第32卷 第12期 计 算 机 工 程 2006年6月
Vol.32 № 12 Computer Engineering June 2006
·软件技术与数据库· 文章编号：1000—3428(2006)12—0071—03 文献标识码：A 中图分类号：TP309.2

异构分布式CSCW委托授权模型及其访问控制

张志勇，普杰信
(河南科技大学电信学院，洛阳 471003)

摘 要：基于角色和活动的重要特性，提出了一种面向CSCW环境基于角色-活动并具有时序特征和约束规则的委托授权模型RABDM for CSCW，以及CSCW访问控制体系架构和委托授权工作机制。该模型解决了基于CSCW图形图像协同处理实际应用中访问授权过于集中的问题，实现了分布式和动态时序性等特征。

关键词：访问控制；CSCW；委托授权；时序特征；约束规则

Delegation Model for Heterogeneous Distributed CSCW and Its Access Control

ZHANG Zhiyong, PU Jiexin
(Coll. of Electron. Inf. Eng., Henan Univ. of Sci.& Technology, Luoyang 471003)

【Abstract】 Role-activity based delegation model for CSCW with time and constraint characters is proposed based on the important properties of role and activity, and CSCW access control architecture and delegation mechanism are described in the basis of the model. It solves authorization centralization in the actual application of graphics and images collaboration processing based on CSCW, and realizes distributed and dynamic time characters.

【Key words】 Access control; Computer support cooperative work; Delegation; Time-order character; Constraint rule

CSCW旨在基于异构分布式网络环境平台，实现多用户间的协同处理和资源共享等基本任务，其中访问控制是CSCW体系中保障多用户协调、有序工作，高效而安全地使用共享资源的核心部分。迄今CSCW访控研究主要集中在利用基于角色的策略和模型实现集中式管理访问许可权限的授权与撤销。然而鉴于系统中用户实体和访问对象数量逐渐增大，仅依靠传统集中式授权管理将不能满足分布式CSCW环境安全体系的构建，集中式的授权服务器管理工作也因复杂而庞大将不堪重负。

委托授权机制能够较好地解决上述问题，但目前缺少全面且深入的研究和具体应用。文献[1]较集中地提出了基于角色的协同工作中需要解决的问题及基本解决方案，如角色分配与迁移等；文献[2]利用XML实现了满足动态安全需求的角色模型，但未给出一个具体形式化的模型；文献[3]给出了基于角色CSCW访问控制模型中基本组件和普通授权规则的形式化描述，也未涉及委托授权机制。本文研究将根据委托授权基本特性提出一种具有时序特征和约束机制的委托授权模型RABDM for CSCW(Role-Activity Based Delegation Model for CSCW)及其CSCW访问控制体系架构。

1 委托授权及其相关问题

委托授权(Delegation)的本质是用户实体将自己所具有的角色或许可转授给其它用户，使其可以代表自己的利益行使一定的职责，协同或独立地完成某些任务，最终达到权利和资源共享的目的。此外委托者还可以撤销委托，收回所共享的特权。和委托授权相关的概念有：委托者(Delegator)，委托角色/许可(Delegated Role/Permission)和受托者(Delegatee)。委托机制主要涉及以下基本问题：

(1)委托授权粒度：委托的基本单位主要分为Zhang Xinwen等提出的基于许可的细粒度[4]，Ezedin Barka和Ravi Sandhu基于角色的中粒度以及Zhang Zhiyong提出的基于角色-许可的粗粒度[5]。细粒度是指允许用户将角色中的部分许可委托给另一用户，而不只是角色的整体委托。这样降低了可委托授权的粒度，遵循了最小特权原则，但是会产生大量逻辑意义上不完整的角色，从而又增加了授权管理的复杂性和实际应用系统的开销；中粒度是指用户只能将自身的角色整体委托给其他用户，从而使其获得该角色所具有的全部许可权限，在某种程度上违背了最小特权原则；粗粒度委托是用户可以任意将自身的角色和(或)许可委托给他人，这样的委托较前两者灵活，然而实现时较为复杂。关于委托粒度需要根据实际应用系统的需求折中选择合适的委托授权基本单位。

(2)单步委托或多步委托：单步委托是指受托者不可以进一步地将委托角色或许可再次委托给其它用户，多步委托则允许受托者进一步实施委托，但撤销委托将变得复杂和困难。

(3)委托撤销：委托的逆操作称为撤销(Revoke)，它完成被委托角色或许可的回收。撤销的主要方式有级联撤销、非级联撤销、独立于授权的撤销、非独立于授权的撤销、系统自动撤销和用户撤销等。

基金项目：国家自然科学基金资助项目(60475021)；河南省杰出青年基金资助项目(0412000400)
作者简介：张志勇(1975—)，男，讲师、硕士，主研方向：RBAC与访问控制，智能决策支持系统；普杰信，院长、教授
收稿日期：2005-06-15 **E-mail：**zhangzy@mail.haust.edu.cn

2 RABDM for CSCW 的构建与形式化描述

2.1 RABDM for CSCW 的基本思想

对于 1.2 节涉及的委托基本问题，RABDM for CSCW 把角色作为委托授权的基本单位，委托过程采用多步特性，撤销授权则使用用户和系统两者相结合地独立于授权的级联撤销。

委托授权是 RABDM 的核心过程，为便于其实现引入了委托角色组(Delegated Role Group，DRG)的概念，它是委托角色 DR 的集合。在该模型中，用户不需经过系统管理员可独立创建 DRG 后，把若干个 DR(包括显式自身角色和隐式继承角色)指派给 DRG，最后将 DRG 委托给另一用户来完成一次委托授权过程，从而使受托者能够代表自己的职责(角色)行使一定的权限。由于 DRG 具有时效性，因此在 RABDM for CSCW 中描述了“DRG 生命周期”，丰富了该模型的语义。

RABDM for CSCW 结合 CSCW 环境特征在 RBAC96 的基础上，同时引入任务(Task)和活动(Activity)的概念。任务作为一次完整的工作流程，具体分可细划为若干具有时序性的活动。活动执行中所需的许可权限经过活动-许可指派获得；角色行使职责可执行的活动由角色-活动指派赋予。最终角色通过活动实体和许可相连，用户则通过角色和活动实体相联系，角色-活动之间与用户-活动会话之间都是一一映射关系，其他则是多对多的关系。该模型主要由用户、普通角色、委托角色、DRG、许可、约束规则、任务、活动和会话等 9 部分构成，如图 1 所示。

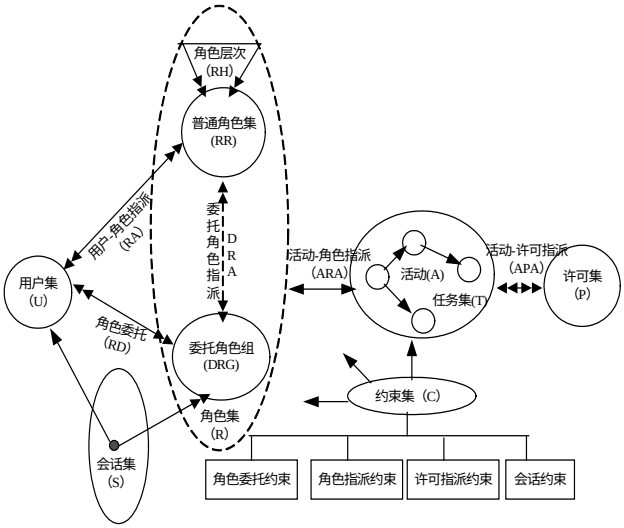

图 1 面向 CSCW 基于角色-活动的委托模型

2.2 RABDM for CSCW 基本组件及关系

用集合论和谓词逻辑形式化描述该模型如下：

定义普通角色集 RR，活跃角色集 AR，委托角色集 DR，委托角色组 DRG 及其状态集 S，许可集 P，约束集 C，角色委托约束集 RDC，活动会话集 AS、任务集 T 和活动集 A。

定义 1 操作(Operation) 用户主体对访问客体(共享资源，如图形图像文件、数据库、画板等)可施加的动作。这里的操作既可以定义为实际的读、写和执行操作，也可以为抽象的操作。例如在 CSCW 图形图像处理中，操作可以是图像提取、图像格式转换等。

定义 2 任务和活动(Task & Activity) 角色间协同处理所完成的一项工作称为任务，任务中的若干步骤称为活动。活动具有动态特征和原子性，它是任务中不可划分的最小基本单位。

$\forall t(t \in T)t=\{a_1,a_2,\ldots,a_n \mid a_i \in A\}$

定义 3 活动会话(Activity Session) 活动会话是用户和其所具有的角色集中活跃角色子集之间的映射关系，记为 f(u,ar)。

$f(u,ar): u \rightarrow ar(u \in U, ar \in AR)$

定义 4 委托角色组(Delegated Role Group) DRG 是待委托角色的集合，它是普通角色的子集。$DRG=\{r_1,r_2,\ldots r_n \mid r \in RR\}$，即 $TDR \subseteq RR$。

定义 5 (委托角色指派 Delegated Role Assignment) 根据应用需求将待委托普通角色分配给 DRG，DRA 是普通角色与 DRG 之间多对多的关系。

$$DRA \subseteq RR \times DRG$$

定义 6 角色委托(Role Delegation) 委托授权关系是一个 5 元组(u_1,u_2,DRG,TL,RDC)，其中 u_1 为委托者，u_2 为受托者，TL(Time Limit)为委托时限，DC 是委托约束。该五元组的语义解释为用户实体 u_1 在满足 RDC 的前提下可以将 DRG 委托授权给 u_2，使得 u_2 在 TL 内享有 DRG 所有角色所属的显式或隐式许可。

2.3 RABDM for CSCW 时序特征及相关性质

定义 7 状态集(Status Set) DR 的状态集 S={init,invoke, sleep,expire}，其中 init 为初始态，invoke 为激活态，sleep 为睡眠态，expire 为终止态。

定义 8 委托时限(Delegation Time Limit) DR 具有时效性，委托时限 $TL=\{x \mid x=[\tau_{bi},\tau_{ei}](i=1,2\ldots n)\}$，其中 τ_{bi} 为该时段的起始时间，τ_{ei} 为终止时间。

定义 9 状态迁移(Status Migration) DR 在其生命周期内会发生以下状态转换：假定 ST 为系统时间，$\forall i(i \in N)ST \notin [\tau_{bi},\tau_{ei}] \wedge ST<\tau_{b1} \rightarrow S=init$；$\exists i(i \in N)ST \in [\tau_{bi},\tau_{ei}] \rightarrow S=invoke$；$\forall i(i \in N)ST \notin [\tau_{bi},\tau_{ei}] \wedge (ST>\tau_{b1}) \wedge (ST<\tau_{en}) \rightarrow S=sleep$；$\forall i(i \in N)ST \notin [\tau_{bi},\tau_{ei}] \wedge ST>\tau_{en} \rightarrow S=expire$。

性质 1 活动时序性(Activity Time -Order) 任务中活动之间关系为异步和同步，任意两个活动之间有稳定的时间顺序，并满足全序关系，记为“□”。

$\forall t,a_i,a_j(t \in T,a_i,a_j \in A)(a_i \in t \wedge a_j \in t \rightarrow a_i \square a_j)$

$\forall t,a_i,a_j,a_k(t \in T,a_i,a_j,a_k \in A)(a_i \square a_j \wedge a_j \square a_k \rightarrow a_i \square a_k)$

性质 2 DR 执行时序 (DR Run-Order)DR 在活动执行过程中是串行或并发的，DR 之间的时序关系满足偏序关系，这里记为“$\geq_{DR}$”。

$\forall t,dr_i,dr_j,dr_k(t \in T,dr_i,dr_j,dr_k \in t)(dr_i \geq_{DR} dr_j \wedge dr_j \geq_{DR} dr_k \rightarrow dr_i \geq_{DR} dr_k)$

性质 3 (活动-DR 时序一致性 Activity-DR Time–Order Consistent) 由于活动和 DR 之间之间是一一映射关系(记作 $g(a_i,dr_i)$)，因此两者在时序上保持一致性。

$\forall t,a_i,a_j,dr_i,dr_j(a_i,a_j \in t)(g(a_i,dr_i) \wedge g(a_j,dr_j) \wedge a_i \square a_j \rightarrow dr_i \geq dr_j \vee \neg(dr_i \geq dr_j) \wedge \neg(dr_j \geq dr_i))$

2.4 RABDM for CSCW 委托约束规则

普通基于角色的授权管理实施者一般为系统管理员或系统安全员，授权管理过程相对集中；而在分布式环境下委托授权的实施者可以是系统中任意用户实体，委托操作比较分散。因此实施委托约束有利于加强委托管理，以防止某些用户有意或无意地进行非法授权。委托约束规则主要包括非委托角色、委托冲突角色、委托步、委托基数约束等，它们将

构成实际 CSCW 应用系统的委托授权策略。

定义 10 非委托角色集(Non-Delegated Role Set) 非委托角色集 NDR={r_1,r_2,…r_i}。

约束规则 1 无冲突委托约束(Non-Collision Delegation Constraint) 非委托角色集中的任意元素不能进行委托。

$$\forall x(x \in NDR) \rightarrow (x \notin DRG)$$

定义 11 委托冲突角色(Delegation Collision Role) 如果角色 r_i 和 r_j 不能同时委托给其他用户，则称两者为委托冲突角色，记为 collr(r_i, r_j)。

约束规则 2 DRG 无冲突约束(DRG Non-Collision Constraint) 委托角色组中任意两个角色都不能存在委托冲突。

$$\forall r_i,r_j\ (r_i \in DRG,\ r_j \in DRG) collr(r_i, r_j)=F$$

定义 12 委托步和委托基数(Delegation Depth & Cardinality) 委托步 d 为自然数，表示角色 r_i 可以级联委托的次数。当 d=1 时，称为单步委托；当 d>1 时，称为多步委托。委托基数 n 为自然数，表示角色 r_i 可以委托的用户数。

约束规则 3 多步委托约束(Multi-Steps Delegation Constraint) DRG 的委托步和委托基数取决于 DR 集中所有角色的委托步或委托基数的最小值。

$$\forall r_i\ (r_i \in DRG)\ d_{DRG}<d_{ri}$$

$$\forall r_i\ (r_i \in DRG)\ n_{DRG}<n_{ri}$$

性质 4 级联撤销(Cascading Delegation Revoke) 当委托步大于 1 时，DRG 撤销过程将委托路径中的每一个用户获得 DRG 同时收回。

性质 5 独立于授权撤销(Grant-Independent Revoke) 委托路径中的任意用户都可以将自身委托的 DRG 收回，并非只有源用户可以撤销授权。

性质 6 系统强制撤销(System Imperative Revoke) 当系统时钟超出了 DRG 委托时限，CSCW 系统自动撤销 DRG 的委托许可，其中包括显式和隐式的所有许可。

约束规则 1 增强了应用系统中对委托授权的控制，满足了“最小特权原则”；约束规则 2 解决了企业级委托授权的冲突问题，实现了“责任分离原则”。许可集中的任意权限既可以为普通读、写、执行等，也可以是企业级抽象的许可权限，如图像处理中的图像采集、图像预处理、图像分割与转换等，从而达到“数据抽象原则”。

3 CSCW 访问控制

3.1 CSCW 访问控制体系架构

在实际应用中，“基于 CSCW 图形图像协同处理系统”采用了基于 RABDM 的 CSCW 访问控制体系架构，如图 2 所示。它主要包括访问授权与访问决策，其中前者主要由集中式普通授权管理、开放分布式委托授权管理、审计子系统、委托授权数据库和约束规则数据库等 5 部分组成。整个体系采用“责任分离”思想将 CSCW 系统用户分为 4 类：普通用户，系统管理员，系统安全员和系统审计员。普通授权管理由系统管理员负责为普通用户指派角色、为角色指派所能够执行的任务活动等，授权信息写入授权数据库；委托授权终端系统接收用户的委托请求，完成委托授权指派并将数据存入委托授权数据库，最后由委托授权服务器对委托授权和约束规则设置委托时限时间戳；系统安全员则根据应用级授权策略管理约束规则库；系统审计员负责 CSCW 的审计任务，尤其是对于分布式委托授权的审计和跟踪监视。

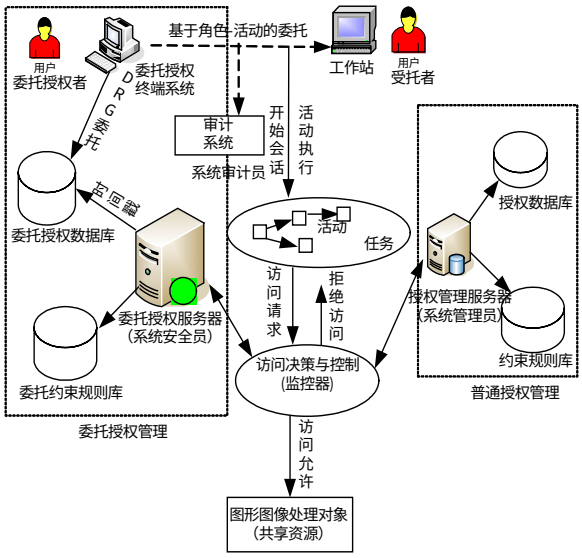

图 2 CSCW 访问控制体系架构

3.2 CSCW 委托授权过程与访问控制

CSCW 系统委托授权采用开放分布式体系，普通用户无需经过系统管理员而由用户自身完成委托授权的处理。如图 2 中委托者使用终端设备上的跨平台委托授权系统决定受托者、委托角色组 DRG、委托时限等，最终委托信息将存入委托授权数据库。委托者在委托过程中不能违背约束规则库的各项规则，否则委托授权将被拒绝。受托者接受 DRG 后获得其所属许可，然后对图形图像处理对象等共享资源的访问由监视器通过两个授权服务器进行访问决策与访问控制，最终确定是否允许访问该客体或是拒绝访问。

4 结束语

本文根据委托特性所提出的 RABDM for CSCW 弥补了异构分布式环境下 CSCW 授权体系中缺少委托授权的不足，完善了其授权管理与访问控制的功能，同时保持了基于角色授权管理中高效、灵活的特点，是一种在分布式 CSCW 环境下解决委托问题较为完备的模型。关于 RABDM for CSCW 委托授权中基于上下文环境的约束问题以及依据 PRBDM 面向对象的建模[5]完成对本文模型的可视化工作等，需要做进一步的研究。

参考文献

1 Zhu Haibin. Some Issues of Role-based Collaboration[C]. IEEE CCECE'03- CCGEI'03, Montreal, 2003-05.

2 Tripathi A R, Ahmed T, Kumar R. Specification of Secure Distributed Collaboration System[C]. IEEE Proceedings of the 6th International Symposium on Autonomous Decentralized Systems, 2003.

3 李成锴, 詹永照, 茅 兵等. 基于角色的 CSCW 系统访问控制模型[J]. 软件学报, 2000, 11(7): 931-937.

4 Zhang Xinwen, Oh S, Sandhu R. PBDM: A Flexible Delegation Model in RBAC[C]. SACMAT'03, Como, Italy, 2003.

5 Zhang Zhiyong, Pu Jiexin. Permission-role Based Delegation Model and Object-oriented Modeling[C]. China DPCS'04, Beijing, 2004.