计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20170250
55(8):1809-1825,2018

位置约束的访问控制模型及验证方法

曹 彦[1] 黄志球[1,2,3] 阚双龙[1] 彭焕峰[1] 柯昌博[1,4]
[1](南京航空航天大学计算机科学与技术学院 南京 211106)
[2](高安全系统的软件开发与验证技术工业和信息化部重点实验室(南京航空航天大学) 南京 211106)
[3](软件新技术与产业化协同创新中心 南京 210093)
[4](南京邮电大学计算机学院 南京 210023)
(caoyan926@nuaa.edu.cn)

Location-Constrained Access Control Model and Verification Methods

Cao Yan[1], Huang Zhiqiu[1,2,3], Kan Shuanglong[1], Peng Huanfeng[1], and Ke Changbo[1,4]
[1](*School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing* 211106)
[2](*Key Laboratory of Safety-Critical Software (Nanjing University of Aeronautics and Astronautics), Ministry of Industry and Information Technology, Nanjing* 211106)
[3](*Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing* 210093)
[4](*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023)

Abstract With the advent of Internet of things and cyber-physical systems, location-constrained access control systems need to consider security requirements of cyber spaces and physical spaces simultaneously, because the boundary between the physical and the cyber world becomes unclear in these new paradigms. However, the most existing access control models consider physical and cyber security separately, and they are oblivious to cyber-physical interactions. Authorization models are needed to help the security policy design and express higher-level organizational security rules. Firstly, the environment model (EM) and location-constrained role-based access control (LCRBAC) model are proposed. The environment model is presented for describing the static topology configuration of cyber space and physical space. The LCRBAC model is used to describe dynamic behaviors of cyber entities and physical entities. Secondly, given the bigraphs and bigraphs reactive systems that describe the environment configuration and entities behaviors respectively, a labeled transition system is obtained by applying reaction rules to the environment configuration. Thirdly, policy modification proposals are proposed for deadlock states, violation states, and unreachable states based on the verification results on the labeled transition system. Finally, a case study concerned with a bank building automation access control system is conducted to evaluate the effectiveness of the proposed approach.

Key words location-constrained access control system; model checking; bigraphs; reaction rules; verification

收稿日期:2017-04-10;**修回日期**:2018-01-18

基金项目:国家"八六三"高技术研究发展计划基金项目(2015AA015303);国家自然科学基金项目(61772270,61602262,61602237);江苏省自然科学基金青年项目(BK20150865,BK20170809)
This work was supported by the National High Technology Research and Development Program of China (863 Program) (2015AA015303), the National Natural Science Foundation of China (61772270, 61602262, 61602237), and Jiangsu Natural Science Foundation of China (BK20150865, BK20170809).

通信作者:黄志球(zqhuang@nuaa.edu.cn)

摘 要 随着物联网和信息物理融合系统等新一代信息技术的发展,位置约束的访问控制系统的安全性需求不仅体现在虚拟的信息空间,还体现在现实的物理空间.如何在这种新需求下制定位置约束的访问控制模型与验证方法成为保证访问控制系统安全的关键所在.首先提出位置约束访问控制模型,包括LCRBAC模型和EM模型,实现对信息空间和物理空间的静态结构以及两空间中实体动态行为的刻画;其次利用偶图和偶图反应系统建模位置约束访问控制模型,生成访问控制策略标注转移边的标号变迁系统;然后根据标号变迁系统验证结果,提出针对死锁状态、违反状态和不可达状态的策略修改方案;最后通过银行访问控制系统实例分析说明所提方法能够对信息空间和物理空间以及两空间交互行为的访问控制策略进行建模和验证.

关键词 位置约束访问控制系统;模型检测;偶图;反应规则;验证

中图法分类号 TP311

随着无线定位技术、无线通信技术的发展以及移动终端的普及,基于位置的信息服务已经深入人们的日常生活.位置服务几乎涵盖了人类生活的方方面面,包括军事、交通、物流等[1-3].但位置服务为人们生活带来便利的同时,其安全问题受到越来越多的关注.访问控制作为一种有效的网络安全防护和保护手段,一直备受人们的青睐,其通过限制主体对虚拟信息空间中客体的访问权限,保证客体不被非法使用和访问.为保证基于用户位置服务中网络资源的安全性,现已有大量研究人员针对位置服务在传统访问控制模型的基础上进行了位置属性的扩展,把用户当前的位置信息作为定义用户是否能够获得访问权限的限制之一[4].随着微机电系统技术、传感器技术等在物理设备中的应用,物理设备已逐步具有计算能力、感知能力和通信能力,从而催生了以实现虚拟信息世界与现实物理世界高度融合为目标的新一代信息技术,如物联网、信息物理融合系统.这也使得位置服务访问控制策略的制定在该场景下具有了新内涵.由于物理世界的融入,访问控制系统不仅要关注位置对虚拟信息空间中访问行为的约束,还要关注其对物理空间以及两空间交互行为的约束[5].如何针对新需求下的位置服务建立访问控制模型以及验证模型的正确性,是保证新一代信息技术下位置服务安全的一个重要方面[6].

传统的访问控制模型,包括强制访问控制(mandatory access control, MAC)、自主访问控制(discretionary access control, DAC)和基于角色的访问控制模型(role based access control, RBAC)[7].但以上模型是非上下文敏感的,对用户的位置信息都无法进行描述.虽已有大量研究人员在传统访问控制模型上进行位置属性扩展,但现有的模型与验证方法主要存在如下问题:

1) 已有的位置约束访问控制模型,多是在传统访问控制模型的基础上,引入位置属性对角色、权限和客体进行限制,实现建立用户-角色赋予/撤销、角色-权限赋予/撤销、角色层次、职责分离等关系或约束时符合位置属性.但这些模型大多针对信息空间,不能描述物理空间的访问行为和实体的动态行为.

2) 已有的位置约束访问控制模型验证方法,多数未考虑物理空间访问行为以及实体动态行为的建模.文献[8]虽利用环境演算[9]能够解决已有模型无法表达物理空间访问策略的限制,但因环境演算对连接关系不能很好地表达,导致其对信息空间访问策略的建模能力受限.

针对以上2个问题,本文提出位置约束访问控制模型以及基于该模型的正确性验证方法和策略修改方案.主要贡献有3个方面:

1) 提出同时关注信息空间与物理空间的位置约束访问控制(location-constrained role-based access control, LCRBAC)模型和描述系统运行环境的环境模型(environment model, EM).利用LCRBAC模型实现物理空间、信息空间及两空间交互的访问控制策略的制定,EM模型实现对信息空间和物理空间拓扑结构的刻画.

2) 利用由英国学者Milner[10]提出的偶图和偶图反应系统建模位置约束访问控制模型并给出相应的转换规则.利用偶图在EM模型的基础上建立初始模型,偶图反应规则描述LCRBAC模型定义的位置约束访问控制策略,通过初始模型与反应规则中反应物的匹配,生成以访问控制策略标注转移边的标号变迁系统.

3) 提出访问控制策略修改方案.根据标号变迁系统对安全属性的验证结果,提出针对死锁状态、违反状态和不可达状态的策略修改方案.

1　相关工作分析

为实现访问控制中位置属性的描述,国内外的研究人员在传统访问控制模型基础上提出具有上下文约束的访问控制模型.表1从位置约束的访问控制模型与访问控制策略的验证2个方面对相关工作进行比较分析.

Table 1　Comparison of Related Works

表1　相关工作比较

Model	Reference	Policy Specification					Policy Verification	
		CS	PS	CPS	EL	EM	FD	VT
GEO-RBAC	Ref [11]	√	×	×	√	×	×	×
LRBAC	Ref [12]	√	×	×	√	×	Z Language	×
SC-RBAC	Ref [13]	√	×	×	√	×	×	×
LOT-RBAC	Ref [14]	√	×	×	√	×	×	×
STRBAC	Ref [15]	√	×	×	√	×	×	×
GSTRBAC	Ref [16-17]	√	×	×	√	×	UML/OCL or Timed-automata	USE or UPPAL
GemRBAC	Ref [18]	√	×	×	√	×	UML/OCL	×
A Spatio-Temporal Access Control Model	Ref [19-20]	√	×	×	√	×	CPN or Alloy	CPN Tools or Alloy Analyzer
STRBAC-PS	Ref [21]	⊙	√	×	√	⊙	Alloy	Alloy Analyzer
FPM-RBAC	Ref [22-23]	⊙	√	⊙	√	√	Ambient Calculus	Java Language and NuSMV
LCRBAC	Our Work	√	√	√	√	√	Bigraph and BRS	BigMC

Notes: √: support; ×: no support; ⊙: partial support; CS: cyber space; PS: physical space; CPS: the interaction between cyber spaces and physical space; EL: support for entities location; EM: support for entities mobility; FD: formal description; VT: verification tools.

在位置约束的访问控制模型方面,GEO-RBAC[11],LRBAC[12],SC-RBAC[13]在RBAC模型的基础上进行了位置属性的扩展,用于约束角色、权限和客体以及模型中关系的建立.之后又陆续提出了有关位置-时序约束的访问控制模型[14-20],在模型中同时考虑位置和时间对实体的约束.但以上模型的定义大多是针对信息空间,并没有考虑物理空间和实体移动特性.因此,现有模型并不适用于物联网、信息物理融合系统等范型.1)由于物理空间的引入,需要实现物理访问控制与信息访问控制的融合.物理空间划定了访问控制策略在物理世界的作用范围,因此,空间拓扑结构将约束访问控制策略的制定;另一方面需要考虑两空间交互策略,包括物理空间状态对信息空间访问行为的约束和信息空间状态对物理空间访问行为的约束.2)拓扑空间中实体移动行为的描述,包括主体的移动和客体的移动.已有的位置约束访问控制模型,大多是静态的描述位置关系,如SC-RBAC,GSTRABC等模型中定义(teacher,class1)和(teacher,class2)表示用户在class1和class2都可以赋予teacher角色,但不能表示teacher从class1至class2的移动行为.表1从是否支持信息空间、物理空间及两空间交互、是否支持实体位置描述以及实体位置动态变化5个方面对相关工作进行比较分析.

在位置约束的访问控制模型验证方面,已提出多种形式化建模方法,包括Z语言[12]、UML/OCL[16,18]、UML to Alloy[20]、CPN[19]、时间自动机[17]和环境演算[22-23].Z语言缺乏自动化的检测工具;UML/OCL是一种半形式的验证方法,并不能验证行为属性,因此文献[20]提出UML to Alloy方法,将UML转换到形式化的Alloy语言进行模型检测,但UML至Alloy转换的正确性是无法保证的;CPN和时间自动机并不能直观地表达位置属性,需要不断地定义变量来表达位置以及位置之间的关系;文献[23]中利用环境演算建模访问控制模型,环境演算以描述进程间的位置移动性为主要特征,对于连接关系及其变化并不能很好地表达,导致其对信息空间访问行为的描述能力有限.表1从是否对模型有形式化的建模方法以及工具支持2个方面对相关工作进行比较分析.

2 位置约束的访问控制模型

信息物理融合系统和物联网都是由传感器节点、执行器节点、计算系统和网络系统组成. 传感器节点实现对物理世界的感知,将感知信息通过网络系统传递给计算系统,计算系统按照预先设定原则处理信息,并将处理结果通过网络系统发送给执行器节点,最后由执行器节点接收消息,实现对物理世界的控制. 依据以上系统的组成构件,2.1 节引入位置约束访问控制系统应用场景[21,24],并对系统中基本概念进行分析;2.2 节根据概念分析结果提出 LCRBAC 模型和 EM 模型.

2.1 应用场景

图 1 为某银行部署结构图,该部署结构图展示了银行的物理空间结构和信息空间结构. 访问控制管理系统部署于银行小云服务器(cloudlet),控制着主体对客体的访问行为以及物理空间出入行为.

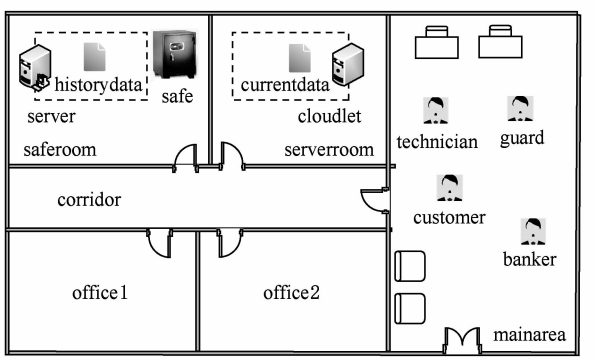

Fig. 1 Bank deployment diagram

图 1 银行部署结构图

物理空间用于描述物理实体及相应位置、区域人员及相应位置、建筑分布. 物理实体是指物理空间中与数据信息无关的硬件设备. 图 1 中银行的物理实体为资金存储保险柜(safe). 资金存储保险柜主要用于银行资金的储备,通过在保险柜中嵌入感知器,感知保险柜的开关状态和位置信息. 银行区域中的人员按照角色划分为客户(customer)、银行主管(guard)、银行职员(banker)和技术维护人员(technician). 利用用户所带手机(phone)对进入区域中的人员进行位置感知,银行主管、银行职员和技术维护人员通过手机登入访问控制管理系统实现角色分配,其他未登入用户分配角色为客户. 物理实体和人员位置在图 1 中已清晰标注. 银行建筑分布包括大厅(mainarea)、走廊(corridor)、安全屋(saferoom)、职员办公室(office1,office2)和服务器房间(serverroom). 大厅主要是为用户提供柜面服务,所有人员可自由出入;走廊连接各个房间,除用户之外其他人员可自由出入;安全屋内放置一台服务器和保险柜,只有银行主管具有权限可以出入该房间并读取客户历史交易信息;职员办公室为银行职员办公区域,银行主管和银行职员可自由出入;服务器房间内放置小云服务器,为银行日常工作提供技术支撑,银行主管和技术人员可以进入. 每个房间的门都具有执行器,控制着门的开关.

信息空间用于描述信息实体及位置. 信息实体是指数据信息. 银行的信息实体包括客户历史交易记录(historydata)、客户当天交易记录(currentdata). 每个信息实体的位置在图 1 中已清晰标注. 除物理实体和信息实体之外,还有一类特殊的实体,称为混合实体,其是对能够存储信息实体的物理实体的一种描述. 图 1 中混合实体包括小云服务器、安全屋中服务器(server)以及手机. 为简单起见,图 1 利用人员节点表示手机节点.

信息空间和物理空间的交互既可以是通过物理空间中的信息控制信息空间的访问行为,如"只有在安全屋,银行主管才能读取用户历史交易信息",也可以通过信息空间中的行为约束物理空间访问,如"银行主管只有删除客户历史交易记录才能离开安全屋". 物理实体、信息实体和混合实体统称为客体. 客体和人员统称为实体. 银行区域内通过网关实现实体间互联. 文中不关注网络系统,假设网络系统是高可靠的.

2.2 LCRBAC 模型与 EM 模型

在不同领域中提出的位置描述主要分为 2 类:层次式的(比如房间)和笛卡儿的(比如 GPS). 由于层次式具有良好的用户可读性,且能很好地表达位置之间的关系[13],本文采用它来表达位置. 层次式的位置模型可把物理空间结构分为不同的层次,如案例中的位置关系采用层次式描述如图 2 所示:

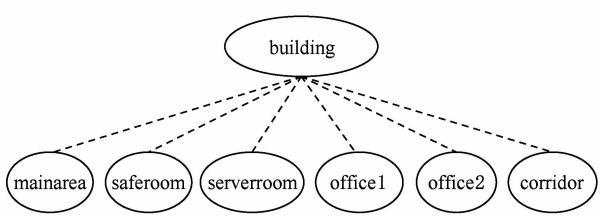

Fig. 2 Hierarchical spatial tree

图 2 层次空间树

位置约束访问控制系统运行的物理空间,划定了访问控制策略在物理世界的作用范围. 用 *Loc*

表示建筑分布中空间区域集合,$Loc=\{l_1,l_2,\cdots,l_n\mid n\in\mathbb{N}_+\}$,$l_i(i\in\mathbb{N}_+)$为某个具体物理空间区域,称为物理位置域,如案例中包括 6 个物理位置域.

定义 1. 物理位置域邻近关系. 在层次空间树中,如果物理位置域 l_i 与物理位置域 l_j 为兄弟节点,则称物理位置域 l_j 与物理位置域 l_i 为邻近关系,表示为 $l_i\infty l_j$.

定义 2. 物理位置域包含关系. 在层次空间树中,如果物理位置域 l_i 为物理位置域 l_j 的孩子节点,则称物理位置域 l_j 包含物理位置域 l_i,表示为$l_i\subseteq l_j$.

在实际的物理空间中,许多不同物理位置域具有相同的访问权限,提出逻辑位置角色的概念实现对相同访问权限的物理位置域的统一.

定义 3. 逻辑位置角色. 逻辑位置角色代表物理空间和信息空间中特定的访问权限.

由所有逻辑位置角色组成的集合表示为 $LocR=\{lr_1,lr_2,\cdots,lr_k\mid k\in\mathbb{N}_+,k\leqslant n\}$,$lr_i(i\in\mathbb{N}_+)$为某个具体逻辑位置角色,$n$ 为物理位置域个数.

具有包含和邻近关系的物理位置域映射为逻辑位置角色时,需要根据物理位置域访问权限的不同映射为不同的逻辑位置角色. 如图 3 所示,当 l_i 和 l_j 具有相同的访问权限时,l_i 和 l_j 物理位置域映射为同一个逻辑位置角色 lr_i;当 l_i 和 l_j 区域的访问权限不同时,映射为不同的逻辑位置角色 lr_i 和 lr_j. 注意,在包含关系的物理位置域具有不同的访问权限时,l_i 映射为逻辑位置角色 lr_i,灰色区域映射为逻辑位置角色 lr_j. 因此,不同的逻辑位置角色代表不同的权限范围.

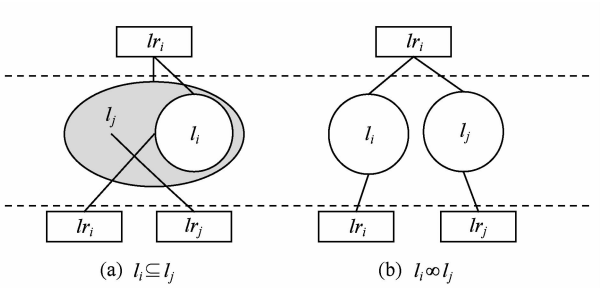

Fig. 3　Physical local to logical location role mapping

图 3　物理位置域到逻辑位置角色映射

定义 4. 物理位置域与逻辑位置角色之间映射函数. 物理位置域与逻辑位置角色的映射函数为 f:$Loc\rightarrow LocR$,表示物理位置域 l_i 到逻辑位置角色 lr_i 的映射,函数 f 为多对一的关系. 而函数 f':$LocR\rightarrow Loc$ 表示逻辑位置角色 lr_i 到物理位置域 l_i 的映射,函数 f'为一对多的关系.

传统的访问控制模型中,RBAC 模型是目前公认最有效的模型,相比 MAC 和 DAC 具有简单的表达能力,其通过将权限与角色相关联,用户通过成为适当角色获取相应权限. 本文在 RBAC 的基础上提出 LCRBAC 模型,以下先给出 RBAC 模型定义.

定义 5. RBAC 模型[7]. RBAC 模型定义如下:

1) U,R,OP,O,S. 其中,U 表示用户集合;R 表示角色集合;OP 表示操作集合;O 表示客体集合;S 表示会话集合.

2) $UA\subseteq U\times R$ 表示用户和角色之间多对多关系.

3) $P\subseteq OP\times O$ 表示权限集合.

4) $PA\subseteq P\times R$ 表示权限和角色之间多对多关系.

5) $S\rightarrow U$ 表示会话到用户的映射函数.

6) $S\rightarrow 2^R$ 表示会话到角色的映射函数.

针对信息空间,现有的位置约束访问控制模型,如 GSTRBAC[16]是在 RBAC 中对角色、权限和客体进行位置属性关联.(r,lr_r)表示当用户的位置为 lr_r 时,用户可具有角色 r;(p,lr_p)表示只有在位置 lr_p,才能执行权限 p;(o,lr_o)表示客体 o 位于位置 lr_o. 因为权限 p 是由角色 r 执行,所以在 1 条策略中$(u,(r,lr_r)(p,lr_p))$权限 p 的位置 lr_p 与角色 r 的位置 lr_r 是一致的,即 $lr_p=lr_r=lr$. 因此在 LCRBAC 模型中策略修改为(u,r,p,lr),表示当用户 u 位于 lr 时,可具有角色 r 并获得权限 p. 针对物理空间,要描述用户出入行为,逻辑位置角色成为操作对象,策略描述为(u,r,op,lr). 通过以上分析,给出 LCRBAC 模型定义.

定义 6. LCRBAC 模型. LCRBAC 模型定义如下:

1) $U,R,OP,O,LocR$. 其中,U 表示用户集合;R 表示角色集合;OP 表示操作集合;O 表示客体及相应位置集合,为可选项;$LocR$ 表示逻辑位置角色集合.

2) $UA\subseteq U\times R$ 表示用户和角色之间多对多关系.

3) $OP\subseteq\{OPLocR,OPobjects\}$表示操作集合.

4) $OPLocR=\{\text{enter},\text{exit}\}$表示物理空间操作集合.

5) $OPobjects=\{Oph,Opp,Opc\}$分别表示混合实体、物理实体和信息实体操作集合,需根据具体需求定义.

6) $O \subseteq Objects \times LocO$ 表示客体与其位置之间一对多的关系.

7) $Objects = \{Physicalen, Hybriden, Cyberen\}$ 表示客体集合,由物理实体、混合实体、信息实体组成.

8) $LocO \subseteq LocR \cup Hybriden$ 表示客体位置集合.

9) $ObjLoco(o:Objects) \rightarrow 2^{LocO}$ 表示客体到位置的映射函数.其中:

① $ObjLoco(o:Physicalen) \rightarrow LocR$;

② $ObjLoco(o:Hybriden) \rightarrow 2^{LocR}$;

③ $ObjLoco(o:Cyberen) \rightarrow 2^{Hybriden \times LocR}$.

10) $PA \subseteq P \times R$ 表示权限和角色之间多对多关系.

11) $P \subseteq P_1 \cup P_2$ 表示访问权限的集合且 $P_1 \cap P_2 = \varnothing$.

12) $P_1 = 2^{OPLocR \times LocR}$ 表示物理空间中出入行为控制策略.

13) $P_2 = 2^{OPobjects \times Objects \times LocO \times LocR}$ 表示客体上操作行为的控制策略.

根据 LCRBAC 模型的定义,位置约束的访问控制策略有 2 种表达方式,分别为 $(U, R, OPLocR, LocR)$ 和 $(U, R, OPobjects\ (Objects, LocO), LocR)$.

1) $(R, OPLocR, LocR)$ 用于描述物理空间中主体出入行为的访问控制策略,如"银行职员进入走廊",表示为(banker,enter,corridor).

2) $(R, OPobjects, (Objects, LocO), LocR)$ 分 3 类:

① $(R, Opp, (Physicalen, LocO), LocR)$ 表示物理空间中主体在某位置对物理实体的访问策略,由于物理实体不可远程访问,所以 $LocO$ 与 $LocR$ 相等.如"在安全区域,银行主管可以打开安全屋中保险柜",表示为(guard,open,safe,saferoom).

② $(R, Opc, (Cyberen, LocO), LocR)$ 表示信息空间中主体在某位置对信息实体的访问策略.信息实体的位置包括 2 层结构,1 层为信息实体所处的混合实体,1 层为混合实体所在的逻辑位置角色区域.因为信息实体可以远程访问,$LocO$ 与 $LocR$ 可以不同.如"在安全区域,银行主管可以获得小云服务器上的用户当前交易记录",表示(guard,copy,(currentdata,cloudlet,serverroom),saferoom).

③ $(R, Oph, (Hybriden, LocO), LocR)$ 表示主体在某位置对混合实体的访问策略,其中,$LocO$ 与 $LocR$ 也可不同.如"在大厅区域,银行职员可以登入小云服务器",表示为(banker,login,(cloudlet,serverroom),mainarea).

因位置约束访问控制系统与空间拓扑结构紧密联系,以下给出系统运行环境模型定义.

定义 7. 系统运行环境模型.EM 模型为 8 元组 $EM = (LocR, Role, Object, LocO, Locrelation, RoleObject, RoleLocation, ObjectLocation)$:

1) $LocR, Role, Object, LocO$ 分别表示逻辑位置角色集合、角色集合、客体集合和客体位置集合;

2) $RoleLocation \subseteq Role \times LocR$ 表示当前环境下角色与位置关系集合;

3) $RoleObject \subseteq Role \times Object$ 表示当前环境下角色对客体访问关系集合;

4) $ObjectLocation \subseteq Object \times LocO$ 表示当前环境下客体与位置关系集合;

5) $Locrelation \subseteq LocR \times LocR$,表示物理空间可达关系,集合元素 (lr_i, lr_j) 表示从建筑物入口出发可以经 $f'(lr_i)$ 到达 $f'(lr_j)$.

定义 8. 逻辑位置角色等价关系.如果物理位置 $f'(lr_i)$ 可以执行的权限集合 P_{2i} 与物理位置 $f'(lr_j)$ 可以执行的权限集合 P_{2j} 相等,则逻辑位置角色 lr_i 与 lr_j 等价,表示为 $lr_i = lr_j$.

具有等价关系的逻辑位置角色 lr_i 和 lr_j 可以合并为一个逻辑位置角色 lr_k,且 $f'(lr_k) = f'(lr_i) + f'(lr_j)$,即具有相同访问权限的物理位置域赋予相同的逻辑位置角色,且逻辑位置角色对应的物理位置空间为相同访问权限物理位置域的和.如银行应用场景中 office1 和 office2 具有相同的访问权限,将这 2 个物理位置域都赋予逻辑位置角色 office,则逻辑位置角色 office 对应的物理位置域为 office1 区域与 office2 区域的和.具有等价关系的逻辑位置角色的合并,使每个逻辑位置角色的访问权限都不相同.

定义 9. 权限依赖关系.如果用户在执行权限 p_i 前一定要执行权限 p_j,则称 p_i 依赖于 p_j,表示为 $p_i \leqslant p_j$.如果逻辑位置角色 lr_i 的访问权限集合 P_i 中操作行为发生前一定存在逻辑位置角色 lr_j 的访问权限集合 P_j 中操作行为的发生,则称 P_i 依赖于 P_j,表示为 $P_i \leqslant P_j$.

定义 10. 逻辑位置角色包含关系.如果逻辑位置角色 lr_i 的访问权限 P_i 和逻辑位置角色 lr_j 的访问权限 P_j 之间存在 $P_i \leqslant P_j$ 依赖关系,则称逻辑位置角色 lr_j 包含逻辑位置角色 lr_i,表示为 $lr_i \subseteq lr_j$.

3　位置约束访问控制策略建模与验证

针对位置约束访问控制策略的建模,既要实现对 EM 模型定义的空间拓扑结构的形式化描述,也要实现对 LCRBAC 模型定义的位置约束的访问控制策略的形式化描述. 偶图和偶图反应系统是融合了 Pi 演算和环境演算的一种形式化建模方法,是同时强调位置和连接的图形化模型,并能通过反应规则描述位置或连接关系的动态变化. 因此,本文采用偶图和偶图反应系统建模 EM 和 LCRBAC 模型.

3.1　偶图和偶图反应系统

偶图和偶图反应系统不但具有完备的公理系统,而且提供了图形化的表示方法,相比进程代数等其他形式化方法,有利于软件开发人员和用户之间对系统理解的一致性[25]. 本节采用非形式化的方式介绍偶图和偶图反应系统的基本概念.

1) 偶图(bigraphs)

偶图用于描述静态结构,由位置图(place graph)和连接图(link graph)组成. 位置图用于表示各个节点之间的嵌套关系;连接图用于表示节点之间的连接关系. 位置图与连接图是相互独立的,是从不同视角对同一个偶图观测得到的不同结果. 以下结合图 4 对相关概念加以介绍,图 4(a)为一个偶图 F,图 4(b)(c)分别为 F 分解得到的位置图和连接图. 图 4(a)中虚线框表示一个区域(region),每个区域用一个自然数 n 标识,V_1,V_3,V_4,V_5 为节点标识(node),节点之间根据建模对象位置关系建立嵌套关系. 偶图中的每个节点对应控制(control)类型,控制是对相同类型节点的描述. 每个节点上的黑色圆点表示端口(port),端口之间通过边连接(link),连接分为封闭连接(closed link),如 e_1,e_2,开放连接(open link),如 x,y. x 和 y 为外部名(outer name),图 4 利用上方伸出的边表示外部名,从下方伸出的边表示内部名(inner name). F 的位置图 F^{P} 对应以区域数为根节点的森林,连接图 F^{L} 对应超图.

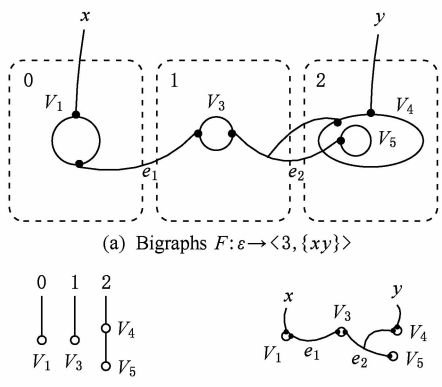

Fig. 4　Bigraphs F structure diagram

图 4　偶图 F 结构图

位置图是以序数集为对象的态射,$F^{\mathrm{P}}:m\to n$ 表示 F^{P} 有 m 个地点、n 个区域. 连接图是以名字集为对象的态射,$F^{\mathrm{L}}:X\to Y$ 表示 F^{L} 的内部名为 X、外部名为 Y. 偶图为位置图和连接图的合成,是以序数集和名字集为对象的态射,即 $F:\langle m,X\rangle\to\langle n,Y\rangle$. $\langle m,X\rangle$称为内部界面(inner face),$\langle n,Y\rangle$称为外部界面(outer face).

2) 偶图反应系统(bigraphs reactive system, BRS)

偶图反应系统用于描述动态结构,通过定义反应规则(T,T')对自身进行重构,反应规则中 T 称为反应物(redex),T'称为生成物(reactum). 反应物和生成物都是偶图. 反应规则可以根据具体的应用自由地加以定义. 如图 5 上面为反应物 T,图 5 下面为生成物 T',反应规则表示 V_3 节点位置的变化和 V_2 节点的删除,变迁过程中连接关系不变. 如果偶图或者偶图部分与反应物匹配,则将该偶图中与反应物匹配的部分替换成生成物.

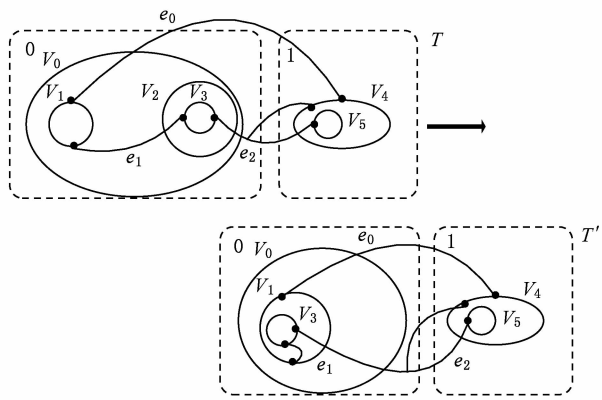

Fig. 5　Reaction rule

图 5　反应规则

偶图和偶图反应系统的图形表示具有直观性的特点,但是不利于系统的理解和处理,因此 Milner 等人提出了利用代数系统来描述偶图和偶图反应系统模型. 表 2 中给出了偶图和偶图反应系统的部分代数表示,具体可参看文献[25]. 相对于图形化的表示,代数系统便于系统的构建、演化和推导.

根据表 2,可得图 5 的项语言描述如下:

$$/x./y./z.V_0.(V_{1xy}\mid V_2.(V_{3yz}))\parallel V_{4xz}.(V_{5z})\to /x./y./z.V_0.(V_{1xy}.(V_{3yz}))\parallel V_{4xz}.(V_{5z}),$$

其中,反应物和生成物用"→"连接.

Table 2 Term Languages

表 2 项语言

Term Language	Meaning
$U \parallel V$	Concatenation of roots.
$U \mid V$	Concatenation of children which are under one node.
$U.(V)$	Nesting.
$-_i$	Site numbered i.
$/x.U$	U with outer name x replaced by an edge.

3.2 位置约束访问控制系统环境模型建模

偶图的位置图和连接图能够从不同的侧面建模位置约束访问控制系统的运行环境. 通过偶图的位置图,能够清晰地表达建筑分布、人员分布、物理实体、信息实体和混合实体的位置. 通过偶图的连接图,能够表达主体对客体的访问行为. 以下先介绍位置约束访问控制系统偶图的形式化定义,然后给出EM模型到偶图的转换规则.

定义 11. 标签. 标签为一个三元组 $\mathcal{R}=(K,ar,st)$,其中 K 为控制节点集合,$ar:K\to\mathbb{N}$ 为控制节点与其上端口数的映射,st 为控制节点的状态 $st\in\{\text{atomic},\text{active},\text{passive}\}$. 其中:原子节点(atomic)不允许有孩子节点和施加反应规则;活跃节点(active)和不活跃节点(passive)统称为复合节点,复合节点可以有孩子节点,但活跃节点可以施加反应规则,不活跃节点不允许施加反应规则.

EM模型中逻辑位置角色和实体对应的标签如表3所示. $Role$ 和 $Hybriden$ 的端口数为1,表达角色对混合实体的访问. 图形形状的不同只是为了标识不同的控制类型,与具体含义无关.

Table 3 System Signatures

表 3 系统标签

K	P_B	st	Graph
$LocR$	0	active	
$Role$	1	active	
$Hybriden$	1	active	
$Physicalen$	0	active	
$Cyberen$	0	active	

定义 12. 位置约束访问控制系统偶图. 位置约束访问控制系统偶图是由位置图 F^{P} 与连接图 F^{L} 组成的五元组:

$B=(V_B,E_B,ctrl_B,prnt_B,link_B):\langle m,X\rangle\to\langle n,Y\rangle$.

1) 位置图 $F^{\mathrm{P}}=(V_B,ctrl_B,prnt_B):m\to n$. 其中,$m$ 为地点数,n 为区域数,V_B 为节点集合,$ctrl_B$ 为节点到控制的映射,$ctrl_B:V_B\to K$,$prnt_B$ 为节点间嵌套关系,$prnt_B:m\uplus V_B\mapsto V_B\uplus n$,"$\mapsto$"指向节点嵌套箭头尾部节点.

2) 连接图 $F^{\mathrm{L}}=(V_B,E_B,ctrl_B,link_B):X\to Y$. 其中,$X$ 为内部名,Y 为外部名,V_B 为节点集合,E_B 为连接边集合,$ctrl_B$ 为节点到控制的映射,$link_B$ 为边的映射关系,$link_B:X\uplus P_B\Leftrightarrow E_B\uplus Y$,$P_B$ 为节点端口集合.

由定义7可知,EM 模型表达了系统运行环境中实体以及实体连接关系和位置关系. 由定义12可知,位置约束访问控制系统偶图是由位置图和连接图组成,能够与 EM 模型形成概念上的映射.

转换规则 1. EM模型到偶图的转换规则.

$V_B:Role,Object,LocR\Rightarrow V_B$;

/* 角色、客体、逻辑位置角色对应节点 */

$ctrl_B:V_B\to K$; /* 节点到控制的映射 */

$prnt_B:Locrelation(lr_i,lr_j)\Rightarrow lr_j\mapsto lr_i$;

/* 逻辑位置角色节点的嵌套关系 */

$RoleLocation(lr_i,r_i)\Rightarrow r_i\mapsto lr_i$;

/* 角色与逻辑位置角色节点的嵌套关系 */

$ObjectLocation(lo_i,o_i)\Rightarrow o_i\mapsto lo_i$;

/* 客体与逻辑位置角色节点的嵌套关系 */

$link_B:RoleObject(r_i,o_i)\Rightarrow r_i\Leftrightarrow o_i$;

/* 角色和客体节点之间的连接关系 */

$P_B\Leftrightarrow Y$; /* 实体的外部名 */

$E_B:link_B$ 中连接边的集合;

$m=k,k\in\mathbb{N}$; /* 地点数为 k */

$n=1$; /* 区域数为1 */

$X=\varnothing$; /* 内部名为空 */

Y 为 $Role$ 和 $Hybriden$ 节点端口对应的外部名. 其中,$\Rightarrow$ 表示转换关系;$K=\{LocR,Role,Hybriden,Cyberen,Physicalen\}$.

如应用场景中,通过大厅能够到达走廊,则大厅对应的节点嵌套走廊对应的节点. 人员分布、物理实体、信息实体和混合实体嵌套关系,则对应着现实中嵌套关系. 如图1中所有人员位于大厅,则人员节点位于大厅节点内、走廊节点外;小云服务器位于服务器房间内,则表示为小云服务器的节点嵌套在代表服务器房间的节点内. 银行职员在大厅内可以连接小云服务器,则通过边实现银行职员与小云服务器端口的互连. 根据转换规则1和表3标签的定义,得到图1中EM模型的图形化偶图如图6所示:

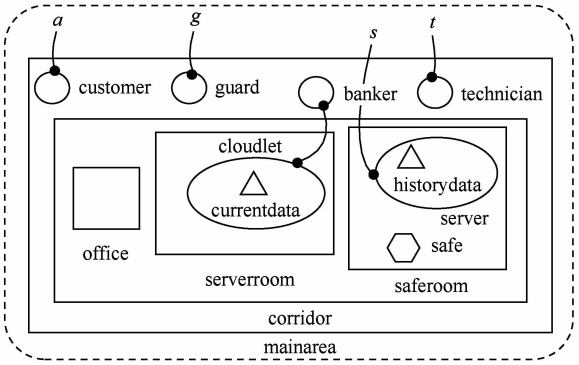

Fig. 6　Bigraphs of the environment model

图 6　运行环境偶图

3.3　基于 LCRBAC 模型的访问控制策略建模

利用反应规则建模基于 LCRBAC 模型的位置约束访问控制策略,即实现策略$(R,OPLocR,LocR)$和$(R,OPobjects,(Objects,LocO),LocR)$到反应规则的转换.转换规则 2 中考虑了 8 种操作,具体应用中可根据需求进行扩展.转换规则 2 中,针对混合实体和信息实体的操作,编号 1 为客体位置与主体位置不同,编号 2 表示客体位置与主体位置相同,编号 3 为客体位于主体内.

转换规则 2. 访问控制策略到反应规则转换.

$(R,\text{enter},LocR)\Rightarrow R_a.-_0|LocR.-_1|-_2\rightarrow LocR.(R_a.-_0|-_1)|-_2.$

$(R,\text{exit},LocR)\Rightarrow LocR.(R_a.-_0|-_1)|-_2\rightarrow R_a.-_0|LocR.-_1|-_2.$

$(R,\text{open},Physicalen,LocR)\Rightarrow LocR.(R_a.-_0|Physicalen|-_1)|-_2\rightarrow LocR.(Physicalen.R_a.-_0|-_1)|-_2.$

$(R,\text{close},Physicalen,LocR)\Rightarrow LocR.(Physicalen.R_a.-_0|-_1)|-_2\rightarrow LocR.(R_a.-_0|Physicalen|-_1)|-_2.$

$(R,\text{login},(Hybriden,LocO),LocR)\Rightarrow$

1) $LocR.(R_a.-_0|-_1)|LocO.(Hybriden_b.-_2|-_3)|-_4\rightarrow/x.LocR.(R_x.-_0|-_1)|LocO.(Hybriden_x.-_2|-_3)|-_4$;

2) $LocR.(R_a.-_0|Hybriden_b.-_1|-_2)|-_3\rightarrow/x.LocR.(R_x.-_0|Hybriden_x.-_1|-_2)|-_3.$

$(R,\text{logout},(Hybriden,LocO),LocR)\Rightarrow$

1) $/x.LocR.(R_x.-_0|-_1)|LocO.(Hybriden_x.-_2|-_3)|-_4\rightarrow LocR.(R_a.-_0|-_1)|LocO.(Hybriden_b.-_2|-_3)|-_4$;

2) $/x.LocR.(R_x.-_0|Hybriden_x.-_1|-_2)|-_3\rightarrow LocR.(R_a.-_0|Hybriden_b.-_1|-_2)|-_3.$

$(R,\text{copy},(Cyberen,Hybriden,LocO),LocR)\Rightarrow$

1) $/x.LocR.(R_x.-_0|-_1)|LocO.(Hybriden_x.(Cyberen|-_2)|-_3)|-_4\rightarrow/x.LocR.(R_x.(Cyberen|-_0)|-_1)|LocO.(Hybriden_x.(Cyberen|-_2)|-_3)|-_4$;

2) $/x.LocR.(R_x.-_0|Hybriden_x(Cyberen|-_1)|-_2)|-_3\rightarrow/x.LocR.(R_x.(Cyberen|-_0)|Hybriden_x.(Cyberen|-_1)|-_2)|-_3.$

$(R,\text{delete},(Cyberen,Hybriden,LocO),LocR)\Rightarrow$

1) $/x.LocR.(R_x.-_0|-_1)|LocO.(Hybriden_x.(Cyberen|-_2)|-_3)|-_4\rightarrow/x.LocR.(R_x.-_0|-_1)|LocO.(Hybriden_x.-_2|-_3)|-_4$;

2) $/x.LocR.(R_x.-_0|Hybriden_x.(Cyberen|-_1)|-_2)|-_3\rightarrow/x.LocR.(R_x.-_0|Hybriden_x.-_1|-_2)|-_3$;

3) $LocR.(R_a.(Cyberen|-_0)|-_1)|-_2\rightarrow LocR.(R_a.-_0|-_1)|-_2.$

通过转换规则 2 得到的反应规则作用于转换规则 1 得到的偶图模型,从而不断产生新的状态,最终形成以访问控制策略标注转移边的标号变迁系统(labeled transition system)[26].

定义 13. 标号变迁系统.标号变迁系统为六元组$(S,I,Act,\rightarrow,AP,L)$.其中,$S$ 表示所有状态的集合;I 表示初始状态;Act 表示转移边的集合;$\rightarrow\subseteq S\times Act\times S$ 表示变迁关系;AP 表示原子命题的集合;$L:S\rightarrow 2^{AP}$用于标记每个状态满足的原子命题.

如应用场景中位置约束的访问控制策略“技术人员进入走廊”是允许的访问行为,对应的反应规则根据转换规则 2 得:

$$\text{technician}_t.-_0|\text{corridor}.-_1|-_2\rightarrow \text{corridor}.(\text{technician}_t.-_0|-_1)|-_2,$$

对应的图形化表示如图 7 所示:

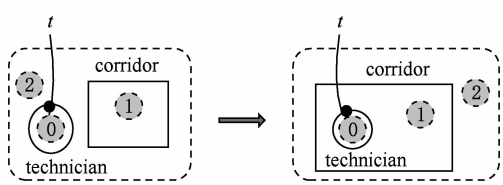

Fig. 7　Reaction rule of the operation-enter

图 7　进入反应规则

其中,灰色虚线框表示地点(site),它是一类特殊的节点,用于抽象无需关心的信息.

图 7 中反应物与图 6 中的偶图进行匹配,图 6 中 technician 和 corridor 之间的关系与反应物中两者

之间的关系是一致的,就利用生成物代替反应物,即图 6 中偶图在图 7 反应规则的作用下,变迁为新的状态,如图 8 所示. 如此反复下去,不断应用反应规则产生新的状态,最终可形成访问控制策略标注转移边的标号变迁系统.

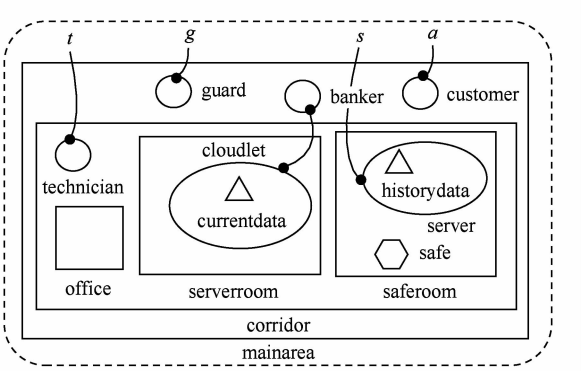

Fig. 8 Reactum model

图 8 生成物模型

3.4 位置相关的安全属性描述

对于需要验证的位置相关的安全属性,也可采用偶图描述. 如安全需求 $SR1$:"银行主管不能将用户历史交易记录带离安全屋(至走廊)",利用偶图项语言表达为 $\overline{SR1}$: corridor. (guard_g. historydata | $-_0$). 安全需求 $SR2$:"技术人员不能进入安全屋",项语言表达为$\overline{SR2}$: saferoom. (technician_t | $-_0$). 另外,还可以通过安全需求的并、或、非实现需求的合成. 如要求访问控制系统即要满足 $SR1$ 又要满足 $SR2$,安全需求表达为:$SR1 \wedge SR2$.

由于安全需求可以利用偶图描述,那么验证一个偶图 A 是否满足某个安全属性 B,等价于检测偶图 A 是否与偶图 B 匹配,类似反应规则中反应物与偶图之间的匹配过程. 当匹配成功,则表示偶图 A 满足安全需求;否则,不满足安全需求,为违反状态. 对安全属性的验证本质上就是检测标号变迁系统中,是否所有状态都与安全属性的偶图 B 一致.

在访问控制策略正确性的验证方面,本文遵循关注点分离的思想采用分层的方式. 首先验证单个角色访问控制策略的正确性,在保证单个角色访问控制策略正确性的基础上,建立所有角色访问控制策略模型,验证多个角色策略交互行为的正确性,以此减少在所有角色访问控制策略上的验证负担. 如案例中首先针对银行主管、职员、技术人员和客户的访问控制策略分别进行验证,然后再对 4 个角色之间交互行为的访问控制策略进行验证,具体可参看 5.2 节的案例分析.

4 位置约束的访问控制策略修改方案

根据模型检测结果,依据访问控制策略在标号变迁系统中的作用把访问控制策略分为 4 类:导致死锁的访问控制策略、导致违反状态的访问控制策略、不可达访问控制策略、正常的访问控制策略. 根据访问控制策略分类得到标号变迁系统中 4 种状态:死锁状态、违反状态、不可达状态、正常状态. 如图 9 所示,e 为死锁状态,h 为违反状态,j 为不可达状态. 死锁状态、违反状态和不可达状态统称为非正常状态;其余节点为正常状态.

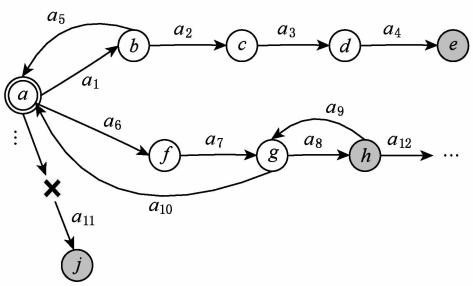

Fig. 9 Example of a labeled transition system

图 9 标号变迁系统示例

介绍具体的策略修改方案之前,定义一些约定符号:$policies$ 表示所有访问控制策略集合;$pl(s_t, s_k)$ 表示状态 s_t 与状态 s_k 之间的策略边;$deadlockstates$ 表示死锁状态集合;$violatestates$ 表示违反状态集合;$unreachablestates$ 表示不可达状态集合;$inpolicies(s)$ 表示状态 s 的入度边访问控制策略集;$outpolicies(s)$ 表示状态 s 的出度边访问控制策略集;$outedgecount(s)$ 表示状态 s 的出度.

4.1 针对死锁状态策略修改方案

1) 删除访问控制策略. 删除导致死锁状态的访问,控制策略需要从死锁状态反向追踪,直到遇到出度不为 1 的状态,将该状态转移至死锁状态路径上的策略边全部删除,即删除表 4 中 $delete1(s_i, s_j)$ 定义的策略集合. 如图 10(a)中,通过删除策略 a_2, a_3, a_4 消除死锁状态 e.

2) 增加访问控制策略. 位置约束访问控制策略的制定,不仅要能够保证所有的访问控制策略不会造成死锁,还要保证所有策略不会形成活锁,即不仅要控制访问的行为,还要控制退出的行为. 需要增加的策略集合为表 4 中 $add1(s_i, s_j)$ 定义的策略集,其中,$addpolicies(s_j, s_i)$ 表示从 s_i 到 s_j 可增加的反向边集合,$selectpolicies(s_j, s_i)$ 表示 s_j 到 s_i 的可达路径,

即从 $addpolicies(s_j,s_i)$ 中选取反向边能够连接状态 s_j 到 s_i. 如图 10(a)中解决死锁状态 e,可增加的访问控制策略集合为:$addpolicies(e,b)=\{d_1,d_2,d_3,d_4,d_5,d_6\}$ $add1(e,b)=\{(d_3),(d_1,d_5),(d_2,d_6),(d_1,d_4,d_6)\}$. 也可通过增加边引入新状态辅助死锁状态的消除,如图 10(b)中增加 1 条边 a_5 引入新状态 f,从 $selectpolicies(f,b)$ 集合中选择 1 组反向边实现死锁状态的消除.

Table 4　Location-Constrained Access Control Policies Modifications

表 4　位置约束访问控制策略调整

States	Access Policies Modifications
Deadlock States	$delete1(s_i,s_j)=\{a_i,a_{i+1},\cdots,a_{j-1}\mid \forall s_i,s_i\xrightarrow{a_i}s_{i+1}\cdots s_l\xrightarrow{a_l}s_{l+1}\cdots s_{j-1}\xrightarrow{a_{j-1}}s_j,outedgecount(s_l)=1,s_j\in deadlockstates,l\in\{i+1,i+2,\cdots,j-1\}\}$ $addpolicies(s_j,s_i)=\{pl(s_t,s_k)\mid \forall s_i,s_i\xrightarrow{a_i}s_{i+1}\cdots s_l\xrightarrow{a_l}s_{l+1}\cdots s_{j-1}\xrightarrow{a_{j-1}}s_j,outedgecount(s_l)=1,s_j\in deadlockstates,l\in\{i+1,i+2,\cdots,j-1\},t\in\{j,j-1,\cdots,i+1\},k\in\{t-1,t-2,\cdots,i\}\}$ $add1(s_j,s_i)=\{selectpolicies(s_j,s_i)\mid selectpolicies(s_j,s_i)\subseteq addpolicies(s_j,s_i)\}$
Violate States	$delete2(s_n)=\{inpolicies(s_n)\cup outpolicies(s_n)\mid s_n\in violatestates\}$ $add2(s_n)=\{A_k\mid s_0\xrightarrow{a_0}s_1\cdots s_{n-1}\xrightarrow{a_{n-1}}s_n\cdots,s_n\in violatestates,A_k\not\subset policies\}$ $priority(s_n)=\{a_{n-1}\leqslant a_k\mid s_0\xrightarrow{a_0}s_1\cdots s_k\xrightarrow{a_k}s_{k+1}\cdots s_{n-1}\xrightarrow{a_{n-1}}s_n\cdots,s_n\in violatestates\}$
Unreachable States	$delete3(s_j)=\{a_j\mid s_0\xrightarrow{a_0}s_1\cdots s_{n-1}\xrightarrow{a_{n-1}}s_n,\xrightarrow{a_j}s_j,s_j\in unreachablestates\}$ $add3(s_j)=\{a'_0,a'_1,\cdots,a'_{k-1}\mid s_0\xrightarrow{a_0}s_1\cdots s_n\xrightarrow{a'_0}s'_1\cdots s'_{k-1}\xrightarrow{a'_{k-1}}s'_k\xrightarrow{a_j}s_j,s_j\in unreachablestates\}$

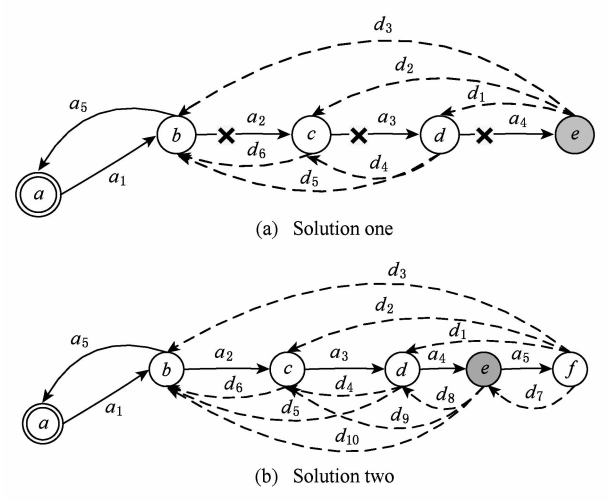

Fig. 10　Solutions of the deadlock state

图 10　死锁状态解决方案

4.2　针对违反状态策略修改方案

1) 删除访问控制策略. 删除导致违反状态的入度边策略 $inpolicies$ 和出度边策略 $outpolicies$,即删除表 4 中 $delete2(s_n)$定义的策略集合. 如图 9 中,通过删除状态 h 的入度边策略 a_8 和出度边策略 a_9 与 a_{12}解决违反状态 h.

2) 增加访问控制策略. 需根据具体问题分析增加策略,见表 4 中 $add2(s_n)$公式,A_k 表示需要增加的策略边集合. 如案例中,"要求技术人员在服务器房间时,必须有银行主管陪同",定义 a_n 为(technician,enter,serverroom),若系统中无策略 a_k 为(guard,enter,serverroom),则 s_n 处于违反状态,需要在 a_n 前增加策略 a_k. 无形中定义了访问控制策略间的依赖关系.

3) 定义策略依赖关系. 通过定义策略间的依赖关系,消除违反状态,见表 4 中公式 $priority(s_n)$. 如案例中,"要求技术人员在服务器房间时,必须有银行主管陪同",a_{n-1} 为(technician,enter,serverroom),a_k 为(guard,enter,serverroom),则要求 $a_{n-1}\leqslant a_k$.

4.3　针对不可达状态策略修改提议

1) 删除访问控制策略. 对于不可达策略,可直接删除,具体定义为表 4 中公式 $delete3(s_j)$. 如图 9 中,可将策略 a_{11}删除,解决状态 j 的不可达问题.

2) 增加访问控制策略. 通过增加策略,实现策略互联,使不可达状态变为可达状态,见表 4 中公式 $add3(s_j)$. 如案例中可通过增加访问控制策略(guard,enter,saferoom)消除独立策略(guard,open,safe,saferoom).

以上 3 种策略调整方案为非正常状态的消除提供建议,但在某些情况下并非最优方案,如要求策略调整所带来的成本最小等,因此,实际应用中需要根据具体需求进行方案选取. 对于访问控制策略的修改,在满足安全需求的前提下,优先选择删除策略和定义策略依赖关系,然后选择增加策略方案. 访问控制策略的增加,需要重新考虑策略间的一致性问题[27-28]. 以下给出访问控制策略修改路径生成算法.

算法 1. 策略修改路径生成算法.

输入:标号变迁系统 lts、反例路径 cp、安全属性规约类型 $spec$、访问控制策略编号集合 pi;

输出:需修改的策略路径.

① if($spec$==1) /* 属性规约为死锁类型 */
② $dlpath=cp.getCounterPath(1)$;
/* 根据反例路径获取死锁节点 */
③ $i=2$;
④ for each $i\leqslant cp.length$
⑤ if ($lts.outEdgeCount(cp.getCounterPath(i))$==1) /* 反例路径中状态节点出度为 1 */
⑥ $pl=lts.Read(cp.getCounterPath(i),cp.getCounterPath(i-1))$;
/* 读取反例路径中状态节点间的策略边 */
⑦ $dlpath=dlpath+pl+cp.getCounterPath(i)$;
⑧ end if
⑨ i++;
⑩ end for
⑪ $pl=lts.Read(cp.getCounterPath(i),cp.getCounterPath(i-1))$;
⑫ $dlpath=dlpath+pl+cp.getCounterPath(i)$;
⑬ return $dlpath$;
/* 返回需要修改的反例路径状态节点及策略边 */
⑭ end if
⑮ if($spec$==2) /* 属性规约为违反类型 */
⑯ return $vipath=getViPolicies(LTS,cp)$;
/* 返回违反状态节点的策略边 */
⑰ end if
⑱ if ($spec$==3)
⑲ if ($Equal(getLtsPolicies(lts),pi)$)
/* 标号迁移系统包含所有策略边的标识 */
⑳ return NULL;
㉑ else
㉒ return $unreachablepl=ChenkLTS(LTS,pi)$;
/* 返回标号迁移系统中未包含的策略边的标识 */
㉓ end if
㉔ end if

5 偶图建模工具介绍和案例分析

5.1 偶图建模工具

针对偶图和偶图反应系统已有很多工具支持,如 DBtk 工具[29]、BigRed[30]原型编辑器、BigMC[31]工具.其中,BigMC 语言描述与偶图和偶图反应系统的项语言描述比较相近,有利于理解.BigMC 可以检验偶图和偶图反应系统模型是否满足系统安全需求属性,如果不满足,给出反例.BigMC 可以将衍化过程生成 dot 脚本,使用 XDOT 软件、graphviz 软件进行图形化的表达.

根据 3.2 节和 3.3 节提出的转换规则,本文设计并实现了 EM 模型和 LCRBAC 模型到 BigMC 语言转换的原型系统.如图 11 所示,通过 EM 模型参数的输入,得到初始模型(InitialModel),通过访问控制策略的输入,得到对应的反应规则.

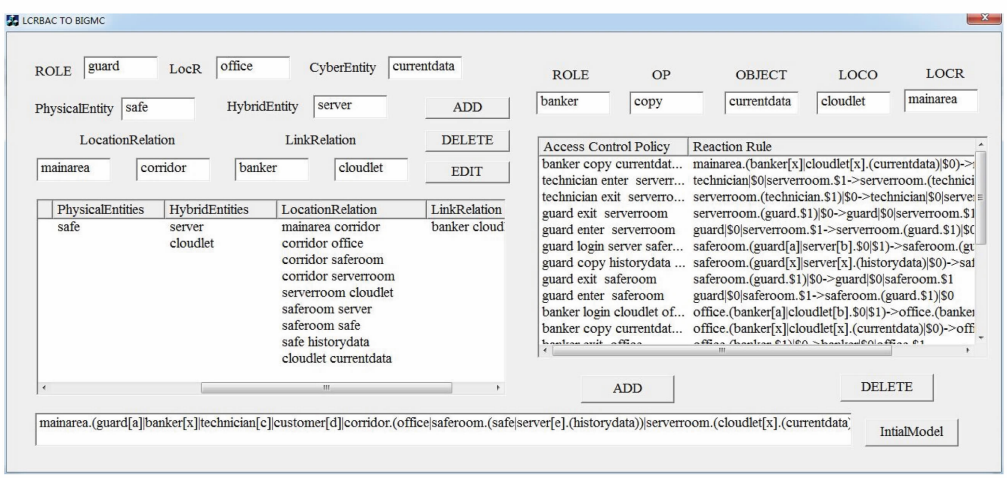

Fig. 11 Conversion toolkit from the location-constrained access control model to the BigMC language

图 11 位置约束访问控制模型至 BigMC 语言转换工具

5.2　案例分析

5.2.1　EM模型和LCRBAC模型

根据2.1节中银行访问控制系统需求描述,基于逻辑位置角色,提取访问控制策略,如表5所示.

5.2.2　位置约束访问控制策略建模

利用LCRBAC TO BIGMC转换工具,得到银行主管的访问控制策略对应的反应规则(表7所示)

Table 5　Access Control Policies of the Bank

表5　银行系统访问控制策略

LocR	Access Control Policies
mainarea	(banker,copy,(currentdata,cloudlet,serverroom),mainarea)
corridor	(guard,enter,corridor)(guard,exit,corridor)(banker,enter,corridor)(banker,exit,corridor)(technician,enter,corridor)(technician,exit,corridor)
office	(guard,enter,office)(guard,exit,office)(banker,enter,office)(banker,exit,office)(banker,copy,(currentdata,cloudlet,serverroom),office)(banker,login,(cloudlet,serverroom),office)
saferoom	(guard,enter,saferoom)(guard,exit,saferoom)(guard,copy,(historydata,server,saferoom),saferoom)(guard,login,(server,saferoom),saferoom)(guard,open,safe,saferoom)
serverroom	(guard,enter,serverroom)(guard,exit,serverroom)(technician,enter,serverroom)(technician,exit,serverroom)

Table 6　Environment Model of the Bank Access Control System

表6　银行访问控制系统的EM模型

Elements	Values
LocR	mainarea,serverroom,office,corridor,saferoom
Object	$Cyberen=\{$historydata,currentdata$\}$,$Physicalen=\{$safe$\}$,$Hybriden=\{$server,cloudlet,guardphone,customerphone,technicianphone,bankerphone$\}$
LocO	mainarea,serverroom,office,corridor,saferoom,server,cloudlet
RoleObject	(banker,cloudlet)
Locorelation	(mainarea,corridor),(corridor,saferoom),(corridor,serverroom),(corridor,office)
RoleLocation	(banker,mainarea),(customer,mainarea),(technician,mainarea),(guard,mainarea)
ObjectLocation	(safe,saferoom),(server,saferoom),(cloudlet,serverroom),(currentdata,cloudlet,serverroom),(historydata,server,saferoom)

Table 7　Reaction Rules of Guard Access Control Policies

表7　银行主管访问控制策略对应的反应规则

Edge Num*	Guard Access Control Policies	Reaction Rules
(1)	(guard,enter,corridor)	guard[g]|corridor. $0\|$ $1→corridor. (guard[$g$]|$0)|$1
(2)	(guard,exit,corridor)	corridor. (guard[g]|$0)|$1→guard[g]|corridor. $0|$1
(3)	(guard,enter,office)	guard[g]|office. $0|$1→office. (guard[g]|$0)|$1
(4)	(guard,exit,office)	office. (guard[g]|$0)|$1→guard[g]|office. $0|$1
(5)	(guard,enter,serverroom)	guard[g]|serverroom. $0|$1→serverroom. (guard[g]|$0)|$1
(6)	(guard,exit,serverroom)	serverroom. (guard[g]|$0)|$1→guard[g]|serverroom. $0|$1
(7)	(guard,enter,saferoom)	guard[g]|saferoom. $0|$1→saferoom. (guard[g]|$0)|$1
(8)	(guard,exit,saferoom)	saferoom. (guard[g]|$0)|$1→guard[g]|saferoom. $0|$1
(9)	(guard,copy,(historydata,server,saferoom),saferoom)	saferoom. (guard[x]|server[x]. historydata|$0)|$1→saferoom. (guard[x]. historydata\|server[x]. historydata|$0)|$1
(10)	(guard,login,(server,saferoom),saferoom)	saferoom. (guard[g]|server[s]. historydata|$0)|$1→saferoom. (guard[x]\|server[x]. historydata|$0)|$1
(11)	(guard,open,safe,saferoom)	saferoom. (guard[g]|safe|$0)|$1→saferoom. (safe. guard[g]|$0)|$1
(12)	(guard,close,safe,saferoom)	saferoom. (safe. guard[g]|$0)|$1→saferoom. (guard[g]|safe|$0)|$1
(13)	(guard,logout,(server,saferoom),saferoom)	saferoom. (guard[x]. $0\|server[$x$]. $1|$2)|$3→saferoom. (guard[$g$]. $0\|server[$s$]. $1|$2)|$3
(14)	(guard,delete,(historydata,guardphone,saferoom),saferoom)	saferoom. (guard[g]. historydata|$0)|$1→saferoom. (guard[g]|$0)|$1

* Edge num indicates the edge number in Fig. 12 and Fig. 14.

和位置约束访问控制系统初始模型：

mainarea.(guard[g]|banker[b]|technician[t]|customer[a]|corridor.(office|saferoom.(safe|server[s].historydata)|serverroom.(cloudlet[c].currentdata))).在系统初始模型的基础上，根据银行主管访问控制策略，生成的标号变迁系统如图 12 所示.图 12 中的 11 条迁移边对应表 7 中定义的编号(1)～(11)的访问控制策略，图 12 中的 8 个状态对应表 8 中编号 0～7.类似地，可生成银行职员和技术维护人员的访问控制策略标号变迁系统.

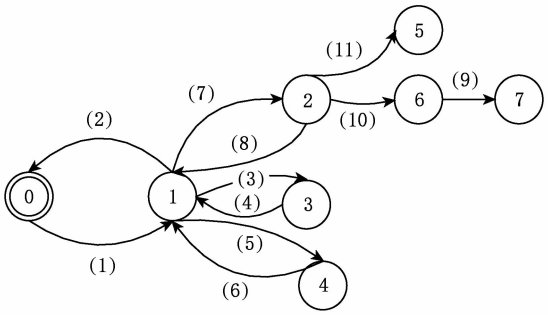

Fig. 12 Labeled transition system of guard access control policies

图 12 银行主管访问控制策略标号变迁系统

Table 8 States Implication of the Guard Labeled Transition System

表 8 银行主管标号变迁系统状态含义

Node Num*	BigMC Language	Description
0	mainarea.(guard[g]|corridor.(saferoom.(safe|server[s].historydata)|serverroom.cloudlet[c].currentdata|office))	Guard is in mainarea
1	mainarea.(corridor.(guard[g]|saferoom.(safe|server[s].historydata)|serverroom.cloudlet[c].currentdata|office))	Guard is in corridor
2	mainarea.(corridor.(saferoom.(guard[g]|safe|server[s].historydata)|serverroom.cloudlet[c].currentdata|office))	Guard is in saferoom
3	mainarea.(corridor.(saferoom.(safe|server[s].historydata)|serverroom.cloudlet[c].currentdata|office.(guard[g])))	Guard is in office
4	mainarea.(corridor.(saferoom.(safe|server[s].historydata)|serverroom.(guard[g]|cloudlet[c].currentdata)|office))	Guard is in serverroom
5	mainarea.(corridor.(saferoom.(safe.guard[g]|server[s].historydata)|serverroom.cloudlet[c].currentdata|office))	Guard opens safe
6	mainarea.(corridor.(saferoom.(guard[－]|safe|server[－].historydata)|serverroom.cloudlet[c].currentdata|office))	Guard logins server
7	mainarea.(corridor.(saferoom.(guard[－].historydata|safe|server[－].historydata)|serverroom.cloudlet[c].currentdata|office))	Guard copys historydata
8	mainarea.(corridor.(saferoom.(guard[g].historydata|safe|server[s].historydata)|serverroom.cloudlet[c].currentdata|office))	Guard logouts server

* Node num indicates the node number in Fig. 12 and Fig. 14.

5.2.3 性质验证和访问控制策略调整

1) 银行主管的访问控制策略验证与调整

① 死锁检测.经验证性质满足，如图 13 所示.反例路径为 5(11)2(7)1(1)0，状态 5 为死锁状态.根据访问控制策略修改算法，得到修改路径为 5(11)2.可通过 2 种方式修改策略：删除策略(11)，即禁止银行主管打开保险柜的权限；增加编号为(12)的策略(guard,close,safe,saferoom)，实现状态 5 至状态 2

```
cc@cc-VirtualBox:~/Downloads/bigmc-master/doc/access-control$ bigmc guard.bgm
*** Found violation of property: deadlock_free
*** deadlock_free: !terminal()
#0  mainarea.(corridor.(serverroom.cloudlet[c].currentdata.nil | office.nil | sa
feroom.(safe.(guard[g].nil) | server[s].historydata.nil)))   <- *** VIOLATION **
*
 >> p11

#1  mainarea.(corridor.(saferoom.(guard[g].nil | safe.nil | server[s].historydat
a.nil) | serverroom.cloudlet[c].currentdata.nil | office.nil))
 >> p7

#2  mainarea.(corridor.(guard[g].nil | saferoom.(safe.nil | server[s].historydat
a.nil) | serverroom.cloudlet[c].currentdata.nil | office.nil))
 >> p1

#3  mainarea.(guard[g].nil | corridor.(saferoom.(safe.nil | server[s].historydat
a.nil) | serverroom.cloudlet[c].currentdata.nil | office.nil))
 >> (root)
[mc::step] Counter-example found.
```

Fig. 13 Counter path

图 13 反例路径

的迁移,即银行主管打开保险柜后,一定要执行关闭保险柜的动作才能离开安全屋.

② 死锁检测. 经验证性质满足,反例路径为7(9)6(10)2(7)1(1)0,状态7为死锁状态. 根据访问控制策略修改算法,得修改路径为7(9)6(10)2. 可通过2种方式修改策略:删除策略(9)(10),即禁止银行主管登入安全屋中服务器和读取用户历史交易信息;增加策略(guard,logout,(server,saferoom),saferoom)和(guard,delete,(historydata,guardphone,saferoom),saferoom),编号分别为(13)和(14).

最终,针对银行主管的访问控制策略修改为(1)～(14),生成的标号变迁系统包括9个状态,14条变迁. 具体如图14所示:

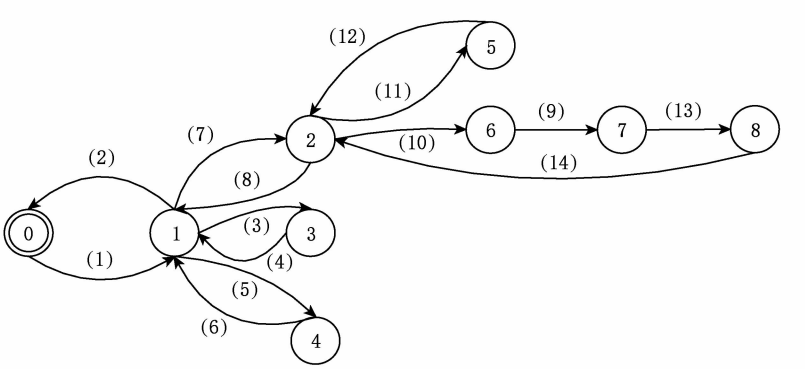

Fig. 14　Modified labeled transition system of guard access control policies

图14　银行主管访问控制策略更改后标号变迁系统

2) 银行职员访问控制策略验证与策略调整

① 不可达策略检测. 根据访问控制策略修改算法,得到访问控制策略(banker,copy,(currentdata,cloudlet),mainarea)为未执行状态. 通过2种方式调整策略:删除该策略;增加策略(banker,login,(cloudlet,serverroom),mainarea),使不可达策略可执行.

② 死锁检测. 经验证性质满足. 通过2种方式修改策略:增加策略(banker,logout,(cloudlet,serverroom),office)或(banker,logout,(cloudlet,serverroom),mainarea),即银行职员只有退出登入,才能离开相应区域;删除策略(banker,login,(cloudlet,serverroom),office)和(banker,copy,(currentdata,cloudlet),mainarea),即禁止银行职员在办公室登入小云服务器和在大厅获取客户当天交易记录.

3) 技术人员访问控制策略验证与策略调整

① 死锁检测,经验证性质不满足.

② 安全需求描述为:要求技术人员进入服务器房间时,必须有银行主管陪同. 经验证访问控制策略违反该安全需求. 2种修改方案:删除策略(technician,enter,serverroom),即禁止技术人员进入服务器房间;定义策略依赖关系,限定(technician,enter,serverroom)之前有策略(guard,enter,serverroom).

4) 全局访问控制策略正确性验证

基于单个角色访问控制策略的调整,建立全局访问控制策略变迁图,最终访问控制策略为28条,生成的标号迁移系统共有87个状态. 经检测,访问控制策略不存在死锁状态. 通过对单个角色访问控制策略的修改,在较小的状态空间中进行检测,能够简化验证复杂度. 在全局访问控制策略中只需关注策略之间交互行为的验证即可.

6　结论及下一步工作

物联网、信息物理融合系统等新一代信息技术的出现,为位置约束的访问控制模型提出了新需求,不仅要关注信息空间中位置对访问行为的约束,还要考虑物理空间以及两空间交互过程中位置对访问行为的约束. 如何在这种新需求下实现位置约束访问控制模型的建立与验证成为当前信息安全领域的研究热点之一. 本文针对物理空间、信息空间和两空间的交互,制定不同的访问控制策略,提出LCRBAC模型,并通过EM模型实现对系统运行环境的描述. 利用偶图和偶图反应系统对EM和LCRBAC模型进行形式化建模,并对位置约束的安全属性进行验证,根据验证结果,提出对非正常状态的策略修改方案. 最后,结合案例和原型工具说明了方法的有效性.

下一步工作将从以下3个方面展开：

1）本文未考虑全局访问控制策略正确性验证的状态空间约减问题.全局访问控制模型涉及多个角色,容易导致标号变迁系统过大,引发状态空间爆炸问题.由于单个角色的相关属性在前期已经得到验证,如何在全局访问控制模型中对其进行抽象,是实现状态空间约减的关键.

2）本文未考虑用户安全需求保持的策略更新方法.策略的每次调整需要重新对策略集进行验证,效率较低.如何针对不同类型的用户安全需求,提出相应的策略更新方案或者部分策略的选取与验证方法,是提高策略更新效率的关键.

3）本文所提模型和方法只针对一个物理区域,不适用于跨域环境下模型的建立与验证.由于移动终端的普及,如何在开放的网络环境下实现跨域的访问控制策略的制定与验证也是我们下一步的研究方向.

参 考 文 献

[1] Dey A, Hightower J, Lara E D, et al. Location-based services [J]. IEEE Pervasive Computing, 2017, 9(1): 11-12

[2] Wang Senzhang, He Lifang, Stenneth L, et al. Estimating urban traffic congestions with multi-sourced data [C] //Proc of the 17th IEEE Int Conf on Mobile Data Management. Piscataway, NJ: IEEE, 2016: 82-91

[3] Wang Senzhang, Zhang Xiaoming, Cao Jianping, et al. Computing urban traffic congestions by incorporating sparse GPS probe data and social media data [J]. ACM Trans on Information System, 2017, 35(4): 1-30

[4] Chen Weihe, Ju Shiguang, Xue Anrong. Survey on the novel access control model of location-based serveice based on the spatial location of mobile user [J]. Computer Science, 2008, 35(10): 19-24 (in Chinese)
(陈伟鹤，鞠时光，薛安荣. 基于移动用户位置的信息服务中的访问控制模型研究综述[J]. 计算机科学，2008，35(10)：19-24)

[5] Rajkumar R R, Lee I, Sha L, et al. Cyber-physical systems: The next computing revolution [C] //Proc of the 47th Design Automation Conf. New York: ACM, 2010: 731-736

[6] Hu V C, Kuhn R. Access control policy verification [J]. Computer, 2016, 49(12): 80-83

[7] Sandhu R, Ferraiolo D, Kuhn R. The NIST model for role-based access control: Towards a unified standard [C] //Proc of the 5th ACM Workshop on Role-Based Access Control. New York: ACM, 2000: 47-63

[8] Unal D, Akar O, Caglayan M U. Model checking of location and mobility related security policy specifications in ambient calculus [C] //Proc of the 5th Int Conf on Mathematical Methods, Models, and Architectures for Computer Network Security. Berlin: Springer, 2010: 155-168

[9] Cardelli L, Gordon A D. Mobile ambients [C] //Proc of the 1st Int Conf on Foundations of Software Science and Computation Structure. Berlin: Springer, 1998: 140-155

[10] Milner R. Pure bigraphs: Structure and dynamics [J]. Information and Computation, 2006, 204(1): 60-122

[11] Damiani M L, Bertino E, Catania B, et al. GEO-RBAC: A spatially aware RBAC [J]. ACM Trans on Information and System Security, 2007, 10(1): 1-42

[12] Ray I, Kumar M, Yu Lijun. LRBAC: A location-aware role-based access control model [C] //Proc of the 2nd Int Conf on Information Systems Security. Berlin: Springer, 2006: 147-161

[13] Zhang Hong, He Yeping , Shi Zhiguo. A formal model for access control with supporting spatial context [J]. SCIENTIA SINICA Informationis, 2007, 37(2): 254-271 (in Chinese)
(张宏，贺也平，石志国. 一个支持空间上下文的访问控制形式模型[J]. 中国科学：信息科学，2007，37(2)：254-271)

[14] Chandran S M, Joshi J B D. LoT-RBAC: A location and time-based RBAC model [C] //Proc of the 6th Int Conf on Web Information Systems Engineering. Berlin: Springer, 2005: 361-375

[15] Ray I, Toahchoodee M. A spatio-temporal role-based access control model [C] //Proc of the 21st IFIP Annual Conf on Data and Applications Security. Berlin: Springer, 2007: 211-226

[16] Abdunabi R, Al-Lail M, Ray I, et al. Specification, validation, and enforcement of a generalized spatio-temporal role-based access control model [J]. IEEE Systems Journal, 2013, 7(3): 501-515

[17] Abdunabi R, Ray I, France R. Specification and analysis of access control policies for mobile applications [C] //Proc of the 18th ACM Symp on Access Control Models and Technologies. New York: ACM, 2013: 173-184

[18] Fadhel A B, Bianculli D, Briand L. A comprehensive modeling framework for role-based access control policies [J]. Journal of Systems and Software, 2015, 107: 110-126

[19] Toahchoodee M, Ray I. On the formalization and analysis of a spatio-temporal role-based access control model [J]. Journal of Computer Security, 2011, 19(3): 399-452

[20] Toahchoodee M, Ray I, Anastasakis K, et al. Ensuring spatio-temporal access control for real-world applications [C] //Proc of the 14th ACM Symp on Access Control Models and Technologies. New York: ACM, 2009: 13-22

[21] Geepalla E, Bordbar B, Du X. Spatio-temporal role based access control for physical access control systems [C] //Proc of the 4th IEEE Int Conf on Emerging Security Technologies. Piscataway, NJ: IEEE, 2013: 39-42

[22] Ünal D, Çağlayan M U. A formal role-based access control model for security policies in multi-domain mobile networks [J]. Computer Networks, 2015, 57(1): 330-350

[23] Ünal D, Çağlayan M U. Spatiotemporal model checking of location and mobility related security policy specifications [J]. Turkish Journal of Electrical Engineering & Computer Sciences, 2013, 21(1): 144-173

[24] Tsigkanos C, Pasquale L, Ghezzi C, et al. On the interplay between cyber and physical spaces for adaptive security [J]. IEEE Trans on Dependable and Secure Computing, 2016 (99): 1-14

[25] Milner R. The Space and Motion of Communicating Agents [M]. Cambridge, UK: Cambridge University Press, 2009

[26] Clarke E M, Grumberg O, Peled D. Model Checking [M]. Cambridge, MA: MIT Press, 1999

[27] Li Ruixuan, Lu Jianfeng, Li Tianyi, et al. An approach for resolving inconsistency confilcts in access control policies [J]. Chinese Journal of Computers, 2013, 36(6): 1210-1223 (in Chinese)
(李瑞轩, 鲁剑锋, 李添翼, 等. 一种访问控制策略非一致性冲突消解方法[J]. 计算机学报, 2013, 36(6): 1210-1223)

[28] Hu Hongxin, Ahn G J, Jorgensen J. Multiparty access control for online social networks: Model and mechanisms [J]. IEEE Trans on Knowledge and Data Engineering, 2013, 25(7): 1614-1627

[29] Bacci G, Grohmann D, Miculan M. DBtk: A toolkit for directed bigraphs [C] //Proc of the 3rd Int Conf on Algebra and Coalgebra in Computer Science. Berlin: Springer, 2009: 413-422

[30] Faithfull A J, Perrone G, Hildebrandt T T. Big red: A development environment for bigraphs [J]. Electronic Communications of the Easst, 2013, 61: 1-10

[31] Perrone G, Debois S, Hildebrandt T T. A verification environment for bigraphs [J]. Innovations in Systems and Software Engineering, 2013, 9(2): 95-104

Cao Yan, born in 1985. PhD candidate. Member of CCF. Her main research interests include service-oriented architecture, formal verification, and security and privacy information system.

Huang Zhiqiu, born in 1965. PhD, professor, PhD supervisor. Senior member of CCF. His main research interests include software engineering, formal methods and service-oriented architecture.

Kan Shuanglong, born in 1988. PhD. Member of CCF. His main research interests include model checking, theoreom proving, and refinement-based software development (61707227@qq.com).

Peng Huanfeng, born in 1978. PhD candidate. His main research interests include cloud computing and service computing, privacy protection, and formal verification (penghf@njit.edu.cn).

Ke Changbo, born in 1984. PhD. Member of CCF. His main research interests include security and privacy information system, cloud computing, and ontology-based software engineering (brobo.ke@njupt.edu.cn).