移动 Agent 访问控制机制研究

谭 湘 顾毓清 包崇明
(中国科学院软件研究所 北京 100080)

摘 要 本文在分析了移动 agent 系统的访问控制机制研究现状之后,提出了一种基于属性证书的访问控制机制。该机制的核心思想是将相关安全属性信息集成在外部实体——属性证书。

关键词 移动 agent 系统,访问控制,属性证书

The Research on Access Control for Mobile Agent

TAN Xiang GU Yu-Qing BAO Chong-Ming
(Institute of Software, Chinese Academy of Sciences, Beijing 100080)

Abstract After analyzing the present research on the access control method for mobile agent system, a method based on attribute certificates is proposed. The key idea of this method is to push the security attribute information to an external object—an attribute certificate.

Keywords Mobile agent system, Access control, Attribute certificates

移动 agent 是一个能在异构网络中自主地从一台主机迁移到另一台主机,并可以与其他 agent 或资源交互的程序,实际上是 agent 技术与分布式计算技术的结合体,具有移动性和自主性等特点[1]。随着移动 agent 技术向电子商务、分布式计算、信息搜索等领域的深入,安全性问题显得日益重要。本文首先分析了移动 agent 的访问控制机制及其相关工作,然后提出了一种基于属性证书的移动 agent 访问控制机制,并对该机制进行了分析。

1 移动 agent 系统的访问控制

移动 agent 服务器安全问题是移动 agent 系统安全研究的重要课题之一。agent 服务器需保护其资源免于被未授权 agent 访问,以防止恶意 agent 的攻击,同时合法授权的移动 agent 必须能够在控制之下访问到它们所需要的资源[2]。因此,访问控制机制是必需的。

目前的移动 agent 系统,如 mole[3]、Aglet[4]等,都是采用以下方法:移动 agent 运行环境首先对进入平台的移动 agent 的身份进行验证,判断它是否是合法的移动 agent,这通常是数字签名来解决的。通过认证之后,就需要分配给移动 agent 相应的可以支配的资源和操作权限,一般使用存取控制列表 ACL 来描述。通过预先在要使用的机器上建立帐户,并且为该帐户分配相应的资源和权限。

目前的这种访问控制机制,存在以下缺点:

(1)使用存取控制列表 ACL,预先在要使用的机器上建立帐户,并且为该帐户分配相应的资源和权限。而在庞大的网络系统中,为各个移动 agent 建立一套这样的帐户系统是困难的,这极大地限制了移动 agent 的应用。

(2)安全属性信息是嵌入在 agent 代码中,产生的问题就是无法扩展。当同一段代码需要不同属性运行的时候,该 agent 就必须被重写。

(3)在 agent 应用之中,安全属性设置者和所需要的信任关系变化很大。然而,在 agent 系统中,这些却是变化很小的,可能很多应用所需要的安全属性是相同的。

(4)不同的 agent 系统之间的安全信息,在粒度、语言、资源实体等方面的表达不同。对于应用开发者来说,修改或者扩展是困难的。

(5)安全属性信息一旦被装载在一个内部数据结构中,在不同的 agent 系统中,这个结构是不同的。agent 系统的互操作性被严重地限制了。

为了克服以上缺点,我们提出一种基于属性证书的方法。通过属性证书来表达安全属性信息,从而将安全属性信息从 agent 代码中分离出来。

2 属性证书与安全属性

PKI(Public Key Infrastructure,公钥基础设施)[5]已经成为网络应用中不可缺少的安全支撑系统。它通过方便灵活的密钥和证书管理方式,提供了在线身份认证的有效手段,为访问控制、抗抵赖、保密性等安全机制在系统的实施奠定了基础。

PMI(Privilege Management Infrastructure,特权管理基础设施)[6]是建立在 PKI 提供的可信任的身份认证服务的基础上的,以属性证书的形式来实现授权的管理。PMI 体系和模型的核心内容是实现属性证书的有效管理,包括属性证书的产生、使用、吊销、失效等。

2.1 属性证书[6]

属性证书是由 PMI 的权威机构 AA(Attribute Authority)签发的将实体与其享有的权力属性捆绑在一起的数据结构,权威机构的数字签名保证了绑定的有效性和合法性。属性证书主要用于授权管理。

属性证书建立在基于公钥证书的身份认证的基础上。公钥证书保证实体及其公钥的对应性,为数据完整性、实体认证、保密性、授权等安全机制提供身份服务。

属性证书的格式如表1：

表1

字段	含义
version	标识证书的版本
Holder	该属性证书的持有者
Issuer	证书颁发者名称
Issuer Unique ID	证书颁发者的唯一标识符
Signature Algorithm ID	签名算法标识符，用于说明本证书所用的数字签名算法
Serial Number	由证书颁发者分配的本证书的唯一标识符
Validity Period	证书的有效时间段
Attributes	持有者所拥有的权力属性
extensions	可选的扩展项

属性证书的吊销与公钥证书类似，也是通过证书撤销列表CRL(Certificate Revocation List)的方式。通常对于有效期较长的属性证书系统需要维护属性证书撤销列表ACRL(Attribute Certificate Revocation List)，而对于生存周期非常短的属性证书来说，证书撤销是没有必要的。

2.2 移动agent系统的安全属性

目前，在移动agent系统中常用的几种安全属性如下：

(1)系统资源：进程时间、内存空间、磁盘空间、网络存取权限、本地窗口系统、执行优先权、文件系统。

(2)Agent能力：包括完成一定的面向agent的功能的能力，如克隆(cloning)、发布消息、订阅消息、改变路线等。使用者或其他角色也想限制agent的活动，如允许迁移的平台最大数目、返回到宿主平台的最长时间，经济交易的最大货币数目。

(3)安全服务：使用属性来激化平台上的安全机制，例如完成主机跟踪、部分结果封装、保护平台内部通信的机密性和完整性，限制迁移到安全域、限定迁移路由。

(4)Agent通信：除了平台级别的服务，其他属性也可以应用于agent通信级别。例如，控制agent是否能够直接封装agent自身通信语言对话。

3 基于属性证书的移动agent访问控制机制

3.1 基本框架

在该机制中，不是把预先定义的安全策略信息嵌入到agent中，而是采用将相关安全策略信息集成在外部实体——属性证书。该证书的颁布者可以调整其内容，从而控制agent对计算资源的使用和安全机制。系统基本框架如图1所示。

系统运行基本过程如下：

(1)用户从证书中心(Certificate Center)取得证明自己身份的公钥证书，并从属性中心(Attribute Center)取得相应的属性证书，该证书决定了持有者所拥有的权限。

(2)用户创建一个移动agent，该移动agent代表某人运行，他(她)将agent和他(她)的公钥证书以及属性证书打包成jar文件，通过网络迁移到目标agent平台。属性证书的这种使用方式属于推模式(push model)。

(3)当agent移动到agent平台时，带有它被颁布的属性证书和公钥证书，证书中包含有给该agent设置安全信息的颁布者的身份。移动agent平台接受到移动agent的进入请求后，查看移动agent的公钥证书，同时查看相应的证书中心的证书撤销列表，检查该证书是否被注销。如果证书有效，则载入移动agent代码，并允许其运行。否则拒绝执行。

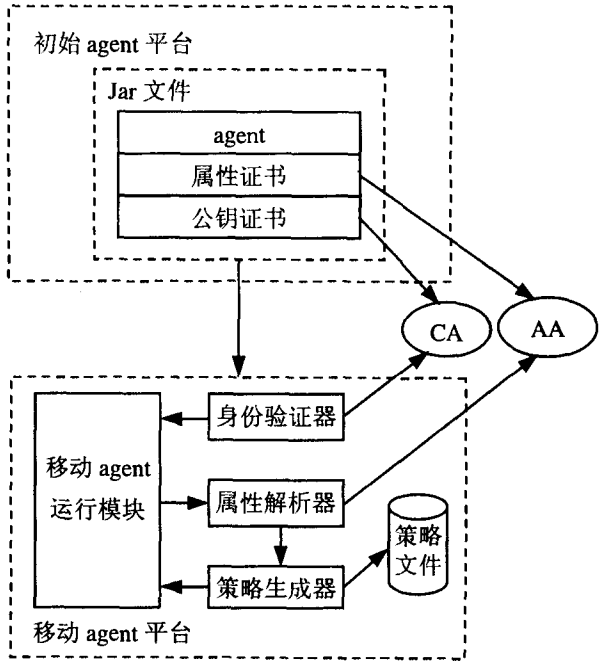

图1 基本框架

(4)移动agent在平台上执行，请求使用某资源时，移动agent平台查看该agent的属性证书，检查该agent是否拥有这项权力。同时检查属性证书注销列表，查看该证书是否被注销。如果证书有效且有该项权力，则允许移动agent使用此项资源。否则拒绝其请求。

(5)重复过程(4)，直到移动agent完成任务或者因某项资源请求访问遭到拒绝而不能完成任务，从该平台迁移出去。

3.2 功能模块分析

在这种基于属性证书的方案中，在原有移动agent系统的基础上需要增加一些部件。系统主要由以下部分组成：

(1)身份验证器

身份验证器的作用是确认公钥证书与agent的关系、验证签名和证书有效期。在系统实现中，需要借助PKI来认证agent的身份。身份验证未通过的agent，运行环境将拒绝其执行。

(2)属性解析器

属性解析器的作用是效验属性证书，分析出属性值，将分析结果给策略生成器。效验属性证书包括验证属性证书与agent的关系、验证签名和证书有效期等。确认属性证书与agent的关系本身是一个复杂的工作，涉及到过期的或撤销的证书以及取回支持信息的必要性，这需要借助于身份验证器验证的结果，也需要借助于PMI。

(3)策略生成器

策略生成器的作用是把证书处理器所分析的结果和该平台的安全策略进行对比，判断是否允许agent进行活动或者在哪种特权下活动，生成合适的安全策略，授予给该agent。

当agent到达一个平台时，无论是使用者的域内还是域外，接受平台的属性解析器对证书进行解析之后，提交给策略生成器。策略生成器把属性解析器所提交的安全信息和平台的策略相比较，引起了可允许的权限设置的变化。这个过程也就是本地和域的权限许可集。在简单的方式下，agent平台的策略生成器必须计算出这些特权的交集。因此，该计算必

(下转第78页)

删除过程的指针操作没有插入过程复杂。上述情况表明副本对查询的响应性能有明显改善，但相应增加了一些插入和删除操作的开销。

结束语 随着计算机应用领域的不断扩大，数据的规模越来越大，查询也越来越复杂，分布式并行索引以其高性能而逐渐成为解决这类复杂问题的有效手段，并且成为数据挖掘、数据仓库、网格计算和普适计算等研究中的一个热点问题。本文提出一种适合于分布式并行的新索引树结构——DPB$^+$-Tree，此索引树以 B$^+$ 树和 hash 结构为基础，其叶子结点被组织为有 n 个散列表元的 hash 表链，从树的根结点到叶子结点，结点的副本数量逐渐减少，并且其数量的变化是动态的。为了验证 DPB$^+$-Tree 系统的有效性及评估其性能，我们对 DPB$^+$-Tree 的响应时间进行了仿真，结果表明 DPB$^+$-Tree 系统提高了系统的查询效率。

在 DPB$^+$-Tree 系统中，我们主要考虑的是一维索引的分布和并行，对于高维索引考虑较少，特别是高维索引中各维数据如何进行分布，各维数据之间如何进行并行查询等，这些都是需要进一步研究的问题。

参 考 文 献

1 Matsliach G, Shmueli O. Distributing a B$^+$-tree in a loosely coupled environment. Information Processing Letter, 1990, 34(3): 313～321

2 Whang K Y, Kim S W, Wiederhold G. Dynamic Maintenance of Data Distribution for Selectivity Estimation. VLDB Journal, 1994, 3(1): 29～51

3 Lomet D. Replicated Indexes for Distributed Data. In: Proc. of the Fourth Intl. Conf. on Parallel and Distributed Information Systems. Miami Beach, Florida, USA, 1996. 108～119

4 Lomet D, Salzberg B. Access Method Concurrency with Recovery. In: Proc. ACM SIGMOD Conf. San Diego, CA, 1992. 351～360

5 Yokota H, Kanemasa Y, Miyazaki J. Fat-Btree: An update-conscious parallel directory structure. In: 15th Intl. Conf. on Data Engineering. Sydney, Australia, 1999. 448～457

6 Ghandeharizadeh S, DeWitt D. Hybrid-Range Partitioning Strategy: A New Declustering Strategy for Multiprocessor Database Machines. In: Proc. of the 16th VLDB Conf. Brisbance, Australia, 1990. 481～492

7 Liebeherr J, Akyildiz I F, Omiecinski E. Petformance Comparison of Index Partitioning Schemes for Distributed Query Processing. In: 24th Hawaii Intl. Conf. on System Sciences (HICSS-24). Koloa, Hawaii, 1991. 317～323

8 Liebeherr J, Omiecinski E, Akyildiz I F. The Effect of Index Partitioning Schemes on the Performance of Distributed Query Processing. IEEE Transactions on Knowledge and Data Engineering, 1993, 5(3): 510～522

9 Matsliach G, Shmueli O. A combined method for maintaining large indices in multiprocessor multidisk environments. IEEE transaction on knowledge and data engineering, 1994, 6(3): 420～429

10 Boral H. Parallelism and Data Management. In: Proc. of 3rd Intl. Conf. on Data and Knowledge Bases. Jerusalem, 1988. 362～373

11 Das S K, Demuynck M A. B^{mad}-tree: an efficient data structure for parallel processing. Eighth IEEE Symposium on Parallel and Distributed Processing. New Orleans, 1996. 384～391

12 Kanth K V R, Agrawal D, Abbadi A E, et al. Parallelizing multidimensional index structures. Eighth IEEE Symposium on Parallel and Distributed Processing. New Orleans, 1996. 376～383

13 姚卿达，杨桂桢，张俊欣. RFN-B$^+$ 树索引文件及其有效性. 软件学报，1998, 9(11): 820～827

(上接第 62 页)

须考虑到策略设置者的继承关系。例如，在发生不一致时，我们希望平台所有者的策略比 agent 使用者的策略优先考虑。

之所以将属性解析器与策略生成器分离，是为了将来的扩展性而考虑的：第一，支持多种证书结构，如 x.509/PGP 证书结构，采用统一的策略生成接口；第二，为了支持多种安全技术，可以将其它安全技术的分析结果来生成安全策略和权限。

(4)策略文件

目前大多数移动 agent 系统是基于 Java 语言的。Java 提供的应用程序环境的安全策略，使得不同的代码对系统资源拥有不同的访问许可。Java 应用程序安全策略由 Policy 对象来表达，通过定义安全策略文件来实现[7]。移动 agent 平台管理员可以为该 agent 平台设置安全策略文件，该文件采用的是 Java2 平台所支持的策略文件格式。

(5)Jar 文件

当 agent 在平台之间移动时，保持它的相关的公钥证书和属性证书的责任由 agent 系统完成。通过 Jar 文件中增加证书并把所有的 agent 代码放置在 Jar 文件中，Jar 文件能够被用来作为证书的容器。在 Java 框架中，Jar 文件是使用数字签名技术签名和认证代码的预定义方法。除了存档代码，Jar 文件还包含有对该文件的每一个签名者的一对文件，(签名指令和数字签名文件)。额外的信息，如签名代码的实体的身份证书也被包含在文档中，以便接受者简化移动代码的确认过程。

3.3 特点

与现有的移动 agent 系统的访问控制机制相比，该机制具有以下特点：

(1)采用了 PKI/PMI 双证书结构，由 PKI 和 PMI 分别通过公钥证书和属性证书完成身份认证和访问控制。PMI 的授权是建立在 PKI 认证服务的基础之上的。

(2)属性证书采用 Push 模式，实现起来比 Pull 模式简单，效率也较高。

(3)可扩展性好，通过属性证书来表述安全属性，可以增加新的安全属性。

(4)属性证书是一个签名了的实体，它的破坏能够被检测到。在那些容易受到恶意平台通过修改安全信息攻击 agent 的 agent 系统中，这可以作为一个额外的保护措施而发挥作用。

(5)该系统框架适用于基于 Java 的移动 agent 系统。

结论 本文针对移动 agent 的访问控制机制这一特定问题，提出了一种基于属性证书的移动 agent 访问控制机制，并对该机制进行了分析。目前，移动 agent 系统在安全上存在着很多问题，但是随着研究工作的进一步深入，移动 agent 技术必将得到广泛的应用。

参 考 文 献

1 Jansen W, Karygiannis T. NIST Special Piblications 800-19: Mobile Agent Security. National Institute of Standards and Technology: [Tech Rep: MD208999]. 1999

2 Jansen W. Countermeasures for mobile agent Security. Computer Communications, 2000, 23(10): 1667～1677

3 Karjoth G, Lange D B, Oshima M. A Security Model For Aglets. IEEE Internet Computing, 1997. 68～77

4 Baumann J, Hohl F, Rothermel K, et al. Mole - Concepts of a Mobile Agent System. World Wide Web, 1998, 1(3)

5 Adam C, Farrell S. Internet X.509 Public Key Infrastructure Certificate Management Protocols. RFC 2510, IETF Networking Group, March 1999

6 Farrell S. An internet Attribute Certificate Profile for Authorization. RFC3281, 2002. 18～32

7 Li Gong. Inside Java 2 Platform Security: Architecture, API Design, and Implementation. Addison Wesley, 1999