协作环境中基于场所的访问控制模型

於光灿 李瑞轩 卢正鼎 宋 伟 唐 卓
(华中科技大学计算机科学与技术学院 武汉 430074)

摘 要 授权模型是协作环境中不可缺少的关键部件,为协作系统提供合适的授权机制很具挑战性。直接应用于协作系统的传统访问控制模型对多用户之间的协作支持不够,一些协作相关的访问控制必须在应用层上实现;针对特定协作应用背景的访问控制模型,仅适用于特定应用背景的协作系统,不能满足协作环境中更广泛的安全性需求;而现有的协作环境中通用的访问控制模型授权约束比较单一,不能满足协作环境中对授权的灵活性要求。针对这些问题,以Locale-BAC模型为基础提出协作环境中基于场所的访问控制模型,对角色、权限、场所等主要模型部件进行重新定义,实现全局访问控制和协作小组内部自主访问控制相结合的灵活的分层授权机制。

关键词 场所,访问控制,协作环境,授权约束

Locale-based Access Control Model in Collaborative Environment

YU Guang-can LI Rui-xuan LU Zheng-ding SONG Wei TANG Zhuo
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Collaborating systems require an appropriate authorization model to specify and maintain policies that not only facilitate group activities but also enforce restrictions and accountability. It is a great challenge to provide appropriate authorization models for collaborating systems. Existing models fail to incorporate adequately authorization decisions into the rich notion of context and all kinds of authorization constraints that are inherent to any collaborative settings. We presented the locale-based access control (Locale-BAC) model in collaborative environment. Some major components, such as roles, permissions and locales, were redefined in Locale-BAC model. Our model combines global access control policies and discretionary access control policies of collaboration locales to provide a flexible and hierarchy authorization mechanism.

Keywords Locale, Access control, Collaborative environment, Authorization constraints

1 介绍

协作活动被看作人类文明进步的推动力之一,互联网的飞速发展更是将人类的协作手段提高到一个全新的水平[1]。计算机支持的协同工作系统允许协作组成员为了共同的目标互相沟通协作工作,在政府、商业、教育、医疗、军事等多个领域得到广泛的应用,典型的应用包括电视电话会议、协作文档共享和编辑、远程教育、工作流管理等。尽管这些协作系统具有各自不同的功能,但是都有安全性需求。协作系统的交互特性要求协作成员都能及时得到其所需要的所有资源,而安全性要求保证信息的有效性、机密性、完整性,同时保证信息只提供给授权用户。由于在协作组成员之间及成员与系统之间不可预知的行为和交互方式,在协作环境中保护上下文信息和资源必须解决比传统信息系统中更为特殊的安全问题[2]。

现有的一些被应用于协作系统的访问控制模型可分为三种类型,第一种类型为传统的访问控制模型如访问矩阵模型[3]和基于角色的访问控制模型[4],这种把传统的访问控制模型直接应用于协作系统的缺点就是对多用户之间的协作支持不够,一些协作相关的访问控制必须在应用层上实现。第二种类型为一些针对特定协作应用背景的访问控制模型,其中,基于任务的访问控制模型(TBAC)[5]通过引入"域"概念扩展传统的基于主体客体的访问控制模型,该模型中的域包括基于任务的上下文信息,通过这些上下文信息实现对任务的分步、动态的授权;基于组的访问控制模型(TMAC)[6]的核心概念是"组",在组中封装为了完成特定任务的用户和对象,并引入用户上下文和对象上下文的概念实现细粒度的访问控制,但是对该模型的管理较为复杂,比如为特定用户激活特定的权限等操作实现起来过于烦琐,而且该模型对一些组活动的支持也不够,如通过组内成员投票做出某种决定等;空间访

到稿日期:2008-01-30 本文受国家自然科学基金项目(60403027, 60773191, 70771043),国家高技术研究发展计划(863计划)项目(2007AA01Z403),中国博士后科学基金项目(20060400846),湖北省自然科学基金项目(2005ABA258),软件工程国家重点实验室开放基金项目(SKLSE05-07),华为科技基金项目(YBIN2006089)资助。

於光灿(1974-),男,博士研究生,主要研究领域为分布式计算、分布式系统安全;**李瑞轩**(1974-),男,博士,副教授,主要研究领域为分布式异构系统、分布式系统安全;**卢正鼎**(1944-),男,教授,博士生导师,主要研究领域为分布式计算、软件集成环境、数据库系统、信息安全;**宋 伟**(1978-),男,博士研究生,主要研究领域为分布式异构系统及安全;**唐 卓**(1981-),男,博士研究生,主要研究领域为分布式异构系统及安全。

问控制模型(Space)[7]中两个关键部件是边界和访问图,访问控制主体对客体的访问权取决于客体所处的位置以及主体是否能够通过某种路径进入客体所在的位置,该模型的主要问题是访问控制的粒度过于粗糙,处于同一区域中的所有用户具有相同的访问权限;这种类型的模型的共同点是针对性较强,仅适用于特定应用背景的协作系统,不能满足协作环境中更广泛的安全性需求。第三种类型为协作环境中通用的访问控制模型,基于场所的访问控制模型(Locale-BAC)[8]主要特点是引入了"场所"的概念,通过在权限上定义约束实现一些基本的组操作,但是该模型对场所的使用比较僵化,授权约束比较单一,不能满足协作环境中对授权的灵活性要求。

研究表明,在协作环境中上下文信息是影响授权决定的重要因素,上述的几种访问控制模型也充分体现了这一点。除了前面介绍的被应用于协作系统的访问控制模型外,还有其他几个模型突出不同方面上下文信息对授权决定的影响。其中,基于角色的通用时态访问控制模型(GTRBAC)[9]主要解决时间方面的授权约束,包括周期和时间段约束,能够控制用户在特定的时间里才能执行特定的操作;基于角色的空间感知访问控制模型(GEO-RBAC)[10]中定义了空间对象,能够控制用户在特定的空间获得特定的权限;组通信系统中基于角色的访问控制框架[2]中引入了组上下文和会话上下文变量,实现了组内多用户通过投票机制做出授权决定。这些模型从不同的方面做出了有益的探索,为协作环境中访问控制模型提供了相关的理论基础。

本文所提出的协作环境中基于场所的访问控制模型以Locale-BAC模型为基础,对Locale-BAC模型中的角色、权限、场所等主要部件进行了重新定义,扩展了该模型对权限的约束机制,提出了基于时间、空间、上下文状态变量的授权约束,并引入了组成员通过投票确定授权决定的方法。我们的模型能够实现在全局访问控制策略约束下制定协作小组内部的一些自主访问控制策略,实现全局访问控制和协作小组内部自主访问控制相结合。

2 协作环境中基于场所的访问控制模型

协作环境中基于场所的访问控制模型是以Locale-BAC模型为理论基础,而Locale-BAC模型的理论基础来源于Fitzpatrick的基于场所的框架理论[11]和目前被广泛使用的基于角色的访问控制模型(RBAC)[4]。场所可以理解为可视化的组空间[12],为用户提供交互的场所及各种交互手段。本文所提出的协作环境中基于场所的访问控制模型在以下几个方面对Locale-BAC模型进行了扩展:(1)对角色、权限、场所等模型主要部件重新定义,赋予各自不同的新特性;(2)在模型中新提出基于时间、空间、上下文状态变量的授权约束,并引入了组成员通过投票确定授权决定的方法。这些扩展的意义和作用在下文中详细说明。

2.1 相关概念

如图1所示,协作环境中基于场所的访问控制模型包括用户(U)、角色(R)、权限(P)、会话(S)、场所模板(LT)、场所(L)及约束等7个基本部件。

用户的定义与RBAC模型中用户的定义相同,是一个通用概念,可以包括智能代理(例如机器人等),出于简化目的,用户被简单视为普通的人。

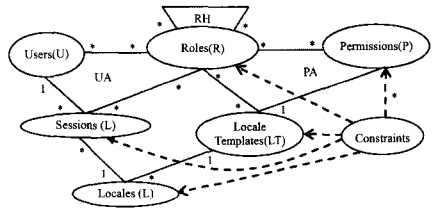

图1 协作环境中基于场所的访问控制模型图

角色在语义上与RBAC模型中角色的定义相同,但为了实现协作环境中更为灵活的访问控制,在形式上采用基于角色的信任管理语言(RT)中角色的形式[13],RT结合了基于角色的访问控制模型与信任管理系统的优点,其核心思想就是角色(或属性)概念。角色由主体(用户)和属性项组成,属性项由属性名和零个或多个参数构成。例如,admin. student (name="John Smith",category="fulltime")是一个由安全管理员admin定义的学生角色,只有安全管理员admin可以将用户指派给该角色。

权限的定义也与RBAC模型中权限的定义基本相同,但是为了更方便、直观地体现多用户的协作关系,在RBAC模型的权限基础上就以下两个方面加以扩展:(1)明确地将权限定义到场所中,因为一个特定的场所为一组用户提供多种访问资源的能力和交互手段以实现共同的目标,所以在场所中定义一组权限是较为直观和便于理解的。(2)提出权限的可传递性的概念,通常在组织内部存在一个层次化的人力资源模型,例如:公司、学校、政府、军队等,在层次化的人力资源模型中,处于较高层次的用户往往比处于较低层次的用户具有更多的权限,所以,人们很自然地想到将人力资源模型中的层次转化为访问控制模型中的角色层次;但是不同层次的岗位具有不同的职责,行使特定的权限,根据组织的安全策略和组织分工,一些权限只允许由岗位对应的用户才能行使,而不能由处于更高层次岗位的用户行使,而在角色层次中,较高层次角色自动继承其下层角色的权限;为了解决这个矛盾,本文提出权限的可传递性概念,将权限分为可传递和不可传递的两种,只有可传递的权限才可被上层角色所继承;从用户角度看,用户想要获得不可传递的权限,该用户必须直接被指派给那些指派了不可传递的权限的角色。

场所的概念来源于Fitzpatrick的基于场所的框架理论,场所可以理解为可视化的组空间,为用户组提供交互的场所及各种交互手段。Locale-BAC模型中引入场所作为访问控制基本部件。因为场所是一个组空间,用户组在场所内通过交互以完成共同的任务,所以场所内需要控制策略以实现对诸如加入场所等组操作的控制;另外,对于场所的创建等操作的控制不可能在场所内的控制策略中加以实现,所以必须有一个控制策略在场所之外,先于场所而存在,用于确定场所的创建者、控制者。在Locale-BAC模型中的场所只有安全管理员才可创建场所并确定场所内的所有控制策略,而且对于功能相同或相近的场所,也必须由安全管理员重复创建场所和重复定义场所内的控制策略,例如,安全管理员为课程A创建了"教室"场所,并定义了场所内的控制策略,如果要增设课程B的"教室"场所,安全管理员需要将所有的工作重新再做一次;而且不同的场所在满足全局安全性要求的条件下,可能有不同的自主性控制要求,比如,课程A的教师可能不允许

迟到的学生进入教室，而课程 B 的教师则可能相反；Locale-BAC 模型难以满足这种全局访问控制和场所中的自主访问控制相结合的灵活性要求。为了解决这个问题，本文在 Locale-BAC 模型的基础上，提出场所和场所模板的概念。场所模板定义一类具有相同或相似特征场所的共性的特征，而场所是根据场所模板的定义创建的，是多用户进行协作工作的物理组空间。在实际应用中，访问控制往往要考虑到环境的因素，为了满足这一需求，文中引入场所上下文的概念，场所的上下文类似于 Unix 操作系统中环境变量的概念，包括一个名称/值对的集合，场所的上下文提供当前场所的状态信息，如当前时间、课程是否已经开始等。场所的上下文在场所模板中定义，而在不同的具体的场所中，这些上下文变量被赋予不同的值，以表示这些场所所处的状态。场所和场所模板的关系是多对一的关系，即根据一个场所模板可创建多个场所；场所模板中定义场所内的全局性访问控制策略，定义存在于场所之外的先于场所而存在的一些必要的控制策略，如场所内所包含的权限、角色场所指派关系、场所上下文、场所的创建者、控制者等；而场所一经创建，场所的控制者可根据场所的协作需要，在场所全局访问控制策略约束下制定本场所内部的一些自主访问控制策略，实现全局强制性访问控制和场所中的自主访问控制相结合。比如，在“教室”场所模板中，定义“教师”和“学生”角色，以及相关的上下文变量，而在特定的场所“教室-502”中，场所的控制者可控制教师和学生何时以及如何才能激活其对应角色进入“教室-502”场所中。

会话的定义与 RBAC 模型中基本相同，不同之处有以下两点：(1)在协作环境中基于场所的访问控制模型中，会话被定义在场所上，是联系用户与场所之间的桥梁。当用户想要加入某一场所，用户必须在该场所上建立一个会话，在建立会话的过程中，用户可以激活一个或多个其被指派的角色，同时用户将要激活的角色还要受到角色场所指派关系的限制，即用户不能激活没有被指派到该场所的角色，即使用户被用户安全管理员指派给该角色。会话在用户和场所之间建立一对一的联系，但是可以在用户和角色之间建立一对多的联系。(2)在会话中引入上下文的概念。因为在实际应用中，访问控制除了要考虑到场所的上下文所能表达的场所的状态信息，同时还要考虑到用户会话中与用户相关的一些上下文信息，如用户所使用的 IP 地址、用户所激活角色的参数值以及用户的认证信息等，这些上下文信息是在场所上下文中所不能或不便于表达的。与场所的上下文类似，会话上下文也采用类似于 Unix 操作系统中环境变量的概念，包括一个名称/值对的集合，会话上下文提供当前用户的状态信息。

2.2 模型定义

模型的基本部件包括用户集合(*Users*)、角色集合(*Roles*)、权限集合(*Permissions*)、场所模板集合(*Locale Templates*)、场所集合(*Locales*)以及会话集合(*Sessions*)。

• U,R,P,LT,L,S 分别代表用户、角色、权限、场所模板、场所、会话。

• 角色 R 的基本形式为 $A.r(h_1,h_2,\cdots,h_n)$，A 代表有权将用户指派给该角色的管理用户，本文不考虑分布式授权管理，所以此处的 A 代表全局安全管理员，在本文下面的论述中出于简化目的将省去管理用户 A。$h_1,h_2,\cdots,h_n$ 代表角色的参数，参数的个数可以为零也可为多个，被指派给该角色的不同的用户可以被赋予各自不同的参数值。

• 对于 $\forall lt\in LT$，$\exists V_{lt}$(场所模板 lt 的上下文变量集合)，即每个场所模板对应一个上下文变量的集合。对应于场所模板上下文，$\forall lt\in LT$，$\exists VP_{lt}\subset P$，VP_{lt} 为能够设置场所中上下文变量的值的权限，$VP_{lt}=\{(set,v)\mid \forall v\in V_{lt}\}$。对于 $\forall lt\in LT$，$\exists\{creator(lt\_name=\text{‘}lt\text{’},l\_name),controller(lt\_name=\text{‘}lt\text{’},l\_name)\}\subset R$，即每个场所模板中存在两个内置的角色：创建者(*creator*)和控制者(*controller*)，参数名 *lt_name* 指示该场所模板的名，*l_name* 指示根据场所模板所创建的场所名。即被指派给这两个场所模板内置角色的用户在场所被创建后，其对应的 *l_name* 参数被设置为该场所的名称。

• $UA\subseteq U\times R$，多对多的用户－角色指派关系。

• $RA\subseteq R\times LT$，多对多的角色－场所模板指派关系。

• $PA\subseteq P\times R$，多对多的权限－角色指派关系。

• $RH\subseteq R\times R$，角色集合的偏序关系，称为角色的层次关系或统治关系，记为$\geqslant$。

• $lt\_perm:LT\rightarrow 2^P$，*lt_perm* 函数将任意场所模板 lt_i 映射为一个权限的集合，并且 $\forall lt_i,lt_j\in LT(i\neq j)$，$lt\_perm(lt_i)\cap lt\_perm(lt_j)=\emptyset$。

• $locales:LT\rightarrow 2^L$，*locale* 函数将任意场所模板 lt_i 映射为一个场所的集合，该集合中的场所为根据场所模板 lt_i 所创建，并且 $\forall lt_i,lt_j\in LT(i\neq j)$，$locales(lt_i)\cap locales(lt_j)=\emptyset$，$L=\bigcup_{(\forall lt)[lt\in LT]}locales(lt)$。

• $can\_trans:P\rightarrow\{true,false\}$，*can_trans* 函数将任意思权限 p_i 映射为布尔值 *true* 或 *false*。如果 $can\_trans(p_i)=true$，且 $(p_i,r_m)\in PA$，对于 $\forall r\geqslant r_m$，角色 r 可继承权限 p_i，反之则不能。

• $user:S\rightarrow U$，*user* 函数将任意会话 s_i 映射为单一用户 $user(s_i)$(该用户在会话的生命周期内保持不变)。

• $locale:S\rightarrow L$，*locale* 函数将每个会话 s_i 映射为单一场所 $locale(s_i)$(该场所在会话的生命周期内保持不变)。

• $sessions:L\rightarrow 2^S$，*sessions* 函数将每个场所 l_i 映射为一个会话的集合，$sessions(l_i)=\{s\mid \forall s\in S,locale(s)=l_i\}$(该会话的集合在场所的生命周期内随着用户的加入和退出动态变化)。

• $roles:S\rightarrow 2^R$，$roles(S)$ 函数将每个会话 s_i 映射为一个角色的集合，$roles(s_i)\subseteq\{r\mid(\exists r'\geqslant r(r,r'\in R),\exists lt\in LT),(user(s_i),r')\in UA\wedge locale(s_i)\in locales(lt)\wedge(r,lt)\in RA\}$，该角色的集合表示用户在会话 s_i 中所激活的角色(该集合随着用户激活和取消激活角色而动态变化)。

• $roles:L\rightarrow 2^R$，$roles(L)$ 函数将每个场所 l_i 映射为一个角色的集合 $roles(l_i)\subseteq\bigcup_{s\in session(l_i)}\{r\mid r\in roles(s)\}$，该角色的集合表示在场所 l_i 中所激活的角色。

• $permissions:S\rightarrow 2^P$，$permissions(S)$ 函数将每个会话 s_i 映射为一个权限的集合，$permissions(s_i)=\bigcup_{r\in roles(s_i)}\{p\mid(user(s_i),r)\in UA\wedge(p,r)\in PA\}\bigcup\bigcup_{r\in roles(s_i)}\{p\mid(user(s_i),r)\notin UA\wedge(p,r)\in PA\wedge can\_trans(p)=true\}$，该权限的集合表示会话 s_i 中所拥有的所有权限。

• $permissions:L\rightarrow 2^P$，$permissions(L)$ 函数将每个场所 l_i 映射为一个权限的集合，$permissions(l_i)=\bigcup_{s\in session(l_i)}\{p\mid p\in permissions(s)\}$，该权限集合表示当前参与到场所 l_i 中所有

用户所拥有的权限的集合。

2.3 模型的一个示例场景

为了便于模型的展示，我们构建了一个虚拟的、简化的教学机构，该教学机构的角色层次图如图 2 所示。

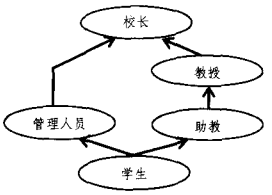

图 2　虚拟教学机构角色层次图

针对该教学机构，我们的模型中用户角色指派及角色场所模板指派关系如表 1 和表 2 所示，表 3 和表 4 描述教师办公室和教室两个场所模板里的权限角色指派关系。

表 1　用户角色指派（UA）

		角色				
		校长	管理人员	教授	助教	学生
用户	赵一	√				
	钱二		√			
	孙三			√		
	李四				√	
	周五				√	
	武六					√
	郑七					√

表 2　角色到场所模板指派（RA）

		角色				
		校长	管理人员	教授	助教	学生
场所	行政办公室	√	√			
	教师办公室			√	√	
	教室	√	√	√	√	√

表 3　教师办公室场所模板里权限角色指派

权限	角色	是否可传递
教学准备	教授，助教	False
批改试卷	教授，助教	False
修改学生课程记录	教授，助教	False
查阅学生课程记录	教授，助教	True

表 4　教室场所模板里权限角色指派

权限	角色	是否可传递
讲课	教授，助教	False
布置作业	教授，助教	False
参加考试	学生	False
做作业	学生	False
提问题	学生	True

在该教学机构中，根据语义特性，角色被指派到特定的场所模板，比如教授角色被指派到教师办公室和教室场所模板，被赋予教授角色的用户可以在由这两个模板创建出的场所中开展工作；在场所模板中根据应用需求定义的权限被指派给对应的角色，比如教师办公室场所模板里的教学准备权限被指派给教授和助教角色。示例中还展示了权限的可传递特性，根据角色的层次图，被指派为校长的用户可以在根据教室场所模板创建出的特定教室场所中激活学生角色，该用户不能使用参加考试、做作业等不可传递权限，但是可用使用提问题等可传递权限。通过引入权限的可传递特性，可以很方便地将组织的人力资源模型转换为角色的层次模型，具有一定的现实意思。当然在传统 RBAC 模型中，可以用私有角色这一概念解决相同的问题，但是有可能造成角色数量的膨胀，给角色的管理以及用户角色的指派带来管理负担。

在上述的示例中，通过定义模型的基本部件，如用户角色指派、角色场所模板指派、角色权限指派、角色层次等，实现了虚拟教学机构中的一个较为粗糙的访问控制策略，该策略控制到场所模板级别的访问，体现组织中总体的安全需求，属于组织的全局性安全策略。但是不能满足不同协作场所中灵活的细粒度的访问控制需求，比如被赋予教授角色的用户何时、何地及如何才能激活教授角色进入特定的教室场所等。在下一节中我们将通过约束机制，来满足这种灵活的细粒度的访问控制需求。

2.4 授权约束

将场所框架理论引入到访问控制模型意味着授权决定往往要考虑到环境因素，授权约束机制是体现环境因素对授权决定的影响的有效手段。本节从对权限的约束和对角色的约束两个层次上讨论授权约束。

2.4.1 角色约束

GTRBAC 模型中提出了角色的三种状态，不可激活状态（disabled）、可激活状态（enabled）和激活状态（active），以及角色状态的相互转化规则。根据角色的三种状态及其转化规则，本文的角色约束从大的方面分为两种，一种为使能约束，用于控制角色从不可激活状态向可激活状态转化，另一种为激活约束，用于控制角色从可激活状态向激活状态转化。GTRBAC 模型中较为详细地讨论了基于时态的角色约束，但是该模型中没有考虑到引入场所及场所模板后的情况，约束的粒度较为粗糙，我们将通过引入场所的概念对该模型进行扩展。

角色的周期性使能约束用于指定角色处于不可激活状态或可激活状态的时间间隔，GTRBAC 模型中给出的周期性约束通用形式为：

$(I, P, pr; enable/disable\ r)$

其中 P 为周期性时间表达式，可以表达如“每月第一天的第三个小时”类似的时间间隔，I 为一个时间区间，如[1/1/2001，12/31/2001]，其形式化定义参见 GTRBAC 模型，pr 为优先级定义。该表达式表示在 (I, P) 指定的时间间隔内，角色 r 处于可激活（enable）或不可激活（disable）状态。本文引入场所模板及场所概念后，周期性约束通用形式变为：

$([lt: lt\_name | l: l\_name], I, P, pr; enable/disable\ r)$

$lt: lt\_name$ 选项将约束限制在根据场所模板 lt_name 所创建出的所有场所中，$l: l\_name$ 选项将约束限制在特定的场所 l_name 中，如果省略 $[lt: lt\_name | l: l\_name]$，则该约束与 GTRBAC 模型中的约束形式与意义均相同，即前者是后者的一个特例。GTRBAC 模型中约束的粒度较为粗糙，我们通过引入场所的概念对该模型进行扩展后，更细粒度和更灵活的基于时态的约束机制得以实现。例如，定义 (I, P) 为 NightTime（9:00 pm-9:00 am）：

$\text{NightTime} = ([12/1/2000, \infty], all.\ Days + 22.\ Hours \triangleright 12.\ Hours)$

则在 GTRBAC 模型中只能使用（NightTime，disable 教授）表

达“教授角色在晚上处于不可激活状态”的约束，该约束被应用于所有的场所，包括“教室”、“教师办公室”等，使用该约束后，在“教师办公室”场所，“教授”角色晚上处于不可激活状态。引入场所模板及场所概念后，可以使用(lt:教室，Night-Time，disable 教授)表达“教授角色晚上在教室场所中处于不可激活状态”的约束，该约束只被应用于“教室”场所，使用该约束后，教授们晚上只是不能激活“教授”角色进入“教室”场所，而不影响在其他场所(如“教师办公室”)角色的状态。对角色其他几种形式时态约束的扩展方法与此类似，在此不再一一描述。

2.4.2 权限约束

Locale-BAC 模型中提出了两种类型的权限约束：全部特权法则(Principle of All Privileged)和最大授权法则(Principle of Greatest Authority)。在此基础上，本文提出两种有用的权限约束：权限的排他性约束和权限的势约束。当然，随着协作工作研究的进展，可能有更多有用的约束被发现，所以我们的模型采用开放的约束机制，将来被发现的新约束可以不断地充实到模型中。因为我们的模型对 Locale-BAC 模型的场所的概念进行了扩展，全部特权法则和最大授权法则的表现形式也发生了变化，文中将对这两个法则重新描述。

全部特权法则：如果权限 p 被定义为全部特权权限，当场所中的某个会话试图调用该权限时，要求该场所中当前所有会话都具有调用该权限的能力。设 AP 为场所模板 lt 上全部特权权限的集合，显然 $AP \subseteq lt\_perm(lt)$，$access(s,p)$ 表示在会话 s 中调用权限 p，则：

$$(\forall p \in AP, \forall l \in locales(lt), s \in sessions(l))[access(s,p) \Rightarrow (\forall s' \in sessions(l)[p \in permissions(s')])]$$

最大授权法则：如果权限 p 被定义为最大授权权限，当场所中的某个用户想要调用该权限，则该用户必须激活一个特定的角色，该角色是场所所有具有该权限(直接指派或继承)且被激活角色中处于角色层次中最高层次的角色。设 GP 为场所模板 lt 上最大授权权限的集合，显然 $GP \subseteq lt\_perm(lt)$，则：

$$(\forall p \in GP, \forall l \in locales(lt), s \in sessions(l))[access(s,p) \Rightarrow (\exists r \in roles(s)[((\exists r' \leqslant r)[(p,r') \in PA]) \wedge ((\neg \exists r'' \in roles(l))[r < r'']])]$$

排他性权限：如果权限 p 被定义为排他性权限，场所中同一时刻只允许有一个用户调用该权限。设 EP 为场所模板 lt 上排他性权限的集合，显然 $EP \subseteq lt\_perm(lt)$，则：

$$(\forall p \in EP, \forall l \in locales(lt), s \in sessions(l))[access(s,p) \Rightarrow (\neg \exists s' \in sessions(l) \wedge (s \neq s'))[access(s',p)]]$$

例如，在 2.2 节的示例场景中，教室场所模板中的“提问题”权限可以定义为排他性权限，即虽然所有的学生都拥有“提问题”的权限，但是同一时刻只允许有一个学生提问题。

势约束权限：如果权限 p 被定义为势约束权限，设势为 n，则该权限在场所中被调用的前提条件是该场所中当前拥有该权限的用户数不低于 n。设 p 为场所模板 lt 上的势约束权限，则：

$$(\forall l \in locales(lt), s \in sessions(l))[access(s,p) \Rightarrow (\exists S' \subseteq sessions(l) \wedge (\forall s' \in S, 'p \in permessions(s)))[\# S' \geqslant n]]$$

例如，在军事指挥系统中，一些重要的操作，比如发布重要的作战命令等，往往需要多名指挥员同时在场的情况下才能发布。

结束语 本文在 Locale-BAC 模型基础上提出协作环境中基于场所的访问控制模型，引入 RT 中相关概念重新定义角色，提出权限的可继承性，便于将组织内的人力资源模型直接转化为角色层次模型，将场所的概念扩展为场所模板和场所(实例)，这样在场所模板上定义全局安全策略，在全局安全策略的约束下在场所上定义协作组内的自主访问控制策略，实现全局访问控制和协作小组内部自主访问控制相结合的灵活分层授权机制。随着社会的进步和经济全球化，多领域大范围的协作成为一种趋势，不同组织为了共同的利益建立协作关系，研究多组织间协作环境下的访问控制模型成为必要。我们将以协作环境中基于场所的访问控制模型为基础，在对现有组织内部及组织间协作模式进行深入研究的基础上，研究针对该模型的分布式管理模型及多组织间协作环境下基于场所的访问控制模型。

参 考 文 献

[1] Tolone W J, Ahn G J, Pai T. Access Control in Collaborative Systems. Technical Report. UNC Charlotte: SIS Department, 2002

[2] Bhatti R, Bertino E. A Framework for Role — Based Access Control in Group Communication Systems // Proceedings of the Second IEEE International Symposium on Network Computing and Applications. 2003:562-569

[3] Sandhu R, Samarati P. Access control: Principles and practice. IEEE Communications, 1994,9: 40-48

[4] Sandhu R, Coyne RS, Feinstein EJ, et al. Role-based access control models. IEEE Computer, 1996, 29(2):38-47

[5] Thomas R, Sandhu R. Task - based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management // 11th IFIP Working Conference on Database Security. Lake Tahoe Califorttia, August 1997:166-181

[6] Thomas R. Team-based access control (TMAC) // Proceedings of 2nd ACM Workshop on Role-Based Access Control. Fairfax, VA, 1997:13-19

[7] Bullock A, Benford S. An access control framework for multi-user collaborative environments // ACM GROUP. Phoenix, AZ, 1999:140-149

[8] Tolone W J, Gandhi R A, Gail - Joon A. Locale - Based Access Control: placing collaborative authorization decisions in context // Proc. of the IEEE Conference on System, Man and Cybernetics. 2003:4120-4127

[9] Joshi JBD, Bertino E, Latif U, et al. Generalized Temporal Role Based Access Control Model. IEEE Transaction on Knowledge and DataEngineering, 2005,17:4-23

[10] Bertino E, Catania B, Damiani ML, et al. GEO-RBAC: a spatially aware RBAC // Proceedings of the tenth ACM symposium on Access control models and technologies. June 2005:29-37

[11] Fitzpatrick G. The Locales Framework: understanding and Designing for Cooperative Work. Ph. D. Thesis. The Univ. of Queensland, Australia, 1999

[12] Fitzpatrick G, Mansfield T, Kaplan S. Locales Framework Exploring foundations for collaboration support // IEEE Proceedings of OzCH1. Hamilton, New Zealand, 1996:34-41

[13] Li NH, Mitchell J. Datalog with constraints: A foundation for trust management languages // Proceedings of the Fifth International Symposium on Practical Aspects of Declarative Languages (PADL 2003). Springer, January 2003:58-73