文章编号：1005-8451（2015）04-0019-04

RBAC在ATP车载设备管理信息系统中的应用

康仁伟，田　青，程剑锋，赵显琼
（中国铁道科学研究院　通信信号研究所，北京　100081）

摘　要：基于角色的访问控制（RBAC）是保证信息系统资源安全的一种策略。本文详细介绍了RBAC模型，并给出了其形式化定义。将RBAC模型应用于ATP车载设备管理信息系统，设计了该系统访问控制的数据物理模型，实现了该信息系统对关键资源的限制访问。该系统成功地投入使用，表明RBAC模型可有效实现信息系统的权限控制。

关键词：ATP；信息系统；访问控制
中图分类号：U284：TP39　**文献标识码：**A

Application of RBAC in Management Information System of ATP on board equipment

KANG Renwei, TIAN Qing, CHENG Jianfeng, ZHAO Xianqiong
(Signal & Communication Research Institute, China Academy of Railway Sciences, Beijing　100081, China)

Abstract: Role-Based Access Control (RBAC) was a means to ensure the security of information system resources. This paper described the RBAC model and given its formal definition. RBAC model was applied to ATP Management Information System, and physical data model of access control was designed. Finally it was implemented restrict access to the critical resources of the System. The System was used successfully, and indicated that RBAC model could effectively control access of Information System.

Key words: ATP; Information System; RBAC

访问控制技术作为国际化标准组织定义的5项标准安全服务之一，是实现管理信息系统安全的一项重要机制[1]。基于角色的访问控制（RBAC，Role Based Access Control）模型是一种较新的访问控制模型，其基本思想是：对系统的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。用户通过被授予一定的角色而获得相应的权限。RBAC解决了具有大量用户、数据客体和各种访问权限的系统中的授权管理问题。

本文介绍RBAC模型的定义，将RBAC模型运用于ATP车载设备管理信息系统（ATPMIS，ATP Management Information System）中，设计该系统访问控制模块的数据模型。防止对信息越权访问、篡改数据和信息的滥用，从而保证该系统安全有序地运行。

收稿日期：2014-09-18
基金项目：中国铁路总公司科技研究开发计划课题（2014X008-H）；中国铁道科学研究院基金课题（2013YJ046）。
作者简介：康仁伟，研究实习员；田　青，工程师。

1　基于角色的访问控制

1.1　RBAC的基本思想

RBAC的核心是引入了角色的概念，它使得操作权限不是直接授予用户而是授予角色，用户通过角色身份获得相应的操作权限[2]。

简单地说，角色授权机制是系统通过特定的操作将用户和资源联接。通过该机制，角色具有一定的权限，同时角色又分配给用户，这样，用户由赋予的角色而获得该角色具有的相应权限。用户与角色、角色与权限之间构成多对多的关系。用户进行系统操作的访问控制流程如图1所示。

图1中，用户通过用户名、密码经过身份验证后进入系统。通过角色服务，获取其角色身份；依据角色身份，获取具体的操作权限。当用户操作某些内置了权限的功能时，需要进行用户访问权限判定，以确认用户是否具有这些操作权限。

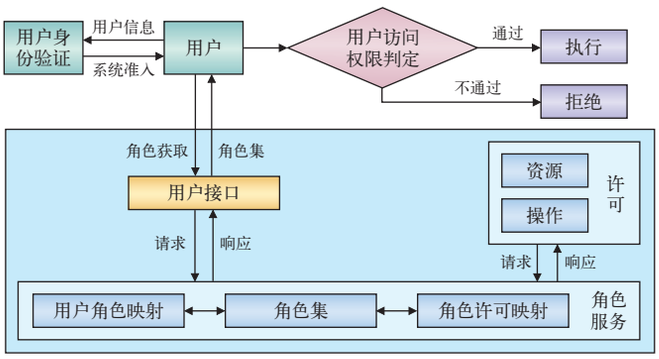

图1　访问控制流程

1.2　RBAC模型

美国国家标准和技术研究所（NIST）定义的RBAC96模型[3~4]包括$RBAC_0$、$RBAC_1$、$RBAC_2$、$RBAC_3$。$RBAC_0$定义了RBAC模型的基本概念，满足RBAC访问控制的最低需求。$RBAC_1$和$RBAC_2$在$RBAC_0$基础上，分别引入了角色继承和约束的概念。$RBAC_3$包括$RBAC_1$和$RBAC_2$模型。

$RBAC_0$是基础，它由4个基本要素构成：用户（U）、角色（R）、会话（S）和授权（P）。

（1）U表示用户集，R表示角色集，S表示会话集，P表示权限集。

$P=2^{OPS\bullet OBS}$其中：OPS、OBS分别表示操作和资源的集合。

（2）$UA\subseteq U\bullet R$，是从用户集到角色集的多对多映射，表示用户被赋予的角色。

（3）$PA\subseteq P\bullet R$，是从权限集到角色集的多对多映射，表示角色被赋予的权限。

（4）$roles(s_i)\subseteq\{r|\ (user(s_i),r)\in UA\}$

其中，roles：$S\rightarrow 2^R$，是会话S到角色集R的映射。User：$S\rightarrow U$，是会话S到用户U的映射。

ATP车载设备管理信息系统中，角色之间具有明显的层次性。RBAC模型用偏序（≥）描述这一层次关系。形式化表示为：

$RH\subseteq R\bullet R$，表示角色继承而形成的角色层次关系。

实际上，角色间的偏序关系体现为角色间的继承关系。$r_1\geqslant r_2$表示r_1继承自r_2，其中r_1为高级角色，r_2为低级角色。通过继承，r_2的所有权限同时也被r_1所拥有，r_1的所有用户同时也是r_2的用户。这种偏序关系满足如下性质：

自反性：$\forall r\in R,\ r\geqslant r$

反对称性：$\forall r_1,r_2\in R,\ r_1\geqslant r_2\cap r_2\geqslant r_1$

$\forall r_1,r_2\in R,r_1\geqslant r_2\cap r_2\geqslant r_1\Rightarrow r_1=r_2$

传递性：

$\forall r_1,r_2,r_3\in R,r_1\geqslant r_2\cap r_2\geqslant r_3\Rightarrow r_1\geqslant r_3$

约束规定了角色被赋予用户，或操作权限被赋予角色时，以及用户在某一时刻激活一个角色时所应遵循的强制性规则。其中，职责分离是其中的一种约束。

职责分离约束是指不允许一个用户同时拥有冲突角色集合中的两个或多个角色，又分为动态职责分离和静态职责分离。

本文重点介绍静态职责分离（SSD，Static Separation of Duty）[1]。其定义为：$SSD\subseteq(2^R\bullet N)$，表示若干二元对(rs,n)的集合。其中$rs\subseteq R$，$n\in N$且$n>1$。SSD关系中，每一个(rs,n)表示为：用户不能同时被赋予rs中的n个或n个以上的角色。

由此，在$RBAC_0$模型的基础上，添加角色分层和约束的概念，得到$RBAC_3$的模型如图2所示。

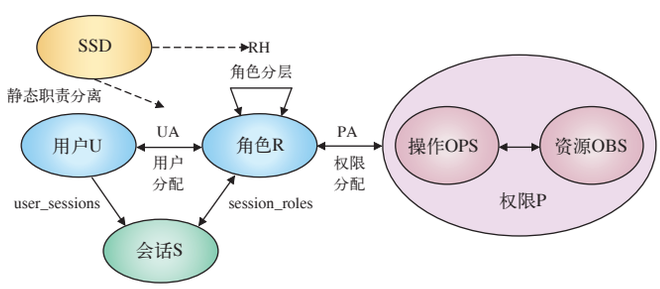

图2　RBAC模型

2　RBAC在ATP车载设备管理信息系统中的应用

ATP车载设备管理信息系统是对列车车载设备的运用和维护进行管理的信息系统。访问控制是用户通过账号、密码进行身份认证之后保护该系统资源安全的又一道屏障。将RBAC模型运用至该系统，可以限制对关键资源的访问，防止非法用户的侵入或者因合法用户的不慎操作所造成的破坏。

2.1　系统需求

ATP车载设备管理信息系统通过权限管理模块实现资源的访问控制。具体包括铁路总公司、铁路局级数据分发权限、终端数据查询权限、基础数据维护权限和系统操作权限。

其中铁路总公司、铁路局级数据分发权限主要包括委托维修数据分发、跨局运行故障上报和动车组转配属数据分发；终端数据查询权限根据动车组配属信息控制各个终端数据访问权限；基础数据维护权限包括基础数据导入、修订和删除等维护工作；系统操作权限包括应用服务器、数据库服务器和系统软件的操作权限。

系统分配给每个用户的权限应该是该用户完成其职能所具有的最小权限的集合。系统不应该给予用户超过其执行任务所需权限之外的任何权限。

2.2 访问控制的实现

ATP 车载设备管理信息系统访问控制的设计流程如下：(1) 设计用户、角色和权限之间的基本关联；(2) 实现角色分层和职责分离的需求；(3) 设计访问控制的数据物理模型。

2.2.1 基本设计

(1) 设角色集合 R={ 管理员，技术专职，工长，…}。

(2) 设定函数 assigned_users(r:R) → 2^U：返回被直接指派到一个角色的用户的集合。形式化表示为：

assigned_users(r)={u ∈ U|(u,r) ∈ UA}

(3) 设定函数 assigned_permissions(r:R) → 2^P：返回被直接指派到一个角色的权限的集合。形式化表示为：

assigned_permissions(r) ={p ∈ P|(p,r) ∈ PA}

(4) 设定函数 session_roles(s:S) → 2^R：返回一个与会话相关联的角色的集合。形式化表示为：

session_roles(s_i)⊆{r ∈ R|(session_users(s_i),r) ∈ UA}。其中：session_users(s_i) 是会话所属的用户。

(5) 设定函数 avail_session_perm(s:S) → 2^P：返回在一个会话活动中当前用户可用权限的集合 P_{si} 形式化表示为：

$$P_{s_i} = \bigcup_{r \in session\_roles(s_i)} \{p \mid (p,r) \in PA\}$$

2.2.2 角色分层

ATP 车载设备管理信息系统分 B/S（Browser Server）架构和 C/S（Client Server）架构，前者供铁路总公司、铁路局管理层使用，后者由电务段、车间工区的作业人员使用。两者的用户相互独立，互不通用。用户与权限之间通过角色间接关联，角色通常和“岗位”对应，因而，角色表现出明显的层次性。

角色之间的层次关系形式化表示为：

$r_1 \geqslant r_2 \Rightarrow$authorized_permissions($r_2$)⊆ authorized_permissions(r_1) ∩ authorized_users(r_1)⊆authorized_users (r_2)

设定函数 authorized_ users (r:R) → 2^U：表示层次性 RBAC 中角色到用户的映射，形式化表示为：

authorized_ users (r)={u ∈ U| $r_1 \geqslant r(u,r_1)$ ∈ UA }。

设定函数 authorized_ permissions (r:R) → 2^P：表示层次性 RBAC 中角色到权限的映射，形式化表示为：

authorized_ permissions (r)={ p ∈ P| $r_1 \geqslant r(p,r_1)$ ∈ PA }。

通过以上函数，可以实现 ATP 管理信息系统中分层角色之间的继承关系，满足该系统角色分层的实际需要。

2.2.3 职责分离

ATP 管理信息系统中，涉及行车安全和故障责任的内容，比如运行故障等信息，其填报与删除应该严格分离，同一个用户不允许同时拥有填报和删除两个权限。ATPMIS 采用 SSD 策略限制用户获得相互冲突的权限。SSD 定义了一个角色集，它们在用户指派关系上互斥，即如果一个用户获得了一个角色，那么该用户就不能获得与这个角色相排斥的其它角色。

前文已经提到，ATPMIS 权限管理采用角色分层。在角色分层的前提下再使用 SSD 约束时，应保证用户继承不会破坏 SSD 策略。因而，角色分层定义在包括 SSD 约束的继承关系上，SSD 的用户是基于角色的拥有授权的用户（authorized users），而不是直接指派的用户（assigned users）。形式化表示为：

$$\forall (rs,n) \in SSD, \forall t \subseteq rs : |t| \geq n$$
$$\Rightarrow \mathrm{I}_{r \in t} \, authorized\_users(r) = \Phi$$

非继承环境下静态职责分离的形式化定义如下：

$$\forall (rs,n) \in SSD, \forall t \subseteq rs : |t| \geq n$$
$$\Rightarrow \mathrm{I}_{r \in t} \, assigned\_users(r) = \Phi$$

2.2.4　数据物理模型

通过以上分析，建立图 3 所示 ATP 车载设备管理信息系统权限控制数据物理模型。明确用户、角色、权限之间复杂而又明晰的关系。按照该数据模型，从数据层刻画访问控制间的关联关系。

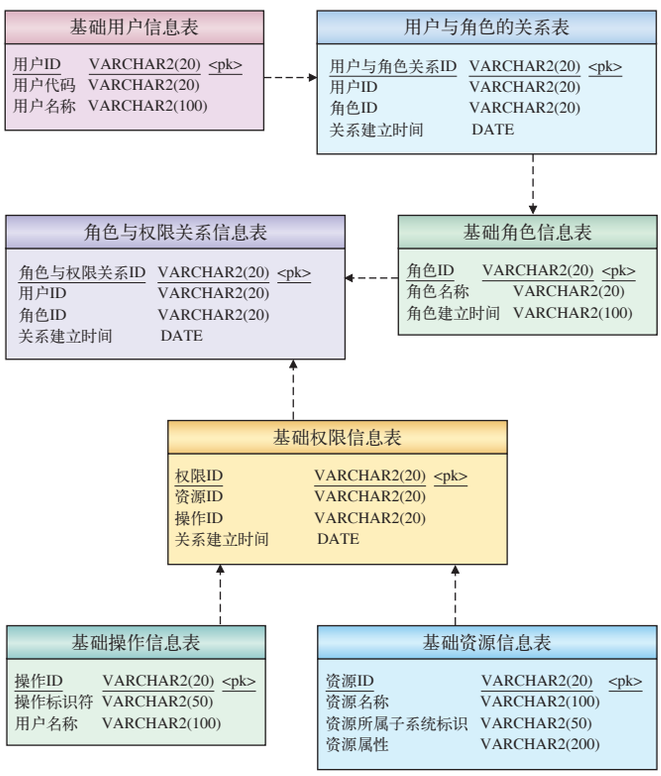

图3　ATPMIS权限控制数据物理模型

3　数据应用

ATP 车载设备管理信息系统的权限表现为 ATP 的数量和用户所具有的角色权限。以该系统中列车运行故障管理模块为例，表 1 列出了故障模块的功能以及哪些角色可以操作这些功能。

表1　ATPMIS运行故障管理模块的操作权限

模块	功能	CS			BS	
		系统管理员	确认人	维护人员	铁路总公司级用户	铁路局级用户
列车运行故障管理模块	增加	✓	×	✓	×	×
	确认	✓	✓	✓	✓	✓
	统计	✓	✓	×	✓	✓
	取消	✓	×	×	✓	×
	提交	✓	✓	✓	×	✓
	发布	✓	×	×	✓	×

此外，根据铁路现场实际，表 2 列出了 ATP 的数量以及用户可以操作的权限。表明任何一个用户都有非常严格的操作权限，同时，说明图 3 所示物理模型成功地解决了 ATPMIS 的访问控制问题。

表2　ATP数量和权限个数统计

	铁路总公司级用户	铁路局级用户	维修人员
ATP数量	1 680	258	82
权限个数	86	72	64

4　结束语

本文介绍了 RBAC 模型，并将该模型运用于 ATP 车载设备管理信息系统中，详细设计了该系统访问用户、角色和权限之间的相互关联关系、角色继承关系以及职责分离关系，最后得出该系统访问控制的数据模型。表明 RBAC 模型可有效实现信息系统的权限管理。

参考文献：

[1] 马水平．基于角色的安全访问控制机制的研究 [D]．青岛：中国海洋大学，2005.

[2] 洪　帆．访问控制概论 [M]．武汉：华中科技大学出版社，2010.

[3] 刘　强．基于角色的访问控制技术 [M]．广州：华南理工大学出版社，2010.

[4] 朱亚宁．分布式环境下的权限控制系统的研究与实现 [D]．大连：大连理工大学，2007.

责任编辑　方　圆