DOI:10.3969/j.issn.1003-9511.2014.03.012

基于角色的水利行业监理信息系统访问控制优化模型

张柳军[1,2],丰景春[1,2]

(1.河海大学商学院,江苏 南京 211100;2.河海大学项目管理研究所,江苏 南京 211100)

摘要:分析水利行业监理信息系统访问控制现状和存在的问题,在 RBAC 模型及其扩展模型的基础上,提出了主体与角色二次定义的方法,构建了基于角色的访问控制的优化模型,并应用该模型对某水利行业监理企业进行优化设计。结果表明,该模型增加了 RBAC 模型授权的柔性,从而较好地解决了水利行业监理企业信息系统的授权问题。

关键词:水利行业;监理信息系统;RBAC 模型;优化模型

中图分类号:TP391 **文献标识码**:A **文章编号**:1003-9511(2014)03-0048-04

信息化是国家"十二五"规划的重要内容,也是水利行业监理企业提高自身管理效率的重要手段。随着计算机网络和信息技术的发展,水利行业监理管理信息系统在满足企业复杂应用需求的同时面临系统访问控制策略滞后的问题,利用基于角色的访问控制技术虽能在一定程度上优化权限管理,但由于角色与权限的高度耦合,使得已定义主体与角色的内部权限不可再分,导致不能较好地实现主体内部授权与跨角色执行部分权限的问题,难以满足水利行业监理企业实际管理工作的需要,系统访问控制已成为水利行业监理信息系统亟待解决的问题。

访问控制技术出现于 20 世纪 70 年代,最初用于解决大型主机数据共享的访问权限问题[1],经过多年发展,基于角色的访问控制(RBAC)模型以其独特的权限与主体分离的优势得到广泛应用,它通过建立权限与角色、角色与主体之间的映射,实现对系统的访问控制,成为现代访问控制技术研究的基础。目前,尚未提出针对水利行业监理信息系统访问控制问题的有效的访问控制模型。文献[2-4]研究并提出了基于任务的访问控制模型,通过工作流规范业务流程,为每个任务定义相应权限,但由于该控制模型对业务流程的规范性要求较高,难以直接用在水利行业监理信息系统中;文献[5]提出了在基于角色的访问控制(RBAC)模型上建立了时间特性的约束条件,但应用较为单一;文献[6]在时间约束的授权方面进行了深入的研究,并在文献[7]中通过对无时间特性的角色访问控制形式化表达的基础上扩展了时间特性,提出了一种带时间特性的角色访问控制模型;其他访问控制模型大多也是以基于角色的访问控制(RBAC)模型为核心的扩展与衍生,包括具有环境适应性的角色访问控制模型[8]、具有委托功能的角色访问控制模型[9]、具有空间特性的角色访问控制模型[10]等。

综上所述,现有访问控制模型在相关领域内较好地优化了系统访问控制,但由于现有访问控制模型中的权限与角色、角色与主体之间表现为硬性关系,访问控制策略的柔性较差,使其不能较好地适应水利行业监理信息系统的访问控制,难以满足水利行业监理企业的实际工作与信息系统对接的需要。本文在总结分析现有研究成果的基础上,提出主体与角色的内部再分,即"二次定义"的概念,通过对已定义的主体与角色内部的再次定义,即定义二级主体与角色,有效地解决了水利行业监理企业实际工作中信息系统权限分配等问题,并据此建立了基

基金项目:国家社会科学基金重大项目(11&ZD168);江苏省教育厅高校哲学社会科学基金(07SJD630006);国家社会科学基金重点项目(12AZD108);贵州省水利厅科技专项经费项目资助(KT201321);广西水利厅科技项目(201224)

作者简介:张柳军(1990—),男,河南卫辉人,硕士研究生,主要从事项目管理信息化研究。E-mail:1017812119@qq.com

通讯作者:丰景春(1963—),男,浙江金华人,教授,博士生导师,从事管理科学与项目管理信息化研究。E-mail:feng.jingchun@163.com

于二次定义的角色访问控制优化模型。

1 水利行业监理信息系统访问控制现状与问题分析

1.1 现状分析

水利行业监理企业管理一般分为3个层面,分别是领导层、职能层和监理层,如图1所示。

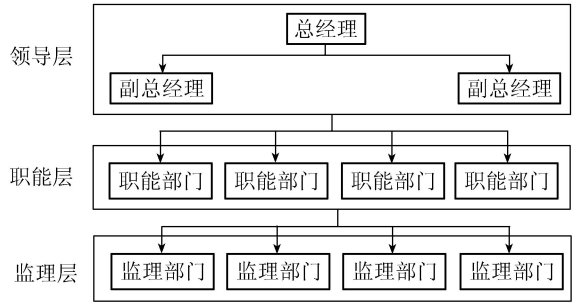


图1 水利行业监理企业组织结构

领导层的主要任务是对企业整体的把握,保证企业良好运营,并负责对报审信息进行审核与审批工作;职能层的主要职能是完成企业日常具体业务需求;监理层是被管理的对象,水利行业监理信息系统数据的重要提供者。RBAC模型出现在自主访问控制(DAC)和强制访问控制(MAC)之后,能够较好地解决DAC的安全性和MAC的局限性问题。通过引入角色的概念,实现主体与权限的分离;通过在权限与角色、角色与主体之间建立映射关系,实现主体访问权限的分配,规范系统的授权管理。

由于水利行业监理企业职能部门具有主体庞大、监理部门管理模式统一等特点,基于角色的访问控制(RBAC)方法存在系统主体与角色定义比较笼统、职能部门和监理部门主体权限过于集中、不能满足实际工作的要求等缺陷,但是过度定义主体与角色又会使授权难以控制。水利行业监理信息系统的访问权限控制大多是根据水利行业监理企业组织结构进行设计的,根据企业所包含的组织机构定义角色,由于监理层定义了监理企业所有的监理部门,且各监理部门自身的管理模式是相同的,因此,一般情况下监理部门所拥有的权限相对固定,在分配角色到主体的过程中通常将监理部门作为一个整体来处理,监理部门内部不允许进行权限与角色、角色与主体的再分配。职能部门虽然可以通过管理员进行授权,但授权方式还是以部门为单位。

1.2 存在的问题

a. 职能部门与监理部门内部权限的不可再分性使得系统的使用权限只属于职能部门和监理部门负责人,权限的过度集中,增加了部门负责人的工作强度,同时也不利于系统职能层与监理层的授权管理,职能部门和监理部门其他人员无法通过使用系统行使自身的实际工作职能,这是RBAC模型无法有效解决水利行业监理信息系统访问控制的主要问题。

b. 角色与权限的映射较为硬性。水利行业监理企业的人员调动较为频繁,包括监理部门人员的相互调动和职能部门与监理部门之间的人员调动等。通过对主体角色的授予与撤销,RBAC模型虽在一定程度上解决了人员变动所带来的权限变化问题,但水利行业监理企业的主体经常需要跨角色执行系统所有或者部分权限,由于所有权限的授予可通过赋予主体角色实现,因此跨角色执行部分权限成为需解决的主要问题。目前RBAC模型中的角色与权限之间的映射较为硬性,不能较好地解决上述问题,无法满足水利行业监理信息系统的实际工作需要。主体跨角色执行权限如图2所示。

图2 主体跨角色执行权限示意图

2 基于角色的访问控制优化模型

2.1 主体与角色的二次定义

主体与角色的二次定义是在主体与角色第一次定义完成后,每个主体和角色依据需要进行第二次定义,定义所得主体权限的总和等于一级主体的权限集。RBAC模型虽然可以定义多个主体与角色,但在水利行业监理企业,一个主体一般是以一个组织存在,组织的职能是由同一角色下不同的个人行使不同的权限实现的,在系统整体层面为每个个人建立角色显然是不合理的,而角色二次定义的目的就在于将同一角色下不同权限授予拥有该角色的同一主体二次定义的不同个体。

2.2 优化模型的建立

目前认可度较高的角色访问控制模型为RBAC96模型,它是在原有RBAC模型的基础上增加了角色的层次关系和约束条件,由权限、角色、主体、会话、层次和约束6部分组成,如图3所示。图中,RH表示角色与角色之间的继承关系;UA表示

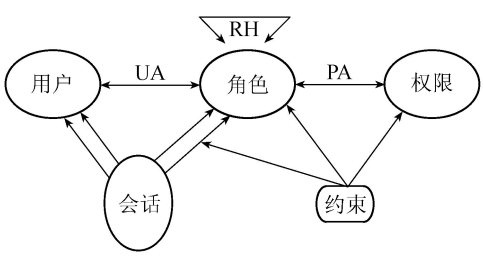


图3 RBAC96模型

一次定义中用户与角色之间的指派关系;PA 表示一次定义中权限与角色之间的指派关系。

本文针对水利行业监理信息系统在访问控制方面存在的问题,对 RBAC96 模型进行优化,即在原有模型的基础上建立了二次定义模型,二次定义模型中的用户、角色和权限的作用域已经发生变化,它是一次定义所产生的某用户及该用户被赋予的某角色和该角色所拥有的权限的集合,如图 4 所示。图 4 中,ua 表示二次定义中用户与角色之间的指派关系;pa 表示二次定义中权限与角色之间的指派关系。

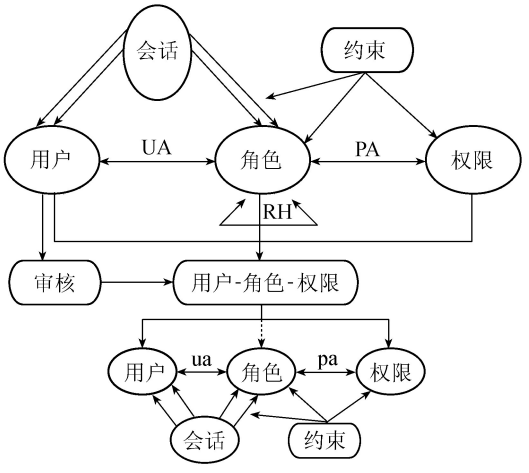


图 4　基于角色的访问控制优化模型

2.3　优化模型的应用

从图 4 中的整体结构上看,该模型分为一级和二级定义,一级定义由系统管理员按照企业管理结构进行设置,二级定义由一级主体按照实际工作需求对主体自身进行再分,对所属角色通过映射关系进行再分,授权方式与现有模型类似,主要区别在于二级授权的用户域、角色域和权限域发生了变化,主体与角色的二次定义及其授权方案通过领导审查后即可生效。该模型较好地解决了原有模型中角色与权限高度耦合的问题,系统访问控制具备一定的柔性,这样不仅能够解决主体内部授权问题,还能满足主体跨角色行使部分权限的要求,从而满足了水利行业监理企业信息系统的实际工作需要。

在水利行业监理企业信息化的应用中,基于角色的水利行业监理信息系统访问控制优化模型的特点主要体现在访问控制的灵活性上,首先由系统开发人员依据企业组织架构建立以组织为单位的角色-权限体系,用户按角色类型获取相关访问权限,该过程是本模型实现访问控制优化的第一阶段,第二阶段的实现是在某一主体-角色-权限这一子体系内进行再次定义,子体系的主体一般是二级定义的实施者,根据主体自身的业务需要,可定义多个子用户与子角色,形成多个子用户-子角色-子权限的访问控制体系,经领导审核通过后,子体系权限便可下放到同一主体的不同个体,实现主体内部的访问控制优化,由于优化的操作是在子体系内进行,对第一阶段的访问控制策略不会产生影响,在增加访问控制灵活性的同时,安全性也不会因此降低。通过案例分析可以对该模型的优化过程形象地进行说明。

3　案例分析

3.1　案例背景

以江苏某水利行业监理企业为例,该企业的业务范围较广,涉及水利工程、水运工程、公路工程等,其监理业务系统访问控制方法是依据较为基础的 RBAC 模型进行设计的,如图 5 所示。

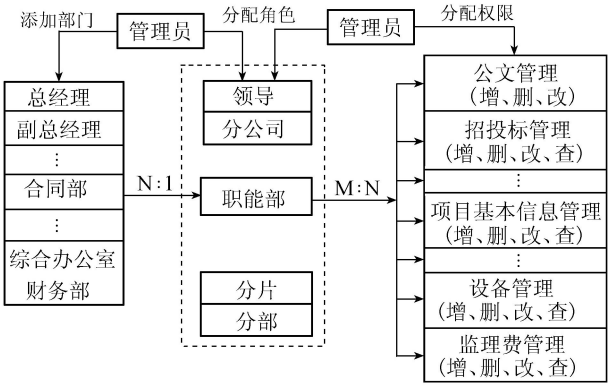


图 5　江苏某监理企业信息系统授权结构

3.2　监理部门授权结构

案例分析中以合同部作为该企业的主体,以职能部作为角色。系统角色是在系统设计阶段按照该企业组织结构进行划分的,并以特定标识存入数据库角色表中;职能部通过管理员添加得到,并由管理员为所添加主体赋予角色;系统权限是依企业需求在系统开发过程中形成并存入数据库权限表中,由管理员针对角色进行分配。监理部是由合同部在创建项目基本信息时自动生成主体,同时被赋予监理部这一角色,并获得该角色下已定义的所有权限,如图 6 所示。

该监理企业信息系统的访问控制方法的优点在于 RBAC 模型能够简化系统访问权限的控制过程,提高了管理员对授权的控制能力和系统自身的安全性,但也存在一定的缺陷,无论是职能部门还是监理部门主体与角色是不可再分的,主体只有拥有角色的全部权限或者无权限两种选择,主体内部其他人员无法被授权访问系统,造成系统与实际工作的脱节。采用二次定义优化后的 RBAC96 模型可在一定程度上解决上述问题,主体与角色的二次定义增加了职能部门和监理部门等主体内部的灵活性。该监理企业信息系统采用二次定义优化后的 RBAC96 模型的授权结构如图 7 所示(以监理部门为例)。

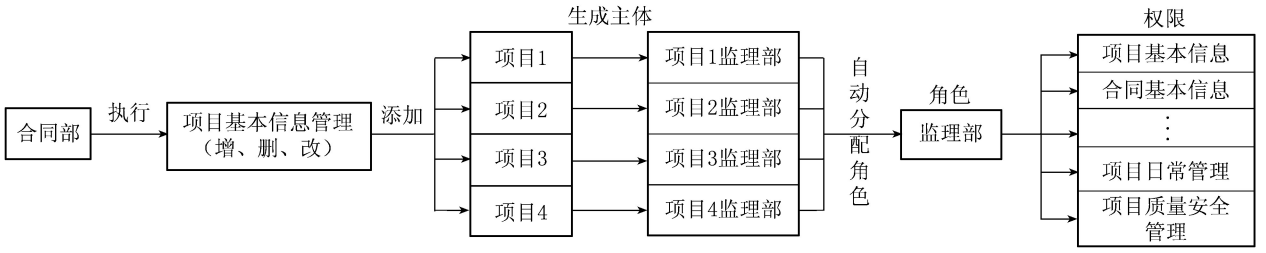


图 6　监理部门授权结构

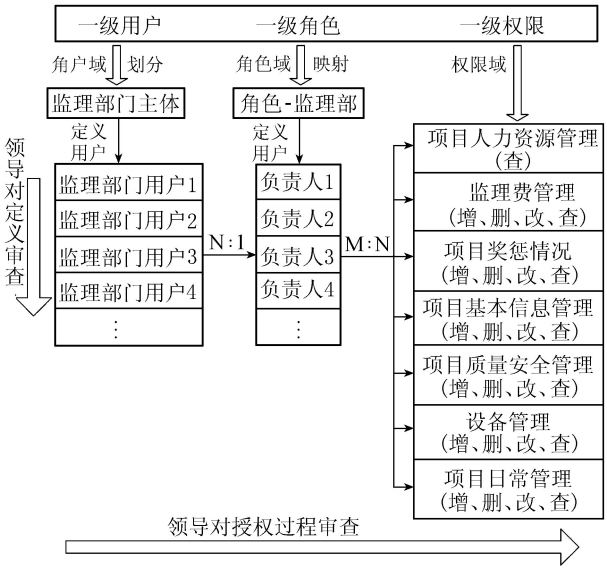


图 7　主体与角色二次定义授权结构

通过图 6 与图 7 两种授权模式的对比可知，基于二次定义的角色访问控制模型在不增加管理复杂度和降低系统安全性的前提下，能够有效地实现水利行业监理企业的访问控制，具有更加灵活的特点，符合现代监理企业实际业务的需求。

4　结　语

访问控制是企业信息化实施过程中不可避免的问题，水利行业监理企业的行业特点使其权限的分配具有一定的复杂性。在现有的研究中，RBAC 模型的主体、角色和权限三者之间表现为硬性关系，无法很好适应水利行业监理信息系统访问控制的需要，水利行业监理企业信息化需要具备一定柔性的访问控制模型。

基于角色的水利行业监理信息系统访问控制优化模型体现了“二次定义”的思想，通过对用户主体与角色的二次定义使主体与角色内部细分，从而便于系统的授权，并且二次定义由主体内部进行，角色二次定义通过映射关系实现，上层授权不会受到干扰。基于角色的访问控制优化模型能够较好地满足水利行业监理企业的实际工作需要，提高了系统的可用性。

参考文献：

[1] 李凤华，苏锑，史国振，等. 访问控制模型研究进展及发展趋势[J]. 电子学报，2012，40(4)：805-813.

[2] COULOURIS G，DOLLIMORE G，ROBERTS M. Role and task-based access control in the PerDiS groupware platform[C]//Proceedings of the 3rd ACM Workshop Role-Based Access Control. Fairfax：ACM Press，George Mason University，1998：115-121.

[3] THOMAS R，SANDHU R. Task-based authorization controls(TBAC)：a family of models for active and enterprise oriented authorization management[C]//. Proceedings of the IFIP WG11. 3 Workshop on Database Security. California：IFIP WG11. 3Conference on Database Security，1997：166-181.

[4] 邓集波，洪帆. 基于任务的访问控制模型[J]. 软件学报，2003，14(1)：76-82.

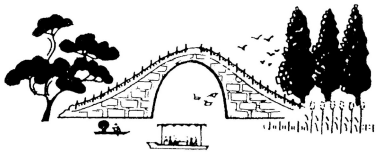
[5] BERTINO E，BONATTI P，FERRARI E. TRBAC：a temporal role-based access control model[J]. ACM Transactions on Information and System Security，2001，4(3)：191-223.

[6] 董光宇，卿斯汉，刘克龙. 带时间特性的角色授权约束[J]. 软件学报，2002，13(8)：1521-1527.

[7] 黄建，卿斯汉，温红子. 带时间特性的角色访问控制[J]. 软件学报，2003，14(11)：1944-1954.

[8] 吴新松，贺也平，周洲仪，等. 一个环境适应的基于角色的访问控制模型[J]. 计算机研究与发展，2011，48(6)：983-990.

[9] 刘正涛，毛宇光，王建东，等. 基于角色的层次受限委托模型[J]. 电子科技大学学报. 2010，39(1)：114-118.

[10] DAMIANI M，BERTINO E，CATANIA B. GEO-RBAC：a spatially aware RBAC[J]. ACM Transactions on Information and System Security，2007，10(1)：1-42.

（收稿日期：2013-10-25　编辑：张志琴）