一个组播分布式访问控制系统

刘民岷[1]，刘 璟[2]

(1. 电子科技大学机械电子工程学院 成都 610054; 2. 电子科技大学计算机科学与工程学院 成都 610054)

【摘要】鉴于简单公钥基础设施技术在授权方面所具备的优点，提出了基于简单公钥基础设施技术的组播分布式访问控制系统，设计了组播分布式访问控制系统鉴别和授权协议，并进行了模拟仿真实验及性能评价。与其他方案相比，组播分布式访问控制系统具备分布式、支持非对称组播、授权委托和隐私保护、边缘路由器计算开销小等特性。

关 键 词 Internet组管理协议; 组播; 分布式访问控制; 简单公钥基础设施

中图分类号 TP309.7 文献标识码 A

A Multicast Distributed Access Control System

LIU Min-min[1]，LIU Jing[2]

(1. School of Electromechanical Engineering, UEST of China Chengdu 610054

2. School of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract As SPKI technology has advantage on the aspect of authorization, this paper presents an access control system for large multicast system named MDAC based on SPKI and MDAC authentication and authorization protocol was also designed. Experiment of simulation and performance evaluation was also done. Compared with other solutions, MDAC has not only excellent performance, but also characteristics of distribution, supporting asymmetrical multicast, delegation and privacy protection, less computing cost in border router.

Key words internet group management protocol; multicast; distributed access control; simple publickey infrastructure

从发送者和接收者两个方面考虑，目前的组管理协议(Internet Group Management Protocol, IGMP)都可能遭受到攻击，解决这类攻击问题的关键是必须提供一种机制使得边缘路由器可以对组播用户(发送者和接收者)实现鉴别和授权，这就是IP组播的访问控制问题。目前涉及组播访问控制领域的研究成果相当少，大量的工作主要集中在端到端的数据保护上。现有方案存在的共同问题是：1) 没有实现真正意义上的分布式访问控制，仅仅提出将多个授权服务器分散于网络的各个域中，各个授权服务器之间是相对独立的。2) 不能支持非对称组播或对称组播。3) 不能实现访问控制中(尤其是在电子商务应用中)的隐私性。4) 不能实现授权委托。本论文试图在简单公钥基础设施的基础上，构造一个分布式访问控制系统，以在组播访问控制领域做一些有益的探索。

1 SPKI技术简介

简单公钥基础设施(Simple Public Key Infrastructure，SPKI)的提出是为了克服基于X.509标准的PKIX系统

收稿日期：2005 – 03 – 31

作者简介：刘民岷(1973 –)，男，在职博士生，主要从事网格计算、网络安全以及虚拟仪器技术方面的研究.

过于复杂以及在证书授权方面的局限，其主要目的是提供对行为的授权而不是对身份的鉴别。SPKI证书又称委托证书，其主要作用是授予和传递许可权。委托证书将授权与实体公钥直接绑定，使得SPKI证书独立于命名机制，使用上更加自由。SPKI委托证书可以用于分布式应用的委托和授权控制，进而实现面向公钥的分布式访问控制系统。

2　系统框架

基于SPKI的组播分布式访问控制系统(Multicast Distributed Access Control，MDAC)系统框架如图1所示。该系统基于文献[1]的GKM协议的基础设施。在利用单点组播(一点到多点)路由算法建立单点组播组后，当同一组播组内部的接收者希望向组内发送组播数据时，该接收者需要和发送源点建立安全单播连接并将数据发送给该发送源点；发送源点(相当于转发代理)再将数据通过组播方式转发给全组。由于该模式混合使用了组播和单播模式，故称为非对称组播。

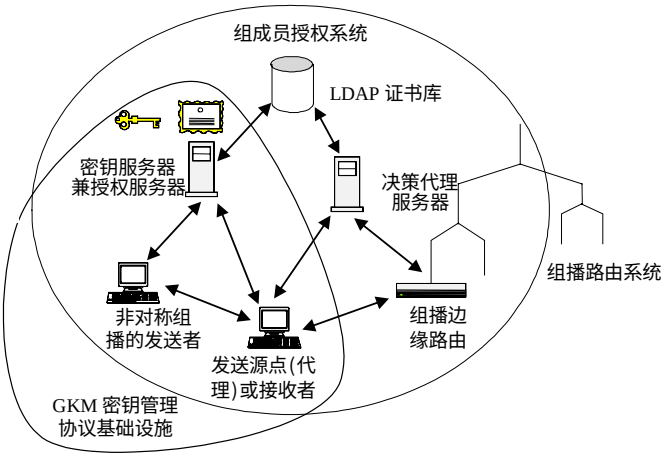

图1　MDAC系统框架

现存的其他组播访问控制解决方案均只考虑了单点到多点的单点组播通信方式，没有考虑组播接收者需要发送组播数据的情况。MDAC基于文献[1]密钥管理协议基础设施，将组播通信分为两类：第一类是发送源点到端用户的组播数据通信；第二类是密钥管理协议基础设施中的组安全控制器(Group Security Controller，GSC)到子组安全控制器(Sub-Group Security Controller，SGSC)，以及SGSC到端用户之间的密钥管理信息通信。

对SPKI证书的授权域作出如下规定：授权域分为多个授权子域，每个授权子域规定了对于给定的组播地址证书主体被授予的两个操作权限：1) 向该组播地址发送组播数据；2) 从该组播地址接收组播数据。

MDAC系统的鉴别和授权流程为：接收者、非对称组播的发送者或发送源点向组密钥服务器申请SPKI证书；边缘路由器或发送源点在决策代理服务器的帮助下，验证接收者、非对称组播的发送者或发送源点提交的SPKI证书，并确认其是否具有从相应组播地址接收或向相应组播地址发送组播数据的权限。

3　MDAC鉴别和授权协议

MDAC鉴别和授权系统以及协议工作流程如图2所示。其中包括：密钥服务器(Key Server，KS)兼授权服务器(Authorization Server，AS)、主机Host、组播边缘路由器Router、转发代理Source、决策代理服务器(Decision Agent Server，DAS)和LDAP SPKI证书库(LDAP SPKI Certificate Storage，LSCS)。KS兼AS包括：文献[1]中密钥管理协议基础设施中的组安全控制器GSC或子组安全控制器SGSC。协议中的主机Host包括：接收者、非对称组播发送者或发送源点。所有的密钥服务器(GSC或SGSC)虽然不参加第一类组播通信，但默认具有发送(通过转发代理)和接收第一类组播通信的权限。即GSC或SGSC的SPKI授权证书的第一个子域具有“Send to”和“Receive from”的许可权限(简称为S和R权限)。因此，对第一类组播通信的S和R这两种权限可以按如下委托路径传递：GSC→SGSC→端用户。规定对第一类组播通信，S和R权限可以委托；而对第二类组播通信，S和R权限不可委托。系统中AS和Host之间的交互受到GKM密钥管理协议基础设施的保护(见文献[1]密钥管理协议)；AS和LSCS之间、DAS和LSCS之间利用传输层安全(Transport Layer Security，TLS)建立安全通信连接；Router和DAS之间利用IPSec建立安全通信连接。MDAC授权协议的工作方式如图2所示。

1) Host→AS：AR={GID，ID，$CERT_{Host}$}。Host为了加入组播通信向授权服务器AS发送授权请求(Authorization Request，AR)。AR中包含了Host希望加入的组播通信的GID、Host的身份信息ID和PKI证书$CERT_{Host}$等。2) AS：鉴别。利用PKIX的单向鉴别协议(或双向鉴别协议)，授权服务器AS根据AR请求对Host进行鉴别(如果是双向鉴别Host还可对AS进行鉴别)。成员的加入和撤离由GKM密钥管理基础设施(更新组通

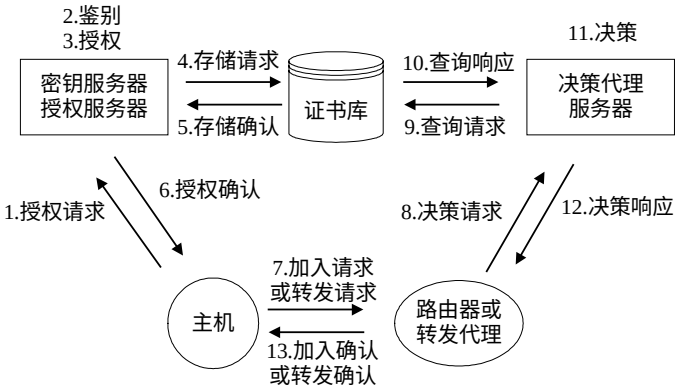

图2 鉴别和授权系统

信密钥)和AS共同控制(鉴别、颁发SPKI证书、并通过SPKI证书的时效来进行控制)[1]。3) AS：授权。授权服务器AS根据授权策略对经过鉴别的Host进行授权，同时为Host生成公钥对K_{pulic}和$K_{private}$以及SPKI授权证书。4) AS→LSCS：SR={SPKI证书}$_{TLS}$。授权服务器AS向LDAP SPKI证书库发送证书存储请求(Storage REQ，SR)。5) LSCS→AS：{SA}$_{TLS}$。LDAP SPKI证书库服务器向AS发送存储确认信息(Storage ACK，SA)。6) AS→Host：AA={SPKI授权证书}。授权服务器AS向Host发送授权确认信息(Authorization ACK，AA)，AA包含了Host的SPKI授权证书。1)～6)步在Host第一次请求加入组播通信时，为Host颁发授权证书而执行。以后Host再次访问组播通信(例如：因为网络中断恢复或暂时离开后回来等)时，由于已经持有SPKI授权证书，协议就从第7)步开始执行。7) Host(非对称组播发送者)→Router(Source)：JR={IGMP(SPKI证书)}$K_{private}$(FR={ SPKI证书} $K_{private}$)。Host向路由器发送IGMP加入请求(Join REQ，JR)。该信息包含了Host的SPKI证书，整个信息用Host的私钥$K_{private}$签名。当Host为非对称组播发送者时，该步骤为非对称组播发送者向组播通信的转发代理Source发送转发请求信息 (Forwarding REQ，FR)。8) Router(Source)→DAS: DR={Router信息，SPKI证书}$_{IPSec}$。路由器使用Host的SPKI证书中的公钥K_{public}验证签名信息，生成决策请求(Decision REQ，DR)，向决策代理服务器发送决策请求DR。当Host为非对称组播发送者时，该步骤为转发代理Source向DAS发送决策请求DR。9) DAS→LSCS：{CCQ}$_{TLS}$。决策代理服务器DAS验证了Router的请求后，根据Host的SPKI证书，生成并向LDAP证书库提交证书链查询请求(Certificate Chain Query, CCQ)。10) LSCS→DAS：{QR}$_{TLS}$。LDAP证书库服务器向决策代理服务器DAS发回查询响应(Query Response, QR)；9)、10)可能往返很多次。11) DAS：决策。决策代理服务器DAS根据证书链查询响应信息。利用证书链搜索算法确定有效的证书委托链并利用证书链缩减算法为Host产生缩减后的SPKI证书。10)～11)步在Host第一次访问组播通信时[2]，DAS使用证书链搜索算法和证书链缩减算法时执行。以后Host再次请求授权服务时，直接使用缩减后的SPKI证书。10)、11)步可以跳过，直接执行12)步。12) DAS→Router(Source)：DA={缩减后的SPKI证书}$_{IPSec}$。决策代理服务器DAS向Router发回决策响应信息(Decision ACK，DA)。该信息包含了Host的缩减后的SPKI证书。这时路由器就可以向组播路由系统发送相应的路由信息，组播路由算法将组播树扩展到该边缘组播路由器所在的子网。当Host为非对称组播发送者时，该步骤为DAS向转发代理Source发送决策响应信息DA。13) Router(Source)→Host：JA(FA)={缩减后的SPKI证书}K_{public}。路由器向Host发回加入确认信息(Join ACK，JA)。该信息用Host的公钥K_{public}加密并包含了Host的缩减后的证书。当Host为非对称组播发送者时，该步骤为转发代理Source向Host发送转发响应信息(Forwarding ACK，FA)。当Host再次访问组播通信时(网络中断后恢复、Host离开后又加入等)，协议可以得到大幅度简化1)～6)步，10)～11)步均可跳过只用5)步即可完成。

4 模拟仿真和性能评价

下面对MDAC和现存的部分组播访问控制解决方案进行性能对比。这里，简称文献[3]提出的方案为Hardjono；文献[4]提出的方案为Ballardie；文献[5]等提出的方案为He；文献[6]提出的方案为Gothic。

为了分析各种方案在边缘路由器和访问控制服务器(MDAC中对应的决策代理服务器)上的计算开销，首先计算了每种方案需要调用各种运算(包括标准密码函数)的次数；乘以每种运算的实际处理时间，就能够估算出每种方案的实际计算开销。涉及的运算包括：主机鉴别、数字签名及校验、授权查找以及加密等。涉及密码算法的运算处理时间是基于Crypto++库给出的各种标准密码算法的运算速度基准[7]。计算如下：

$$\text{计算开销}=\frac{\text{需加密的数据量}}{\text{3DES 加密速度}}+\frac{\text{需进行消息摘要的总数据量}}{\text{MD5执行速度}}+\text{签名次数}\times$$
$$\text{RSA签名时间}+\text{签名验证次数}\times\text{RSA验证时间}$$

仿真实验是在以下环境中进行的：Celeron 850 MHz、Windows 2000的PC。模拟仿真中使用了128 bit的Triple DES加密算法、MD5消息摘要算法、RSA 1 024 bit数字签名算法、和HMAC-MD5 的IPSec AH协议。每种算法的执行速度如表1所示。

表1　标准密码算法运算速度

操作	性能
3DES加密	4.748 MB/s
MD5 消息摘要	100.738 MB/s
HMAC/MD5 消息摘要	99.863 MB/s
RSA 1 024 签名	10.29 s
RSA 1 024 校验	0.30 s

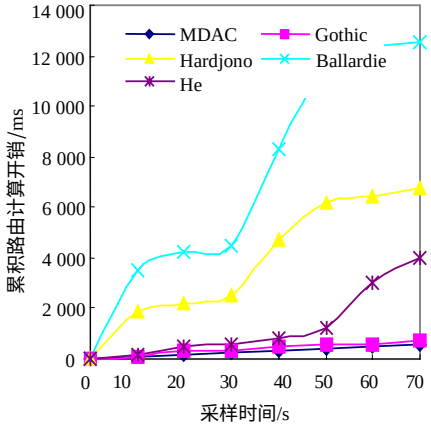

图3　边缘路由器上的计算开销

图3所示给出了各种方案在边缘路由器上的计算开销对比，模拟结果显示，MDAC方案具有最小的计算开销，因为采用决策代理服务器作为边缘路由器的访问控制代理，减轻了边缘路由器的负担，提高了边缘路由器的效率和通用性。事实上，也不应该占用宝贵的路由器资源。在Ballardie和Hardjono方案中，路由器参与了相当一部分的访问控制任务，因而边缘路由器上的计算开销很大。

5　结　论

本文利用SPKI技术实现了组播分布式访问控制服务MDAC。通过和其他方案的对比，可以看出MDAC在具备优越性能的同时具备很多其它方案所不具备的特性，如分布式、授权委托和隐私保护等。目前，在组播安全学术界和工程界，针对大型组播系统的安全访问控制问题的研究结果不多，已有的结果存在很多局限。MDAC是在该领域作出的一次尝试。

参　考　文　献

[1] 刘　璟, 周明天. 大型动态多播群组的密钥管理和访问控制[J]. 软件学报, 2002, 13(2): 291-297

[2] Ellison C. SPKI certificate theory [Z]. RFC2963, 1999

[3] Hardjono T, Cain B. Key establishment for IGMP authentication in IP multicast[C]. IEEE European Conference on Universal Multiservice Networks (ECUMN), CERF, Colmar, France, 2000

[4] Ballardie T, Crowcroft J. Multicast-specific security threats and counter-measures [C]. Proceedings of the Symposium on Network and Distributed System Security, San Diego, California, 1995

[5] He H, Hardjono T, Cain B. Simple multicast receiver access control[R]. Internet-Draft, 2001

[6] Judge P, Ammar M. Gothic: a group access control architecture for secure multicast and anycast[C]. IEEE Infocom 2002

[7] Dai W. Crypto++ [EB/OL]. http://www.eskimo.com/~weidai/benchmark.html, 2004-07-23

[8] Ishikawa N, Yamanouchi N, Takahashi O. IGMP extension for authentication of IP multicast senders and receivers, draft-ishikawa-igmp-auth-01.txt[R]. Work in Progress, 1998

[9] Rigney C, Rubens A, Simpson W, et al. Remote authentication dial in user service (RADIUS) [R]. RFC 2138, 1997

编　辑　孙晓丹