文章编号:1001 - 9081(2006)02 - 0323 - 04

# 具有时限性和区域性特征的基于角色转授权模型

徐洪学[1,2],刘永贤[1]
(1. 东北大学 机械工程与自动化学院,辽宁 沈阳 110004;
2. 营口职业技术学院 计算机信息工程系,辽宁 营口 115000)
(hongxuexu@yahoo.com.cn)

**摘 要**:对分布式系统基于角色转授权模型(Role-based Delegation Model,RDM)进行深入研究。RDM 更适合于分布式系统的授权管理,但当前的几种 RDM 都不支持时限性和区域性。根据分布式系统的特点,首先提出了转授权的区域性特征;基于转授权的时限性特征和区域性特征对 RDM2000 模型进行扩充,提出了完备的具有时限性和区域性特征的基于角色的转授权模型(Temporary and Domain Role-based Delegation Model,TDRDM);并给出了基于 TDRDM 的转授权(delegation)和转授权撤销(delegation revocation)机制;最后通过分布式系统实例对 TDRDM 模型的转授权进行描述。

**关键词**:基于角色;转授权;时限;区域
**中图分类号**: TP309 **文献标识码**:A

# Temporary and domain role-based delegation model

XU Hong-xue[1,2], LIU Yong-xian[1]
(1. *College of Mechanical Engineering and Automation, Northeastern University, Shenyang Liaoning* 110004, *China;*
2. *Department of computer information engineering, Yingkou Higher Vocational Technical Institute, Yingkou Liaoning* 115000, *China*)

**Abstract:** Access control delegation model of distributed systems was researched in this paper. Role-based delegation model(RDM) is more suitable for distributed system environments, but current RDMs don't support temporal and domanial delegation. The domain feature of delegation was proposed firstly, which based on the character of distributed systems. A temporary and domain role-based delegation model(TDRDM) was presented, which was an extension of RDM2000 by supporting temporary and domain role-based delegation. The new mechanisms of delegation and delegation revocation were explored, which based on TDRDM. Finally, a model test was presented by an example of distributed system. As results, TDRDM not only ensures the time constraints, but also ensures the domain constraints of delegation in distributed system environments.

**Key words:** role-based; delegation; temporary; domain

## 0 引言

在分布式系统环境下,系统的授权管理工作异常繁重。完全依赖于系统安全管理员(Seco)的集中式管理,需要 Seco 参与系统中所有的授权行为,加重了系统的管理负担。转授权(Delegation)技术的使用,允许将分布式系统环境下的集中式授权管理工作分散实施,是提高分布式系统伸缩性的重要手段。转授权的基本思想是用户将自己所具有的部分或全部权限转授给其他用户,让接受授权的用户代表发出授权的用户执行某些任务[1]。

基于角色的访问控制(RBAC)正越来越多地被信息安全领域所重视[2,3]。具有代表性的 RBAC 模型是 Sandhu 等提出的 RBAC96 模型以及对该模型的补充模型[4,5]。RBAC96 可以适应于不同的访问控制策略要求,因而得到广泛应用[6,7]。基于角色的转授权以 RBAC96 模型为基础,实现访问权限在用户之间的转移,为在分布式系统环境中实现 RBAC 提供了一种有效途径。

基于角色的转授权模型主要有 RBDM0[8,9] 和 RDM2000[1] 两种,但 RBDM0 和 RDM2000 既不支持时间限制也不支持区域约束,而时间限制和区域约束是分布式系统环境中转授权的重要组成部分。本文分析了转授权的时间限制和区域约束,并基于 RDM2000 提出了具有时限性和区域性特征的基于角色的转授权模型(TDRDM),通过具体的分布式系统实例对 TDRDM 模型进行描述。

## 1 转授权特征及转授权模型

### 1.1 转授权特征

在转授权操作中,发起转授权动作的用户称为授权用户(Delegating user),记作 $u_{ing}$,$u_{ing}$ 所具有的角色称为授权角色(Delegating role),记作 $r_{ing}$,被转授出去的角色称为转授权角色(Delegated role),记作 $r_{ed}$,接受 $r_{ed}$ 的用户称为转授权用户(Delegated user),记作 $u_{ed}$。

转授权特征主要有时限性、单调性、完全性、执行性、传递性、多重性、协议性、可撤销性以及区域性等,其中除区域特征外其他特征在文献[8]中有详细描述,本文结合分布式系统的特点,提出转授权的区域性特征。

**收稿日期**:2005 - 08 - 20;**修订日期**:2005 - 10 - 21 **基金项目**:国家"十五"重大攻关课题资助项目(2001BA201A14)
**作者简介**:徐洪学(1962 - ),男,辽宁大连人,副教授,博士研究生,主要研究方向:计算机应用、协同设计等; 刘永贤(1945 - ),男,辽宁鞍山人,教授,博士生导师,主要研究方向:先进制造与自动化技术等.

所谓转授权的区域性特征是指 $r_{ed}$ 的作用范围。按照 $r_{ed}$ 作用范围的不同将转授权分为广域性转授权和局域性转授权,前者是指 $r_{ed}$ 不受作用范围的限制,一旦具有 $r_{ing}$ 的 $u_{ing}$ 把 $r_{ed}$ 转授予 $u_{ed}$,则任何范围内的满足条件的 $u_{ed}$ 都将具有 $r_{ed}$ 所包含的权限,直到 $u_{ed}$ 的 $r_{ed}$ 被撤销为止;而后者则是指在转授权的同时要指定 $r_{ed}$ 的作用范围,一旦 $r_{ed}$ 超过指定范围,系统将拒绝转授权。

### 1.2 转授权模型

RBDM0 和 RDM2000 是两种主要的基于角色的转授权模型。基于 RBAC96 的基本模型(如图 1 所示),RBDM0 首次将角色引入转授权之中,并建立了用户至用户的转授权模型,实现了两个用户之间转授权[8,9]。RDM2000 是通过扩展 RBDM0,以支持角色层次关系和传递性转授权[1]。

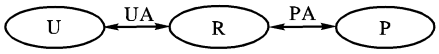


图 1 RBAC96 扁平模型

RBDM0 和 RDM2000 将角色的成员分为两类:1) 初始用户 Users - O(r):由 Seco 最初分配到角色中的成员;2) 转授权用户 Users - D(r):由其他用户分配到角色中的成员(通过转授权进行分配的)。RBDM0 和 RDM2000 区分对待这两类用户。

RDM2000 定义了一种新的转授权关系 DLGT(Delegation),如图 2 所示。在具有传递性特征的基于角色的转授权中,DGLT 可进一步划分为 ODGLT(Original user delegation)和 DDGLT(Delegated user delegation)。RDM2000 模型[1]如图 2 所示。

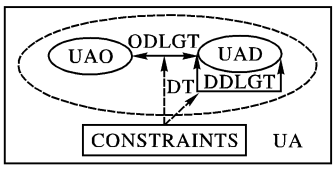


图 2 RDM2000 的转授权模型

### 1.3 RBDM0 和 RDM2000 的不足

RBDM0 既没有完全涵盖转授权的主要特征,如时限性、区域性、传递性和授权依赖撤销等,也没有给出形式化的描述;RDM2000 支持层次角色和传递性授权,是基于 RBDM0 扩充而成的较完善的基于角色的转授权模型,但是该模型仍然没有考虑时间限制和区域约束问题。

事实上,时限性和区域性是分布式环境下授权的重要组成部分,任何授权都具有时限性和区域性,永久的和广域的授权不但不能满足实际需求也不便于系统管理,而且还会带来一定的系统安全隐患[10~12]。

例如,在某计算机支持的协同设计(CSCD)系统中,$r_1$、$r_2$ 和 $r_3$ 分别代表设计主管、设计组长和设计组员的角色,且 $r_1 \geqslant r_2 \geqslant r_3$。$r_3$ 只具有“图纸设计”的权限,$r_2$ 具有“图纸设计”和“图纸审核”两项权限,$r_1$ 具有“图纸设计”、“图纸审核”和“图纸签发”三项权限。项目主管 $D_1$ 因故不能行使具有权限“图纸审核”的角色 $r_2$ 和“图纸设计”的角色 $r_3$,需要把 $r_2$ 和 $r_3$ 转授给其他相关人员,假设设计组长 $D_2$ 被授予 $r_2$,设计组员 $D_3$ 被授予 $r_3$。在不支持时间限制和区域约束的转授权模型中,存在以下问题:

1) $D_2$ 被授予 $r_2$ 以及 $D_3$ 被授予 $r_3$,意味着如果没有 Seco 或者 $D_1$ 的参与,则无论 $D_1$ 和 $D_2$ 处于任何区域内都将永远具有 $r_2$ 和 $r_3$,即使 $D_1$ 可以行使其所具有的权限;

2) $D_2$ 在 $D_3$ 行使 $r_3$ 的权限未结束之前就对 $D_3$ 行使 $r_2$,以及 $D_3$ 在 $D_2$ 开始行使 $r_2$ 的权限以后再次行使 $r_3$ 的权限,都会造成经 $D_2$ 审核的图纸和 $D_3$ 最终设计提交的图纸不一致;

3) $D_1$ 可以将其具有的角色转授给非协同设计联盟中的设计人员,这意味着协同设计联盟之外的设计人员也可以参与该系统的“图纸设计”、“图纸审核”或“图纸签发”活动。

以上问题的根本原因在于忽略了基于角色的转授权的时限性和区域性特征以及各授权时限和区域之间的关系,这也正是本文要解决的问题。

## 2 TDRDM

### 2.1 具有时限性和区域性的转授权表示

设用 $[t_b,t_e]$ 来表示时限 $duration$,$[t_b,t_e]$ 是一个时间段,$t_b$ 是时间段的开始,$t_e$ 是时间段的结束,其中,$t_b \in N, t_e \in N, t_b < t_e$;设用 $[s_b,s_e]$ 来表示区域 $dominion$,$[s_b,s_e]$ 是一个区域段,$s_b$ 是区域段的开始,$s_e$ 是区域段的结束,其中,$s_b \in N, s_e \in N, s_b < s_e$。

具有时限性和区域性的转授权的含义是:在转授权操作中,$u_{ing}$ 仅仅赋予 $u_{ed}$ 在时间段 duration 和区域段 dominion 中具有 $r_{ed}$,即 $u_{ed}$ 仅仅在时间段 duration 和区域段 dominion 中可行使 $r_{ed}$ 所具有的权限,一旦当前时间 $t > t_e$ 或当前位置 $s \notin [s_b, s_e]$,系统将自动撤销 $u_{ed}$ 的 $r_{ed}$ 或拒绝授权。为便于突出 TDRDM 中具有实质性的问题,本文将 RBAC96 中有关授权管理的部分简化为由 Seco 统一行使所有的授权管理工作。

在 RDM2000 中,不具有时限性和区域性的转授权 auth 的形式是 $(ing,ed)$,而考虑时限性和区域性后的转授权 ts-auth 的形式是 $(ing,ed,time,space)$,$ing = (u_{ing},r_{ing})$,$ed = (u_{ed},r_{ed})$,$time = (duration,t_d)$,$duration = [t_b, t_e]$,$space = (dominion,s_d)$,$dominion = [s_b,s_e]$,即 $ts-auth = ((u_{ing},r_{ing}),(u_{ed},r_{ed}),([t_b,t_e],t_d),([s_b,s_e],s_d))$。其中 $u_{ing} \in U$,$u_{ed} \in U, r_{ing} \in R, r_{ed} \in R, t_b \in N, t_e \in N \cup \infty, t_d \in N$ 为转授权时间,$s_b \in N, s_e \in N \cup \infty, s_d \in N$ 为转授权位置。

为便于描述,定义以下几类映射函数。

**定义 1** 授权用户和授权角色映射函数:

$ing(ts-auth) = ing = (u_{ing},r_{ing})$;

$ingu(ts-auth) = ingu(ing) = u_{ing}$;

$ingr(ts-auth) = ingr(ing) = r_{ing}$。

**定义 2** 转授权用户和转授权角色映射函数:

$ed(ts-auth) = ed = (u_{ed},r_{ed})$;

$edu(ts-auth) = edu(ed) = u_{ed}$;

$edr(ts-auth) = edr(ed) = r_{ed}$。

**定义 3** 时限和授权时间映射函数:

$time(ts-auth) = time = (duration,t_d)$;

$timed(ts-auth) = timed(time) = duration$;

$timet(ts-auth) = timet(time) = t_d$。

**定义 4** 区域和授权位置映射函数:

$space(ts-auth) = space = (dominion,d_d)$;

$spaced(ts-auth) = spaced(space) = dominion$;

$spaces(ts-auth) = spaces(space) = s_d$。

基于以上叙述,有如下授权关系:

$uao \in UAO \Leftrightarrow$

$uao = \{(Seco,A),(u_{ed},r_{ed}),([t_b,t_e],t_d),([s_b,s_e],s_d)\}$;

$uad \in UAD \Leftrightarrow$

$uad = \{(u_{ing}, r_{ing}), (u_{ed}, r_{ed}), ([t_b, t_e], t_d), ([s_b, s_e], s_d)\}$。

其中 $t_e \geqslant t_b \geqslant t_d, s_e \geqslant s_b \geqslant s_d$,$A$ 表示 Seco 具有系统授予用户任何角色的权限,尽管 Seco 可能并不具有这些角色,$u_{ing} \neq$ Seco。

### 2.2　TDRDM 的形式化表示

**定义 5**　TDRDM 的基本元素:

1) $U$、$R$、$P$、$S$ 和 $C$ 分别是用户集、角色集、权限集、会话集和约束集;

2) $TIME$、$SPACE$ 和 $N$ 分别是时限集、区域集和自然数集;

3) $UAO$:用户到初始角色之间的多对多的关系;

4) $UAD$:用户到转授权角色之间的多对多的关系;

5) $UA = UAO \cup UAD \cup U \times R$:用户到角色之间的多对多的关系;

6) $PA \subseteq P \times R$:权限到角色之间的多对多的关系;

7) $RH \subseteq R \times R$:角色与角色之间的继承关系,该关系是一偏序关系;

8) $ODLGT \subseteq UAO \times UAD$:原始转授权关系;

9) $DDLGT \subseteq UAD \times UAD$:传递性转授权关系;

10) $DLGT = ODLG \cup DDLGT \subseteq UA \times UA$:转授权关系;

11) $DT \subseteq UA \times UA$:转授权树。

**定义 6**　$TDRDM$ 的映射函数:

1) $Users - O: R \rightarrow 2^U$;

$Users - O(r,t,s) = \{u \mid (\exists r' \geqslant r)[uao = \{(Seco, A), (u, r'), (duration, t_d), (dominion, s_d)\} \in UAO \wedge t \in timed(uao) \wedge s \in spaced(uao)]\}$;

2) $Users - D: R \rightarrow 2^U$;

$Users - D(r,t,s) = \{u \mid (\exists r' \geqslant r)[uad = \{(u_{ing}, r_{ing}), (u, r'), (duration, t_d), (dominion, s_d)\} \in UAO \wedge t \in timed(uad) \wedge s \in spaced(uad)]\}$;

3) $Users: R \rightarrow 2^U$;

$Users(r,t,s) = Users - O(r,t,s) \cup Users - D(r,t,s)$;

4) $User: S \rightarrow U$;

$User(s_i,t,d) = \{u \mid ua = \{(u_{ing}, r_{ing}), (u, r'), (duration, t_d), (dominion, s_d)\} \in s_i \wedge t \in timed(ua) \wedge s \in spaced(ua)\}$;

5) $Role: S \rightarrow 2^R$;

$Role(s_i,t,s) \subseteq \{r \mid (\exists r' \geqslant r)[ua = \{(u_{ing}, r_{ing}), (User(s_i,t,s), r'), (duration, t_d), (dominion, s_d)\} \in UA \wedge t \in timed(ua) \wedge s \in spaced(ua)]\}$;

6) $Permissions: S \rightarrow 2^P$;

$Permissions(s_i,t,s) = \{p \mid (\exists r' \geqslant r)[(p, r') \in PA \wedge r' \in Role(s_i,t,s)]\}$;

7) $Roles - u(u,t,s) = \{r' \mid u \in Users(r',t,s), r' \geqslant r\}$;

8) $Prior: U \times R \rightarrow U \times R$;

$Prior(\{ing_1, (u,r), time_1, space_1\}) = \{\{ing_2, (u', r'), time_2, space_2\} \mid \{ing_1, (u,r), time_1, space_1\} \in UAD \wedge \{(u', r'), (u,r), time_3, space_3\} \in DLGT\}$;

$Prior\{(Seco, A), (u,r), time_1, space_1\} = \{\varnothing \mid \{(Seco, A), (u,r), time_1, space_1\} \in UAO\}$;

9) $Path: U \times R \rightarrow ((u_0, r_0), \cdots, (u_i, r_i))$;

$Path(u_0, r_0) = \{(u_0, r_0), (u_1, r_1), \cdots, (u_i, r_i), \cdots, (u_n, r_n) \mid \{ing_1, (u_i, r_i), time_1, space_1\} = Prior(\{ing_2, (u_{i-1}, r_{i-1}), time_2, space_2\} \in UA), i > 0\}$;

$Path(\{(Seco, A), (u,r), time_1, space_1\}) = \{\varnothing \mid \{(Seco, A), (u,r), time_1, space_1\} \in UAO\}$;

10) $Depth: U \times R \rightarrow N$;

$Depth(u,r) = \{n \mid (n = \mid Path(u,r) \mid)[(u,r) \in UAD]\}$;

$Depth(u,r) = \{0 \mid \{(Seco, A), (u,r), time_1, space_1\} \in UAO\}$;

11) $Valid - d: U \times R \times TIME \times SPACE \rightarrow TIME \times SPACE$;

$$Valid - d(u,r,t,s) = \begin{cases} ([t_b, t_e], [s_b, s_e]), & \text{当 } t \leqslant t_b \wedge s \in [s_b, s_e]; \\ ([t, t_e], [s_b, s_e]), & \text{当 } t \in [t_b, t_e] \wedge s \in [s_b, s_e]; \\ \varnothing, & \text{当 } t \geqslant t_e \vee s \in [s_b, s_e]; \end{cases}$$

其中 $\{(u_{ing}, r_{ing}), (u,r), ([t_b, t_e], t_d), ([s_b, s_e], s_d)\} \in DLGT$。

TDRDM 中各种授权之间的相互关系如图 3 所示,表 1 描述了 TDRDM 的映射函数的具体含义。

**表 1**　TDRDM 中的映射函数

| 函数 | 定义 | 描述 |
|---|---|---|
| $Users - O(r,t,s)$ | $R \rightarrow 2^U$ | 返回时刻 $t$ 位置 $s$ 具有初始角色 $r$ 的所有用户 |
| $Users - D(r,t,s)$ | $R \rightarrow 2^U$ | 返回时刻 $t$ 位置 $s$ 具有转授权角色 $r$ 的所有用户 |
| $Users(r,t,s)$ | $R \rightarrow 2^U$ | 返回时刻 $t$ 位置 $s$ 具有角色 $r$ 的所有用户 |
| $User(si,t,s)$ | $S \rightarrow U$ | 返回时刻 $t$ 位置 $s$ 会话 $s_i$ 所属的用户 |
| $Role(si,t,s)$ | $S \rightarrow 2^R$ | 返回时刻 $t$ 位置 $s$ 会话 $s_i$ 所具有的所有角色 |
| $Permissions(si,t,s)$ | $S \rightarrow 2^P$ | 返回时刻 $t$ 位置 $s$ 会话 $s_i$ 所具有的所有权限 |
| $Role - u(u,t,s)$ | $U \rightarrow 2^R$ | 返回时刻 $t$ 位置 $s$ 用户 $u$ 所具有的所有角色 |
| $Prior(ing1,(u,r),time1)$ | $U \times R \rightarrow U \times R$ | 返回授权路径中在$(u,r)$ 之前的所有授权 |
| $Path(u,r)$ | $U \times R \rightarrow ((u_0, r_0), \cdots, (u_i, r_i))$ | 返回授权$(u,r)$ 的授权路径 |
| $Depth(u,r)$ | $U \times R \rightarrow N$ | 返回授权$(u,r)$ 的授权路径的长度 |
| $Valid - d(u,r,t,s)$ | $U \times R \times TIME \times SPACE \rightarrow TIME \times SPACE$ | 返回时刻 $t$ 位置 $s$ 用户 $u$ 具有角色 $r$ 的有效时限与区域 |

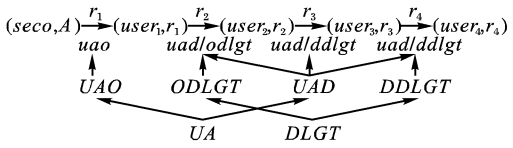


图 3　TDRDM 中的转授权关系

### 2.3　转授权

在分布式环境中对转授权进行判定,除了要依据参与转授权的用户和角色之外,时限与区域也应该是判断的依据之一。借用 ARBAC97 和 RDM2000 中定义的先决条件,有如下基于角色的转授权判定定义:

**定义 7** 先决条件 $CR$ 是用操作符"&"(与)和"|"(或)将元素 $cr$ 结合起来的布尔表达式。其中 $cr$ 可以是 $x$ 或者 $-x$ 的形式,前者表示具有角色 $x$,后者表示不具有角色 $x$。

**定义 8** 基于角色的转授权判定:

$can-delegation \subseteq R \times CR \times N \times TIME \times SPACE$;

$dlgt = \{r, cr, n, ([t_b, t_e], t_d), ([s_b, s_e], s_d)\} \in can-delegate \Leftrightarrow$

1) $u_{ing} \in \{u \mid Users(r'), r' \geqslant r\} \cap$

2) $Roles-u(u_{ed}, t, s) \in cr \cap$

3) $n(dlgt) \leqslant n \cap$

4) $([t_b, t_e], [s_b, s_e]) \subseteq Valid-d(u_{ing}, r, t_d, s_d)$。

其中 $CR$ 为先决条件集合,$n(dlgt)$ 表示转授权操作 $dlgt$ 中转授角色 $r$ 被再次转授的次数,即转授权的深度。

例如:$\{r, cr, n, time, space\} \in can-delegation$ 表示具有角色 $r$(或者 $r'$,其中 $r' \geqslant r$)的用户能够将角色 $r$(或者 $r''$,其中 $r \geqslant r''$)转授给当前所具有的角色满足 $cr$ 的用户,使之在时间段 $time$ 和区间段 $space$ 中具有被授予的角色的权限,而且当前转授权操作的深度分布不超过 $n$,因此有如下推论:

推论: 在授权路径中,任何授权的时限和区域不会超过处于该授权前面的授权的时限和区域。

图 4 给出了前例 CSCD 系统中 TDRDM 的时限和区域实例。设在时限段 $\tau_1 = [t_b, t_e]$ 和区域段 $\delta_1 = [s_b, s_e]$ 内,设计主管 $D_1$ 具有 $r_1$ 角色。在满足转授权条件前提下,如果 $D_1$ 在 $(t_{d1}, s_{d1})$ 点将 $r_3$ 转授予设计组员 $D_3$,则 $D_3$ 具有角色 $r_3$ 的时限 $\tau \in \tau_3 = [t_b, t_e]$ 和区域 $\delta \in \delta_3 = [s_b, s_e]$;如果 $D_1$ 在 $(t_{d2}, s_{d1})$ 点将 $r_2$ 授予设计组长 $D_2$,则 $D_2$ 具有 $r_2$ 的时限 $\tau \in \tau_2 = [t_{d2}, t_e]$ 和区域 $\delta \in \delta_2 = [s_b, s_e]$;在 $t_{d3}$ 时刻 $D_1$ 已不具有角色 $r_1$,因此 $D_1$ 不能给其他用户转授任何角色。$D_1$、$D_2$ 和 $D_3$ 在 $s_{d1}$ 和 $s_{d2}$ 位置任何时候都不具有 $r_1$、$r_2$ 和 $r_3$ 角色。

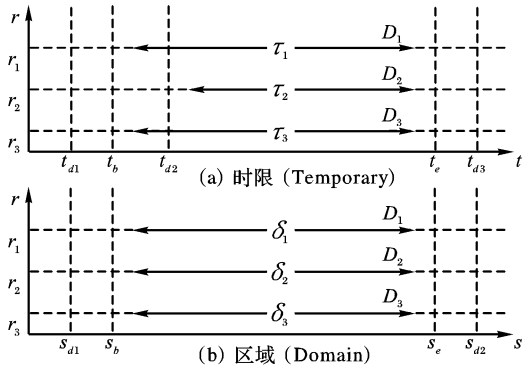


图 4 TDRDM 的时限和区域

### 2.4 转授权撤销

与授权相对应,转授权撤销也是安全系统访问控制中的重要过程[1]。系统运行过程中,如果 $u_{ing}$ 发现 $u_{ed}$ 滥用被授予的角色 $r_{ed}$ 中的权限,不论是系统 Seco 还是 $u_{ing}$,都应该及时撤销 $r_{ed}$。转授权撤销既包括撤销 UAO 中授予的角色,也包括撤销 DLGT 中转授予的角色。转授权撤销在方法上又分为基于时限的自动转授权撤销和用户对转授权的主动撤销。

基于时限的自动转授权撤销的基础是转授权的时限性。当系统时间超过转授权的最大时限时,系统将自动撤销 $u_{ed}$ 的 $r_{ed}$。基于时限的自动转授权撤销方式是一种自触发过程(Self triggered process)。定义 9 给出了基于时限的自动转授权撤销的判定公式:

**定义 9** $can-auto-revoke \in R \times TIME \times SPACE$;

$(r, t, s)\delta \in can-auto-revoke \Leftrightarrow$

$Valid-d(u, r, t, s) = ([t_b, t_e], [s_b, s_e])$

$t > t_e, s \in [s_b, s_e]$。

基于时限的自动转授权撤销方式是一种比较有效的撤销方式,可以让系统自动撤销到期的 $r_{ed}$,从而减轻 Seco 的负担。但是,仅仅具有这种方式的系统不能够及时撤销 $u_{ed}$ 对 $r_{ed}$ 权限的滥用,因此系统还必需支持用户主动的转授权撤销方式。

## 3 结语

时间限制与区域约束是分布式访问控制中的重要组成部分。不具有时间限制与区域约束的访问控制模型是不完备的模型,不能很好地适应实际应用。本文在介绍了转授权的基本特征、并引入转授权区域性特征的基础上,分析了当前两种主要的基于角色的转授权模型 RBDM0 和 RDM2000,指出其不支持转授权的时间限制与区域约束的不足;在对 RDM2000 模型的相关部分进行扩充的基础上,提出具有时限性与区域性特征的转授权模型(TDRDM),并通过分布式系统实例对其进行描述;最后对该模型的转授权和转授权撤销规则进行了系统的讨论。

**参考文献:**

[1] ZHANG LH, AHN GJ, CHU BT. A rule-based framework for role-based delegation[J]. ACM Transactions on information and system security, 2003, 6(3): 404-441.

[2] SANDHU RS, COYNE EJ, FEINSTEIN HL, *et al.* Role-based access control models[J]. IEEE Computer, 1996, 29(2): 38-47.

[3] SANDHU RS, MUNAWER Q. How to do discretionary access using roles[A]. In Proceeding of the third ACM workshop on role-based access control [C]. Barkley: ACM Press, 1998. 47-54.

[4] SANDHU RS, BHAMIDIPATI V, MUNAWER Q. The ARBAC97 model for role-based administration of roles[J]. ACM Transactions on information and system security, 1999, 2(1): 105-135.

[5] MUNAWER Q. Administrative models for role-based access control [D]. George: George Mason University, 2000.

[6] PARK JS, SANDHU RS. RBAC on the Web by smart certificates [A]. In Proceeding of the 4th ACM workshop on role-based access control[C]. New York: ACM Press, 1999.1-9.

[7] PARK JS, SANDHU RS, GHANTA SL. RBAC on the web by secure cookies[A]. International federation for information processing the 13th Int'l conference on database security[C]. Washington: Deventer, 1999.

[8] BARKA E, SANDHU RS. Framework for role-based delegation models[A]. The 16th annual computer security applications conference[C]. New Orleans: Louisiana, 2000.

[9] BARKA E, SANDHU RS. A role-based delegation model and some extensions[A]. In Proceeding of 23rd national information systems security conference[C]. Baltimore, MD, USA: NIST, 2000.101-114.

[10] BERTINO E, BETTINI C, FERRARI E, *et al.* A temporal access control mechanism for database systems[J]. IEEE Transactions on knowledge and data engineering, 1996, 8(1): 67-80.

[11] BERTINO E, BETTINI C, FERRARI E, *et al.* An access control model supporting periodicity constraints and temporal reasoning[J]. ACM Transactions on data-base systems, 1998, 23(3): 231-285.

[12] BERTINO E, BETTINI C, FERRARI E, *et al.* Decentralized administration for a temporal access control model[J]. Information systems, 1997, 22(4): 223-248.