

# 基于 Graphplan 的 ARBAC 策略安全分析方法

刘 强<sup>1,2)</sup> 姜云飞<sup>1)</sup> 饶东宁<sup>1)</sup>

<sup>1)</sup>(中山大学信息科学与技术学院软件研究所 广州 510275)

<sup>2)</sup>(广东工业大学机电工程学院 CIMS 实验室 广州 510006)

**摘 要** 策略安全分析是访问控制系统保持安全状态的重要机制. 针对具有角色继承层次和角色静态互斥特征的分  
布式访问控制系统, 文中采用智能规划技术进行策略安全分析. 首先, 提出了策略安全分析问题向规划问题转换的整  
体思路, 定义“虚动作”模型以描述角色继承关系, 使用领域互斥表述静态互斥角色, 引入领域公理处理 ARBAC 策  
略的开放世界假设问题和前提条件中的负谓词问题. 其后, 运用图规划(Graphplan)算法求解转换而来的规划问题,  
重点分析了领域公理对规划图中部分 NooP 动作的剪枝作用, 提出了领域公理在规划图扩展阶段的应用方式以及  
据此改进的图规划算法, 介绍了已开发的面向 ARBAC 策略安全分析实验型规划系统. 最后, 进行了应用示例说明.

**关键词** 基于角色的访问控制; 策略; 安全性分析; 图规划

**中图法分类号** TP309 **DOI 号:** 10.3724/SP.J.1016.2009.00910

## Safety Analysis of ARBAC Policy Based on Graphplan

LIU Qiang<sup>1,2)</sup> JIANG Yun-Fei<sup>1)</sup> RAO Dong-Ning<sup>1)</sup>

<sup>1)</sup>(Software Research Institute, School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275)

<sup>2)</sup>(CIMS Laboratory, Faculty of Electromechanical Engineering, Gongdong University of Technology, Guangzhou 510006)

**Abstract** Safety analysis is the prerequisite mechanism for distributed access control system. Graphplan theory was imported to perform safety analysis on those access control system which support role hierarchy and Static Mutual Exclusion Roles (SMER). A complete resolution for the reachability problems, a principal safety analysis problem, is planned and designed. Firstly, a description model using planning language is set up, virtual action is put forward to express the inheritance relation between roles, and SMERs is transformed to domain constraints. Secondly, to settle the negative predicate problem and open world assumption problem, domain axiom is employed. Then the Graphplan arithmetic is modified by trimming ‘Noop’ actions and relative predicates from plan graph using those axioms. Based on the amended arithmetic, the corresponding experiment system is developed. At last, a application case of the analysis process is illustrated.

**Keywords** role-based access control; policy; security analysis; graphplan

## 1 引 言

访问控制是计算机安全领域中的一个重要主

题. 基于角色的访问控制(Role-Based Access Control, RBAC)模型已成为当前主流的访问控制模型. RBAC 思想最早由 Ferraiolo 和 Kuhn 于 1992 年提出<sup>[1]</sup>, 其后, Sandhu 等设计出一个完整的访问控制

模型——RBAC96<sup>[2]</sup> 及其管理模型 ARBAC97<sup>[3]</sup>. ARBAC97 包括 3 大授权管理组件:URA 管理用户到角色的指派;RRA 管理由继承引起的角色与角色之间的层次关系;PRA 管理权限到角色的指派. 策略(policy)是 RBAC 模型中表述安全操作规范的语言,一般意义上,策略可做如下划分:(1) 安全策略(RBAC policy),用以规范用户的安全操作;(2) 管理策略(ARBAC policy),改变安全策略的上层管理规则,用以规范安全管理员对安全策略集的操作. 我们将遵循管理策略的授权操作行为表述为管理策略的执行. ARBAC97 模型中,管理策略的形式化描述涉及 3 个要素:安全管理员、前提条件和目标角色集. 如 URA 管理策略 *can\_assign*(SSO, DIR  $\vee$  PL, DRC)中,SSO 为系统安全管理员,是策略的合法施动者,DIR  $\vee$  PL 为策略执行的前提条件(前提条件是由  $X$ ( $X$  表示角色),  $\neg X$ ,  $\vee$  和  $\wedge$  组成的布尔表达式),DRC 为目标角色,也是策略的执行效果. 策略表示:允许系统安全管理员指派担任技术指导委员会委员(DIR)或项目主管(PL)的用户担任设计评审委员会委员(DRC).

在大型的、分布式的系统中,用户、角色成百上千,管理逻辑相当复杂,管理事务异常繁琐,集中式的管理不具备可行性. 依赖于管理策略的语义表示,ARBAC97 提供一种分散式的管理模式,上层安全管理员将管理权限委派(delegation)给可信的(trusted)下层安全管理员,形成分散式的管理格局. 然而,由于前提条件的存在,管理策略之间可能形成持续的因果推理,使得其执行效果难于直观判断,这可能导致安全管理员在进行授权时决策失误,给系统带来严重的安全隐患. 智能化的策略安全性分析方法和程序可以为授权决策提供必要的支持,提升系统的安全性能.

安全分析(safety analysis)问题最早由 Harrison 等提出<sup>[4]</sup>,用以分析权限的泄漏问题,即安全的访问控制系统经执行命令序列后,是否可到达不安全的状态,使得系统允许不可信用户访问受控资源. 最初的安全分析问题基于著名的访问矩阵模型,被证明是不可判定的,在一些特殊的约定下,如不允许增加主客体情况下,可以转化为可判定问题. Li 等面向 RBAC96 模型,提出了安全性分析(security analysis)的概念<sup>[5-6]</sup>,并提炼出几类典型安全性问题:简单安全(simple safety)问题,即上述的安全分析问题,又称为可达性(reachability)问题、简单可用性(simple availability)问题、限定安全性(bounded

safety)问题、活性(liveness)问题、互斥(mutual exclusion)问题和包容(containment)问题,其中简单安全问题和简单可用性是策略安全性分析中两类最基本的问题. 可达性问题是分析是否存在不可信用户可以访问指定资源的系统状态,其否定回答表示系统是安全的. 可用性问题是分析在所有可达的系统状态中,用户是否总是可以访问指定资源,其肯定回答表示系统是安全的.

在 ARBAC 策略安全分析的研究进程中,人们总是对研究对象预设一些假设条件,采用合适的方法,得出一些重要的结论. Munawer 与 Sandhu 使用一种扩展的访问矩阵模型(Augmented Typed Access Matrix, ATAM)来表述 RBAC 模型,基于已有的安全分析结论,得出了 RBAC96 模型下的安全分析问题是不可判定的<sup>[7]</sup>. 这一结论引发了争议, Li 等认为<sup>[6]</sup>: ATAM 方法在 RBAC96 上强加了过于复杂的管理模型,本质上,简单安全分析问题是可判定的. Li 等得出了两类简化的安全性分析问题的复杂度: AATU (Assignment And Trusted Users) 属于较难问题(coNP-Hard),但半静定的 AATU 可以在多项式时间内求解, AAR (Assignment And Revocation)问题属于 coNP-Complete 问题,半静定的 AAR 问题可以在多项式时间内可以求解. 杨秋伟等使用图灵机理论,以 PRA97 为分析对象进行安全性分析,证明了必然性安全查询(近似于可用性问题)和状态无关的可能性安全查询(近似于简单安全问题)能在多项式时间内求解,而一般的可能性查询是不可判定的<sup>[8]</sup>. 文献[4]和文献[8]均使用图灵机模型,将简单安全问题转换为图灵机的停机问题,因而是不可判定的. 事实上,ARBAC 管理模型的简化设定和 ARBAC 策略特征的假设,使得简单安全分析问题可以转化为可判定问题. Sasturkar 等提出应用智能规划技术进行策略安全性分析<sup>[9]</sup>,并分别讨论了 ARBAC 策略前提条件具有非显式负谓词(命题)、非析取,前提条件中的文字数受限等特征下的复杂性问题,得出可达性问题(即简单安全问题)属于 PSPACE-Complete 问题这一重要结论.

在上述分析过程中,角色之间的关系被假定为平行关系(无继承关系),用以简化分析过程. 文献[9]中提到完全实例化的思路:将具有角色继承层次的安全分析问题转换为角色扁平化情况下的安全分析问题,进而利用角色扁平化情况下的分析方法和分析结论. 然而,文献也认为,这一转换过程本身具有指数时间的复杂度,一种直接的分析方法比完全实例

化的转换方法要更为有效. 基于文献[9]的研究工作, 论文采用图规划技术, 针对具有角色继承层次和角色静态互斥等特征的 ARBAC 策略安全问题展开研究. 论文主要贡献在于:

(1) 提出了安全分析问题向规划问题转换和建模的方法. 有效解决了 ARBAC 策略状态空间的开放世界假设问题、前提条件中的负命题问题、角色继承关系和角色静态互斥的表述问题.

(2) 引入领域公理, 进行规划图的剪枝, 改造图规划算法, 依此设计和开发了面向安全分析的实验型规划系统.

本文第 2 节介绍研究内容与方法, 第 3 节描述了安全分析问题向规划问题的转化过程, 第 4 节描述领域公理的应用方式和图规划算法的改造过程, 第 5 节进行了应用说明.

2 研究内容与方法

2.1 ARBAC97 模型简介

ARBAC97 模型中, 三大组件具有显式的语义范围, PRA97 对应岗位设置和岗位职责的定义; URA97 对应岗位人选的委任; RRA97 对应岗位与岗位之间的由部分职责重叠引起的关联关系. RBAC96 和 ARBAC97 的形式化表示如下<sup>[3]</sup>.

**定义 1.**  $U$  为用户集,  $R$  为角色集,  $P$  为操作许可集,  $S$  为会话集,  $AR$  为授权管理角色集,  $CR$  为授权前提条件(由  $X(X$  表示角色),  $\neg X$ ,  $\vee$  和  $\wedge$  组成的布尔表达式),  $2^R$  指某一常规角色集.

$UA \subseteq U \times R$ , 表示用户到角色的指派关系.  
 $PA \subseteq R \times P$ , 表示操作许可到角色的指派关系.  
 $RH \subseteq R \times R$ , 表示角色之间所形成的继承关系.  
URA97 组件中策略的表示如下.

**定义 2.**  $can\_assign \subseteq AR \times CR \times 2^R$ , 用户角色指派, 表示  $AR$  可以将满足  $CR$  条件的用户指派给  $2^R$  的角色.

**定义 3.**  $can\_revoke \subseteq AR \times 2^R$ , 用户/角色指派回收, 表示  $AR$  用户可以无条件撤销已是  $2^R$  中某角色成员的用户到该角色指派.

角色继承层次是 RRA 组件的基本数据结构, 通常使用“ $r_1 \leq r_2$ ”表示  $r_2$  与  $r_1$  的继承关系, 包含两层含义:  $r_2$  继承  $r_1$  的权限,  $r_1$  继承  $r_2$  的用户. RRA 组件中的策略用来规范对这一层次关系进行调整的操作. 角色静态互斥分离 (Static Mutually Exclusive Roles, SMER) 是 RBAC96 模型中一类重要的约束,

用以保证关键角色和岗位不能被同一用户所担任, 如确保会计和出纳不会为同一用户担任.

2.2 研究对象和问题的假定

**假设 1.** 以  $UA/RH$  为研究对象.

由 RBAC96 的定义可知,  $UA$  和  $PA$  的取值空间相互独立, 且相对于  $RH$  对称. 鉴于这种对称性, 取  $UA/RH$  或  $PA/RH$  为研究对象均不失一般性, 其分析过程和分析方法可以应用到另外一个研究对象上, 我们选定  $UA/RH$  作为研究对象.

**假设 2.** 静态  $RH$ .

在进行安全分析时, 总是取  $RH$  的快照, 因此, 在进行安全策略分析时  $RH$  的取值是固定的, 可以把  $RH$  作为分析环境的组成部分, 在领域建模时再予以考虑.

**假设 3.** 不考虑管理策略中的安全管理员.

进行安全分析前, 我们总是根据问题的需要, 提取出可执行的 ARBAC 授权管理策略集合展开分析. 也就是说, 分析过程中, 任一 ARBAC 授权管理策略是可执行的, 分析过程并不会关心执行的主体是谁, 而只关心执行管理策略后的效果, 只有得到分析结论后, 才需要考虑执行的主体. 因此, 描述策略时可以省略对安全管理员的描述, 如对策略  $can\_assign(EDSO, ENG, DIR)$  而言, 只需考虑参数  $ENG$  和  $DIR$ .

**假设 4.** 以可达性分析问题为主要研究问题.

由于可用性问题的转化可达性问题<sup>[9]</sup>, 本文仅对可达性问题展开研究.

2.3 安全分析中的规划问题

**定义 4(RBAC 状态).** RBAC 状态  $s = \{UA, RH\}$ , 其中  $UA, RH$  为状态变量.

**定义 5(RBAC 状态转换系统).** RBAC 状态转换系统  $\Sigma = \{S, A, \delta\}$ , 其中,  $S$  为 RBAC 状态集合;  $A$  为授权动作集合, 其定义由 ARBAC 管理策略和  $RH$  转换而来;  $\delta: S \times A \rightarrow S$  为状态转移函数, 表示动作作用在状态上导致状态变量取值变化, 进而引发状态变迁的一般性规律, 使用符号“ $\mapsto$ ”表示状态的转移.

**定义 6(U-R 可达性问题).** 以  $UA/RH$  为研究对象的可达性问题, 指从当前状态  $s_0$  出发是否存在一种可达状态  $s_g$ , 使得  $s_g \Rightarrow q$ , 即  $\exists s_g (s_0 \mapsto s_g) \wedge (s_g \Rightarrow q)$  是否为真, 其中  $q$  为不可信用户与目标角色所组成的元组. 其否定回答表明系统是安全的, 安全管理员可以据此拒绝不可信用户对资源的访问.

**定义 7(U-R 可用性问题).** 以  $UA/RH$  为研

究对象的可用性问題,指从当前状态  $s_0$  出发,对于所有的可达状态  $s_g$ ,是否均存在  $s_g \Rightarrow q$ ,即  $\forall s_g ((s_0 \mapsto s_g) \rightarrow (s_g \Rightarrow q))$  是否为真.其中  $q$  为可信用户与目标角色所组成的元组.其肯定回答表明系统是安全的,可以确保可信用户总是可以访问指定资源.

同样,U-R 可用性问題可以转换为 U-R 可达性问題,因此,仅研究 U-R 可达性问題.回答 U-R 可达性问題的关键在于确认是否存在一个安全的授权动作序列,使得  $s_0$  可以转移到  $s_g$ ,这可以构造成一个智能规划问題.

**定义 8**(安全分析中的规划问題). 安全分析中的规划问題  $P = \{\Sigma, s_0, s_g\}$ ,其中,  $s_0$  为初始状态,由当前用户与其所承担的角色组成的元组构成;  $s_g$  为目标状态,由当前用户与目标角色集中角色组成的元组构成.

如果存在这样一个动作序列  $\pi$ ,使得初始状态可以转移到目标状态,即  $s_0 \mapsto_{\pi} s_g$ ,则问題存在规划解  $\pi$ .我们可以把 U-R 可达性问題转换为定义 8 所示的规划问題进行求解.

3 安全分析问題的规划模型

3.1 安全分析问題向规划问題转换的过程

3.1.1 安全分析问題向规划问題转化的步骤

求解规划问題之前,需要构建该问題的领域模型,说明该领域的变量及类型、谓词、动作等要素.针对安全分析问題,定义谓词集如下.

**定义 9**(RBAC 领域模型的谓词集). 定义谓词  $playRole(u, r)$  表示用户  $u$  担任角色  $r$ ,  $ownPerm(r, p)$

表示角色  $r$  拥有操作许可  $p$ ,  $getPerm(u, p)$  表示用户获得了许可  $p$ .其中,  $u \in U, p \in P, r \in R$ .相对应的具有否定语义的谓词形式为  $unplayRole(u, r)$ ,  $unownPerm(r, p)$ ,  $ungetPerm(u, p)$ .以下将  $unplayRole(u, r)$ ,  $unownPerm(r, p)$ ,  $ungetPerm(u, p)$  统称为“un 谓词”,实例化后的“un 谓词”成为“un 命题”.

存在领域公理(Domain Axiom, DA):

$$playRole(u, r) \wedge ownPerm(r, p) \rightarrow getPerm(u, p) \tag{DA1}$$

这一公理在进行用户到资源可达性分析时需要使用到,当只研究 U-R 可达性问題时,仅仅使用到谓词  $playRole$  和  $unplayRole$ .

通过如下步骤,可以将具有角色继承层次关系和角色静态互斥特征的安全分析问題转换为规划问題:

1. 将角色继承层次关系表述成特殊的动作模型.
2. 结合领域 SMER 集合与角色继承层次关系,生成规划领域内的领域命题互斥集合.
3. 简化角色继承层次关系,将 ARBAC 管理策略转化为动作模型.
4. 定义初始状态与目标状态,将安全分析实例转化为具体的规划问題.
5. 针对规划问題进行求解,将规划问題求解结论翻译回安全分析领域.

其中步 1~3 建立了领域模型,步 4 获取规划问題,步 5 进行求解和领域翻译.以如图 1 所示角色继承层次为实例,分别对各个步骤进行说明.该实例取自某一制造企业以项目形式组织产品的研发工作过程中的角色设置.

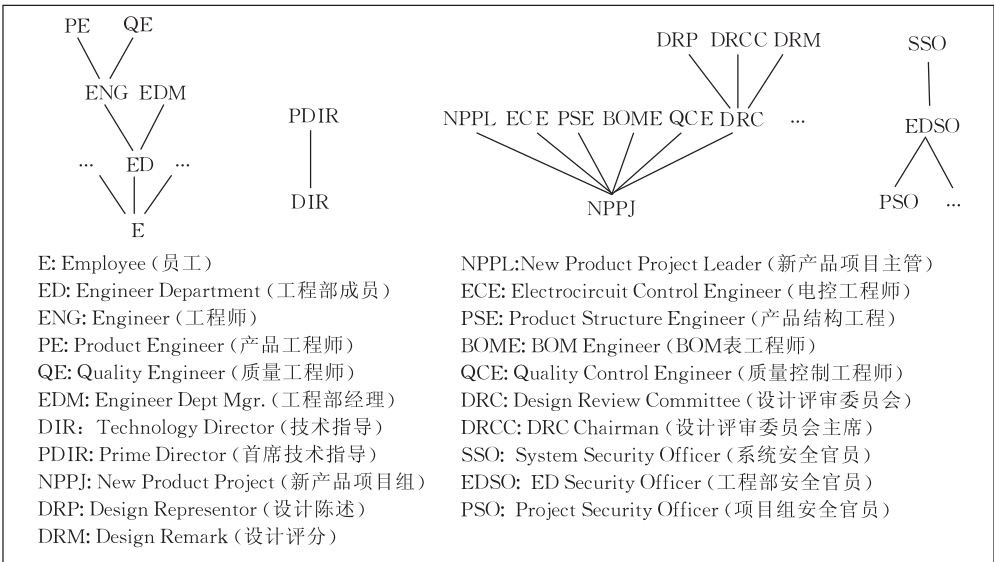


图 1 角色继承层次

3.1.2 开放世界假设说明和领域公理

ARBAC 授权管理策略满足开放世界假设 (Open World Assumption, OWA); 即表示“没有规定的是未知的”. 如策略  $can\_assign(PSO, NPPJ \wedge (\neg ECE) \wedge (\neg PSE) \wedge (\neg BOME), QCE)$  表示只要当前用户是角色 NPPJ 的成员同时非 PSE、ECE 和 BOME 的成员时, 就可以被 PSO 指派为 QCE 的成员, 至于其是否是否是其他角色的成员, 策略并不关心. 显然, “ $\neg ECE$ ”不单纯表示对于 ECE 的否定, 还蕴含着“指称除 ECE 的其余角色”这一语义. 例如: 如果当前用户既是 NPPJ 的成员又是 ECE、PSE 或 BOME 的成员, 则上述策略的前提条件不满足, 策略不能执行; 如果当前用户是 NPPJ 和其他非 ECE、PSE 和 BOME 的成员, 如 NPPL 的成员, 则满足上述策略的前提条件, 该策略可以被执行.

然而, STRIPS<sup>[10]</sup> 语言对于规划问题的描述总是基于封闭世界假设 (Close World Assumption, CWA), 即表示“未明确赋值为真的命题总为假命题”. 尽管 PDDL<sup>[11]</sup> 语言描述支持 OWA<sup>[12]</sup>, 但很少有相应的规划器或规划算法支持 OWA, 我们使用 STRIPS 语言来描述领域模型和规划问题. 在安全分析问题向规划领域转换过程中, 对于类似于“ $\neg PE$ ”命题的领域语义进行转换时, 容易产生两类错误:

(1) “扭曲”. 如果我们把“ $\neg R$ ”中的“ $\neg$ ”看成“逻辑非”, 则根据 CWA 中的“假命题无需声明”的原则, 上述策略  $can\_assign(PSO, NPPJ \wedge (\neg ECE) \wedge (\neg PSE) \wedge (\neg BOME), QCE)$  与  $can\_assign(PSO, NPPJ, QCE)$  等同. 事实上, 若当前用户既是 NPPJ 的成员又是 ECE 的成员, 上数两策略具有不同的可执行性. 显然, 对“ $\neg R$ ”的转换扭曲原有策略的领域语义, 从而导致安全隐患.

(2) “丢失”. 如果我们把“ $\neg R$ ”看成一个谓词符号, 其中“ $\neg$ ”只是谓词命名中的组成部分, 则将策略  $can\_assign(PSO, NPPJ \wedge (\neg ECE) \wedge (\neg PSE) \wedge (\neg BOME), QCE)$  转换到规划领域时, 丢失了“ $\neg ECE$ ”蕴含的“指称除 ECE 的其余角色”这一领域语义, 使得对于同时为 NPPJ 和 NPPL 成员的用户而言, 策略本身可以执行, 而转换后的授权动作不可执行 (还需要满足前提条件  $(\neg ECE) \wedge (\neg PSE) \wedge (\neg BOME)$ ), 因而导致领域语义的丢失.

针对上述问题, 在转换过程中采用添加领域公理和领域约束的方式来规避. 具体地: 把“ $\neg R$ ”看成谓词符号并改写成“ $unplayRole(u, R)$ ”, 添加

“ $playRole(u, R)$ ”与“ $unplayRole(u, R)$ ”为领域约束, 同时, 添加领域公理:

$$\neg playRole(u, r) \leftrightarrow unplayRole(u, r) \quad (DA2)$$

3.2 从角色继承层次关系到虚动作

**定义 10**(虚动作). 虚动作是用来表示角色继承关系的特殊的规划动作.

“虚动作”的引入实质上是将领域问题中的领域知识在领域模型中予以表征. 之所有称为“虚动作”是指其具有常规动作的表达形式和使用方式, 但不具有执行过程, 不需要执行耗费. 虚动作的生成过程相对简单, 当以 UA/RH 为研究对象时, 使用  $playRole(u, R_i)$  作为前提条件,  $playRole(u, R_f)$  作为效果, 其中  $R_i$  为子角色,  $R_f$  为父角色. 如针对图 1 中“ $ENG \rightarrow ED \rightarrow E$ ”这一继承链, 形成虚动作 VAssign1 和 VAssign2, 如图 2 所示. 其中对应 VAssign1 和 VAssign2 中的命题, 存在由对应“un 命题”形成的虚动作, 如图 2 所示的 VAssign3 和 VAssign4.

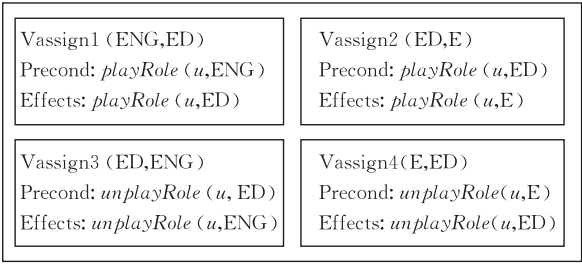


图 2 虚动作模型

虚动作的意义在于: 避免在问题求解前, 因为继承关系而带来大量的动作实例, 取而代之, 在问题求解过程中需要的时候再进行实例化.

3.3 领域命题互斥的生成

SMER 约束中, 只规定了角色与角色的互斥, 当考虑角色之间的继承关系时, 由于“父角色继承了子角色的用户<sup>[3]</sup>”, 使得担任子角色的用户, 同时也担任父角色. 依照这种关系, 可以衍生出一系列的领域命题互斥. 如图 1 中, 若角色 DRP 与 DIR 互斥, 则可以衍生出命题互斥对:  $(playRole(u, DIR), playRole(u, DRP)); (playRole(u, PDIR), playRole(u, DRP))$ . 由于领域公理 2 的存在, 在规划问题求解中, 同样需要将命题与对应的“un 命题”看成领域命题互斥, 如  $(playRole(u, DIR), unplayRole(u, DIR))$ .

3.4 从管理策略到规划动作模型

由于 3.2 节和 3.3 节的处理过程已经蕴含了角色继承层次的领域含义, 因此可以不在考虑角色之



间继承关系,据此,由管理策略生成规划动作模型的具体步骤如下:

1. 授权管理策略的前提条件  $CR$  转换为析取范式,假定其子句数为  $N$ .
2. 分别以每个子句作为动作的前提条件.
3. 由授权管理策略的目标角色集  $2^R$  生成  $|2^R|$  个  $playRole$  谓词实例(命题),并与由步 2 所得到的子句集进行笛卡儿积,形成  $(|2^R| \times N)$  个动作实例.
4. 给每个动作实例命名,并记录其对应的授权管理策略.

这一过程不但完成了管理策略到规划动作模型

Assign (PE) Precond: $playRole(u, ENG)$ Effects: $playRole(u, PE)$	Assign (QE) Precond: $playRole(u, ENG)$ Effects: $playRole(u, QE)$	Revoke (ENG) Precond: $playRole(u, ENG)$ Effects: $unplayRole(u, ENG)$
--	--	--

图 3 授权管理策略的规划动作模型

### 3.5 从可达性分析实例到规划问题

一个可达性分析实例通过如下过程转换为规划问题:RBAC 角色映射为规划问题的对象,授权管理策略和角色继承关系形成动作模型及其实例,据此生成规划问题的领域模型;当前用户与所担任的角色集  $R_0$  组合形成规划问题的初始状态,当前用户与目标角色集  $R_g$  组合形成目标状态集.

对所转化而成的规划问题进行求解,规划解中的动作序列最终被解析或映射成 ARBAC 策略序列和  $RH$  中的组成元素,用以回答安全管理员的询问——“是否可达,如果可达则相应的策略执行序列是什么?”.

初始状态中,并非需要对所有命题(实例化后的谓词)进行声明.一方面,由于缺少动作支持,部分命题的真值不发生变化,这部分命题在初始状态和求解过程中都可以剔除.另一方面,由于领域公理 2 的存在,当声明了某命题时,其对应的“un 命题”不需要声明,反之则反;否则,会使得初始状态存在领域互斥命题,直接导致问题不可解.

### 3.6 建模过程的复杂性

对一个具有  $K$  个角色的可达性问题实例,经由上述转换,存在  $(2 \times K)$  个命题,角色继承层次关系为无环有向图,最多可以生成  $K \times (K - 1)$  个虚动作,时间复杂度为  $O(K^2)$ . 由  $M$  个 ARBAC 策略,至多可以生成  $\max(|2^R|) \times n \times M$  个动作,其中  $\max(|2^R|)$  为 ARBAC 策略的目标角色集合势的上限,令  $\alpha = \max(|2^R|)$ ,  $n$  为策略前提条件的析取范式中子句数的上限,其转换过程的时间复杂度为

的转化过程,也完成了动作的实例化过程.在图 1 所示的角色继承层次关系中,  $can\_assign(EDSO, ENG, (PE, QE))$  和  $revoke(EDSO, ENG)$  表示设计部安全管理员可以指派任一工程师为产品设计工程师或质量工程师,亦可以无条件撤销某用户的工程师资格,转化成的规划动作模型如图 3 所示. Revoke 动作是一类特殊的动作,其动作效果为前提效果的否定,即删除前提效果.由于公理 2 的存在,可以使用  $unplayRole(u, E)$  来替代负效果  $\neg playRole(u, E)$  ( $\neg$  在这里表示逻辑“非”).

$O(\alpha \times n \times M)$ . 显然,转换过程可以在多项式时间内完成.由此,对应的规划问题规模为  $(2 \times K)$  个命题和  $(K \times (K - 1) + \alpha \times n \times M)$  个动作.

## 4 面向安全分析的图规划算法改进

### 4.1 图规划算法介绍

图规划是由 Blum 和 Furst 于 1995 年提出的一种规划方法<sup>[13]</sup>,图规划算法的出现使得与领域无关(domain independent)的智能规划算法的效率得到了较大的提高.规划图(planning graph)是图规划算法的基本数据结构,是一个具有两类节点和三类边的有向无环分层图.规划图以命题层(proposition levels)和动作层(action levels)交替形式出现,命题层包含命题节点,动作层包含动作节点.规划图的首层是命题层,包括规划问题初始条件下的所有命题.图规划包含两个阶段(phases):图扩展(graph expansion)阶段和解提取(solution extraction)阶段.图扩展阶段正向扩展规划图直到目标状态的所有命题出现或到达不动点为止,解提取阶段反向搜索规划图以求出规划解.空动作(No Operation, NoOp)是图规划中一类特殊的动作,即将当前层的命题保持到下一层,其动作和效果均为相同命题.互斥是图规划算法中重要的概念,在规划图的某层内,如果下列三者中任一成立,则两动作实例互斥:

- (1) 不一致效果(Inconsistent Effects):一个动作的效果是另一个动作效果的否定.
- (2) 冲突(Interference):一个动作的效果之一

是另一个动作前提之一的否定形式。

(3) 竞争需要 (competing needs): 一个动作的前提之一和另一个动作的前提之一互斥。

两个命题互斥的情况亦存在 3 种:

- (1) 领域互斥: 领域规定的命题互斥。
- (2) 正负谓词互斥: 谓词与其否定形式互斥。
- (3) 互斥动作导致的互斥: 获得此命题的所有动作之间具有互斥关系。

显然第 1、2 类命题互斥独立于规划图结构, 不随规划图的扩展而变化; 第 3 类型命题互斥依附于规划图结构, 随规划图的扩展而变化。

图规划方式属于类经典规划范畴, 图规划算法是可靠的、完备的和可终止的算法<sup>[14]</sup>, 当存在规划解时, 其一定可以找到规划解, 因此应用图规划方法进行安全分析, 不会遗漏不安全状态的可达授权路径。图规划算法是典型的不动点算法 (Fixed-Point), 具有良好的算法效率。在算法中, 动作和命题之间存在的互斥关系可以方便地表示, 这使得领域命题互斥关系可以方便地表述和运用。

4.2 关于动作与命题互斥的推论

根据第 3 节所述转换过程所获得的领域模型的特点, 可以得出如下推论。

**推论 1.** 动作无删除效果。

说明: 根据 3.3 节和 3.4 节所述的转化过程, 出现删除效果的只有 Revoke 动作, 由于领域公理 2 的存在, Revoke 动作的删除效果转换为添加“un 谓词”形式。因此所有动作中不存在删除效果。

**推论 2.** 不会出现第 1、2 类动作互斥。

说明: 由于不存在删除效果, 或者说删除效果由

产生“un 谓词”效果取代, 使得第 2 类动作互斥不存在, 同时, 使得第 1 类动作互斥变为动作之间的效果互斥, 从而转换为第 3 类命题互斥, 而不形成动作互斥。

**推论 3.** 不会出现第 2 类命题互斥。

说明: 由推论 1 可知, 动作无删除效果, 因而不会出现否定命题, 也就不会出现第 2 类命题互斥。

4.3 领域公理的处理

规划问题求解前, 初始状态中需要声明所有真命题。对一个具有  $K$  个角色的可达性分析实例而言, 由于“un 命题”的出现, 其对应的规划图初始层就需要声明  $K$  个命题 (包括“un 命题”), 这将导致图扩展阶段出现大量的命题互斥和动作互斥, 既不利于规划图扩展, 又影响解提取的效率。事实上, 并不需要声明“un 命题”, 我们可以采用一种更灵活的方法处理这些“un 命题”。这一方法的核心思想是“在初始状态下, 并不显式声明‘un 命题’, 在规划图的扩展过程中需要的时候, 使用领域公理 DA2 动态添加”。以图 4 为例详细阐述这一处理过程, 如图 5 所示。在图 4 中, 如果初始命题层中存在  $unR$  命题, 即不存在  $R$  命题时, 常规的图规划算法会通过 NooP 动作传递这些“un 命题”至当前层, 如图 4 中的方式①所示, 我们称之为 NooP 方式。图 5 所示的处理过程实质上是删减了“un 命题”从初始层经过 NooP 动作传递到当前层的这一过程, 取而代之, 使用领域公理 DA2 来动态提供“un 命题”, 如图 4 中的方式②所示, 我们称之为 DA2 方式。问题在于, 以 DA2 方式替代 NooP 方式, 是否会影响规划问题的可解性?

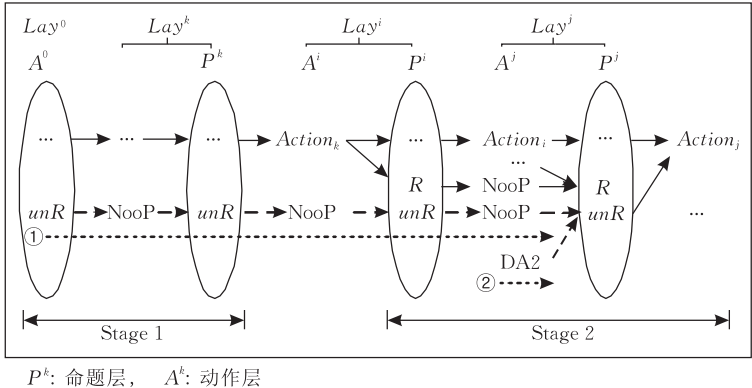


图 4 领域公理 DA2 的使用

**定理 1.** 使用 DA2 方式替代 NooP 方式, 不会影响规划问题的可解性。

证明. 分情况讨论以 DA2 方式替代 NooP 方式是否会影响规划问题的可解性。

情形 1.  $Lay^j$  层不存在某命题  $R$ 。

显然, 初始层也不存在命题  $R$  (否则将通过 NooP 动作传递到  $Lay^j$  层), 因此, 初始层肯定存在  $unR$  命题。在 NooP 方式下,  $unR$  命题经 NooP 动作

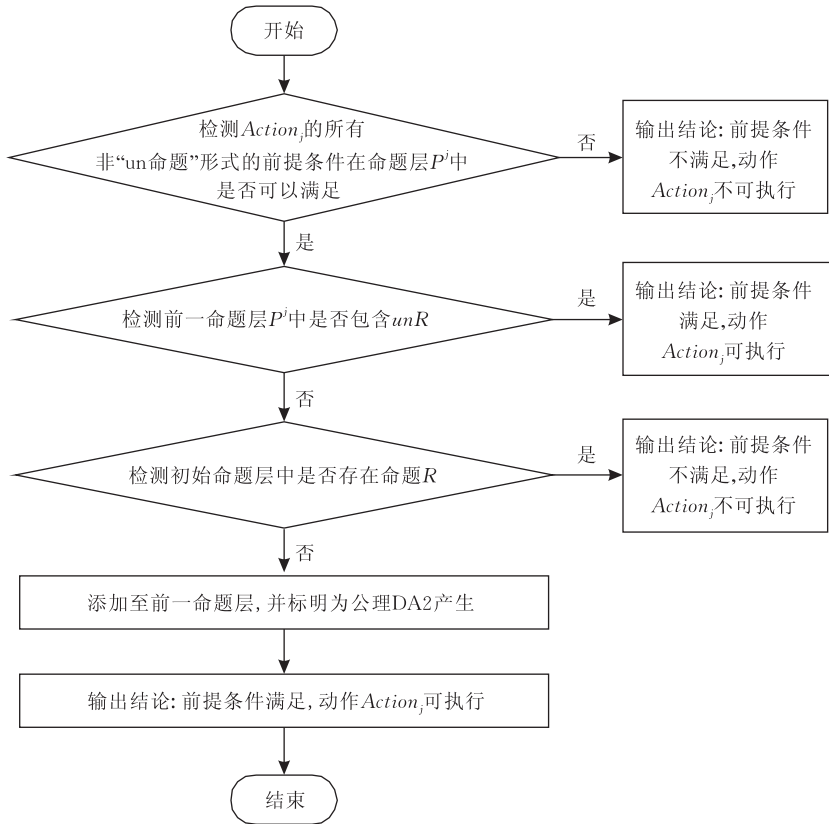


图 5 动作  $Action_j$  执行条件判断流程

传递到  $Lay^j$  层. 同样, 再 DA2 方式下运用领域公理, 亦可以在  $Lay^j$  层中添加  $unR$  命题. 然而, 差别在于: 相对于 NooP 方式而言, 由 DA2 方式产生的  $unR$ , 之前所有层中并不出现包含  $unR$  命题的动作互斥或命题互斥, 如果删除这些互斥是否影响问题的可解性? 由推论 2 可知, NooP 动作和其他动作只产生第 3 类互斥. 由于推论 3 可知, 产生 NooP 动作与其他动作互斥的原因是其前提条件之间存在第 3 类命题互斥或领域命题互斥中的  $(R, unR)$  形式. 由于不存在  $R$ , 所以只存在第 3 类命题互斥, 即获得此命题的所有动作之间互斥, 这些动作之间的互斥又是由于先前的第 3 类命题互斥产生, 由此递归推论, NooP 动作与其他动作产生动作互斥的原因是初始层中  $unR$  命题与其他命题形成的第 3 类命题互斥. 由于初始层的互斥只存在领域互斥命题 (类似于命题互斥对  $(unR, R)$ ), 上述的命题互斥并不存在. 故可知, 在 NooP 动作传递命题  $unR$  至当前层的过程中不产生动作互斥, 这和通过 DA2 方式一致. 因而, 在情形 1 所示情况下, 以 DA2 方式代替 NooP 方式并不改变规划问题的可解性.

情形 2. 在  $Lay^j$  层存在某命题  $R$ .

如果  $R$  出现在初始层, 则初始层命题中不存在

$unR$  命题, 故所以 NooP 方式下  $unR$  不会经 NooP 动作传递到  $Lay^j$  层. 同样, DA2 方式下领域公理亦不能使用来产生  $unR$  命题. 在这种情况下 DA2 方式和 NooP 方式保持一致.

如果  $R$  并不出现在初始层, 而是通过中间层动作的效果产生, 如图 4 所示, NooP 方式下,  $unR$  在初始层  $Lay^0$  存在, 并经 NooP 动作传递到  $Lay^j$  层, 使得  $Lay^{j+1}$  层动作  $Action_j$  的前提条件得以满足. 在 DA2 方式下, 也可以应用领域公理在  $Lay^j$  产生命题  $unR$ , 使得  $Lay^{j+1}$  层动作  $Action_j$  的前提条件得以满足. 问题在于通过 NooP 方式和 DA2 方式在  $Lay^j$  产生命题  $unR$  对于问题的可解性是否等价? 这需要我们考察图规划的解抽取过程:

如果在  $Lay^j$  层,  $unR$  与  $R$  位于同一子目标集合, 则抽取解失败, 这点 NooP 方式可以通过  $Lay^{j+1}$  层动作之间存在的互斥来判断, 而 DA2 可以通过  $Lay^j$  层的命题互斥来判断, 由第 3 类命题互斥的构成特征可以推出, 两者的判断结果是一致的.

如果在  $Lay^j$  层中,  $unR$  与  $R$  位于不同子目标集合中, 则需要对比 NooP 方式和 DA2 方式下规划图中的相关的动作互斥对. 由情形 1 的推理过程可知: 在图 4 中的 Stage 1 阶段, NooP 与 DA2 两种方式



构建的规划图相同;在 Stage 2 阶段的每层中,NooP 方式会增加一些动作互斥,增加的动作互斥仅包含 NooP 动作和产生命题  $R$  的动作之间的互斥. 由于  $unR$  与  $R$  位于不同子目标集合中,增加的互斥动作也位于不同的子目标集合中,并不妨碍子目标的解抽取过程,因此,在情形 2 所示情况下,应用 DA2 方式取代 NooP 方式也就不会影响问题的可解性.

证毕.

在图规划扩展过程中,我们可以使用 DA2 方式代替 NooP 方式,来缩减命题层规模,提高规划图的扩展和提取阶段的效率.

4.4 图规划算法的改造

由于在图规划算法的扩展阶段中使用了 DA2 方式,需要修改 Expand 程序和 GP-Search 程序,如图 6 所示.

在 Expand 程序中,判断可执行动作时,根据上述原理,使用领域公理来添加“un 命题”到前一层中的命题层中,并修改数据结构,添加 Hash 表类  $DAP_i$ ,记录各命题层中来自领域公理的“un 命题”. 在 GP-Search 程序中,添加对子目标集内互斥命题的判断,同时,判断子目标是否来自领域公理,如果是,则该子目标可达,转而判断下一个子目标是否可达.

```
Expand( $\langle P_0, A_1, \mu A_1, P_1, \mu P_1, DAP_1, \dots, A_{i-1}, \mu A_{i-1}, P_{i-1}, \mu P_{i-1}, DAP_{i-1} \rangle$ )
 $A_i \leftarrow \{a \in A \mid Adapted(a, P_{i-1}, \mu P_{i-1})\}$ 
...
end
GP-Search( $G, g, \pi_i, i$ )
if  $g = \emptyset$  then do
...
else do
if  $(p, q) \in \mu P_i$  and  $p, q \in g$  return failure
select any  $p \in g$ 
while( $g \notin DAP_i$ ) do
...
end
Adapted( $a, P_{i-1}$ )
for each  $P \in a.precondition$ 
if  $P \notin P_{i-1}$  then return false
else
if  $P$  like  $un-p$  then
if  $p \notin init-P$  then  $P_{i-1} \cup \{P\}, DAP_{i-1} \cup \{P\}$ 
else return false
else return false
return true
end
```

图 6 改进 Graphplan 程序

4.5 安全分析实验系统

基于改进的 Graphplan 算法,运用 Java 语言,开发了可视化的安全分析实验系统,系统基本框架如图 7 所示,图中虚线框表示需要根据具体的应用环境进行整合处理. 实验系统可以在编译环境 Eclipse3. 3 中运行,亦可以 Applet 方式集成到 Web 系统.

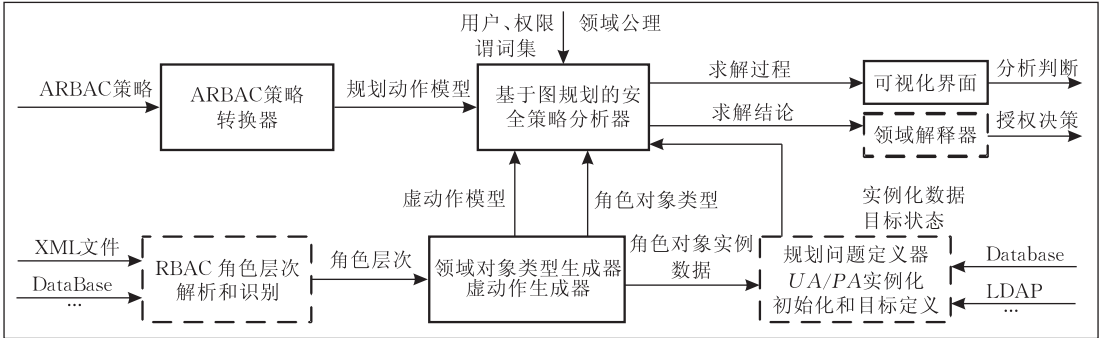


图 7 安全分析实验系统框架图

5 应用范例

以图 1 为例,根据系统上层策略知:设计陈述(DRP)和设计评审(DRM)为静态互斥角色,任意用户不能同时承担 DRP 和 DRM. 假定:相关的管理策略如表 1 所示,存在安全分析实例:某工程师(ENG)是否可以同时承担 DRP 和 DRM? 对这一问题的否定回答,表明系统处于安全状态.

表 1 can\_assign 管理策略

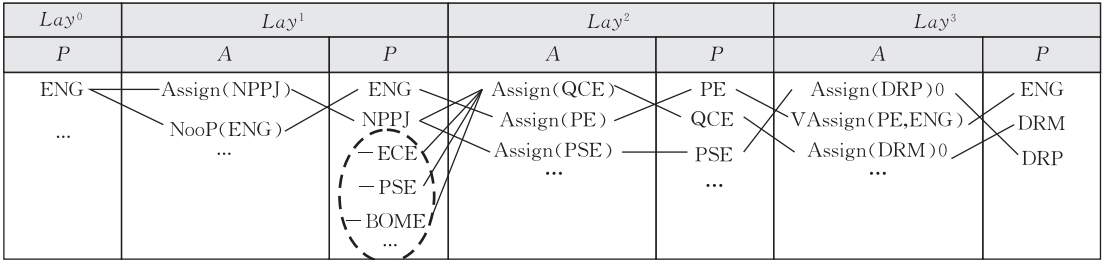
序号	安全管理员	前提条件	目标角色集
P1	EDSO	ENG	PE, QE
P2	EDSO	ENG	NPPJ
P3	EDSO	ENG	DIR
P4	PSO	DIR	DRC
P5	PSO	NPPJ	NPPL, ECE, PSE, BOME
P6	PSO	$(\neg ECE) \wedge (\neg PSE) \wedge (\neg BOME) \wedge NPPJ$	QCE
P7	PSO	$PSE \vee ECE \vee BOME \vee NPPL$	DRP
P8	PSO	$QCE \vee DRC$	DRM

运用本文所述方法将这一问题转化为规划问题, 相关信息如表 2 所示.

表 2 规划问题			
领域模型		规划问题	
相关命题数	32	初始状态	$playRole(ENG)$
动作数总数	64	目标状态	$playRole(ENG)$
虚动作数	15		$playRole(DRP)$
NooP 动作	18		$playRole(DRM)$

经运行试验系统, 得到如图 8 所示结论. 显然, 系统处于不安全状态. 一般而言, 系统的安全依赖于

可信用户的授权操作, 这里的可信用户指的是安全管理官员或者代理安全管理员履行管理职能的自动授权程序. 即使对于被委派有管理权限的可信用户, 由于策略集执行效果的非直观性, 仍然需要具有智能的策略分析程序予以支持. 如对于上述的策略分析问题, 如果将 DRP 和 DRM 作为领域约束, 加入到规划模型中, 则得到的是否定回答, 下层安全管理员得不到授权动作路径, 从而保证系统处于安全状态.



ENG:  $playRole(u, ENG)$ ;  $-ECE: unplayRole(u, ECE)$   
注: 本图由[附录]经处理后获得, 图中虚线椭圆所指说明此处应用领域公理产生了“un命题”

图 8 可达性问题实例的规划解

6 结 论

ARBAC 策略的安全分析是大型分布式系统保持安全状态的重要机制, 角色继承层次和角色静态互斥是这些系统的重要特征, 论文针对这类型安全分析问题, 运用智能规划方法和技术, 提出了完整的建模方法, 设计开发了专用于安全分析的实验系统, 以期推动安全分析方法走向应用实践. 同时, 本文探索了领域公理在规划过程中的应用模式, 尝试在规划过程中加入推理, 以期获得理论上的突破.

后续的研究可以集中在放宽研究对象限制, 考虑更多 ARBAC 因素(势约束、最小权限准则等)的情况下的安全分析方法上. ARBAC 管理策略的制定具有一定的盲目性, 如何通过授权路径优化分析进行调整和优化不失为一个研究方向. 此外, 研究领域对象具有继承关系的规划问题具有一定的研究价值和应用价值.

致 谢 感谢项目组给予的支持, 感谢参考文献作者提供了宝贵的参考素材!

参 考 文 献

[1] Ferraiolo David, Kuhn Richard. Role-based access controls//Proceedings of the 15th NIST-NCSC National Computer Security Conference. Baltimore, MD, 1992: 554-563

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

[3] Sandhu Ravi, Bhamidipati Venkata, Munawer Qamar. The ARBAC97 model for role-based administration of roles. ACM Transactions on Information and System Security, 1999, 2(1): 105-135

[4] Harrison M A, Ruzzo W L, Ullman J D. Protection in operating systems. Communications of the ACM, 1976, 19(8): 461-471

[5] Li N H, Winsborough W H, Mitchell J C. Beyond proof-of-compliance: Safety and availability analysis in trust management//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, 2003: 123-139

[6] Li N H, Tripunitara M V. Security analysis in role-based access control//Proceedings of the 9th ACM Symposium on Access Control Models and Technologies (SACMAT 2004). New York, 2004: 126-135

[7] Munawer Q, Sandhu R. Simulation of the augmented typed access matrix model (ATAM) using roles//Proceedings of the International Conference on Information and Security. Shanghai, China, 1999

[8] Yang Qiu-Wei, Hong Fan, Yang Mu-Xiang et al. Security analysis on administrative model of role-based access control. Journal of Software, 2006, 17(8): 1804-1810(in Chinese)  
(杨秋伟, 洪帆, 杨木祥等. 基于角色访问控制管理模型的安全性分析. 软件学报, 2006, 17(8): 1804-1810)

[9] Sasturkar A, Yang Ping, Stoller S D et al. Policy analysis for administrative role based access control//Proceedings of

the 19th IEEE Workshop on Computer Security Foundations. Venice, Italy, 2006: 183-196

[10] Lifschitz E. On the semantics of STRIPS//Proceedings of the Reasoning about Actions and Plans. Timberline, Oregon, 1987: 1-9

[11] Mcdermott D. PDDL — The planning domain definition language. Yale University, New Haven, Connecticut, USA: Technical Report CVC TP-98-003/DCS TP-1165, 1998

[12] Fox M, Long D. PDDL 2. 1: An extension to PDDL for ex-

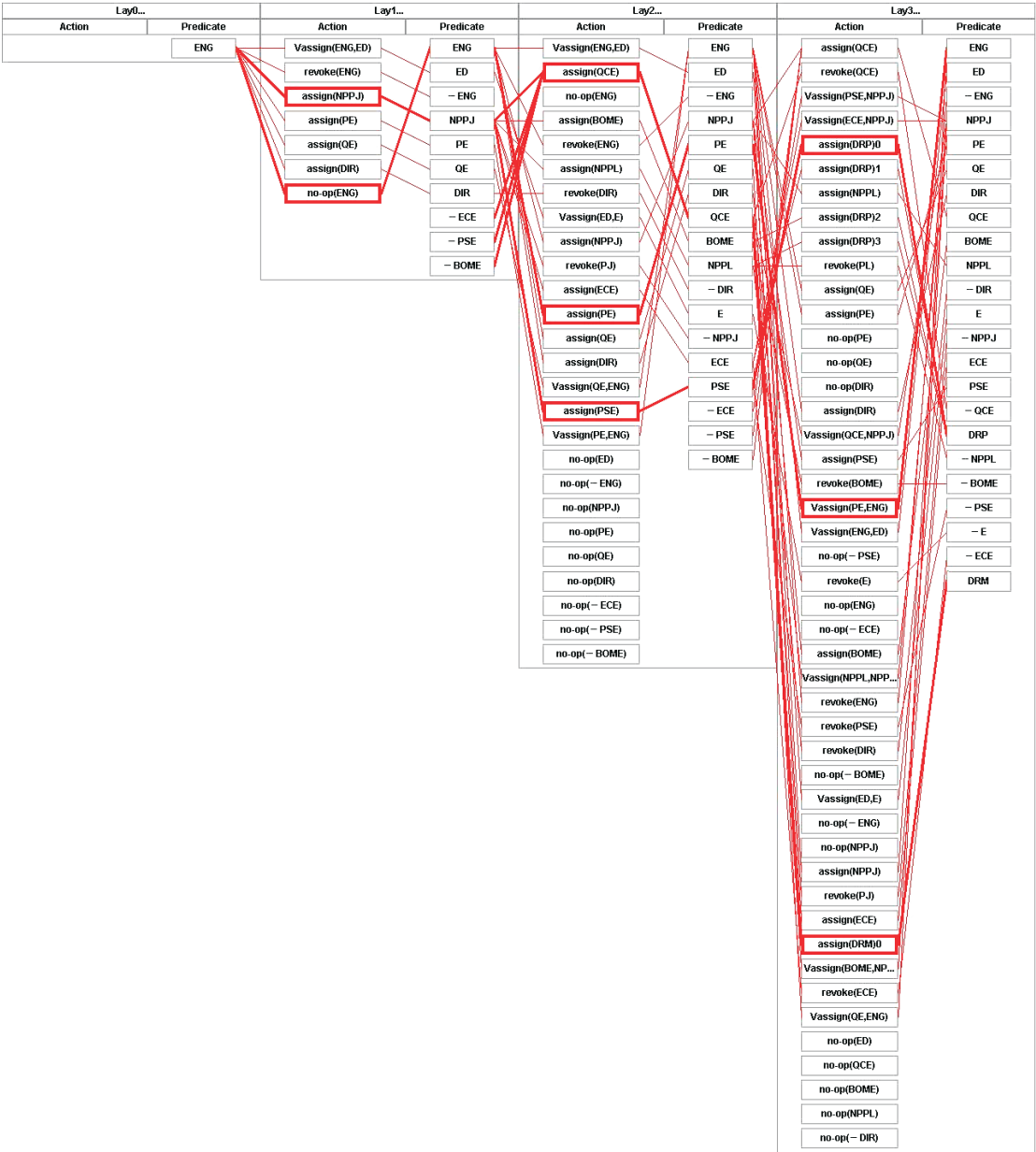
pressing temporal planning domains. Journal of Artificial Intelligence Research, 2003, 20: 61-124

[13] Blum A, Furst M. Fast planning through planning graph analysis//Proceedings of the 14th International Joint Conference on Artificial Intelligence. Quebec, Canada, 1995: 1636-1642

[14] Ghalilab Malik, Nau Dana, Traverso Paolo. Automated Planning Theory and Practice. San Francisco, CA, USA: Morgan Kaufmann Publishers, 2004

附录. 策略安全性分析实验系统运行结果.

由于屏幕的限制,本图由 4 个拷屏图经 photoshop 合并而成.





**LIU Qiang**, born in 1978, Ph. D. candidate. His research interests include AI planning, role-based access control.

**JIANG Yun-Fei**, born in 1945, professor, Ph. D. supervisor. His research interests include automate reasoning, AI planning and model-based diagnosis.

**RAO Dong-Ning**, born in 1977, Ph. D. candidate. His research interests focus on AI planning

**Background**

This paper is supported by the National Nature Science Foundation of China under grant No. 60773201, namely the Research on Extraction Method of Domain Knowledge and Reasoning Algorithms on Domain Knowledge in AI Planning Field. This project focuses on the extraction and application of domain knowledge during the resolving process of AI planning problem in order to improve the efficiency of planner. The team of this project had designed some effective method in extraction of domain knowledge. This paper engaged in the application of AI planning and the application method of domain axiom when resolving planning problem.

The work of this paper involved in two fields, AI plan-

ning and Information security. Safety analysis is the prerequisite mechanism for distributed access control system. Now how to deal with role hierarchy and static mutual exclusion roles when executing safety analysis is a difficult task when executing safety analysis. This paper focuses on the Graphplan method, a classical AI planning method, to perform the safety analysis and settle the expression and application problem of role hierarchy and static mutual exclusion roles effectively by importing domain axioms and domain constraints into the domain model of safety analysis problems. It will extend the application scope greatly, and provide an application mode of domain axiom when resolving planning problem.