

基于要素约束的空间隐私保护的实施

张爱娟¹, 高井祥²

(1 中国矿业大学 计算机学院, 江苏 徐州 221116; 2 中国矿业大学 环境测绘学院, 江苏 徐州 221116)

摘 要: 目前, 在不同的应用领域地理数据已经成为进行决策的重要信息基础. 为了在满足公众对地理数据的共享需求的同时实现对地理数据访问的隐私保护, 已经出现了多个空间访问控制模型, 但大部分模型没有实现针对地理要素对象的细粒度空间对象访问控制, 通过为主体引入位置属性, 在授权过程中引入语义属性约束和拓扑关系约束实现了基于地物属性的空间访问控制机制. 然后提出了语义属性约束和拓扑关系约束的规则描述方法, 并重点分析了复合拓扑关系约束可以出现的约束组合最后, 开发了原型系统对该模型进行了验证, 说明上述地物对象级的访问控制是可以在有限规则范围内实施的.

关键词: 空间; 隐私保护; 拓扑关系; 语义属性

中图分类号: TN402

文献标识码: A

文章编号: 1000—7180(2013)12—0167—06

Spatial Privacy-Preserving Enforcement Based on the Feature Constraints

ZHANG Ai-juan¹, GAO Jing-xiang²

(1 School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China;

2 School of Environment Science and Spatial Informatics, China University of Mining and Technology, Xuzhou 221116, China)

Abstract: At present, geographic data has become an important information base for decision-making in different application areas. In order to meet the public demand for geographic data sharing as well as achieve privacy protection during data access, there have been multiple spatial access control models, but most of them can not achieve fine-grained access control to geographic feature objects, therefore, a spatial access control model based on attribute constraints is proposed, in which, location attributes are added to users, and attribute constraints (semantic attributes and geometry attributes) are introduced during the authorization. Then, the method is proposed to enforce semantic attribute constraints and topological relation constraints, and it is focused on analyzing the complex topological constraint combinations. Finally, a prototype system is developed to verify the feasibility of the model within limited rules.

Key words: spatial; privacy-preserving; topological relation; semantic attribute

1 引言

面向服务的 GIS 框架得到迅速发展, 但是, 地理数据因为与国家安全或商业利益息息相关, 所以需要用户的访问请求进行控制, 通用 IT 访问控制机制不能满足空间应用领域对空间数据的访问控

制需求, 空间访问控制有如下需求^[1]:

(1) 不仅要限制访问的整个服务, 还要限制服务所提供的数据.

(2) 上下文相关的访问约束.

(3) 访问可以约束到某个特定的类上, 这种需求是指对地图的访问可限制到单个或一组图层.

收稿日期: 2013—01—27; 修回日期: 2013—03—29

基金项目: 国家自然科学基金(41074010, 41171343); 江苏省研究生创新计划资金(CX09B_116Z, CX10B_156Z); 高校基础科研资助专项基金(2010QNB21)

(4)访问可以约束到某个类的单个对象(或者一部分对象)上。

(5)可以根据资源对象的几何属性与一个给定的几何之间存在的空间关系进行访问约束。

通用的 IT 访问控制模型无法实现上述多粒度及基于时空约束的访问需求,空间数据有其自身的特点,如果沿用通用的 IT 访问控制模型,其访问控制的粒度至多到图层级,但要实现细化到地物级且具有属性约束空间访问控制,目前缺乏现成的访问控制机制来满足要求,所以空间访问控制已成为空间信息安全的热点研究问题。

矢量数据访问控制模型的研究大多都是在粗粒度控制空间数据的基础上,增加主体、授权的上下文环境作为授权依据,进行动态授权。如, Yu 提出了增加了时间约束的 LTAM 模型^[2],这是一种 DAC 访问控制模型,其模型用于控制在不同区域中对服务的访问。后续很多模型考虑到授权管理问题,在 RBAC 模型的基础上,增加空间属性约束。这方面比较完善的模型是 Bertino 的 GEO-RBAC^[3], GEO-RBAC 在用户、角色激活方面都引入了空间位置的概念,且实现了对角色的空间继承和带约束的 RBAC 的空间扩展。张宏等提出了 SC-RBAC 空间访问能控制模型^[4],该模型给出了空间角色的概念,为角色赋予逻辑位置域,作为其可以激活的上下文环境,并通过层次化的空间角色实施多级安全策略。邹志文、鞠时光等^[5-7]在 VISTA 系统的基础上研究了带有空间特性的角色访问控制模型(Spatial Role-Based Access Control),此模型利用空间主体的责任分离约束和空间角色的基数约束及继承关系实现基于上下文和分层的授权。张洪军提出了基于 UCON 的空间访问控制模型^[8],通过在空间角色中增加可变的空間位置属性,作为进行动态授权的依据。在考虑主体位置的基础上,又出现了一些增加时间属性的模型,如 Ray I 提出的 Spatio-temporal RBAC^[9]模型;Chandran 等人提出的 LoT-RBAC 模型^[10],此模型中角色需要在特定区域中才可以被激活且在角色的整个生命周期中都会受到时间约束。而针对空间客体不同粒度的访问控制模型有如下研究:朱霞等提出了基于角色的图元授权粒度控制^[11],该模型中,利用图元标识码表示地物进行授权。於光灿提出了基于特征的空间数据访问控制模型^[12],该模型的授权约束将授权限制在特定的地理区域或空间对象集合内,以控制权限的行使范围。张颖君提出了基于尺度的时空 RBAC 模型^[13],该模型

在 RBAC 模型的基础上增加了尺度属性用以控制图层级空间数据,而在角色上增加了位置和时间属性作为角色激活的上下文环境。张妍提出了空间矢量数据细粒度强制查询访问控制模型 SV_MAC (spatial vector data mandatory access control model)^[14],此模型在强制访问控制模型的基础上进行空间扩展。通过为客体对象增加密级,为主体增加空间区域和密级属性,实现空间矢量数据强制查询访问控制。

上述空间访问控制模型可以满足访问控制的下列需求:可以利用上下文(用户位置、访问时间)相关的访问约束,限制对服务的访问;访问可以约束到某个特定的类。但在对某个类的单个对象(或者一部分对象)的控制只能满足数据量很小的空间数据,而且对利用拓扑关系约束进行访问涉及的很少,所以,本文要解决的问题是如何利用语义属性约束和拓扑关系约束对细粒度的地物对象进行控制。

2 基于空间属性约束的访问控制模型

空间访问控制通过主体(用户和角色)、操作、空间数据、属性表达式约束进行授权。空间数据是已有数据,其约束属性来源于空间数据的特定属性,通过分析空间访问控制需求,在面向对象的基础上,将空间数据的粒度划分为由粗到细的地图、图层、空间要素对象。同时,模型需要空间位置相关,所以进入系统的主体需要空间属性,而对于受控的空间要素对象,可以通过地物类的属性表达式来确定,上述目标模型中主体及空间客体的属性描述如下所示。

2.1 用户属性

用户属性除了有确定身份唯一性的标识和继承自 RBAC 的角色属性外,还需要有确定自己所属物理区域的物理区域(位置)属性,因为在要素对象粒度上,拓扑关系约束需要有一个用于确定空间关系的授权几何,这个授权几何源自主体的属性,本文将这个属性放在用户级的主体上,用 location 表示,目前基于位置的空间访问控制模型中主体位置的获取无一例外的都是通过 GPS 或者传感器网络获得物理位置,但在分布式 GIS 系统中大多数的用户,还需要在不具备定位设备的前提下描述位置。在不同领域中提出的各种位置模型分为两类:

语义位置(区域)^[15]:语义层次式的具有良好的用户可读性和自描述的位置表示特性,比如“北京”。它是描述性的或符号化的。

笛卡尔式位置(区域)^[16]:坐标的、几何的,比如

GPS 位置.

在模型中,这两种位置将用两类属性表示:实际位置(real location; Rloc)和逻辑位置(logical location; Lloc). 模型中对两种位置属性描述如下所示:

(1) Rloc

Rloc 可以表示一个物理点或者区域,如果是后者,区域将用闭合边上的点(phyP)表示,而且要注意所使用的坐标系 SRS,其中 $\text{phyP} \in (\text{Long} \times \text{Long} \times \text{Hig})$, $\text{Long} \in (-180, 180]$ 是经度的集合, $\text{Lat} \in [-90, 90]$ 是纬度值的集合 Hg 是高度值. 所以 $\text{Rloc} = (\text{SRS}, \text{phyPs})$.

(2) Lloc

逻辑位置指对一个或多个物理位置的抽象概念,也可以称为语义位置.

(3) 位置映射函数

$\text{logTorealMap: logTorealMap}(\text{Lloc}, s) \rightarrow \text{Rloc}$. 该函数是将 Lloc 映射到特定尺度 s 下的 Rloc.

一个物理位置可能包含在一个逻辑位置中,反之也成立. 所以当判断两个位置之间的拓扑关系时,可利用映射函数将逻辑位置转变成物理位置再作比较.

2.2 要素对象属性

要素对象的约束属性很多,可以分为语义属性和非空间属性,他们来源于元空间数据. 空间访问控制要求模型是空间相关的,因此,对象的空间属性与用户的授权几何间的拓扑关系会成为授权的一种约束,而语义属性是空间数据库中对地物对象的描述,选择何种属性作为约束量,由系统的安全需求分析决定.

2.3 要素对象粒度的访问控制模型

由上述分析可知,要素对象粒度的访问控制模型如图 1 所示.

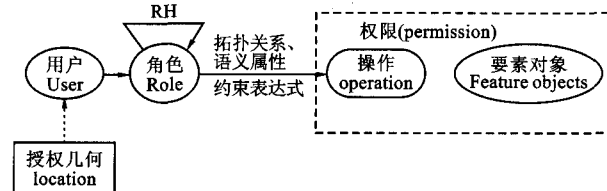


图 1 要素对象级访问控制模型

(1) $\text{User} = (\text{Identifier}, \text{Location}, \text{Roles})$; Identifier 属性用于确认用户身份,如,用户名及密码、生物特征、智能卡、IP、数字证书等. Location 属性表示主体所属区域,role 属性标示用户权限集.

(2) $\text{Role} = (\text{Name}, \text{PPS: policy permission set})$:连接用户与权限分配的中间者,当用户的角色

被激活,具有 PPS 表示的权限.

(3) Operations:空间类型的操作方法.

$\text{Feature objects} = (\text{FeatureClass}, [\text{semantic Constraint} \mid \text{spatialConstraints} *])$:是要素对象级的数据粒度,FeatureClass 表示对象所属的类型,semanticConstraints 表示语义属性约束表达式,spatialConstraints 表示拓扑关系约束表达式.

3 要素对象粒度资源控制

要素对象粒度是指控制粒度细化到空间对象集. 下面基于面向对象数据模型定义上述控制粒度的访问规则,访问控制规则被表示成五元组,主体(角色),操作,资源,条件,最后的授权结果是 Permit 或 Deny. 所以,访问控制规则可以表示成如下所示.

$\text{Rule} = \{S_R, O, TM, C\} \rightarrow \{\text{Deny}, \text{Permit}\}$

(1) S_R :表示被授予权限的主体.

(2) O :表示服务中操作.

(3) TM :目标资源类,为了表现资源类型之间的层次关系本文用 XPath 表示.

(4) C :一个表示属性约束的条件表达式.

Re 是来自客户端的请求,访问控制实施模块根据客户端请求,查询是否有访问控制规则允许请求通过.

3.1 语义属性约束表达

attrExpress 是语义属性约束表达式,attrExpress 表达式包含的运算符有: $>$, $<$, $=$, $\neq$, $\leq$, $\geq$, $\in$, $\notin$.

$$C = (\bigwedge_{i=1}^n \bigvee) \{ \text{attrExpress}[i] \}$$

$$C =$$

$$\begin{cases} 1, (\bigvee_{i=1}^n \bigwedge) TM. \text{attr}[i] \subset \{x \mid x \in \text{attrExpress}[i]\} \rightarrow \text{True} \\ 2, (\bigwedge_{i=1}^n \bigvee) TM. \text{attr}[i] \cap \{x \mid x \in \text{attrExpress}[i]\} \neq \emptyset \rightarrow \text{True} \\ 3, \emptyset \rightarrow \text{True}; \\ 4, \text{else} \rightarrow \text{False} \end{cases}$$

例如,admin 对图层 City,能 getInfo 其面积小于 50 万的要素对象.

$\text{Rule1} = \langle \text{admin}, \text{getInfo}, \{ /cInfo: \text{ChinaInfo-Model/gml: FeatureMember/cInfo: City; area} < 50 \} \rangle \rightarrow \text{permit}$

3.2 空间属性约束表达

$C = \text{spatial Rel}(\text{Geo}_R, \text{Geo}_P)$

$$C = \begin{cases} 1, \text{spatial Rel}(\text{Geo}_P, \text{Geo}_R) \rightarrow \text{True} \\ 2, \varphi \rightarrow \text{True} \\ 3, \text{else} \rightarrow \text{false} \end{cases}$$

$\text{Geo}_P =$

$\text{S}_R, \text{location}, \sqsubset \text{lloc? logTorealMap}(\text{Lloc}, s):$

Rloc

$\text{Geo}_R = \text{Query}(\text{TM}_F)$

Geo_P 表示授权几何, 来自访问主体的空间属性, Geo_R 表示请求客体的几何属性. spatialRel 表示两个空间几何之间的拓扑关系函数和度量关系函数.

$\text{Spatial Rel} \in \{\text{Equals}, \text{Disjoints}, \text{Touches}, \text{Crosses}, \text{Within}, \text{Overlaps}, \text{Intersects}, \text{IsWithinDistance}, \neg \text{Equals}, \neg \text{Disjoints}, \neg \text{Touches}, \neg \text{Crosses}, \neg \text{Within}, \neg \text{Overlaps}, \neg \text{Intersects}\}$

因为要素对象级的授权只能进行肯定授权, 所以为了能够实现类似否定授权的效果, 需要对空间拓扑关系描述进行否定扩展, 描述与授权几何不满足某种空间关系的拓扑, 所以有了 $\neg \text{Equals}, \neg \text{Disjoints}, \neg \text{Touches}, \neg \text{Crosses}, \neg \text{Within}, \neg \text{Overlaps}$, 和 $\neg \text{Intersects}$ 关系. 例如:

规则: 角色 admin 访问 Building 图层的 getInfo 操作时, 对象被限制在坐标系为 srs1 物理区域为 $\{0, 10, 0, 10, 10, 0, 0\}$ 内.

$\text{Rule1} = \{\text{admin}, \text{getInfo}, \{/\text{cInfo: ChinaInfo-Model/gml: FeatureMember/cInfo: City}\}; \text{Within}(\text{shape}, (\text{srs1}, 0, 0, 10, 0, 10, 10, 0, 0))\} \rightarrow \text{Permit}..$

3.3 复合拓扑约束表达

当需要对空间关系进行进一步的精确约束是, 需要用复合的空间约束限制空间对象, 空间约束之间可用 AND、OR 运行表达, 表示为 $\wedge$ 、 $\vee$ 联合. 许可几何和请求几何的维度不同, 他们能实施的空间关系也不尽相同, 假设许可几何是 2D 的, 我们将分析当请求几何为 0D、1D 和 2D 时, 根据两个几何之间可能存在的拓扑, 应该选用哪些关系来对具有复杂的空间拓扑关系的几何进行授权. 为了简化描述, 用向量 $[\text{Equals}, \text{Disjoints}, \text{Intersects}, \text{Touches}, \text{Crosses}, \text{Within}, \text{Overlaps}]$ 表示所使用的函数, 每个项可用的函数用 1|0 表示, 不可用的函数直接用空表示.

(1) 请求几何为 0D

当请求几何为 0D 时, Equals, Crosses, Over-

laps 函数不能使用, 许可几何为多边形 (也包括有洞的多边形), 所有可能的拓扑类型及用到的空间关系组如图 2 所示.

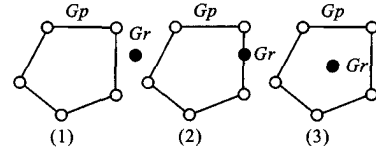


图2 请求几何与许可多边形的关系状态

①使用的空间关系向量为 $['', 1, 0, 0, '', 0, '']$

②使用的空间关系向量为 $['', 0, 1, 1, '', 0, '']$

③使用的空间关系向量为 $['', 0, 1, 0, '', 1, '']$

(2) 请求几何为 1D

当请求几何为 1D 时, Equals, Overlaps 函数不能使用, 许可几何为多边形 (也包括有洞的多边形), 所有可能的拓扑类型及用到的空间关系组如图 3 所示.

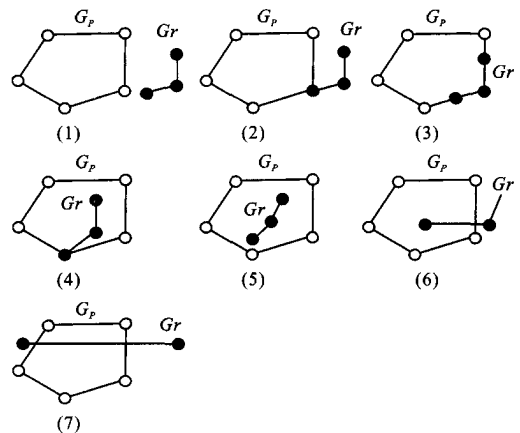


图3 1D 请求几何与许可多边形的关系状态

①使用的空间关系向量为 $['', 1, 0, 0, 0, 0, '']$

②使用的空间关系向量为 $['', 0, 1, 1, 0, 0, '']$

③使用的空间关系向量为 $['', 0, 1, 1, 0, 0, '']$

④使用的空间关系向量为 $['', 0, 1, 0, 0, 1, '']$

⑤使用的空间关系向量为 $['', 0, 0, 0, 0, 1, '']$

⑥使用的空间关系向量为 $['', 0, 1, 0, 1, 0, '']$

⑦使用的空间关系向量为 $['', 0, 1, 0, 1, 0, '']$

(3) 请求几何为 2D

当请求几何为 2D 时, Crosses 函数不能使用, 许可几何为多边形 (这时有洞和无洞的多边形与许可几何之间的关系, 某些情况下有区别), 下面利用有一个洞的情况, 列出所有可能的拓扑类型及用到的空间关系组, 结果如图 4 所示.

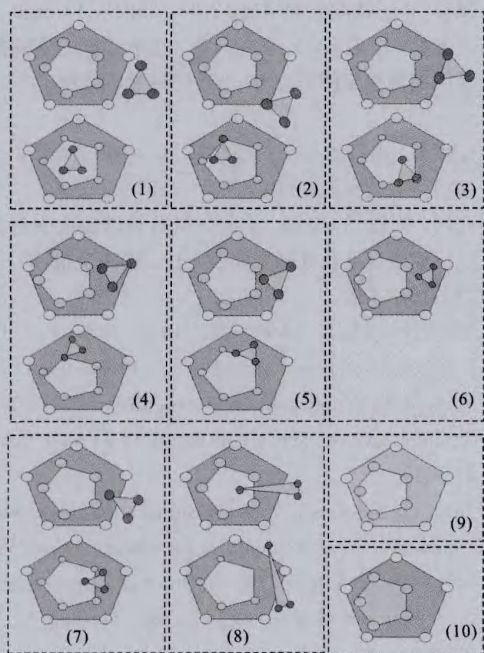


图4 2D请求几何与许多多边形的关系状态

- (1) 使用的空间关系向量为 $[0, 1, 0, 0, ", 0, 0]$
- (2) 使用的空间关系向量为 $[0, 0, 1, 1, ", 0, 0]$
- (3) 使用的空间关系向量为 $[0, 0, 1, 1, ", 0, 0]$
- (4) 使用的空间关系向量为 $[0, 0, 1, 0, ", 1, 0]$
- (5) 使用的空间关系向量为 $[0, 0, 1, 0, ", 1, 0]$
- (6) 使用的空间关系向量为 $[0, 0, 1, 0, ", 1, 0]$
- (7) 使用的空间关系向量为 $[0, 0, 1, 0, ", 0, 1]$
- (8) 使用的空间关系向量为 $[0, 0, 1, 0, ", 1, 0]$
- (9) 使用的空间关系向量为 $[1, 0, 1, 0, ", 1, 0]$
- (10) 使用的空间关系向量为 $[0, 0, 1, 0, ", 0, 0]$

复合规则的表达式举例,例如:admin 用户可以读取省区域 GP1 和 Gp2 范围内的城市。

Policy1 = { *, *, /*, or, Rule1, Rule2 }

Rule1 = { admin, read {, /cInfo: ChinaInfoModel/gml: FeatureMember/cInfo: City; within(shape, Gp1) } } → permit

Rule2 = { admin, read {, /cInfo: ChinaInfoModel/gml: FeatureMember/cInfo: City; null; within(shape, Gp2) } } → permit

4 系统实现

为了验证上述模型,在实验中利用 1:100 万中国地图库验证上述模型的控制效果,在 Arcgis 平台上开发的 Webgis 系统运行效果图如下所示。

(1) 语义约束

测试用例:地图显示两个图层:省界图层和城市

图层。其中省界图层中的对象只显示面积属性 area 小于 50 万的省份信息,而大于 50 万的为隐藏对象,未被授权显示,且不能进行操作。控制效果如图 5 所示。



图5 面积属性约束运行界面

(2) 拓扑关系约束

测试用例:地图显示三个图层有地区界线图层、公路图层、省区域图层,空间约束只能拥有河北省范围内的地图操作权限。河北省范围以外的区域无法访问。图 6 是添加约束的运行对比效果图。



图6 空间约束运行效果图

5 结束语

基于地理要素约束的空间访问控制模型可以解决地物要素级的访问控制需求,能够实现基于语义属性约束的控制需求和基于空间拓扑关系的控制需求,且在定义空间拓扑关系表达式时,对三种维度的目标对象可以实施的空间约束关系进行了详细的分析,为检验空间关系定义的合理性提供了依据。另外,文中没有解决的问题是当请求的对象跨越了授权几何时需要对象进行打断处理,如果对这些对象进行了修改操作,回写数据时应该如何处理,这部分将在后续工作中进行研究。

参考文献:

- [1] Herrmann J. Interoperable access control for geo web services in disaster management [C]// 2th Proceedins of the sium on Geo-information for Disaster Management. Goa, India: IEEE, 2006.
- [2] Yu Hai, Lim Ee-peng. LTAM: a location-temporal authorization model[J]. Secure Data Management[J].

- Lecture Notes in Computer Science, 2004 (3178): 172-186.
- [3] Bertino E, Catania B, Daminai M L. GEO-RBAC: a spatially aware RBAC [J]. ACM Trans on Information and System Security, 2007, 20 (10):1-42.
- [4] 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:E 辑:信息科学, 2007, 37(2):254-271.
- [5] 鞠时光, 陈伟鹤, 顾怡. 带有空间特性角色约束[J]. 计算机辅助设计与图形学学报, 2008, 20 (10): 1374-1382.
- [6] 邹志文, 鞠时光, 陈昌乾. 带空间特性角色访问控制模型的冲突会话[J]. 计算机应用研究, 2009, 26 (10):3903-3905.
- [7] 邹志文, 陈昌乾, 鞠时光. 带空间特性的角色访问控制研究[J]. 计算机科学, 2010, 37(1): 189-196.
- [8] 张洪军. 基于 UCON 的空间访问控制模型的研究与应用[D]. 镇江:江苏大学, 2010.
- [9] Ray I, Toahehoodie M. A spatio-temporal role-based access control model [C]// LNCS 4602. Berlin: Springer, 2007: 211-226.
- [10] Chandran S M, Joshi J B D. LoT-RBAC: A location and time-based RBAC model[C]// Web Information Systems Engineering-WISE 2005. Berlin: Springer, 2005: 361-375.
- [11] 朱霞, 孙振冰. GIS 中基于角色的图元授权粒度控制研究 [J]. 武汉大学学报, 2004, 29(2): 157-160.
- [12] 於光灿, 李瑞轩, 卢正鼎, 等. 基于特征的空间数据访问控制模型研究[J]. 计算机科学, 2008, 35(10): 122-125.
- [13] 张颖君, 冯登国. 基于尺度的时空 RBAC 模型[J]. 计算机研究与发展, 2010, 47(7):1252-1260.
- [14] 张妍, 陈驰, 冯登国. 空间矢量数据细粒度强制查询访问控制模型及其高效实现 [J]. 软件学报, 2011, 22 (8):1872-1883.
- [15] Hulsebosch R J, Salden A H, Bargh MS, et al. Context-sensitive access control[C]// Proceedings of the 10th ACM Symposium on Access Control Models and Technologies. New York: ACM Press, 2005: 111-119.
- [16] Jiang C, Steenkiste P. A hybrid location model with a computable location identifier for ubiquitous computing [C]// Proceedings of the 4th International Conference on Ubiquitous Computing. London: Springer-Verlag, 2002:246-263.

作者简介:

张爱娟 女, (1979—), 博士生. 研究方向为信息安全, 分布式 GIS.

高井祥 男, (1960—), 博士生导师. 研究方向为大地测量, 矿山 GIS.