



扩展 RBAC 访问控制模型在家庭开放平台中的应用

李 蔚,王 晶

(北京邮电大学网络技术研究院 北京 100876)

摘 要:基于角色的访问控制(role-based access control, RBAC)技术是目前访问控制领域研究的热点,具有灵活和高效的特点。在 RBAC 模型的基础上,将权限进行细化,添加了对象、操作、域和分组 4 个要素,提出了域的可继承性,深入地控制角色可管理的数据内容和操作,提供了更细粒度化的权限功能。将扩展后的模型作为解决家庭开放平台终端管理子系统分权分域问题的理论基础,解决了系统中访问控制约束的问题,提出了多样化的角色和权限设计方案,实现了复杂的职责分配。

关键词:RBAC 模型;访问控制;操作;对象;家庭开放平台;机顶盒

doi: 10.11959/j.issn.1000-0801.2015249

Application of the Extension RBAC Model in the Family Open Platform

Li Wei, Wang Jing

(Network Technology Research Institute, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Role-based access control (RBAC) technology is one of the hotspots in the research of access control. It is of great flexibility and high efficiency. The permission of RBAC model was refined, and four elements such as object, action, domain and group were added to the model. The inheritance of domain was put forward. The extended model (ODG-RBAC) provided a more fine-grained access control. Through using ODG-RBAC model in the family open platform STB manage system, the problem of access control was resolved. Meanwhile, by providing diversified design scheme of permissions and roles, the complex responsibility assignment was implemented.

Key words: RBAC model, access control, action, object, family open platform, STB

1 引言

随着家庭数据业务的快速发展,业务需求不断增多。家庭业务的运营涉及的步骤较为繁琐复杂,不利于业务的快速开展和部署,因此需要一个管理平台为多样化的家庭业务提供统一且通用的管理、服务和支撑保障机制,以营造良好的家庭业务生长环境。在这个平台中,可

管理的数据或资源具有集中控制、分域协作及分散接入的特点,因此,分权分域管理功能成为家庭开放平台的一项关键管理能力。其本质是为不同的管理员提供不同的功能权限,并将集中控制的可管理的数据或资源划分为多个管理实体^[1]。自主访问控制(discretionary access control, DAC)、强制访问控制(mandatory access control, MAC)和基于角色的访问控制(role-based access control,

收稿日期:2015-05-29;修回日期:2015-09-23

论文引用格式:李蔚,王晶.扩展 RBAC 访问控制模型在家庭开放平台中的应用.电信科学,2015249

Li W, Wang J. Application of the extension RBAC model in the family open platform. Telecommunications Science, 2015249

对象。

3.2 形式化表示

DA : 表示域和角色的分配关系, 则 $DA \subseteq D \times R$ 表示多对多的关系。

AA : 表示操作和角色的分配关系, 则 $AA \subseteq A \times R$ 表示多对多的关系。

O_dA : 表示对象和域的分配关系, 则 $O_dA \subseteq O \times D$ 表示多对多的关系。

O_gA : 表示对象和分组的分配关系, 则 $O_gA \subseteq O \times G$ 表示多对多的关系。

G_dA : 表示分组和域的分配关系, 则 $G_dA \subseteq G \times D$ 表示多对一的关系。

A_oA : 表示操作和对象的分配关系, 则 $A_oA \subseteq A \times O$ 表示多对多的关系。

域: $S \rightarrow 2^D$, 从会话集到管理域集的映射, 且包含了会话中所有角色的管理域, $\text{domain}(s_i) = \bigcup_{r \in \text{role}(s_i)} \{d | (d, r) \in DA\}$ 。

对象: $D \rightarrow 2^O$, $S \rightarrow 2^{D \cap O} \rightarrow 2^O$, 从会话集到管理对象的映射, $\text{object}(s_i) \subseteq \{o | (o, d) \in O_dA \wedge d \in \text{domain}(s_i)\}$ 。

操作: $S \rightarrow 2^A$, 从会话集到操作集的映射, $\text{action}(s_i) = \bigcup_{r \in \text{role}(s_i)} \{a | (a, r) \in AA\}$, 包含了这个会话中所有对象上的操作, $\text{action}(s_i) = \bigcup_{o \in \text{object}(s_i)} \{a | (a, o) \in A_oA\}$ 。

分组: $S \rightarrow G$, 从会话集到分组建的映射, $\text{group}(s_i) \subseteq \{g | (o, g) \in O_gA \wedge o \in \text{object}(s_i)\}$ 。

$DH \subseteq D \times D$ 表示 D 上的偏序关系, 表示域继承, 也记为 $\geq$ 。

域: $S \rightarrow 2^D$, 满足 $\text{domain}(s_i) \subseteq \{d | (\exists d' \geq d) [(d', \text{role}(s_i)) \in DA]\}$,

$\text{role}(s_i) \cup_{d \in \text{domain}(s_i)} \{r | (\exists d'' \leq d) [(d'', r) \in DA]\}$, $\text{action}(s_i) = \bigcup_{d \in \text{domain}(s_i)} \{a | (a, o) \in A_oA \wedge o \in \text{object}(s_i)\}$, 其中 $\text{object}(s_i) \subseteq \{o | (\exists d'' \leq d) [(o, d'') \in O_dA \wedge d \in \text{domain}(s_i)]\}$ 。

3.3 域的层级关系表示

域的层级关系用前缀来表示, 根据前缀可以确定一个域的父域, 有利于向上追溯或者向下查询。域的层级关系如图 2 所示。

每个域都有一个唯一的 ID , 表示层级关系的 $prefix$ 和限制域的层级深度的 $max-depth$ 。规定超级域的 ID 为 0, 其 $prefix$ 为 $/0/$, $max-depth$ 为 inf 表示不限制层级深度, $max-depth$ 不可为负数。

3.3.1 域的创建

图 2 中, 创建超级域的子域, 域 A、B、C、O 表示如下:

$ID_{\text{域A}}=1, prefix_{\text{域A}}=/0/1/, max-depth_{\text{域A}}=6$

$ID_{\text{域B}}=2, prefix_{\text{域B}}=/0/2/, max-depth_{\text{域B}}=inf$

$ID_{\text{域C}}=3, prefix_{\text{域C}}=/0/3/, max-depth_{\text{域C}}=inf$

$ID_{\text{域O}}=15, prefix_{\text{域O}}=/0/15/, max-depth_{\text{域O}}=0$

创建子域时, 根据父域的个数和所处继承层次的不同分为多种情况讨论。

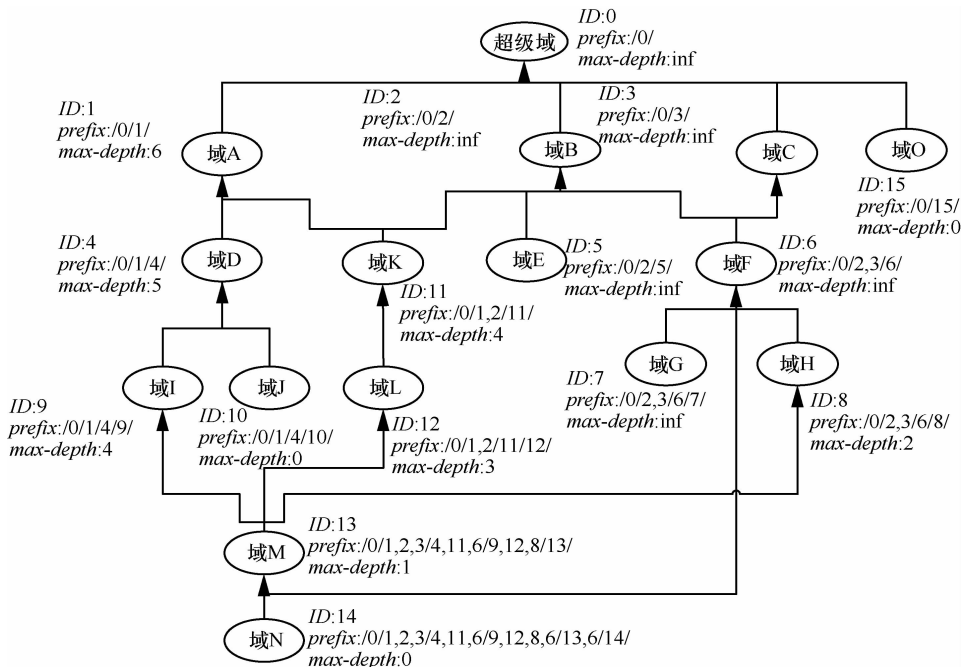


图 2 域层级关系



(1)域 A 下创建域 D,此时域 D 的 $max\text{-}depth$ 必须小于其父域 A 的 $max\text{-}depth$,默认为父域的 $max\text{-}depth$ 减 1,表示如下:

$ID_{域D}=4, prefix_{域D}=/0/1/4/, max\text{-}depth_{域D}=5$

(2)域 I、L 和 H 下创建域 M,M 是这 3 个域的公共子域,此时域 M 的 $max\text{-}depth$ 必须小于其父域 I、L 和 H 的 $max\text{-}depth$,则只能为 1 或者 0。域 M 的 $prefix$ 应为其父域 $prefix$ 的合并,因为域 I、L 和 H 所处的继承层次一致,则 $prefix$ 逐层合并即可,表示如下:

$ID_{域M}=13, prefix_{域M}=/0/1, 2, 3/4, 11, 6/9, 12, 8/13/, max\text{-}depth_{域M}=1$

(3)域 M 和 F 下创建域 N,其 $max\text{-}depth$ 只能为 0。域 N 的 $prefix$ 应为域 M 和 F 的 $prefix$ 的合并,因为域 M 和 F 所处的继承层次不一致,域 F 的 $prefix$ 需要补全为 $/0/2,3/6/6/$,之后 $prefix$ 逐层合并即可,则表示如下:

$ID_{域N}=13, prefix_{域N}=/0/1, 2, 3/4, 11, 6/9, 12, 8, 6/13, 6/14/, max\text{-}depth_{域N}=0$

(4)域 O 下创建子域,由于域 O 的 $max\text{-}depth$ 为 0,其子域的 $max\text{-}depth$ 必须小于 0 但不可为负数,那么域 O 下无法创建子域。

3.3.2 域的撤销

域的撤销影响的不仅是当前操作的域,还会影响到继承于这个域的各个子域。图 2 中撤销域 F,首先获取域 F 的 $prefix$ 值为 $/0/2,3/6/$ 。域 F 的子域分为两种情况:一种是单继承于域 F 的,即 $prefix$ 开头为 $/0/2,3/6/$ 的域,为 $/0/2,3/6/7/$ 和 $/0/2,3/6/8/$,对应域 G 和 H;另一种是多继承于域 F 的,即 $prefix$ 中包含 $/*,6/、/6,*/或/*,6/*$ ($*$ 为任意符合 $prefix$ 要求的字符)的域,为 $/0/1,2,3/4,11,6/9,12,8/13/$ 和 $/0/1,2,3/4,11,6/9,12,8,6/13,6/14/$,对应域 M 和 N。撤销时可以选择,分为全部撤销和局部撤销。

(1)全部撤销

如果是单继承于域 F,即为域 G 和 H,这些子域直接撤销, ID 分别为 6、7 和 8,如果有多继承关系,即为 M 和 N,删除域 M 和 N 中所有属于域 F 的部分,不论这个对象是否是从域 F 继承而来,并且处理 M 和 N 的 $prefix$,删除 6、7 和 8,更新后:

$ID_{域M}=13, prefix_{域M}=/0/1,2,3/4,11/9,12/13/, max\text{-}depth_{域M}=1$

$ID_{域N}=14, prefix_{域N}=/0/1, 2, 3/4, 11/9, 12/13/14/, max\text{-}depth_{域N}=0$

(2)局部撤销

修改继承关系,如果是单继承于域 F,即为域 G 和 H,这些子域内包含的对象范围不变,直接更新 $prefix$,使其直接继承于域 F 的父域。如果有多继承关系,即为域 M 和 N,这些子域内包含的对象范围也不变,更新 $prefix$,用 F 的父域代替 F 的 ID , $max\text{-}depth$ 均不做修改,更新后:

$ID_{域G}=7, prefix_{域G}=/0/2,3/7/, max\text{-}depth_{域G}=inf$

$ID_{域H}=8, prefix_{域H}=/0/2,3/8/, max\text{-}depth_{域H}=2$

$ID_{域M}=13, prefix_{域M}=/0/1, 2, 3/4, 11, 2,3/9, 12, 8/13/, max\text{-}depth_{域M}=1$

$ID_{域N}=14, prefix_{域N}=/0/1, 2, 3/4, 11, 2, 3/9, 12, 8, 2, 3/13, 2, 3/14/, max\text{-}depth_{域N}=0$

3.4 角色和域的继承关系

角色的继承和域的继承各自作用但又紧密相连,角色的影响范围包括:继承于这个角色的子角色、角色创建的关联域的子域和这些子域关联的角色。域的影响范围包括:域关联的角色、继承于这个域的子域和子域关联的角色。分组隶属于域,域由对象组成,任何域的影响范围还包括这个域里的所有分组和对象,分组和对象与角色无直接关联。

在 RBAC 模型中角色继承与会话有关,所以角色继承可以解释为激活继承和权限继承^[6]。域的继承属于这里所说的权限继承,当一个会话被激活,这个继承关系也就被激活了。由于可能限制了域的继承深度,角色会与域相关联,则角色间接地被限制了继承深度。

形式化表示如下: $role(u_i)\{r|(u_i, r) \in UA\}, domain(u_i) = \bigcup_{r \in role(u_i)} \{d|(d, r) \in DA\}$, 用户 u_i 创建子域 d_x , 其 $max\text{-}depth_{域d_x} = \min(\{max\text{-}depth_{域d} | d \in domain(u_i)\}) - 1$, 那么被分配了域 d_x 的角色 $r(r \geq role(u_i))$ 的继承深度必然小于 $max\text{-}depth_{域d_x}$ 。

4 ODG-RBAC 模型在家庭开放平台中的应用

家庭开放平台由门户子系统、运营管理子系统、认证鉴权子系统、终端管理子系统、终端侧的用户认证中间件、业务管理 SDK、屏幕管理程序和应用管理程序等构成。终端管理子系统包括终端管理、屏幕管理和应用管理,系统用户包括超级管理员和普通管理员。管理员通过终端管理实现对机顶盒参数采集配置、固件升级和状态监控等功能;通过屏幕管理实现对屏幕配置文件的分发和屏幕程序的升级;通过应用管理实现对终端上安装的各类应用程序的操作控制,包括应用远程控制(安装、卸载、

升级)。

不同的管理员可管理不同的对象并进行不同的操作,即细化了管理的权限,在系统中被称为分权分域管理。分权管理的本质是为不同的管理员提供不同操作权限的设置,分域管理的本质是将集中控制的可管理数据按管理域划分多个管理实体(可以有多个层次,即域的继承),这样就能由不同的管理员管理,实现分域协作。

4.1 数据关系设计

用户、角色、域、对象、分组和操作之间的关系用分配表来记录,域和角色的继承都各由一张层次表记录,系统的分权分域的数据关系如图 3 所示。

图 3 反映了角色和域的重要性,分组和对象都不直接与角色关联,用户通过角色获得域和操作,即基本 RBAC 模型中的权限。在实际应用中,系统根据角色需要进行对应操作数据的分配^[7],用户登录后可以看到所属角色能够管理的域中的所有对象,然后可执行被授权的操作,不属于角色可管理的域中的对象对这个用户来说是不可见的,必然也不能被操作,不属于角色被授权的操作,用户也是不可发起的。

4.2 权限分配设计

在家庭开放平台中应用了 ODG-RBAC 模型,角色的划分需要综合考虑组织内部的岗位职责和安全策略^[9],根据具体的业务需求划分了角色和权限,设计如图 4 所示。

首先是角色的划分,系统有一个超级角色,下面分为 3 个角色(超级终端角色、超级屏幕角色和超级应用角色),然后这 3 个角色下面再各自细化。再者是域的划分,系统有一个超级域,包含了系统内所有的对象(在家庭开放平台中就是终端),然后 4 个超级角色对应的都是这个超级域,之后域各自划分出不同的子域,不是超级角色的其余角色都与这些子域关联。

这样划分后职责分明,没有关联终端操作的角色就不能去查看终端信息或是发起终端任务,并且一个管理员只能看到并操作自身角色的域中的终端,更易于符合最小权限^[8]这一特性。

5 模型比较

5.1 授权过程

在一个授权会话中,采用 ODG-RBAC 模型和基本

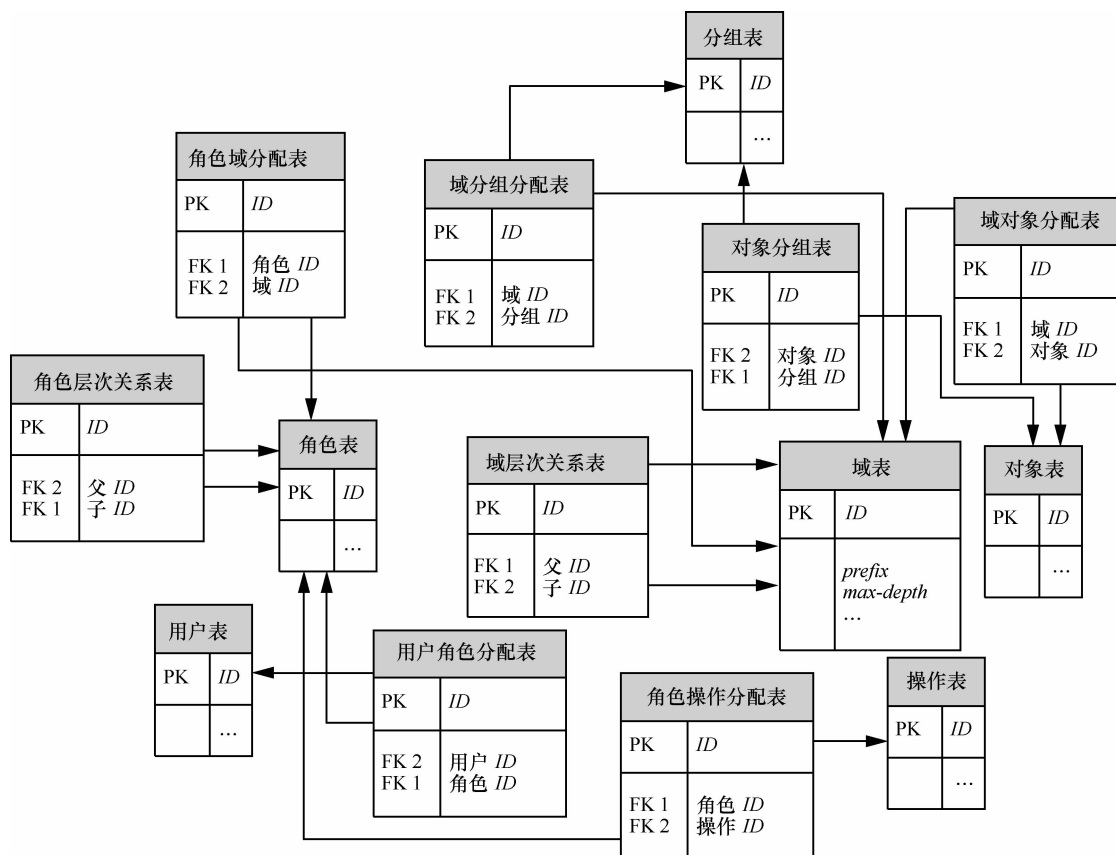


图 3 系统数据关系

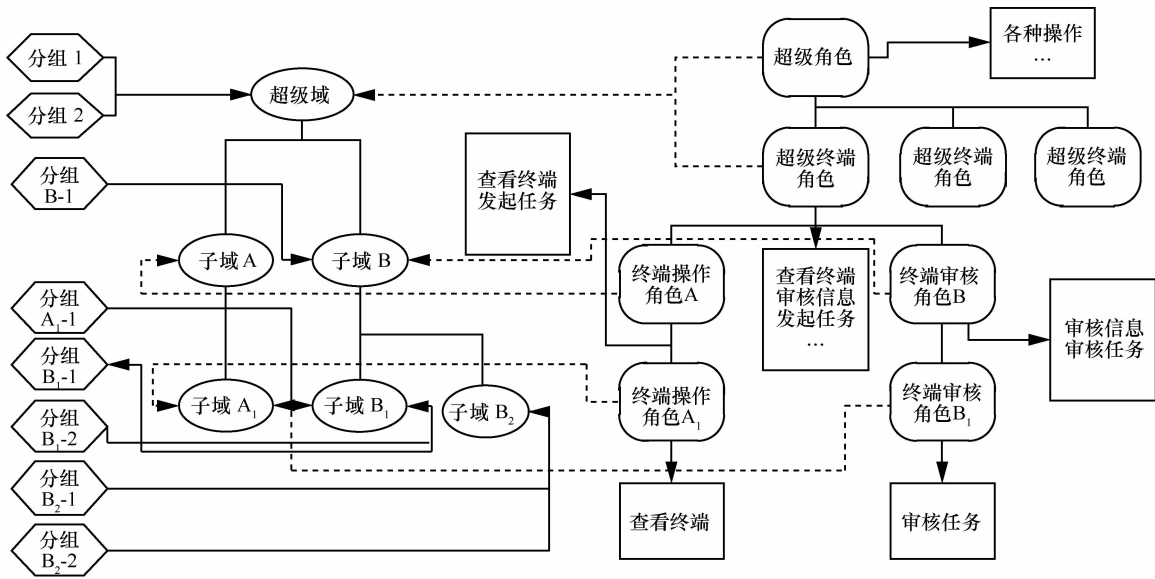


图4 角色和权限分配

RBAC 模型所做的操作步骤是不同的,为达到同样的授权效果,所要操作的次数也是不同的。为比较出采用改进后的模型效率上的提高,现引入操作数减少的百分比 P_r ,另 O_{RBAC} 和 $O_{ODG-RBAC}$ 分别表示两个模型后所做的操作的次数,则 $P_r = 1 - \frac{O_{ODG-RBAC}}{O_{RBAC}}$ 。

现设整个系统中有 N 个对象,目前需要对 M 个域分别分配不同的可执行的操作形成 M 个不同的权限集合,之后再分配给角色。另 $N_i (1 \leq i \leq M, i \in Z)$ 表示每个域中包含的对象的个数,规定不存在空域,则 $N_i \geq 1$ 。如果采用 ODG-RBAC 模型,首先设置 M 个域,然后对每个域分配操作,则有 $O_{ODG-RBAC} = M + M = 2M$;如果采用基本 RBAC 模型,则需要分别对这个 M 个域中的每个对象分配权限,则有

$O_{RBAC} = \sum_{i=1}^M N_i > \sum_{i=1}^M 1 > M$ 。由于每个域内包含的对象是不一定的,如果每个域内都只有 1 个对象,则与基本 RBAC 模型一样,并且操作数还是原来的 2 倍,这时改进后的模型并不能提高授权过程的效率,一般来说一个域内包含的对象个数应大于 1,另 $N_a (2 \leq N_a \leq N)$ 表示每个域中包含的对象个数的平均值,则 $O_{RBAC} = MN_a$,则 $P_r = 1 - \frac{2M}{MN_a} = 1 - \frac{2}{N_a}$,当系统中每个域包含的对象个数越多,ODG-RBAC 模型的改进效果越明显,如图 5 所示。

5.2 域的撤销过程

当撤销一个域的时候,除了处理这个域,还需要查询并处理这个域的所有子域。采用 ODG-RBAC 模型和基本

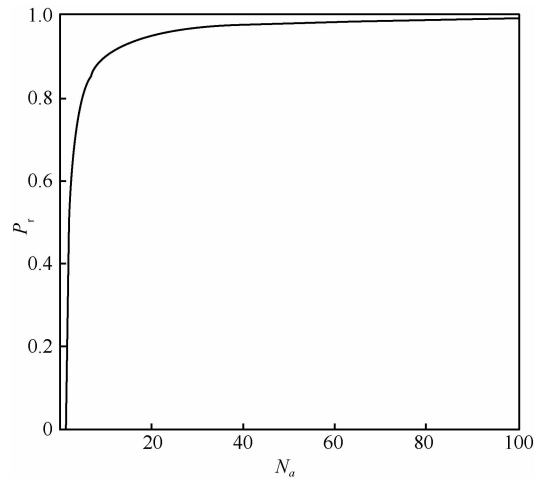


图5 授权操作分析结果

RBAC 模型所需要的查询次数是不同的,为比较出查询效率的提高,现引入查询次数减少的百分比 P_s ,另 N_{RBAC} 和 $N_{ODG-RBAC}$ 分别表示两个模型的查询次数,则 $P_s = 1 - \frac{N_{ODG-RBAC}}{N_{RBAC}}$ 。

由于 ODG-RBAC 模型采用了前缀表示域的层次关系,查询到某个域的子域只需要执行 2 次查询,分别为查询单继承和多继承关系的子域。接下来讨论采用基本 RBAC 模型需要的查询次数,假设一个域下面的子域个数的平均数为 C ,平均深度为 L ,每个域是多继承产生的平均概率为 P_m ,另撤销一个域时要获取到所有的子域的查询次数(查询域层次关系表的次数)为 N_c 。

$$\begin{aligned} N_c &= 1 + C + C^2(1 - P_m) + \dots + C^L(1 - P_m) \\ &= (1 - P_m) + C(1 - P_m) + C^2(1 - P_m) + \dots + C^L(1 - P_m) + P_m + CP_m \end{aligned}$$

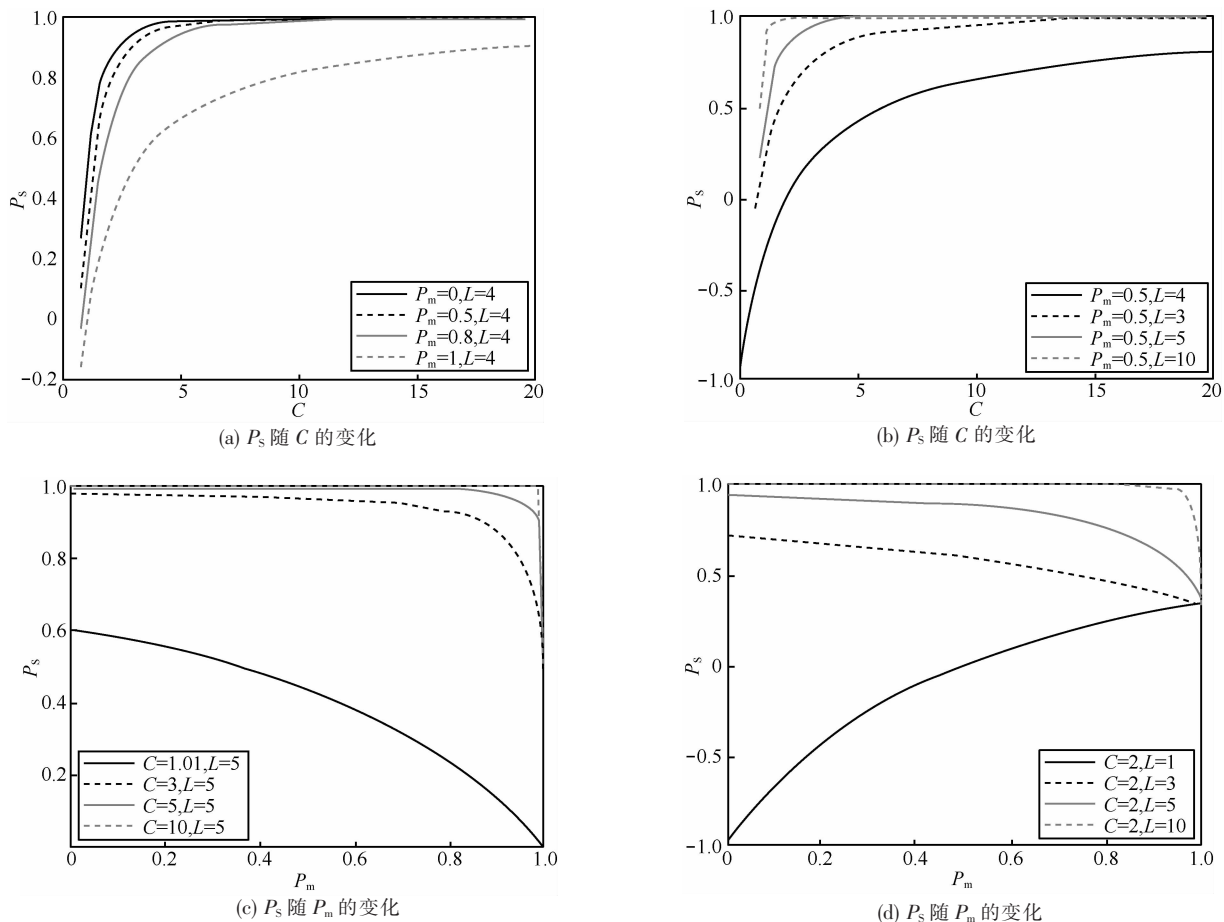


图 6 查询次数分析结果

$$\begin{aligned}
 &= (1-P_m)(1+C+\dots+C^L)+P_m+CP_m \\
 &= \frac{C^L-1}{C-1}(1-P_m)+P_m+CP_m \\
 P_s &= 1 - \frac{2}{N_c} = 1 - \frac{2}{\frac{C^L-1}{C-1}(1-P_m)+P_m+CP_m}
 \end{aligned}$$

考虑最坏的情况就是每个域只有一个子域, 则 $C=$

$$\frac{L-1}{L}, \text{ 那么有 } C \geq \frac{L-1}{L}.$$

从图 6 中可以发现, 系统中域的层次关系越复杂, 即在子域个数越多, 继承深度越大的情况下, 采用改进后的模型在查询效率上的提高越明显。因此, 在操作对象也存在复杂的层次关系时, 应该采用 ODG-RBAC 模型。

6 结束语

在 RBAC 基本模型的基础上, 细化了权限这一概念, 根据家庭开放平台终端管理系统的业务需求, 添加了对象、操作、域、分组 4 个要素以及域的继承。通过

ODG-RBAC 模型能更深入地控制权限的范围, 划分方式更加灵活、高效, 将模型运用到终端管理系统中后, 多样化的角色设置有效地解决了其复杂的访问控制问题, 并且增强了系统的安全性。

参考文献

- 1 中国移动通信集团有限公司. 中国移动家庭开放平台技术规范 v1.0.0, 2014
China Mobile Group. Technical Specification for Home Service Open Platform v1.0.0, 2014
- 2 Sandhu R S, Coyne E J, Feinstein H L, *et al.* Role-based access control models. IEEE Computer, 1996, 29(2):38~47
- 3 陈溪源. 基于角色的访问控制在分布式环境下应用的关键问题研究(硕士学位论文). 杭州: 浙江大学, 2010
Chen X Y. Research on the key issues of role based access control under distributed environments (master dissertation). Hangzhou: Zhejiang University, 2010
- 4 夏启寿. RBAC 在考试系统中的应用研究 (硕士学位论文). 西安: 西北大学, 2007



- Xia Q S. Researching and implementation of RBAC in examination system(master dissertation). Xi'an: Northwest University, 2007
- 5 尹泉. 基于扩展 RBAC 模型访问控制理论在工商电子政务系统中的研究与实现(硕士学位论文). 北京: 北京邮电大学,2007
- Yin Q. Research and implementation of e-governement system based on RBAC in bureau of industry and commercial(master dissertation). Beijing: Beijing University of Posts and Telecommunications, 2007
- 6 马丽, 马世龙, 陆跃飞等. 一种 RBAC 的描述逻辑表示方法. 计算机科学, 2010, 37(3):29~35
- Ma L, Ma S L, Gui Y F, *et al.* Representation for RBAC model in description logic. Computer Science, 2010, 37(3):29~35
- 7 庞春江, 庞会静. RBAC 模型的改进及其在电力 ERP 权限管理中的应用. 电力系统自动化, 2008, 32(13):49~52
- Pang C J, Pang H J. Improvement of RBAC model and its application in the competence management of electricity ERP. Automation of Electric Power Systems, 2008, 32(13):49~52
- 8 邢永明. 一种改进的 RBAC 权限系统的研究与实现 (硕士学位论文). 哈尔滨: 哈尔滨理工大学, 2007

Xing Y M. Research and implementation of an improved RBAC permission system(master dissertation). Harbin:Harbin University of Science and Technology, 2007

[作者简介]



李蔚,女,北京邮电大学硕士生,主要研究方向为通信网络技术与智能服务。



王晶,女,北京邮电大学副教授、硕士生导师,主要研究方向为业务网络智能化、基于内容的多媒体检索、大数据挖掘与支撑管理。