第 36 卷 第 4 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.4 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)04—0152—03 文献标识码：A 中图分类号：TP309

基于 RBAC 的工作流管理系统授权约束方法

单徐梅[1]，虞慧群[2]
(1. 华东理工大学计算机科学与工程系，上海 200237；2. 上海市计算机软件评测重点实验室，上海 201112)

摘 要：针对工作流管理系统动态授权的特性，在基于角色的访问控制(RBAC)模型基础上，提出一种权限约束支持的 RBAC 模型，利用 Datalog 逻辑语言描述约束策略，借助 Datalog 推理机实现一个“任务角色”分配的授权算法，解决工作流管理系统动态授权约束的问题。
关键词：授权约束；基于角色的访问控制；工作流；Datalog 逻辑语言

Authorization Constraint Method in Workflow Management Systems Based on RBAC

SHAN Xu-mei[1], YU Hui-qun[2]
(1. Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237;
2. Shanghai Key Laboratory of Computer Software Evaluating and Testing, Shanghai 201112)

【Abstract】To satisfy dynamic authorization of WorkFlow Management System(WFMS), this paper proposes a Role-Based Access Control(RBAC) model that supports authorization constraint. In this model, authorization constraint model for WFMS is specified by Datalog logical language and an authorization algorithm is implemented using Datalog's decision, making mechanisms. WFMS's dynamic constrained authorization problem is solved with the method.
【Key words】 authorization constraint; Role-Based Access Control(RBAC); workflow; Datalog logical language

1 概述

目前，基于角色的访问控制(Role-Based Access Control, RBAC)模型[1]仍是工作流管理系统访问控制的主要模型。约束是访问控制技术中的一个重要方面，从某种意义上是提出访问控制模型的原动力。

对约束的研究最早可以追溯到 1989 年，其后，文献[2]提出了一种在 WFMS 中对角色和用户任务指派的约束规则定义的语言，这种语言支持静态和动态职责分离(SOD)的描述。安全流则是对用户、角色、任务进行动态授权约束的工作流管理系统。文献[3]详细定义了连个相邻任务间的基数约束和蕴含约束(entailment constraints)。文献[4]提出了针对不同工作流模式的任务授权约束。

本文在基于 RBAC 的工作流模型的基础上以 Datalog[5]逻辑语言定义工作流中的授权约束策略，借助 Datalog 实现授权约束的自动决策，并给出一个“任务-角色”分配的授权算法。

2 工作流授权约束模型的定义

2.1 模型的基本概念和形式化描述

定义 1 概念

$W=\{T_i \mid i=1, 2, \cdots, n\}$表示工作流的任务集合；

$U=\{u_i \mid i=1, 2, \cdots, n\}$表示所有用户的集合；

$R=\{r_i \mid i=1, 2, \cdots, n\}$表示所有角色的集合；

$P=\{p_i \mid i=1, 2, \cdots, n\}$表示所有权限的集合。

$RTA \subseteq R \times T$ 是从任务集合到角色集合的多对多映射，表示任务可授权的角色；$URA \subseteq U \times R$ 是从角色集合到用户集合的多对多映射，表示角色可授权的用户；$PRA \subseteq P \times R$ 是从权限集合到角色集合的多对多映射，表示角色被赋予的权限；$RH \subseteq R \times R$ 是 R 上的一个偏序关系，称作角色层次或角色支配关系，用“$<$”表示。如果 $P(r_1) \subset P(r_2)$，则定义 $r_1 < r_2$；若 $P(r_1) \subseteq P(r_2)$，则定义 $r_1 \le r_2$。

定义 2 函数

$Role(T_i)=\{r \mid \exists(r' \ge r)[(r', T_i) \in RTA]\}$，返回任务授权权限时允许授权的角色集合；

$User(r_i)=\{u \mid (\exists r' \ge r_i)[(u, r') \in URA]\}$，返回指定给角色的用户集合；

$User(T_i)=User(T_{ir})=\{u \mid (\exists r' \ge T_{ir})[(u, r') \in URA]\}$，返回指定给任务的用户集合；

$P(r_i)=\{p \mid (\exists r' \le r_i)[(p, r') \in PRA]\}$，返回指定给角色的权限集合。

2.2 基于角色的工作流访问控制模型定义及其约束描述

工作流被定义为四元组 (W, E, A, CB)，其中，W 是所有任务的集合；$E=T \times T$ 表示任务间执行先后顺序的集合，如果 $(t, t') \in E$，则每个工作流实例任务 t 必须先于任务 t' 执行；$A \subseteq T \times R \times U$，且 $(t, r, u) \in A$ 表示用户 u 能够以角色 r 来执行任务 t；C 是工作流的约束集，$CB=\{C_1, C_2, \cdots, C_m\}$，$C(t_i) \in CB$，$C(t_i)$ 表示对任务 i 的约束；对于工作流实例 I 的一次执行分配可以表示为 $AU=\{(t_1, u_1, r_1), (t_2, u_2, r_2), \cdots, (t_n, u_n, r_n)\}$。$(t_i, u_i, r_i)$ 表示任务 $t_i \in T$ 由拥有 $r_i \in Role(t_i)$ 角色的用户 $u_i \in User(t_i)$ 执

基金项目：国家自然科学基金资助项目(60773094, 60473055)；上海市曙光计划基金资助项目(07SG32)
作者简介：单徐梅(1983－)，女，硕士研究生，主研方向：信息安全，软件工程；虞慧群，教授、博士、博士生导师
收稿日期：2009-08-08 **E-mail：**yhq@ecust.edu.cn

行，t_i 是任务 T_i 的执行实例。

2.3 基于 Datalog 的约束定义

2.3.1 约束规范的性质

在工作流中，任务的授权受到许多条件的制约。这些制约条件有些来自于工作流自身的规定，另一些来自于原系统内部的角色、用户及权限之间。工作流所涉及的所有约束关系集合用 $CB(W)$表示。$CB(w)$中的约束关系形如：$H \leftarrow Al, A2, \cdots, Am, \neg B1, \neg B2, \cdots, \neg Bm, n, m \geq 0$，其中，$H$, A, B 都是逻辑表达式；“ $\leftarrow$ ”表示逻辑递推关系。表 1 给出了下文用到的约束授权的逻辑表达式。

表 1 约束授权的逻辑表达式

逻辑谓词	表达式语义
pra	如果 $pra(U_i,T_j)$为真，则用户 U_i 允许执行任务 T_j ;同样如果 $pra(R_i,T_j)$ 为真，角色 R_j 允许执行任务 T_i
dra	如果 $dra(U_i,T_j)$为真，则用户 U_i 不允许执行任务 T_j；同样如果 $dra(R_i,T_j)$为真，则角色 R_j 不允许执行任务 T_i
execute	$execute(R_i,T_j,k)$表示角色 R_j 激活了任务 T_j 的第 k 次实例 $execute(U_i,T_j,k)$表示角色 U_i 激活了任务 T_j 的第 k 次实例
success	$success(T_i,k)$表示任务 T_i 的第 k 次实例执行完成
abort	$abort(T_i,k)$表示任务 T_i 的第 k 次实例执行中止

本节将以基于 RBAC 的工作流模型为基础，借助于 Datalog 语言对该模型的权限约束进行规范和实施。表 2 用一组规则集合表示授权约束策略。

表 2 基于 Datalog 的授权约束

Rule Name	Rule
(1)Inheriting Rule	senior(father, son)←; senior(*X*, *Y*) ← senior(*X*, *Z*), senior(*Z*, *Y*)
(2)User-Role Assigning Rule	ura(u, r) ← L1, L2, ⋯, Ln. Li($0 \leq i \leq n$) can be in, ura, app_; eg. ura(u,r) ← ; ura(u,r) ← ura(u,r1), in(r1 ,r, RH); ura(u, manager) ← ura(u, employee), level(u) > 5
(3)Task-Role Assigning Rule	pra(ur, T) ← L1,L2,⋯, Ln. Li($0 \leq i \leq n$)can be active, pra, app_; dra(ur, T) ← L1, L2, ⋯, Ln. Li($0 \leq i \leq n$)can be active, pra, app_; eg. dra (ri, T2) ←execute(rj, T1,k), in(ri, rj, RH); pra(Role, t2) ← senior(Role, R), pra(R, t1)
(4) Role Activation Rule	active(u, r) ← ura(u,r), C; eg. active(u, r) ← ura(u,r), r=manager
(5)Decision Rule	execute(ur, T, k) ← L1, L2, ⋯, Ln. Li($0 \leq i \leq n$) can be in, pra, app_; eg. execute(r, T, k) ← ; execute(r2, T', k) ← execute(r2, T, k), in(r1, r2, RH), in(T, T', T)
(6)Integrity Rule	error ←L1, L2, ⋯, Ln. Li($0 \leq i \leq n$)can be in, active, ura, pra, app_; eg. error ← active(u, r1), active(u, r2); error ← pra(u, T), dra(u,T)

2.3.2 实施机制

基于 Datalog 推理机的具体工作流程如图 1 所示。

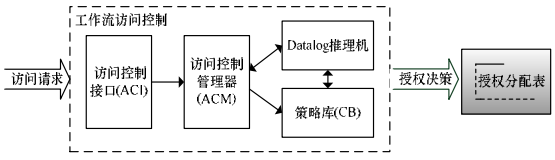

图 1 约束授权过程

由于工作流的动态特性，约束策略库也是动态的，每当任务 T 成功执行，都必须往策略库添加 success(t)和 execute(r,t,k)作为新的策略。文献[2]中的 BFA 模型定义了约束的规范和执行的算法，Datalog 推理机和策略库的引入使决策过程能够得到具体的实现。其中，引入策略库和推理机后，可以根据约束规则生成所有可行的角色分配方案。具体的算法步骤如下：递归调用函数 Assignment(int, int[])，每次递归从任务 i 的角色中取出一个角色加入 List 数组，然后通过 Datalog 推理机验证 List 数组中角色分配的合法性，如果合法，则从任务 i+1 的角色集中再取一个角色加入 List，直至 $i=n$ 时形成一个完整的任务-角色授权分配路径，将它加入授权分配表 DB，再开始寻找下一条路径，最后，生成完整的授权分配表 $DB = \{(T1, r_i), (T2, r_j), \cdots, (Tn, r_k)\}, r_i, r_j, r_k \in R$。

3 应用分析

3.1 案例描述

下文通过一个简单的企业原材料采购订单流程说明 Datalog 授权约束策略的规范和实施。图 2 是流程审核片断，包括 6 个流程任务：$T1$，采购人员制定原材料采购订单；$T2$，其他采购人员或采购主管对采购订单进行校对；$T3$，财务人员核算采购订单金额；$T4$，财务人员复核采购订单金额，如果订单金额小于 1 万元，则订单直接交给采购人员，如果订单金额大于 1 万元，则需要采购经理批准；$T5$，采购经理批准或否决订单；$T6$，采购订单由采购人员发送给供货商。此流程涉及以下角色：r_1 采购经理，r_2 采购主管，r_3 采购人员，r_4 财务人员。角色之间层次关系如图 3 所示。

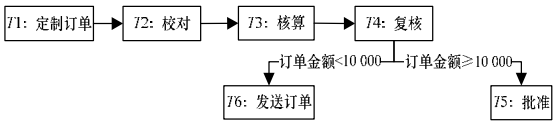

图 2 采购流程审核片段

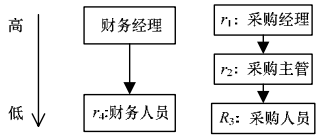

图 3 角色层次结构

3.2 约束定义

3.2.1 RBAC 模型元素

(1)相关的集合

USERS＝{bob, marry, tom, alice}，ROLES＝{purchase manager, finance manager, account, finance general, finance staff, purchase staff}，TASKS={T1, T2, T3, T4, T5, T6}。

(2)约束策略描述

流程的授权约束有：1)任务 T1 和 T2 必须由 2 个不同的角色执行；2)执行任务 T5 的角色支配执行任务 T2 的角色；3)任务 T1 和 T6 必须由同一个角色执行；4)任务 T1 的实例数不大于 3 次。

利用职责分离、职责绑定约束规则可以完成企业的流程安全策略，准确地界定执行动态职责分离要记录的系统上下文范围，降低系统运行时开销。

3.2.2 基于 Datalog 的规则描述

```
% role order
senior(purchase_manager,purchase_general)
senior(purchase_general,purchase_staff)
senior(finance_manager,finance_staff)
senior(X, Y) :- senior(X, Z), senior(Z, Y)
% task sequence
after(t2, t1)
after(t3, t2)
after(t4, t3)
after(t6, t4)
after(t5, t4)
% constraints definition
execute(R, T2, K) :- success(T1), after(T2, T1), pra(R, T2)
dra(R, T) :- not(pra(R, T))
pra(R, t2) :- execute(R1, t1, K), R1\=R
```

```
pra(R, t5) :- execute(R2, t2, K), senior(R, R2)
pra(R, t6) :- execute(R1, t1, K), R1=R
execute(R, t1, K) :- execute(R, t1, K), K<3
```

说明：程序中以大写字母开头的参数表示变量，如 T, R, X, Y，小写字母开头的参数表示常量，如 t1, bob。

3.3 执行结果

进入 DES 系统[5]时，首先导入 authorization.dl 程序，当程序被编译成功时，用户可以输入访问请求，系统执行程序，返回结果 yes 或 no，比如，系统规定任务 T1 的实例数不大于 3 次，但当不满足约束规则时则拒绝请求，如图 4 所示。

图 4　Datalog 执行结果

本例中，函数 Assignment(int, int[])的输入参数 n 为任务总数，等于 6，各个任务的允许角色集分别为 R1= $\{r_1, r_2, r_3\}$, $R2=\{r_2, r_3\}$, $R3=\{r_4\}$, $R4=\{r_4\}$, $R5=\{r_1\}$, $R6=\{r_1, r_2, r_3\}$。CB 则是 Datalog 逻辑语言描述的策略库，通过递归计算和 Datalog 推理机的决策最终生成如下授权分配表 DB：

$\{(T1, r_1), (T2, r_2), (T3, r_4), (T5, r_4), (T6, r_1), (T7, r_2)\}$, $\{(T1, r_1), (T2, r_2), (T3, r_4), (T4, r_4), (T5, r_1), (T6, r_3)\}$, $\{(T1, r_1), (T2, r_3), (T3, r_4), (T4, r_4), (T5, r_1), (T_6, r_2)\}$, $\{(T1, r_1), (T2, r_3), (T3, r_4), (T4, r_4), (T5, r_1), (T6, r_3)\}$, $\{(T1, r_2), (T2, r_3), (T3, r_4), (T4, r_4), (T5, r_1), (T6, r_1)\}$, $\{(T1, r_2), (T2, r_3), (T3, r_4), (T4, r_4), (T5, r_1), (T6, r_3)\}$, $\{(T1, r_3), (T2, r_2), (T3, r_4), (T4, r_4), (T5, r_1), (T6, r_2)\}$, $\{(T1, r_3), (T2, r_2), (T3, r_4), (T4, r_4), (T5, r_1), (T6, r_1)\}$

4　结束语

本文基于现有的 RBAC 模型，针对工作流环境下权限的动态性，提出基于 RBAC 的授权约束模型，详细定义了工作流的模型，用 Datalog 逻辑语言描述了授权约束，并以算法实现了授权分配，增强了 RBAC 模型在工作流应用中的实用性，弥补了传统模型权限描述与管理机制的不足。

今后的研究方向包括：约束的描述不限于 2 个任务间的蕴含约束和基数约束，可以加入上下文约束、时序约束、授权分配具体到任务-角色-用户的形式等。

参考文献

[1] Sandhu R S. Role-based Access Control Models[J]. IEEE Computer, l996, 29(2): 38-47.

[2] Bertino E, Ferrari E, Atluri V. The Specification and Enforcement of Authorization Constraints in Workflow Management Systems[J]. ACM Transactions on Information and System Security, 1999, 2(1): 65-104.

[3] Crampton J. A Reference Monitor for Workflow Systems with Constrained Task Execution[C]//Proceedings of the 10th ACM Symposium on Access Control Models and Technologies. New York, USA: ACM Press, 2005: 38-47.

[4] Wolter C, Schaad A, Meinel C. Task-based Entailment Constraints for Basic Workflow Patterns[C]//Proc. of SACMAT'08. Estes Park, Colorado, USA: [s. n.], 2008: 52-58.

[5] Pérez F S. Datalog Educational System V1.1 User's Manual[EB/OL]. (2004-10-23). http://www.fdi.ucm.es/profesor/fernan/DES/,

编辑　张正兴

(上接第 151 页)

如果 $\frac{p-1}{6}$ 是奇数，$\frac{q-1}{6}$ 是偶数，根据引理 5，$S_0(\alpha^k)=0, \forall k \in P \cup Q$。即

$$\left|\{k \mid S_0(\alpha^k)=0, k \in P \cup Q\}\right| = p-1+q-1 = p+q-2$$

再考虑式(2)，可得线性复杂度的下界为

$$L(s^\infty) = pq-1-\frac{(p-1)(q-1)}{2}-(p+q-2)=\frac{(p-1)(q-1)}{2}$$

由于 $6=\gcd(p-1,q-1)$，因此 $\frac{p-1}{6}$ 和 $\frac{q-1}{6}$ 不可能都为偶数，考虑到定理 1 和定理 2，定理 3 给出的下界也是所有 6 阶 W-广义割圆序列的线性复杂度的下界。

4　结束语

序列的伪随机性分析是密码学研究的重要内容[10-11]。本文考虑了 6 阶的第 1 类 W-广义割圆序列的线性复杂度。主要定理表明这类序列的线性复杂度下界为 $(p-1)(q-1)/2$，而且下界只可能在 $p-1/6$ 是奇数、$q-1/6$ 是偶数时取得；当 $p-1/6$ 是偶数、$p-1/6$ 是奇数时，这类序列总具有大于半个周期的线性复杂度；当 $p-1/6$ 和 $q-1/6$ 都是奇数时，6 阶 W-广义割圆序列的线性复杂度的下界是 $L(s^\infty)=pq+p-q+1/2$，当 p 和 q 的值比较接近时，这类序列的线性复杂度也能满足密码学的要求。由于用作密钥流的序列通常具有较大的周期，因此可以认为这里大多数的 6 阶 W-广义割圆序列的线性复杂度是好的。

参考文献

[1] Cusick T W, Ding Cunsheng, Renvall A. Stream Ciphers and Number Theory[M]. Amsterdam, Netherlands: Elsevier, 1998.

[2] Ding Cunsheng. Linear Complexity of Generalized Cyclotomic Binary Sequence of Order 2[J]. Finite Fields and Their Applications, 1997, 3(2): 159-174.

[3] Ding Cunsheng. Autocorrelation Values of Generalized Cyclotomic Sequences of Order Two[J]. IEEE Transactions on Information Theory, 1998, 44(5): 1699-1702.

[4] Bai Enjian, Fu Xiaotong, Xiao Guozhen. On the Linear Complexity of Generalized Cyclotomic Sequences of Order Four over Zpq[J]. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 2005, 88(1): 392-395.

[5] 闫统江, 张　宁, 肖国镇. 8 阶二元广义割圆序列的线行复杂度[J]. 中国石油大学学报: 自然科学版, 2006, 30(1): 142-145.

[6] Yan Tongjiang, Xiao Guozhen. Linear Complexity of Binary Whiteman Generalized Cyclotomic Sequences of Order 2^k[J]. Information Sciences, 2009, 179(7): 1019-1023.

[7] 闫统江, 范　凯, 杜小妮, 等. 二元 W-广义割圆序列的线性复杂度[J]. 西安电子科技大学学报: 自然科学版, 2006, 33(4): 617-621.

[8] Li Shengqiang, Chen Zhixiong, Sun Rong, et al. On the Randomness of Generalized Cyclotomic Sequences of Order Two and Length pq[J]. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 2007, 90(9): 2037-2041.

[9] Li Shengqiang, Chen Zhixiong, Fu Xiaotong, et al. The Autocorrelation Values of New Generalized Cyclotomic Sequences of Order Two and Length pq[J]. Journal of Computer Science and Technology, 2007, 22(6): 830-834.

[10] 白恩健, 刘晓娟. 阶数为 2 的 pq 周期广义割圆序列的自相关值[J]. 计算机工程, 2007, 33(19): 138-139.

[11] 杜小妮, 肖国镇. 周期为 p≡7(mod 8)的一类新六次剩余序列的迹表示[J]. 计算机工程, 2007, 33(7): 21-22.

编辑　张正兴