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*)

陈伟鹤　鞠时光　薛安荣

(江苏大学计算机科学与通信工程学院　镇江 212013)

摘　要　在实际生活中,随着人们所处空间位置的变化,其扮演的角色也会相应发生改变。基于位置的服务作为IT信息服务的重要内容,它根据用户所处空间位置向其提供在当前环境下所需的数据信息。为了保护隐私,保证数据资源不被非法利用,迫切需要对基于移动用户位置的信息服务中的访问控制模型技术进行研究。对现有的具有代表性的空间访问控制模型作了介绍,并进行了分析比较,探讨了在空间访问控制模型的进一步研究中需要解决的关键问题。

关键词　基于位置服务,访问控制模型,空间,隐私,信息安全

Survey on the Novel Access Control Model of Location-based Service Based on the Spatial Location of Mobile User

CHEN Wei-he　JU Shi-guang　XUE An-rong

(School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract　In the real life, the playing role of everyone is changed when the physical location of this man/woman is located in another different spatial extension. Location-based service is the essential element of the IT information service. It provides the requested data to the authorized user who is authenticationed based on his/her physical location. In order to protect users privacy and stop the illegal using of protected data, it is urgent to promote the study of the novel access control model of the location-based service based on the spatial location of each mobile user. Several representative spatial access control models were studyed and compared in details. Some key problems which must be resolved in the future study were listed and briefly discussed.

Keywords　Location-based service, Access control model, Spatial, Privacy, Information security

1　研究的背景

基于位置的服务(Location-based Services)[1]是IT服务中的重要内容,它向用户提供经过搜集、整理、过滤过的信息。它提供服务时必须依据用户当前所处的空间位置、信息(数据)存储的位置,以及系统的访问控制策略等因素,做出是否向特定用户提供信息服务的决策,并进行相应的后续操作。

随着现代通信技术日新月异,用户期望利用移动终端可以在任何时间、任何地点使用网络信息和服务,而无线定位技术的发展为这种需求提供了可能性,尤其是全球定位系统(GPS)的出现使得无线定位技术产生了质的飞跃,定位精度得到了大幅度的提高,由此导致对基于用户位置服务(Location-based service)和移动应用(mobile applications)的需求也相应增加。

为了比较清楚地说明基于位置的服务的概念,我们考虑医院的例子。假定这个医院的信息化程度很高:所有的病人信息,包括病历和医疗诊断信息都存放到一个统一的信息服务器上面;所有在这个医院工作的医生和护士的信息,包括他们所属的工作部门等信息,也存放在这个服务器上面。另外,这个医院的每个医生、护士、病人都随身携带一个可以空间定位的无线信息处理终端,利用它用户可以获取各种必要的信息。为了简化起见,在这个例子中我们只考虑医生、护士、病人这三种人。医生按科室划分成不同病种的主治医生,每个医生只负责诊断和治疗一种病症,比如:心脏科的医生、肿瘤科的医生、妇产科的医生等。护士也按照所属科室的不同而护理不同病种的患者,每个护士只负责护理一种病症的患者,比如:心脏科的护士、肿瘤科的护士、妇产科的护士等等。为了保护病人的隐私,在这个医院信息服务系统中,规定不同种类的用户所能够获取的信息根据他们在医院的日常工作中所扮演的角色的不同而不同。不仅如此,对于同一个用户,当他处在不同的空间位置的时候能够获取的信息也会受到不同的限制。不妨以一个心脏科的医生为例子进行说明,他在上班时间能够通过其随身携带的无线信息处理终端获取他所负责诊断和治疗的那一部分心脏科病人的情况,包括详细病历、病史和其他的相关情况。而在下班以后,即使他还在诊室,也不能再利用无线信息处理终端查询他白天负责治疗的病人的信息。而对一个心脏病病区的护士而言,她通过她所携带的无线信息处理终端,只能够查到她所负责护理的那几个心脏病病人的每日护理要求信息。而且她只能够在上班时间,且在她所工作的病房内才能够查询并获得这些信息。一旦她所处的空间位置离开了她所负责的病房,那么即使是在上班时间,她也不能够利用无线信息处理终端从医院的信息服务器查到她所负责护理的病员的数据。医院的信息服务器要能够实现这样的访问控制约束,就必须能够在处理用户的访问请求的

*)受国家自然科学基金"基于移动用户位置的服务中的访问控制模型研究"(项目编号:60603041),江苏省自然科学基金(BK2006073)和江苏大学高级人才启动基金(07JDG031)支持。**陈伟鹤**　副教授,博士,主要研究方向为信息安全、数据库理论;**鞠时光**　教授,博导,主要研究方向为数据库理论与应用、信息安全、计算机图形学;**薛安荣**　副教授,主要研究方向为数据挖掘、多媒体技术。

时候，首先根据用户的信息，判断出发出访问请求的用户所扮演的角色，也就是他究竟是医生还是护士或者病人。如果是医生，那么他是负责治疗什么病种疾病的医生；如果是护士，那么她是负责护理什么病症病人的护士，她所负责护理的病房是哪些病房。医生、护士或者病人所携带的具有无线定位功能的信息处理终端能够在用户提交信息查询请求给医院的信息服务器的时候，把该用户当前所处的空间位置信息、发出查询请求的时间、用户的身份识别信息一同提交给信息服务器。这样，对医院信息服务器上运行着的负责存储和管理医疗信息的数据库系统而言，必须能够灵活地、智能地根据信息查询者所扮演的角色、所处的空间位置、发出查询请求的时间信息以及用户期望获取的具体信息来进行访问控制决策。只有当请求信息的用户的角色、所处的位置、发出查询请求的时间符合系统的访问控制策略的时候才允许向用户的无线信息处理终端返回所查询的信息。

实际上除了像医院这样的应用场合以外，在银行、环境保护和国防信息系统中都有着相同的访问控制策略。例如，在一个银行的个人客户保险柜访问控制系统中，租用了保险柜的客户拥有一个角色，该角色具有打开其所租用的保险柜的权限。从我们日常生活的经验可以知道，实际上一个用户要能够正常打开所租用的保险柜至少要满足下面的两个条件：(1)用户必须在保险柜附近；(2)同时必须是银行上班时间才能打开这个保险柜。这种情况下，激活这个角色的约束条件是银行上班时间和用户在这个保险柜附近。由于篇幅有限，就不再举例子说明这种访问控制系统应用到环境保护和国防信息系统中的例子了。

通过分析上面这两个例子，可以发现尽管具体的应用场合不同，但是它们在实施访问控制的时候都受到相同因素的制约：根据用户所处的空间位置、用户扮演的角色、用户提出查询请求的时间这三个信息共同进行访问控制决策。因此，我们称这类基于移动用户位置的服务中的访问控制模型为空间访问控制模型。为了便于文章余下部分的论述，下面尝试给出它的描述性定义。

定义 1(基于移动用户位置的服务中的访问控制模型)
它是基于位置的信息服务系统中的访问控制模型。它在进行访问控制决策时，根据提交信息访问请求的用户在本次会话中所扮演的角色、用户所处的当前空间位置、用户提交信息访问请求的时间和信息服务系统的访问控制策略进行判断。只有当提交信息访问请求的用户当前所扮演的角色、所处的当前空间位置、用户提交访问请求的时间都符合信息服务系统中所定义的安全策略的时候，才允许该用户的本次访问请求。否则，系统拒绝用户的本次访问请求。

Google Earth[2]是一个在对地理信息进行共享时，由于缺乏对地理信息的合适访问控制从而导致危害国家安全的反面例子[3]。它是美国 Google 公司推出的集卫星图像、航拍图像和地图于一体的免费地理信息服务。虽然 Google 公司一再强调它作为教学和导航工具的作用，但是世界各国(除了美国)普遍感受到 Google Earth 对各自国家安全的威胁，因为 Google Earth 不加限制地提供了许多国家的敏感目标的信息。例如，Google Earth 上公布了许多外国政府办公机构的详细位置和外部特征照片、军事设施以及其它重要设施的图像等。这客观上降低了恐怖分子策划恐怖袭击的难度，因为原来需要花较长时间进行的拟攻击目标信息收集工作，借助 Google Earth 这个价廉"物美"的工具就能够很方便地完成。另外别有意味的是，人们也已经发现 Google 公司在推出 Google Earth 服务时，并没有做到它所宣称的平等对待，一个明显的证据就是 Google Earth 所提供的美国的敏感政府部门的地理信息，无论是照片还是空间定位信息都是不准确的，甚至存在极大的错误，这并不是偶然的技术失误，实际上表明美国政府和 Google 公司都知道 Google Earth 对国家安全的危害，它这么做的真实目的也就值得怀疑了。可以设想一下，如果 Google Earth 具有合适的访问控制机制，使普通用户不能够查询到敏感的信息，那么至少可以增加恐怖分子发动袭击的准备时间和实施难度。

随着基于移动用户位置的信息服务种类的不断丰富和发展，以及人们越来越意识并关注到地理空间信息在国家安全和环境保护等战略应用中的重要作用，这类信息服务系统对能够根据用户所处空间位置信息进行访问控制的空间访问控制模型产生了强烈需求，它是保障各种基于用户位置 IT 服务安全的重要措施。

本文余下部分组织如下，按照访问控制模型提出的时间顺序，首先介绍最早出现的适用于卫星图像访问控制的地理空间授权模型 GSAM(Geo-Spatial Authorization Model)，GSAM 模型在实施访问控制时仅仅考虑了被保护的数据本身所具有的空间特性。随着空间访问控制模型研究的深入，和 GSAM 模型相比，在后续提出的空间访问控制模型中，同时考虑了被保护的数据本身所具有的空间特性和访问请求提出者提出访问请求时的空间位置信息。作为同时考虑数据和数据请求者空间位置信息的空间访问控制模型的典型代表，分别介绍 Web 服务地图访问控制模型、基于拓扑空间模型的访问控制模型、基于 XML 的面向服务的地理空间数据基础设施中的访问控制模型。最后，归纳总结出在空间访问控制模型的进一步研究工作中需要解决的关键问题。

2 相关研究工作

卫星技术很早就在军事领域得到了广泛应用，由于所获得的卫星图像涉及到很多敏感信息，因此对它的访问控制问题的研究也是最早得到学术界重视的。

2.1 仅考虑数据本身空间信息的访问控制模型

从目前掌握的文献来看，美国 Rugters 大学的 Chen 和 Atluri 在 1999 年最早提出了称为 GSAM(Geo-Spatial Authorization Model)的地理空间授权模型[4]，它是第一个用于对地理数据进行访问控制的模型，它保护的对象是卫星所拍摄的地面照片。

GSAM 模型在实施访问控制时仅仅考虑了被保护的数据本身所具有的空间特性。

2.1.1 GSAM 模型

Chen 和 Atluri 进行 GSAM 研究的原因在于这样一个事实：目前卫星轨道上有许多为政府部门和私人公司所拥有的卫星，随着卫星成像技术的不断进步，这些卫星给消费市场和信息服务领域提供了许多价格便宜、清晰度高的卫星照片。它们在环境监控、地图制作、救灾、基础设施的规划布局、国家安全、农作物收成预测等方面有广泛的应用，但是这些高清晰度的卫星图像是一把双刃剑，它在造福于国计民生、国家安全的同时，如果使用不当也将给国家安全、个人隐私、商业竞争带来很严重的负面影响。这是由下面两个方面的因素结合在一起所导致的：(1)对许多卫星图像提供商而言，他们有能力提供近乎实时的高清晰卫星图像；(2)许多政府机构和社会公

用事业部门组织搜集、存储、发布大量不涉及到个人隐私的信息。有了这两部分公开信息。一些别有用心的组织或者个人可以利用 GIS 系统的分析和信息集成能力，以及其所感兴趣的目标的经纬度数据，结合所获取的公开的个人信息和高清晰的卫星图像对特定的人、企业等感兴趣的目标的日常活动进行近乎实时的监控，这种情况对个人而言就会对个人隐私形成技术侵犯，对企业而言就可能存在不正当竞争。因此，在不久的将来，如果不对高清晰的卫星图像数据加上合适的访问控制机制的话，任何人都能够坐在家中，通过点击鼠标对世界任何角落的人进行监控，记录他的户外活动情况。在军事上，外国政府可以监控其他国家的军事调动和重要政府官员的日常活动情况。另外，对商业竞争而言，一个企业的竞争对手可以利用高清晰的卫星图像监控企业的日常货物运输情况，从而确立不正当的竞争优势。

Chen 和 Atluri 提出 GSAM 模型时考虑了两个关键因素：

(1)卫星图像的清晰度。显然关于同一目标的两张照片，如果其他方面都一样，而仅仅是清晰度有差异的情况下，一幅清晰度低的卫星照片给用户提供的信息与高清晰度的照片相比要少得多，因此在用户利用 GIS 和通过其他公开的渠道获得的感兴趣的目标对象的其他信息对目标进行监控时，由于清晰度低的卫星照片不能够提供足够的细节信息，那么他也无法对目标对象实施有效的监控，也就不能够侵犯目标对象的隐私信息。

(2)同一幅高清晰卫星图像的不同区域的保护级别不同，对不同的用户要区别对待。之所以高清晰卫星图像的覆盖范围在设计 GSAM 模型时很重要，是因为对一张反映大面积地面信息的高清晰卫星照片而言，它有很多局部细节信息，但是并不是对其中的每一个局部信息对该卫星照片的所有(潜在)用户都是敏感的，需要保密的。例如，一个企业主显然有权利从高清晰的卫星照片上看到他所拥有的企业所呈现的信息。但是，他的权限应该就局限在该卫星照片的这一部分，卫星照片上超出他所拥有的企业的地理空间范围的其他企业的卫星图像，尤其是竞争对手企业的高清晰度卫星照片数据就不应该泄漏给此用户，否则就可能造成不正当竞争。

简而言之，GSAM 的基本思想就是：对清晰度低的卫星照片不需要进行访问控制，对高清晰度的卫星照片必须进行访问控制；而且在进行访问控制时需要根据提出空间数据访问请求的用户的信息来进行访问控制决策，决定该用户能否获取整张高清晰度的卫星照片，还是仅仅允许获得此卫星照片中的某一个局部的数据。

在 GSAM 模型中，所支持的所有操作可以分成两大类：查看操作和维护操作。查看操作包括：view，zoom-in，overlay 和 identify 四个操作。而维护操作涉及到卫星图像数据库中数据的更新，包括：insert，delete 和 update 操作。其中，view 操作允许授权用户根据其权限查看卫星图像中某个特定部分或是整张卫星照片，当然该卫星照片的清晰度也必须是此授权用户有权查看的。放大操作 zoom-in 允许用户对卫星照片的某一个感兴趣的部分进行放大，在更高的图像清晰度的情况下查看特定地理空间的进一步信息。因此，在 GSAM 模型中，在对特定用户的放大操作定义授权许可时，必须对 zoom-in 操作相应地给出一个称为放大层次(zoom level)的规则，表示特定用户对卫星图像的放大操作可以达到的最高清晰度，例如记为(zoom-in:5)，GSAM 模型在进行访问控制决策时利用这个规则将用户对卫星照片细节进行放大的权限限制在照片清晰度最高为 5 米。对于 zoom-in 操作在进行授权规则定义的时候还要额外注意一点：因为可以通过图形学的方法对细节进行放大，但是对于照片而言，当照片的清晰度一定的情况下，单独利用图形学的放大算法放大该照片的任何一个部分一旦超过一定的比例以后就失去了意义，这是因为照片的像素是固定的，对于清晰度低的照片而言，像素较大，对地面目标的细部特征表现能力较弱，这样的低清晰度的照片一旦放大到一定比例后就不能够提供有价值的信息。因此，在给特定用户授权可以查看的卫星照片的最高清晰度的时候，必须考虑到用户有可能利用图形学的放大算法对卫星照片进行处理，所以授权用户可以查看的照片清晰度应该确保在用户对其进行图形学放大处理后获得的信息不能够侵犯他人的隐私，不妨碍公平竞争，不危害国家安全。要实现 zoom-in 操作，卫星照片数据库系统中必须存储同一地理空间对象在同一时间点上的不同清晰度的照片，以便当用户授权查看某一清晰度的地理空间对象的卫星照片时，如果他希望对其中的某个区域进行放大操作，就可以通过检索并查看卫星照片数据库中清晰度更高，但是其清晰度又在此用户得到授权的清晰度范围之内的照片来实现。

GSAM 模型的访问控制流程如下：当一个主体对一幅覆盖了某一地理空间的具有一定清晰度的卫星照片提出访问请求的时候，访问控制模块首先从地理空间授权基中找出与用户请求有关的所有授权规则；如果没有授权规则存在，则拒绝用户的访问请求；否则授权评价模块计算用户的访问请求中所包含的客体是否和地理空间授权基中找出的授权规则里面的客体有重合；如果有重合，那么就将用户的访问请求发送到后端的卫星图像数据库，检索出图像；由于返回的图像可能和用户有权查看的图像不完全匹配，那么还要对从卫星图像数据库返回的照片进行编辑、裁减，过滤掉多余的信息。

2.1.2 对 GSAM 模型的探讨

由于 GSAM 模型设计时考虑到了受保护的数据本身所具有的空间特性，因此 GSAM 模型被认为是一个最早提出来的空间访问控制模型，它适用的领域主要是卫星照片信息的保护。另外，在诸如 Internet 上的淫秽图像过滤、数字图像版权保护(防止未授权用户非法利用受版权保护的图像)以及基于内容的访问控制等应用领域都需要提供合适的能够对图像进行访问控制的安全机制，GSAM 模型都能够在其中找到用武之地。

GSAM 模型着眼于对卫星拍摄到的光栅图像的访问控制，目的是防止高清晰的卫星照片泄漏敏感信息。它所保护的实际上是一幅卫星照片或是一幅卫星照片中的某一个局部所蕴含的敏感信息。它并不支持对基于向量或者是基于拓扑关系的空间数据的保护，显然它是不能够解决 GIS 及空间数据库的访问控制问题的。另外，GSAM 只涉及到对卫星照片“读取”权限的处理，并没有考虑到对空间数据的动态更新问题，而数据的动态更新在 GIS 及空间数据库的应用中往往是大量存在，难以忽略的。

在 GSAM 模型的研究中还需要解决下列问题：(1)在传统的访问控制模型中，授权体现为访问控制列表。但是在 GSAM 模型中，由于授权涉及到空间属性数据，因此在增加了空间属性数据后如何对 GSAM 授权基进行维护？如何提高授权规则检索时的效率？如何对授权规则进行索引？这许多问题都需要进一步研究。(2)需要设计新的方法来验证授

权规约(authorization specification)的一致性。分析当同时出现 contains,overlap 和其他操作时是否会出现冲突? 是否需要以及如何设计消除冲突的策略? (3)另外,对授权基中授权规则的查找涉及到空间属性,因此需要进一步研究授权基的索引问题,并且需要进一步考虑如何将时间属性添加到索引结构中去。

2.2 同时考虑数据和数据请求者空间信息的访问控制模型

在数据库领域到目前为止已经提出了多种访问控制模型,但是由于空间数据库中数据的特殊性,它们并不适用于对空间数据的保护。这是因为以下几个原因:(1)空间数据库中的数据对象可以是 0 维的、1 维,或者是二维的,甚至更高维的;(2)用户只有在特定的空间区域才有权访问某些敏感的地理数据;(3)同一个空间数据对象既可以用几何学的方法描述,又可以用一组拓扑关系的集合进行描述,这种同一空间对象的多样化描述也是在研究新型空间访问控制模型时必须考虑的。

由于 GSAM 模型的设计目的只是为了对卫星照片数据库中所存储的不同清晰度的卫星照片进行访问控制,因此 GSAM 模型的适用范围比较有限:它仅仅能够对卫星照片这样的特殊类型的数据进行访问控制,并不能够对其他类型的符合 GIS 标准的空间数据对象进行有效的访问控制。

而且,GSAM 模型在实施访问控制时仅仅考虑了被保护的数据本身所具有的空间特性。随着空间访问控制模型研究的深入,人们发现在设计空间访问控制模型时有必要同时考虑被保护的数据本身所具有的空间特性和访问请求提出者提出访问请求时所处的空间位置信息。

Elisa Bertino 等人于 2004 年提出了一个对 Web 上的空间数据进行访问控制的模型[5],该模型同时考虑了被保护的数据对象和访问请求提出者提出访问请求时的空间位置信息。

2.2.1 Web 服务地图访问控制模型

Web 服务地图访问控制模型基于以下两个前提假设:(1)空间数据是地理空间中有确定边界的空间对象构成的集合;(2)远程用户对以 Web 方式共享的空间数据的操作都必须通过 Web 地图管理(服务)软件系统进行。Web 服务地图访问控制模型的目的是保证不同的用户能够以适当的方式对空间数据进行操作。这个模型的核心思想是把每个授权和特定的地理空间区域联系起来,这个区域称为"有界区域"(bounded region),特定的授权仅仅在这个空间区域内才成立。

Web 服务地图访问控制模型中引入了"空间授权"的概念,空间授权用于定义空间特性方面的约束。当用户需要访问某个空间数据对象时,Web 服务地图访问控制模型首先计算这个被请求的空间数据对象是否位于被授权的空间里,如果是,就准予访问。

在 Web 服务地图访问控制模型中,主体定义为所有使用 Web 地图管理服务系统的用户,按照用户在系统中所扮演的角色的不同,可以将用户划分成不同的类型。从本质上说 Web 服务地图访问控制模型采用了基于角色访问控制模型的基本思想:把不同类型的用户抽象成为不同的角色,每一个角色拥有不同的权限。在 Web 地图访问控制模型中,授权规则中的客体是一个空间特征类(spatial feature class)。在 Web 地图访问控制模型中,所涉及到的空间对象的类型采用 OGC(OpenGIS Consortium)所提出的几何模型,包括点、线、多边形、多点(multi-point)、多线(multi-line)、多多边形(multi-polygon)。相同的几何模型作为一个特征类,每个特征类有一个唯一的标识符。一个特征类表示一个实例的集合,对一个特征类的授权表示"何角色、以何种方式对何特征类进行操作"。角色对特定特征类的操作由角色的权限决定。为了提高授权管理的灵活性,在 Web 地图访问控制模型中,根据实际应用的安全需求把相似的操作放在同一个权限集合 P 中。P 实际上是由系统所支持的所有操作构成的集合中的部分操作形成的一个子集,这样"一个用户授予特权 P"实际上表示用户能够使用权限集合 P 中所有的操作。

Web 地图访问控制模型中的操作包括:Notify,Analysis,ViewGeometry 和 ViewAttribute。基本授权定义为三元组 $\langle r,f,p\rangle$,其中:$r\in R$,$f\in FC$,$p\in P$,R 是角色集,FC 是特征类集合,O 是操作集合,P 是定义在操作集合 O 上的一个集合。

在 Web 服务地图访问控制模型中,为了表示授权和地理空间之间的制约关系,引入了授权窗口(Authorization Window)的概念,用户只有在特定的地理空间中才有权执行授权的操作。在引入授权窗后,基本授权扩展为空间授权,它是一个四元组 $\langle r,fc,p,w\rangle$,其中:$r\in R$,$f\in FC$,$p\in P$,R 是角色集,FC 是特征类集合,O 是操作集合,P 是定义在操作集合 O 上的一个集合,$w\in Polygon$,$Polygon$ 是多边形几何体构成的集合,表示空间区域。

在 Web 服务地图访问控制模型中,定义了授权管理策略,利用其对权限进行管理。缺省情况下,由 Administrator(管理员)负责对授权规则的管理,管理员的权限包括:创建/删除用户、创建/删除角色、权限的授予/回收。而且,Web 服务地图访问控制模型允许管理员将部分权限委托给别的用户管理。因此,授权管理在 Web 地图访问控制模型中实际是分散式的。Web 服务地图访问控制模型采用的授权和权限回收机制就是关系数据库管理系统中经典的权限管理方法。

在 Web 服务地图访问控制模型中定义了带有 grant 选项的授权规则。设 R 是角色集,FC 是特征类的集合,P 是特权操作集合构成的集合,W 是多边形的集合。一个授权规则可以表示成一个元组:$\langle r,fc,p,w,gr,gr\_op\rangle$,其中:$r\in R$,$f\in FC$,$p\in P$,$w\in W$,$gr\in R$,$gr\_op\in\{\text{true},\text{false}\}$。布尔变量 gr_op 为 true 表示角色 r 可以将权限集合 p 再转授给其他角色;gr_op 为 false 则角色 r 不能够将权限集合 p 再转授给其他角色。属性 gr 表示由哪一个角色对角色 r 授予特权操作集 p。一个角色在一个授权空间中对一个空间特征类拥有权限,如果它被允许将此权限转授给其他用户,那么这些获得转授权权限的用户只有在此授权空间内,或此授权空间中的某一个部分才能够使用此权限。简而言之,就是授权的转授也受到授权空间的限制,不能够超出此空间范围。

创建了一个授权规则以后就要将其插入到授权规则集中,要注意的是必须保证插入新的授权规则后所形成的新的规则集是一致的,不出现冲突授权。

对于权限的回收操作,Web 服务地图访问控制模型规定只有权限的授予者才能够回收权限。为了维护授权规则集的一致性,对一个授权规则只有当所有依赖于它的授权规则都撤销以后才能够回收此权限。如果这条授权规则带 grant 选项,权限的回收操作直接并间接影响所有转授给其他角色的权限。可以分为递归删除和非递归删除两种方式。

Web 服务地图访问控制模型可以用来支持对 Web 上的

空间数据进行访问控制，但是 Web 地图访问控制模型所支持的空间数据模型相对而言比较简单，而且不支持空间数据的多粒度特性。该模型需要进一步研究解决的问题包括：如何利用此方法实现高效的空间访问控制？如何扩展该访问控制模型使其与当前正在不断推进的基于角色访问控制模型的标准化工作相一致？

在文献[6]中提出了一个类似的访问控制模型，它用来处理采用 XML 表示的空间数据的访问控制问题。

2.2.2 基于拓扑空间数据模型的访问控制模型

在对地理信息数据进行访问控制时，一种最朴素的思想就是由安全管理员根据需要定义专门的地理信息数据集合（也就是服务于不同各种目的的专用地图），把它们提供给具有不同信息需求和权限的用户使用。实际上在纸质地图制图领域这种方法已经应用了很多年了。但是这种方法对于基于 Web 的 GIS 系统而言是不合适的，主要是因为基于 Web 的 GIS 系统的用户群很大而且是动态变化的，很难做到事先预先生成适合不同用户所需的特定地图。而且这种方法很难实现细粒度的保护，同时也不能够及时反映访问控制策略的变化。因此，为了保证敏感地理数据信息的安全，在 GIS 系统中必须研究新型访问控制模型。

A. Belussi 等在 2004 年提出了另一个适用于保护 GIS 系统中地图数据的授权模型[7]。它基于拓扑空间数据模型，在这个空间访问控制模型中假设每一幅地图都是由若干个特征地物（feature）构成，而每一个特征地物以空间对象（spatial object）的形式出现在一幅或多幅地图中。这些空间对象可以借助不同的空间特性进行刻画。例如，借助几何特征可以确定空间对象的形状、位置和范围；而借助拓扑特性可以确定不同的空间对象之间的拓扑关系。基于面向对象的思想，在拓扑空间数据模型中提出了特征地物类型（feature type）的概念描述同型地物的共性，例如道路、湖泊、房屋等。而每一幅地图都包含了不同的特征地物类型的若干个实例：比如，若干条不同的道路和几个湖泊。每个特征地物在相关的地图中都至少有一个空间表示（或者是几何的，或者是拓扑的）。值得注意的是采用拓扑空间数据模型所带来的额外的一个好处是可以利用在拓扑空间数据模型上所定义的空间查询语言的强大的查询表达能力，这对于研究适用于地理数据的访问控制模型是十分有益的。

A. Belussi 等了提出的基于拓扑空间数据模型的访问控制模型与文献[8,9]中提出的模型相比，它的主要改进在于：(1)所支持的空间数据模型更复杂，对同一个空间对象同时支持几何表示和拓扑表示；(2)授权的传播机制更复杂，除了文献[8,9]中提出的与应用有关的权限层次相关的传播路径以外，授权的传播已经成为其所提出的访问控制模型的一个重要组成部分，可以沿着空间对象的层次和权限层次进行传播；(3)和文献[8,9]中的模型相比，新模型支持正授权和负授权，同时在权限传播的时候提供了定义例外情况的例子。

在拓扑空间数据模型 TSDM 中，空间数据库模式是由特征地物类型（a set of feature type）集合和地图类型集合（a set of map type）这两个集合构成。其中，每个地图类型是由若干种特征地物类型（feature type）构成的；而每种特征地物类型（feature type）都可以出现在不同的地图类型中。每个特征地物类型均有若干个描述性的属性和一个空间属性，其中空间属性在不同的地图中具有不同的维数。

在 A. Belussi 等人提出的基于拓扑空间数据模型的访问控制模型中，除了经典的访问控制模型中已有的主体（subject）、客体（object）、权限（privilege）等概念以外，还增加了授权符号（authorization sign）、授权类型（authorization type）、授权窗口等机制。其中，授权符号表示一个具体的授权是“正”授权还是“负”授权。“正授权”表示对一个给定的主体赋予对一个特定客体的某一特定权限，而“负授权”则明确表示特定主体不拥有对特定客体的某一特定权限。因此，在此模型中，一个主体对某个客体不具有某项权限有两种可能性：一种可能是因为主体没有获得授权，另一种可能是主体有“负授权”。在模型中，采用“负授权”优先原则，即主体如果同时对同一个客体在某个权限上有“正授权”和“负授权”，那么主体就不能够以此权限操作该客体。

授权类型把授权区分为强授权（weak authorization）和弱授权（strong authorization），它表示授权是否允许被覆盖（overridden），弱授权可以被强授权所覆盖。授权的强弱和授权的“正/负”机制结合起来可以用来表示授权中的特殊情况。在模型中，“强正”授权优先“弱负”授权，这样利用强/弱授权机制又可以灵活改变“正/负”授权的优先关系，从而使授权更灵活。

在 A. Belussi 等人提出的基于拓扑空间数据模型的访问控制模型中，为了进一步限制授权所作用的客体，把基于拓扑空间数据模型的查询也引入到访问控制模型中作为授权的一部分，从而提供了基于内容的访问控制（content-based access control）。利用查询可以把授权所涉及到的客体限于查询结果里面的那些客体。同时，在此访问控制模型中还有授权窗口的概念，原理是主体对特定客体的授权仅仅局限于特定的空间区域，它的最初设计目的是对将一个空间对象插入到地图中的操作进行限制。但是，实际上由于授权窗口仅仅对实际存在的客体才有作用，因此它的功能完全可以利用对特定地图的选择操作这样的查询来实现。为了方便起见，在此访问控制模型中同时提供了这两种机制，而且它们还可以组合起来，对被授权的客体做进一步的限制：即授权仅仅作用于查询结果中的一部分空间客体，它们的空间位置位于某一个授权窗口中。

和经典的访问控制模型一样，在 A. Belussi 等提出的基于拓扑空间数据模型的访问控制模型中，也有授权者（grantor）和授权选项（grant option）的概念。授权者可以把其所拥有的权限转授给系统中的其他主体，甚至可以通过授权选项的机制把授权者所拥有的权限的管理委托给其他的主体，就像经典的关系数据库管理系统中的授权机制那样。在此访问控制模型中，授权选项是一个布尔值，其为“真”时，被授权的主体可以对其他的主体进行转授权（grant），或者是将其转授出去的权限撤销掉（revoke），这也和经典的关系数据库管理系统一样。在此访问控制模型中，只允许对“正授权”进行授权代理，“负授权”不允许进行授权代理。在此访问控制模型中，授权规则构成的集合必须满足：最小性（minimality）和安全性（safety）两个性质。

在 A. Belussi 等人提出的访问控制模型中，由于授权通常涉及到授权窗口，而授权窗口是一个空间区域，因此可以将授权规则看作是拓扑空间数据模型 TSDM 中带有空间和非空间信息的一类特殊实体，并可以将其抽象为单独的特征型（feature type）。另外值得注意的是，由于授权窗口也可以用拓扑空间数据模型 TSDM 中的被授权地图表示，因此可以用一个统一的模型来表示应用数据和授权规则，并对其进行统一的索引，这是一个值得进一步研究的课题。

2.2.3 面向服务的地理空间数据基础设施中的访问控制模型

在许多重要领域，地理信息都已经成为决策支持的重要依据。众多政府机构、私人组织和商业机构提供各种各样的地理数据。由于各自的相对独立性和缺乏有效协调，这些来源不同的地理数据的格式往往存在很大差异。为了能够充分利用这些格式不同的数据，必须有一个能够对异质(heterogenous)和分布式的数据进行处理和共享的基础设施。显然，面向服务的地理信息基础设施必须能够对不同格式的地理数据进行有效的互操作。Geo Web Service 就是这种地理信息基础设施的一个具体实现。所谓 Geo Web 服务就是一种 Web Service 的规范，它所刻画的 Web Service 能够对地理数据进行表示、存储和处理。这些操作功能可以通过标准的 Web 服务接口获得。当需要使用不同格式的空间数据的时候，通过 Web Service 的调用，就能够利用其能力，将空间数据从原有的格式转换成别的可以互操作的数据格式。

在 Andreas Matheus 提出的面向服务的地理空间数据访问控制模型[10]中，采用面向对象的数据模型表示地理数据，因此该访问控制模型支持三类访问限制：基于类的访问限制；基于单个对象的访问限制；基于单个对象所处的空间区域的访问限制。

在面向服务的地理空间数据访问控制模型中，在实施访问控制时主要考虑了以下三个方面：

(1)应该对地理数据资源进行访问控制，而不是对服务进行访问控制。这是因为，一个 Web Service 的运作通常同时涉及到对同一个资源的多个权限状态不同操作，而不同的用户在调用同一个 Web Service 时，Web Service 显然应该根据用户的差异来确定该用户所能够获得的资源访问权限。例如，对天气预报这样的一个 Web Service 而言，它的日常运作就同时涉及到对共享的数据资源的创建(create)、删除(delete)、更新(update)和检索等权限不同的操作。

(2)基于类和对象的访问控制。基于类的访问控制作用于该类的所有实例，而基于对象的访问控制仅作用于某一个特殊的实例。在面向服务的地理空间数据访问控制模型中，地理数据采用面向对象模型表示。对这些数据的访问通过面向服务的基础设施来实现，服务的请求(request)和响应(response)也以面向对象数据模型表示。因此，在面向服务的地理空间数据访问控制模型中，根据简单特征地物规范(the simple feature specification)，利用 GML 语言对交换的地理数据进行编码。

(3)由于地理数据都来自某一个坐标系，因此在对地理数据进行访问控制的时候也需要从空间维度进行考虑。在面向服务的地理空间数据访问控制模型中，它的着眼点是客体所处的地理位置和某一个特定的空间授权区域之间的拓扑关系。例如 Within 和 Touch 这两种拓扑关系。其中，Within 关系限制主体只能够在特定的空间区域内对其中的客体进行操作。而 Touch 关系则限制了主体只能够对两个相邻接的空间区域内的客体进行操作。空间区域上的限制在模型中看作是基于类的访问控制的补充，它把主体对客体的访问权限作了进一步的限制：即在进行访问控制决策的时候还必须考虑主体和客体所处的空间位置。

Andreas Matheus 等人在文献[10]中提出的用于保护地理数据的面向服务的地理空间访问控制模型也是基于授权规则的。它同样支持“正授权”和“负授权”，授权规则表示为四元组：主体(subject)、操作(operation)、资源(resource)和条件(condition)，显然访问控制系统对用户访问请求的判定结果只可能是下面的两个选项之一：允许(permit)/禁止(deny)。为了描述和实现此访问控制模型，Andreas Matheus 等对 XACML 标准进行了扩充，引入了 GeoXACML，使其能够支持空间限制条件的声明和检查。

由于授权规则库中存在很多条规则，为了保证规则库中的规则都是不矛盾的，Andreas Matheus 等人在文献[10]中利用 GeoXACML 的丰富功能提出了检查规则是否存在冲突的方法。

Andreas Matheus 所提出的空间访问控制模型的特点在于采用 XML 处理异质数据，并且在 XACML 标准的基础上对其进行了空间扩展，使其能够表示和处理空间数据的访问控制问题。但是，它的应用是面向 Web Service 技术的，在其他空间数据应用架构中能否使用需要进一步的研讨。

2.2.4 其他访问控制模型

除了上面介绍的几个典型的空间访问控制模型以外，在相关研究文献中还提出了其他一些空间访问控制模型。限于篇幅，下面只简单介绍一下。

2000 年，Covington 等人提出了著名的 GRBAC 模型[11,12]。它引入了“环境角色”的概念，根据提出访问请求的角色所处环境条件来判定角色是否可以激活。环境条件包括时间、地点和其它一些与访问控制有关的背景信息。在文献[13,14]中提出一种访问控制模型，其中最重要的内容就是空间维的访问控制，它提出了“空间角色”的概念。当用户在一个给定的位置上时，系统就自动激活其扮演的一个特定角色。它的空间模型非常简单，主要用在无线网络中。它的空间模型由若干个相邻单元构成，用户的位置就是一个单元或者是几个单元。因此位置的空间粒度就是固定的，空间是严格结构化并且位置本身就仅仅是一个几何值而没有特殊的语义。

GEO-RBAC 模型[15,16]中的角色作用域，以及用户位置的概念与 GRBAC 模型中的背景变量概念比较接近。但是 GRBAC 模型的背景机制过于简单，不能充分表达空间信息的特征，例如多粒度的位置信息和不同的空间元素之间可能存在的空间上的相互关系。此外，GEO-RBAC 中采用了一个通用的空间数据模型用于提供一个统一的、标准的空间位置表示方法，其中不仅涉及角色，也包括被保护的客体。Chandran 和 Joshi 在 2005 年提出一种把空间和时间结合起来考虑[17]的访问控制模型，它借用了 GEO-RBAC 模型中的真实位置和逻辑位置的概念，同时也借用了 GTRBAC 模型中提出的时间背景的概念。但是这个模型不支持 GEO-RBAC 中诸如就绪角色的层次概念和责任分离约束等一些重要特性。

Joshi 等提出了 GTRBAC(Generalized TRBAC)模型[18]。它提出了一个语言用于定义角色上的多个时态约束，这些约束包括对就绪角色(role enabling)的约束、对激活角色(role activation)的约束、用户和角色之间指派关系的约束、权限和角色之间指派关系的约束等等。Bhatti 等把 XML 引入 GTRBAC 以支持在异构的分布式环境中实现访问控制策略[19]。该模型除了支持时态约束以外，也支持非时态的背景约束机制。但是，这个方法并没有把重点放在所定义的语言的描述能力上。

3 需要研究解决的问题

空间访问控制模型是所有基于移动用户位置的信息服务

(下转第 52 页)

and Tracking in an Ad-hoc Sensor Network // Proc. of the Fourth International Symp. on Information Processing in Sensor Networks. UCLA, Los Angeles, California, USA, 2005
[7] 邓自立. 自校正滤波理论及其应用——现代时间序列分析方法. 哈尔滨: 哈尔滨工业大学出版社, 2003
[8] Hu C W, Chen W, Chen Y Q, et al. Adaptive Kalman Filtering for Vehicle Navigation. Journal of Global Positioning Systems, 2003, 2(1): 42-47
[9] 耿延睿, 崔中兴, 张洪钺, 等. 衰减因子自适应滤波及在组合导航中的应用. 北京航空航天大学学报, 2004, 30(5): 434-437
[10] 周东华, 席裕庚, 张钟俊. 一种带多重次优渐消因子的扩展卡尔漫滤波器. 自动化学报, 1991, 17(6)
[11] Mehra R K. On the Identification of Variances and Adaptive Kalman Filtering. IEEE Transactions on Automatic Control, 1970, 15(2): 175-184
[12] Mehra R K. Approaches to Adaptive Filtering. IEEE Transactions on Automatic Control, 1972, 17: 693-698
[13] Sage A P, Husa G W. Adaptive Filtering with Unknown Prior Statistics // Joint Americal Control Conference. 1969: 769-774
[14] Mohamed A H, Schwarz K P. Adaptive Kalman Filtering for INS/GPS. Journal of Geodesy, 1999, 73: 193-293
[15] Chen G R, Chui C K. A Modified Adaptive Kalman Filter for Real-Time Applications. IEEE Transactions on Aerospace and Electronic System, 1991, 27(1): 149-154
[16] 刘冀春, 李明. 改进卡尔曼滤波器作动态谐波估计. 四川电力技术, 2005(1. 增刊): 29-32
[17] Dash P K, Liew A C, Ramakrishna G. Power-demand Forecasting Using a Neural Network with an Adaptive Learning Algorithm. IEEE Proc. -Gener. Transm. Distrib., 1995, 142(6): 506-568
[18] 刘广军, 吴晓平, 郭晶. 一种次优并行 Sage 自适应滤波器. 测绘学院学报, 2002, 19(1): 8-10
[19] 郭晶, 吴晓平, 刘广军. 一种数值稳定的次优并行 Sage 自适应滤波器. 测绘学报, 2002, 31(4): 283-288
[20] 吕伟, 王艳东. Sage-Husa 自适应卡尔曼滤波算法在 SINS 初始对准中的应用研究. 战术导弹控制技术, 2005(3): 52-55
[21] 颜东. 导航、制导系统状态估计方法及容错理论研究. 北京: 北京航空航天大学, 1995

(上接第 24 页)

中都必须考虑的核心问题。一个真正的能够在基于移动用户位置的信息服务中应用的访问控制模型必须同时考虑受保护的数据对象本身所具有的空间特性, 以及提出数据访问请求的主体在提出访问请求时所处的空间位置信息。这里涉及到几个关键问题: (1)如何将基于角色访问控制的思想应用到空间数据的保护? 在不同的空间数据应用架构中是否需要采用不同的空间访问控制模型? 如何推进空间访问控制模型标准化? (2)如何构造授权基? 如何维护授权规则集, 使其不出现冲突? 如何验证授权规则集中不存在冲突? 授权规则的高效检索算法? (3)如何将授权规则和数据对象进行统一检索以提高访问控制决策的效率? 如何组织和存储授权规则集与空间数据对象? (4)如何将时间维信息加入到空间访问控制模型中?

结束语 目前, 对空间数据的访问控制模型研究还处在起步阶段, 虽然已经有了一些研究成果, 但是还有许多问题尚待进一步研究。随着基于移动用户位置的信息服务种类的不断丰富, 适用于空间数据的访问控制模型必将会得到日益广泛的应用。

参 考 文 献

[1] Küpper A. Location-based services: Fundamentals and Operations. John Wiley & Sons, Ltd., 2005
[2] earth. google. com
[3] Barlow K. Google Earth prompts security fears. http://www.abc.net.au/news/indepth/featureitems/s1432602.htm
[4] Chun S, Atluri V. Protecting Privacy from Continuous High-resolution Satellite Surveillance. Technical report. CIMIC, Rutgers University, 1999
[5] Elisa B, Luisa D M, Davide M. An Access Control System for a Web Map Management Service // Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04). IEEE Computer Society, 2004
[6] Purevjii B, et al. An access control model for geographic data in an XML-based framework // Proceedings of the 2nd International Workshop on Security In Information Systems (WOSIS'04). INSTICC Press, Porto, Portugal, 2004
[7] Belussi A, et al. An authorization model for geographical maps // Proceedings of the 12th annual ACM international workshop on geographic information systems. ACM: Washington DC, USA, 2004
[8] Atluri V, Chun S A. An authorization model for geospatial data. IEEE Transactions on Dependable and Secure Computing, 2004, 1(4): 238-254
[9] Belussi A, Catania B, Bertino E. A reference framework for integrating multiple representations of geographical maps // Proceedings of the 11th ACM international symposium on Advances in geographic information systems. ACM: New Orleans, Louisiana, USA, 2003
[10] Andreas M. Declaration and enforcement of fine-grained access restrictions for a service-based geospatial data infrastructure // Proceedings of the tenth ACM symposium on Access control models and technologies. ACM: Stockholm, Sweden, 2005
[11] Michael J C, Moyer M J, Ahamad M. Generalized Role-Based Access Control for Securing Future Applications // Proceedings of the 23rd National Informational Systems Security Conference. 2000
[12] Michael J C, et al. Securing context-aware applications using environment roles // Proceedings of the sixth ACM symposium on Access control models and technologies. ACM: Chantilly, Virginia, United States, 2001
[13] Hansen F, Oleshchuk V. Spatial role-based access control model for wireless networks // IEEE 58th Vehicular Technology Conference, 2003. VTC 2003-Fall., 2003
[14] Hansen F, Oleshchuk V. SRBAC: a spatial role-based access-control model for mobile systems // Proceedings of the 7th Nordic Workshop on Secure IT Systems (NORDSEC'03). Gjøvik, Norway, 2003
[15] Elisa B, et al. GEO-RBAC: a spatially aware RBAC // Proceedings of the tenth ACM symposium on Access control models and technologies. ACM: Stockholm, Sweden, 2005
[16] Maria Luisa D, et al. GEO-RBAC: A spatially aware RBAC. ACM Transactions on Information and System Security, 2007, 10(1): 2
[17] Chandran S, Joshi J B D. LoT-RBAC: A Location and Time-Based RBAC Model // Web Information Systems Engineering-WISE 2005. 2005: 361-375
[18] Joshi J B D, et al. A generalized temporal role-based access control model. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(1): 4-23
[19] Rafae B, et al. X-GTRBAC: an XML-based policy specification framework and architecture for enterprise-wide access control. ACM Transactions on Information and System Security, 2005, 8(2): 187-227