第34卷 第13期 计 算 机 工 程 2008年7月
Vol.34 No.13 Computer Engineering July 2008
·软件技术与数据库· 文章编号：1000—3428(2008)13—0040—03 文献标识码：A 中图分类号：TP311

协同设计中层次访问控制模型的研究

严 巍[1]，黄志球[1]，刘 毅[2]，王 凯[2]
(1. 南京航空航天大学计算机系，南京 210016；2. 南京航空航天大学航天学院，南京 210016)

摘 要：访问控制是系统安全的重要技术，但在协同设计中应用较少。该文提出一个基于零件层次建模的多层访问控制框架用于协同设计，其中的层次权限模型为3D图形设计提供了部件层和特征层的多级访问许可，通过结合层次权限概念和传统的角色访问控制，实现基于角色的扩展层次访问控制模型。

关键词：协同设计；基于角色的访问控制模型；层次权限模型

Research of Hierarchy Access Control Model in Collaborative Design

YAN Wei [1], HUANG Zhi-qiu[2], LIU Yi[2], WANG Kai[2]
(1. Department of Computer Science, Nanjing University of Aeronautics & Astronautics, Nanjing 210016;
2. College of Aeronautics, Nanjing University of Aeronautics & Astronautics, Nanjing 210016)

【Abstract】 Access Control is an important technology in system security, but it is new for collaborative design. This paper provides a new framework of multi-level access control based on hierarchical product modeling. A layered privilege model is developed to provide multi-granularity access permissions in the part level and feature level. It implements Role-Based Extended Hierarchy Access Control(RBEHAC) model, which is integrated with layered privilege model and common RBAC.

【Key words】 collaborative design; Role-Based Access Control(RBAC) model; layered privilege model

随着网络技术和计算机辅助设计的迅速发展，工程设计方式在不断改变，工程设计的环境更趋于全球化、网络化、分布化，使得产品设计者的交流沟通更加有效，并能交互大量设计资源。不同地区的设计者之间的协同操作变得愈加重要。在协同过程中，设计者只需要了解其各自设计的部分，无须掌握所有的细节。因此，需要建立一个灵活、安全的访问控制机制，为每个设计者提供不同的安全权限。本文提出一种多层访问控制机制框架来完善安全的协同设计，使多用户在同一产品模型的协同设计中拥有不同的权限。其中的对象层次建模将产品模型分为部件/组件层和设计特征层。

1 相关工作

20世纪70年代，Lampson提出了访问矩阵的概念，并将其成功地应用在操作系统中。Conway等人在对数据的访问控制中也使用了安全矩阵[1]，并将矩阵标准化，从而形成了自主访问控制(DAC)的思想。Denning对安全系统中信息的流向进行了研究，并在1976年提出了格模型理论[2]。该模型将系统中的数据和用户按照安全级别进行分类，禁止高安全级别的数据流向低安全级别的用户，以防止信息的泄漏。这就是强制访问控制(MAC)。在总结前人研究成果的基础上，Sandhu等人在1996年提出了基于角色的访问控制模型(RBAC)[3]，第1次形式化地描述了基于角色的访问控制，并在1997年提出了RBAC的管理模型AR-BAC。这2个模型是经典的基于角色的访问控制模型，被分别称为RBAC96模型和ARBAC97模型。

与DAC和MAC相比，RBAC显示了良好的适应性，并在实际中得到广泛应用，许多研究者对其进行了深入的研究，并提出了一些改进模型。如文献[4]提出了增加权限控制实体方案，文献[5]提出基于负权限概念对RBAC进行约束，结合角色的访问控制与强制访问控制，建立访问矩阵对用户进行访问控制，以及在RBAC中引入属性证书。

综上所述，已有的模型较多地考虑了访问控制的主体(用户/角色)以及访问控制所处的环境(静态/动态)，但很少研究访问控制的客体(受控对象)和操作类型，导致在实际应用中权限定义较为复杂，而且容易产生冲突[6]。下面以实际应用中的问题为例进行说明。

示例 设受控对象为{模具零件流盘，模具零件，阶梯轴，模具零件，配盘}，操作类型为{READ, UPDATE}。要让所有受控对象具有操作类型READ，需要定义以下权限*P*:

define *P*(模具零件，流盘, Read)

define *P*(模具零件，阶梯轴, Read)

define *P*(模具零件，配盘, Read)

当受控对象很多时，如零件有多种特征属性，则需要对各零件特征属性分别定义，权限定义比较复杂。

针对现有3D图形访问控制方法在权限定义时遇到的问题，本文提出基于受控对象的层次关系进行权限定义，对已有的RBAC模型进行改进。

2 对象层次建模

在基于特征的3D建模中，零件作为受控对象是呈树状结构的。任意一个对象(Object)*O*都由一系列部件(Part)*P*组成，一些部件装配为组件(Component)*C*，此外，部件和组件

基金项目：国家“863-706”重大专项基金资助项目“面向飞行器研制的协同设计方法研究与环境实现”(2005AA761020)

作作者简介：严 巍(1982－)，男，硕士研究生，主研方向：计算机支持的协同工作，数据库访问控制，软件工程；黄志球，教授、博士生导师；刘 毅，教授；王 凯，博士研究生

收稿日期：2007-08-09 **E-mail：**silverhero@163.com

可以装配成更高一级的组件，而每个部件由特征(Feature)F构成，特征包括特征属性(如尺寸、位移、颜色)及其他属性。模型如图 1 所示，其中，$O=\{Ci\}\cup\{Pi\}$；$C=\{Ck\}\cup\{Pk\}$；$P=\{Fm\}$。

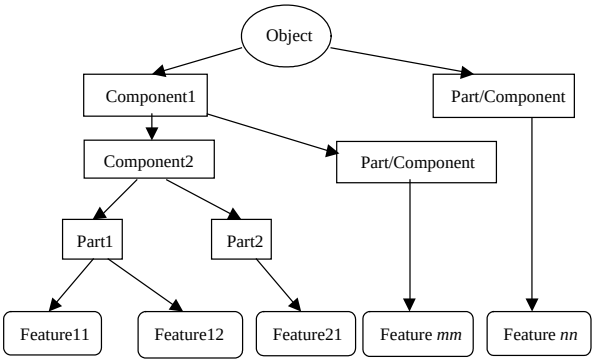


图 1　零件对象层次模型

在协同设计中，多个设计者可以对某一对象同时进行操作。设计者们将被授予该对象中不同组件/部件的操作权限。每个设计者都有一个不同的对象模型，无须知道整个模型的所有细节。因此，在协同环境中需要一个灵活安全的访问控制机制，为每个设计者提供不同的安全权限。在大多数协同装配系统中，当多用户对同一对象模型进行操作时，一般采用严格锁机制作用于部件或者特征上，以解决同步问题。作用于部件，虽然方便实现，但是形式上比较僵硬，不利于进一步安全控制；作用于特征，控制颗粒度太小，使得权限设计过于复杂。下面就对象层次关系提出相应规则。

规则 1　$\forall o1, o2\in O, op\in Op, o1\leq o2: (o2, op)\Rightarrow(o1, op)$

其中，“$\leq$”表示一种偏序关系，$o1\leq o2$ 表示在受控对象的层次树中，$o1$ 位于 $o2$ 的子树中。

规则 1 表示在受控对象的层次树中，受控对象自动继承其祖先所具有的权限。对于第 1 节的示例，模具零件-流盘、模具零件-阶梯轴、模具零件-配盘这 3 个对象可进一步抽象为模具零件。利用规则 1，只须定义一个权限 P(模具零件, Read)，就可以达到问题所定义的 3 个权限具有的效果。

3　扩展层次 RBAC 模型

3.1　基于角色的访问控制模型

在第 2 节的零件层次建模中，受控的零件对象由一组部件和组件构成。为了进行安全的协同设计工作，本文提出了层次权限访问框架，该框架建立在 RBAC 的基础上，如图 2 所示。

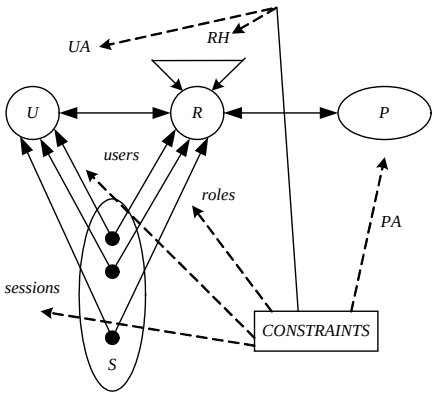


图 2　经典角色访问控制模型框架

RBAC 的基本定义如下：

定义 1　用户集　用户是对系统资源进行访问的独立主体。用 Su 表示用户集合，则有 $u\in Su$。

定义 2　权限集　用户对系统资源(客体)进行访问的许可。用 Sp 表示权限集合，则有 $p\in Sp$。

定义 3　角色集　指一个组织或任务中的工作，它代表一种权利、资格和责任，用 Sr 表示一个角色集合，则有 $r\in Sr$。

定义 4　客体集　客体通常为系统中的文件和目录等资源定义。用 So 表示客体集合，则有 $o\in So$。

定义 5　数据操作集　对数据库系统中数据资源执行的各项操作，如增加、修改、删除。用 Sm 表示数据操作集合，则有 $m\in Sm$ 。

定义 6　许可对角色指派关系 $PA\subseteq P\times R$(多对多关系)。

定义 7　用户对角色指派关系 $UA\subseteq U\times R$(多对多关系)。

3.2　基于角色的扩展层次访问控制模型

在 RBAC 模型中，访问权限 P 与受控对象、操作类型相关联。本文提出了层次权限模型来解决 3D 图形的多维访问控制问题。该模型将权限分成 2 层，高层对应部件权限，低层则对应特征权限。每层都有其不同的定义和属性，第 3 节提到的组件层可以被应用到一些场景中，但会使访问控制模型变得更加复杂，从而造成不便，因此，本文将部件作为最大的访问控制单位。

在传统 RBAC 模型的基础上进一步扩展其定义：

定义 8　部件权限(Part Privilege)PP

$(part, type, flag)\in PP$

其中，$part$ 为受控的部件；$type$ 为访问模式，如 READ 操作、UPDATE 操作；$flag$ 为标识符，包括 all-features, none-features 2 种形式，构成部件的默认特征权限，其中，all-features 表示角色在访问模式 t 的条件下具有访问该部件特征数据的权限；none-features 表示角色在访问模式 t 的条件下不具有访问该部件特征数据的权限。

定义 9　特征权限(Feature Privilege)FP

$(feature, type, flag)\in FP$

其中，$feature$ 为受控部件特征；$type$ 与部件权限一样；$flag$ 标志符有 true 和 false 2 种形式，表示是否具有访问该特征数据的权限。

根据定义 8、定义 9，假设一个零件对象 O 有 4 个部件：

$O=\{P1,P2,P3,P4\}$

每个部件都有各自的特征项：

$P1=\{F11, F12, \cdots, F1i\}$

$P2=\{F21, F22, \cdots, F2j\}$

$P3=\{F31, F32, \cdots, F3m\}$

$P4=\{F41, F42, \cdots, F4n\}$

定义角色 $R1$ 的权限集合为 $SP1$，其中，$P1$ 部件的所有特征都可以读取；$P2$ 部件的所有特征不可以删除；$P3$ 部件的特征除了 $F31$ 以外都可以读取；$P4$ 部件只有特征 $F42$ 可以修改：

$PP1=(P1,$ Read, all-features)

$PP2=(P2,$ Delete, none-features)

$PP3=(P3,$ Read, all-features)

$FP1=(F31,$ Read, false)

$PP4=(P4,$ Update, none-features)

$FP2=(F42,$ Update, true)

$SP1=\{PP1, PP2, PP3, FP1, PP4, FP2\}$

当特征权限与部件权限相符时，默认继承部件权限；如果不相符，则以特征权限为最终修正结果。

定义 10　权限配置 r, pp 和 fp 之间的三元关系，假定 PA

是一个权限配置(privilege assign)关系集合，那么

$(r, pp, fp) \in PA$

表示角色 r 可分配的对应部件权限 pp 和特征权限 fp。

由上述定义可得以下推论:

推论 1 如果角色 r 只拥有特征权限 fp，而没有分配部件权限 pp，则 r 不能进行权限配置。

推论 2 如果角色 r 拥有访问权限 Sp，那么其必然同时拥有部件权限 pp 和对应的特征权限 fp。

由推论 2 可知，只有特征信息而没有部件信息的角色是不能被分配权限的，即这种角色授权信息不足。为了确保权限分配的安全性，引入了事务的概念。

定义 11 事务 角色 r 与相关的部件权限 pp 和对应的特征权限 fp 的三元关系,并将此过程组合成一个逻辑操作单元，以保证权限分配的正确性和完整性。假定 St 是一个事务关系集合，则有

$t = (r, pp, fp) \in St$

推论 3 事务的不可分割性(即原子性)：事务必须全部执行完，即一旦角色 r 分配了特征权限 fp，必须为其分配部件权限 pp；否则，数据库状态回退到操作前，即角色 r 已拥有的特征权限信息。

图 3 给出了扩展层次角色访问控制模型(Role-based Extended Hierarchy Access Control, RBEHAC)的框架，本文主要关注权限的层次控制方面。

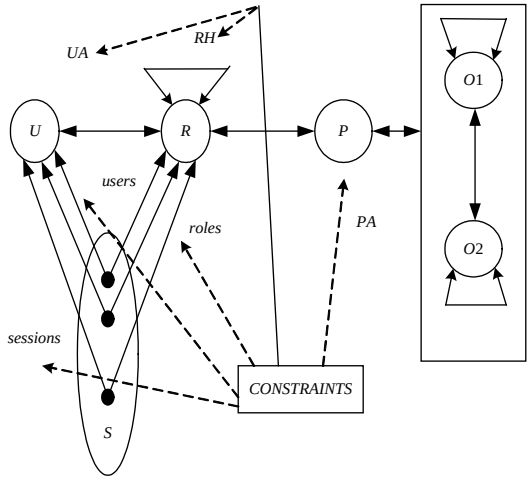


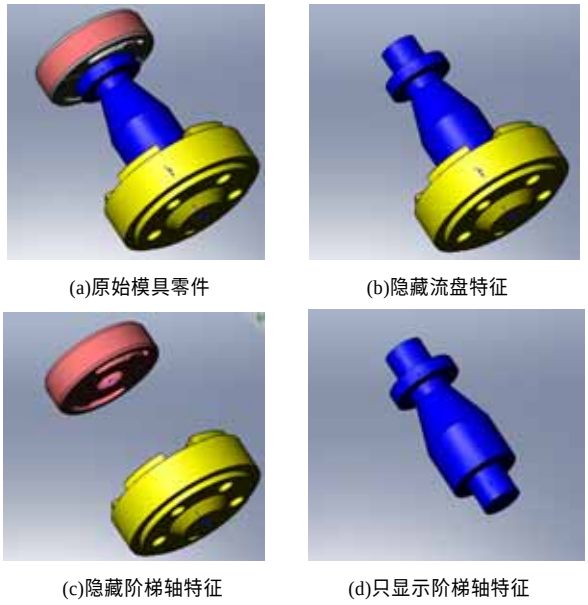
图 3 扩展层次角色访问控制模型框架

在三维制图中，层次权限访问模型较其他普通模型更加直观，因为协同环境中的零件模型一般比较大，而且其访问矩阵的尺寸和密度也很庞大。如果以特征属性作为最大的访问控制单位，那么访问控制将变成一项很巨大的工程；如果以零件的部件作为最大单位，则控制颗粒度过大，不易进行更细微的权限调节。本文的层次模型可以有效缓解这些问题，适应灵活动态模型的不同需求。

4 工程应用

本文的模型在协同设计 CATIA 的二次开发 CAA 的计算系统网络服务和协同装配系统中得到了初步应用。其中，协同特征模型在多层访问控制机制下得以实现。

图 4 是一个模具零件在协同装配中的设计视图，图 4(a)是原始零件模型，包含了所有特征；图 4(b)隐藏了流盘特征；图 4(c)隐藏了阶梯轴特征，因为该设计者没有这个特征的访问权限；图 4(d)只显示了阶梯轴，因为该设计者只有该特征的访问权限。



(a)原始模具零件　(b)隐藏流盘特征

(c)隐藏阶梯轴特征　(d)只显示阶梯轴特征

图 4 协同装配中的模具零件实例

从图 4 中可以看出，本文为协同设计提出一种新的多层访问控制模型。对象模型共分为 2 层：组件/部件层，特征层。根据设计者的权限，层次访问控制模型提供与设计者访问权力对应的特征数据，分别为设计者提供不同的模型视图。

该协同装配系统在 VS2005.NET 平台下基于 Web Service 技术实现。通过 Web 服务的跨平台性、易传输性，很好地将 CAA 扩展程序整合其中，完成了分布异构协同操作平台的设计。

5 结束语

访问控制在各种网络环境中广泛用于限制对资源的访问。在 3D 图像协同设计中，相关工作集中在几何造型模型上。本文提出了协同 3D 特征设计的框架结构，采用的层次模型可高效地建立多层零件模型。层次访问控制模型提出了复合访问权限颗粒度，结合传统的 RBAC，将访问许可权限分成部件层和特征层，以更有效地进行多层访问控制。今后的工作是进一步完善本模型，并将其应用到其他工程领域。

参考文献

[1] Conway R, Maxwell W, Morgan H. On the Implementation of Security Measures in Information Systems[J]. Communications of the ACM, 1972, 15(4): 211-220.

[2] Denning D E. A Lattice Model of Secure Information Flow[J]. Communications of the ACM, 1976, 19(5): 236-243.

[3] Sandhu R, Coyne E, Feinstein H. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

[4] Kern A. Rule Support for Role-based Access Control[C]// Proceedings of ACM SACMAT'05. Stockholm, Sweden: ACM Press, 2005.

[5] 周　伟, 陈小安, 罗天洪, 等. 面向协同装配设计的基于角色显示的研究[J]. 计算机集成制造系统, 2007, 13(1): 88-92.

[6] 李成锴, 詹永照, 茅　兵, 等. 基于角色的 CSCW 系统访问控制模型[J] . 软件学报, 2000, 11(7): 93-97.