·安全技术· 文章编号：1000—3428(2013)04—0146—05 文献标识码：A 中图分类号：TP309.2

# 基于信任度和协作安全策略的委托模型

孙 伟[1]，汪 磊[2]

(1. 信阳师范学院计算机与信息技术学院，河南 信阳 464000；2. 信阳供电公司，河南 信阳 464000)

**摘 要：**为提高委托过程的可信度并保证系统的安全性，提出一种基于信任度和协作安全策略的委托模型。利用信任资历、信任经验和信任推荐综合计算不同用户的信任度，选取值得信任的受托对象，采用互斥角色约束间接实施协作分工策略的方法，进一步选取保证系统安全性的受托对象。理论分析与应用实例证明，与现有模型相比，该模型通过量化计算信任度及最小约束构造算法确定的受托用户能够较好地体现委托的可靠性，并且满足系统状态的安全性要求。

**关键词：**委托；信任度；协作分工策略；信任资历；信任经验；信任推荐

# Delegation Model Based on Trust Degree and Secure Strategy of Collaboration

SUN Wei[1], WANG Lei[2]

(1. School of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China;
2. Xinyang Power Supply Company, Xinyang 464000, China)

**【Abstract】**In order to enhance reliability in delegations and ensure system security, this paper proposes a delegation model based on trust degree and secure strategy of collaboration. Trust qualifications, trust experiences and trust recommendations are utilized to comprehensively compute trust values, and trustworthy candidates with higher values are chosen. Mutually exclusive role constraints are adopted to indirectly enforce division policy of collaboration, and the most appropriate delegate is chosen in the secure collaborative environment. Compared with existing models, theoretical analyses and experimental results show that the model can efficiently reflect reliability in delegations, and it satisfies requests of system security.

**【Key words】**delegation; trust degree; policy of collaboration division; trust qualification; trust experience; trust recommendation
**DOI:** 10.3969/j.issn.1000-3428.2013.04.034

## 1 概述

建立在基于角色的访问控制(Role-based Access Control, RBAC)模型基础上的委托允许将集中式授权管理工作分散给普通用户去实施，已被证明是一种灵活、方便的访问控制技术。随着信息技术的不断发展和大规模应用，信息系统的安全性与可靠性成为越来越突出的问题。计算机支持的协同工作系统要求多个用户相互协作、彼此沟通，以达到相互牵制，共同决策资源的访问权限。信任协作作为一种有效的访问控制策略，可以满足被访问资源或信息的机密性和隐私性要求，防止由于委托的随意性而产生权限滥用的危险。因此，在协作环境下当某一用户临时出差(或休假)而需要另一值得信任的用户代替参与协作时，如何设计安全、可靠的委托模型很具挑战性。为防止因受托对象不可信、随意委托而导致权限滥用、系统状态的安全性难以得到保证，本文提出一种基于信任度和协作安全策略的委托模型 TSSCBDM(Trust degree and Secure Strategy of Collaboration-based Delegation Model)，其能够提高协作环境下委托的可信度，并满足系统状态的安全性要求。

## 2 相关工作

针对 RBAC 中集中式授权存在的管理负担繁重、缺乏灵活性等问题，文献[1]提出了基于 RBAC 的委托，将授权管理灵活地下放给普通用户去实施，减轻了系统的管理负担，支持角色层次上以角色为委托单位、粗中粒度相结合、约束可控的委托，并给出了工作流系统中的委托描述，对于协作环境下的委托研究具有一定的借鉴性。文献[2]提出了一种基于阈值的协作访问控制模型 TBCACM，将资源的访问权限与阈值相关联，并能够将带贡献系数的权限转授给其他用户代替参与协作，共同决策资源的访问权限。文

**基金项目：**河南省教育厅科学技术研究基金资助重点项目(13A520765)；河南省信息技术教育研究基金资助项目(ITE12192)
**作者简介：**孙 伟(1981－)，男，讲师、硕士，主研方向：访问控制，安全模型；汪 磊，工程师
**收稿日期：**2012-04-28 **修回日期：**2012-07-02 **E-mail：**sw_810715@163.com

献[3]提出了一种基于角色的细粒度委托限制框架RBFDCF，给出了委托限制的形式化描述，能够有效防止委托冲突，保证系统的安全性，并给出了协作环境下委托应用示例。文献[4]提出了一种基于场所的协作访问控制模型LCACM，给出了协作小组内的分层授权机制，能够满足协作环境下委托的安全性、灵活性要求。TBCACM、RBFDCF、LCACM 能够满足系统的安全性要求[5]，但均未对受托对象的信任度进行详细地分析或讨论，一旦选择可信度不高的受托对象，委托就是不可靠的，且存在权限滥用的危险。文献[6]提出了一种基于信任的访问控制模型 TBACM，将传统的 RBAC 和信任管理相结合，通过综合计算不同用户的信任值，并评价其行为能力，能够实现细粒度、准确可靠的委托授权。文献[7]提出了一种基于用户信任的动态多级访问控制模型 UTDMACM，根据用户行为的动态变化，将用户信任划分为静态信任级别和动态信任级别，能够实现分级的访问控制及细粒度的动态授权。文献[8]提出了一种基于多维度量和上下文的访问控制模型 MMCBACM，根据网络环境和用户状态的动态多变性，引入信任度量和上下文约束概念，能够实现委托授权的动态、实时控制。TBACM、UTDMACM、MMCBACM 能够较好地体现委托过程的可靠性，但均不能满足给定协同工作环境下安全性要求[9]，容易破坏系统状态的安全性，存在安全隐患。针对基于现有模型的委托在可靠性、安全性等方面存在的问题，本文将信任关系和协作安全策略相结合，提出 TSSCBDM 模型。

## 3　信任关系

委托方与受托对象的信任关系[6-8]取决于三方面因素：信任资历，信任经验及信任推荐。

### 3.1　信任资历

**定义 1**(任务属性 $ta_i$)　多个用户 $u_1,u_2,\cdots,u_j,\cdots$在协作执行某项任务 $t_i$ 前，须具备 $t_i$ 所要求的一系列资格条件 $a_{i1},a_{i2},\cdots,a_{in}$，称其为 $t_i$ 的属性，用 $ta_i$ 表示：$ta_i=\{a_{i1},a_{i2},\cdots,a_{in}\}$。

**定义 2**(用户属性 $ua_j$)　协作用户 $u_j$ 本身所具备的一系列资格 $a_{j1},a_{j2},\cdots,a_{jm}$，称为 $u_j$ 的属性，用 $ua_j$ 表示：$ua_j=\{a_{j1},a_{j2},\cdots,a_{jm}\}$。

**定义 3**(基本资历 $A_{j\to i}$)　用 $A_{j\to i}$ 表示 $u_j$ 关于 $t_i$ 的基本资历。若用权值 $wa_{i1},wa_{i2},\cdots,wa_{in}$ 分别表示 $a_{i1},a_{i2},\cdots,a_{in}$ 对 $t_i$ 的重要程度，且 $\sum_{r=1}^{n} wa_{ir}=1$，其中，$0\leqslant wa_{ir}\leqslant 1$，则 $A_{j\to i}=\sum_{k=1}^{p} wa_{ik}$。其中，$p\leqslant|ua_j\cap ta_i|$，$wa_{ik}$ 是隶属于 $a_{ik}$ 的权值，$a_{ik}\in ua_j\cap ta_i$。

**定义 4**(附属资历 $RA_{j\to i}$)　$u_d$ 在协作参与执行 $t_i$ 时，需将其权利通过 $r_d$ 委托给 $u_j$。若$(u_j,r_j)\in UAO$，$dist(r_d,r_j)$表示 $r_d$、$r_j$ 在角色层次 $RH$ 上的距离，其中，$0\leqslant dist(r_d,r_j)\leqslant 1$，则称 $dist(r_d,r_j)$为 $u_j$ 关于 $t_i$ 的附属资历，用 $RA_{j\to i}$ 表示。

**定义 5**(信任资历 $P_{j\to i}$)　基本资历 $A_{j\to i}$ 与附属资历 $RA_{j\to i}$ 共同构成 $u_j$ 关于 $t_i$ 的信任资历，用 $P_{j\to i}$ 表示。若用权值 $w_a$、$w_{ra}$ 分别表示 $A_{j\to i}$、$RA_{j\to i}$ 对 $P_{j\to i}$ 的贡献系数，且 $w_a+w_{ra}=1$，其中，$0\leqslant w_a,w_{ra}\leqslant 1$，则 $P_{j\to i}=w_a\times A_{j\to i}+w_{ra}\times RA_{j\to i}$。

### 3.2　信任经验

**定义 6**(信任经验 $E_{j\to i}$)　$u_j$ 在以往代替委托方 $u_d$ 参与执行 $t_i$ 的过程中，所有完成效果的叠加称为 $u_j$ 关于 $t_i$ 的信任经验，用 $E_{j\to i}$ 表示。若用 $wt_{jk}=k/n(1\leqslant k\leqslant n)$表示 $u_j$ 第 $k$ 次执行 $t_i$ 的经验系数，且规定在某时期内较近一次执行 $t_i$ 比较久远发生的拥有更大的 $wt_{jk}$；用 $e_{jk}$ 表示 $u_j$ 第 $k$ 次完成 $t_i$ 的效果，其中，$0\leqslant e_{jk}\leqslant 1$，并作如下规定：(1)$e_{jk}=1$，执行任务成功；(2)$e_{jk}=0$，执行任务失败；(3)$e_{jk}\to 1$，表现效果较好；(4)$e_{jk}\to 0$，表现效果较差，那么，$E_{j\to i}=\sum_{k=1}^{n} wt_{jk}\times e_{jk}$。

### 3.3　信任推荐

**定义 7**(信任推荐 $R_{j\to i}$)　$u_d$ 需将其权利通过 $m$ 个用户 $ur_1,ur_2,\cdots,ur_m$，共同推荐委托给 $u_j$。若用 $t_k(1\leqslant k\leqslant m)$表示系统关于 $ur_k$ 的信任度，$r_{kj}$ 表示 $ur_k$ 对 $u_j$ 的推荐值，则 $u_j$ 关于 $t_i$ 的信任推荐为：$R_{j\to i}=\frac{\sum_{k=1}^{m} t_k\times r_{kj}}{\sum_{k=1}^{m} t_k}$，$0\leqslant t_k,r_{kj}\leqslant 1$。

### 3.4　信任度

**定义 8**(信任度 $T_{j\to i}$)　信任资历 $P_{j\to i}$、信任经验 $E_{j\to i}$ 及信任推荐 $R_{j\to i}$ 三者共同构成 $u_j$ 关于 $t_i$ 的信任度 $T_{j\to i}$。若用权值 $w_p$、$w_e$、$w_r$ 分别表示 $P_{j\to i}$、$E_{j\to i}$、$R_{j\to i}$ 对 $T_{j\to i}$ 的贡献系数，且 $w_p+w_e+w_r=1$，其中，$0\leqslant w_p,w_e,w_r\leqslant 1$，则 $T_{j\to i}=w_p\times P_{j\to i}+w_e\times E_{j\to i}+w_r\times R_{j\to i}$。对于由系统设定的信任阈值 $H_{j\to i}$，若 $T_{j\to i}\geqslant H_{j\to i}$，则表明 $u_j$ 值得信任；否则，$u_j$ 并不值得信任。

## 4　协作安全策略

**定义 9**(系统状态 $\gamma$)　系统状态 $\gamma$ 是一个三元组<$UA,PA,RH$>，其中，$UA$、$PA$、$RH$ 为 RBAC 的基本元素集。用 $Roles_\gamma(u)$、$Perms_\gamma(u)$分别表示状态 $\gamma$ 下关联用户 $u$ 的角色及分配给 $u$ 的权限，形式化描述如下：

$$Roles_\gamma(u)=\{r\in R\mid\exists r_1\in R,(u,r_1)\in UA\wedge(r_1,r)\in RH\}$$

$$Perms_\gamma(u)=\{p\in P\mid\exists r_2\in R,(p,r_2)\in PA\wedge(Roles_\gamma(u),r_2)\in RH\}$$

### 4.1　系统状态的安全性

**定义 10**(协作职责分工 $k$-$n$ RSSOC)　执行某项任务需要 $n$ 个不同角色 $r_1,r_2,\cdots,r_n$，至少需要 $k$ 个用户相互协作，才能共同拥有该任务的 $n$ 个角色，用 $rssoc$<$\{r_1,r_2,\cdots,r_n\},k$>表示，记为 $e=rssoc$<$\{r_1,r_2,\cdots,r_n\},k$>, $1<k\leqslant n$[9]。

**定义 11**(系统状态的安全性 $safe_e(\gamma)$)　对于 $e=rssoc$<$\{r_1,r_2,\cdots,r_n\},k$>，如果状态 $\gamma$ 下任意$(k-1)$个用户都不能共同拥有$\{r_1,r_2,\cdots,r_n\}$，那么称 $\gamma$ 关于 $e$ 是安全的，记为 $safe_e(\gamma)=1$；否

则，$\gamma$关于 $e$ 是不安全的，记为 $safe_e(\gamma)=0$。由 $n$ 个不同协作分工组成的集合 $E=\{e_1,e_2,\cdots,e_n\}$，如果状态$\gamma$对于任意 $e_i(1\leqslant i\leqslant n)$都是安全的，那么称$\gamma$关于 $E$ 是安全的，记为 $safe_E(\gamma)=1$；否则，$\gamma$关于 $E$ 是不安全的，$safe_E(\gamma)=0$。

安全的系统状态形式化描述如下：

$$\forall(u_1,u_2,\cdots,u_{k-1})\in U:$$

$$\{r_1,r_2,\cdots,r_n\}\not\subset\bigcup_{i=1}^{k-1}Roles_\gamma(u_i)\Rightarrow safe_e(\gamma)=1$$

不安全的系统状态形式化描述如下：

$$\exists(u_1,u_2,\cdots,u_{k-1})\in U:$$

$$\bigcup_{i=1}^{k-1}Roles_\gamma(u_i)\supseteq\{r_1,r_2,\cdots,r_n\}\Rightarrow safe_e(\gamma)=0$$

**定理 1** 对于给定的系统状态$\gamma$和协作分工策略集 $E$，检验 $safe_E(\gamma)$是否为真的过程是 $P$ 类问题。

证明：(1)对于$\gamma$中的某用户 $u$，计算出 $Roles_\gamma(u)$。(2)计算出 $Roles_\gamma(u)$出现在 $e$ 的个数，记为 $s$。(3)将 $s$ 与 $e$ 中的 $k$ 进行比较。上述每一步都是可计算的。如果用 $N_u$、$N_r$、$M$ 分别表示$\gamma$中的用户数、角色数、$E$ 中出现的协作分工策略数，那么检验 $safe_E(\gamma)$过程的时间复杂度 $O(N_u\times N_r\times M)$为多项式形式，在有效时间 $P$ 内是可计算的。定理 1 得证。

### 4.2 系统状态的满足性

**定义 12**(互斥角色约束 *t-m* SMER) 任意用户都不能同时拥有$\{r_1,r_2,\cdots,r_m\}$的 $t$ 个或更多的角色，用 $smer<\{r_1,r_2,\cdots,r_m\},t>$表示，记为 $c=smer<\{r_1,r_2,\cdots,r_m\},t>,1<t\leqslant m$[9]。

**定义 13**(系统状态的满足性 $sat_c(\gamma)$) 对于 $c=smer<\{r_1,r_2,\cdots,r_m\},t>$，如果状态$\gamma$下任意用户拥有$\{r_1,r_2,\cdots,r_m\}$的角色数都少于 $t$，那么称$\gamma$关于 $c$ 是可满足的，记为 $sat_c(\gamma)=1$；否则，$\gamma$关于 $c$ 是不满足的，$sat_c(\gamma)=0$。由 $n$ 个不同约束组成的集合 $C=\{c_1,c_2,\cdots,c_n\}$，如果状态$\gamma$对于任意的 $c_i(1\leqslant i\leqslant n)$都是可满足的，那么称$\gamma$关于 $C$ 是可满足的，记为 $sat_c(\gamma)=1$；否则，$\gamma$关于 $C$ 是不满足的，$sat_c(\gamma)=0$。

可满足的系统状态形式化描述如下：

$$\forall u\in U:|Roles_\gamma(u)\cap\{r_1,r_2,\cdots,r_m\}|<t\Rightarrow sat_c(\gamma)=1$$

不满足的系统状态形式化描述如下：

$$\exists u\in U:|Roles_\gamma(u)\cap\{r_1,r_2,\cdots,r_m\}|\geqslant t\Rightarrow sat_c(\gamma)=0$$

**定理 2** 对于给定的系统状态$\gamma$和约束集 $C$，检验 $sat_C(\gamma)$是否为真的过程也是 $P$ 类问题。

证明过程同定理 1。因此，对$\gamma$直接实施 *t-m* SMER 也是有效的。

### 4.3 协作分工策略的间接实施

**定义 14**(*k-n* RSSOC 策略的间接实施) 对于给定的$\gamma$、$c=smer<\{r_1,r_2,\cdots,r_m\},t>$及 $e=rssoc<\{r_1,r_2,\cdots,r_n\},k>$，称 $c$ 可间接实施 $e$，当且仅当 $\forall\gamma:sat_c(\gamma)\Rightarrow safe_e(\gamma)$。

**定义 15**(强约束关系$\succ$) 对于任意两约束 $c_1$、$c_2$ 以及协作分工策略 $e$，如果 $c_1$和 $c_2$都可实施 $e$，那么说 $c_1$的约束性不弱于 $c_2$，当且仅当 $\forall\gamma:sat_{c_1}(\gamma)\Rightarrow sat_{c_2}(\gamma)$，表示为 $c_1\succcurlyeq c_2$。如果 $c_1\succcurlyeq c_2$，且不存在 $c_2\succcurlyeq c_1$，那么称 $c_1$比 $c_2$具有更强的约束性，约束范围更大，表示为 $c_1\succ c_2$。

**定义 16**(最小约束) 对于给定 $e$，当且仅当存在 $c$ 可间接实施 $e$ 且不存在 $c'$ ($c\succ c'$)，使得 $c'$也可间接实施 $e$，称 $c$ 是实施 $e$ 的最小约束。

**定义 17**(*k-n* RSSOC 策略的准确实施) 约束集 $C$ 可准确实施协作分工策略 $e$，当且仅当 $\forall\gamma:safe_e(\gamma)\wedge live_e(\gamma)\Rightarrow sat_C(\gamma)$，其中，$live_e(\gamma)$表示 $C$ 中任一约束在实施 $e$ 时能够覆盖 $e$ 的所有角色[10]。

**引理 1** 若给定$\gamma_1$及 $e_1=rssoc<\{r_1,r_2,\cdots,r_n\},n>$，则 $c_1=smer<\{r_1,r_2,\cdots,r_n\},t>$可准确实施 $e_1$，当且仅当 $t=2$。

**引理 2** 若给定$\gamma_2$及 $e_2=rssoc<\{r_1,r_2,\cdots,r_n\},2>$，则 $c_2=smer<\{r_1,r_2,\cdots,r_n\},t>$可准确实施 $e_2$，当且仅当 $t=n$。

最小约束的构造算法 Smers-Construct 步骤如下：

**输入** 给定协作分工策略的一个实例 $e=rssoc<\{r_1,r_2,\cdots\},k>$，令 $n=|\{r_1,r_2,\cdots\}|,1<k\leqslant n$

**输出** 所有最小约束的集合 $C_{\text{Smers-Construct}}=\{smer<\{r_1',r_2',\cdots\},t>\}$，其中，$\{r_1',r_2',\cdots\}\subseteq\{r_1,r_2,\cdots\}$，并令 $m=|\{r_1',r_2',\cdots\}|,1<t\leqslant m$

Begin

初始化 $C_{\text{Smers-Construct}}=\varnothing$;

if (k=2) then

$C_{\text{Smers-Construct}}=\{\text{smer}<\{r_1,r_2,\cdots\},n>\}\cup C_{\text{Smers-Construct}}$;

else if (k=n) then

$C_{\text{Smers-Construct}}=\{\text{smer}<\{r_1,r_2,\cdots\},2>\}\cup C_{\text{Smers-Construct}}$;

else if (2<k<n) then

for(t=2;t≤$\lfloor(n-1)/(k-1)\rfloor$+1;t++)

{ m=(k–1)×(t–1)+1;

for(从$\{r_1,r_2,\cdots\}$中任选 m 个角色的子集$\{r_1',r_2',\cdots\}$)

$C_{\text{Smers-Construct}}=\{\text{smer}<\{r_1',r_2',\cdots\},t>\}\cup C_{\text{Smers-Construct}}$;}

End

**定理 3** 对于任意 $e=rssoc<\{r_1,r_2,\cdots\},k>$，其中，$|\{r_1,r_2,\cdots\}|=n$；$1<k\leqslant n$，由 Smers-Construct 算法生成的一定是实施 $e$ 的最小约束。

根据定义 11、定义 13、定义 14、引理 1、引理 2 可证定理 3。

## 5 模型分析

根据信任关系、协作安全策略，对 TSSCBDM 的可靠性、安全性作以下分析。

### 5.1 问题描述

某企业购进一批产品的角色层次关系 *RH* 如图 1 所示，表 1、表 2 分别表示多部门协同工作环境下系统原始指派的用户-角色分配关系 *UA*、权限-角色分配关系 *PA*。假设副经理 2 出差，需要临时将其权限委托给其他协作者(如 $e$、$g$、$h$)代为执行相应的岗位任务 $t_{S\_DM_2}$，则对 $e$、$g$、$h$ 的分析如下文所示。

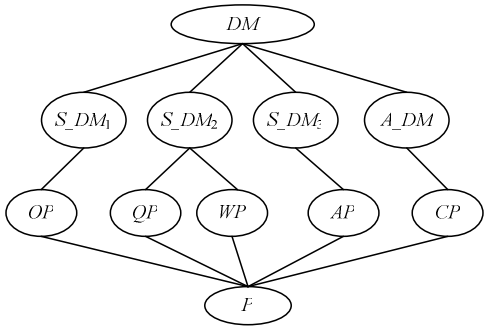


**图 1　角色层次关系**

**表 1　用户-角色分配关系**

| 角色 | 用户 |
|---|---|
| *DM*(部门经理) | *a* |
| *S-DM*$_1$(副经理 1，负责产品订购) | *b* |
| *S-DM*$_2$(副经理 2，负责仓库保管) | *c* |
| *S-DM*$_3$(副经理 3，负责财务账) | *d* |
| *A-DM*(经理助理，负责现金账) | *e* |
| *OP*(订购员) | *f* |
| *QP*(质检员) | *g* |
| *WP*(保管员) | *h* |
| *AP*(会计员) | *i* |
| *CP*(出纳员) | *j* |
| *P*(一般职员) | *k* |

**表 2　权限-角色分配关系**

| 角色 | 权限 |
|---|---|
| *DM* | $p_1$(产品购进总决策权) |
| *S-DM*$_1$ | $p_2$(产品订购决策权) |
| *S-DM*$_2$ | $p_3$(仓库保管决策权) |
| *S-DM*$_3$ | $p_4$(财务管理决策权) |
| *A-DM* | $p_5$(现金管理决策权) |
| *OP* | $p_6$(订购产品) |
| *QP* | $p_7$(检查产品质量) |
| *WP* | $p_8$(储存产品) |
| *AP* | $p_9$(记账、开据发票) |
| *CP* | $p_{10}$(收、支现金) |
| *P* | $p_{11}$(收集、整理文档) |

## 5.2　信任关系计算及安全策略实施

### 5.2.1　信任资历的量化

系统预置的 $t_{S\_DM_2}$ 与权值的关系为：

$wa_{\text{经理级别}}=0.6, wa_{\text{仓库保管系统}}=0.4$

*e*、*g*、*h* 关于 $t_{S\_DM_2}$ 的基本资历分别为：

$$A_{e\to t_{S\_DM_2}}=0.6, A_{g\to t_{S\_DM_2}}=0.4, A_{h\to t_{S\_DM_2}}=0.4$$

*e*、*g*、*h* 关于 $t_{S\_DM_2}$ 的附属资历分别为：

$$RA_{e\to t_{S\_DM_2}}=0, RA_{g\to t_{S\_DM_2}}=0.7, RA_{h\to t_{S\_DM_2}}=0.7$$

若基本资历、附属资历对信任资历具有同等的贡献作用，即 $w_a$=$w_{ra}$=0.5，则通过量化计算 *e*、*g*、*h* 关于 $t_{S\_DM_2}$ 的信任资历值分别为：

$$P_{e\to t_{S\_DM_2}}=0.3, P_{g\to t_{S\_DM_2}}=0.55, P_{h\to t_{S\_DM_2}}=0.55$$

### 5.2.2　信任经验的量化

规定 *e*、*g*、*h* 在同一计量单位拥有相同的经验系数。根据表 3 给出的计量单位、经验系数及 *e*、*g*、*h* 各自完成任务效果的对应关系，则通过量化计算 *e*、*g*、*h* 关于 $t_{S\_DM_2}$ 的信任经验值分别为：

$$E_{e\to t_{S\_DM_2}}=0.8, E_{g\to t_{S\_DM_2}}=0.56, E_{h\to t_{S\_DM_2}}=0.44$$

**表 3　经验系数与完成效果的对应关系**

| 计量单位 *k* | 经验系数 $wt_k$ | 完成效果 $e_{ek}$ | 完成效果 $e_{gk}$ | 完成效果 $e_{hk}$ |
|---|---|---|---|---|
| 1 | 0.2 | \ | \ | 0.7 |
| 2 | 0.4 | \ | 0.6 | \ |
| 3 | 0.6 | \ | \ | 0.5 |
| 4 | 0.8 | \ | 0.4 | \ |
| 5 | 1.0 | 0.8 | \ | \ |

### 5.2.3　信任推荐的量化

根据表 4 给出的推荐人、推荐人信任度及对 *e*、*g*、*h* 推荐值的对应关系，则通过量化计算 *e*、*g*、*h* 关于 $t_{S\_DM_2}$ 的信任推荐值分别为：

$$R_{e\to t_{S\_DM_2}}=0.66, R_{g\to t_{S\_DM_2}}=0.34, R_{h\to t_{S\_DM_2}}=0.4$$

**表 4　推荐人与推荐人信任度、推荐值的对应关系**

| 推荐人 $ur_k$ | 推荐人信任度 $t_k$ | 推荐值 $r_{ke}$ | 推荐值 $r_{kg}$ | 推荐值 $r_{kh}$ |
|---|---|---|---|---|
| *a* | 0.6 | 0.9 | 0.2 | 0.3 |
| *b* | 0.2 | 0.5 | 0.4 | 0.5 |
| *d* | 0.2 | 0.1 | 0.7 | 0.6 |

### 5.2.4　信任度的综合计算

根据信任资历、信任经验、信任推荐对信任关系的不同贡献作用，分别取值 $w_p=0.2$、$w_e=0.7$、$w_r=0.1$ 且 $w_p+w_e+w_r=1$，*e*、*g*、*h* 关于 $t_{S\_DM_2}$ 信任度的综合计算如下：

$$T_{e\to t_{S\_DM_2}}=w_p\times P_{e\to t_{S\_DM_2}}+w_e\times E_{e\to t_{S\_DM_2}}+w_r\times R_{e\to t_{S\_DM_2}}=0.2\times0.3+0.7\times0.8+0.1\times0.66=0.686$$

$$T_{g\to t_{S\_DM_2}}=w_p\times P_{g\to t_{S\_DM_2}}+w_e\times E_{g\to t_{S\_DM_2}}+w_r\times R_{g\to t_{S\_DM_2}}=0.2\times0.55+0.7\times0.56+0.1\times0.34=0.536$$

$$T_{h\to t_{S\_DM_2}}=w_p\times P_{h\to t_{S\_DM_2}}+w_e\times E_{h\to t_{S\_DM_2}}+w_r\times R_{h\to t_{S\_DM_2}}=0.2\times0.55+0.7\times0.44+0.1\times0.4=0.458$$

对于给定信任阈值 $H_{t_{S\_DM_2}}=0.5$，有 $T_{e\to t_{S\_DM_2}}>T_{g\to t_{S\_DM_2}}>H_{e\to t_{S\_DM_2}}>T_{h\to t_{S\_DM_2}}$，表明 *e*、*g* 比较值得信任，而 *h* 不值得信任。于是对 *c* 而言，待选可信受托对象集 *TU*={*e*,*g*}。

### 5.2.5　安全策略的实施

若用$\gamma_1$、$\gamma_2$分别表示对 *e*,*g* 实施委托后的系统状态，则对于 $k(1<k\leqslant5)$取不同值情况下的协作分工策略 *rssoc*<{*DM*, *S_DM*$_1$, *S_DM*$_2$,*S_DM*$_3$, *A_DM*}, *k*>、由 Smers-Construct 算法构造的最小约束集 $C_{\text{Smers-Construct}}$ 及状态$\gamma_1$、$\gamma_2$ 满足性、安全性描述的对应关系如表 5 所示。

**表 5 协作分工策略、最小约束集及状态满足性、安全性描述对应关系**

| 协作分工策略 | 由 Smers-Construct 算法构造的最小约束集 | $\gamma_1$ 满足性描述 | $\gamma_1$ 安全性描述 | $\gamma_2$ 满足性描述 | $\gamma_2$ 安全性描述 |
|---|---|---|---|---|---|
| $e_1$=*rssoc*<{*DM*,*S_DM*$_1$, *S_DM*$_2$,*S_DM*$_3$,*A_DM*},2> | $C_1$={*smer*<{*DM*,*S_DM*$_1$,*S_DM*$_2$, *S_DM*$_3$,*A_DM*},5>} | $sat_{C_1}(\gamma_1)=1$ | $saf_{e_1}(\gamma_1)=1$ | $sat_{C_1}(\gamma_2)=1$ | $safe_{e_2}(\gamma_2)=1$ |
| $e_2$=*rssoc*<{*DM*,*S_DM*$_1$, *S_DM*$_2$,*S_DM*$_3$,*A_DM*},3> | $C_2$={*smer*<{*DM*,*S_DM*$_1$,*S_DM*$_2$},2>, *smer*<{*DM*,*S_DM*$_1$,*S_DM*$_3$},2>, *smer*<{*DM*,*S_DM*$_1$,*A_DM*},2>, *smer*<{*DM*,*S_DM*$_2$,*S_DM*$_3$},2>, *smer*<{*DM*,*S_DM*$_2$,*A_DM*},2>, *smer*<{*DM*,*S_DM*$_3$,*A_DM*},2>, *smer*<{*S_DM*$_1$,*S_DM*$_2$,*S_DM*$_3$},2>, *smer*<{*S_DM*$_1$,*S_DM*$_2$,*A_DM*},2>, *smer*<{*S_DM*$_1$,*S_DM*$_3$,*A_DM*},2>, *smer*<{*S_DM*$_2$,*S_DM*$_3$,*A_DM*},2>, *smer*<{*DM*,*S_DM*$_1$,*S_DM*$_2$,*S_DM*$_3$,*A_DM*},3>} | $sat_{C_2}(\gamma_1)=0$ | $safe_{e_2}(\gamma_1)=0$ | $sat_{C_2}(\gamma_2)=1$ | $safe_{e_2}(\gamma_2)=1$ |
| $e_3$=*rssoc*<{*DM*,*S_DM*$_1$, *S_DM*$_2$,*S_DM*$_3$,*A_DM*},4> | $C_3$={*smer*<{*DM*,*S_DM*$_1$,*S_DM*$_2$,*S_DM*$_3$},2>, *smer*<{*DM*,*S_DM*$_1$,*S_DM*$_2$,*A_DM*},2>, *smer*<{*DM*,*S_DM*$_1$,*S_DM*$_3$,*A_DM*},2>, *smer*<{*DM*,*S_DM*$_2$,*S_DM*$_3$,*A_DM*},2>, *smer*<{*S_DM*$_1$,*S_DM*$_2$,*S_DM*$_3$,*A_DM*},2>} | $sat_{C_3}(\gamma_1)=0$ | $safe_{e_3}(\gamma_1)=0$ | $sat_{C_3}(\gamma_2)=1$ | $safe_{e_3}(\gamma_2)=1$ |
| $e_4$=*rssoc*<{*DM*,*S_DM*$_1$, *S_DM*$_2$,*S_DM*$_3$,*A_DM*},5> | $C_4$={*smer*<{*DM*,*S_DM*$_1$,*S_DM*$_2$, *S_DM*$_3$,*A_DM*},2>} | $sat_{C_4}(\gamma_1)=0$ | $safe_{e_4}(\gamma_1)=0$ | $sat_{C_4}(\gamma_2)=1$ | $safe_{e_4}(\gamma_2)=1$ |

### 5.3 与现有模型的比较

通过以上对模型的分析，发现 TSSCBDM 具有以下主要优点：(1)受托对象更加可信。TSSCBDM 基于信任资历、信任经验及信任推荐的量化分析，通过综合计算不同待选对象的信任度，从 *e*、*g*、*h* 中淘汰信任度较低的 *h*，选取 *e*、*g* 作为待选可信对象，提高了委托过程的可信度。(2)系统状态依然安全。TSSCBDM 运用间接实施协作分工策略的方法，通过 Smers-Construct 算法构造最小约束集，从待选对象 *e*、*g* 中淘汰不符合系统状态满足性要求的 *e*，选取 *g* 实施委托，保证了系统状态的安全性。(3)算法效率可接受。Smers-Construct 算法中第 1 个 for 循环的时间复杂度为 $O(n)$；第 2 个 for 循环共执行 $\left\lfloor \frac{n-1}{k-1} \right\rfloor$ 次，每次要从 *n* 个角色中任取 *m* 个角色的组合。因此，该算法总的时间复杂度为 $O(2^n)$。在协作分工策略覆盖的角色数较小时，Smers-Construct 算法的效率是可接受的。但模型仍存在以下不足：对于 $k(1<k\leqslant 5)$取不同值情况下的协作分工策略 $e_1$、$e_2$、$e_3$、$e_4$，由定义 17 可知，在 Smers-Construct 算法构造的最小约束集 $C_1$、$C_2$、$C_3$、$C_4$中，$C_1$、$C_4$能准确实施 $e_1$、$e_4$，而 $C_2$、$C_3$ 不能准确实施 $e_1$、$e_4$。因此，算法所构造的最小约束未必都能准确实施协作分工策略，存在局限性。

## 6 结束语

本文提出了一种基于信任度和协作安全策略的委托模型。该模型运用量化计算信任度、间接实施协作分工策略的方法，选取合适的受托对象代替参与协作过程，在保证系统状态安全性的同时，有效地体现了委托过程的可靠性。下一步的研究方向是改进 Smers-Construct 算法，进一步提高实施协作分工策略的准确性。

## 参考文献


[1] Crampton J, Khambhammettu H. Delegation in Role-based Access Control[J]. International Journal of Information Security, 2008, 7(2): 123-136.

[2] Alsulaiman F A, Miege A, Saddik A E. Threshold-based Collaborative Access Control(T-CAC)[C]//Proc. of International Symposium on Collaborative Technologies and Systems. Orlando, USA: IEEE Press, 2007.

[3] 刘 伟, 蔡嘉勇, 贺也平. 协同环境下基于角色的细粒度委托限制框架[J]. 通信学报, 2008, 29(1): 83-91.

[4] 於光灿, 李瑞轩, 卢正鼎, 等. 协作环境中基于场所的访问控制模型[J]. 计算机科学, 2009, 36(1): 81-85.

[5] Wang Qihua, Li Ninghui, Chen Hong. On the Security of Delegation in Access Systems[C]//Proc. of the 13th European Symposium on Research in Computer Security. London, UK: IEEE Press, 2008.

[6] 刘 武, 段海新, 张 洪, 等. TRBAC: 基于信任的访问控制模型[J]. 计算机研究与发展, 2011, 48(8): 1414-1420.

[7] 朱一群. 基于用户信任的动态多级访问控制模型[J]. 计算机工程, 2011, 37(23): 129-131.

[8] 刘 飞, 常朝稳. 基于多维度量和上下文的访问控制模型[J]. 计算机工程, 2011, 37(24): 129-131.

[9] Li Ninghui, Bizri Z, Tripunitara M V. On Mutually-exclusive Roles and Separation of Duty[C]//Proc. of the 11th ACM Conference on Computer and Communication Security. New York, USA: ACM Press, 2004.

[10] 汤 铸, 鞠时光, 陈伟鹤. 空间职责分离约束的实施[J]. 小型微型计算机系统, 2009, 30(12): 2348-2355.


编辑 张 帆