第 30 卷 第 1 期　　华 中 科 技 大 学 学 报(自然科学版)　　Vol. 30 No. 1
2002 年 1 月　　J. Huazhong Univ. of Sci. & Tech. (Nature Science Edition)　　Jan. 2002

多级安全工作流授权模型

洪 帆 李 静

(华中科技大学计算机科学与技术学院)

摘要:论述了用于工作流管理系统中的工作流授权模型.针对工作流在多级安全环境下的应用,提出了一种多级安全工作流授权模型.模型增加了安全级及任务相关性的表示,对原模型的授权规则进行了改造.提出了判断可达性的算法,对新模型的终点是否可达进行了分析.

关 键 词:工作流;多级安全;授权;相关性;可达性

中图分类号:TP309　　**文献标识码**:A　　**文章编号**:1671-4512(2002)01-0020-03

目前,工作流管理系统(WFMS)作为协调信息资源与人力资源的手段越来越受到研究机构与产业界的重视. Atluri 等提出了一种实现动态授权的工作流授权模型①(WAM),该模型能够根据任务的执行情况动态地授予相关权限,但该模型无法适应多级安全需求.

本文在研究了 WAM 的基础上,提出了一种新的授权模型-多级安全工作流授权模型(MLS WAM),文中对模型进行了描述及分析.

1 工作流授权模型

通常,一个工作流由若干个完成独立功能的任务构成,这些任务相互联系,具有一定的相关性,因此要以一种协同的方式进行.为了确保任务能被合法主体在任务的真正执行期间按规定权限执行,相关的工作流授权机制就应体现在工作流管理系统中.图 1 显示了商品销售处理的情况,某公司的商品销售包括 4 项任务:确认订单(w_1)、检查货款(w_2)、从仓库中提货(w_3)和发送商品(w_4).当收到来自客户的一份订单时,系统首先授权给销售部人员进行相关活动,在核实订单及检查货款已到公司后,销售部将开出一张提货单,以提货单的形式授权给储运部从仓库中提取提货单上所标明的商品,提出了所有商品后该提货单失效,由储运部发出发货单,授权货运部将商品送至客户手中.上述情况的授权流必须与工作流进程同步,从而保证权限的实时授予与撤销.

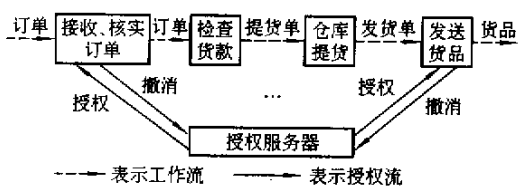

图 1 商品销售系统流程图

根据 WAM,一个工作流是一个任务偏序集,即 $W=\{w_1, w_2, \cdots, w_n\}$,对任务的授权通过授权模版($AT$)来实现.它形式化定义了任务、授权模版和授权,另外还制定了权限授予与撤消规则.

定义 1 任务 $w_i=(OP_i, \Gamma_{\text{in}_i}, \Gamma_{\text{out}_i}, [\tau_{\xi_i}, \tau_{\mu_i}])$,式中 OP_i 表示 w_i 中的执行的操作集,$\Gamma_{\text{in}_i}\subseteq\Gamma$ 表示允许输入的客体类型集,$\Gamma_{\text{out}_i}\subseteq\Gamma$ 表示输出的客体类型集,$[\tau_{\xi_i}, \tau_{\mu_i}]$ 表示任务执行的有效期,也就是说任务必须在 τ_{ξ_i} 之后开始执行,在 τ_{μ_i} 之前结束.

定义 2 授权模版 $AT(w_i)=(s_i,(\gamma_i, -), pr_i)$,表示授予主体 s_i 相关权限对类型为 γ_i 的客体进行操作 pr_i.一个任务可以有多个授权模版,用 AT 表示授权模版集.

定义 3 授权是一个四元组,即 $P_i=(s_i, o_i, pr_i, [\tau_{b_i}, \tau_{e_i}])$,表示在 τ_{b_i} 时刻授予主体 s_i 对客体 o_i 执行 pr_i 操作的权限,在 τ_{e_i} 时刻撤消其权限.

假定有任务 $w_i=(OP_i, \Gamma_{\text{in}_i}, \Gamma_{\text{out}_i}, [\tau_{\xi_i},$

收稿日期:2001-08-13.

作者简介:洪 帆(1942-),女,教授 武汉,华中科技大学计算机科学与技术学院 (430074).

① Atluri V., Huang W K. An authorization model for workflows, proc. of the fifth european symposium on research in computer security, 1996.9

τ_{μ_i}]) 及其授权模版 $AT(w_i)=(s_i,(\gamma_i,-),pr_i)$，则授权 $P_i=(s_i,o_i,pr_i,[\tau_{b_i},\tau_{e_i}])$ 由如下规则而来.

权限授予规则：设客体 $o_i\in\Gamma_{\mathrm{in}_i}$ 在时刻 τ_{a_i} 发往任务 w_i，则

if $\tau_{a_i}\leqslant\tau_{\mu_i}$ then

{$s_i\leftarrow s(AT)$，$pr_i\leftarrow pr(AT)$，$\tau_{e_i}\leftarrow\tau_{\mu_i}$

if $\tau_{a_i}\leqslant\tau_{\xi_i}$ then

$\tau_{b_i}\leftarrow\tau_{\xi_i}$

otherwise $\tau_{b_i}\leftarrow\tau_{a_i}$

}

权限撤消规则：假定任务在时刻 τ_{f_i} 结束，此时客体离开任务 w_i

if $\tau_{f_i}\leqslant\tau_{\mu_i}$ then $\tau_{e_i}\leftarrow\tau_{f_i}$

2　多级安全工作流授权模型

在多级安全的环境下，工作流可以包括不同安全级别的任务.

2.1　任务相关性

工作流中，每个任务 t_i 都有一个生命周期，在任一时刻任务处于生命周期中的下列状态之一 初始态 in_i、执行态 ex_i、提交态 cm_i 和夭折态 ab_i. 任务状态的变化通过任务原语来实现，开始原语的触发使任务由 in_i 变为 ex_i，提交原语将任务由 ex_i 变为 cm_i，夭折原语将任务由 ex_i 变为 ab_i，图 2 说明了任务的状态变迁图. 任务的相关性定义了任务间状态变化的依赖性. 假定有两个任务 t_i 和 t_j，它们之间的任务相关性 $t_i\xrightarrow{x}t_j$ 表示 t_i 和 t_j 之间存在依赖性，x 表示相关性的类型. 如 bc 表示只有 t_i 提交后 t_j 才能开始，b 表示只有 t_i 开始后 t_j 才能开始，a 表示如果 t_i 夭折那么 t_j 也一定夭折，sc 表示如果 t_i 提交那么 t_j 也一定提交.

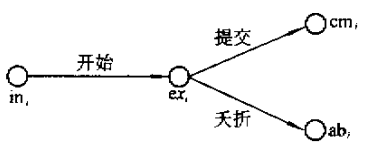

图 2　任务状态变迁图

2.2　MLS WAM

先引入任务相关性集合 D_{depd} 和安全级集合 S 的概念，其中〈S，$\leqslant$〉是一偏序集.

定义 4　任务相关性用一个三元组表示，即 $D_{\mathrm{depd}_{ij}}=(t_i,t_j,x)$，$x\in\{bc,b,a,sc,\cdots\}$ 表示相关性类型.

定义 5　多级安全工作流 MLSW 是一个 6 元组，MLSW=$(W,D_{\mathrm{depd}},S,l,w_0,w_t)$，式中：

a. W 是任务集，它的每一个元素的定义见定义 1；

b. D_{depd} 是任务相关性集合，它的每一个元素的定义见定义 4；

c. S 是安全级集合，其中的小于等于关系 $\leqslant$ 构成了偏序关系；

d. l：$W\cup\Gamma\rightarrow S$，$l(w_i)=s_i$ 表示任务 w_i 的安全级为 s_i，$l(\gamma)=s_i$ 表示类型为 γ_i 的客体的安全级是 s_i；

e. $w_0\in W$，是唯一的初始任务；

f. $w_t\in W$，是唯一的终止任务.

显然，定义的多级安全工作流模型满足：**a**. 简单安全性. 当且仅当任务的安全级大于等于客体类型的安全级时，该任务才能读取客体内容. **b**. $*$ 特性. 当且仅当任务的安全级小于等于客体类型的安全级时，该任务才能向客体写入信息. 根据这两条特性，可以重写上述的授权规则，使之适应 MLS WAM，而权限撤消规则不变，其中 $\gamma(o_i)$ 表示客体 o_i 的类型.

多级安全权限授予规则：设客体 o_i，且 $\gamma(o_i)\in\tau_{\mathrm{in}_i}$ 在时刻 τ_{a_i} 发往任务 w_i，则

if pr_i 为只读 and $l(\gamma(o_i))\leqslant l(w_i)$ then 执行上述授权规则；

if pr_i 为只写 and $l(w_i)\leqslant l(\gamma(o_i))$ then 执行上述授权规则；

if pr_i 为既读又写 and $l(w_i)\leqslant l(\gamma(o_i))$ and $l(\gamma(o_i)\leqslant l(w_i)$ then 执行上述授权规则.

3　分析

根据上述定义，可以将多级安全工作流看作是一个有向图，因此可以采用图论的相关定理来分析工作流的终点可达性. 终点可达性是指工作流中是否存在一条从初始节点到结束节点的有效路径，即工作流能否正确地于终点结束. 在文献[1]中给出了采用 Petri Nets 的分析方法，这里根据图论相关定理给出针对本文中 MLS WAM 的算法.

设邻接矩阵 $\boldsymbol{A}$ 是一个 $n\times n$ 矩阵，n 为工作流中的节点数，将初始节点的编号定为 1，终止节点的编号为 n，$a_{ij}=1$ 表示任务 w_i 和 w_j 之间具有相关性，$a_{ij}=0$ 表示任务 w_i 和 w_j 之间不具有相关性，则 $A^l(l=1,2,\cdots)$ 的 (i,j) 项元素 $a_{ij}^{(l)}$ 是从 w_i 到 w_j 长度为 l 的有向路的总数[2]. 要

判断终点是否可达,则需判断 a^{l}_{1n}是否不为 0.

判断算法 判断终点可达性.

a. 根据 D_{depd}初始化邻接矩阵 $\boldsymbol{A}$;

b. if $a(1,n)=1$ then return true

c. for $i=2$ to $n-1$

{$\boldsymbol{A}=\boldsymbol{A}*\boldsymbol{A}$

if $a(1,n)\neq 0$ then return true

}

return false

参 考 文 献

[1] Adam N R, Atluri V, Huang W K. Modeling and analysis of workflows using petri nets. Journal of Intelligent Information Systems, 1998, 10(2): 131~158

[2] 洪 帆. 离散数学基础(第二版). 武汉: 华中理工大学出版社, 1995.

Authorization model for multilevel security workflow

Hong Fan *Li Jing*

Abstract: This paper briefly describes the workflow authorization model for workflow management system, and presents authorization model for a multilevel security workflow in the multilevel secure environments. The model adds the presentation of security level and task dependence and reforms the authorization rule for the improved model. An algorithm to detect the accessibilities of terminal nodes is also put forward.

Key words: workflow; multilevel security; authorization; dependence; accessibility

Hong Fan Prof.; College of Computer. Sci. & Tech., HUST, Wuhan 430074, China.

(上接第 16 页)

A new scheme for integration transmission based on PRMA wireless networks

Wen Yuanbao *Rao Bo*

Abstract: This paper focuses on low bit-rate wireless applications like video conferencing and visual telephone, and proposes a new scheme——pseudo reservation scheme for the integration of video, voice and data transmission based on Packet Reservation Multiple Access wireless networks. With the packet dropping probability of the active voice terminals, the system bandwidth utilization performance is superior to the original PRMA without sacrificing the video capacity.

Key words: wireless network; PRMA; pseudo reservation scheme; ITU-T H.263

Wen Yuanbao Prof.; College of Computer Sci. & Tech., HUST, Wuhan 430074, China.

多级安全工作流授权模型

作者： 洪帆， 李静
作者单位： 华中科技大学计算机科学与技术学院,武汉,430074
刊名： 华中科技大学学报(自然科学版) ISTIC EI PKU
英文刊名： JOURNAL OF HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY
年，卷(期)： 2002,30(1)
被引用次数： 9次

参考文献(2条)

1. 洪帆 离散数学基础 1995

2. ADAM N R;Atluri V;Huang W K Modeling and analysis of workflows using petrinets 1998(02)

引证文献(9条)

1. 张昭理. 洪帆. 廖俊国 基于Petri网的保密性策略建模与验证[期刊论文]-华中科技大学学报（自然科学版） 2007(10)

2. 刘丁. 王小明. 付争方 安全工作流管理系统体系结构研究[期刊论文]-微电子学与计算机 2006(10)

3. 史旭东 基于AGENT的工作流管理系统的设计与实现[学位论文]硕士 2006

4. 杜思祥 基于Web的跨平台的工作流管理系统AgileFlow的设计和实现[学位论文]硕士 2005

5. 刘大欣. 陈蔚芳 基于Petri网工作流的动态访问控制[期刊论文]-微机发展 2004(2)

6. 陈卓. 骆婷. 石磊. 洪帆 基于Perti网的工作流访问控制模型研究[期刊论文]-上海大学学报(英文版) 2004(1)

7. 张栋 工作流平台的安全体系框架的研究[学位论文]硕士 2004

8. 刘英 空间数据访问控制策略和模型[学位论文]博士 2004

9. 洪帆. 李静 基于任务的授权模型[期刊论文]-计算机研究与发展 2002(8)