一种RBAC的描述逻辑表示方法

马 丽[1] 马世龙[1] 眭跃飞[2] 伊胜伟[1]
(北京航空航天大学计算机学院 北京 100191)[1]
(中国科学院计算技术研究所智能信息处理国家重点实验室 北京 100190)[2]

摘 要 基于角色的访问控制(RBAC)通过角色来控制用户对资源的访问,极大地简化了安全管理。虽然对RBAC的研究比较成熟,但由于RBAC目前缺乏形式化的表示,使得RBAC中的一些概念和性质存在不同的理解。描述逻辑(DL)是一种基于对象的知识表示的形式化系统,它是一阶逻辑的一个可判定的子集,具有合适定义的语义,并且具有很强的表示能力。为了给出RBAC的形式化方法,以描述逻辑为工具,RBAC96模型为基础,提出了RBAC的描述逻辑DL_{RBAC}。用描述逻辑的符号给出了RBAC中主要的元素和关系的形式化定义,并证明了这种描述逻辑表示对于RBAC模型的忠实性。所提出的RBAC形式化模型可以作为进一步研究RBAC的理论基础。

关键词 访问控制,角色,权限,描述逻辑,角色继承
中图法分类号 TP309 **文献标识码** A

Representation for RBAC Model in Description Logic

MA Li[1] MA Shi-long[1] SUI Yue-fei[2] YI Sheng-wei[1]
(Department of Computer Science, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)[1]
(Key Laboratory of Intelligent Information Processing Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China)[2]

Abstract Role-Based Access Control (RBAC) controls the user's access to resources by indirectly using roles, which simplifies the security management greatly. Although the research of RBAC model is a mature area, the lack of formalization of RBAC results in uncertainty and confusion about the concepts and meaning of RBAC. Description Logic (DL) is a kind of object-based knowledge representation formalism, and also a decidable fragment of first-order predicate logic, with well-defined semantics and powerful representation capability. To give a formal description of RBAC, this paper took RBAC96 as a reference model and proposed a new formalized method to RBAC with description logic, called DL_{RBAC}, which gives formal definitions to the concepts and relations of RBAC. This paper also proved that the formal representation is faithful to RBAC model. Based on the formalized model, we can further study RBAC.

Keywords Access control, Role, Permission, Description logic, Role inheritance

基于角色的访问控制(Role-Based Access Control, RBAC)[1-3]通过角色控制用户对资源的访问,从而简化安全管理。RBAC还可以支持多种安全策略,如自主型(DAC)和强制型访问控制(MAC)[4]。尽管现有的RBAC模型,如RBAC96[1],NIST RBAC模型[2](及后来的ANSI RBAC标准[3])等都对RBAC进行了系统的分析和描述,但由于缺乏对RBAC形式化的表示,使得RBAC中的一些概念和性质描述存在很多争议[5,6]。例如RBAC中角色层次是对组织机构权力分配的一种自然的模型,RBAC96模型、NIST RBAC模型和ANSI RBAC标准都把角色层次看成是一种偏序关系,但角色层次的含义却没有统一。在RBAC96模型中角色继承与会话有关,所以角色继承可以解释为激活继承和权限继承。NIST RBAC模型[2]和ANSI RBAC标准[3]把角色层次看成是用户继承和权限继承,而Li等认为角色继承应该是激活继承、用户继承和权限继承三者的有机结合[5]。由于这些模型对角色继承都没有给出形式化的定义,所有的继承关系都是隐含表示的,因此在讨论继承的含义时没有统一的解释,只有在形式化表示的基础上讨论这些问题才有意义。并且,对RBAC进行形式化的分析有助于验证RBAC的说明是否能够满足系统的安全需求,还可以比较不同的访问控制模型和预测不同安全策略下的系统行为[7]。

描述逻辑(Description Logic, DL)[8]是一种基于对象的知识表示的形式化系统,它是一阶逻辑的一个可判定的子集,具有合适定义的语义,并且具有很强的表示能力。为了给出一种RBAC的形式化表示方法,本文以描述逻辑为理论基础,以RBAC96模型为参考模型,提出了一种基于描述逻辑

到稿日期:2009-04-09 返修日期:2009-06-16 本文受国家自然科学基金(60273019,60496326,60573063和60573064)和国家重点基础研究发展规划(973)(No. 2005CB321902)资助。

马 丽(1974—),女,博士生,主要研究方向为信息安全、服务计算,E-mail:mali@nlsde.buaa.edu.cn;马世龙(1953—),男,博士生导师,主要研究方向为信息安全、服务计算、网格;眭跃飞(1963—),男,研究员,主要研究方向为本体、服务计算、信息安全;伊胜伟(1977—),男,博士生,主要研究方向为信息安全、集群计算。

的 RBAC 形式化方法。

1 描述逻辑介绍

描述逻辑(Description Logics,DLs)是一类通过定义一个应用领域(世界)的相关概念(concepts),即领域的术语,并用这些概念说明领域中对象(objects)和个体(individuals)的性质(properties),即世界的描述,来表示该领域知识的知识表示形式化语言。它是一阶谓词逻辑的一个可判定子集。但与一阶逻辑不同的是,描述逻辑系统能提供可判定的推理服务。描述逻辑的重要特征是它具有很强的表达能力和可判定性,它保证推理算法总能停止,并返回正确的结果。本节接下来简单介绍基本描述逻辑的语法和语义。

基本的描述逻辑语言 ALC[8]包含如下基本符号:个体常元 $a_0,a_1,\cdots$;原子概念名 $A_0,A_1,\cdots$;概念名 $C_0,C_1,\cdots$;角色 $r_0,r_1,\cdots$;顶概念$\top$,底概念$\bot$;概念构造子$\neg,\sqcap,\sqcup,\exists$;断言算子$\sqsubseteq$;逻辑连接词:$\rightarrow,\neg$。

定义 1 概念 C 定义如下:

$C::=A\mid\top\mid\bot\mid\neg C\mid C_1\sqcap C_2\mid\exists R.C$

定义 2 断言 φ 定义如下:

$\varphi::=C(a)\mid R(a,b)\mid C_1\sqsubseteq C_2\mid\neg\varphi\mid\varphi_1\rightarrow\varphi_2$

其中,C 为概念,R 为角色,a,b 为个体常元。

定义 3 在一定领域中,一个知识库 $KB=(TBox,ABox)$由两个部分组成。其中 $TBox$ 是一个关于包含断言的有限集合,亦称为术语公理的集合;$ABox$ 是概念断言和角色断言的有限集合。

ALC 语义将概念解释为一个非空的论域的子集,角色是该论域上的二元关系。形式上,一个解释 $I=(\Delta^I,\cdot^I)$由一个非空集合 Δ^I 和一个解释函数 $\cdot^I$ 组成,使得对每个原子概念 A,都有 $A^I\subseteq\Delta^I$,对每个原子角色 r,都有 $r^I\subseteq\Delta^I\times\Delta^I$。

解释函数通过如下归纳定义扩展概念描述:

- $\top^I=\Delta^I;\bot^I=\emptyset$;
- $(\neg C)^I=I-C^I$;
- $(C\sqcap D)^I=C^I\cap D^I;(C\sqcup D)^I=C^I\cup D^I$;
- $(\forall r.C)^I=\{x\in\Delta^I\mid\forall y.(x,y)\in r^I\rightarrow y\in C^I\}$;
- $(\exists r.C)^I=\{x\in\Delta^I\mid\exists y.(x,y)\in r^I\wedge y\in C^I\}$。

定义 4 在解释 I 下,一个断言 φ 解释为真,记为 $I\models\varphi$,如果

- $C^I\subseteq D^I$,如果 $\varphi=C\sqsubseteq D$;
- $a^I\in C^I$,如果 $\varphi=C(a)$;
- $(a^I,b^I)\in r^I$,如果 $\varphi=r(a,b)$;
- $I\not\models\neg\psi$,如果 $\varphi=\neg\psi$,其中 ψ 为断言;
- $I\models\psi_1$ 蕴涵 $I\models\psi_2$,如果 $\varphi=\psi_1\rightarrow\psi_2$,其中 ψ_1 和 ψ_2 为断言。

解释 I 是知识库 KB 的模型,记为 $I\models KB$。如果 I 是 KB 中每个包含断言和实例断言的模型,则有 1) 若 KB 有模型,则称 KB 是可满足的;2) 若断言 φ 对于 KB 的每个模型都是可满足的,则称 KB 逻辑蕴含 φ,记为 $KB\models\varphi$;3) 对概念 C,若 KB 有一个模型 I 使得 $C^I\neq\emptyset$,则称 C 是可满足的。

本文将在 ALC 及其扩展的语言[9]基础上提出 RBAC 的描述逻辑。

2 RBAC 模型

定义 5 一个 RBAC 模型,S 为 11 元组,$S=(U,R,P,S,UA,PA,RH,user,roles,permissions,Constraints)$。其中,

(1)U,R,P 和 S 分别为用户、角色、权限和会话的集合;

(2) $UA\subseteq U\times R$,用户-角色分配关系;

(3) $PA\subseteq P\times R$,权限到角色的分配关系;

(4) $RH\subseteq R\times R$,角色层次的偏序关系(也可以用$\geqslant$表示);

(5) *user*,*roles* 和 *permissions* 为函数,其中

(5.1) $user:S\rightarrow U$ 将每个会话 s 映射为一个用户(在会话的生命周期中不会改变);

(5.2) $roles:S\rightarrow 2^R$ 将每个会话 s 映射到集合 $roles(s)\subseteq\{r:\exists r'\geqslant r((user(s),r')\in UA)\}$ (会随时间变化);

(5.3) 每个会话 s 都有权限 $permissions(s)$[1] $=\bigcup_{r\in roles(s)}\{p:\exists r''\leqslant r((p,r'')\in PA)\}$;

(6) *Constraints* 为约束的集合。

注:1) 本文只考虑互斥角色关系,用 *mutuallyexclusive* 表示;2) 这里的 RBAC 模型简化了 RBAC96 模型,不包含管理组件。

为了和下面的描述逻辑模型区别开,本文接下来用 RBAC 状态来对应 RBAC 模型。

3 RBAC 的描述逻辑表示

为了描述 RBAC,我们提出 RBAC 的描述逻辑 DL_{RBAC}。令 L 为描述逻辑 DL_{RBAC} 的语言,包含如下符号:

- 顶概念和底概念:$\top,\bot$;
- 原子概念名:U,R,P,S;
- 原子角色名:$PA,UA,RH,roles,user,permissions,mutuallyexclusive$;
- 概念构造子:$\neg,\sqcap,\forall$;
- 角色构造子:$^-,\circ,\sim$。

其中,$^-,\sim$为一元构造子,分别表示角色的逆和否;$\circ$为二元构造子,表示角色的复合。

给定一个 RBAC 状态,我们可以扩充语言 L 使得 L 包含如下符号:

(1)对每个 $u\in U$,存在常量符号 $u\in L$;

(2)每个 $r\in R$,存在常量符号 $r\in L$;

(3)对每个 $p\in P$,存在常量符号 $p\in L$;

(4)对每个 $s\in S$,存在常量符号 $s\in L$。

本文接下来用 M 表示 DL_{RBAC} 模型,KB 表示 DL_{RBAC} 的知识库。

3.1 DL_{RBAC} 语法

定义 6 在知识库 KB 中,概念 C 定义如下:

$C::=U\mid R\mid S\mid P\mid\neg C\mid C\sqcap D\mid\forall R.C\mid\exists R.C$

其中角色 R 定义如下:

$R::=RH\mid UA\mid PA\mid user\mid roles\mid permissions\mid mutuallyexclusive\mid R^-\mid\sim R\mid R\circ R'$

定义 7 KB 中的断言 φ 定义如下:

$\varphi::=U(u)\mid R(r)\mid P(p)\mid S(s)\mid UA(u,r)\mid PA(p,r)\mid user$

[1] 在 RBAC96 模型中没有函数 *permissions*,本文为了表示权限和会话之间的关系,将这种关系用 *permissions* 表示。

$(s,u)\mid roles(s,r)\mid permissions(s,p)\mid RH(r',r)\mid mutuallyexclusive(r'',r)$

$\mid \exists PA.R\sqsubseteq P$(公理 1)$\mid \exists PA^{-}.P\sqsubseteq R$(公理 1′)

$\mid \exists UA.R\sqsubseteq U$(公理 2)$\mid \exists UA^{-}.U\sqsubseteq R$(公理 2′)

$\mid (=1)user.U\sqsubseteq S$(公理 3)$\mid \exists user^{-}.S\sqsubseteq U$(公理 3′)

$\mid \exists roles.R\sqsubseteq S$(公理 4)$\mid \exists roles^{-}.S\sqsubseteq R$(公理 4′)

$\mid \exists permissions.P\sqsubseteq S$(公理 5)$\mid \exists permissions^{-}.S\sqsubseteq P$(公理 5′)

$\mid \exists RH.R\sqsubseteq R$(公理 6)$\mid \exists RH^{-}.R\sqsubseteq R$(公理 6′)

$\mid \exists RH.\top\equiv \exists RH.R$(公理 7)

$\mid \exists RH.(\exists RH.R)\sqsubseteq \forall\exists RH.R$(公理 8)

$\mid \exists RH.(\exists UA^{-}.U)\sqsubseteq \exists UA^{-}.U$(公理 9)

$\mid \exists roles^{-}.S\sqsubseteq \exists RH.(\exists UA^{-}.(\exists user^{-}.S))$(公理 10)

$\mid roles\sqsubseteq(\sim(user\circ\sim UA))\circ RH^{-}$(公理 11)

$\mid \exists RH^{-}.(\exists PA^{-}.P)\sqsubseteq \exists PA^{-}.P$(公理 12)

$\mid permissions\sqsubseteq\sim(roles\circ\sim(RH^{-}\circ PA^{-}))$(公理 13)

$\mid \exists mutuallyexclusive.R\sqsubseteq R$(公理 14)$\mid \exists mutuallyexclusive^{-}.R\sqsubseteq R$(公理 14′)

$\mid \exists UA^{-}.u\sqcap\exists mutuallyexclusive.(\exists UA^{-}.u)\equiv\bot$(公理 15)

$\mid \exists roles^{-}.s\sqcap\exists mutuallyexclusive.(\exists roles^{-}.s)\equiv\bot$(公理 16)

$\mid\neg\varphi\mid\varphi_1\rightarrow\varphi_2$。

注:1)公理 11 是对 RBAC 状态 S 的条件 5.2 的形式表示;2)公理 13 是对条件 5.3 的形式表示。

定义 8 DL_{RBAC}的知识库 $KB=(TBox,ABox)$,其中:

(1)$TBox$ 包含了公理 1—公理 16;

(2). $ABox=\{U(u):u\in U\}\cup\{R(r):r\in R\}\cup\{P(p):p\in P\}\cup\{S(s).s\in S\}\cup\{UA(u,r):(u,r)\in UA\}\cup\{PA(p,r):(p,r)\in PA\}\cup\{user(s,u):u\in user(s)\}\cup\{roles(s,r):r\in roles(s)\}\cup\{permissions(s,p):p\in permissions(s)\}\cup\{RH(r',r):\exists r'\leqslant r\}\cup\{mutuallyexclusive(r',r):\exists(r',r)\in mutuallyexclusive\}$。

3.2 DL_{RBAC}语义

定义 9 DL_{RBAC}的模型 M 为序对(Δ,I),满足:

(1) Δ 为非空集合;且

(2) I 为解释,使得对原子概念 A,$I(A)\subseteq\Delta$;对原子角色 P,$I(P)\subseteq\Delta\times\Delta$,且 I 满足如下的条件:

1) 对任意的原子概念 A_1 且 A_2,$A_1\neq A_2$ iff $I(A_1)\cap I(A_2)=\emptyset$;

2) 对角色,I 满足如下条件:

$\mathrm{dom}(I(UA))=I(U)$,$\mathrm{range}(I(UA))=I(R)$;

$\mathrm{dom}(I(PA))=I(P)$,$\mathrm{range}(I(PA))=I(R)$;

$\mathrm{dom}(I(RH))=I(R)$,$\mathrm{range}(I(RH))=I(R)$;

$\mathrm{dom}(I(mutuallyexclusive))=I(R)$,$\mathrm{range}(I(mutuallyexclusive))=I(R)$;

3) $I(user)$,$I(roles)$,$I(permissions)$为函数,满足如下条件:

$\mathrm{dom}(I(user))=I(S)$,$\mathrm{range}(I(user))=I(U)$;

$\mathrm{dom}(I(roles))=I(S)$,$\mathrm{range}(I(roles))=I(R)$;

$\mathrm{dom}(I(permissions))=I(S)$,$\mathrm{range}(I(permissions))=I(P)$;

4) 对角色构造子的解释 I 可以定义为:对任意 R_1 和 R_2,有

$I(\sim R_1)=(\Delta\times\Delta)-I(R_1)=\Delta^2-I(R_1)$;

$I(R_1\circ R_2)=\{(x,y)\in\Delta^2:\exists z((x,z)\in R_1\ \&\ (z,y)\in R_2)\}$。

定义 10 概念 C 的解释 C^I 定义如下:

1) $C^I=A^I$,如果 $C=A$ (A 为原子概念);

2) $C^I=\Delta-D^I$,如果 $C=\neg D$;

3) $C^I=D_1^I\cap D_2^I$,如果 $C=D_1\sqcap D_2$;

4) $C^I=\{x\in\Delta:\forall y((x,y)\in R^I\rightarrow y\in D^I)\}$,如果 $C=\forall R.D$。

定义 11 断言 φ 在 M 中是可满足的,记为 $M\models\varphi$,如果

1) $C^I\subseteq D^I$,如果 $\varphi=C\sqsubseteq D$;

2) $M\not\models\psi$,如果 $\varphi=\neg\varphi$;

3) $M\models\psi\Rightarrow M\models\theta$,如果 $\varphi=\psi\rightarrow\theta$。

命题 1 在模型 M 中公理 1—公理 16 都是可满足的。

证明:(1)对公理 1:若要证 $M\models\exists PA.R\sqsubseteq P$ 即证 $I(\exists PA.R)\subseteq I(P)$。由 $x\in I(\exists PA.R)$,可得 $\exists y\in I(R)\wedge(x,y)\in I(PA)$,又根据 $I(PA)\subseteq I(P)\times I(R)$,可知 $x\in I(P)$,所以 $I(\exists PA.R)\subseteq I(P)$成立,即 $M\models\exists PA.R\sqsubseteq P$;

若要证 $M\models\exists PA^{-}.P\sqsubseteq R$,即证 $I(\exists PA^{-}.P)\subseteq I(R)$。由 $x\in I(\exists PA^{-}.P)$可得 $\exists y\in I(P)\wedge(x,y)\in I(PA^{-})$,根据 PA 和 PA^{-}的关系可知 $I(PA^{-})\subseteq I(R)\times I(P)$,也就是说 $x\in I(R)$,即 $I(\exists PA^{-}.P)\subseteq I(R)$成立,即 $M\models\exists PA^{-}.P\sqsubseteq R$。

同理可证公理 2—公理 5 在 M 中是可满足的。

(4) 对公理 6:$\exists RH.R\sqsubseteq R$,公理 6′ $\exists RH^{-}.R\sqsubseteq R$ 和公理 7:$\exists RH.\top\equiv\exists RH.R$:

1)若要证 $M_1\models\exists RH.R\sqsubseteq R$ 即证 $I(\exists RH.R)\subseteq I(R)$。由 $x\in I(\exists RH.R)$,可得 $\exists y\in I(R)\wedge(x,y)\in I(RH)$,又根据 $I(RH)\subseteq I(R)\times I(R)$,可知 $x\in I(R)$,所以 $I(\exists RH.R)\subseteq I(R)$成立,即 $M_1\models\exists RH.R\sqsubseteq R$;

2) 对公理 6′:若要证 $M_1\models\exists RH^{-}.R\sqsubseteq R$,即证 $I(\exists RH^{-}.R)\subseteq I(R)$。由 $x\in I(\exists RH^{-}.R)$可得 $\exists y\in I(R)\wedge(x,y)\in I(RH^{-})$,根据 RH 和 RH^{-}的关系可知 $I(RH^{-})\subseteq I(R)\times I(R)$,也就是说 $x\in I(R)$,即 $I(\exists RH^{-}.R)\subseteq I(R)$成立,即 $M\models\exists RH^{-}.R\sqsubseteq R$。

3) 对公理 7:若证 $M\models(\exists RH.\top\equiv\exists RH.R)$,即证 $I(\exists RH.\top)=I(\exists RH.R)$。

$x\in I(\exists RH.\top)$ iff $\exists y(x,y)\in I(RH)$,这里 $y\in\Delta^I$,显然 y 可以$\in I(R)$,即 $x\in(\exists RH.R)$,即有 $M_1\models(\exists RH.\top\sqsubseteq\exists RH.R)$。另要证 $M_1\models(\exists RH.R\sqsubseteq\exists RH.\top)$,即证 $M_1\models(\exists RH.R\sqcap\neg(\exists RH.\top)\sqsubseteq\bot)$。

$x\in I(\exists RH.R\sqcap\neg(\exists RH.\top))$ iff $x\in I(\exists RH.R)\wedge x\in I(\neg(\exists RH.\top))$

iff $\exists y\in I(R)\wedge(x,y)\in I(RH)\wedge x\in I(\forall RH.\bot)$

iff $\exists y\in I(R)\wedge(x,y)\in I(RH)\wedge\forall y\in\emptyset\wedge(x,y)\in I(RH)$

显然,$x\in\emptyset$,这样 $M_1\models(\exists RH.R\sqsubseteq\exists RH.\top)$,由此可证 $M_1\models(\exists RH.\top\equiv\exists RH.R)$。证毕。

(5)对公理 8:$\exists RH.(\exists RH.R)\sqsubseteq\exists RH.R$:

在模型 M 中有 $RH=I(RH)$,$R=I(R)$,则:$r\in I(RH.$

$(\exists RH.R))$ iff $r\in\{r\mid\exists r'((r,r')\in RH\ \&\ r'\in I(\exists RH.R))\}$

iff $r\in\{r\mid\exists r'((r,r')\in RH\ \&(\exists r''((r,r'')\in RH\ \&\ r''\in R)))\}$

iff $r\in\{r\mid\exists r'\ \exists r''((r,r')\in RH\ \&\ (r',r'')\in RH\ \&\ r''\in R)\}$

显然$\{r\mid\exists r'\ \exists r''((r,r')\in RH\ \&\ (r',r'')\in RH\ \&\ r''\in R)\}\subseteq\{r\mid\exists r'(r,r')\in RH\ \&\ r'\in R\}$，也就是说在模型$M$中，$I(\exists RH.(\exists RH.R))\subseteq I(\exists RH.R)$，即$M\models\exists RH.(\exists RH.R)\sqsubseteq\exists RH.R$。

注：公理8也称为RH的传递性，也可以直接用角色的复合形式表示：$RH\circ RH\sqsubseteq RH$。

(6) 对公理9：$\exists RH.(\exists UA^{-}.U)\sqsubseteq\exists UA^{-}.U$

在模型M中，有$UA=I(UA)$，$U=I(U)$，$RH=I(RH)$。

$r\in(\exists RH.(\exists UA^{-}.U))^{I}$ iff $r\in\{r\mid\exists r'((r,r')\in RH\ \&\ r'\in(\exists UA^{-}.U)^{I})\}$

iff $r\in\{r\mid\exists r'((r,r')\in RH\ \&\ (\exists u((r',u)\in I(UA^{-})\ \&\ u\in U)))\}$

iff $r\in\{r\mid\exists r'\ \exists u((r,r')\in RH\ \&\ (u,r')\in UA\ \&\ u\in U)\}$

显然$\{r\mid\exists r'\ \exists u((r,r')\in RH\ \&\ (u,r')\in UA\ \&\ u\in U)\}\subseteq\{r\mid\exists u((r,u)\in I(UA^{-})\ \&\ u\in(U)\}$，由此可知$r\in\{r\mid\exists u((r,u)\in I(UA^{-})\ \&\ u\in U)\}$，所以有$I(\exists RH.(\exists UA^{-}.U))\subseteq I(\exists UA^{-}.U)$，即$M\models\exists(RH.(\exists UA^{-}.U)\sqsubseteq\exists UA^{-}.U$。

注：公理9也称为UA-继承性，可以表示为$UA\circ RH\sqsubseteq UA$。

(7)对公理10：$\exists roles^{-}.S\sqsubseteq\exists RH.(\exists UA^{-}.(\exists user^{-}.S))$

在M中，$UA=I(UA)$，$U=I(U)$，$RH=I(RH)$，$user=I(user)$，$S=I(S)$，$roles=I(roles)$。

$r\in I(\exists roles^{-}.S)$ iff $r\in\{r\mid\exists s((r,s)\in I(roles^{-})\ \&\ s\in S)\}$

iff $r\in\{r\mid\exists s((s,r)\in roles\ \&\ s\in S)\}$

根据$roles(s)\subseteq\{r\mid\exists r'\geqslant r((user(s),r')\in UA)\}$，则由$r\in\{r\mid\exists s((s,r)\in roles\ \&\ s\in S)\}$，可知

$r\{r\mid\exists r'\geqslant r((user(s),r')\in UA)\}$ iff $r\in\{r\mid\exists r'\ \exists u\ \exists s((r,r')\in RH\ \&\ (u,r')\in UA\ \&\ (s,u)\in user\ \&\ s\in S)\}$

iff $r\in\{\exists r'((r,r')\in RH\ \&\ (\exists u((u,r')\in UA\ \&\ \exists s((u,s)\in I(user^{-})\ \&\ s(S))))\}$

iff $r\in\{\exists r'((r,r')\in RH\ \&\ (\exists u(r',u)\in I(UA^{-})\ \&\ u\in(\exists user^{-}.S)))\}$

iff $r\in\{\exists r'((r,r'\in RH\ \&\ r'\in I(\exists UA^{-}.(\exists user^{-}.S)))\}$

iff $r\in I(\exists RH.(\exists UA^{-}.(\exists user^{-}.S)))$

这样，可证$M_1\models\exists roles^{-}.S\sqsubseteq\exists RH.(\exists UA^{-}.(\exists user^{-}.S))$。

(8)对公理11：$roles\subseteq(\sim(user^{\circ}\sim UA))^{\circ}RH^{-}$：

证明：对任意$s\in S$和$r\in R$，

$(s,r)\in roles$ iff $\exists r'\geqslant r((user(s),r')\in UA)$

iff $\exists r'((r',r)\in RH\ \&\ (user(s),r')\in UA)$

iff $\exists r'((r',r)\in RH\ \&\ \forall u(u\in user(s)\rightarrow(u,r')\in UA))$

iff $\exists r'((r',r)\in RH\ \&\ (s,r')\in I(\sim(user^{\circ}\sim UA)))$

iff $(s,r)\in I((\sim(user^{\circ}\sim UA))^{\circ}RH^{-})$

(9)对公理12：$\exists RH^{-}.(\exists PA^{-}.P)\sqsubseteq\exists PA^{-}.P$

在M中$RH=I(RH)$，$PA=I(PA)$，$P=I(P)$，则

$r\in I(\exists RH^{-}.(\exists PA^{-}.P))$

iff $r\in\{r\mid\exists r'((r',r)\in RH\ \&\ r'\in I(\exists PA^{-}.P))\}$

iff $r\in\{r\mid\exists r'((r',r)\in RH\ \&\ \exists p((p,r')\in PA\ \&\ p\in P))\}$

iff $r\in\{r\mid\exists r'\ \exists p((r',r)\in RH\&(p,r')\in PA\ \&\ p\in P)\}$

显然$r\in\{r\mid\exists p((p,r)\in PA\ \&\ p\in P)\}$，这样$I(\exists RH^{-}.(\exists PA^{-}.P))\subseteq I(\exists PA^{-}.P)$，即$\exists RH^{-}.(\exists PA^{-}.P)\sqsubseteq\exists PA^{-}.P$在$M_1$中是可满足的。

注：公理12表示了PA-继承性. PA-继承性是指低角色的权限可以被高角色的权限包含。

(10)对公理13：$permissions\subseteq\sim(roles^{\circ}\sim(RH^{-}\circ PA^{-}))$

证明：对任意$s\in S$和$p\in P$，条件表明

$permissions(s,p)$ iff $\forall r\in roles(s)\ \exists r'\leqslant r((p,r')\in PA)$

iff $\forall r((s,r)\in roles^{I}\rightarrow\exists r'(r,r')\in RH\ \&\ (p,r')\in PA)$

iff $\forall r((s,r)\in roles^{I}\rightarrow\exists r'(r',r)\in I(RH^{-})\ \&\ (r',p)\in I(PA^{-}))$

iff $\forall r((s,r)\in roles^{I}\rightarrow(r,p)\in I(RH^{-}\circ PA^{-}))$

iff $(s,p)\in I(\sim(roles^{\circ}\sim(RH^{-}\circ PA^{-})))$

注：公理13也称为权限激活公理，反映了权限与激活的角色之间的对应关系。

(11)对公理14：$\exists mutuallyexclusive.R\sqsubseteq R$ 和公理14′：$\exists mutuallyexclusive^{-}.R\sqsubseteq R$，公理15：$\exists UA^{-}.u\sqcap\exists mutuallyexclusive.(\exists UA^{-}.u)\equiv\perp$，公理16：$\exists roles^{-}.s\sqcap\exists mutuallyexclusive.(\exists roles^{-}.s)\equiv\perp$。

1)若要证$M\models(mutuallyexclusive.R\sqsubseteq R$即证$I(\exists mutuallyexclusive.R)\subseteq I(R)$。由$x\in I(\exists mutuallyexclusive.R)$，可得$\exists y\in I(R)\wedge(x,y)\in I(mutuallyexclusive)$，又根据$I(mutuallyexclusive)\subseteq I(R)\times I(R)$，可知$x\in I(R)$，所以$I(\exists mutuallyexclusive.R)\subseteq I(R)$成立，即$M\models(mutuallyexclusive.R\sqsubseteq R$；

同理可证2) $M\models\exists mutuallyexclusive^{-}.R\sqsubseteq R$。

3) 若要证明$M\models\exists UA^{-}.u\sqcap\exists mutuallyexclusive.(\exists UA^{-}.u)\equiv\perp$，即要证$I(\exists UA^{-}.u\sqcap\exists mutuallyexclusive.(\exists UA^{-}.u))=\emptyset$，假设$I(\exists UA^{-}.u\sqcap\exists mutuallyexclusive.(\exists UA^{-}.u))\neq\emptyset$，则$\exists x\in\Delta$，使得$x\in I(\exists UA^{-}.u\sqcap\exists mutuallyexclusive.(\exists UA^{-}.u))$，即$x\in I(\exists UA^{-}.u)$且$x\in I\exists(mutuallyexclusive.(\exists UA^{-}.u))$：

·对$x\in I(\exists UA^{-}.u)$，可知对$u=I(u)$，$(u,x)\in I(UA)$；

·对$x\in I(\exists mutuallyexclusive.(\exists UA^{-}.u))$，可知$\exists y\in I(\exists UA^{-}.u)$，即$(u,y)\in I(UA)$，使得$(x,y)\in I(mutuallyexclusive)$。

显然根据M的定义，对u，如果$(u,x)\in I(UA)$，则$(u,y)\notin I(UA)$，显然$(u,y)\in I(UA)$与之矛盾，所以$I(\exists UA^{-}.u\sqcap$

$\exists mutuallyexclusive.(\exists UA^{-}.u))=\emptyset$，即证 $M\models \exists UA^{-}.u\sqcap \exists(mutuallyexclusive.(\exists UA^{-}.u)\equiv\perp$；

4) 若要证明 $M\models \exists roles^{-}.s\sqcap\exists mutuallyexclusive.\exists(roles^{-}.s)\equiv\perp$，即证 $I(\exists roles^{-}.s\sqcap\exists mutuallyexclusive.(\exists roles^{-}.s))=\emptyset$，假设 $I(\exists roles^{-}.s\sqcap\exists mutuallyexclusive.(\exists roles^{-}.s))\neq\emptyset$，即 $\exists x\in\Delta$，使得 $x\in I((roles^{-}.s)$ 且 $x\in I(\exists mutuallyexclusive.(\exists roles^{-}.s))$：

· 对 $x\in I(\exists roles^{-}.s)$，可知对 $s=I(s)$，$(user(s),x)\in I(roles)$；

· 对 $x\in I(\exists mutuallyexclusive.(\exists roles^{-}.s))$，可知 $\exists y\in I(\exists roles^{-}.s)$，即 $(user(s),y)\in I(roles)$，使得 $(x,y)\in I(mutuallyexclusive)$。

显然根据 M 的定义，对任意 s，如果 $(user(s),x)\in I(roles)$，则 $(user(s),y)\notin I(roles)$，显然 $(user(s),y)\in I(roles)$ 与之矛盾，所以 $I(\exists roles^{-}.s\sqcap\exists mutuallyexclusive.(\exists roles^{-}.s))=\emptyset$，即证 $M\models\exists roles^{-}.s\sqcap\exists mutuallyexclusive.(\exists roles^{-}.s)\equiv\perp$。证毕。

3.3 S,M 和 KB 之间的关系

为了说明用描述逻辑表示 RBAC 的模型与一个 RBAC 状态之间的关系，本节提出两种转换 σ 和 τ，其中 σ 表示 RBAC 的描述逻辑模型到 RBAC 状态的转换，用 τ 表示 RBAC 状态到 RBAC 的描述逻辑模型的转换。

RBAC 状态 S 可以用断言 ψ 表示元素之间以及元素与集合之间的关系及约束：

$\psi::=\theta|\delta$

其中，

1) $\theta::=u\in U|s\in S|r\in R|p\in P|(u,r)\in UA|(p,r)\in PA|(r',r)\in mutuallyexclusive|(r'',r)\in RH|user(s,u)|permissions(s,p)|roles(s,r)|\neg\theta|\theta_1\rightarrow\theta_2$；

2) $\delta::=roles(s)\subseteq\{r:\exists r'\geqslant r((user(s),r')\in UA)\}|permissions(s)=\{p:\forall r\in roles(s)\ \exists r'\leqslant r((p,r')\in PA)\}$。

定义 12 如果断言 ψ 在 S 中为真，则称 ψ 是可满足的，记为 $S\models\psi$。

这样，我们可以把 M,S 和 KB 之间的关系表示出来。这里把 S 到 KB 的转换称为 σ，将每个 M 到 RBAC 的状态 S 称为 τ，变化过程如图 1 所示。

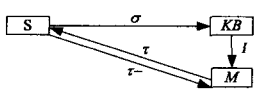

图 1 S,KB 和 M 之间的转换关系

其中，σ 将 S 中的每个符号和断言转换为 KB 中的符号和断言，τ 将 M 中的每个关系转换为 S 中的关系，τ^{-} 为 τ 的逆转换，则 σ,τ 和 τ^{-} 分别定义如下：

(a) 令 S 为 RBAC 的状态，$S=(U,R,S,P,UA,PA,RH,user,roles,permissions,mutuallyexclusive)$，存在一个描述逻辑语言 L，使得：

1) 对 S 中的每个符号，有

· $\sigma(u)=u$ 对每个 $u\in U$ 且 $u\in L$；

· $\sigma(r)=r$ 对每个 $r\in R$ 且 $r\in L$；

· $\sigma(s)=s$ 对每个 $s\in S$ 且 sL；

· $\sigma(U)=U$；

· $\sigma(R)=R$；

· $\sigma(P)=P$；

· $\sigma(UA)=UA$；

· $\sigma(PA)=PA$；

· $\sigma(RH)=RH$；

· $\sigma(user)=user$；

· $\sigma(roles)=roles$；

· $\sigma(permissions)=permissions$；

· $\sigma(mutuallyexclusive)=mutuallyexclusive$。

2)对断言 θ，如果满足 $S\models\theta$，则有：

· 如果 $\theta=(u\in U)$，则 $\sigma(u\in U)=U(u)$；

· 如果 $\theta=(s\in S)$，则 $\sigma(s\in S)=S(s)$；

· 如果 $\theta=(r\in R)$，则 $\sigma(r\in R)=R(r)$；

· 如果 $\theta=(p\in P)$，则 $\sigma(p\in P)=P(p)$；

· 如果 $\theta=((u,r)\in UA)$，则 $\sigma((u,r)\in UA)=UA(u,r)$；

· 如果 $\theta=((p,r)\in PA)$，则 $\sigma((p,r)\in PA)=PA(p,r)$；

· 如果 $\theta=((r',r)\in RH)$，则 $\sigma((r',r)\in RH)=RH(r',r)$；

· 如果 $\theta=(r\in roles(s))$，则 $\sigma(r\in roles(s))=roles(s,r)$；

· 如果 $\theta=(u\in user(s))$，则 $\sigma(u\in user(s))=user(s,u)$；

· 如果 $\theta=(p\in permissions(s))$，则 $\sigma(p\in permissions(s))=permissions(s,p)$；

· 如果 $\theta=((r',r)\in mutuallyexclusive)$，则 $\sigma((r',r)\in mutuallyexclusive)=mutuallyexclusive(r',r)$；

· 如果 $\theta=\neg\theta_1$，则 $\sigma(\neg\theta_1)=\neg\sigma(\theta_1)$；

· 如果 $\theta=\theta_1\rightarrow\theta_2$，则 $\sigma(\theta_1\rightarrow\theta_2)=\sigma(\theta_1)\rightarrow\sigma(\theta_2)$。

3)对约束断言 δ，

· 如果 $\delta=(roles(s)\subseteq\{r:\exists r'\geqslant r((user(s),r')\in UA)\})$，则根据命题 1 定义 $\sigma(roles(s)\subseteq\{r:\exists r'\geqslant r((user(s),r')\in UA)\})=roles\subseteq(\sim(user\circ\sim UA))\circ RH^{-}$；

· 如果 $\delta=(permissions(s)=\{p:\forall r\in roles(s)\ \exists r'\leqslant r((p,r')\in PA)\})$，根据命题 1 定义 $\sigma(permissions(s)=\{p:\forall r\in roles(s)\ \exists r'\leqslant r((p,r')\in PA)\})=permissions\subseteq\sim(roles\circ\sim(RH^{-}\circ PA^{-}))$

(b) 给定模型 M，我们可以定义 RBAC 的状态 S 为 $\tau(M)$，其中 τ 为 M 到 S 的转换，使得

· $\tau(I(u))=u$ 对每个 $u\in L$；

· $\tau(I(r))=r$ 对每个 $r\in L$；

· $\tau(I(p))=p$ 对每个 $p\in L$；

· $\tau(I(s))=s$ 对每个 $s\in L$；

· $\tau(I(U))=U$；

· $\tau(I(R))=R$；

· $\tau(I(P))=P$；

· $\tau(I(S))=S$；

· $\tau(I(UA))=UA$；

· $\tau(I(PA))=PA$；

· $\tau(I(user))=user$；

· $\tau(I(roles))=roles$；

· $\tau(I(permissions))=permissions$；

且对 S 中的任意元素 α 和 β，τ 还满足如下的关系：

· 如果 $\alpha\in\beta$，$\tau(\alpha\in\beta)=\tau(\alpha)\in\tau(\beta)$；

· 对任意 $\alpha\subseteq\beta$，$\tau(\alpha\subseteq\beta)=\tau(\alpha)\subseteq\tau(\beta)$；

· 对任意序对 (α,β)，有 $\tau((\alpha,\beta))=(\tau(\alpha),\tau(\beta))$。

这样在 M 中，有 $I(u)\in I(U)$，则 $\tau(I(u)\in I(U))=\tau(I(u))\in\tau(I(U))=(u\in U)$ 为 S 满足的断言，同理有：

- $\tau(I(r)\in I(R))=(r\in R)$；
- $\tau(I(p)\in I(P))=(p\in P)$；
- $\tau(I(s)\in I(S))=(s\in S)$；

且 $\tau((I(u),I(r))\in I(UA))=\tau((I(u),I(r)))\in\tau(I(UA))=(\tau(I(u)),\tau(I(r)))\in\tau(I(UA))=(u,r)\in UA$，同理有：

- $\tau((I(u),I(s))\in I(user))=(u\in user(s))$；
- $\tau((I(s),I(r))\in I(roles))=(r\in roles(s))$；
- $\tau((I(s),I(p))\in I(permissions))=(p\in permissions(s))$。

(c) 定义 τ^- 为：给定 RBAC 状态 S 和 KB 的模型 $M=(\Delta,I)$，有：

- $\tau^-(u)=I(u)$对每个 $u\in U$；
- $\tau^-(r)=I(r)$对每个 $r\in R$；
- $\tau^-(p)=I(p)$对每个 $p\in P$；
- $\tau^-(s)=I(s)$对每个 $s\in S$；

且

- $\tau^-(U)=I(U)$；
- $\tau^-(R)=I(R)$；
- $\tau^-(P)=I(P)$；
- $\tau^-(S)=I(S)$；
- $\tau^-(UA)=I(UA)$；
- $\tau^-(PA)=I(PA)$；
- $\tau^-(user)=I(user)$；
- $\tau^-(roles)=I(roles)$；
- $\tau^-(permissions)=I(permissions)$；

且对 S 中的任意元素 α 和 β，τ^- 还满足如下的关系：

- 如果 $\alpha\in\beta$，$\tau^-(\alpha\in\beta)=\tau^-(\alpha)\in\tau^-(\beta)$；

这样，对断言 θ，如果 $S\vdash\theta$，则有

- 如果 $\theta=(u\in U)$，则 $\tau^-(u\in U)=(I(u)\in I(U))$；
- 如果 $\theta=(r\in R)$，则 $\tau^-(r\in R)=(I(r)\in I(R))$；
- 如果 $\theta=(p\in P)$，则 $\tau^-(p\in P)=(I(p)\in I(P))$；
- 如果 $\theta=(s\in S)$，则 $\tau^-(s\in S)=(I(s)\in I(S))$；
- 如果 $\theta=(u\in user(s))$，则 $\tau^-(u\in user(s))=((I(u),I(s))\in I(user))$；
- 如果 $\theta=(r\in roles(s))$，则 $\tau^-(r\in roles(s))=((I(s),I(r))\in I(roles))$；
- 如果 $\theta=(p\in permissions(s))$，则 $\tau^-(permissions(s,p))=((I(s),I(p))\in I(permissions))$；
- 如果 $\theta=\neg\theta_1$，则 $\tau^-(\neg\theta_1)=\neg\tau^-(\theta_1)$；
- 如果 $\theta=\theta_1\rightarrow\theta_2$，则 $\tau^-(\theta_1\rightarrow\theta_2)=\tau^-(\theta_1)\rightarrow\tau^-(\theta_2)$。

其中 u,r,p 和 s 为 KB 中的个体，U,P,S 和 R 为概念，*user*，*roles* 和 *permissions* 为 KB 中的角色。

命题 2 $\tau^-=I\circ\tau$，即对任意 RBAC 状态 S，有

$\tau^-(S)=I(\sigma(S))$

证明：对任意 RBAC 状态 $S=(U,R,S,P,UA,PA,RH,user,roles,permissions,mutuallyexclusive)$，有，对每个 $u\in U,u\in L,\tau^-(u)=I(u)$且 $\sigma(u)=u$，可得 $\tau^-(u)=I(\sigma(u))$；

类似地，有 $\tau^-(r)=I(\sigma(r))$，$\tau^-(s)=I(\sigma(s))$，$\tau^-(p)=I(\sigma(p))$，$\tau^-(U)=I(\sigma(U))$，$\tau^-(S)=I(\sigma(S))$，$\tau^-(R)=I(\sigma(R))$，$\tau^-(P)=I(\sigma(P))$，$\tau^-(UA)=I(\sigma(UA))$，$\tau^-(PA)=I(\sigma(PA))$，$\tau^-(user)=I(\sigma(user))$，$\tau^-(roles)=I(\sigma(roles))$，$\tau^-(permissions)=I(\sigma(permissions))$

且，对断言 θ，满足 $S\vdash\theta$，则有：

- 如果 $\theta=(u\in U)$，根据 τ^- 的定义，有 $\tau^-(u\in U)=(I(u)\in I(U))$，而对 $I(\sigma(u\in U))=I(U(u))$，对断言 $U(u)$要成立，必须 $I(u)\in I(U)$，这样显然有 $\tau^-(u\in U)=I(\sigma(u\in U))$，同理可证：
- 如果 $\theta=(r\in R)$，则 $\tau^-(r\in R)=I(\sigma(r\in R))$；
- 如果 $\theta=(s\in S)$，则 $\tau^-(s\in S)=I(\sigma(s\in S))$；
- 如果 $\theta=(p\in P)$，则 $\tau^-(p\in P)=I(\sigma(p\in P))$；
- 如果 $\theta=(u\in user(s))$，则 $\tau^-(u\in user(s))=I(\sigma(u\in user(s)))$；
- 如果 $\theta=(r\in roles(s))$，则 $\tau^-(r\in roles(s))=I(\sigma(r\in roles(s)))$；
- 如果 $\theta=(p\in permissions(s))$，则 $\tau^-(p\in permissions(s))=I(\sigma(p\in permissions(s)))$；
- 如果 $\theta=\neg\theta_1$，且 $\tau^-(\theta_1)=I(\sigma(\theta_1)$，则 $\tau^-(\neg\theta_1)=\neg\tau^-(\theta_1)$，对 $I(\sigma(\neg\theta_1))=I(\neg\sigma(\theta_1))=\neg I(\sigma(\theta_1))$，则有 $\tau^-(\neg\theta_1)=I(\sigma(\neg\theta_1))$；
- 如果 $\theta=\theta_1\rightarrow\theta_2$，且 $\tau^-(\theta_1)=I(\sigma(\theta_1)$，$\tau^-(\theta_2)=I(\sigma(\theta_2)$，则对 $\tau^-(\theta_1\rightarrow\theta_2)=\tau^-(\theta_1)\rightarrow\tau^-(\sigma_2)$，$I(\sigma(\theta_1\rightarrow\theta_2))=I(\sigma(\theta_1)\rightarrow\sigma(\theta_2))=I(\sigma(\theta_1))\rightarrow I(\sigma(\theta_2))=\tau^-(\theta_1)\rightarrow\tau^-(\theta_2)$。

这样对 S，$\tau^-(S)=I(\sigma(S))$。证毕。

命题 3 给定 DL_{RBAC} 模型 $M=(\Delta,I)$，则 $\tau(M)$ 为 RBAC 状态。

根据 τ 的定义，该命题成立。

命题 4 给定 RBAC 的状态 S，则 $M=\tau^-(S)$ 为 DL_{RBAC} 的模型。

根据命题 2 和 τ^- 的定义，该命题显然成立。

定理 1 (1) 给定模型 $M=(\Delta,I)$，存在状态 $S=\tau(M)$，使得对每个断言 φ，$M\vdash\varphi$ 当且仅当存在断言 ψ，使得 $S\vdash\psi$；

(2) 对任意状态 S，存在模型 $M=\tau^-(S)$ 使得对任意断言 ψ，$S\vdash\psi$ 当且仅当存在断言 φ，使得 $M\vdash\varphi$。

证明：(1)给定模型 $M=(\Delta,I)$，存在状态 $S=\tau(M)$ 使得对每个断言 φ，$M\vdash\varphi$ 表示断言 φ 在 M 中是可满足的，$S\vdash\psi$ 表示断言 ψ 在 S 中成立，则：

(a)对 $ABox$ 中的断言，如 $UA(u,r)$，$M\vdash UA(u,r)$，则 $(I(u),I(r))\in I(UA)$，根据 M 的定义，如果 $I(u)=u$，$I(r)=r$，$I(UA)=UA$，显然 $(I(u),I(r))\in I(UA)$ iff $(u,r)\in UA$ 在 S 中成立，即 $S\vdash(u,r)\in UA$。又根据 τ 的定义，有 $\tau((I(u),I(r))\in I(UA))=(u,r)\in UA$，所以有 $M\vdash UA(u,r)$ iff $S\vdash(u,r)\in UA$。同理可证：

$M\vdash PA(p,r)$ iff $S\vdash(p,r)\in PA$；

$M\vdash user(s,u)$ iff $S\vdash(s,u)\in user$；

$M\vdash roles(s,r)$ iff $S\vdash(s,r)\in roles$；

$M\vdash permissions(s,p)$ iff $S\vdash(s,p)\in permissions$；

$M\vdash RH(r',r)$ iff $S\vdash(r',r)\in RH$；

$M\vdash mutuallyexclusive(r'',r)$ iff $S\vdash(r'',r)\in mutuallyexclusive$。

(b) 对 $TBox$ 中的断言 $roles\subseteq(\sim(user\circ\sim UA))\circ RH^-$ 和 $permissions\subseteq\sim(roles\circ\sim(RH^-\circ PA^-))$。

对断言 $roles(s)\subseteq\{r:\exists r'\geqslant r((user(s),r')\in UA)\}$，则

根据命题1可知：$M\models roles\subseteq(\sim(user\circ\sim UA))\circ RH^{-}$ iff $S\models roles(s)\subseteq\{r:\exists r'\geqslant r((user(s),r')\in UA)\}$；

对断言 $permissions(s)=\{p:\forall r\in roles(s)\exists r'\leqslant r((p,r')\in PA)\}$，则根据命题1可知：$M\models permissions\subseteq\sim(roles\circ\sim(RH^{-}\circ PA^{-}))$ iff $S\models permissions(s)=\{p:\forall r\in roles(s)\exists r'\leqslant r((p,r')\in PA)\}$。

同理可证(2)。这里省略证明过程。证毕。

定理1说明了 DL_{RBAC} 可以忠实地表示 RBAC 中的各种关系。

4 相关研究比较

目前已有的用描述逻辑来研究 RBAC 建模的有 Zhao 等提出的表示[10]，还有用描述逻辑对 RBAC 的扩充模型进行的形式化描述[11,12]，这些表示在基本 RBAC 建模方面都有类似的表达。

本文与它们的主要区别如下：

(1) DL_{RBAC} 和 Zhao 的 DL 方法都包含了 RBAC96 模型的组件中的 U,R,P,S,UA,PA 等。由于 Zhao 的方法中没有对角色层次 RH 的表示，直接利用子概念 RR_1 和 RR_2 之间的包含关系来表示它们实例之间的优势关系。这样做显然存在缺陷。首先找不到语义模型来解释这种关系，其次对 RBAC 模型中隐含的角色继承无法表示；(2) 对于用户和权限的关系，在 RBAC96 模型中，用户是通过角色的激活来获得权限的，如果表示了 *roles* 和 *permissions*，就不需要再用 *authorized* 来表示用户和权限之间的联系，这样 Zhao 的表示违背了 RBAC96 的本意。而在 DL_{RBAC} 表示中没有对用户的直接授权，而是用权限激活约束公理(公理13)来表示角色间接授权，这样更忠实于 RBAC96 模型的本意。

从以上分析可以看出，本文对基本 RBAC 模型的形式化表示体现了 RBAC 模型的特点，即用户不是直接被授予权限，而是通过激活他所在的角色，间接获得该角色所分配的权限，并且补充了 RBAC 模型中的继承性定义。

结束语 根据 RBAC 的特点，结合基本描述逻辑语言 ALC 及其扩展语言，对基本的 RBAC 模型进行了形式化描述。这种描述不但表示出了基本 RBAC 模型中的各种关系，还将 RBAC 中与角色继承有关的 RH 继承性、UA 继承性和 PA 继承性等都定义出来，从而弥补了 RBAC 模型对这些关系只有隐含说明，没有明确表示的缺陷。在表示了 RBAC 中的关系和约束基础上，还通过定义 RBAC 状态和 DL_{RBAC} 模型之间的转换关系，得出 DL_{RBAC} 模型是忠实对应一个 RBAC 状态的表示方法，从而为进一步研究 RBAC 的性质打下基础。

参 考 文 献

[1] Sandhu R, Coyne E, Feinstein H, et al. Role-based access control models[J]. IEEE computer, 1996, 29(2): 38-47

[2] Ferraiolo D, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274

[3] ANSI INCITS 359-2004. Role Based Access Control[S]. American National Standards Institute, 2004

[4] Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies[J]. ACM Transactions on Information and System Security (TISSEC), 2000, 3(2): 85-106

[5] Li N, Byun J W, Bertino E. A critique of the ANSI standard on role-based access control[J]. IEEE Security and Privacy, 2007, 5(6): 41-49

[6] Ferraiolo D, Kuhn R, Sandhu R. RBAC standard rationale: Comments on "A critique of the ANSI standard on role-based access control"[J]. IEEE Security and Privacy, 2007, 5(6): 51-53

[7] Koch M, Mancini L V, Parisi-Presicce F. A graph-based formalism for RBAC[J]. ACM Transactions on Information and System Security, 2002, 5(3): 332-365

[8] Baader F, Calvanese D, McGuinness D L, et al. Description Logic Handbook[M]. Cambridge University Press, 2002

[9] Baader F, Küsters R, Wolter F. Extensions to Description Logics [M]. Cambridge University Press, 2002: 226-268

[10] Zhao C, Heilili N, Liu S, et al. Representation and reasoning on RBAC: a description logic approach[C]// Hung D V, Wirsing M, eds. ICTAC2005, LNCS 3722. Berlin: Springer, 2005: 381-393

[11] Ji G, Tang Y, Jiang Y, et al. A description logic approach to represent and extend RBAC model[C]// 1st International Symposium on Pervasive Computing and Applications. 2006: 151-156

[12] Yu H, Xie Q, Che H. Description Logic Based Conflict Detection Methods for RB-RBAC Model[J]. International Journal of Computer Science and Network Security, 2006, 6(1A): 120-125

(上接第28页)

[36] Seamons K E, Winslett M, Yu T, et al. Requirements for Policy Languages for Trust Negotiation [C]// Proc. of the 3rd IEEE Int'l Workshop on Policies for Distributed Systems and Networks. 2002: 68-79

[37] Bertino E, Ferrari E, Squicciarini A C. Trust Negotiations: Concepts, Systems and Languages [J]. Computing in Science & Engineering, 2004, 6(4): 27-34

[38] Herzberg A, Mass Y, Mihaeli J, et al. Access Control Meets Public Key Infrastructure, or: Assigning Roles to Strangers [C]// Proc. of the 21th IEEE Symposium on Security and Privacy (SP'00). 2000: 2-14

[39] Viljanen L. Towards an Ontology of Trust [C]// LNCS 3592. 2005: 175-184

[40] Li N, Mitchell J C. Beyond Proof-of-Compliance: Security Analysis in Trust Management [J]. Journal of the ACM, 2005, 52(3): 474-514

[41] Li N, Tripunitara M V. Security Analysis in Role-based Access Control [J]. ACM Transactions on Information and System Security, 2006, 9(4): 391-420

[42] Sun Y, Han Z, Liu K J R. Defense of Trust Management Vulnerabilities in Distributed Networks [J]. IEEE Communications Magazine, 2008, 46(2): 112-119

[43] 廖振松，金海，李赤松，等. 自动信任协商及其发展趋势[J]. 软件学报, 2006, 17(9): 1933-1948

[44] Liimatainen S. Usability of Decentralized Authorization Systems-A Comparative Study [C]// Proc. of the 38th Hawaii International Conference on System Sciences (HICSS'05). 2005: 186b-186b

[45] Kinateder M, Baschny E, Rothermel K. Towards a Generic Trust Model-Comparison of Various Trust Update Algorithms [C]// Proc. of the iTrust 2005. LNCS 3477. 2005: 177-192

[46] Fullam K K, Sabater-Mir J, Barber K S. A Design Foundation for a Trust-Modeling Experimental Test Bed [C]// LNAI 3577. 2005: 95-109

[47] Hassan J, Sirisena H, Landfeldt B. Trust-based Fast Authentication for Multiowner Wireless Networks [J]. IEEE Transactions on Mobile Computing, 2008, 7(2): 247-261