doi :10.3969/j.issn.1671-1122.2017.05.012

安全性优化的 RBAC 访问控制模型

顾春华 , 高远 , 田秀霞
(上海电力学院计算机科学与技术学院 , 上海 200082)

摘 要 : 基于角色的访问控制（RBAC，Role-Based Access Control）凭借其授权的灵活性以及模型的可靠性被电力信息系统广泛采用。但随着智能采集设备的日渐普及，电力系统规模的不断扩大，再加上电力信息系统较于传统信息系统对资源安全性要求更高，传统 RBAC 模型应用在电力信息系统中的安全问题（如权限滥用等）日益暴露。针对传统 RBAC 模型的不足，文章提出一种安全性优化的 RBAC 模型，引入了监察组 SG（Supervise Group）概念以及重要权限监察、层级代理机制，并设计了 SG 的生成算法和优化模型的流程、伪代码。经实例验证，优化的算法有效地对敏感权限进行了合理的监察，在满足电力信息系统功能的同时加强了系统的安全性。

关键词 : 基于角色的访问控制 (RBAC); 信息安全 ; 电力信息系统 ; 权限监察
中图分类号 : TP311.5 **文献标识码 :** A **文章编号 :** 1671-1122（2017）05-0074-06

中文引用格式 : 顾春华 , 高远 , 田秀霞 . 安全性优化的 RBAC 访问控制模型 [J]. 信息网络安全，2017（5）: 74-79.

英文引用格式 : GU Chunhua, GAO Yuan, TIAN Xiuxia. Security Optimized RBAC Access Control Model[J]. Netinfo Security,2017(5):74-79.

Security Optimized RBAC Access Control Model

GU Chunhua, GAO Yuan, TIAN Xiuxia
(*Institute of Computer Science and Technology*, *Shanghai University of Electric Power*, *Shanghai* 200082, *China*)

Abstract: Role-Based Access Control(RBAC) have been adopted bythe electric power information system rely on its reliable security and flexibility of authorization. But due to the popularization and expansion of Intelligent acquisition equipment and the electrical powersystem, combined with the stricter security requirement of electrical informationsystem, the security issues exposed when the traditional RBAC model be applied to the electric power information system. This paper put forward a kind of safety optimized RBAC model. In this model, we import the concept of SG(Supervise Group) and the machine-made of the supervision of sensitive permission to expand the traditional RBAC in safety field. In this paper,the generating algorithm of SG and the pseudo code, flow chart of the optimized model is also be given.An example is given to show that the proposed algorithm can effectively supervise the sensitive permission and enhance the security of the electric power information system while satis-fying the function of it.

Key words: role-based access control(RBAC); information security; electric power information system; permission supervise

收稿日期 : 2017-2-1
基金项目 : 国家自然科学基金 [61532012] ; 上海市科委地方能力建设项目 [15110500700]
作者简介 : 顾春华（1970—）, 男 , 江苏，教授，博士 , 主要研究方向为电力信息安全、软件工程 ; 高远（1993—）, 男 , 河南，硕士研究生 , 主要研究方向为电力信息安全、软件工程 ; 田秀霞（1976—）, 女 , 河南，教授，博士 , 主要研究方向为数据库安全、隐私保护。
通信作者 : 高远 422800886@qq.com

0 引言

随着近年来电力信息系统的推广普及，越来越多的资源被集中在这个平台上，其中涉及一些用户以及电力公司隐私的重要资源，一旦它们被恶意使用，后果将不堪设想。访问控制作为解决这些问题的一个重要方法，近些年得到了大量研究者的关注。传统的访问控制策略大概可以分为两种：自主访问控制（DAC，Discretionary Access Control）、强制访问控制（MAC，Mandatory Access Control）等。但是，DAC 可以通过传递进行授权，会导致主体的权限过大，容易造成信息泄露 [1]。而 MAC 安全属性是强制性的，由管理员统一发放与回收，虽然在信息泄露方面有着非常严格的控制和预防能力，但因此降低了系统的灵活性且实现困难，管理也相当复杂 [2]。

基于角色的访问控制（RBAC，Role-Based Access Control）提出之后弥补了这两种传统访问控制策略的不足。基于角色的访问控制中，用户的授权是通过授予用户角色来实现的，一个用户可以被分配角色，从而实现授权的灵活性 [3]。RBAC 模型通过建立起用户 – 角色 – 权限之间的多对多映射关系，把传统模型中管理员 – 用户的这种直接授权方式转化为更为灵活的分段式授权，使得基于 RBAC 访问控制的系统更加灵活，故而更加适合电力信息系统这样的大型信息系统。

然而传统 RBAC 模型的角色层次中却存在问题：上级角色会自动拥有下级角色的全部权限。这个继承机制不管从现实层面还是从模型算法的层面来看都存在着一定的缺陷：这会导致上级角色通过继承获得了大量的权限，而且这些权限在行使的过程当中并没有任何监管措施，如果上级角色对这些权限随意滥用，或是随意更改，将会对整个系统造成一定的安全隐患，引起不必要的损失。

本文就以上 RBAC 模型中存在的以上问题进行了深入分析，主要贡献体现在以下方面：1）对角色继承与权限约束进行了优化定义；2）使用层级代理来实现角色层级间的交流；3）对角色继承可能带来的重要敏感权限缺少监督等问题通过建立监察组 SG（Supervise Group）来进行约束与监督。

1 RBAC 模型的相关研究工作

基于角色的访问控制首次被提出是在 20 世纪 90 年代初。1992 年，David Ferraiolo 和 Richard Kuhn 在著作中首次给出了基于角色访问控制的基本概念，引入了角色的概念，并率先对 RBAC 模型框架进行了形式化定义 [4]。之后，1996 年，美国乔治梅森大学的 R.sandhu 发表了经典文献《Role-Based Access Control Models》[4]，提出了经典的 RBAC96 模型，RBAC96 把 RBAC 模型框架进行了详尽的描述，而且把传统的 RBAC 模型依照环境需求的不同分为 4 种相互组合嵌套的单元，随后还给出了模型相关的阐述以及说明。RBAC96 模型较优化之前的模型更加灵活方便，并且更易于实现，奠定了 RBAC 模型的发展基础 [5]。随后，以此为基础，美国国家标准与技术研究院（The National Institute of Standards and Technology，NIST）于 2001 年对 RBAC 模型制定了通用标准。标准把 RBAC 模型框架分为四个基本模块，其中包括：基本模型 RBAC0、角色继承模型 RBAC1、角色限制模型 RBAC2 和统一组合模型 RBAC3 [6]。其中，RBAC1 和 RBAC2 都以 RBAC0 模型为基础针对不同问题进行了优化，而 RBAC3 则把 RBAC1 和 RBAC2 进行了融合，把 RBAC1 和 RBAC2 各自的优化——角色继承和约束限制组合在了一起，构成了一个相对完整的模型。RBAC 模型族之间的关系如图 1 所示。

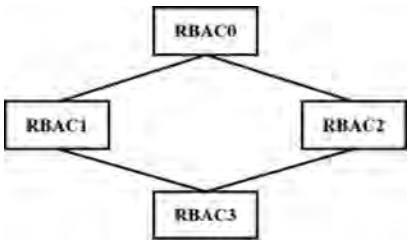

图 1 RBAC 模型家族关系图

后面的相关研究者基于 RBAC 模型的研究工作大多是以此模型为对象开展的。

在此模型的基础上，针对权限滥用等问题，已有一些研究成果：文献 [7] 和文献 [8] 在模型的基础上使用了权限的私有继承，通过定义传播深度来规定某权限在经过一定次数的继承之后变为不可继承，以此来限制权限在系统纵向的深度。但是权限的传播深度阈值因为实际环境是时常变化的，故而权限的传播深度阈值难以确定。文献 [9] 定义了权限继承时的不同方式，包括多角色完全继承、，多角色部分继承等，并且使用最小角色来优化角色权限的分配，从而对权限继承的过程提供了一定的限制作用，并且模型

有一定的伸缩性。但是模型对于系统的运行效率有一定的影响。另外，文献 [10] 提出一种加入了动态多维度信任度的 RBAC 模型，对恶意动态节点攻击能起到一定的遏制，但并没有考虑到权限滥用的问题。虽然以上研究在防止权限滥用等方面对 RBAC 模型有着一定的优化，但是很少有文献研究当实际权限已经分配给角色之后的安全防护，故本文从这方面进行优化，提出了权限行使过程中的监察机制。

2 传统 RBAC 模型

RBAC 模型的基本思想是建立用户 – 角色 – 权限之间的多对多映射关系，把权限的分配分为两段式授权：第一阶段，权限管理员只对角色负责，把不同的权限分配给不同的角色；第二阶段，角色管理员通过用户创建的会话把角色动态地分配给不同的用户或是用户组。

以研究者使用较多的 RBAC3 模型为例定义 RBAC 模型如图 2 所示。

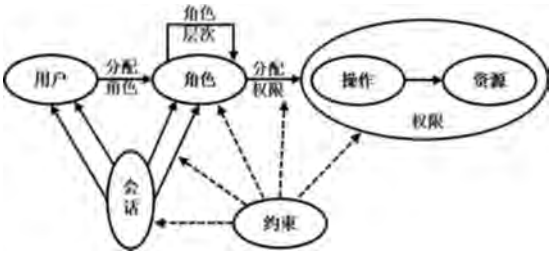

图 2 RBAC3 模型示意

RBAC 模型中有四个数据元素 [9]：U,R,P,S：分别代表用户（User），角色（Role）权限（Permission）和会话（Session）。

RBAC 模型中的这四个元素有如下四种关系：

1）角色权限分配 *PA*（Permission Assignment）：根据不同角色的职能，为其分配不同的权限。需要遵循最小特权原则，防止角色集之间可能出现的权限冗余。在给角色分配权限时应考虑到权限之间的互斥关系。

2）用户角色分配 *UA*（User Assignment）：为访问系统的用户 *U* 分配角色的过程，用户 *U* 和角色 *R* 之间通常是多对多的关系。

3）角色层次 *RH*（Role Hierarchy）：指角色之间存在的上下级继承关系映射，它同时也反映了现实世界中权限集的层次关系。在传统的 RBAC 模型中，上级角色自动拥有下级角色的全部权限。

4）角色激活 *RA*（Role Activation）：指用户通过建立会话 *S* 来动态地激活被授予角色中的一组角色的过程。

3 安全性优化的 RBAC 模型

SGRBAC(Supervise Group RBAC) 模型在传统 RBAC 模型的基础上进行了安全性优化，对角色层次以及权限约束进行了优化定义，并且引入了层级代理机制和权限监察机制。

3.1 SGRBAC 的角色层次定义

在传统的 RBAC 模型中，为了使权限分配的层次更加清楚，便于管理员对角色关系的管理，引入了角色层次的概念。角色层次即角色的继承，设定有上级角色（父级）以及下级角色（子级）。角色层次示意如图 3 所示。

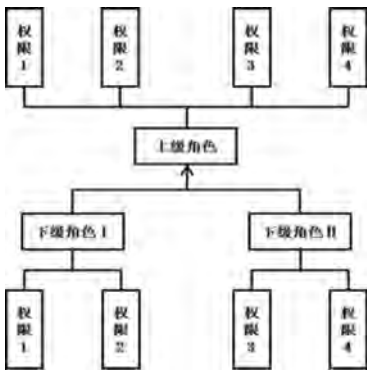

图 3 RBAC 模型角色权限继承示意

但在传统模型的角色层次定义中，对于角色权限继承轨迹的描述并不完善，高层角色通过继承拥有的权限来源不够清晰，导致角色权限划分模糊，给权限的使用带来了安全隐患。因此，SGRBAC 对角色层次定义如下：

定义 1 模型中角色 r 的权限集表示为：$\sigma(r)=\{p\in Permission|(p,r)\in PA\}$。

定义 2 设角色 r_d, r_u 为角色层次中的两个普通角色，且满足 $\sigma(r_d)$ $\sigma(r_u)$，则称角色 r_u 为角色 r_d 的上级角色，角色 r_d 为角色 r_u 的下级角色，表示为 $r_d \downarrow r_u$。角色的上下级关系是相对的。

定义 3 设 r_i, r_j, r_k 是角色层次中的三个普通角色，并且 r_i r_k, r_j r_k，如果满足公式 $\sigma(r_k)$ $(\sigma(r_i)\cup\sigma(r_j))$，那么称角色 r_k 为角色 r_i, r_j 的共同上级角色，记为 $\{r_i, r_j\}\overset{\uparrow}{=}r_k$。$r_i$, r_j 之间的关系为共同继承。

定义 4 权限继承路径 [9]。它是指满足如下公式的无环通路：$\sigma(r_i).p \rightarrow \sigma(r_{i+1}).p \rightarrow\cdots\rightarrow \sigma(r_{i+n}).p \rightarrow \sigma(r_j).p(n \geqslant 0)$，记

作 $Path(p)$。其中，$\sigma(r_i).p \rightarrow \sigma(r_{i+1}).p$ 表示角色 r_{i+1} 通过“→”角色继承关系从角色 r_i 中继承权限 p。$Path(p)$ 反映了权限 p 在角色层级中通过继承所经历的角色路径。

定义 5 继承路径长度。设 $p \epsilon \sigma(r)$ 为角色 r 通过继承获得的一个权限，若权限 p 在权限继承路径 $Path(p)$ 上第一个下级角色到当前上级角色继承经历的角色数量为 n，则记权限 p 的继承路径长度 $L(Path(p))=n$。

3.2 SGRBAC 的权限约束定义

权限约束指的是工作流任务与权限或者角色与权限之间的映射所对应的规则 [11]。权限约束作为一种规则，它通常都遵循权责分离、最小权限等原则。它的作用通常是在角色划分或者用户在行使权限的时候提供一定的限制条件或者简化流程以使过程更加简洁。而且，权限约束对防止权限的滥用和重要权限的监督也会起到一定的作用。但传统模型的权限约束并没有对权限的收回进行适当的限制：任意角色可以随意行使其拥有的任意权限，这样的定义显然既不符合实际的应用环境，也不利于系统对资源的有效保护。因此，SGRBAC 对权限约束有如下定义：

定义 6 若有两个权限 $p_1,p_2 \in P$ 互斥，记作 $p_1 \quad p_2$。互斥的两个权限不能分配给个同一个角色，即设角色 r 的权限集为 $\sigma(r) \quad P$，有两个互斥的权限 p_1,p_2，并且 $p_1 \in \sigma(r)$，则必有 $p_2 \quad \sigma(r)$，这称作权限的互斥约束 MEC（Mutual Exclusion Constrain）。

定义 7 设角色 $r \in R$ 有权限 $p \in \sigma(r)$，权限集 $P_e=\{p_{e1},p_{e2},\cdots,p_{en}\}(n \geqslant 1) \quad P$ 是 n 个与权限 p 互斥的权限集合，记作 $p \quad P_e$，若这些与 p 互斥的 n 个权限分别属于角色集 $R_e=\{r_{e1},r_{e2},\cdots,r_{em}\}(1 \leqslant m \leqslant n) \quad R$，则称角色集 R_e 为角色 r 的互斥角色集，记作 $r \quad R_e$。

定义 8 对于整个权限集合 P，存在两个权限集合把 P 分为两个部分，其中一个集合为一般权限集合 P_c（Permission Common），另外一个集合为受监察权限集合 P_s（Permission Supervised）。即 $P_c \cup P_s=P$。对于一般权限集 P_c，它代表用户在行使该集合中的权限时不需要另加的监督，安全级别为低。例如信息平台上一般通告的阅读权限，不同部门的日常权限等。对于受监察权限集 P_s，它代表用户在行使该集合中的权限时需要另外的监督与跟踪或者审查，安全级别为高。例如，对一些关键位置数据的修改权限，或者核心客户的重要资料等。

定义 9 对于受监察权限集合 P_s，定义权限资源约束 RC（Resource Constraint）。权限集中的元素被重新定义为 (P,η)，其中 η 代表权限 P 拥有的操作资源数，即权限 P 可以执行的次数或者时间等限制，η 的值被初始化为 0。

经过以上的定义可以把改进传统的 RBAC 权限模型表示为如图 4 所示。

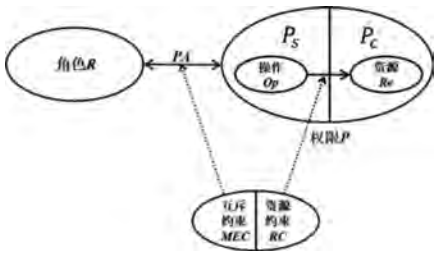

图 4 优化定义后的权限集和权限约束

3.3 SGRBAC 的层级代理机制

定义 10 若有角色集 R'，其拥有的通过继承而来的权限的最长权限继承路径经过的角色数量相同，则称角色集 R' 中的角色互为同层级角色。形式化定义为：$R'=\{r_1,r_2,\cdots,r_n\}(n>1) \quad R$，$\{\sigma(r_1),\sigma(r_2),\cdots,\sigma(r_n)\} \quad P$ 分别对应角色集 R' 中元素的权限集，若有 $MaxL(Path(\sigma(r_1)))=MaxL(Path(\sigma(r_2)))=\cdots=MaxL(Path(\sigma(r_n)))=l$，则记 $Layer_{(l)}(r_1,r_2,\cdots,r_n)$，代表角色集 $r=\{r_1,r_2,\cdots,r_n\}$ 中角色层级相同且处在层级系统的第 l 层。

定义 11 对于同层的角色集 $Layer_{(l)}(r_1,r_2,\cdots,r_n)$ 来说，其同外层以及同层内部交互的中介称为第 l 层层级代理，记作 $Agent_{(l)}$。

SGRBAC 模型引入角色层级的概念，每一层的角色与外层以及同层角色进行信息交换时都需要通过各自层次设立的代理 $Agent_{(l)}$ 来进行。代理对角色层级间的交互做出整体应答，避免了单个角色之间直接交流时可能存在的系统资源浪费，在一定程度上降低了系统的运行负担。同时，层级代理的引用也使得监察组 SG 内的角色做出自己的判断并不受其他角色的干扰：在 $Agent_{(l)}$ 做出判断前，任何角色都不知道其返回结果。这样既保证了监察组的公正性，也在一定程度上提高了模型的整体安全性。

层级代理的使用还可以通过资源约束来确保各层代理对过期权限的有效回收，使权限拥有者在行使权限的过程中也会受到监督，有效地防止了权限滥用的问题。

3.4 SGRBAC 的权限监察机制

SGRBAC 模型对角色的继承和权限的行使过程引入了监察组 *SG*, 并提出了基于上下级反馈的监察机制，在角色继承和防止权限滥用方面进行一定的优化，从而提高访问控制系统的整体安全性。

定义 12 基于角色层级概念，对于受监察权限 P_s，定义监察组 *SG*（Supervise Group），其中 $SG=\{r_{SG1},r_{SG2},\cdots r_{SGn}\}$ 用于对受监察权限 p_s 的监督。监察组 *SG* 的生成算法如算法 1 所示。

算法 1 监察组 *SG* 的生成

输入：受监察权限 $P_s=(p_s,\eta)\in P$,行使该权限角色 r 所在的角色层级 l 以及整个系统角色层级和权限分配情况。

输出：对于受监察权限 P_s 生成其监察组 SG_{P_s}。

①初始化权限资源 $\eta=0$，监察组 $SG_{P_s}=\emptyset$；

②检查 P_s 从当前角色开始的 $MaxLPath(P_s)=0$？若等于 0 跳至第④步；

③查找 P_s 的继承路径 $Path(P_s)$ 中位于角色层级 l、$l+1$ 以及 $l-1$ 层的角色集 $Layler_{(l)}(Path(P_s))$，$Layler_{(l+1)}(Path(P_s))$，$Layler_{(l-1)}(Path(P_s))$ 并将它们加入监察组 SG_{P_s}；

④检查 P_s 的互斥权限集 $P_s\otimes P'_s=\{P'_{s1},P'_{s2},\cdots,P'_{sm}\}(m\geq 1)\subseteq P$ 是否为空集，若为空集跳至第⑦步；

⑤R'_s 为角色层次 1 中拥有 P'_s 中权限的角色集，将 R'_s 添加到 SG_{P_s} 中；

⑥检查 $SG_{P_s}=\emptyset$？若 SG_{P_s} 不为空则跳到第⑩步；

⑦设 i 为角色层次中的一层，该层角色集为 $R_i\subseteq R$，且有 $R_i\overset{\uparrow}{=}\phi$。即该层角色没有上级角色。将角色集 R_i 添加到 SG_{P_s} 中；

⑧输出 SG_{P_s} 为当前权限 P_s 的监察组；

⑨结束

SGRBAC 模型的权限监察机制如下：当需要执行受监察权限 P_s 的角色 r 向其监察组 SG_r 发起 $\eta=\eta_q$ 的访问请求时，请求会通过角色 r 所在角色层级 l 的代理 *Agent*(l) 发给 SG_r 内元素各自所在的层级代理，再通过各层的代理把请求的内容发送给监察组成员，监察组成员会对 r 的请求完成各自的回复（*true* 或者 *false*），并把结果返回其所在层次的代理，继而再通过层级代理间的通信把结果返回给 *Agent*(l)，*Agent*(l) 完成整个 SG_r 回复的收集后，再将结果统计并判断 r 是否能执行 P_s。若 r 的请求得到 *Agent*(l) 回复的 true，则 r 可以在 η=0 之前任意执行 P_s。一旦 *Agent*(l) 监察到 η=0，它将立即收回权限 P_s。

3.5 SGRBAC 模型的总体概念图

在对传统 RBAC 模型进行了以上的优化以后，SGRBAC 模型的总体概念图如图 5 所示。

4 SGRBAC 模型的应用实例

在电力信息系统中有许多敏感权限，如用户用电信息发布、断电、调度等。这些权限与用户的隐私以及电网公司的稳定运行息息相关，如果对这些敏感权限的行使不进行适当的监察，电力信息系统将存在一定的安全隐患。现以断电权限为例，对 SGRBAC 模型进行示例说明。

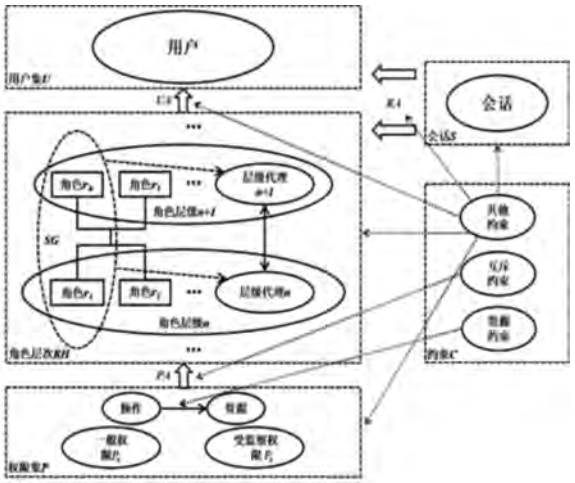

图 5 SGRBAC 模型图示

4.1 数据库设计

SGRBAC 的数据库设计如图 6 所示。其中，User 表对应图 5 中用户集 U，用以表示用户所拥有的属性；Role 表对应图 5 中角色层次 *RH*，其中字段 RoleLayer 表示角色所在层级；Permission 表对应图 5 中权限集 P，其中字段 SuperviseProperty 用于区分权限是否需要受到监察。在 SGRBAC 的数据库设计中，添加了权限的监察组表 *SG* 用以记录其所拥有的监察组：在通过相关算法得出监察组 *SG* 后，动态地把其属性更新到对应权限的 *SG* 表。另外，为了体现图 5 中模型的约束 C，对于资源约束，在 Permission 表中添加了 Resource 字段用以记录权限的资源情况；对于互斥约束，添加了互斥权限表 MEPermission，用来记录权限之间的互斥关系，并把约束关系应用到 *SG* 的生成和角色权限分配的过程中。

4.2 SGRBAC 的实例说明

为了方便说明，不再单独设计 User 表成员。Role 表成员设计如下：送电部主任，送电部员工，调度部主任，调度部员工，运行部主任，运行部员工，公司经理。其中各部门员工 RoleLayer 字段值为 1，主任为 2，公司经理为 3。Permission 表成员有断电权限，因断电不当可能对用户和电网公司造成巨大的损失，故将其设定为受监察权限，即其 SuperviseProperty 字段值为 *True*，并把 Resource 值初始化为 0。

实例的具体步骤如下：

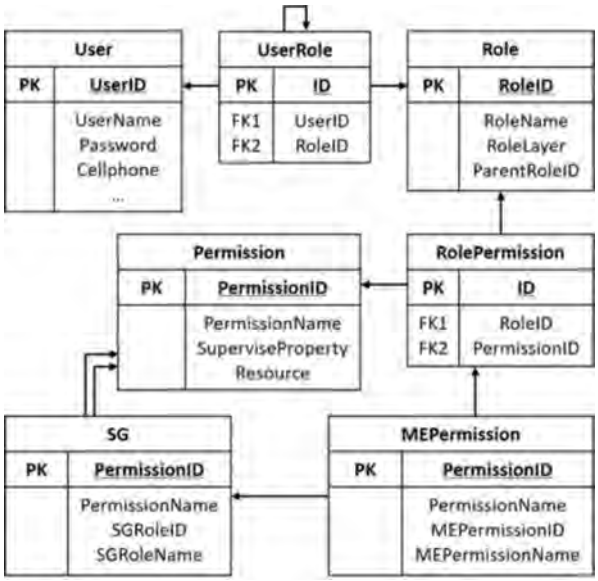

图 6 SGRBAC 数据库设计

1）送电部主任拥有断电权限，其继承于送电部员工且被公司经理继承。

2）当送电部主任要行使其断电权限对某用户进行断电操作时，通过算法 2 计算断电权限的监察组 *SG*={ 公司经理，送电部员工，运行部主任，调度部主任 }，并把这些成员更新到断电权限的 *SG* 表中。

3）送电部主任通过层级代理向 *SG* 中角色发送 Resource=1 的断电权限访问请求。

4）当 SG 接收到请求后，其中角色各自行使其相关权限进行相应的判断并做出决定：运行部主任行使其权限查询该用户是否应该被断电，调度部调度该地区用电情况审查断电的可行性，公司经理根据实际情况综合判断。然后通过各层的代理将决定结果汇总到送电部主任所在层级代理。

5）送电部主任所在层级代理再通过收集到的信息来判断送电部主任是否能执行该请求。若允许执行，将断电权限的 Resource 字段值置为 1，并监视断电权限的行使直到其访问次数 1 次用完后（即 Resource=0 时）立即收回断电权限。

实例分析得知，本模型对受监察权限的监察符合电力信息系统的实际应用场景，并且重要敏感权限的行使过程得到了应有的监察，模型在安全性方面得到了提升。

5 结束语

本文在相关研究基础上，针对传统 RBAC 模型应用在电力信息系统中安全性不足的问题，对传统 RBAC 模型的安全性进行了优化。针对传统 RBAC 模型中角色继承可能带来的权限滥用等问题，引入了监察组，提出了权限监察机制，使重要权限在行使的过程中可以得到应有的监督，在一定程度上加强了传统模型的安全性。在权限的回收方面，本文对权限的结构进行了优化，加入了资源约束，使权限在过期之后能被正确及时回收。另外，引入了角色层级代理，用来优化角色之间的交互，以提高系统模型的安全性和工作效率。最后，设计了优化模型的数据库，并以实例加以说明。经实例验证，安全性优化的 RBAC 模型在权限的监督方面更加完善，在系统安全方面更加突出。（责编 吴晶）

参考文献：

[1] 姜俊萍 . 基于 RBAC 模型的通用权限管理组件的设计与实现 [D]. 上海：复旦大学 , 2010.

[2] 程思嘉，张昌宏，潘帅卿 . 基于 CP-ABE 算法的云存储数据访问控制方案设计 [J]. 信息网络安全，2016（2）：1-6.

[3] 陈胜 , 娄渊胜 , 张文渊 . RBAC 模型中角色互斥研究及应用 [J]. 计算机技术与发展 , 2012(12):21-24+28.

[4] 池亚平，姜停停，戴楚屏，等 . 基于 BLP 的虚拟机多级安全强制访问控制系统设计与实现 [J]. 信息网络安全，2016（10）：1-7.

[5] 陈丹丹 . 基于 RBAC 的权限管理组件的设计与实现 [D]. 武汉：武汉理工大学 , 2008.

[6] 金鑫 , 王晶 , 李炜 . 基于 RBAC 的扩展权限管理模型 [J]. 计算机系统应用 , 2012 (6):20-24+105.

[7] 袁中兰 , 温巧燕 , 杨义先 . RBAC 角色继承关系中私有权限问题的研究 [J]. 中国电子科学研究院学报 ,2006(1):50-53.

[8] 高川 , 朱群雄 . RBAC 角色继承关系中私有权限问题的研究 [J]. 计算机应用 , 2010(5):1230-1232+1235.

[9] 蔡婷 , 聂清彬 , 欧阳凯 , 等 . 基于角色扩展的 RBAC 模型 [J]. 计算机应用研究 , 2016(3):882-885.

[10] 叶重阳 , 庄毅 . 一种基于多维信任度的动态 RBAC 模型 [J]. 计算机与现代化 , 2015(6):7-11.

[11] 段隆振 , 文锋 , 黄水源 , 等 . 一种描述 RBAC 角色层次关系和互斥关系的模型及实现 [J]. 南昌大学学报（理科版）, 2006(6):601 - 604.