基于空间特性的访问控制模型①

郭 磊, 刘用麟

(武夷学院 数学与计算机系, 武夷山 354300)

摘 要: 针对传统 RBAC 模型中无法有效对移动用户进行授权的缺陷, 提出了一个支持空间与时间维度的访问控制模型——SDT-RABC, 定义了在空间环境下的激活空间区域约束、激活空间角色基数约束和空间职责分离约束, 给传统的基于角色的访问控制模型增加了空间安全描述能力.最终建立了一个通用性较好, 描述性较强的访问控制模型.

关键词: 信息安全; 基于角色的访问控制; 空间数据; 空间约束; 访问控制策略; 空间数据库

Access Control Model Based on Spatial Specialty

GUO Lei, LIU Yong-Lin

(Department of Mathematics and Computer Science, Wuyi University, Wuyishan 354300, China)

Abstract: Targeting on the ineffectiveness of authorizing mobile clients in the access control system, SDT_RABC--an access control model, which based on supporting space and time dimension was provided. It defined the constraint of the activation area in the spatial environment, spatial cardinality constraint of role activation and separation of duties spatial constraint, a generalized and well-represented control mode was finally set up which enhanced the capacity of spatial safety description to the traditional role-based access control model.

Key words: information security; role-based access control; spatial data; spatial constraints; access control strategy; spatial database

1 引言

随着现代通信技术的日新月异, 尤其是第三代移动通信技术、GIS 技术等的广泛应用, 人们可以在任何地方通过互联网连接许多免费的空间数据库, 获得国家任何区域的详细的位置信息, 甚至能够监控个人的活动, 查看国家重点保护地区的信息等, 给国家安全和个人隐私带来了严重威胁, 而传统的访问控制方法并不能直接应用于空间数据库的保护, 因此, 本文提出了一个带有空间特性的访问控制模型, 该模型对 RBAC 模型进行扩展, 针对基于地理位置的数据信息的空间特性, 定义了含有空间特性的约束机制, 并通过该机制对用户角色分配, 角色授权等进行控制.

基于角色的访问控制(role based access control, RBAC)是一种经典的访问控制模型, 它通过给用户分配和取消角色来完成对用户的权限管理, 实现了用户与访问权限的逻辑分离, 提高了安全管理的效率. 后来, RBAC 被扩展以支持各种约束, 如支持上下文感知的约束[1,2], 时间约束[3]等. 但由于空间数据的复杂性及空间操作的特殊性, 传统的访问控制模型, 如访问控制列表、基于角色的访问控制模型等都不能有效解决其安全性问题, 因此, 近年来, 国内外的研究人员也提出了众多的空间数据访问控制模型.

美国 Rugters 大学的 Chen 和 Atluri 在 1999 年最早提出了地理空间授权模型 GSAM[4], 它被用于对地理数据进行访问控制, 它主要对卫星拍摄的地面照片进行保护, 但该模型在实施时仅考虑了被保护的数据本身所具有的空间特性. Elisa Bertino 等人[5]提出了一个对 WEB 上得空间数据进行访问的模型 GEO-RBAC 模

① 基金项目:福建省科技重点项目(2011Y0049);福建省教育厅支助项目(JA11265);武夷学院科技项目(XQ0932)
收稿时间:2012-05-10;收到修改稿时间:2012-06-12

型, 对 RBAC 模型进行扩展, 用于处理基于地理位置的数据信息的访问控制, 用户角色的激活取决于用户所在地理位置. 同时, 为了使模型更具有灵活性与重用性, GEO-RBAC 模型中引入了角色模式的概念, 该模型同时考虑了被保护的数据对象和访问请求者提出访问请求时的空间位置信息, 但对角色的空间约束规则并没有进行充分的研究. A.Belussi 等提出了另一个适用于保护 GIS 系统中地图数据的授权模型[6], 它基于拓扑空间数据模型, 使所支持的空间数据模型更复杂, 授权传播的机制也更复杂.

本文对原有的 RBAC 模型进行改进, 主要研究基于移动用户的信息服务系统对访问控制模型的特殊需求, 提出一种含空间数据特性的角色访问控制模型(Spatial Data and Time Role-base Access Control, SDT-RBAC), 定义带有空间特性的约束机制, 使系统通过这些新定义的约束机制实现控制角色状态、用户-角色映射、角色授权和角色激活等.

2 SDT-RBAC模型定义

由于不同角色在同一空间位置权限不同, 而同一角色在不同空间位置权限也不同, 在 SDT-RBAC 模型中引入空间对象、空间位置等元素, 具体模型元素如下:

定义 1. SDT-RBAC 模型

模型主要由 6 个实体集组成, 分别为 User(U), Role(R), Objects(OB), Permission(P), Session(S) 和 Local(IP). User 表示用户集合, Role 表示角色集合, Objects 表示访问客体集合, Permission 表示权限集合, Session 表示会话集合, Local 表示空间位置集合, 表示空间对象所处位置的集合, LOC={IPi｜i∈N}, IP 代表空间中的一个地址, 为一个四维向量 IPi= {ai,bi,ci,di}.

UA⊆(U×LOC×R)c 表示用户 U 在空间位置 LOC 被分配角色 R, 且满足约束规则 c.

PA⊆(P×LOC×R)c 表示角色 R 在空间位置 LOC 被授权权限 P, 且满足约束规程 c.

S=<U, R, UA, PA, C, TIME, OP, Task>表示用户的一次回话操作, 其中 U, R, UA, PA, TIME 分别表示用户、角色、用户-角色指派、角色-权限映射关系的集合和会话发起时间; C 表示该会话必须满足的约束规则; Task 为会话需完成的一系列操作; op⊆P×OB=Tryrequest(r,ob,p,loc),表示角色在空间位置 LOC 上请求对客体 ob 的访问权限 p;操作状态集为 OP={Auth, Permint, Deny, Suspend, Recover, Revoke, Appoint / un Appoint ,Acticate/unActicate,Return_object, Return_Accessing, SessionRoles, EffectiveSessionRoles, Return_Request, countr}

• Auth(r,ob,p,loc)/unAuth(r,ob,p,loc): 对角色空间位置 loc 上的权限授予/回收, 角色、权限与位置存在多对多的联系, 即角色可同时获得一个位置的多个权限, 也可同时获得不同在位置的权限.

• Permit(r,ob,p,loc)/deny(r,ob,p,loc): 表示角色 r 在空间位置 loc 有效/无效.

• Suspend(r,ob,p,loc): 权限挂起, 即将角色 r 在 loc 上对客体 ob 的访问权限设为无效.

• Recover(r,ob,p,loc):权限恢复, 即恢复角色 r 在 loc 上对客体 ob 的访问权限的有效性.

• Revoke(r,ob,p,loc): 权限撤销, 即撤销角色 r 在空间位置 loc 上对客体 ob 的访问权限.

• Appoint(u,r,loc)/un Appoint(u,r,loc): 用户角色指派, 表示指派用户 u 在空间位置 loc 上得角色 r.

• Acticate(u,r,loc)/unActicate(u,r,loc): 用户 u 在空间位置 loc 激活/不激活角色 r.

• Return_object(r,loc,p): 返回当前在位置 loc 上的拥有权限 p 的所有角色.

• Return_Accessing(r,loc): 返回当前正在空间位置 loc 上有效的角色.

• SessionRoles(s): 返回会话 s 中的会话角色.

• EffectiveSessionRoles(s): 返回会话 s 中的有效角色.

• Return_Request(r, loc): 返回角色 r 在空间位置 loc 上的所有请求权限.

• countr(loc, S(Appoint(u,r,loc))): 返回角色 r 在空间位置 loc 中 被成功请求的次数.

…

3 SDT-RBAC模型空间约束规则库定义

在 SDT-RBAC 模型中, 针对空间特性的扩展上, 我们将空间约束分为激活空间区域约束、激活空间角色基数约束和空间职责分离约束.

为了方便描述, 对空间范围进行定义:

定义 2. 空间范围 SR={(IP_i,IP_j)｜IP_i,IP_j∈LOC, IP_i<IP_j},空间范围由两个空间地址构成的区间, 对<关

系我们定义如下:

$\forall i, j \in N, \forall IP_i, IP_j \in LOC, IP_i < IP_j <=> a_i < a_j \mid a_i = a_j \cap b_i < b_j \mid a_i = a_j \cap b_i = b_j \cap c_i < c_j \mid a_i = a_j \cap b_i = b_j \cap c_i = c_j \cap d_i < d_j$

3.1 激活空间区域约束

定义 3. 激活空间区域约束 记为 In_Range(SR, S). 表示在空间范围 SR 内, 能否做用户角色分配或角色授权或改变角色状态等, 从而实现一次会话.

激活空间区域约束集大概可分为如下几类:

1) 角色有效约束: 记为 In_Range(SR,S(Permit(r, ob,p,loc))={r | r∈R∧r∈SessionRoles (s) ∧Contains (SR, LOC)=TRUE};

2) 角色无效约束: 记为 In_Range(SR,S(Deny(r, ob,p,loc))={r | r∈R∧r∈EffectiveSessionRoles(s) ∧ Contains(SR, LOC)=FALSE};

3) 角色授权约束: 记为 In_Range(SR,S(Auth(r, ob,p,loc))={<r, p> | r∈R∧p∈P∧Contains(SR, LOC)= TRUE};

4) 角色权限收回约束: 记为 In_Range(SR,S(un Auth(r,ob,p,loc))={<r, p> | r∈R∧p∈P∧Contains(SR, LOC)=FALSE};

5) 用户角色授权约束: 记为 In_Range(SR,S (Appoint(u,r,loc))={<u, r> | r∈R∧u∈U∧Contains (SR, LOC)=TRUE};

6) 用户角色撤销约束: 记为 In_Range(SR, S(unAppoint(u,r,loc))={<u, r> | r∈R∧u∈U∧Contains (SR, LOC)=FLASE};

3.2 激活空间角色基数约束

使用空间信息来定义基数限制的方法可以让我们更细粒度的表达访问控制策略. 我们将激活空间角色基数约束分为三类: 空间角色最大基数约束、对象最大访问约束和用户最大访问约束.

定义 4. 空间角色最大约束 主要是限制在一个特定空间内, 一个角色激活基数的最大上限. 形式化的表达为

$\forall r_i \in R, \forall SR_j \in SR, \forall MAX_r \in N\{countr(SR_j, S(Appoint(u,r, SR_j))) \leqslant MAX_r$.

其中MAXr是空间位置LOC可激活角色的最大次数.

定义 5. 最大访问约束: 规定在一个特定空间位置, 一个客体被访问的最大上限, 不论这些访问是否同时申请. 记为 COUNTx(loc,MAXs,S(Appoint (o,p,loc))), 表示为

$\forall SR_j \in SR, \forall MAXs \in N\{COUNTt(SRj, S(Appoint (o,p. SR_j))) \leqslant MAXs\}$,

其中, Appoint (o,p,loc)表示在该空间位置正在执行对客体 o 的访问 p, MAXs 是空间位置 LOC 可执行的最大访问数目约束.

定义6. 用户最大访问约束: 规定在一个特定的空间位置, 一个用户可同时执行的最大上限. 记为 COUNTu(loc,MAXu,S(Access (u,o,p,loc))), 表示为

$\forall u_i \in U, \forall SR_j \in SR, \forall MAXs \in N\{COUNTu (SR_j,S(Appoint (u,o,p. SR_j))) \leqslant MAXs\}$,

其中, Appoint (u,o,p,loc)表示在该空间位置用户 u 正在执行对客体 o 的访问 p,MAXs 是空间位置 LOC 可执行的最大访问数目约束.

3.3 空间职责分离约束

在传统的 RBAC 模型中, 职责分离约束主要是防止授权冲突, 如一个企业中, 出纳和会计是不允许同时授权给一个用户的. 在 SDT-RBAC 模型中, 我们通过对用户角色分配与激活的情况对角色授权进行了互斥约束, 该约束被定义为静态职责分离和动态职责分离两类.

定义7. 静态职责分离: 静态职责分离的目的是对授权过程进行约束, 以防止主体获得足够权限而进行的自我欺诈行为, 主要规则如下:

1) 若 $cr \subseteq R$ 且 cr 中的任意两个角色是冲突的, 则称 cr 为冲突角色(U-SSoD). 冲突角色集的表示为 $CR=\{cr_1,cr_2 \cdots cr_n\}$. 同理可定义冲突用户 cu 和冲突用户集 CU,冲突权限 cp 和冲突权限集 CP.

2) 冲突角色约束(UR-SSoD1): 即同一用户不能属于冲突的角色, 表示为 $\forall cr_i \in CR(\forall_{r1,r2} \in cr_i \Rightarrow user (r_1) \cap user(r_2)= \phi)$, 其中 user(r)表示属于角色 r 的用户集.

3) 冲突用户约束(UR-SSoD2): 即冲突的用户不能指派为冲突的角色, 表示为 $\forall cu_i \in CU, cr_j \in CR (\forall_{u1,u2} \in cui \Rightarrow (role(u_1) \times role(u_2)) \cap (cr_j \times cr_j)= \phi)$, 其中 role(u)表示分配给用户 u 的角色集.

4) 角色-权限约束(RP-SSoD1): 即不能赋予角色冲突的权限, 表示为 $\forall cp_i \in CP(\forall_{p1,p2} \in cp_i \Rightarrow role (p_1) \cap role(p_2)= \phi)$, 其中 role(p)表示拥有权限 p 的角色集.

5) 权限-角色约束(RP-SSoD1): 即冲突的权限不能授予冲突的角色, 表示为 $\forall cp_i \in CP, cr_j \in CR (\forall_{p1,p2}$

$\in cp_i \Rightarrow (role(p_1) \cap role(p_2)) \cap (cr_j \times cr_j) = \phi$).

定义 8. 动态职责分离: 动态职责分离主要是对角色在激活的过程中进行的限制, 规则如下:

1) 位置-角色约束(ACT-DSoD): 任意一个用户不能在同一位置 LOC 得到冲突角色集 R 中的 2 个或以上角色, 表示为: $\forall r_i, r_m \in R, \forall u_j \in U, \forall loc_l \in LOC(r_i \in Acticate(u_j,r,loc_l) \wedge r_m \in Acticate(u_j,r,loc_l) \rightarrow (r_i,=r_m))$.

2) 冲突角色激活约束(UR-DsoD): 任意一个用户不能同时激活 2 个或 2 个以上的冲突角色(), 表示为 $\forall cr_i \in CR(\mid role(sessions(u_j)) \cap cr_j \mid <=1))$, 其中 $role(sessions(u_j))$表示用户 u_j 通过会话激活的所有角色, 运算符“丨丨”表示集合的基数, 即元素的个数.

3) 冲突激活约束(S-DSoD): 任意一个会话不能同时激活 2 个或 2 个以上的冲突, 表示为 $cr_i \in CR (\forall s_j \in S(\mid cr_I \cap role(s_j) \mid <=1))$, 其中 $role(s_j)$是会话 s_j 激活的角色集.

用户在一个空间区域内建立会话, 如果该会话与某约束相关, 系统自动触发对应约束; 若不存在于该会话相关约束, 则会话可运行知道结束或被其他会话中止. 因此, 在整个会话的生命期中, 他分为 run, down, error 和 stop 四种状态, 如图 1 所示. 一个会话状态的转换, 是依据对约束的判定.

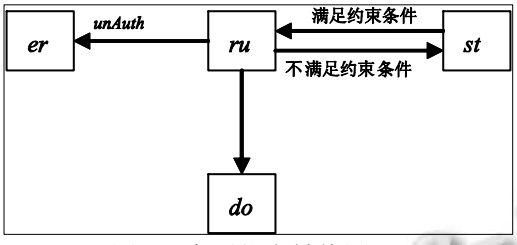

图 1　会话状态转换图

此外, 为了让本模型更加完善, 本文还定义了一些其他约束, 由于篇幅有限, 列举如下两个约束进行说明.

定义 9. 其他约束

时间约束: 即用户指派角色的时间或角色获得权限的时间. 地理空间数据中部分数据较敏感, 需限定用户访问的有效时间, 有效期内可访问, 超时后角色权限自动回收.

角色层次(RH): $RH \subseteq R \times R$ 是角色集 R 上的偏序关系, 用>表示, 设 $r_1, r_2 \in R$ 且 $r_1 > r_2$,表示 r_1 是 r_2 的上级角色, r_1 拥有的 r_2 的所有权限, 角色层次可以看作是一种静态约束, 表示授予下级角色的权限, 也必须授予该角色的上级权限.

4　模型应用

本项目为福建省科技重点项目, 主要是针对福建省的生物信息多样性特点, 构建实时监控系统. 在该项目中, 需要对国家珍稀植物的分布数据进行保护, 其他植被分布属于一般数据, 无需权限控制. 在该系统中有这样几个角色: 主任, 主要进行信息的最后审核, 包含珍惜物种的信息更新、新物种的上报等; 技术员, 负责处理技术问题, 可在办公室阅览机密的技术资料; 巡山员, 负责对所管辖区域的物种进行定期的检测和信息上报.

在上述场景中, 我们构建 R={DC, TC, PC}, 其中, DC 表示主任, TC 表示技术员, PC 表示巡山员. LOC={DA, AUO, TCO, PCO}, 其中, DA 表示档案室, TCO 表示技术人员办公室, PCO 表示巡山员所负责区域. 由 3.1 节定义的角色授权约束可知, 只有在审核员办公室, 才可以给审核员分配信息审核的权限, 只有在档案室, 巡山员才可以查阅以往的珍惜物种基本信息, 只有在技术人员办公室才可以给技术人员和巡山员分配查阅珍惜物种的详细信息的权限, 只有在巡山员所负责区域, 该巡山员才可以上报珍惜物种的变化情况与新物种的发现确认请求.

假设 A 为巡山员, 并在 loc_1 创建了会话 s_1. 根据 3.1 节角色有效约束可知, 如果 loc_1 对应的逻辑位置在 DA 内, 则空间角色(PC, DA)在会话 s1 中是有效的; 如果 loc_1 对应的逻辑位置在 PCO 中, 则空间角色(PC, PCO)在会话 s_1 中是有效的. 为了保证信息的一致性, 技术员与巡山员不能由同一用户承担, 根据 3.3 节定义的静态职责分离约束定义, 即(PC,DA),(PC,PCO) $\in$ UR-SSoD1. 为了防止珍惜物种信息外泄, 系统约定同一个会话中, 用户不能再位置域 TCO 与 PCO 同时激活技术员这一角色, 根据 3.3 节的定义, 我们需要实施空间动态职责分离约束(TC, TOC),(TC, POC) $\in$ ACT-DSoD.

当一个会话会话相关的空间约束被激活, 访问控制系统将根据用户当前的位置信息进行计算, 若会话状态发生改变, 则进行重新计算. 因此会话会根据对约束的判定, 在它的生命期中在 run, down, error 和 stop 四种状态间转换. 通过对会话状态调整可对用户

进行控制, 发现恶意用户可立即将该角色变为无效状态, 保证系统安全, 也提高了系统效率.

5 结语

本文针对现有 RBAC 模型的不足, 提出了一种支持空间、时间特性的角色访问控制方法—SDT-RBAC, 它能够满足基于移动用户位置的信息服务系统和空间数据库系统对访问控制模型的要求. 本文分析了空间数据的特征后, 对原有的 RBAC 模型在约束、会话等方面进行了空间扩充, 针对空间数据的特点, 提出了激活空间区域约束、激活空间角色基数约束和空间职责分离约束三类约束, 解决了有关访问控制中有关空间约束方面的需求. 下一步的工作中, 我们将对空间数据一致性维护等方面进行研究.

参考文献

1 Bacon J, Moody K, Yao W. A model of OASIS role-based access control and its support for active security. TISSEC, 2002,5(4).

2 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.中国科学 E 辑:信息科学, 2007,37(2):254–271.

3 Joshjbd, et al A generalized temporal role-based access control model. IEEE Trans. on Knowledge and Data Engineering, 2005,17(1):4–23.

4 Chun S, Atluri V. Protecting Privacy form Continuous High-resolution Satellite Surveillance.Technical report. CIMIC, Rutgers University, 1999.

5 Bertino E, Catania B, Damiani ML, et al. GEO-RBAC:a spatially aw are RBAC. Proc. of Symposium on Access Control Models and Teachnologies, Stockholm, 2005:29–37.

6 Belussi A, et al. An authorization model for geographical maps. Proc. of the 12th Annual ACM International Workshop on Geographic Information Systems. ACM: Washingeton DC, USA, 2004.

7 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.软件学报,2011,22(8):1872–1883.

8 Damiani M, Bertin E. Spatial Data on the web: Modeling and Management. Berlin: Springer. 2007:189–214.

9 张颖军,冯登国,陈恺.面向空间索引树的授权机制.通信学报,2010,31(9):64–73.

(上接第 89 页)

和 RBPNN 的文本分类方法具有很好的分类效果. 分类器的查全率和查准率相比较传统的特征向量空间模型的 RBPNN 分类器、加权特征向量空间模型的 RBFNN 和 PNN 分类器的结果都得到了很好的改善, 而且训练时间也相对较短. 一定程度上表明了该方法的有效性, 今后我们将进一步研究如何细化文档中特征项位置的信息及各个部分权值的优化以及 RBPNN 网络的结构参数的优化.

参考文献

1 Wang W, Yu B. Text categorization based on combination of modified back propagation neural network and latent semantic analysis. Neural Comput & Applic. 2008. 2009, (18):875–881

2 Wang Z, He YF, Jiang MH. A Comparison among Three Neural Networks for Text Classification. IEEE.2006.

3 漆随平,于慧彬,刘涛,等.基于径向基概率神经网络的气象参数状态识别.自动化仪表,2008,29(8):5–7.

4 李伦波,马广富.基于 RBPNN 的退化交通标志图像的识别算法.吉林大学学报,2008,38(6):1429–1433.

5 许增福,梁静国,由晓宇.基于 FVSM 和自组织映射网络的 Wreb 文本自动分类方法.哈尔滨工业大学学报,2004,36(9): 1168–1171.

6 庞景安.Web 文本特征提取的研究与发展.信息系统,2006 29(3):338–340.

7 郑凤萍,刘春雨.基于模糊 VSM 和 RBF 网络的文本分类方法.情报科学,2007,25(4):588–591.

8 皱娟,周经野,邓成,等.基于多重启发式规则的中文文本特征提取方法.计算机工程与科学,2006,28(6):78–80.

9 刘松,王展.基于径向基概率神经网络的人脸识别方法.计算机工程与科学,2006,28(2):83–87.

10 周开利,庄耀红.神经网络模型及其 matlab 仿真程序设计. 北京:清华大学出版社,2005.

11 matlab 中文论坛.matlab 神经网络 30 案例分析.北京:北京航空航天大学出版社,2010.