Available online at www.sciencedirect.com
ScienceDirect
Trans. Nonferrous Met. Soc. China 24(2014) 2946−2953
Transactions of Nonferrous Metals Society of China
www.tnmsc.cn

Multi-granularity spatial-temporal access control model for web GIS

Ai-juan ZHANG[1, 2], Jing-xiang GAO[2], Cheng JI[1], Jiu-yun SUN[2], Yu BAO[1]

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

Received 17 November 2013; accepted 15 January 2014

Abstract: The multi-granularity spatial-temporal-related access control (MSTAC) model was proposed to meet the spatial access control requirements for the service-oriented spatial data infrastructure (SDI). MSTAC extends the attribute constraints of role-based access control (RBAC), which includes the user's location attribute, the role's time constraint, the layer vector constraint of a map class, the scale and time constraints of a geographic layer, the topological constraints of geographic features, the semantic attribute expression constraints of geographic features, and the field constraint of feature views. Through this model, authorized users would be limited to access different granularity spatial datasets, such as the map granularity, the graphic layer granularity, the feature object granularity and the feature view granularity. Finally, the MSTAC model is achieved in a web GIS, which shows the positive and negative authorizations to different services in different data granularities and time periods.
Key words: MSTAC; multi-granularity control; space; web GIS

1 Introduction

With the development of web GIS, geographic data sharing is increasing. Because of its economic value and the importance for national security, spatial access control has become a hot issue in GIS security research. Assuming that services are based on object-oriented data model, the requirements of spatial access control have been addressed as follows [1]: it is not sufficient to restrict the access to the entire service; for context dependant access restrictions, context refers to the state of the system (time, number of accesses today, etc.); for class-based restrictions, it shall be possible to restrict access to a class. For WMS (web map service), this requirement refers to restricting the map access for each individual layer or for a set of layers; for object-based restrictions, it should be possible to restrict access to individual object (or parts of objects) of a class. For WFS (web feature service), this requirement refers to restricting the access for a feature type, certain elements or attributes of a feature type; for spatial restrictions, it shall be possible to restrict access based on the resource geometry if a certain spatial relation to a given geometry exists; it is possible to declare positive and negative permissions.

At present, traditional access control models, such as discretionary access control (DAC) and role-based access control (RBAC) cannot achieve multi-granularity control and spatial-temporal constraints. Consequently, new access control models and mechanisms are needed. Since RBAC is policy-neutral, simplified access management, and used by commercial applications, we will base our work on this model. Some work has been done on spatial access control model. SASAOKA and MEDEIROS [2] proposed a spatial data authorization model for spatial databases to solve the space location constraints. BERTINO et al [3] extended the RBAC model, GEO-RBAC, to handle the location context. Afterwards, spatial access control models with physical location and time contexts [4−10] were put forward. Spatial access control models were put forward for distributed multi-domain GIS [11,12]. Fine-grained access control models were proposed for GEO web

Foundation item: Projects (41074010, 41171343) supported by the National Natural Science Foundation of China; Project (BK20140185) supported by Jiangsu Province Natural Science Foundation for Youths, China; Project (51204185) supported by National Youth Science Foundation of China; Project (2014QNA44) supported by Youth Science Fund of China University of Mining and Technology
Corresponding author: Jing-xiang GAO; Tel: +86-516-83885785; E-mail: jxgao@cumt.edu.cn
DOI: 10.1016/S1003-6326(14)63430-0

services [7,13−15]. ZHANG et al [16] proposed mandatory access control model for spatial vector data. These models cannot meet multi-granularity control requirements: class-based control, object-based control and object attribute-based control, and they only achieve single-granularity and even coarse granularity access control for geospatial data. Therefore, a multi-granularity and multi-scale spatial-temporal access control model is proposed in an appropriate way.

Firstly, the MSTAC model is proposed, and then the formalized attribute constraints are given to realize the time context-based, map-based, layer-based, feature-based, and feature view-based authorization. After that, the access control mechanism is presented. Finally, the MSTAC model is achieved for SDI in different granularity control and time control.

2 MSTAC model

The core RBAC model includes four components: user, role, operation and object. It does not take into an account context factors and spatial restraints. In addition, accurate description of different granularity spatial objects will lead to the rapid growth in the number of policy rules, which will make policy definition unrealistic. In order to solve the above problems, we propose MSTAC model to extend the core RBAC with attribute constraints. The MSTAC model is shown in Fig. 1.

The model implements time context-based control by adding the time constraint in the process of URA (user−role assignment). It implements multi-granularity and multi-scale resource control by increasing data constraints. The layer vector constraint can achieve map granularity control in a certain database; the scale and time constraints can achieve multi-scale geographic layer (class-based) granularity control; the geometry and semantic constraints can achieve feature (object-based) granularity control; and the field constraint can achieve feature view granularity control. The elements of MSTAC are defined as follows:

User=(identifier, location, role). The identifier attribute is used to confirm the user's identity, the location attribute represents the region that the subject belongs to, and the role attribute represents the user's permission set.

Role=(name, permissions): the unit of permission assignment. When a session is established in a period of time, the roles of the user would be active with the appropriate permission set.

Permission=(operations, spatial objects). They are associated with objects and operations, and would be assigned to certain roles in policy rules.

Operation: the public methods of a spatial class.

Spatial object: spatial datasets in different granularities which are map objects, graphic layer objects, feature objects and feature view objects.

$URA \subseteq (User \times time \times Role)_{C_1}$, $C_1 \in$ {time constraint, separation of duty constraint}. In certain period, roles are assigned to users.

$PRA \subseteq (P \times time \times R)_{C_2}$: the m:n mapping from the set of permissions to the set of roles in certain period of time.

$C_2 \subseteq C_{\text{map}} \cup C_{\text{lay}} \cup C_{\text{F}} \cup C_{\text{V}}$

$C_{\text{map}} \subseteq$ {time constraint in PRA} $\cup$ {layer vector constraint};

$C_{\text{lay}} \subseteq$ {time constraint in PRA} $\cup$ {scale & mapping time constraints};

$C_{\text{F}} \subseteq C_{\text{lay}} \cup$ {spatial & semantic constraints};
$C_{\text{V}} \subseteq C_{\text{F}} \cup$ {field constraint}

There are context-related constraints during the PRA, and the other four elements of the collection mean constraints to different granularity spatial objects. C_{map} means the map granularity constraint and the context

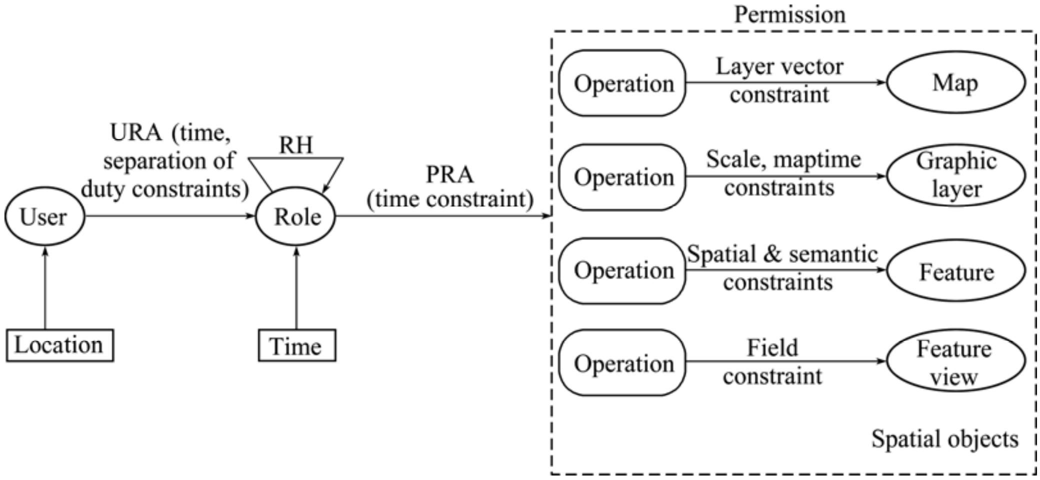

Fig. 1 MSTAC model

constraint; C_{lay} means the graphic layer granularity constraints and the context constraint; C_{F} means the feature granularity constraints and the context constraint; and C_{V} means the feature view granularity constraints and the context constraint.

$RH \subseteq (R\times R)_C$: the partial ordering relation among the role sets. It represents the permission inheritance between two roles.

In order to realize the spatial restriction, the location attribute is added to users, and the user's location is an element of the request from the client.

3 Attributes of spatial subjects

Location is needed in the spatial constraint to implement feature granularity authorization, which is based on the topological relation between resource geometry and the given geometry derived from the location attribute of the subjects. There are two kinds of location descriptions: logic location and real position.

Definition 1 (Logic location: *lloc*): Logic location defines subject's logic spatial boundaries or spatial points. For example, *lloc*= {"Jiangsu", "Anhui", "Beijing"}.

Definition 2 (Real location: *rloc*): Real location may represent a physical point or region [17,18]. If it is the latter, the region will be expressed by the spatial reference system (SRS) and the points (*phyP*) at the closure boundary.

$rloc$= (SRS, $\{phyP_1, phyP_2,\cdots, phyP_n\}$);

$phyP \subseteq (long\times lat\times hig)$;

$long \in [-180,180]$, and it is a longitude value;

$lat \in [-90, 90]$, and it is a latitude value;

$hig \in N$, and it represents elevation.

Definition 3 (*M*: location mapping function): It is related to a particular application.

M: M(*lloc*)→ *rloc*. The function is used to map a location into a real location. If we want to compute the real position of a user playing a role in a session, the location mapping function *M* should be defined in the access decision module.

In order to achieve time context-based authorization, the time attribute is added to the role of MSTAC in the process of URA and PRA. The time attribute is defined as follows:

Definition 4 (*Time*): In this model, we express time as a periodic interval and it is defined as follows [19]:

$time = (I, P)$, $I = [begin, end]$

where *P* is the expression of cycle time; *begin* and *end* indicate upper and lower time points of *P*, respectively.

$$P = \sum_{i=1}^{n} O_i \cdot C_i \rhd x\cdot C_d,\quad O_1=all \quad \text{and} \quad O_i \in 2^N \cup \{all\}$$

where C_d and C_i are calendars, which are of the form in Years, Months, Days and Hours, with hours being the finest in granularity. The $\rhd$ symbol separates the set of starting points defined using C_i from the duration of each period defined using C_d.

4 Multi-granularity object constraints

In web GIS infrastructure, the declaration and enforcement of policy should be independent from the services because one service can carry different operations to be invoked on resources. In such respect, the same operation can obtain the access to different resources using different access modes, so access constraints should be enforced on resource objects. The object control of MSTAC is shown in Fig. 2.

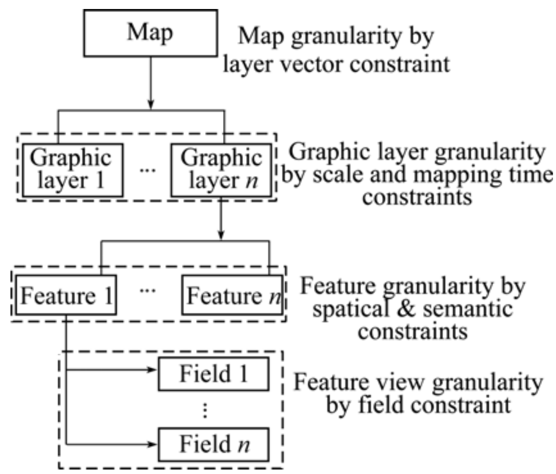

Fig. 2 Multi-granularity description of spatial vector data

There are four kinds of authorization granularities, including map granularity, geographic layer granularity, feature granularity and feature view granularity. We implement the multi-granularity definition by resource constraints. In object-oriented programming design, it is possible to declare and enforce access restrictions on object-oriented data model. The access control rule (*R*) can be represented as a four-valued tuple, namely subject (role), operation, resource, condition and the effort is permit or deny.

$R=\{S_R, O, RM, C\} \rightarrow$ {deny, permit}

$$RM=\{R_{\text{class}}; (G_{\text{map}} \text{ or } G_{\text{Lay}}); G_{\text{F}}; G_{\text{V}}\} \quad (1)$$

where S_R identifies the role to which this permission is associated; *O* defines an operation with fixed name; *RM* is a resource match expression; R_{class} is a resource class; G_{map} is the constraint of the map granularity; G_{Lay} is the constraint of the layer granularity; G_F is the constraint of the feature granularity; G_V is the constraint of the feature object view granularity; C is the condition that is a Boolean expression.

4.1 Map granularity constraint

The map granularity constraint is used to limit the available layers. RM_{map} is used to define map granularity resource matching element. R is a map class of a certain graphic base. *FVec* is used to restrict the available layers. *Re* is the client request.

$$R=\{S_R, O, RM_{map}, C_{map}\} \rightarrow \{\text{deny, permit}\}$$
$$RM_{map} = \{R; G_{map}; null; null\}$$
$$G_{map} = \{FVec \mid FVec = [0 \mid 1^*]\} \quad (2)$$
$$C_{map} = \begin{cases} \text{true}, \ Re.time \in (I, P) \rightarrow true \wedge FVec = [*1*] \\ \text{false}, \ \text{else} \end{cases}$$

Each bit of *FVec* corresponds to a certain feature member of a map class. “1” represents that this layer would be displayed, while “0” represents the opposite. For example, the following rule declares that the role “admin” can read all three graphic layers in the map “ChinaInfo”.

$$\{admin, read, \{ChinaInfo; FVec = [111]; null, all\}, all\} \rightarrow \text{permit}$$

4.2 Geographic layer-based constraints

The geographic layer-based constraint limits the resource to all instances of a class. Therefore, G_F=G_V=*null*. RM_{Lay} is used to define geographic layer-based resource matching element. G_{Lay} constraint is used to restrict a geospatial layer to specific scale or specific time attribute (G_{Lay}) in multi-scale GIS. *Re* is the request from client.

$$R=\{S_R, O, RM_{lay}, C_{Lay}\} \rightarrow \{\text{deny, permit}\}$$
$$RM_{lay} = \{R; G_{Lay}; null; null\} \quad (3)$$
$$G_{Lay} = s \cup time \mid \{s \in N \wedge s \le \phi_{max} \wedge s \ge \phi_{min}\} \cup \{atime \in period\}$$
$$\phi = [\phi_{min}, \phi_{max}](\phi_{min}, \phi_{max} \in N) \quad (4)$$
$$C_{Lay} = C_{map} \cup \begin{cases} Re.time \in (I, P) \rightarrow \text{true} \ (scale = null \cap atime = null); \\ Re.time \in (I, P) \rightarrow \text{true} \ (scale != null \wedge Re.R.scale \in scale) \wedge (atime != null \wedge Re.time \subset atime) \rightarrow \text{true}; \\ \text{false, else} \end{cases} \quad (5)$$

For example, the following rule declares that the *getInfo* access to *Building* is restricted in the time period of [8:00 AM, 11:00 PM], and the scale attribute of the class is restricted into the scale {30, 10, 5}, and its time attribute is in the year 2000.

$$\{*, getInfo, \{Building; scale = \{30, 10, 5\}, atime{=}2000; null; null;\}, [8:00\ \text{AM}, 11:00\ \text{PM}]\} \rightarrow \text{permit}$$

4.3 Feature-based constraints

The feature-based granularity is the extension of the geographic layer-based granularity (G_{Lay} is defined as the above section), and the feature-based matching element (RM_F) is to be enforced for particular objects only. There are two kinds of feature-based constraints: semantic attribute constraints and spatial constraints. *Re* is the client request.

$$R=\{S_R, O, RM_F, C_F\} \rightarrow \{\text{deny, permit}\}$$
$$RM_F = \{R; G_{Lay}, G_F, null\} \quad (6)$$

1) Semantic attribute constraints

$$G_F = \bigcup_{i=1}^{n} AttExpression_{[i]} \quad (7)$$

$$C_F = C_{map} \cup C_{lay} \cup \begin{cases} Re.time \in (I, P) \rightarrow true\,(Re.R.Attr[i] = null); \\ Re.time \in (I, P) \rightarrow true\,(Re.R.Attr[i] != null) \wedge (\bigwedge_{i=1}^{n} Re.Att[i] \cap AttExpression[i]) != null; \\ \text{false, else} \end{cases} \quad (8)$$

If a complex semantic attribute restriction is needed, the logical operators “and” and “or” can be used.

For example, the following rule declares that the role admin can access “City” by *getInfo* function, with the area and the population of the city being respectively less than 50000 km^2 and 5 million.

$$\{admin, read, \{City; null; (area < 50 \wedge population < 500), all\}, all\} \rightarrow \text{permit}$$

2) Spatial constraints

$$G_F = SpatialRel \quad (9)$$

$$C_F = C_{map} \cup C_{lay} \cup \begin{cases} SpatialRel(Geo_P, Geo_R) \rightarrow true \wedge Re.time \in (I, P) \rightarrow true \wedge Re.R \cap Geo_R != null; \\ \text{false, else} \end{cases} \quad (10)$$

$$Geo_P = S_R.location \subset lloc\ ?\ M(lloc) : rloc \quad (11)$$

$$Geo_R = Query(RM_F) \quad (12)$$

$$SpatialRel \in \{Equals, Disjoint, Touches, Crosses, Within, Overlaps, Intersects, getInfo, \neg Equals, \neg Disjoint, \neg Touches, \neg Crosses, \neg Within, \neg Overlaps, \neg Intersects, \neg getInfo\} \quad (13)$$

In order to declare spatial topological relations in a negative way, the *SpatialRel* is extended to the logically negative: $\neg$*Equal*, $\neg$*Disjoint*, $\neg$*Touches*, $\neg$*Crosses*, $\neg$*Within*, $\neg$*Overlaps*, $\neg$*Intersects* and $\neg$*Equals*. For example, *admin* is entitled to read objects of class *Building* if the geometry of the spatial property shape is within the area "Suzhou".

$$\{admin, read, \{Building; null; Within"SuZhou"\}, all \rightarrow \text{permit}$$

If a complex spatial restriction is needed, the logical operators "and" and "or" can be used.

4.4 Feature view-based constraint

The constraint based on feature view is used to control the available attributes of the feature type. With this constraint, part or all of the attributes of geospatial objects can be shown to the clients. The matching element of feature view (RM_{V}) is to be enforced for field control of a feature type. C_{V} is the time context condition. G_{Lay} and G_{F} are defined as the above sections. G_{V} is the field constraint.

$$R=\{S_R, O, RM_{\mathrm{V}}, C_{\mathrm{V}}\} \rightarrow \{\text{deny, permit}\}$$

$$RM_{\mathrm{V}}=\{R; G_{\mathrm{Lay}}, G_{\mathrm{F}}, G_{\mathrm{V}}\} \quad (14)$$

$$G_{\mathrm{V}}=\bigcup_{i=1}^{n} Field_{[i]} \quad (15)$$

$$C_{\mathrm{V}}=C_{\mathrm{map}} \cup C_{\mathrm{lay}} \cup C_{\mathrm{F}} \cup \begin{cases} Re.time \in (I, P) \wedge Re.field \cap G_V \mathrel{!=} null \rightarrow \text{true;} \\ \text{false, else} \end{cases} \quad (16)$$

For example, the following rule declares that when the role *admin* accesses the system, the *getInfo* accesses to *City* (area>500 km^2) is permitted, and in the time period of [8:00 AM, 11:00 PM], the system only shows city objects' fields: *name*, *area*.

$$\{admin, getInfo, \{City; *; area > 500; name, area\}, [\text{8:00 AM, 11:00 PM}]\} \rightarrow \text{permit}$$

5 Implement of MSTAC in web GIS

To manage spatial access control policy, the policy management module achieves user−role assignment (URA) and role−permission assignment (PRA). Furthermore, in order to implement access control policy, the access control decision-making module should be achieved, with which each client request would be judged to see whether it can get the service and what kind of data it would get. The requested data will be described by query constraints. The architecture of management and decision modules is shown in Fig. 3.

5.1 Declaration of multi-granularity data

Multi-granularity permission setting is mainly achieved in the PRA process. Figure 4 shows the role-permission module to set data constraints of every granularity. There are three necessary steps including choosing a layer or layer groups, selecting executable

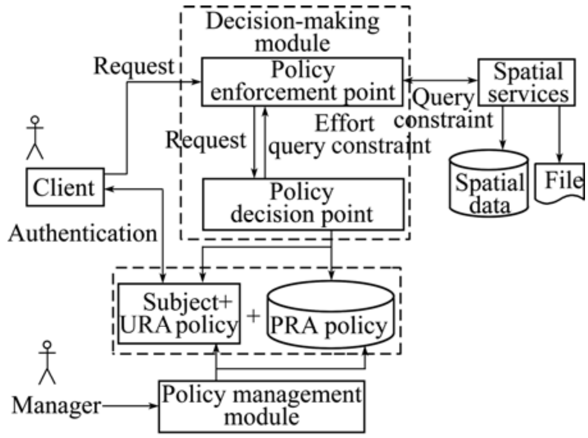

Fig. 3 Management and decision modules of MSTAC mechanism

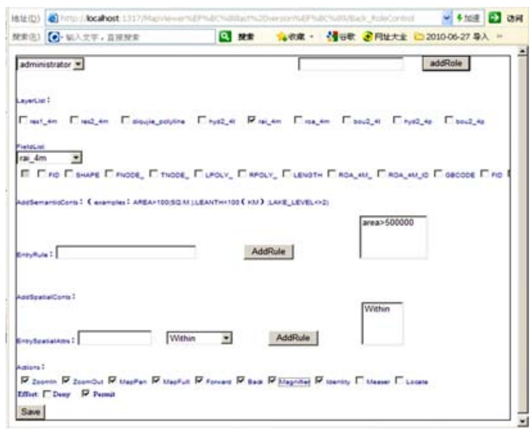

Fig. 4 PRA management module

operations and setting positive or negative permission, and two optional steps including setting feature attribute constraints, and choosing fields to display. And then saving these parameters, a policy rule would be created for a certain GIS.

5.2 Verification system of MSTAC model

The policy achieved from policy management module would be deployed and read by the access control decision-making module to make access decision when a request is sent to the GIS service. A client request will be firstly sent to decision-making module. If the request was permitted, the positive permission with constraint arguments would be sent to the service. Figures 5 and 6 show the control effect of MSTAC in a

Fig. 5 Access control in time context: (a) Complete positive authorization; (b) Deny authorization in certain time context

WMS (web map service) which was developed based on the national fundamental geographic data [20].

Figure 5(a) shows a complete visit to the map. Figure 5(b) shows a deny authorization within illegal access time.

In Fig. 6, we give the effect diagrams of different granularity control. Figure 6(a) shows the layer granularity control. Figure 6(b) shows feature granularity control. The map includes two layers, but the city layer shows part objects with spatial attribute constraint. The contrast of Figs. 6(c) and (d) shows feature-view granularity control. Authorized users in Fig. 6(c) can view all of the information of a city, but authorized users in Fig. 6(d) can only view partial information of a city object. The contrast of Figs. 6(e) and (f) shows the positive and negative operations to a dataset. All of the verification instances include the map-granularity control.

When a user sends a request to query certain feature in WFS, besides a set of feature objects, the access control policy can also control a precise object. Figure 7 shows positive and negative *getInfo* authorization for WFS (web feature service) respectively in Figs. 7(a) and (b). Therefore, MSTAC can control the access to precise

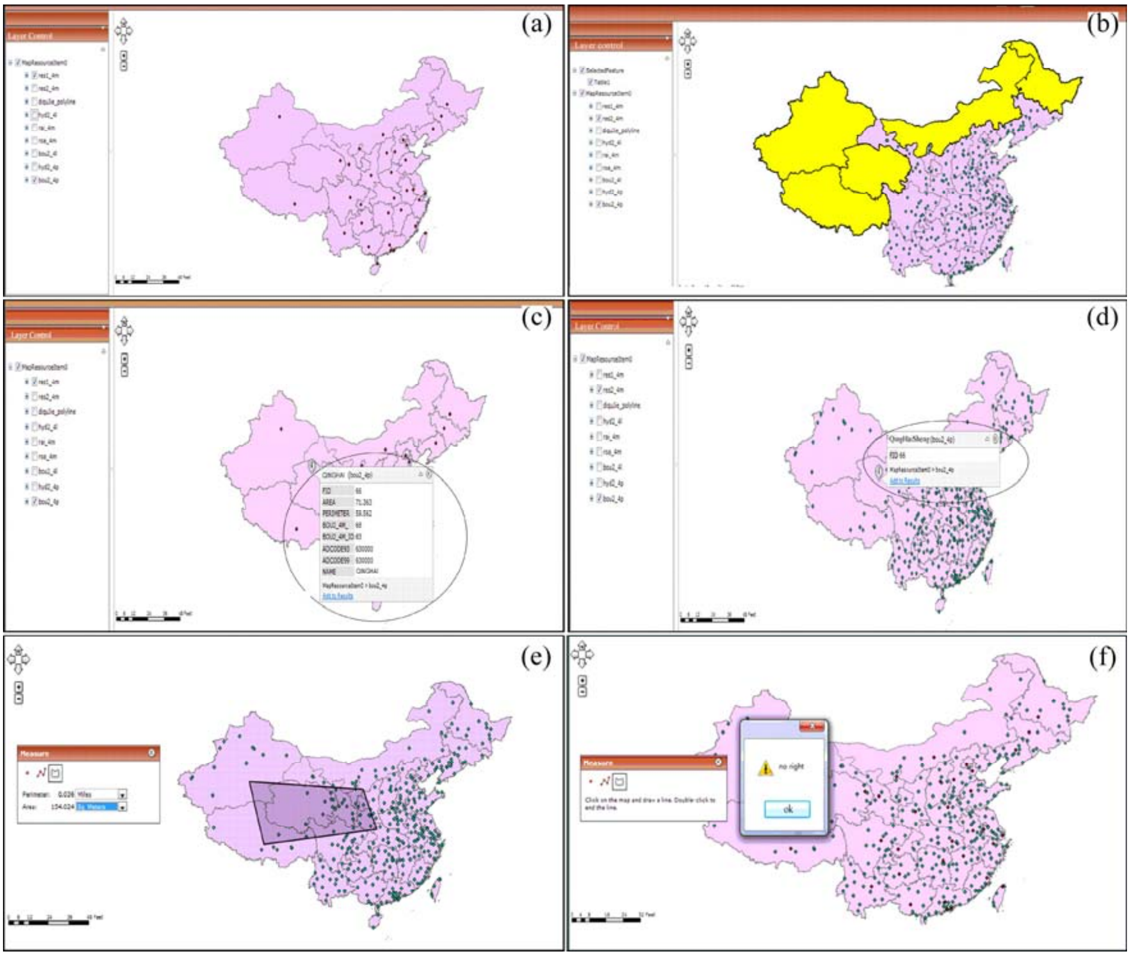

Fig. 6 Authorization based on different granularity controls: (a) Layer control; (b) Feature control with constraints; (c) Complete field constraint; (d) Part field's control; (e) Positive operation control; (f) Deny authorization

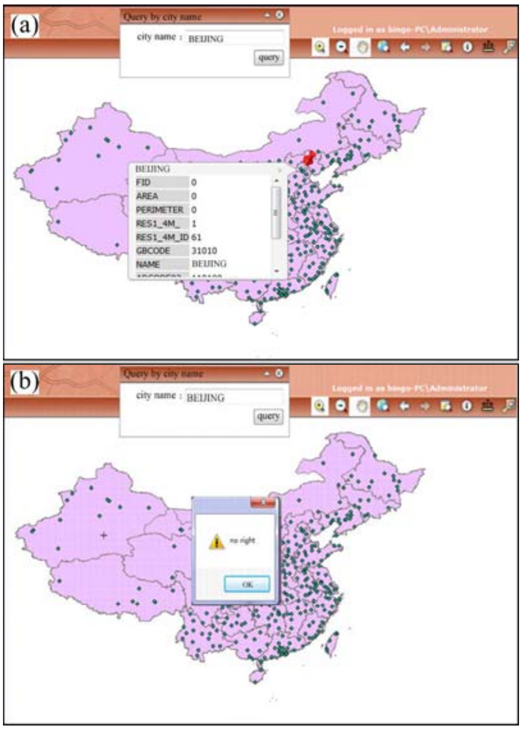

Fig. 7 Feature granularity authorization for WFS: (a) Positive WFS authorization; (b) Deny WFS authorization

spatial object by limited policy rules, which enables this model to be implemented.

6 Conclusions

1) MSTAC can implement not only coarse-grained control, but also fine-grained control.

2) Attribute constraints need to be implemented by different granularities, and attributes are divided into class-based attributes and object-based attributes. The four granularities are: map granularity (object-based), geographic layer (class-based) granularity, geographic feature (object-based) granularity, and feature object view (object-based) granularity.

3) Access control rules are not refined to control specific authorization object, which prevents the number of policy rules from increasing sharply with the spatial data growth. Thus, the implementation of access control decision model does not affect the efficiency of GIS.

References

[1] MATHEUS A. Declaration and enforcement of access restrictions for distributed geospatial information objects [D]. Munich: Technical University of Munich, 2005: 7−13.

[2] SASAOKA L K, MEDEIROS C B. Access control in geographic databases [C]//3rd International Workshop on Conceptual Modeling for Geographic Information Systems. Berlin: Springer, 2006: 110−119.

[3] BERTINO E, CATANIA B, DAMINAI M L, PERLASCA P. GEO-RBAC: A spatially aware RBAC [J]. ACM Transactions on Information and System Security, 2007, 20(10): 1−42.

[4] CHANDRAN S M, JOSHI J B D. LoT-RBAC: A location and time-based RBAC model [C]//Proceedings of the 6th International Conference on Web Information Systems Engineering. Berlin: Springer, 2005: 361−375.

[5] KUMAR M, NEWMAN R E. STRBAC—An approach towards spatio-temporal role-based access control [C]//Proc of the 3rd IASTED Int Conf on Proceedings Communication, Network, and Information Security. Calgary, Canada: ACTA Press, 2006: 150−155.

[6] AICH S, SURAL S, MAJUMDAR A K. STARBAC: Spatiotemporal role based access control [C]//Lecture Notes in Computer Science. Berlin: Springer, 2007: 1567−1582.

[7] ZHANG Hong, HE Ye-ping, SHI Zhi-guo. An access control model based on context [J]. Science in China E, 2007, 37(2): 254−271. (in Chinese)

[8] BERTOLISSI C, FERNANDEZ M. Time and location based services with access control [EB/OL]. [2012-01-28]. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04689152.

[9] ATLURI V, CHUN S A. A geotemporal role-based authorization system [J]. International Journal of Information and Computer Security, 2007, 1(1−2): 143−168.

[10] RAY I, TOAHCHOODEE M. A spatio-temporal role-based access control model [C]//Lecture Notes in Computer Science. Berlin: Springer, 2007: 211−226.

[11] DAMIANI M L, BERTINO E, SILVESTRI C. Spatial domains for the administration of location-based access control policies [J]. Journal of Network and Systems Management, 2008, 16(3): 277−302.

[12] BULATOVIC V, NINKOV T, SUSIC Z. Open geospatial consortium web services in complex distribution systems [J]. Geodetski List, 2010, 64(1): 607−619.

[13] ZHU Xia, SUN Zhen-bing. Role-based geographic entity authorized granularity control in GIS [J]. Wuhan University Journal: Natural Sciences, 2004, 29(2): 157−160. (in Chinese)

[14] MATHEUS A. Declaration and enforcement of fine-grained access restrictions for a service-based geospatial data infrastructure [C]//ACM Symposium on Access Control Models and Technologies. New York: ACM, 2005: 21−28.

[15] HERRMANN J. Interoperable access control for GEO web services in disaster management [J]. Environmental Science and Engineering, 2008, 3: 167−178.

[16] ZHANG Yan, CHEN Chi, FENG Deng-guo. Fine-grained mandatory query access control model and its efficient realization for spatial vector data [J]. Journal of Software, 2011, 22(8): 1872−1883. (in Chinese)

[17] ZHOU Jian, LI Xi-bing, SHI Xiu-zhi, WEI Wei, WU Bang-biao. Predicting pillar stability for underground mine using Fisher discriminate analysis and SVM methods [J]. Transactions of Nonferrous Metals Society of China, 2011, 21(12): 2734−2743.

[18] SHAN Zheng-ying, HAN Hou-zeng, JIANG Kun. Optimization model of GNSS/pseudolites structure design for open-pit mine positioning [J]. Transactions of Nonferrous Metals Society of China, 2013, 23(7): 2201−2208.

[19] JOSHI J B D, BERTINO E, LATIF U, GHAFOOR A. A generalized temporal role-based access control model [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(1): 4−23

[20] National fundamental geographic information system data[EB/OL]. [2012-01-23]. http://nfgis.nsdi.gov.cn/nfgis/chinese/c_xz.htm.

Web GIS 中多粒度时空访问控制模型

张爱娟[1,2]，高井祥[2]，纪 承[1]，孙久运[2]，鲍 宇[1]

1. 中国矿业大学 计算机学院，徐州 221116；
2. 中国矿业大学 环境与测绘学院，徐州 221116

摘 要：为了满足面向服务的空间数据框架对空间访问控制的需求，提出多粒度的时空相关访问控制模型 MSTAC。此模型在基于角色的访问控制模型基础上，进行属性约束扩展。属性约束包括上下文时间属性、用户的位置属性、角色的时间属性约束、地图类的图层向量约束、图层的尺度及制图时间约束、地物要素间的拓扑约束、地物要素的语义属性约束以及要素视图的字段约束。通过此模型，授权用户将受控访问不同粒度的空间数据集。这些粒度包括地图粒度、图层粒度、要素对象粒度和要素视图粒度。最后，将 MSTAC 模型在 web GIS 中实施。该实例显示了在不同的数据粒度上和不同的时间段内，系统可以对不同粒度服务进行肯定和否定授权。

关键词：MSTAC；多粒度控制；空间；web GIS

(Edited by Hua YANG)