网格计算中面向虚拟组织的多级授权机制研究*)

赵曦滨[1,2] 郭 陟[2] 雍建平[1] 顾 明[2]
(江苏大学计算机科学与通信工程学院 江苏镇江212013)[1]
(清华大学软件学院 北京100084)[2]

摘 要 由于虚拟组织的分布性和动态性,在网格计算系统中实施面向虚拟组织的授权服务十分困难。本文分析了网格计算系统中的授权服务需求和已有授权机制存在的问题,提出了多级授权架构MLA。该架构基于门限闭包机制,具有较强的策略描述能力与可扩展性,因而能够更加灵活高效地在网格计算系统中实施授权服务。

关键词 虚拟组织,授权,秘密共享,门限闭包,可扩展性

Research on Multi-level Authorization Mechanism for Virtual Organization in Grid Computing System

ZHAO Xi-Bin[1,2] GUO Zhi[2] YONG Jian-Ping[1] GU Ming[2]
(School of Computer Science and Telecommunications Engineering, Jiangsu University, Zhenjiang Jiangsu 212013)[1]
(School of Software, Tsinghua University, Beijing 100084)[2]

Abstract It is a challenging work to implement authorization service for Virtual Organization in Grid Computing System because of the dynamic and distributed nature of Virtual Organization. After analyzing the requirement of authorization service and the existing mechanisms for implementing authorization services in Grid Computing Systems, the paper proposes an efficient multi-level architecture named MLA for implementing authorization in Grid Computing Systems. With the use of threshold closure mechanism, the proposed architecture has the scalability and the strong power to express authorization policy, hence can provide flexible and efficient approach to implement authorization service in GCS.

Keywords Virtual organization, Authorization, Secret sharing, Threshold closure, Scalability

1 引言

近年来,网格计算系统(Grid Computing System, GCS)逐渐成为分布式计算系统研究和应用的一个热点。与传统分布式系统不同,网格计算关注广域地理分布环境下的动态、大规模资源共享,更易于实现动态环境下的海量数据共享和面向复杂任务的协同工作。GCS中的资源共享和协同工作建立在虚拟组织(Virtual Organization, VO)基础之上[1]。VO实际上是对具有复杂内联关系的分布式系统的抽象描述,而网格计算的目标就是在动态的、多成员的VO中实现资源共享与协同工作。通过提供相应的服务及协议,GCS可以在应用系统中为VO的生成与运作提供支持。其中,VO成员间分享资源的机制及如何为实现特定应用目标而使用资源都是必须解决的关键问题。

在VO生成阶段,必须完成选择参与者及相关资源的操作。在VO执行阶段,则必须建立参与者之间以及参与者和资源之间的各种联系,从而进一步支持为实现特定目标而展开的协同工作。因此,为了管理与实施VO,上述操作必须依据VO的安全策略来加以控制。早期的网格计算系统建立在大学和研究机构共享高性能计算资源的基础之上[2],参与者之间具备良好的信任基础,且资源类型简单,所以对资源的访问控制并没有太多要求。然而,在商业应用中如果不解决互信问题,必将对系统实施与使用产生巨大阻碍。但是,在实际应用系统中定义及实施相关的安全策略非常困难:一方面,在网格计算环境下,VO参与者会面向庞大的用户群体提供对资源的访问,为了有效控制系统资源并提高系统可靠性,必须实施成组访问控制等复杂的访问控制策略;另一方面,VO的参与者和资源都可以在运行期间动态地加入或离开,这也增加了安全控制的复杂性。因此,授权机制对于VO的安全来说至关重要。然而,由于VO的特殊性质,授权问题十分复杂,并不能直接解决。通常,VO参与者的加入与退出使得VO以动态的方式存在。此外,由于GCS的开放性和分布式特点,参与者之间缺少互相信任,很难通过集中控制来保障授权。本文分析了VO管理对授权的需求,并设计了一个基于门限闭包(Threshold Closure)的多级授权机制以满足这些需求。

2 虚拟组织中的授权问题

2.1 虚拟组织的操作特点及授权要求

VO的根本目标就是针对特定任务实现大规模的协同工作与资源共享。因而,对于那些基于任务驱动,且需要大量组织和资源配合的应用来说,尤其适合采用基于VO的解决方案[3]。例如,当类似非典型肺炎这样具有严重危害性的传染病爆发时需要建立应急的传染病监控体系。为了有效监控疫情传播,需要获取一系列不同来源的关键数据进行分析。例如,

*)本文研究受国家863计划项目(Nos. 2003AA148020,2003AA414031)资助。赵曦滨 博士研究生,研究方向为计算机系统安全与软件体系结构;郭 陟 博士后,研究方向为计算机系统安全与软件体系结构;雍建平 讲师,主要研究方向为软件工程与计算机系统安全;顾明 副教授,研究方向为操作系统、分布式应用系统支撑平台和电子商务等。

从来自医院的疑似病例报告中获取疾病症状;从区域人员的出入情况分析传染源;从专业的非典型肺炎监控系统中获取有用的经验数据;从环境和卫生部门获取感染者居住点的卫生情况以分析传染途径等。显然,要想有效控制疫情,上述这些独立组织间的合作是必不可少的。通常,为了完成这些特定任务,要在许多分布在不同地理区域且相互独立的机构上形成一个 VO 并充分利用组织内的资源来完成目标任务。

VO 的运作要求能跨越不同的参与机构来访问计算机系统和数据对象,因而必须提供参与机构间的互连能力。然而,出于法律约束和自身保护措施等方面的考虑,除非在一些特定领域(如科学计算)内或是借助强制性的行政干预,否则实现这样的互连是不可能的。实际上,VO 参与者往往在事前处于互不信任的状态。此外,由于协作任务的需要,各参与机构中实际操作人员的数量和角色也处在动态变化之中。由此可见,对于动态复杂的虚拟组织来说,必须建立高效、可行的访问控制机制来保障参与者之间的资源共享及协同工作。但是,由于 VO 的动态性和复杂性,在对 VO 实施管理时将面临严峻挑战。

通常,VO 中的操作主要包括以下行为:

·VO 生成过程中参与者和相关资源的注册行为;为协作完成任务,参与者还需要将自己可控的共享资源在 VO 中注册。

·对授权用户角色的分派。这些用户在 VO 的执行过程中可以代表参与者来使用资源。

·制定并描述针对共享资源的访问控制策略。

·在用户对 VO 提出资源请求时根据访问控制策略来实施访问控制。

在 VO 这样复杂的分布式系统中,实现上述操作,尤其是定义及实施访问控制是非常困难的。首先,VO 参与者总是动态地加入或离开,因而他们之间的相互关系及相应的访问控制策略总是处在动态变化的过程中;其次,资源的共享是受限的。在不同应用背景下,往往有不同的约束条件。例如,在实际应用中,需要通过双重控制(Dual Control)和责任分离(Seperation of Duty)等手段来保障系统的可靠性和可追查性。这时,对资源的访问往往要求授予来自不同组织或实体的成组对象。

有鉴于此,对 VO 中授权服务的要求主要体现在下述两个方面:

1)较强的策略表达能力。当 VO 中的参与者与资源数量众多时,网格计算系统的授权策略将变得非常复杂。例如,有5个组织参与了 VO,这些组织共指定了20个用户来协同完成任务。假定他们需要非典型肺炎的门诊数据来进行分析,而重要的门诊数据存储在 VO 的特定节点上,为加强对敏感数据存取过程的制约,规定必须是来自不同组织的两个用户才可以一起访问门诊数据。这样一来,访问控制策略将描述为"任意两个用户 P_i 和 P_j 可以共享资源,除非他们来自同一组织"。显然,当用户数量很多且访问控制策略有进一步约束时,问题将变得格外复杂。因而,要求 VO 中的授权服务具备描述复杂授权策略的能力。

2)可扩展性。由于 VO 的动态特性,访问控制规则总是在不断地更新与扩展。因此,要求 VO 中的授权服务能够动态、高效地处理访问控制规则的变化。

2.2 相关的研究工作

作为网格安全机制的代表,Globus 安全基础设施(Globus Security Infrastructure,GSI)[4]提供了大量网格安全应用服务,包括相互认证(Mutual Authentication)和单点登录(Single Sign-On)等。GSI 建立在 PKI、X.509认证以及安全套接字(Secure Socket Layer,SSL)通信协议等基础之上,为网格应用系统提供了包括双向认证、单点登录(Single Sign-On,SSO)等安全服务。尽管 Globus 工具集(Globus Toolkit)实现了 GSI 的协议与 API,以满足网格环境的安全需求,但它主要着重于认证和对消息的保护。随着 Globus 的发展,Globus Toolkit 中又增加了团体授权服务(Community Authorization Service,CAS)[5,6]。CAS 调整了现有的由 GSI 提供的本地授权机制,通过对 VO 访问策略与资源管理者的本地化访问策略的综合评估与均衡,在保障 VO 用户的 GSI 身份在访问任何资源时都一样的同时,借助 GSI 身份认证实现面向整个 VO 的团体授权策略。CAS 的体系结构如图1所示。由图中可以看出,CAS 使用 ACL 作为其基本授权机制。

虽然 GSI 已经为网格应用中的安全问题提供了一个复杂的解决方案,但为了支持在上节中提到的授权策略,还需要改进现有方法,以有效地满足虚拟组织对授权的要求。目前,ACL 因为其简明且易于实施而被广泛地用来描述 GCS 中的授权策略,但其局限性也相当明显。首先,ACL 的表达能力非常有限,它只能直接表达类似于"某人能做某事"的简单策略,而对于复杂访问策略的描述,如"5位官员中的任意3人可以打开非典型肺炎病毒的基因分析报告",则显得十分笨拙。这时,ACL 除了要指定个人的访问权限之外,还需要把用户组也包括进来。这样,"5个之中任意3个"的策略必须分解为一条条的成组访问规则来实现。其次,如果授权策略发生变化,会需要进行大量的 ACL 操作以修改策略描述。例如,形如"5个之中任意3个"的策略被改成"6个之中任意3个"后需要进行大量的 ACL 操作以保证 ACL 与系统的安全策略的一致性。ACL 的另外一些缺点在文[7]中也有所阐述。可见,尽管 ACL 实现起来简单,但使用 ACL 的系统并不能有效处理如上所述的复杂访问控制策略。在基于 ACL 的应用中,安全管理员要分析这些策略,然后再决定创建很多个组以便于复杂策略的描述。当参与者和资源数量很多时,这样去维护一个 ACL 表的效率很低。另外,为了处理策略的变化,设计者还需要不断地分析那些变化的规则并调整对应的 ACL 对象。

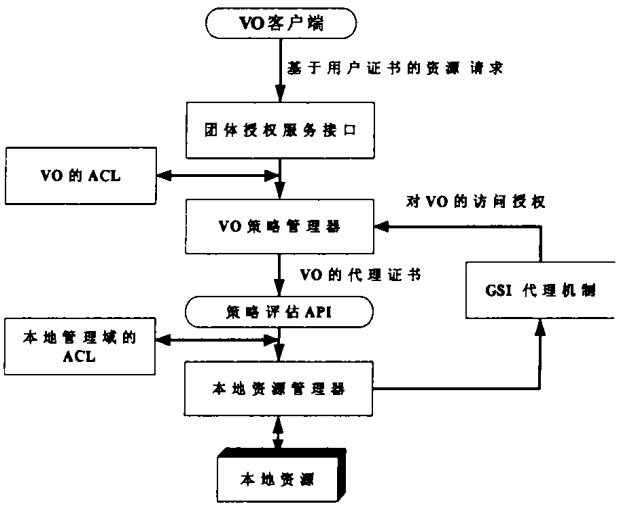

图1 Globus 中的 CAS 系统架构

显然,在用户数量和资源数量都非常大且授权策略变化频繁的 VO 系统中,基于 ACL 的授权服务在表达能力及实施效率方面都存在很多问题。针对上述问题,本文提出一种新型

的多级授权架构(multi-level authorization architecure, MLA)。该架构以一种合理的方式来组织VO的参与者,使之能够更有效地执行访问控制。

3 面向虚拟组织的多级授权机制

3.1 MLA的设计原则

3.1.1 *群组访问控制* 综上所述,在复杂、动态的环境里,管理大规模的VO和执行访问控制都非常困难。为了减少管理代价,MLA根据参与者在协同工作中的权重将其分成几个不同的群组,这样就可以将控制的重点放在一些主要参与者之上,并允许他们能够独立管理其他参与者的访问控制。实际上,在现实世界中这种层次化的管理模式随处可见。从政府运作到企业管理,层次化的管理模式都已经得到广泛的应用并被证明在解决复杂问题上是行之有效的。MLA有两种类型的参与者,即静态参与者(Static Participants,SP)和动态参与者(Dynamic Participants,DP),SP指在VO中完成特定任务,扮演重要角色的参与者,在VO中具有相对稳定的状态。而DP则是指那些扮演次要角色的参与者,在VO中有较强的动态性。例如,在应用于非典型肺炎的VO模型中,对医院来说不可能将非典型肺炎病例报告让VO中所有实体共享。他们通常是首先根据某种访问控制策略,对一些值得信赖的,并可以帮助他们完成医疗研究的相关机构开放研究报告,而其他的参与者可以作为这些部门的子组,并根据这些部门的访问控制策略来共享报告。这样做的优点是可以在控制VO中任务执行代价的同时保持VO的可扩展性。通过这种方式,资源拥有者可以在相对较小的范围内考虑资源共享问题而整个VO仍然能以可扩展的方式来制止大范围的资源共享。

3.1.2 *分级资源共享架构* MLA系统架构如图2所示。

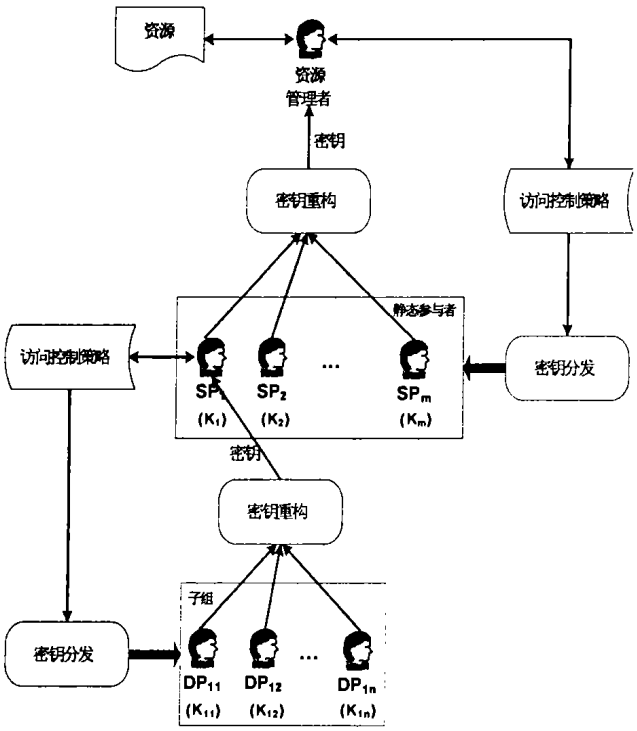

图2 MLA系统架构

在MLA架构中,针对特定资源的参与者在VO中建立了一个多级资源共享树。共享树中接近树顶的层次由SP组成,它们可以依据符合VO管理需求的访问策略来共享资源。远离树顶的层次由DP组成,它们从属于特定的SP并借助其父节点来向VO提交资源访问请求。如果SP的访问请求和父节点的访问控制策略不抵触,则该需求将会通过父节点逐级向上提交。

为了实现MLA,考虑给每个资源分配一个保护密钥,针对该密钥给相关SP都分配一个密码片断(Secrete)并保证只有那些依据访问控制策略可以在一起访问该资源的SP才能够重构密钥。资源共享树上低级的DP由父节点分配密码片断。根据父节点的访问策略,符合条件的DP可以利用它们的密码片断重构所需的密钥并提交给父节点并借助父节点将访问请求上传,直至到达树顶。

研究中发现,密码学领域中的秘密共享(Secret sharing)理论和相关机制可以对MLA提供有力的支持。

3.1.3 *秘密共享及访问结构* 秘密共享理论的主要目标是建立安全可靠的计算机系统,相关的研究工作从20世纪70年代末就已经开始。文[8]为增强密码系统中的密钥管理能力而设计了门限方案(Threshold Scheme)。该方案的主要目标是确保未经授权的用户和遗失了密码的合法用户不能使用系统。由于门限方案只需要简单的拉格朗日插值(Lagrange Interpolation)计算,并且计算效率很高,因此很适合解决此类问题。一个形如(t, n)的门限方案表示给定一个密钥,分配n个相关的密码片断,并确保使用任意t个信息片断都能恢复原始密钥,而$t-1$个或更少的子集则无法恢复密钥。

显然,门限方案可以用来支持对共享资源的访问控制,但它的描述能力局限于类似"n中任取t"的授权规则,不足以支持复杂的访问策略[9]。例如,它并不能明确表示哪些具体的参与者子集可以重构密钥以及哪些具体的子集不能重构密钥。为实现更为复杂的秘密分配方案,访问结构(Access Structure)的概念被提出[10]。

访问结构将系统中的授权策略通过授权子集和非授权子集的形式来加以描述,具备很强的策略表达能力。图2中MLA树的每个节点都存在一个访问结构,它根据该节点的访问控制策略,由下一级参与者所构成的子集组成。但是,访问结构难以实现。而且,如果策略不断发生变化,使用访问结构就会变得相当繁琐。例如,如果基于门限方案来构建访问结构,当有很多类似"n中任取t"的规则加入系统时,用来描述访问结构的门限方案将会非常多且出现大量冗余,这将引起严重的安全管理问题[11]。因此,很多方案被设计出来以简化访问结构的实现[9,12,13]。在MLA中,针对VO的动态性和分布式特点,采用门限闭包(Threshold Closure)来实现密码分配。

3.2 基于门限闭包的秘密共享机制

在VO中,由于授权策略复杂,且潜在的参与者和用户众多,相应的访问结构中会包含数量极大的授权集合,而门限闭包机制因其在算法上的可行性和高效性可以对实施VO授权服务提供有力的支持。

一个门限闭包(用ε表示)是一组满足如下三个条件的(t, S)门限方案(其中,S是一组用户的集合且满足$0<t\leqslant|S|$,$S\subseteq P$,P是所有参与者或用户构成的全集)。

(1)Redundant-free。即不存在两个不同的

$$(t_1,S_1),(t_2,S_2)\in\varepsilon \tag{1}$$

使得

$$S_1\subseteq S \text{ or } |S_1\cap S_2|\geqslant\min\{t_1,t_2\},t_1\neq t_2 \tag{2}$$

(2)Reduced。即不存在

$$(t,S_1),(t,S_2),\cdots,(t,S_m)\in\varepsilon \tag{3}$$

使得

$$\bigcup_{i=1}^{m}[S_i]_t=[\bigcup_{i=1}^{m}S_i]_t \quad (4)$$

其中，$[S]_t=\{S':|S'|=t,S'\subseteq S\}$ (5)

(3)Closed。即对$\forall\ (t,S_1),(t,S_2),\cdots,(t,S_m)\in\varepsilon$和$S'_1\subseteq S_1,S'_2\subseteq S_2,\cdots,S'_m\subseteq S_m$(等号不能都成立)，若

$$\bigcup_{i=1}^{m}[S'_i]_t=[\bigcup_{i=1}^{m}S'_i]_t \quad (6)$$

则 $(t,\bigcup_{i=1}^{m}S'_i)\in\varepsilon$ (7)

或者

$$(t,\bigcup_{i=1}^{m}S'_i)\notin\varepsilon\wedge(\exists\ (t,S)\in\varepsilon)\bigcup_{i=1}^{m}S'_i\subset S \quad (8)$$

可以证明，在某个访问结构Γ_0和ε之间存在一一对应关系[11]。此外，在ε的基础上，可以进一步得到ε的最小覆盖$\min(\varepsilon)$，在$\min(\varepsilon)$中包含了为描述该访问结构所代表的授权策略所需要的最少门限方案。显然，在完成从访问结构到门限闭包的转换运算之后，既保持了对复杂授权策略的描述能力，又提高了描述效率，为进一步的系统实现打下了良好基础。

另外，文[11]还给出了如下针对Γ_0和ε的四类操作：Add (t,S) into ε；Add S into Γ_0；Delete (t,S) from ε；Delete S from Γ_0。利用这四项操作可以保持Γ_0和ε之间的一致性。实际上，由于VO中的授权策略在频繁发生变化，因而要求门限闭包也需要动态调整以正确描述相应的访问结构。而利用这四种运算，门限闭包不但可以自由地扩展和收缩，而且可以和动态的访问结构保持一致性。可见，门限闭包具备类似访问结构的强大策略表达能力，同时也具有良好的可扩展性。

3.3 MLA的授权协议

在描述MLA授权协议时，使用以下定义：

·S 表示资源请求的接受者。

·C 资源共享树中S的子节点。

·$\{C\}$ 表示资源共享树中的特定资源请求者或子节点集合。

·$EK_A[X]$表示由利用参与者A的私钥对数据X的加密操作。

·$Ks[C,Key,P]$ 表示在资源共享树中某个S节点根据其访问控制策略而分配给其子节点的密码片断集合，并保证合法的子节点组可以重构用于访问资源的密钥Key。

·$Se\{C\}$ 表示参与者集合$\{C\}$所持有的密码片断集合。

·Rm 表示确认请求或否决请求的消息。

对资源共享树上的每一个父节点来说，其子节点形成一个参与者群组。根据父节点的访问控制策略，该参与者群组可以形成一个访问结构。由3.2节可知，利用门限闭包机制可以获得能实现该访问结构的最小门限方案集合。访问结构的每一个参与者在进行拉格朗日插值计算后将会得到一个密码片断，而希望访问资源的群组可利用其密码片断重建密钥来获取对资源的控制，或用来作为向上级节点提交请求时所需的父节点的密钥。

授权协议P的形式化描述如下所示：

M1. $S\rightarrow C:Ks[C,EK_S[Key],P]$
M2. $\{C\}\rightarrow S:Se\{C\}$
M3. $S\rightarrow\{C\}:Rm$

首先，资源请求的接受者根据其访问控制策略P制定访问结构，利用自己的私钥对访问密钥Key加密，然后借助门限闭包操作得到最小的门限方案集合，针对每个门限方案利用拉格朗日插值计算的结果生成密码片断并向子节点发放。

资源请求者以群组方式向父节点发送访问请求，父节点接受它们的密码片断，并对密钥重构的结果进行解密操作，如果得到的访问密钥Key正确，则允许请求者访问资源或将该请求向资源共享树顶部上传，否则拒绝资源请求。

基于上述协议可以有效地实现MLA架构。此外，该协议可以支持VO的可扩展性。因为低级参与者仅能够重构经过父节点加密的访问密钥，而无法合谋得到真实的访问密钥，所以当任一参与者离开VO时，除了其子节点外，并不影响其他参与者。反之，当新的参与者加入VO时，父节点将重建访问结构，并重新分配密码，通过使用门限闭包的相关操作将尽可能提高分配工作的效率。

结论 随着全球信息架构的快速发展，虚拟组织作为研究商业应用和组织架构的模型得到了越来越多的重视。借助虚拟组织模型，可以有效提高网格计算系统等分布式系统在资源共享和协同工作等方面的解决能力。为充分发挥虚拟组织的作用，必须建立高效、可行的授权机制。但是，虚拟组织动态性和分布式特性给实施授权服务带来了很大困难，因此需要建立具备较强策略表达能力和扩展能力的授权系统。

本文分析了网格计算系统中面向虚拟组织的授权服务需求，在对已有的授权机制分析比较的基础上，提出了一种基于群组访问控制理论和分级资源共享模式的新型授权机制MLA。MLA充分利用了密码学领域的研究成果，采用基于门限闭包的密钥分配方案来提高系统的执行效率和可扩展性，并针对虚拟组织的运行特点设计了相应的授权协议，从而为虚拟组织提供高效、实用的授权服务。进一步的研究工作包括授权协议的细化、支持访问控制的目录服务系统的设计及成组访问缓冲池的设计等。

参考文献

1 Foster I, Kesselman C, Tuecke S. The anatomy of the grid: enablig scalable virtual organizations. Int. J. Supercomputer Applications, 2001, 15(3): 200～222
2 Foster I, Kesselman C. The Grid: blueprint for a future computing infrastructure. San Francisco: Morgan Kaufmann, 1999
3 Lam K Y, Zhao X B, Chung S L, et al. Enhancing Grid security infrastructure to support mobile computing nodes. In: Proc. of 4th Intl. Workshop on Information Security Applications (WISA 2003), Jeju Island, Korea, 2004. 42～54
4 The Globus Alliance. Overview of the Grid security infrastructure. http://www-fp.globus.org/security/overview.html, 2002
5 Keahey K, Welch V. Fine-grain authorization for resource management in the Grid environment. In: Proc. of Grid2002 Workshop, Baltimore, 2002
6 Pearlman L, Welch V, Foster I, et al. A community authorization service for group collaboration. In: Proc. of the IEEE 3rd Intl. Workshop on Policies for Distributed Systems and Networks, Monterey, CA, USA, 2002
7 Nagaraj S V. Access control in distributed object systems: problems with access control lists. In: Proc. of Tenth IEEE Intl. Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Cambridge, MA, USA, 2001
8 Shamir A. How to share a secret. Comun. ACM, 1979, 22(11): 612～613
9 Benaloh J C, Leichter J. Generalized secret sharing and monotone functions. Lecture Notes in Computer Science, 1989, 403: 27～35
10 Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure. In: Proc. of Globecom'87, Tokyo, Japan, 1987. 99～102
11 Zhang C R, Lam K Y, Jajodia S. Scalable threshold closure. Theoretical Computer Science, 1999, 226: 185～206
12 Brickell E F. Some ideal secret sharing scheme. J. Combin. Math. Combin. Comput, 1989, 9: 105～113
13 Simmons G J, Jackson W, Martin K. The geometry of shared secret schemes. Bull. ICA, 1991, 1: 71～88