安全性完全依赖于密钥.因此,组播安全的核心问题将转化为密钥管理的问题.对动态组播系统而言更是如此,当新成员加入组播组时,需要给新用户分配用户私人密钥以及组播组密钥.而为了保证组播原先的信息的安全性,不允许该新用户可以解读原有的信息,需要更换组播密钥(称为向前安全).一旦有用户退出,为了保证该退出用户都不能解读以后的组播通信信息,也需要更新组播组密钥(向后安全),此外,密钥管理还涉及其他方面的各种问题[1,2].实际的应用中,采用何种密钥管理机制在很大的程度上决定了组播安全协议的设计.

由于组播系统的网络构成比较复杂,用户可能分布在不同的局域网和广域网内,采用不同的网络结构,具有不同的网

收稿日期:2002-08-15;修回日期:2002-08-22
基金项目:国家自然科学基金(No.60172026);清华大学基础研究基金(No.JC2001028)

络特性.对不同的组播系统,其特征和安全性要求也大不相同,本文将根据组播密钥管理机制所需要的基本规则和参数要求,提出设计组播密钥管理系统的原则,从而提出有效的密钥管理方法,并和已有的密钥管理方法进行比较.

2　密钥管理机制的规则和参数要求

目前组播只能采用 UDP 协议对数据进行打包,数据报也只能采用尽力传送模式,可能造成数丢失、延迟、重复或者乱序.在实现组播协议的时候,必须采用可靠的组播协议来处理数据的丢失、重复、损坏和乱序等.

此外,组播所处的环境如同前面讨论的一样,组播用户可能处于不同的地理位置,不同的网络结构,具有不同的网络特性.因此,在构建组播密钥管理系统的时候,需要充分考虑到这些问题.为此,提出了以下设计原则:

(1)系统结构的独立性.由于目前的网络结构不一致,理想的系统结构是不影响原有的网络结构,减少对网络改造的程度.目前并不是所有的路由器、交换器等网络组成都支持 IP 组播,同时现存多种组播路由协议以及其他的组播协议,将来那一种协议会成为组播的主要标准还是个未知数.因此,建立的系统应该独立于所有的协议.

(2)系统的鲁棒性.这从两个方面考虑,首先对密钥管理系统本身而言,系统的设计可以抵抗单点故障等各种系统故障问题.如果采用中央式结构[2-4]就会存在这类问题,而采用分散式结构[5,6],可以避免单点故障问题,但是存在效率等问题.对于整个组播系统而言,一旦系统发生故障,希望密钥管理系统能够很快地从故障中恢复过来,最大限度地恢复到原有的情况,避免对密钥系统进行重新初始化.

(3)升级性要强.密钥管理系统面向范围比较广,应用于各种情况的系统中.即不仅可以处理成员较小的组播系统,还应该可以用于处理成员非常多、分布非常广的组播系统.不仅可以处理动态性比较小或者比较有规律的组播系统(如视频会议)还可以处理成员频繁加入退出的系统(网上视频).

(4)系统的可靠性.组播采用无连接的 UDP 包以尽力而为的方式(best-effort)传输信息,无法保证传递的信息的可靠性,不能有效的检测到信息丢失或者出错的情况.如果在密钥管理系统采用组播方式传输密钥信息,则必须采用相关的可靠性传输协议保证信息的可靠性.此外,也也可以采用单播的方式传输密钥信息,当效率会很低.由此看来,选择何种传输方式,可以根据具体的系统权衡决定.

(5)密钥要尽可能的少.在满足系统的要求的同时,无论是用户还是控制中心,他们掌管的密钥必须尽量少.Kerckhoff 假设表明加密算法的安全性完全依赖于密钥.密钥的增加,同时增大了系统的不安全的因素.

(6)更新密钥时需要发送的更新信息也必须越少越好.需要考虑到两种情况:

(*a*)用户退出时的情况:此时为了保证系统向后的安全性,系统需要更新组密钥.密钥信息的分发可以采用组播或者单播的形式;

(*b*)用户加入时的情况:此时,主要为了保证系统向前安全性.系统不仅需要更新组密钥,还需要给新加入用户发送个人密钥.

(7)效率.更新密钥传送给用户需要多长时间?是否能够有效的传输给需要的用户.用户必须在控制中心采用新的密钥之前取得新的密钥,否则,将无法正常访问组播信息.一旦更新消息丢失,系统是否很快就可以发觉,并进行重传?这些都是构建系统的时候需要考虑到的问题.

通过充分考虑以上的规则与要求,权衡单前的系统要求与环境条件,本文将在分级式密钥管理模式下建立安全可靠的组播系统.

3　安全可靠的组播密钥管理系统的体系结构

3.1　密钥管理的体系结构

密钥管理包括密钥的初始化,密钥更新等.目前存在的密钥管理模式主要有三种形式:中央结构类型,分级结构类型,其他结构类型.根据各种密钥管理方法的优缺点,结合实际系统(考虑系统的大小,成员的动态性,系统存在期、系统所处的环境,期望达到的安全目标等等),充分利用到网络本身的结构,并考虑到上一节提到的要求,本设计将采用分级式管理模式.这样既可以保证集中管理模式的快速、安全的优点,同时可以利用分级的体系结构,避免集中式中的单点障碍问题,减少用户变更带来的影响.

系统的密钥安全管理与数据传输分离,如图 1 所示,虚线部分表示密钥管理系统的主干,实线表示组播系统.采用这样的方式,充分避免对组播系统进行更改,同时可以容易地将该密钥管理系统应用到一般的组播系统.

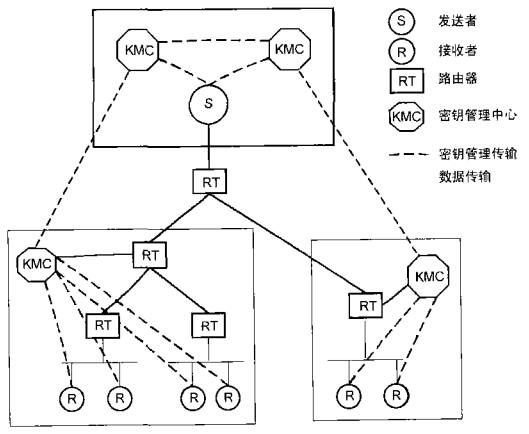

图 1　组播密钥管理系统框架

具体的密钥管理系统采用分级管理结构,如图 2 所示,整个系统呈星形结构,其中各个星形分支又以树型为管理结构.为了便于描述,将各个分支树统一规定为 2 元树图,如图 2 所示.顶级域(域 0)为主要管理域,由 M 个密钥管理中心(KMC)组成,他们相互认证,共同协作,对下级子域中的子密钥管理中心和用户进行身份验证,产生组密钥,给用户授权.N 个子域,每个子域逻辑上可以看作一个密钥分配树,密钥分配树的叶子节点代表授权用户,每个节点代表一个节点密钥.定义为各个子树的高,为各个子树的叶子节点(即用户数),则总的用

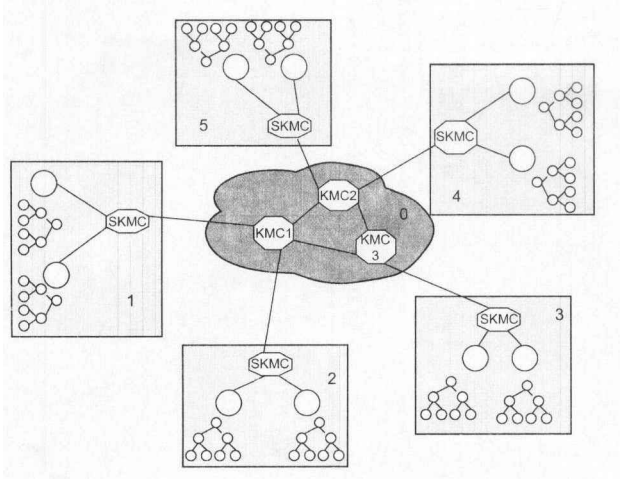

图 2 组播密钥管理系统

户数为 $n=\sum_{i=1}^{N} n_i$，其中 $i=1,2,\cdots\cdots,N$.

3.2 组播用户加入机制

一旦用户申请加入，组播系统希望能对原有的通信信息进行保密，防止新的组播用户加入组播后可以获得原有的信息，即保证系统向后安全.因此需要更新组播组密钥.由于目前单播通信的安全机制比较完善，因此在对组播用户加入的过程中采用了部分单播技术，使得该过程不仅安全而且比较简单.如身份验证、授权、以及为新加入的用户提供密钥都可以采用单播技术实现.

- 用户 μ_A 通过安全通道将申请信息 MSG_A 发送到组播组管理域 0 内.
- 域 0 的管理中心根据各个管理中心的负载情况以及系统的能力，确定由 KMC1 处理该 u_A 信息，进行 u_A 进行身份验证.如果 μ_A 的身份符合要求，KMC1 将根据系统和用户的情况决定将用户加入哪一个子域中：若 $h_i<h_j, i,j=1,2,\cdots,N, j\neq j$，则将 u_A 加入子域中.KMC1 产生组通信密钥 GK' 以及域 i 的子管理中心密钥 $SKMC'_i$，将其通过 SKMC 加密后发送给 $SKMC_i$.
- $SKMC_i$ 更新从 u_A 到根节点路径上的节点密钥树.此后通过安全通道将 u_A 的私人密钥和新的组密钥以及其父节点密钥传送给 u_A.
- KMC1 通过 GK 对 GK' 进行加密，组播给其他的子域.

此过程中需要加密的密钥数为 H_i+1. u_A 的加入只影响将要加入的子域，对其他域内的组播用户影响非常小，由于采用分级分域的结构，系统处理的效率比较高.

3.3 组播用户退出机制

一旦用户退出系统，必须进行调整，使退出的用户无法用原有的密钥访问组播信息，保证组播系统向后的安全性.如果不对退出的组播用户的情况进行处理的话，组播用户的退出会极大的影响组播系统的安全性，使得组播系统泄密，可能是致命的.因此，一旦有用户退出，必须更新组密钥，删除用户的私人密钥.相对于密钥分配树来说，应该删除相应的叶子节点，并更新由它到根节点路径上所有的节点密钥.由于不能采用原有的组密钥对新的密钥进行加密，所以更新的方法与用户加入时的情况有所区别.

- 用户 u_4 通过向域 0 内的 KMC 申请退出组播组（或者 KMC 查到用户 u_4 已经离开了组播组）.
- 域 0 的管理中心根据 u_4 所在的域的情况，产生新的组密钥 GK' 和 GK'_{SKMCi}.用各个子域的 GK'_{SKMCj}，$i=j$ 对 GK' 进行加密，然后组播.
- 用域 i 的 SKMC 私钥对 GK' 和 GK'_{SKMCi} 进行加密，传送给 SKMCi.SKMCi 更新域 i 的密钥分配树.

用户退出组播的情况可以有几种情况.最常见的情况就是用户自动退出.其次是用户的使用期限到期，或者系统强制用户退出.此外，还有用户意外断线等.为了防止用户退出后恶意获取组播组的信息，同时也为了保证意外吊线的用户可以再次安全登陆系统，需要增加必要的附加措施.

检测用户退出的情况，可以采取两种方法.一种可以是主动方式，KMC 周期性地向组播用户发送在线查询消息.如果在一定的期限内 KMC 没有收到组播用户的响应信息，则认为该用户已经退出，从而进行相应的用户退出操作，如密钥更新等.另外一种情况则是被动方式.KMC 采用网络监听的技术对在线用户进行在线测试.

主动的检测用户退出的方式，可以比较好的了解用户在线、退出的情况.但是必须在频繁的用户在线查询和信息安全程度之间进行平衡.为了确保比较快的了解用户退出的情况，就必须加快发出用户在线查询信息的频率，这样也就会加大用户的处理负担.被动检测用户退出的方式，可能会出现用户退出后发送的退出信息无法传送到 KMC，或者用户采用一些特殊的技术将退出信息屏蔽掉，KMC 无法知道用户已经退出，因而不作相应的密钥更新操作.这就会使得组播的安全受到严重的威胁.

为此，可以将两种方法结合起来，共同处理用户退出的情况.一般的情况下，采用被动检测的方法：一旦用户希望退出系统，客户程序向域服务器发出退出申请，域服务器通过接收客户程序发送过来的退出申请，从而确定用户的退出.此外，在被动检测的基础上加上主动检测的方式，以减少由于网络拥塞会造成数据包丢失，从而域服务器无法及时处理用户退出请求，严重影响系统安全性的这类情况的发生.为了避免采用主动检测的方式增大系统和网络的负担，可以将主动检测的方式的查询周期增大.

3.4 密钥更新的周期讨论

用户退出和加入时需要更新密钥.此外，为了维护系统的安全性，还需要周期性地更新组播密钥，以保证在该周期内数据加密没有被攻破.更新密钥的频率可以根据系统的安全级别要求来确定，安全级别越高，更新的频率就越快.用户退出、加入的频率也影响密钥更新的频率.

此外，如果在某个时间段内用户频繁加入退出，系统如果马上响应密钥更新的话，需要频繁的进行操作，不仅增加了系统的负担，同时也加大了系统的危险系数，给用户带来很大的困惑和不便.假设平均用户变更的周期为 T_{re}，密钥管理中心 KMC 产生密钥的时间以及密钥传输以及延迟的时间为 T_g.如果 $T_{re}<T_g$，说明用户还没有收到新的密钥时 KMC 又开始更

新该密钥了.用户无法正常的接收加密的数据.

设系统的更新密钥周期为 T,其中 $T > T_g$ 且 $T > T_{re}$.在每个 T 周期内,对整个系统进行全部的密钥更新.此外在系统密钥更新周期内,如果存在用户变更,如果 $T_{re} < T_g$,则设 $T_{re} = T_g$,进行密钥更新,并进行重新计时.这样不仅保证了系统整体的安全性,同时也考虑到用户加入的效率.

4 方法的评估总结

该方法采用了分级密钥管理系统,充分考虑到了系统安全性和升级性方面的要求,可以比较好地解决系统的动态性带来的安全隐患.当用户加入时,只影响分组播组内的小部分用户,其他的组播用户无需因为有新用户的加入而受到任何的影响.对于用户退出的情况,只需要在用户退出的小组内部进行单一的传送,在其它组播组内部可以采用组播的形式将新的组播组密钥进行发送.同时该方法还支持多个成员同时加入或者退出的情况,不仅简化用户加入的过程,同时还减轻了系统的负担.表 1 是该方法和各种密钥分配方法比较的结果:

表 1　密钥分配方法的比较

	Our's	WGL[7]	GKMP[3]	IOLUS[8]
可扩展性	Y	Y	N	Y
用户的密钥数	$\log_2 n_i + 1$	$\log_2 \sum_{i=1}^{m} n_i + 1$	2	3
SKMC 的密钥数	$2n_i$	—	—	—
KMC 的密钥数	$1 + 2m$	$2\sum_{i=1}^{m} n_i - 1$	$n + 1$	4
用户加入时需要处理的信息数	$\log_2 n_i + 1$	$\log_2 \sum_{i=1}^{m} n_i + 1$	$O(n)$	$O(1)$
用户退出时需要处理的信息数	$\log_2 n_i + m$	$\log_2 \sum_{i=1}^{m} n_i + 1$	$O(n)$	$O(1)$
单点故障	无	有	有	无

该方法避免了单点故障给系统带来的危害.如果某个 KMC 出现问题,其他的 KMC 不仅起到数据备份的功能,还可以将该 KMC 的工作承接过去,不足以影响整个系统的运行.

在该方法中,还对密钥更新的周期进行了详细的研究.

参考文献:

[1] T Hardjono, B Cain, N Doraswamy. A Framework for Group Key Management for Multicast Security [DB/OL]. http://www.dante.net/mbone/refs/draft-ietf-ipsec-gkmframework-03.txt, August 1999.

[2] RFC 2627, Key Management for Multicast: Issues and Architectures [S].

[3] RFC 2094, Group Key Management Protocol (GKMP) Architecture [S].

[4] RFC 2093, Group Key Management Protocol (GKMP) Specification [S].

[5] D Balenson, D Mcgrew, A Sherman. Key management for large dynamic groups: one-way function trees and amortized initialization [DB/OL]. http://www.dante.net/mbone/refs/draft-irtf-smug-groupkeymgmt-oft-00.txt. February 1999.

[6] RFC 1949, Scalable Multicast Key Distribution [S].

[7] Wong C K, Gouda M, Lam S S. Secure group communication using key graphs [J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16 - 30.

[8] Mittra, S Iolus. A Framework for scalable secure multicast [J]. ACM Computer Communication, 1997, 27(3): 277 - 288.

作者简介:

戴琼海　男,1964 年 12 月出生于上海.现为清华大学多媒体中心常务主任,深圳研究生院宽带多媒体中心主任,清华大学数字媒体实验室主任.主要研究领域为宽带信息网络、信号处理、信息编码和网格等.主持国家"九五"、"十五"课题多项.国家自然科学基金多项,包括 ATM 网络的流量控制、IP 网络 QoS 的研究和网络控制、视频编码和网络的复杂建模等.目前承担复杂媒体网络、IP 网络研究的研究工作.

覃毅力　女,1975 年 10 月出生于广西壮族自治区.1994 年 9 月至 1999 年 7 月,就读于清华大学自动化系,获自动化专业工学学士学位;1999 年 9 月至 2002 年 7 月,就读于清华大学,获工学硕士学位.主要研究组播安全方面的内容.