工作流系统带权角色与周期时间访问控制模型*

王小明[1,3+], 赵宗涛[2,3], 郝克刚[3]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](第二炮兵工程学院 计算机科学系,陕西 西安 710025)

[3](西北大学 计算机科学系,陕西 西安 710069)

A Weighted Role and Periodic Time Access Control Model of WorkFlow System

WANG Xiao-Ming[1,3+], ZHAO Zong-Tao[2,3], HAO Ke-Gang[3]

[1](Faculty of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](Department of Computer Science, The Second Artillery Engineering College, Xi'an 710025, China)

[3](Department of Computer Science, North-West University, Xi'an 710069, China)

+ Corresponding author: Phn: 86-29-5308774, E-mail: wangxm@snnu.edu.cn

http://www.snnu.edu.cn

Received 2003-01-09; Accepted 2003-07-14

Wang XM, Zhao ZT, Hao KG. A weighted role and periodic time access control model of workflow system. *Journal of Software*, 2003,14(11):1841~1848.

http://www.jos.org.cn/1000-9825/14/1841.htm

Abstract: A weighted role for activating task and periodic time authorization is an unsolved major problem for the access control of a workflow management system (WfMS). In this paper, a novel weighted role and periodic time access control (WRPTAC) model for WfMS is proposed on the basis of a role-based access control model. The periodic time expression method is discussed and then the new authorization concepts and the temporal authorization derivation rules for WfMS are defined respectively. An algorithm based on the graph theory for verifying the consistency of all the authorization derivation rules is presented, which has the time complexity of $O(n^2)$. The constraint rule for activating task is defined, which can express complex access control constraints for WfMS.

Key words: workflow; task; periodic time; weighted role; authorization constraint

摘 要: 带权角色激活任务和周期时间授权是工作流系统访问控制研究尚未解决的核心问题.以基于角色的访问控制模型为基础,提出了一种新的工作流系统带权角色与周期时间访问控制模型 WRPTAC(weighted role and periodic time access control).讨论了周期时间表示方法,定义了工作流系统授权新概念和时态授权推导规则,给出了时间复杂度为 $O(n^2)$的时态授权推导规则一致性验证图论算法,并定义了任务激活约束规则.它能够表达复杂的工作流系统访问控制约束.

* Supported by the National Natural Science Foundation of China under Grant No.90204012 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2002AA143021 (国家高技术研究发展计划(863))

第一作者简介: 王小明(1964－),男,甘肃天水人,教授,主要研究领域为信息安全,访问控制,工作流安全.

关键词: 工作流;任务;周期时间;带权角色;授权约束
中图法分类号: TP311 **文献标识码**: A

工作流是复杂多任务协同建模的一种有效方法.近年来,其理论研究和应用开发发展迅速.工作流系统的任务由特定的用户按照一定的组织规则执行.为了保证任务执行的安全性,实施组织安全政策(policy)的访问控制模型是工作流系统(简称 WfMS)必不可少的重要组成部分.访问控制主要通过访问授权约束实现组织安全政策,使获得权限的用户在满足所有约束前提下执行相应的操作.虽然已有许多访问控制模型(如 DAC,MAC,RBAC 等),但目前最适合工作流系统的是基于角色的访问控制模型 RBAC[1].然而,现有的 RBAC 模型不能表达复杂的工作流访问控制约束,特别是无法表达角色和用户执行任务的事务特征和周期时间授权约束,而这些恰恰是工作流系统最重要和最普遍的约束需求,是工作流安全研究领域长期以来未得到较好解决的一个重要问题,工作流联盟也尚未制定相关的规范与标准.现有的工作流系统研究主要集中在工作流过程建模上,对工作流系统访问控制讨论较少[2,3].为此,本文以一个简化的企业材料采购工作流为背景,提出一种工作流系统带权角色与周期时间访问控制模型(weighted role and periodic time access control,简称 WRPTAC).

WRPTAC 模型通过对执行任务的角色和用户赋予权值以表达在同一工作流任务实例的一次执行中,同一角色(用户)必须激活同一任务实例的次数,即任务执行的事务完整性约束.引入角色(用户)局部序关系,实现了多角色(用户)执行同一任务的序约束.通过对授权有效性实施周期时间限制以表达执行任务授权的周期时间约束.使用时态授权推导规则可以从显式授权推导出隐式授权,实现了任务执行的最小权限授权原则,并能够有效避免工作流过程建模中太多的任务分解,减少任务调度.

1 问题背景

以下讨论是在 RBAC 模型和 WfMS 基本知识的基础上进行,限于篇幅,RBAC 模型和 WfMS 基本知识请参阅文献[1~3].以一个简化的企业材料采购工作流为例阐述 WRPTAC 模型的原理.设材料采购工作流由以下 5 个任务组成:提出采购申请($task_1$),填制采购单($task_2$),审批采购单($task_3$),确认采购单($task_4$),执行采购($task_5$).其中 $task_1$ 由项目经理角色 *pr* 执行,$task_2$ 由财务职员角色 *cl* 执行,$task_3$ 由总经理角色 *ma* 和财务主管角色 *su* 协同执行,$task_4$ 由角色 *pr* 执行,$task_5$ 由角色 *cl* 执行.角色层次结构如图 1 所示,材料采购工作流如图 2 所示.其中 USER 表示执行任务的用户集合,弧上的数字表示每次执行任务所需要的用户数和角色激活任务的次数.

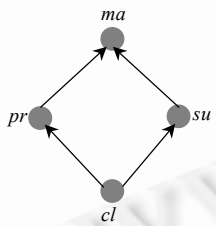

Fig.1 Role hierarchy structure
图 1 角色层次结构

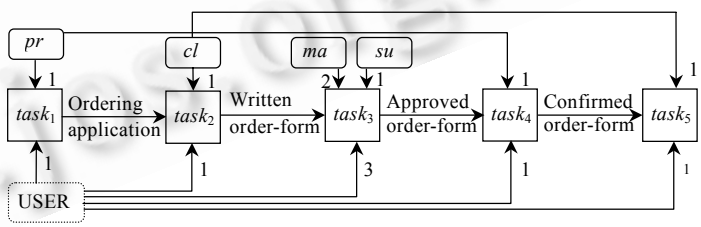

Fig.2 Workflow for material order process
图 2 材料采购工作流程

同一工作流实例的任务执行约束为:用户 *u* 已执行 $task_1$ 或 $task_2$,则禁止 *u* 执行 $task_3$ 和 $task_5$,但 *u* 已执行 $task_1$,则 *u* 必须执行 $task_4$. $task_3$ 必须先由 *ma* 激活,再由 *su* 激活,而两个不同用户分别使用 *ma* 激活 $task_3$ 的先后次序无关紧要.周期时间授权约束为:从 2002 年 1 月~2002 年 10 月,每月 15 日 8 点~15 点执行 $task_1$,每月 15 日和 16 日 8 点~15 点执行 $task_2$,每月 18 日 8 点~12 点执行 $task_3$,每月 18 日 14 点~17 点执行 $task_4$,每月 18 日和 19 日 8 点~12 点执行 $task_5$.为确保任务执行安全,需要授权有效时间与任务执行时间尽可能同步.如果使用传统的 RBAC 模型对上述材料采购工作流访问授权进行建模,则需要把 $task_3$ 分解为 3 个子任务,如图 3 所示.可以看出,当有大量任务需要分解时,必然造成工作流任务体系结构过于庞大,产生任务执行步骤错误时难于回滚(roll back),而且任务分解本身往往是困难或生硬的,有时候还可能破坏任务之间固有的结构.另一方面,传统的

RBAC 无法直接表达上述周期时间和基于任务执行历史的授权约束,不得不使用应用程序编码并嵌入到任务定义之中,使工作流系统难以适应环境约束变化.目前,支持时间约束或周期时间授权的访问控制模型比较少[4].现有的访问授权模型都不是针对工作流系统而提出的,因此不适合或不完全适合工作流系统.

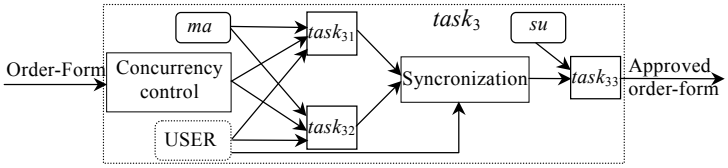

Fig.3 Divided task $task_3$

图 3 被分解任务 $task_3$

从上述材料采购工作流访问控制需求可以得出适合绝大多数工作流系统的 4 条重要访问控制策略:

策略 1. 工作流任务执行必须在特定的时间(包括周期时间)由特定的用户使用特定的角色完成.

策略 2. 在工作流任务实例的一次执行中,多角色可以分别一次或多次激活任务.

策略 3. 在工作流任务实例的一次执行中,多用户可以分别一次或多次激活任务.

策略 4. 在工作流任务实例的一次执行中,多用户或多角色激活任务必须是有序的.

传统的访问控制模型无法直接表达上述工作流访问控制策略 1~策略 4.本文针对这一问题,在 RBAC 模型基础上提出一种适合工作流系统的访问控制模型 WRPTAC,它能够有效地表达策略 1~策略 4,并保持 RBAC 模型原有的主要功能和特点.

2 WRPTAC 模型

2.1 工作流及其访问授权

工作流是一个二元组 Wf=(TASK,CONSTRAINT),其中 TASK 是任务集合,CONSTRAINT 是执行任务约束集合.任务是工作流的最小可执行单元,任务之间可能存在复杂的依赖关系.WfMS 使工作流任务协同执行以实现特定的组织目标.目前,绝大多数 WfMS 把 RBAC 作为其访问控制模型.RBAC 在工作流环境下的主要构成要素是任务、角色、用户、权限、会话和约束.角色是一个组织概念,它可以表示职务、岗位和职责等.任务既分配给角色又分配给用户,授权执行任务的用户如果获得了执行任务所需要的角色,则其具有执行相应任务的资格,只有当会话激活任务和执行该任务所需要的角色和用户时,用户才能使用该角色包含的权限执行任务.与本文相关的 RBAC 模型定义如下.

定义 1. 工作流环境下基于角色的访问控制模型 RBAC=(TASK,ROLE,USER,PERM,SESSION,CONSTRAINT),其中 TASK 是工作流任务集合,ROLE 是角色集合,USER 是用户集合,PERM 是权限集合,SESSION 是用户-角色-任务的会话集合,CONSTRAINT 是激活任务约束集合.定义下列关系:

(1) 任务-角色赋值关系: TRA⊆TASK×ROLE,($task$,r)∈TRA 表示授权角色 r 可以执行任务 $task$.

(2) 任务-用户赋值关系: TUA⊆TASK×USER,($task$,u)∈TUA 表示授权用户 u 可以执行任务 $task$.

(3) 用户-角色赋值关系: URA⊆USER×ROLE,(u,r)∈URA 表示用户 u 享有角色 r.

(4) 角色-权限赋值关系: RPA⊆ROLE×PERM,(r,p)∈RPA 表示角色 r 包含权限 p.

(5) 角色层次偏序关系: RH⊆ROLE×ROLE,(r_i,r_j)∈RH 表示角色 r_i 是角色 r_j 的父角色,r_j 是 r_i 的子角色,父角色继承其子角色的权限.

(6) 激活关系:STRU⊆SESSION×TASK×2^{ROLE}×USER,(s,$task$,{r_1,…,r_m},u)∈STRU 表示会话 s 激活 $task$,授权执行 $task$ 的用户 u 和一组角色 r_1,…,r_m.其中 2^{ROLE} 表示 ROLE 的幂集合.

(7) 任务执行偏序关系:TO⊆TASK×TASK,($task_i$,$task_j$)表示成功执行 $task_i$ 之后才能激活 $task_j$.

工作流的基本执行过程是从首任务开始,在相应约束满足的前提下通过会话激活任务和执行任务所需要的角色以及用户.如果被激活的用户享有被激活的角色,则用户可以执行该任务.但是,上述 RBAC 不能直接表达一次任务执行中角色必须激活任务的总次数和周期时间授权约束,因此任务执行的事务完整性和用户授权的最小权限原则难以保证.

2.2 周期时间表示

执行任务的周期时间约束是绝大多数工作流系统所具有的重要特征.周期时间表示则是实现周期时间约束的关键.时间包括连续时间和离散时间两种.为简单起见,本文以离散时间为讨论对象,连续时间讨论与此类似.设 $T=\{t_0,t_1,\ldots\}$是离散时间轴上的连续点构成的无限集合.周期时间用序偶$([t_s,t_e],P)$表示,其中 P 是周期时间表达式,表示周期时间区间的无限集合;$t_s,t_e\in T$ 是对 P 的时间上下限约束,并且 $t_s\le t_e$.称离散时间轴上的连续点构成的集合$[t_s,t_e]$为时间区间,t_s-t_e 表示其长度,记作$|[t_s,t_e]|$.本文使用文献[4]的日历概念定义周期时间表达式.日历是指相邻时间区间的可数无限集合,其元素用自然数标记,称为时间区间索引.两个时间区间$[t_{s1},t_{e1}]$和$[t_{s2},t_{e2}]$是相邻的,当且仅当 $t_{e1}<t_{s2}$,并且不存在时间点 $t\in T$,使得 $t_{e1}<t<t_{s2}$.两个相邻的时间区间可以归并为一个时间区间,记作 $[t_{s1},t_{e1}]\cup[t_{s2},t_{e2}]=[t_{s1},t_{e2}]$. 例如,$[1,2]\cup[3,4]=[1,4]$. 如果 $t_{s2}\le t_{s1}$, 并且 $t_{e1}\le t_{e2}$, 则称 $[t_{s2},t_{e2}]$ 包含 $[t_{s1},t_{e1}]$, 记作 $[t_{s1},t_{e1}]\Subset[t_{s2},t_{e2}]$.对任意 $t\in T,[t_s,t_e]\in T\times T$,若 $t_s\le t\le t_e$,则称 t 在$[t_s,t_e]$内,记作 $t\in[t_s,t_e]$.对任意$[t_{s1},t_{e1}],[t_{s2},t_{e2}]\in$T×T,若 $t_{s2}\le t_{e1}$,并且 $t_{e1}\le t_{e2}$,则两个时间区间的交为$[t_{s1},t_{e1}]\cap[t_{s2},t_{e2}]=[\max(t_{s1},t_{s2}),\min(t_{e1},t_{e2})]$.其中 max 和 min 分别是取大和取小函数.

定义 2. 已知两个日历 C_1 和 C_2,若断言$\forall[t_{s1},t_{e1}]\in C_1,\exists C_2'\subseteq C_2:[t_{s1},t_{e1}]\Subset\bigcup_{[t_{s2},t_{e2}]\in C_2'}[t_{s2},t_{e2}]$为真,则称 C_1 是 C_2 的子日历,记作 $C_1\sqsubseteq C_2$.

显然,关系$\sqsubseteq$是自反的、反对称的和传递的.使用日历概念定义周期时间表达式如下:

定义 3. 设 $C_1,C_2,\ldots,C_n,C_d$ 是日历,周期时间表达式 P 定义为

$$P=\sum_{i=1}^{n}O_i.C_i\triangleright r.C_d.$$

其中,$O_i\in 2^{\aleph_0}\cup\{all\}$是 C_i 的时间区间索引子集,all 表示 C_i 的所有时间区间索引.$C_i\sqsubseteq C_{i-1},i=1,2,3,\ldots,n,C_d\sqsubseteq C_n$ 是时间区间的长度单位.$\aleph_0$是自然数集合,$r,n\in\aleph_0,r$ 为时间区间长度.

定义 3 的符号▷左端表示周期时间表达式所表示的时间区间左端点的集合.为简化描述,以下使用英文单词表示日历时间,如年(*year*)、月(*month*)、日(*date*)、小时(*hour*)等.例如,

$$\sum_{i=1}^{3}O_i.C_i=all.year+\{2,6\}.month+\{3\}.day$$

表示每年 2 月 3 日和 6 月 3 日构成的时间点集合.周期时间表达式 P 对应的时间区间无限集合记作 $\prod(P)$,形式定义如下:

定义 4. 设 $P=\sum_{i=1}^{n}O_i.C_i\triangleright r.C_d$ 是周期时间表达式,则 P 对应的时间区间无限集合 $\prod(P)=\{[t_s,t_e]\mid|[t_s,t_e]|=r.C_d,t_s\in S\}$,其中日历 C_d 表示时间区间长度单位,S 定义为:

(1) 若 $n=1$,则 S 由日历 C_1 的索引在 O_1 中的所有时间区间左端点构成;

(2) 若 $n>1$,

$$\sum_{i=1}^{n}O_i.C_i=\sum_{i=1}^{n-1}O_i.C_i+O_n.C_n\ ,$$

则 S 由 $\sum_{i=1}^{n-1}O_i.C_i$ 中的每一个时间点与 C_n 的索引在 O_n 中的时间区间左端点连接后形成的时间点构成.

例:设 $P=all.year+\{2,4\}.month+\{3\}.day\triangleright 4.day$,则 $S=\{$每年 2 月 3 日,每年 4 月 3 日$\}$,$\prod(P)=\{[$每年 2 月 3 日,同年 2 月 7 日$]$,$[$每年 4 月 3 日,同年 4 月 7 日$]\}$.

对$\forall[t_s,t_e]\in T\times T$,周期时间$([t_s,t_e],P)$表示的时间点集合形式定义为:

定义 5. 设 $t\in T$ 是时间点,$[t_s,t_e]$是时间区间,P 是周期时间表达式,周期时间$([t_s,t_e],P)$表示的时间点集合 $TPS([t_s,t_e],P)=\{t\mid\tau\in\prod(P),t\in\tau,\ t_s\le t\le t_e\}$.

例:周期时间表达式 $P=all.year+\{8,10\}.month+\{25\}.day+8.hour\triangleright 2.hour$ 表示每年 8 月 25 日 8 点至 10 点和 10 月 25 日 8 点至 10 点,则 TPS([97/9,99/9],*P*)={97/10/25:8,97/10/25:9,97/10/25:10,98/8/25:8,98/8/25:9, 98/8/25:10, 98/10/25:8,98/10/25:9,98/10/25:10, 99/8/25:8,99/8/25:9,99/8/25:10}.

2.3 工作流带权角色周期时间访问授权

为了有效地表达工作流带权角色周期时间访问授权约束,我们定义了下列工作流授权新概念.

定义 6. 工作流基本角色授权是一个四元组 $grant=(task,\langle roleset(task),\prec^r\rangle,\langle userset(task),\prec^u\rangle,n)$,其中 $task\in$TASK,$roleset(task)=\{r|(task,r)\in$TRA$\}\subseteq$ROLE 是执行 *task* 的最小角色集合,$\prec^r$ 是 $roleset(task)$上的局部角色偏序关系,表示角色激活任务的序约束.对 $\forall r_i,r_j\in roleset(task),r_i\prec^r r_j$ 表示 r_i 优先于 r_j 激活任务 *task*. $userset(task)=\{u|(task,u)\in$TUA$\}\subseteq$USER 是执行 *task* 的用户集合,$\prec^u$ 是 $userset(task)$上的局部用户偏序关系,表示用户激活任务的序约束.对 $\forall u_i,u_j\in userset(task),u_i\prec^r u_j$ 表示 u_i 优先于 u_j 激活任务 *task*.*n* 是 *task* 成功执行一次必须激活的总次数.

称角色层次关系 RH 上 *r* 及 *r* 的父角色全集为 *r* 的类,记为 $[r]_{\mathrm{RH}}$,则 $[r]_{\mathrm{RH}}$ 按下列式子求得:

$$[r]_{\mathrm{RH}}=\{r'|r,r'\in\mathrm{ROLE},(r',r)\in\mathrm{RH}\}. \tag{1}$$

对 $\forall r\in roleset(task)$,属于 *r* 类的角色可以相互代理执行任务 *task*,其序约束与 *r* 相同.因此,执行任务的角色集合可以扩展为角色类的集合.按 RBAC 模型中父角色继承子角色的权限语义[1],对 $\forall r'\in[r]_{\mathrm{RH}}$,$r'$ 包含的权限集合为

$$perm(r')=\{p|p\in\mathrm{PERM},r''\in\mathrm{ROLE},(r',r'')\in\mathrm{RH},(r'',p)\in\mathrm{PRA}\}. \tag{2}$$

用 $|r|$ 表示 *r* 包含的权限个数.按 $|r|$ 由小到大排列使 $[r]_{\mathrm{RH}}$ 成为有序集,在保持其他约束的前提下,容易选择包含权限尽可能少的角色执行任务,从而能够实现访问授权的最小权限原则.在一次任务执行中,不同角色激活任务的次数有可能不同.例如,第 1 节的材料采购工作流中任务 $task_3$ 的一次执行需要角色 *ma* 激活 $task_3$ 两次,而仅需 *su* 激活 $task_3$ 一次.把角色(用户)激活任务的次数称为角色(用户)关于任务的权重,用权函数表示.为精确表达这种授权约束,定义工作流的带权角色授权如下:

定义 7. 工作流带权角色授权是一个三元组 $wgrant=(grant,weight_r,weight_u)$,其中 *grant* 是工作流的基本角色授权,函数 $weight_r$:TASK×ROLE→№是角色关于任务的权函数,对 $\forall task\in$TASK,$\forall r\in$ROLE,如果 $r\in roleset(task)$,则 $weight_r(task,r)$表示在 *task* 的一次执行中 *r* 必须激活 *task* 的次数.函数 $weight_u$:TASK×USER→№是用户关于任务的权函数,对 $\forall task\in$TASK,$\forall u\in$USER,如果 $u\in userset(task)$,则 $weight_u(task,u)$表示在 *task* 的一次执行中 *u* 必须激活 *task* 的次数.

当角色或用户激活任务的权函数值为 1,或任务执行一次其必须激活的总次数为 1 时,在授权说明中通常省略.根据定义 6 和定义 7,对 $\forall task\in$TASK,*n* 为一次 *task* 执行必须激活的次数,则下列式子必须满足:

$$\sum_{r\in roleset(task)} weight_r(task,r)=n, \tag{3}$$

$$\sum_{u\in roleset(task)} weight_u(task,u)=n. \tag{4}$$

设 $r\in roleset(task)$,对 $\forall r'\in[r]_{\mathrm{RH}}$,$r'$ 实际激活 *task* 的次数为 $f(task,r')$,则下式必须满足:

$$\sum_{r'\in[r]_{RH}} f(task,r')=weight_r(task,r). \tag{5}$$

在上述周期时间和工作流带权角色授权概念的基础上,定义工作流带权角色周期时间授权如下:

定义 8. 工作流带权角色周期时间授权是一个二元组 $wpgrant=(([t_s,t_e],P),wgrant)$,其中 $([t_s,t_e],P)$是周期时间,*wgrant* 是工作流带权角色授权,*wgrant* 只在 TPS$([t_s,t_e],P)$内的每一个时间点有效.

周期时间约束沿角色层次关系向上继承,即父角色不仅继承子角色的权限,而且继承其周期时间约束.

由以上定义可以看出,工作流基本角色授权可以用角色和用户关于任务的权函数值为 1 的带权角色授权表示,基本角色授权和带权角色授权可以用周期时间为无穷(∞)的带权角色周期时间授权表示.所以,工作流带权角色周期时间授权比前两种授权具有更强的表达能力,它能够简化工作流过程建模和任务调度.显然,使用上述工作流系统授权新概念很容易表达第 1 节的工作流系统访问控制策略 1~策略 4 的授权约束.

2.4 WRPTAC模型时态授权推导规则

在 WRPTAC 模型中,除了显式授权之外,使用时态授权推导规则可以推导隐式授权,实现授权依赖约束,减小显式授权规模,从而提高授权管理效率.设 *wgrant* 是工作流带权角色授权,$([t_s,t_e],P)$是周期时间,它表示时态授权推导规则的有效时间范围,谓词 $\mathcal{J}(t,wgrant)$表示如果在时刻 *t* 授权 *wgrant* 是显式的或者可以推导的,则其值为真,否则为假.时态授权推导规则定义如下:

规则 1. $\forall t\in \mathrm{TPS}([t_s,t_e],P):\mathcal{J}(t,wgrant_1)\rightarrow\mathcal{J}(t,wgrant_2)$.

规则 2. $\forall t\in \mathrm{TPS}([t_s,t_e],P),\forall t'\in \mathrm{TPS}([t_s,t],P):\mathcal{J}(t',wgrant_1)\rightarrow\mathcal{J}(t,wgrant_2)$.

规则 3. $\forall t\in \mathrm{TPS}([t_s,t_e],P),\exists t'\in \mathrm{TPS}([t_s,t],P):\mathcal{J}(t',wgrant_1)\rightarrow\mathcal{J}(t,wgrant_2)$.

规则 4. $\forall t\in \mathrm{TPS}([t_s,t_e],P):\neg\mathcal{J}(t,wgrant_1)\rightarrow\mathcal{J}(t,wgrant_2)$.

规则 5. $\forall t\in \mathrm{TPS}([t_s,t_e],P),\forall t'\in \mathrm{TPS}([t_s,t],P):\neg\mathcal{J}(t',wgrant_1)\rightarrow\mathcal{J}(t,wgrant_2)$.

规则 6. $\forall t\in \mathrm{TPS}([t_s,t_e],P),\exists t'\in \mathrm{TPS}([t_s,t],P):\neg\mathcal{J}(t',wgrant_1)\rightarrow\mathcal{J}(t,wgrant_2)$.

为描述简单,设$\mathcal{E}_{B-E}$=TPS($[t_s,t_e]$,P),B 为规则前件,E 为规则后件.称规则 1~规则 3 为正规则,用$\mathcal{E}_{B-E}$:$+B\rightarrow E$ 表示,其语义为"在时间集$\mathcal{E}_{B-E}$内,若 B,则 E".称规则 4~规则 6 为负规则,用$\mathcal{E}_{B-E}$:$\neg B\rightarrow E$ 表示,其语义为"在时间集$\mathcal{E}_{B-E}$内,若非 B,则 E",正、负规则用通式$\mathcal{E}_{B-E}$:$B\rightarrow E$ 表示.对用户而言,在任何时刻其所获得的显式授权和隐式授权的使用效果完全相同.工作流 Wf 的所有带权角色周期时间授权和时态授权推导规则构成授权推导规则库 DRB(Wf).从 DRB(Wf)中既可以在工作流开始执行之前静态推导授权,也可以在任务调度过程中动态推导授权.静态推导授权能够节省任务调度时间,但不能实现某些授权动态职责分离;动态推导授权能够有效实现授权动态职责分离,但可能延长任务调度时间.因此,采用何种授权推导策略需要根据具体工作流系统需要进行选择.

2.5 时态授权推导规则库一致性判定

一个有效的工作流授权或授权推导规则必须满足 DRB(Wf)的一致性要求.

定义 9. 设 DRB(Wf)是工作流 Wf 的时态授权推导规则库,如果运用 DRB(Wf)中的规则能够推导出矛盾,则称 DRB(Wf)是不一致的,否则称为一致的.

直接根据定义 9 对 DRB(Wf)的不一致性进行判定是困难的.但是,如果把 DRB(Wf)中的规则关系用带标识的有向图表示,用图的有关理论对 DRB(Wf)的不一致性进行判定则相对比较简单.DRB(Wf)的规则关系标识有向图定义为:

定义 10. 设 DRB(Wf)的带标识有向图为 $G(V,H)$.其中,$V=\{E|\mathcal{E}_{B-E}:B\rightarrow E\in\mathrm{DRB(Wf)}\}$ 是顶点集合,$H=\{(B,(\mathcal{E}_{B-E}:+),E)|\mathcal{E}_{B-E}:+B\rightarrow E\in\mathrm{DRB(Wf)},B\in V\}\cup\{(B,(\mathcal{E}_{B-E}:-),E)|\mathcal{E}_{B-E}:\neg B\rightarrow E\in\mathrm{DRB(Wf)},B\in V\}$是带标识的有向边集合,其中$(\mathcal{E}_{B-E}:+)$,$(\mathcal{E}_{B-E}:-)$为有向边的标识.

DRB(Wf)的规则关系用标识有向图表示后,其不一致性等价于标识有向图中存在包含一条"–"边的环,并且这个环的所有边的标识时间集的交集是非空的.这个结论的正确性由下面的定理 1 给予保证.

定理 1. 设 $G(V,H)$是 DRB(Wf)的标识有向图,如果在 $G(V,H)$中存在包含一条"–"边的环,并且这个环的所有边的标识时间集的交集非空,则 DRB(Wf)是不一致的.

于是,DRB(Wf)一致性判定问题转化为判定其标识有向图中是否存在包含一条"–"边的环,并且这个环的所有边标识时间集的交集非空问题.

定理 2. 设 $G(V,H)$是 DRB(Wf)的标识有向图,$G(V,H)$中存在包含一条"–"边的环,当且仅当存在 $G(V,H)$的强连通分量 $L(N,J)$,并且 $L(N,J)$包含一条"–"边.

根据上述定义和定理给出一个基于图理论的 CRB(Wf)一致性验证算法(伪码).

算法 1. DRB(Wf)一致性验证算法.

输入:一个 DRB(Wf);

输出:若 DRB(Wf)是一致的,则返回 true,否则返回 false;

```
begin   /* 构造 DRB(Wf)的标识有向图 G(V,H) */
  V←∅
  H←∅
  for 每一个ℰ_{B-E}:B→E∈DRB(Wf) do V←V∪{E}
  for 每一个ℰ_{B-E}:B→E∈DRB(Wf) do
      begin
        if ℰ_{B-E}: B→E=ℰ_{B-E}:+B→E and B∈V then H←H∪{(B, (ℰ_{B-E}:+),E)}
```

if $\mathcal{E}_{B-E}$: $B\rightarrow E=\mathcal{E}_{B-E}$: $\neg B\rightarrow E$ **and** $B\in V$ **then** $H\leftarrow H\cup\{(B,(\mathcal{E}_{B-E}:-),E)\}$

end

/* 求 $G(V,H)$的强连通分量,查找包含一条"-"边并且所有边的标识时间集的交集非空的环 */

$\mathcal{L}\leftarrow\{G(V,H)$的所有强连通分量$\}$

if 存在 $L(N,J)\in\mathcal{L}$ **and** $L(N,J)$包含一条'-' 边 **and** J 中的所有边的标识时间集的交集非空

then return(false) **else return**(true)

end

定理 3. 算法 1 是正确的,并且时间复杂度为 $O(n^2)$,其中 n 为 DRB(Wf)所包含的规则数.

根据上述定义和定理以及图的强连通算法时间复杂度理论,容易证明定理 3 的正确性.

3 工作流任务激活约束规则

在 WRPTAC 模型中,工作流访问授权的事务特征约束需要在任务激活时实施,通过任务激活约束规则来实现.为形式定义任务激活约束规则,首先定义下列谓词和函数.设$\mathcal{E}$=TPS([t_s,t_e],P).

定义 11(**谓词**). $\mathcal{F}_u(\mathcal{E},u,task,k)$:若 u 在$\mathcal{E}$内某时刻第 k 次成功激活 $task$,则其值为真.$\mathcal{F}_r(\mathcal{E},r,task,k)$:若 r 在$\mathcal{E}$内某时刻第 k 次成功激活 $task$,则其值为真.$\mathcal{P}_u(\mathcal{E},u,task)$:若必须由 u 在$\mathcal{E}$内某时刻激活 $task$,则其值为真.$\mathcal{P}_r(\mathcal{E},r,task)$:若必须由 r 在$\mathcal{E}$内某时刻激活 $task$,则其值为真.$\mathcal{F}_u(\mathcal{E},u,task)$:若禁止 u 在$\mathcal{E}$内某时刻激活 $task$,则其值为真.$\mathcal{C}_u(\mathcal{E},[u]_G,task)$:若用户组 G 中的每一个用户 u 在$\mathcal{E}$内某时刻可以激活 $task$,则其值为真.$\mathcal{F}_r(\mathcal{E},r,task)$:若禁止 r 在$\mathcal{E}$内某时刻激活 $task$,则其值为真.$\mathcal{T}_r(\mathcal{E},[r]_{RH},task)$:若每一个 $r'\in[r]_{RH}$ 在$\mathcal{E}$内某时刻可以激活 $task$,则其值为真.$\mathcal{H}(task,k)$:若第 k 次激活 $task$ 成功,则其值为真.

定义 12(**函数**). $\omega_r(r,task,n)$从授权说明日志中返回 r 激活 $task$ 的权重 n. $\omega_u(u,task,n)$从授权说明日志中返回 u 激活 $task$ 的权重 n.$\chi(task,n)$从授权说明日志中返回一次 $task$ 执行必须激活的次数 n. $\zeta_r(r,task,n)$从任务执行历史日志中返回 r 已成功激活 $task$ 的次数 n.$\zeta_u(u,task,n)$从任务执行历史日志中返回 u 已成功激活 $task$ 的次数 n. $\zeta(task,n)$从任务执行历史日志中返回 $task$ 已成功激活的总次数 n.

工作流任务激活(执行)约束规则定义为:

定义 13. 具有以下形式的规则称为工作流任务激活约束规则 ^cR:

$$C_1\wedge C_2\wedge\ldots\wedge C_m\wedge\neg C'_1\wedge\neg C'_2\wedge\ldots\wedge\neg C'_v\rightarrow D,$$

其中 C_i,C'_j 是上述定义的谓词或由关系运算<,=,>,≠,≤和≥联接的上述定义的函数构成的逻辑比较词,D 是上述定义的谓词,$\neg C'_j$ 表示 C'_j 的否定,$m\geq 0$,$v\geq 0$,$C_i\neq C'_j$.

使用上述规则很容易实现第 1 节的策略 1~策略 4 所要求的任务激活约束.工作流 Wf 的所有任务激活约束规则构成约束规则库 CRB(Wf).有效的任务激活约束规则必须满足 CRB(Wf)的一致性要求.类似时态授权推导规则一致性讨论,可以对 CRB(Wf)一致性进行分析,本文不再详述.

4 实 例

以第 1 节的材料采购工作流为例,用 WRPTAC 模型对其授权与任务执行约束建模.设周期时间点集分别为

$\mathcal{E}_1$=TPS([01,10],*all.month*+{15}.day+8.hour▷7.*hour*).

$\mathcal{E}_2$=TPS([01,10],*all.month*+{15,16}.day+8.hour▷7.*hour*).

$\mathcal{E}_3$=TPS([01,10],*all.month*+{18}.day+8.hour▷4.*hour*).

$\mathcal{E}_4$=TPS([01,10],*all.month*+{18}.day+14.hour▷3.*hour*).

$\mathcal{E}_5$=TPS([01,10],*all.month*+{18,19}.day+8.hour▷4.*hour*).

任务执行偏序关系为($task_1$,$task_2$),($task_2$,$task_3$),($task_3$,$task_4$),($task_4$,$task_5$)∈TO.

限于篇幅,以下只给出执行 $task_2$ 的授权推导规则,并对授权推导过程进行说明,假设执行其他 4 个任务的授权是显式授予的.即假设已存在授权(考虑了角色层次关系):

$g_1=(\mathcal{E}_1,(task_1,\langle\{\{pr,ma\}\}\rangle,\langle\{u_1\}\rangle,1))$.

$g_3=(\mathcal{E}_3,(task_3,\langle\{\{ma\},\{su,ma\}\},su\prec^r ma\rangle,\langle\{u_3,u_4,u_5\},u_3\prec^u u_4,u_3\prec^u u_5\rangle,3),weight_r(task_3,ma)=2))$.

$g_4=(\mathcal{E}_4,(task_4,\langle\{\{pr,ma\}\}\rangle,\langle\{u_1\}\rangle,1))$.

$g_5=(\mathcal{E}_5,(task_5,\langle\{\{cl,pr,su,ma\}\}\rangle,\langle\{u_6\}\rangle,1))$.

定义下列时态授权推导规则:

${}^aR_1$: $\forall t\in\mathcal{E}_2:\mathcal{J}(t,(task_1,\langle\{\{pr,ma\}\}\rangle,\langle\{u_1\}\rangle,1))\rightarrow\mathcal{J}(t,(task_2,\langle\{\{cl,pr,su,ma\}\}\rangle,\langle\{u_2\}\rangle,1))$,

${}^aR_2$: $\forall t\in\mathcal{E}_2:\neg\mathcal{J}(t,(task_1,\langle\{\{pr,ma\}\}\rangle,\langle\{u_1\}\rangle,1))\rightarrow\mathcal{J}(t,(task_2,\langle\{\{cl,pr,su,ma\}\}\rangle,\langle\{u_2\}\rangle,1))$,

则由 g_1 和 ${}^aR_1$ 推导得到 $g'=(\mathcal{E}_1\cap\mathcal{E}_2,(task_2,\langle\{\{cl,pr,su,ma\}\}\rangle,\langle\{u_2\}\rangle,1))$,由 g_1 和 ${}^aR_2$ 推导得到 $g''=(\mathcal{E}_2\backslash\mathcal{E}_1,(task_2,\langle\{\{cl,pr,su,ma\}\}\rangle,\langle\{u_2\}\rangle,1))$,将 g'和 g''关于时间进行归并得到 $g_2=(\mathcal{E}_2,(task_2,\langle\{\{cl,pr,su,ma\}\}\rangle,\langle\{u_2\}\rangle,1))$.所以材料采购工作流的全部有效授权为 g_1,g_2,g_3,g_4,g_5.任务激活约束规则定义为

${}^cR_1$: $\mathcal{H}_r(\mathcal{E}_1,pr,task_1,\omega_r(pr,task_1,n))\rightarrow\wp_r(\mathcal{E}_2,cl,task_2)$ ${}^cR_2$: $\mathcal{H}_r(\mathcal{E}_2,cl,task_2,\omega_r([cl]_{RH},task_2,n))\rightarrow\wp_r(\mathcal{E}_3,ma,task_3)$

${}^cR_3$: $\mathcal{H}_r(\mathcal{E}_3,ma,task_3,\omega_r(ma,task_3,n))\rightarrow\wp_r(\mathcal{E}_3,su,task_3)$ ${}^cR_4$: $\mathcal{H}(task_3,\chi(task_3,n))\rightarrow\wp_r(\mathcal{E}_4,pr,task_4)$

${}^cR_5$: $\mathcal{H}_r(\mathcal{E}_4,pr,task_4,\omega_r(pr,task_1,n))\rightarrow\wp_r(\mathcal{E}_5,cl,task_5)$ ${}^cR_6$: $\mathcal{H}_u(\mathcal{E}_1,u,task_1,1)\rightarrow\mathcal{F}_u(\mathcal{E}_2,u,task_2)$

${}^cR_7$: $\mathcal{H}_u(\mathcal{E}_2,u,task_2,1)\rightarrow\mathcal{F}_u(\mathcal{E}_3,u,task_3)$ ${}^cR_8$: $\mathcal{H}_u(\mathcal{E}_1,u,task_1,1)\rightarrow\wp_u(\mathcal{E}_4,u,task_4)$

${}^cR_9$: $\mathcal{H}_u(\mathcal{E}_3,u,task_3,1)\rightarrow\mathcal{F}_u(\mathcal{E}_5,u,task_5)$ ${}^cR_{10}$: $\mathcal{H}_u(\mathcal{E}_1,u,task_1,1)\rightarrow\mathcal{F}_u(\mathcal{E}_5,u,task_5)$

使用经典逻辑的规则执行算法执行上述规则,即可实现材料采购工作流的访问控制.

5 结 论

工作流系统的访问控制模型是当前 WfMS 研究的一个重要课题.本文以新一代访问控制模型 RBAC 为基础,提出了 WfMS 带权角色与周期时间访问控制模型 WRPTAC,有效解决了 WfMS 的带权角色激活任务和周期时间授权约束建模问题.它能够在保持工作流任务固有的结构下,避免太多的任务分解,减少任务调度次数,通过时态授权推导规则能够实现授权推理,支持激活任务的最小权限授权原则,提高授权管理效率.由 WRPTAC 模型表达的授权说明到访问控制规则系统自动转换算法和高效规则执行算法,我们正在深入研究,将另文介绍.

References:

[1] Ferraiolo DF, Sandhu R, Guirila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, 2001,4(3):224~274.

[2] Botha RA, Eloff JHP. Access control in document centric workflow system: an agent-based approach. Computers & Security, 2001,20(6):525~532.

[3] Wu SL, Sheth A, Miller J, Luo ZW. Authorization and access control of application data in workflow system. Journal of Intelligent Information System, 2002,18(1):71~94.

[4] Bertino E, Bonatti PA, Ferrari E. TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security, 2001,4(3):191~223.

[5] Dong GY, Qing SH, Liu KL. Role-Based authorization constraint with time character. Journal of Software, 2002,13(8):1521~1527 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/1521.pdf.

[6] Deng JB, Hong F. Task-Based access control model. Journal of Software, 2003,14(1):76~82 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/76.htm.

[7] Shi ML,Yang GX, Xiang Y, Wu SG. WfMS: Workflow management system. Chinese Journal of Computers, 1999,22(3):325~334 (in Chinese with English abstract).

[8] Li HF, Fan YS. Overview on managing time in workflow systems. Journal of Software, 2002,13(8):1552~1558 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/13/1552.pdf.

附中文参考文献:

[5] 董光宇,卿斯汉,刘克龙.带时间特性的角色授权约束.软件学报,2002,13(8):1521~1527. http://www.jos.org.cn/1000-9825/13/1521.pdf.

[6] 邓集波,洪帆.基于任务的授权模型.软件学报,2003,14(1):76~82. http://www.jos.org.cn/1000-9825/14/76.htm.

[7] 史美林,杨光信,向勇,伍尚广.WfMS:工作流管理系统.计算机学报,1999,22(3):325~334.

[8] 李慧芳,范玉顺.工作流系统时间管理.软件学报,2002,13(8):1552~1558. http://www.jos.org.cn/1000-9825/13/1552.pdf.