

访问控制模型研究进展

韩道军^{1,2} 高 洁^{1,3} 翟浩良¹ 李 磊¹

(中山大学软件研究所 广州 510275)¹ (河南大学数据与知识工程研究所 开封 475004)²

(吉林大学珠海学院公共基础课教研中心 珠海 519000)³

摘 要 访问控制在众多领域中起着重要的作用,是信息系统中进行资源安全控制和管理不可缺少的一部分。介绍了不同访问控制模型的特点及实现方式,并对每种访问控制模型的优缺点进行了分析和比较。同时,介绍了一种语义丰富的标准访问控制策略描述语言(XACML)及访问控制模型中需要进一步研究的一些内容。

关键词 访问控制, DAC, RBAC, ABAC

中图法分类号 TP301 **文献标识码** A

Research Development of Access Control Model

HAN Dao-jun^{1,2} GAO Jie^{1,3} ZHAI Hao-liang¹ LI Lei¹

(Software Research Institute of Sun Yat-Sen University, Guangzhou 510275, China)¹

(Institute of Data and Knowledge Engineering, Henan University, Kaifeng 475004, China)²

(General Basic Courses Research Center at Zhuhai College of Jilin University, Zhuhai 519000, China)³

Abstract Control plays an important role in some fields, which is one of the necessary parts of information system to manage and control the safety of all kinds of resource. In this paper, we proposed some popular access control models, explained the characteristics and realization method of every access control model, analyzed and compared their advantages and shortcomings. Also, we introduced a standard access control policy language, XACML, with stronger semantic. Furthermore, we pointed out some contents being researched currently.

Keywords Access control, DAC, RBAC, ABAC

访问控制是通过某种途径显式地准许或限制主体对客体访问能力及范围的一种方法,它是针对越权使用系统资源的防御措施,通过显式地访问受保护资源,防止非法用户的入侵或因为合法用户的不慎操作所造成的破坏,从而保证系统资源受控地、合法地使用^[31]。访问控制的核心是授权策略。授权策略是用于确定一个主体是否对客体拥有访问能力的一套规则。在统一的授权策略下,得到授权的用户就是合法用户,否则就是非法用户。访问控制模型是从访问控制的角度出发描述安全系统,建立安全模型的一种方法。在访问控制模型中,访问控制主要描述为访问主体依据某些控制权限对客体本身或其资源进行不同授权的访问使用。访问控制模型定义了主体、客体、访问是如何表示和操作的,它决定了授权策略的表达能力和灵活性。

访问控制在众多领域中有着重要的应用,常见的有复杂信息系统、分布式系统等。亦即只要是需要对资源进行保护和限制访问的系统,都需要使用访问控制。例如,在复杂信息系统中,由于用户和资源众多,不同的用户对不同的资源(数据和流程)有不同的操作权限,需要根据安全需求制定详细的策略来进行访问控制,保证信息安全和业务的正常运转。在

分布式系统中,要按照制定好的策略对访问不同系统资源的请求者进行身份验证,以达到资源保护和正常服务的目的。

目前,访问控制的研究内容众多,包括对访问控制模型的研究和如何应用两种。这两种之间的研究不是孤立的,存在紧密的联系,说明如下:一方面,在实际应用中,发现现有访问控制模型的不足,从而对模型进行扩展,解决某一类具有代表性的问题;另一方面,在解决一个应用问题时,要找到合适的访问控制模型,该模型具有一定的优越性。本文介绍常见的访问控制模型,并分析模型的实现方式和特点,同时指出了访问控制模型需要进一步研究的一些内容。第1节介绍了相关的名称术语;第2节对每种访问控制模型进行介绍和分析;第3节介绍了一种标准的访问控制策略描述语言;最后总结并指出值得研究的一些内容。

1 相关知识介绍

在介绍现有访问控制模型及其特点之前,首先对文中相关的名称术语进行说明^[26]。

(1)主体(Subject) 是指一个提出访问请求或要求的实体,是动作的发起者。主体可以是用户或其它任何代理用户

到稿日期:2009-12-31 返修日期:2010-03-16 本文受国家自然科学基金(60773201)资助。

韩道军(1979—),男,博士生,讲师,主要研究方向为机器学习、形式概念分析、软件工程, E-mail: hdj@henu.edu.cn; 高 洁(1978—),女,博士生,主要研究方向为机器学习、数据库与知识库; 翟浩良(1983—),男,博士生,主要研究方向为智能规划、软件工程、信息安全; 李 磊(1951—),男,教授,博士生导师,主要研究方向为数据库与知识库。

行为的实体(如进程、作业和程序)。

(2)客体(Object) 是接受其它实体访问的被动实体。凡是可以被操作的信息、资源、对象都可以认为是客体,如表、文件等。

(3)操作(Operation) 是指主体对客体的一种行为,如读、写等。

(4)许可(权限):许可(Permission) 是指可以对哪个客体进行何种操作。

许可是一个关于操作和客体的二元组,其关系可以描述为 $P = \langle Op, O \rangle$,其中 P 表示许可, Op 表示操作、读、写、修改等; O 表示客体,如文件、流程等。许可和通常所说的权限(Rights)意义相同,本文在不同环境下使用不同的术语。

(5)授权(Authorization) 是指为主体分配、指定权限的过程。主体被授权后,就能在权限范围内进行对客体的访问操作。授权一般是由系统安全人员进行的,如为用户分配权限、为角色分配权限。

2 访问控制模型介绍

2.1 访问控制矩阵

访问控制矩阵^[14] (Access Control Matrix, ACM)是出现较早的一种访问控制方式。该模型比较简单,列举系统中的主体和客体,组成一个矩阵。常见的一种描述方式如下:将客体作为列,将主体作为行,矩阵元素表示对应的列(客体)与行(主体)之间的操作关系,是一个集合,如读、写、执行等。表1为一个ACM示例。

表1 一种访问控制矩阵示例

	文件1	文件2	文件3	程序1
张三	读;写	读		执行
李四	读		读;写	
王五		读		读;执行

ACM作为一种简单的访问控制方式,在一些简单系统(主体和客体不太多)中可以很好地使用,能够为资源的保护提供一种保障。访问控制矩阵由系统管理员建立和维护,普通用户只能查询本身所拥有的权限,而无其他操作权限。

ACM的优缺点分析如下。优点:表现直观,容易理解,容易查询;缺点:没有一个通用的算法去证明系统的安全性,修改和删除麻烦,可能会引起连锁反应,矩阵一般很大、无法描述约束和带有条件的权限,客体粒度较粗。

2.2 自主访问控制

自主访问控制^[14] (Discretionary Access Control, DAC)是一种较灵活的访问控制技术,易于实现。自主访问控制在访问控制矩阵的基础增加了“自主”特性,这种特性就是任何一个被授权的主体都能自主地将自己所拥有的权限授权给其他的主体或回收他所授予的访问权限而不需要通过系统安全员的允许。这种方式极大地增加了授权管理的灵活性,分散了系统安全管理人员的工作量,任何人都可根据工作的需要在自己的权限范围内进行需要的权限设置。但这样的特性也带来了一些负面的影响,集中表现在系统安全管理员可能很快失去对授权状况的控制,他们将很难了解系统中的授权情况。

在实现方式上,自主访问控制技术主要从两个角度来实现^[26]。

一方面是以主体为核心进行管理,主要描述一个主体对

系统中的各资源拥有怎样的访问操作功能。主要的实现方法分别是:(1)定义一系列的受保护的客体标示,每个标示都代表了一个具体的操作,主体只有在拥有了标示才具有对客体进行相应操作的能力;(2)基于安全口令,将第一种方法中的安全标示用口令进行置换,凭口令获取权限;(3)采用安全配置文件,就是为每个用户对客体的访问操作权限使用一个配置文件进行描述,通过配置文件来确定主体对客体的操作能力。

另一方面是以客体为核心进行管理,主要描述一个客体被哪些主体访问,以及访问该客体的各主体可以进行的操作。主要有两种实现方法,分别是:(1)定义保护位来实现访问控制,保护位是对访问控制矩阵信息的一种不完全表达方式。它将不同的位“bit”与不同的主体相对应。(2)采用访问控制列表(Access Control List, ACL),该列表可以对某个特定资源指定任意一个用户的访问权限,还可以将有相同权限的用户分组,并授权用户组的访问权限。

DAC的优缺点分析如下。优点:授权灵活,较为直观,容易实现;缺点:很难进行授权管理,授权主体无法完全控制权限,DAC机制易遭到特洛伊木马攻击,在大型系统中主、客体的数量巨大,使用DAC将使系统开销大到难以支付的程度。

2.3 强制访问控制

强制访问技术^[14,26] (Mandatory Access Control, MAC)主要用于多层次安全级别的军事应用当中,它预先定义用户的可信任级别及信息的敏感程度(安全级别)。当用户提出访问请求时,系统对两者进行比较,以确定访问是否合法。安全级别是由安全管理员分配,具有强制性,用户或用户进程不能改变自身或其它主/客体的安全级别。MAC的本质是基于格的非循环单向信息流政策,系统中每个主体都被授予一个安全级别,而每个客体都被指定为一定的敏感密级。MAC的两个关键规则是不向上读和不向下写,即信息流只能从低安全级向高安全级流动,任何违反非循环信息流的行为都是禁止的。MAC主要用于多层次安全级别的军事系统中。

图1^[14]为一个MAC示例,图中的 TS 和 S 表示安全级别,且 $TS > S$ 。

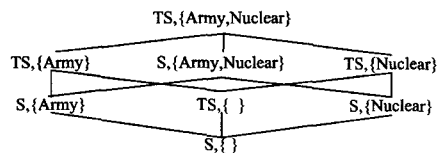


图1 格结构安全级别示例

MAC的优缺点分析如下。优点:安全性较,可控程度较高,保密性强,可以有效地阻止特洛伊木马的泄露;缺点:实现工作量较大,对用户恶意泄漏信息无能为力,过于强调保密性,不够灵活;描述安全策略很难,不满足最小特权原则,权限很难进行动态变化,较难管理。

2.4 基于角色的访问控制

基于角色的访问控制^[17] (Role-Based Access Control, RBAC),在用户(user)和访问权限(permission)之间引入角色(role)的概念,用户与特定的一个或多个角色相关联,角色同一个或多个访问权限相关联,角色可以根据实际的工作需要生成或取消,而且登录到系统中的用户可以根据自己的需要来动态激活自己拥有的角色。在RBAC中,通过分配和取

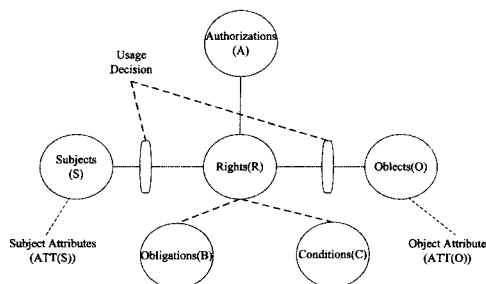
RBAC的发展现在已比较成熟,并且在许多大型系统中得以实现,同时提出了很多扩展模型。2001年8月,美国国家标准技术研究院(National Institute of Standards and Technology, NIST)发表了RBAC建议标准,综合了该领域众多研究者的研究成果,描述了RBAC系统最基本的特征,旨在提供一个权威的、可用的RBAC参考规范,为RBAC的进一步研究指明了方向。

```

graph LR
    USERS((USERS)) -- "User Assignment (UA)" --> ROLES((ROLES))
    ROLES -- "Role Hierarchy (RH)" --> ROLES
    ROLES -- "Permission Assignment (PA)" --> OPS_OBS([OPS, OBS])
    OPS_OBS -- "PRMS" --> OPS_OBS
    SESSIONS((SESSIONS)) -- "user_sessions" --> USERS
    SESSIONS -- "session_roles" --> ROLES
  
```

RBAC的优点是实现了用户与权限的分离,支持角色层次,可描述静态和动态访问约束,与策略无关,支持最小特权原则,安全管理较简单,实用性强。其缺点是模型只对主体特征进行描述,缺乏对客体特征的描述,权限无法动态变化,约束粒度较大,可扩展性不强,难以应用在分布式环境中。

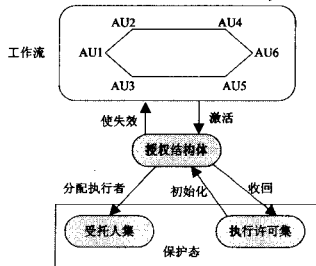
传统访问控制模型(比如自主访问控制、强制访问控制和基于角色访问控制)一个突出的局限性就是仅仅关注访问控制的授权过程。使用控制(Usage CONtrol, UCON)模型^[12, 13, 24, 25],除了授权过程的基本元素以外,还包括义务和条件两个元素。当主体提出访问请求时,授权(Authorization)组件(决策引擎)将根据主体请求的权限,检查主体和客体的安全属性,比如主体身份、角色、安全类别和客体的安全标签等,从而决定该请求是否被允许。义务(Obligation)就是在访问请求执行以前或执行过程中必须由义务主体履行的行为,比如用户需要从某个网站下载某个文件时,该网站要求用户必须进行注册;或者要求在下载过程中点击若干个广告。另外,访问请求的执行必须满足某些系统和环境的约束,比如系统负载、访问时间限制等,这些就称为条件(Condition)。UCON亦称为ABC模型,其一种描述方式如图4^[12]所示。



UCON 的优缺点分析如下。优点:能描述条件和义务,是一个通用模型,能包含其他模型(兼容性强),支持信任管理和数字权限管理,增加了主体属性和客体属性,并且在主体访问过程中加以控制。缺点:没有描述权限的委托,没有一个明确关于管理的描述,缺乏时态描述。

工作流作为开发复杂信息系统一种常见方式,在流程推进中同样面临着访问控制问题,包括流程控制和访问控制在 workflow 中应用访问控制时,传统的访问控制技术显得力不从心。当数据在 workflow 中流动时,执行操作的用户在改变,用户的权限也在改变,这与数据处理的上下文环境相关。采用传统的访问控制技术,如 DAC、MAC,则难以做到这一点,若采用 RBAC,也需要频繁地更换角色,且不适合 workflow 的运转。因此,有必要采用一种新的访问控制模型。

基于任务的访问控制(Task-Based Access Control, TBAC)是一种新的安全模型^[1,22,32],从应用和企业层角度来解决安全问题(而非传统从系统的角度)。它采用“面向任务”的观点,从任务(活动)的角度来建立安全模型和实现安全机制,在任务处理的过程中提供动态、实时的安全管理。在TBAC中,对象的访问权限控制并不是静止不变的,而是随着执行任务的上下文环境发生变化,这是我们称其为主动安全模型的原因。具体说来,TBAC有两点含义。首先,它是在工作流的环境中考虑对信息的保护问题。在工作流环境中,每一步对数据的处理都与以前的处理相关,相应的访问控制也是这样,因而TBAC是一种上下文相关的访问控制模型。其次,它不仅能对不同工作流实行不同的访问控制策略,而且能对同一工作流的不同任务实例实行不同的访问控制策略。这是“基于任务”的含义,所以TBAC又是一种基于实例(instance-based)的访问控制模型。最后,因为任务都有时效性,所以在基于任务的访问控制中,用户对于授予它的权限的使用也是有时效性的。图5^[37]显示了TBAC的模型结构图。



TBAC的优越点分析如下。优点:引入任务,可主动授权,可表示任务状态的变化,适合分布式计算和多点访问控制,支持最小特权和职责分离原则。缺点:任务和角色无法明

确分离,不支持被动访问控制,不支持角色层次。

2.7 面向服务的访问控制

在面向服务架构的分布式系统中,提出请求的主体和提供服务资源的客体都具有较高的动态特性。主体动态特性是由于主体操作方式的多样性和用户计算环境的异构性造成的。服务本身的动态特性表现为:服务提供的功能可能扩充或被修改,服务的组成也具有动态的变动性。这就要求访问控制系统应该能够动态地适应这种变化,能够根据安全相关的环境做出其访问控制决策^[28-30,33,35]。面向服务的访问控制模型(Service-Oriented Access Control, SOAC)主要适用于基于面向服务的体系结构(Service Oriented Architecture, SOA)而开发的软件系统。图 6^[28]为一种面向服务的访问控制模型。另外,可将面向服务的访问控制看作是对 TBAC 的一种改进,基本实现方式类似,只是把原来的任务限制换成服务。

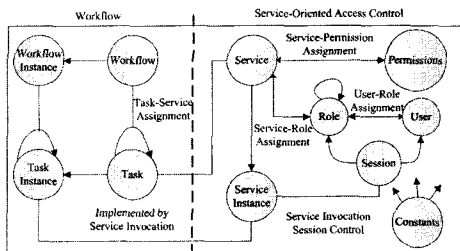


图 6 SOWAC 模型及其与工作流的关系

SOAC 的优缺点分析如下。优点:考虑动态特性,解决“最小特权原则”。缺点:适用领域受限,使用起来较为复杂。

2.8 基于属性的访问控制

ABAM^[16]用属性值元组来描述访问矩阵中行和列对应的主体和客体,并用关于属性的谓词来描述指令执行条件,通过指令来修改系统状态,然后在指令和属性满足某个特定条件下,ABAM 的安全问题是可判定的。在 ABAM 描述的基础上,可将其扩展至统一框架——基于属性的访问控制(Attribute-Based Access Control, ABAC)^[8-11,16]。ABAC 是目前的一个研究热点,表示能力较强,可以作为一种统一访问控制框架,且有相应的访问控制语言 XACML 提供支持。

ABAC 中的基本元素包括请求者、被访问资源、访问方法和条件,将这些元素统一使用属性来描述,而且各个元素所关联的属性可以根据系统需要定义。属性概念的引入,可以将访问控制中对所有元素的描述统一起来,提供一种统一描述的框架。RBAC 通过引入角色中间元素,使得权限先经过角色进行聚合,然后将权限分配给主体。通过这种方式可以简化授权,可将角色信息看成是一种属性,这样 RBAC 就成为了 ABAC 的一种单属性特例。

一种典型的 ABAC 框架如图 7 所示^[17]。

在 ABAC 中,一次访问控制判定过程如下。PEP 接收原始访问请求(NAR),再根据 NAR,利用不同的属性权威(AA)中存储的属性信息构建一个基于属性的访问请求(AAR)。AAR 描述了请求者、资源、方法和环境属性,PEP 将 AAR 传递给 PDP, PDP 根据从 PAP 处获取的策略判定 AAR,并将判定结果传给 PEP, PEP 执行此访问判定结果。

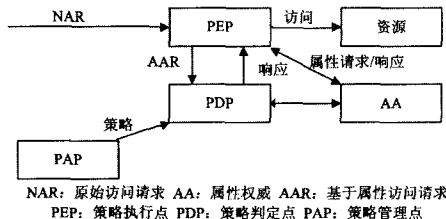


图 7 ABAC 框架示意图

ABAC 的优缺点分析如下。优点:框架式,可与其他访问控制模型结合(如 RBAC)。缺点:所有要素均需要以属性形式进行描述,一些关系用基本的属性不易描述。

2.9 其它访问控制模型介绍

除了上面提到的 8 种访问控制模型外,还有其他一些关于访问控制模型的研究。

BLP 模型^[18]是一个严格的基于强制访问控制模型的形式化数学模型,但它包含了 DAC 和 MAC,并且制定了状态转换规则来描述系统的变化。它是用一种计算机可实现的方式来定义,并且能够形式化证明系统的安全性。但 BLP 模型缺乏灵活性,扩展性不强,依赖于制定的规则,信息流动时可能破坏数据完整性,且不符合最小特权原则。

BIBA 模型^[19]也是基于强制访问控制模型而定义的。但它与 BLP 提供保密性不同, BIBA 模型主要提供对数据完整性的保护。所以它的规则与 BLP 模型刚好相反,是下读和上写。

Chinese wall 模型^[20]是一个多边安全系统的访问控制选择模型,可应用在存在冲突的不同组织的访问控制中。其主要基于两个属性:用户必须选择一个可以访问的区域;用户必须自动拒绝其它与用户所选区域的利益发生冲突的区域访问。

此外,文献[4-7]提出的基于逻辑的信任管理模型具有较大的影响;文献[3,23,27,36]分别对访问控制的灵活性、数学模型、授权语言及寻找通用框架进行研究,以扩充一些模型的表达能力。

2.10 访问控制模型分析对比

以上介绍的访问控制模型,按照一些常规考查指标,可以用表格形式简要描述,如表 2 所列。表格中的符号“√”表示该项性能较好,为空则表示不好或尚未具有该项特征。

表 2 各种访问控制模型比较

	安全性	机密性	直观理解	授权灵活性	最小特权	职责分离	描述能力	控制粒度	上下文环境	约束描述	动态变化	兼容性	扩展性	应用性	管理性	分布式环境
ACM			√	√												
DAC				√												
MAC	√	√						√								
RBAC			√	√	√	√	√			√				√	√	
UCON							√	√	√			√	√			√
TBAC					√	√			√		√			√		√
SOAC					√	√			√		√			√		√
ABAC							√	√	√		√	√	√	√		√

3 策略描述语言介绍

由于访问控制在软件系统中具有重要的作用,需要一种公共的语言来对其策略进行描述,以提供一种公共的访问控制策略开发模式。目前,最重要的访问控制语言为 XACML。XACML(eXtensible Access Control Markup Language,可扩展的访问控制标记语言)是一种基于 XML 的开放标准语言,它设计用于描述安全策略以及对网络服务、数字版权管理(DRM)和企业安全应用信息进行访问的权限。XACML 在 2003 年 2 月由结构化信息标准促进组织(OASIS)批准,开发用于标准化 XML 的访问控制。

值得说明的是,XACML 有一种称为袋子(bag)的特殊数据类型。袋子是允许重复的无序集合。AttributeDesignator 总是返回袋子,即使只有一个返回值。一旦返回一个袋子,就将对袋子中的值与预期值进行比较,以便作出授权决策。该种类型大大提高了 XACML 的描述能力,能够进行常见的集合运算,从而扩充了语义表达能力。

作为国际标准化组织制定的安全策略描述标准,XACML 最大的优点就在于它提供了统一的策略描述语言,提高了 Web 环境下不同组织之间协同工作的效率。XACML 能适应多种应用环境,支持广泛的数据类型和规则联合算法,策略表达能力很强,可用来描述各种复杂的和细粒度的访问控制安全需求。另外,XACML 的异构性和扩展性强,可重用,可强制进行义务操作,考虑了上下文和环境的变化,能描述 RBAC 策略。但是,XACML 在进行安全策略表达时,标签定义比较复杂,且其核心规范认为所有的策略都是可信的,无法适用于委托授权和可信计算,也无法提供一个形式化的机制来联合 Web 服务中不同部分的安全策略。XACML 可以与另一个 OASIS 标准安全性断言标记语言(SAML)协同工作。它的缺点是描述角色继承关系时策略存在冗余,不能充分支持职责分离原则。XACML 的策略语言模型如图 8 所示,体现了各个组件及组件之间的关系。

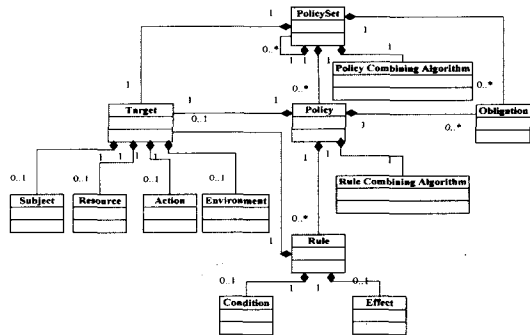


图 8 策略语言模型

结束语 随着计算机应用的普及,各类系统层出不穷,访问控制研究还将面临新的挑战。找到一种维护代价小、表达能力强、高效率的访问控制模型,仍然是当前及近一段时间的重点任务。目前的各种模型都有各自的特点及适用范围。在文献[34]中,指出了当前一段时期内的研究重点,主要是分布式系统(包括工作流)、P2P、无线网络、可信计算中的访问控制研究,亦即和具体的环境相结合,找出合适的访问控制模型。另外,在复杂信息系统中,角色和用户个体的权限有时会

产生冲突(比如某个用户在某些特殊的情况下不具有所属角色的操作权限),从模型上思考,这也是需要解决的一个问题。

参考文献

- [1] Oh Sejong, Park Seog. Task-role-based Access Control Model[J]. Information System, 2003, 28: 533-562
- [2] Wang L Y, Wijesekera D, Jajodia S. A logic-based framework for attribute based access control[C]// Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering. 2004: 45-55
- [3] Barker S, Stuckey P J. Flexible access control policy specification with constraint logic programming[J]. ACM Transaction on Information and System Security, 2003, 6(4): 501-546
- [4] Li Ninghui, Mitchell J C, Winsborough W H. Design of a role-based trust management framework[C]// Proceedings of the 2002 IEEE Symposium on Security and Privacy. 2002: 114-130
- [5] Li Ninghui, Grosz B N, Feigenbaum J. Delegation Logic: A logic-based approach to distributed authorization[C]// ACM Transaction on Information and System Security (TISSEC). February 2003
- [6] Li Ninghui, Mitchell J C. RT: A role-based trust-management framework[C]// The Third DARPA Information Survivability Conference and Exposition (DISCEX III). April 2003
- [7] Li Ninghui, Winsborough W H, Mitchell J C. Beyond proof-of-compliance: Safety and availability analysis in trust management[C]// Proceedings of the 2003 IEEE Symposium on Security and Privacy. May 2003
- [8] Frikken K, Atallah M, Li Jiangtao. Attribute-based Access Control with Hidden Policies and Hidden Credentials[J]. IEEE Transactions on Computers, 2006, 55(10)
- [9] Priebe T, Dobmeier W, Kamprath N. Supporting Attribute-based Access Control with Ontologies[C]// Proc. of the IEEE First International Conference on Availability, Reliability and Security (ARES'06). Vienna, Austria, IEEE Computer Society Press, 2006
- [10] Bobba R, Fatemeh O, Khan F, et al. Using Attribute-Based Access Control to Enable Attribute-Based Messaging[C]// Annual Computer Security Applications Conference (ACSAC'06). Miami Beach, FL, December 2006
- [11] Shen Hai-bo, Hong Fan. An Attribute-Based Access Control Model for Web Services[C]// Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06). 2006
- [12] Park J, Sandhu R. The UCON_{ABC} Usage Control Model[J]. ACM Transactions on Information and System Security, 2004, 7(1): 128-174
- [13] Sandhu R, Park J. Usage Control: A Vision for Next Generation Access Control[C]// MMM-ACNS 2003. LNCS 2776, 2003: 17-31
- [14] Focardi R, Gorrieri R, et al. Access Control: Policies, Models, and Mechanisms[C]// FOSAD 2000. LNCS 2171, 2001: 137-196
- [15] Yang Naikuo, Barringer H, Zhang Ning. A Purpose-Based Access Control Model[J]. Journal of Information Assurance and Security, 2008, (1): 51-58

不仅要求诸如任务分配等预处理的效率上要高速,同时在网格网的通信时间上也要达到最小,这就有效提高了任务调度的速度。在实际情况中,两个条件同时满足的情况不一定能出现,因此需要构造一个包含这些要求的综合性的代价函数,最简单的方式是根据所需网格计算的用户的实际需求,给每一个分量进行加权后构成一个线性组合函数,求该组合函数的极值的方式选择具体的任务调度,从而获得相对较优的调度实施途径。

简要归纳智能化调度实现流程的主要步骤,大致有如下几步:

第一步 网格网用户在所在网格网节点上提出网格计算的任务要求。

第二步 系统根据任务要求,确定任务规模,并把任务进行分割、标注、编码等预处理,获得任务分配函数 $F(n_1, n_2, \dots, n_i, \dots, n_j)$, 其中 $n_i, i=1, 2, \dots, j$ 为预处理后的子任务模块。

第三步 根据网格网用户要求,构造包含多目标要求的综合代价函数。

第四步 调用资源函数 $G(m_1(k_1), m_2(k_2), \dots, m_i(k_i), \dots, m_j(k_j))$, 并与任务分配函数建立映射关系,每一个映射关系就对应一个综合代价函数的值。

第五步 根据综合代价函数的极值,得到要选的任务调度方案。并由此方案,再把子任务模块分配到每一个对应的处理器,各处理器进一步可各自展开计算等处理。

这些步骤中,第五步因需要求综合代价函数的极值,故最能体现任务调度智能化的特色。

结束语 网格网系统的任务调度是网格计算中的主要核心技术之一,智能化调度不仅在提高网格网系统的资源利用

率方面能有效避免不必要的损耗,更体现在能有效提高网格网系统的运算速度,同时对于提高系统的有效性和可靠性也可起到非常重要的作用。

本文对网格网任务智能化的调度展开了研究,不仅讨论了网格网智能化调度所需要的基本条件,而且还针对网格网系统的结构在异构特质条件下,提出了一种可行的智能化调度实现方案,把智能化调度过程转化为求多目标要求的综合代价函数的极值,这种调度方式便于实现,对提高网格网系统的性能可起到促进作用。

网格计算是计算机科学的发展的一个新的分支,通过对网格系统中的诸如智能化任务调度技术、网格互联技术等关键技术的研究和开发,可从根本上认识网格计算技术的本质,并获得新的成果。

参 考 文 献

- [1] Douglass F, Foster I. The Grid Grows Up [J]. IEEE Internet Computing, 2003
- [2] 洪学海, 许卓群, 丁文魁. 网格计算技术及应用综述[J]. 计算机科学, 2003, 30(8): 1-5
- [3] El-Rewini H, Abd-El-Barr M. 先进计算机体系结构与并行处理[M]. 陆鑫达, 林新华, 翁楚良, 译. 北京: 电子工业出版社, 2005: 127
- [4] Chen S, et al. A Selection Theory and Methodology for Heterogeneous Supercomputing[C]//Proc. Workshop on Heterogeneous Processing, Los Alamitos, CA: IEEE CS Press, 1993: 15-22
- [5] Freund R, Siegel H. Heterogeneous Processing[J]. IEEE computer, 1993, 26: 13-17
- [6] 尹绍锋. 访问控制技术研究与应[D]. 长沙: 湖南大学, 2008
- [7] 钟勇, 秦小麟, 郑吉平, 等. 一种灵活的使用控制授权语言框架研究[J]. 计算机学报, 2006, 8: 1408-1418
- [8] 徐伟, 魏峻, 李京. 面向服务的工作流访问控制模型研究[J]. 计算机研究与发展, 2005, 42(8): 1369-1375
- [9] 朱一群, 李建华, 张全海. 一种面向 Web 服务的动态分级角色访问控制模型[J]. 上海交通大学学报, 2007, 41(5): 783-796
- [10] 许峰, 赖海光, 黄皓, 等. 面向服务的角色访问控制技术研究[J]. 计算机学报, 2005, 28(4): 686-693
- [11] 沈海波, 洪帆. 访问控制模型研究综述[J]. 计算机应用研究, 2005, 6: 9-11
- [12] 陈晓苏, 魏林, 肖道举. 面向任务的 RBAC 扩展模型研究[J]. 华中科技大学学报: 自然科学版, 2005, 33(8): 34-36
- [13] 曹春, 马晓星, 吕建. SCoAC: 一个面向服务计算的访问控制模型[J]. 计算机学报, 2006, 29(7): 1209-1216
- [14] 林闯, 封富君, 李俊山. 新型网络环境下的访问控制技术[J]. 软件学报, 2007, 18(4): 955-966
- [15] 邵晓燕, 邵贝恩. 基于 SOA 的企业应用跨安全域访问控制[J]. 清华大学学报: 自然科学版, 2009, 49(7): 1050-1053
- [16] 单智勇, 孙玉芳. 通用访问控制框架扩展研究[J]. 计算机研究与发展, 2003, 40(2): 228-234
- [17] 宋振. 基于角色和任务的权限管理扩展模型研究与应用[D]. 长沙: 长沙理工大学, 2008

(上接第 33 页)

- [16] Zhang X, Li Y, Nalla D. An attribute-based access matrix model [C]//Proceedings of the 2005 ACM Symposium on Applied Computing, 2005: 359-363
- [17] Sandhu R, Coyne E J. Role based access control models [J]. IEEE Computer, 1996, 29(2): 38-47
- [18] Bell D E, La Padula L J. Secure Computer System: Unified exposition and multics interpretation[R]. MTR-2997. Revision 1, The MITRE Corporation, 1976
- [19] Biba K J. Integrity considerations for secure computer systems [R]. MTR-3153. The MITRE Corporation, 1977
- [20] Brewer D F C, Nash M J. The Chinese Wall security policy[C]//Proceedings of the 1989 IEEE Symposium on Security and Privacy, 1989: 206-214
- [21] 李晓峰, 冯登国, 陈朝武, 等. 基于属性的访问控制模型[J]. 通信学报, 2008(4): 90-98
- [22] 邓集波, 洪帆. 基于任务的访问控制模型[J]. 软件学报, 2003, 14: 76-82
- [23] 林莉, 怀进鹏, 李先贤. 基于属性的访问控制策略合成代数[J]. 软件学报, 2009, 2: 403-414
- [24] 崔永泉, 洪帆, 龙涛, 等. 基于使用控制和上下文的动态网格访问控制模型研究[J]. 计算机科学, 2008, 35(12): 37-41
- [25] 戴刚. 基于使用控制和上下文的模糊访问控制模型研究[D]. 重庆: 重庆大学, 2009