第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0178—02 文献标识码：A 中图分类号：TP309.2

协同企业建模中的动态访问控制方法

王洪秀，王 刚，问晓先，高国安
(哈尔滨工业大学机电工程学院，哈尔滨 150001)

摘 要：为了保证在网络化的协同企业建模系统中对模型的安全访问，需要建立一套有效的访问控制机制。在分析基于角色的访问控制、自主型的访问控制及强制型访问控制的基础上，结合协同企业建模系统的特点，提出在模型节点状态约束下，基于角色和任务的动态访问控制方法。该方法确定用户在建模工作中的岗位、该岗位负责的任务和充当的角色，考察任务中对应的模型节点状态及确定访问权限，利于实现用户与受控对象的细粒度的访问控制。给出了系统的实现方法。

关键词：访问控制；协同企业建模；角色；模型状态

Dynamic Access Control Method in Collaborative Enterprise Modeling

WANG Hong-xiu, WANG Gang, WEN Xiao-xian, GAO Guo-an
(School of Mechatronic Engineering, Harbin Institute of Technology, Harbin 150001)

【**Abstract**】To guarantee access security in network collaborative enterprise modeling systems, establishing access control function is in demand. Based on study of the role-based access control, discretionary access control and mandatory access control, combined with the characteristic of the collaborative enterprise modeling system, a role and task based dynamic access control with limitation of the enterprise model node state is proposed. In this method, user's position, the tasks performed by this position and the role are confirmed, the corresponding model node status are examined. And the access authorization is established. These are convenient for realizing the grained security administration to users and objects. Based on the specification, system realization method is presented.

【**Key words**】access control; collaborative enterprise modeling; role; model state

1 概述

现在企业之间的合作越来越多，为了支持这种多企业协作，在企业建模领域，多企业协同建模开始受到关注。在协同建模过程中会有大量的企业模型信息，而企业模型描述了企业的实际运作情况，对模型数据的保护也就是对企业相关信息的保护，因此，对模型的安全管理非常重要。协同企业建模是一项典型的群组协作，具有下述特点：

(1)建模在协同工作环境中进行，企业模型的访问权限控制复杂。建模任务需要多人协同完成，譬如，企业的某部分模型需要几人共同完成，然后再经过审核、发布等步骤之后才能生效，在此过程中，人员和职责是动态的，职责不同时，其访问权限也不同。出于安全和协同工作的考虑，对处于不同状态下的企业模型节点和属于不同建模者的模型节点都可以采取不同的访问控制策略。

(2)协同建模涉及多企业、多部门，用户间的访问权限差别较大。在建模过程中有很多具有不同职责的用户充当不同的角色，具有不同的访问权限。从安全和协同工作考虑，不同的角色、岗位和用户对各种状态下的模型节点具有不同的访问权限。

因此，为了保证系统安全的有效实现，需要根据协作建模过程，灵活地动态调整协作成员的权限，实现对企业模型访问的控制。

传统的访问控制主要有自主型的访问控制(Discretionary Access Control, DAC)和强制型的访问控制(Mandatory Access Control, MAC)。DAC是在确认主体身份和(或)它们所属组的基础上，对访问进行限定的一种方法，在DAC系统中，受控对象的所有者自主负责赋予和回收其他用户对受控对象的访问权限；MAC则是系统强制主体服从访问控制政策的一种访问控制方法，系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。

目前，在对访问控制的研究中，基于角色的访问控制(Role Based Access Control, RBAC)是一种重要的信息存取机制[1]，它通过用户-角色-权限的三层结构实现了用户与权限的分离，有效地提高了系统安全管理的效率，但缺乏对工作流程的控制机制。国内外很多学者进行了许多相关的研究对其改进，文献[2]在RBAC的基础上提出一种增强的分布式安全工作流模型，将任务集引入传统的RBAC中，克服了RBAC模型中固有的一些缺陷，增强了系统的安全性，文献[3]实现了一个Web WFMS中的授权方案，在该方案中，如果用户被指派了某任务所对应的角色，则该用户就拥有执行该任务所需的权限，但未提供支持权责分离的授权约束机制。文献[4]设计了一种基于角色和任务的访问控制模型。除RBAC外，文

基金项目：国家“973”计划基金资助项目(2003AA413210)
作者简介：王洪秀(1978－)，女，博士研究生，主研方向：企业建模，工作流，协同建模；王 刚，教授；问晓先，讲师；高国安，教授
收稿日期：2007-10-20 **E-mail：**littlestone25@126.com

献[5]根据特定的需求提出基于策略的访问控制。

总的来说，上述访问控制模型都难以实现协同企业建模中访问控制权限的需求，例如 DAC 模型和 MAC 模型不适合这种数据量大、用户众多和控制策略复杂的环境；RBAC 模型仅从访问主体方面进行了研究，没有考虑受控对象的复杂性。针对这种情况，综合协同企业建模系统对用户权限管理的需求，本文提出了模型节点状态约束下基于任务和角色的访问控制，该方法综合考虑了受控对象和访问主体两方面，实施访问控制管理。

2 基于任务和角色的动态访问控制

2.1 访问控制模型

在模型节点状态约束下基于任务和角色的访问控制模型如图 1 所示，其实现了主体对处于某状态下的受控对象(即模型节点)的访问控制。访问控制模型中包括访问主体、模型节点(受控对象)、受控对象状态、访问操作方式和访问许可等要素。访问许可集 P 是用户集 U、受控对象集 O、受控对象状态集 OS、操作集 A 的笛卡尔积所生成集合的一个子集，即 $P \subseteq U \times O \times OS \times A$，只有当存在元素 $(u,o,os,a) \in p$ 时，主体 u 才能对处于 os 状态的对象 o 具有操作 a 的访问许可。

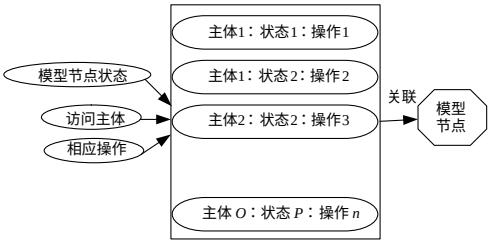

图 1 访问控制模型

2.2 动态访问控制策略实现

从访问控制角度来看，大部分的访问控制模型都采用静态访问控制策略，这些模型在处理某个对象实例访问控制时，没有考虑对象实例所处的状态。而动态访问控制策略是要利用对象实例状态及用户所担当的角色进行访问许可的控制。

2.2.1 访问主体

在访问控制中，主体是最重要的元素之一，主体的形式决定了访问控制模型的特点和管理工作量的大小。访问控制的最终目的是确定某个用户是否具有执行操作的权限，所以，访问控制模型中最直接的主体是用户。在本访问控制模型中，访问主体设为用户，首先给用户指派合适的岗位，用户通过所指派的岗位获得被分配的任务，然后由负责某任务实例的角色来执行它，并在执行任务时获得相应的访问权限，这样方便了对权限粒度的控制和管理。用户、岗位、任务和角色之间的关系如图 2 所示。

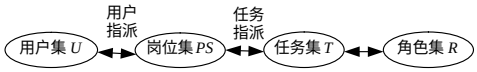

图 2 用户、岗位、任务和角色之间的关系

2.2.2 受控对象及其状态

这里受控对象为模型节点，在建模过程当中模型节点的状态对模型的访问具有约束作用，模型状态不同时，角色对模型的访问权限不同，利于实现细粒度的权限管理。模型节点的主要状态有在建、审核中、预发布、待修改、已发布。图 3 表示企业模型节点的状态变化流程。例如，在建立某食品集团的企业模型时，建模员甲负责建立销售领域的过程模型，当销售过程模型处于“在建”状态时，建模员甲对其有修改(操作)的权限，当该模型处于“审核中”状态时，建模员甲不再对其有修改(操作)权限，而负责该模型审核的审核者乙有批阅(操作)权限。这样就可以实现模型节点不同状态下的动态访问控制策略。

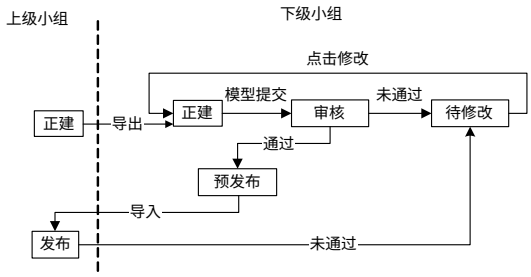

图 3 模型状态变迁

2.2.3 授权流程

为了保证已定义的任务只能被合法的用户执行，必须有一个合适的访问控制机制，应用该机制能够保证授权只有在任务开始执行时才授予，而任务一旦结束，授权就要被收回，从而保证合法的用户在执行某个任务实例时只能拥有该任务实例所允许访问的那些客体的权限。在本文的方法中，授权流程如下：

Step1 系统对用户 u_i 进行身份认证，确认 u_i 是否为建模工具的使用者；

Step2 确定用户 u_i 当前负责的岗位；

Step3 确定该用户目前在该岗位所负责的任务有哪些，并通过任务清单传输给 u_i；

Step4 用户 u_i 在任务清单中选择将要进行的任务 t_i；

Step5 确定针对该任务的角色及任务关联的模型节点 mn_i；

Step6 根据用户 u_i 当前的角色和模型节点的状态，确定其权限；

Step7 任务 t_i 执行结束后，立刻取消与 t_i 相关的所有授权，此时用户 u_i 不再拥有对模型节点 mn_i 的操作权限。

3 系统实现

在协同企业建模系统中，通过用户管理模块来实现对模型节点的访问控制权限，该模块的主要功能包括用户登录、建立新用户、修改权限、查看权限等。当用户登录并通过身份验证后，系统根据用户对应的岗位、岗位负责的任务及针对这个任务的角色、任务对应的模型节点等一系列的判断最终确定用户对模型节点的操作权限(权限集)，不同的用户针对同一模型节点，相同用户在模型的不同状态对模型节点的权限集都会有所变化，如图 4 所示。

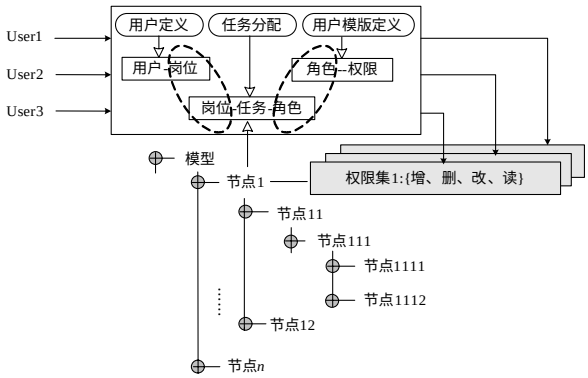

图 4 权限控制示意图

(下转第 182 页)