 doi:10.20944/preprints201611.0092.v1

A Semi-Formal Multi-Policy Secure Model for Semantic Spatial Trajectories

Xingang Wang

Institute of Oceanographic Instrumentation, Shandong Academy of Sciences, Qingdao 266001, China
wangxingang2009@hotmail.com

With the proliferation of locating devices, more and more raw spatial trajectories are formed, and many works enrich these raw trajectories with semantics, and mine patterns from both raw and semantic trajectories, but access control of spatial trajectories is not considered yet. We present a multi-policy secure model for semantic spatial trajectories. In our model, Mandatory Access Control, Role Based Access Control and Discretionary Access control are all enforced, separately and combined, and we represent the model semi-formally in Ontology Web Language.

Keywords: semantic spatial trajectory; role based access control; Bell-Lapadula model; multi-policy; Web Ontology Language

1. Introduction

With the proliferation of locating devices, such as GPS, more and more spatial movement data are created. These data forms spatial trajectories, such as Geolife[24]. At first, raw spatial trajectories are created, managed, and analysed[23,25-26]. After that, some works annotate semantics on these data[7,19-22], present some semantic spatial trajectory models[1,2,4-5,11-13,17], and present some methods for mining patterns from these semantic trajectories[10,16,18]. But all these works did not consider the access control of these trajectories, both in raw and semantic form.

We present a multi-policy secure semantic model for the access control of semantic trajectory data. In our scheme, Role-Based Access Control(RBAC)[3,15], Mandatory Access Control(MAC) and Discretionary Access Control(DAC) are enforced, where we take the Bell-LaPadula model(BLP)[8-9,14] for MAC. We describe our model in Web Ontology Language(OWL).

An illustrative case of our scheme is: a leader of a company is involved in spatial trajectories related with government issues, and some employees in the company will access the spatial trajectories, and some officers int the government need to access the spatial trajectories too, where the company employs a RBAC model, and the government organization employs a MAC model, specifically, BLP model. The access control of these spatial trajectories shall be considered.

Besides, we give the concept of future trajectory to motivate out work further, that is, the two organizations above may give a future trip plan to the leader in

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 November 2016 doi:10.20944/preprints201611.0092.v1

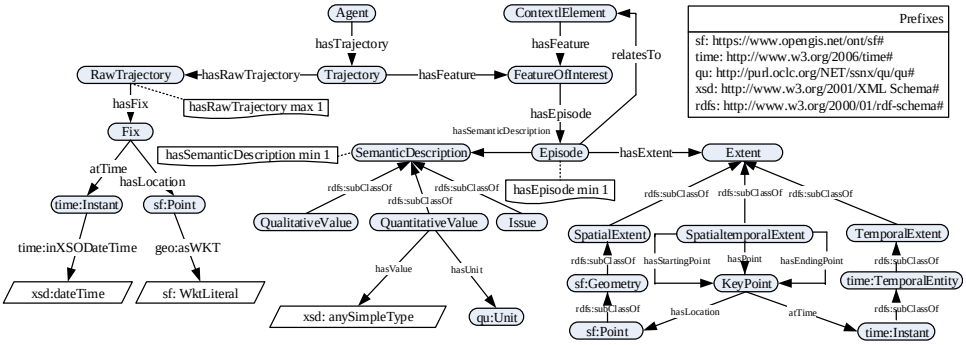

Fig. 1. Ontology of Semantic Trajectory Episode(STEP) model. Diamond-shaped nodes are datatypes.

the company. This is a semantic trajectory, not with raw spatial trajectory data. Then in the real trip, these future trajectories shall be updated with the actual trajectories with semantics enriched. The access control of these future trajectories shall be given as the above spatial trajectories.

Next in section 2 we give the preliminaries, in section 3 we give our multi-policy secure model for semantic spatial trajectories, and draw a conclusion in section 4.

2. Preliminaries

We take the semantic trajectory model of Nogueira and Martin [12] as the base of our secure model, that is, the Semantic Trajectory Episode(STEP) model. They give the model in a relative later time and we think this is a reasonable and useful model. They use STEP to structure trajectories and context into spatial-temporal episodes. A graphical representation of STEP is shown in Fig 1. It is represented in OWL.

The *Agent* class denotes the moving object. A *Trajectory* instance may have a number of *FeatureofInterest* instances and one *RawTrajectory* instance. By the *hasRawTrajectory* property, the *Trajectory* instance has at most one *Raw-Trajectory* instance. A *RawTrajectory* instance may have a series of *Fix* instances and *Fix* is composed of *time:Instant* and *sf:Point*. Through the *hasFeature* property, *Trajectory* is related with *FeatureofInterest*, and *FeatureofInterest* is related to *ContextualElement*, and *Trajectory* and *ContextualElement* instances all may have one more *FeaturesofInterest* instances. A *FeatureofInterest* instance has at least one *Episode* instance.

Episode is the smallest semantic entity, which encapsulates values that a feature of interest may assume. An *Episode* instance should have at least one *SemanticDescription* instance, which can be a quantitative value or a qualitative description, where *quantitativeValue* can be associated with different data types by *anySimpleType* defined in the XML schema,and *QualitativeValue* is used to represent other

kinds of values. Besides, we give another subclass *Issue* to *SemanticDescription*, that is, each episode is related with some semantic issues, for marking what to do in the locations of the episodes. The *Extent* class allows to specify spatial and/or temporal limits for an episode. Three sub class *SpatialExtent*, *TemporalExtent*, and *SpatialtemporalExtent* can represent the extent. A *SpatialtemporalExtent* instance has one or more *Keypoint* instance, and *SpatialtemporalExtent* is connected to *Keypoint* through three properties: *hasStartingPoint*, *hasEndingPoint*, and *hasPoint*. *Keypoint* describes the key location in the trajectory. *Episode* is related to *ContextualElement*.

3. Semi-Formal Multi-Policy Secure Model

We first give the RBAC, BLP and DAC enforcement in semantic spatial trajectories respectively and then give the enforcement of RBAC, BLP and DAC in a combined way.

3.1. *RABC Enforcement*

RBAC is always employed in organizations like companies, and the issues related with authorization is an organization action.

First, we give the permission definition. Because the permission and permission assignment are also used in DAC, not specific to RBAC. So we make the permission part as a part of STEP. We define *Object*, *Operation* and *Permission* as follows.

STEP:Object a owl:Class.
STEP:Operation a owl:Class.
STEP:Permission a owl:Class.

Then we define two properties of *Permission*, to associate an operation on an object with permission.

STEP:hasObject a rdfs:Property;
rdfs:domain STEP:Permission;
rdfs:range STEP:Object.

STEP:hasOperation a rdfs:Property;
rdfs:domain STEP:Permission;
rdfs:range STEP:Operation.

Then a permission can be assigned an operation on an object as follows.

<PermissionName> STEP:hasObject <ObjectName>
<PermissionName> STEP:hasOperation <OperationName>

Here objects mean the instances of the classes in STEP. And the objects and the operations on the objects are illustrated in Table 1. *read*, *modify* and *remove* are related to each object in the STEP model. *annotate* is only related with the *Episode* class, by which a user can annotate an episode, such as creating an issue for an episode, and *relatesto_Context* is only with *Episode* too. *insert* is related to episodes, by which a user can create instances of each subclass of *Extent* and insert

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 November 2016 doi:10.20944/preprints201611.0092.v1

Operation \ Object	read	annotate	modify	insert	remove	relatesto_Context
Trajectory	+	-	+	+	+	-
Raw_Trajectory	+	-	+	+	+	-
Fix	+	-	+	-	+	-
FeatureofInterest	+	-	+	+	+	-
Episode	+	+	+	+	+	+
SpatialExtent	+	-	+	-	+	-
SpatialTemporalExtent	+	-	+	+	+	-
KeyPoint	+	-	+	-	+	-
TemporalExtent	+	-	+	-	+	-
QuantitativeValue	+	-	+	-	+	-
QualitativeValue	+	-	+	-	+	-
Issue	+	-	+	-	+	-

Table 1. Operations on objects in Semantic Trajectory Episode(STEP) model

them to episodes. *insert* is also related to *SpatialtemporalExtent*, by which a user can create *Keypoint* instances. Other classes related with *insert* include *Trajectory*, *RawTrajectory*, and *FeaturesOfInterest*.

Next, we define roles and role hierarchy in the way of roles as values like the work in [6]. we define roles as follows.

rbac:Role a owl:Class.

We define role hierarchy by introducing the property of *subRole*.

rbac:subRole a owl:TransitiveProperty;
rdfs:domain rbac:Role;
rdfs:range rbac:Role.

Then role hierarchy can be constructed as follows.

<RoleName> rbac:subRole <SuperRoleName>.

We give permission-role assignment as follows. Fist, we define a property of *Role*.

rbac:permitted a rdfs:Property;
rdfs:domain rabc:Role;
rdfs:range STEP:Permission.

Then the assignment of permission to role can be represented as follows:

<RoleName> rbac:permitted <PermissionName>

We define *User* as an class of STEP, and this class is used in RBAC,MAC,DAC and the combined case.

STEP:User a owl:Class.

Then we define a property of the class *User*.

rbac:hasRole a rdfs:Property;
rdfs:domain STEP:User;
rdfs:range rbac:Role.

Then users can be assigned roles as follows.

<UserName> rbac:hasRole <RoleName>

We define a subclass of the class *Operation*.

rbac:PermittedOperation subClassOf STEP:Operation

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 November 2016 doi:10.20944/preprints201611.0092.v1

And we present that an operation in the access decision is permitted as follows.

<OperationName> a rabc:PermittedOperation

Then we have the following access decision rule.

read a STEP:Operation
object1 a STEP:Object
?user hasRole ?role1
?role1 hasPermission ?permission
?permission hasObject ?object2
?permissioin hasOperation ?operation
?object1 = ?object2
?operation = read
⇒ read a rbac:PermittedOperation

3.2. *BLP Model Enforcement*

The BLP model is always employed in organizations like government or military organizations. In the BLP model, each object is assigned a security label, and the user to access these objects shall be with a security label too. Each label is composed of two elements: secure level and category. Then we define secure level, category and security label as follows:

mac:Level a owl:Class.
mac:Category a owl:Class.
mac:Label a owl:Class.

And we define two properties of *Label* to associate it with its security levels and category.

mac:hasLevel a rdfs:Property;
rdfs:domain mac:Label;
rdfs:range mac:Level.

mac:hasCategory a rdfs:Property;
mac:domain mac:Label;
mac:range mac:Category.

Then we define the partial order relation of security labels by the following property.

A security level is higher or greater than another security level:

mac:greater a rdfs:Property;
rdfs:domain mac:level
rdfs:range mac:level.

A security level is equal to another security level:

mac:equal a rdfs:Property;
rdfs:domain mac:level
rdfs:range mac:level.

A security level is greater than or equal to another security level:

mac:greater-equal a rdfs:Property;
rdfs:domain mac:level
rdfs:range mac:level.

A security category is greater than another security category:

mac:greater a rdfs:Property;
rdfs:domain mac:category
rdfs:range mac:category.

A security category is equal to another security category:

mac:equal a rdfs:Property;
rdfs:domain mac:category
rdfs:range mac:category.

A security category is greater than or equal to another security category:

mac:greater-equal a rdfs:Property;
rdfs:domain mac:category
rdfs:range mac:category.

Objects in the STEP is assigned a security label as follows.

mac:hasLabel a rdfs:Property;
rdfs:domain STEP:Object
rdfs:range mac:Label.

The operations we consider for BLP includes *read*, *modify*, *annotate*, *insert*, and *relatesto_Context*. We make the *insert*,*annotate*, *relatesto_Context* as *write* in the BLP model, and make the *read* operation as *read* in the BLP model, and make *modify* as both the *read* and *write* operation in the BLP model. Then a user u can perform *annotation* or *insert* or *relates_Context* operation on an object o, only if the level and category of o are both *greater-equal* the level and category of u, and a user u can perform *read* on an object o, only if the level and category of u *greater-equal* the level and category of o, and a user u can perform *modify* on an object o only if the level and category of u *equal* the level and category of o.

We define a subclass of the class *Operation*.

mac:PermittedOperation subClassOf STEP:Operation

And we present that an operation in the access decision is permitted as follows.

<OperationName> a mac:PermittedOperation

Then the access decision rule for *read* is given as follows.

read a STEP:Operation
?user hasLabel ?uLabel
?object hasLabel ?oLabel
?uLabel hasLevel ?uLevel
?uLabel hasCategory ?uCategory
?oLabel hasLevel ?oLevel
?oLabel hasCategory ?oCategory
?uLevel greater-equal ?oLevel
?uCategory greater-equal ?oCategory
$\Rightarrow$ *read a mac:PermittedOperation*

 doi:10.20944/preprints201611.0092.v1

Our scheme supports polyinstantiation[8], for example, if one object is annotated by a user with a security level, then if another user with higher security level modify his annotation, then two corresponding annotations exist, and the former user can only see his annotation and cannot see the modified part.

3.3. *DAC Enforcement*

For DAC, we take the operations: *read*, *annotate*, *insert*, *modify*, *relatesto_Context*. Then we represent issuing permission to users as follows.

dac:hasPermissionDac a rdfs:Property;
rdfs:domain STEP:User
rdfs:range STEP:Permission.

We define a subclass of the class Operation.

dac:PermittedOperation subClassOf STEP:Operation

And we present that an operation in the access decision is permitted as follows.

<OperationName> a dac:PermittedOperation

If a user is issued a permission, then the user can perform the corresponding operation. The access decision rule on *read* is given as follows.

read a STEP:Operation
?user hasPermissionDac ?permission
?permission hasObject ?object
?permissioin hasOperation ?operation
?operation = read
⇒ read a dac:PermittedOperation

3.4. *Multi-Policy Enforcement in a Combined Way*

Here we consider the case of RBAC, BLP and DAC all being enforced in a combined way. We know BLP is employed in military and government organizations, while RBAC is always employed in organization like Companies. Then there may be collaborations between the former organizations and the latter organizations. For example, some employees in a company and some officers in a government department collaborate to complete a task or a trip. Then the spatial objects are related to both of the two organizations, so both RBAC and BLP shall be enforced. The permission-role assignment related with these objects shall be completed by the security administrator of the company, and the label related to these objects shall be given by the security administrator of the government organization. And we make that if an officer has the security label not prohibiting him from perform the operation, then he can do the operation, but if an employee wants to perform the same operation, he must not only be issued the same label, but also be assigned a corresponding role.

We define a class representing the organizations in STEP.

STEP:Organization a owl:Class.

Then we define a property *WorkIn* of the class *User*.

 doi:10.20944/preprints201611.0092.v1

STEP:WorkIn a rdfs:Property;
rdfs:domain STEP:User
rdfs:range STEP:Organization.

We define a property *withOrganization* of the class *Label*; this property is used to mark which organization a security label is issued by.

STEP:withOrganization a rdfs:Property;
rdfs:domain mac:Label
rdfs:range STEP:Organization.

And we define a subclass of the class Operation.

STEP:PermittedOperation subClassOf STEP:Operation

And we present that an operation in the access decision is permitted as follows.

<OperationName> a STEP:PermittedOperation

Then with respect to an object with a label, if a user is with a label allowing this user to perform some operation on this object, and this user belongs to the same organization as the security administrator issuing the label, then this user can perform the operation. This rule is represented as follows, with the *read* operation as an example. Here for simplicity of representation, we only use flat roles.

read a STEP:Operation
?user hasLabel ?uLabel
?object hasLabel ?oLabel
?uLabel hasLevel ?uLevel
?uLabel hasCategory ?uCategory
?oLabel hasLevel ?oLevel
?oLabel hasCategory ?oCategory
?uLevel greater-equal ?oLevel
?uCategory greater-equal ?oCategory
?user WorkIn ?organization_u
?oLabel withOrganization ?organization_o
organization_u = organization_o
$\Rightarrow$ *read a STEP:PermittedOperation*

And with respect to an object with a label, if a user is with a label allowing this user to perform some operation on this object, and this user does not belong to the same organization as the security administrator issuing the label, then this user must have the corresponding role allowing him to do the operation. This rule is represented as follows, with the *read* operation as an example.

read a STEP:Operation
?user hasLabel ?uLabel
?object hasLabel ?oLabel
?uLabel hasLevel ?uLevel
?uLabel hasCategory ?uCategory
?oLabel hasLevel ?oLevel
?oLabel hasCategory ?oCategory
?uLevel greater-equal ?oLevel

?uCategory greater-equal ?oCategory
?User WorkIn ?organization_u
?oLabel withOrganization ?organization_o
organization_u != organization_o
?user hasRole ?role
?role hasPermission ?permission
?permission hasObject ?object
?permissioin hasOperation ?operation
?operation = read
$\Rightarrow$ *read a STEP:PermittedOperation*

We define a property of the class *Object* as follows.

STEP:AssignedToRole a rdfs:Property;
rdfs:domain STEP:Object;
rdfs:range rbac:Role.

We use this property *STEP:AssignedToRole* to see if an object is with RBAC. With respect to an object without label and with RBAC, if a user has a role which makes him do the operation, then the user can do the operation; this is just like in subsection 3.1. And if a user has not a role which makes him do the operation, then the user cannot do the operation, even if the user is allowed to do the operation by DAC.

With respect to the objects without label and without RBAC, then a user can perform operations on them only if DAC allows this as in subsection 3.3.

From above we can see that when RBAC or MAC is enforced, DAC is not considered for access decision, even if DAC permission assignment has been made.

As for our scheme, especially for the collaboration case, role assignment or label association can be completed in the way that the organizations issue credentials to users, and we consider the credential-based way is appropriate for semantic spatial trajectories.

4. Conclusion

We present a multi-policy secure semantic model for the access control of semantic trajectory data. In our model, RBAC, BLP and DAC can be enforced separately for semantic spatial trajectories access control, and can be all enforced in a combined way. Especially, the multi-policy enforcement model is appropriate for the case of collaboration between government or military organizations and other organizations such as companies, where involvers create spatial trajectories security-sensitive both for these organizations.

Acknowledgments

This research was financially supported by the Youth Science Funds of Shandong Academy of Sciences, Grant No. 2013QN040, by the Special Fund for Marine Public Welfare Scientific Research, Grant No. 201505031, and by the Qingdao En-

trepreneurship and Innovation Leading Talent Project, Grant No. 13-CX-23 and 13-CX-24.

References

[1] Alewijnse S, Buchin K, Buchin M, Andrea Kölzsch, Helmut Kruckenberg, Michel A. Westenberg. A framework for trajectory segmentation by stable criteria[C]. Proceedings of the 22nd ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems. ACM, 2014: 351-360.

[2] Damiani M L, Gting R H, Valds F, Hamza Issa. Moving Objects beyond Raw and Semantic Trajectories[C].Proceedings of the 3rd International Workshop on Information Management for Mobile Applications. 2013: 4.

[3] Ferraiolo D F, Sandhu R, Gavrila S, D. Richard Kuhn, Ramaswamy, Chandramouli. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274.

[4] Fileto R, Krger M, Pelekis N, Yannis Theodoridis,Chiara Renso. Baquara: A holistic ontological framework for movement analysis using linked data[C],International Conference on Conceptual Modeling. Springer Berlin Heidelberg, 2013: 342-355.

[5] Fileto R, May C, Renso C, Nikos Pelekis, Douglas Klein, Yannis Theodoridis. The Baquara 2 knowledge-based framework for semantic enrichment and analysis of movement data[J]. Data and Knowledge Engineering, 2015, 98: 104-122.

[6] Finin T, Joshi A, Kagal L, J. Niu, R. Sandhu, W. Winsborough, B. Thuraisingham. R OWL BAC: representing role based access control in OWL[C].Proceedings of the 13th ACM symposium on Access control models and technologies. ACM, 2008: 73-82.

[7] Guc B, May M, Saygin Y, Christine Körner. Semantic annotation of gps trajectories[C]. 11th AGILE international conference on geographic information science. 2008, 38(6): 1-9.

[8] Jajodia, Sushil, and Ravi Sandhu. Toward a multilevel secure relational data model[J]. ACM SIGMOD Record 20.2 (1991): 50-59.

[9] LaPadula, Leonard J., and D. Elliot Bell. Secure computer systems: A mathematical model. Vol. 2. Technical Report 2547, 1996.

[10] Lisette Espín Noboa, Florian Lemmerich, Philipp Singer, and Markus Strohmaier. 2016. Discovering and Characterizing Mobility Patterns in Urban Spaces: A Study of Manhattan Taxi Data. In Proceedings of the 25th International Conference Companion on World Wide Web. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 537-542.

[11] Noël D, Villanova-Oliver M, Gensel J, Pierre Le Quéau. Modeling semantic trajectories including multiple viewpoints and explanatory factors: application to life trajectories[C].ACM SIGSPATIAL International Workshop on Smart Cities and Urban Analytics 2015.

[12] Nogueira T P, Martin H. Querying semantic trajectory episodes[C]. Proceedings of the 4th ACM SIGSPATIAL International Workshop on Mobile Geographic Information Systems. ACM, 2015: 23-30.

[13] Parent C, Spaccapietra S, Renso C, Gennady Andrienko, Natalia Andrienko, Vania Bogorny, Maria Luisa Damiani,Aris Gkoulalas-Divanis, Jose Macedo, Nikos Pelekis, Yannis Theodoridis, Zhixian Yan. Semantic trajectories modeling and analysis[J]. ACM Computing Surveys (CSUR), 2013, 45(4): 42.

[14] Sandhu, Ravi S. Lattice-based access control models[J]. Computer 26.11 (1993): 9-19.

[15] Sandhu R S, Coynek E J, Feinsteink H L, Charles E. Youman. Role-based access control models[J]. IEEE computer, 1996, 29(2): 38-47.

[16] Shreya Ghosh and Soumya K. Ghosh. 2016. THUMP: Semantic Analysis on Trajectory Traces to Explore Human Movement Pattern. In Proceedings of the 25th International Conference Companion on World Wide Web. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 35-36.

[17] Spaccapietra S, Parent C, Damiani M L, Jose Antonio de Macedo a, Fabio Porto a, Christelle Vangenot. A conceptual view on trajectories[J]. Data and knowledge engineering, 2008, 65(1): 126-146.

[18] Ticiana L. Coelho da Silva, Jos A. F. de Macdo, and Marco A. Casanova. 2014. Discovering frequent mobility patterns on moving object data. In Proceedings of the Third ACM SIGSPATIAL International Workshop on Mobile Geographic Information Systems (MobiGIS '14), Shashi Shekhar and Chi-Yin Chow (Eds.). ACM, New York, NY, USA, 60-67.

[19] Wu F, Li Z, Lee W C, Hongjian Wang,Zhuojie Huang. Semantic annotation of mobility data using social media[C]. Proceedings of the 24th International Conference on World Wide Web. ACM, 2015: 1253-1263.

[20] Yan Z, Chakraborty D, Parent C, et al. SeMiTri: a framework for semantic annotation of heterogeneous trajectories[C]. Proceedings of the 14th international conference on extending database technology. ACM, 2011: 259-270.

[21] Yan Z, Giatrakos N, Katsikaros V, Nikos Pelekis, Yannis Theodoridis. SeTraStream: semantic-aware trajectory construction over streaming movement data[C].International Symposium on Spatial and Temporal Databases. Springer Berlin Heidelberg, 2011: 367-385.

[22] Yan Z, Chakraborty D, Parent C, Stefano Spaccapietra,Karl Aberer. Semantic trajectories: Mobility data computation and annotation[J]. ACM Transactions on Intelligent Systems and Technology, 2013, 4(3): 49.

[23] Zheng Y, Liu L, Wang L, et al. Learning transportation mode from raw gps data for geographic applications on the web[C]. Proceedings of the 17th international conference on World Wide Web. ACM, 2008: 247-256.

[24] Zheng Y, Chen Y, Xie X, et al. GeoLife2. 0: a location-based social networking service[C].2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware. IEEE, 2009: 357-358.

[25] Zheng Y, Zhang L, Xie X, et al. Mining interesting locations and travel sequences from GPS trajectories[C]. Proceedings of the 18th international conference on World wide web. ACM, 2009: 791-800.

[26] Zheng, Yu, and Xiaofang Zhou, eds. Computing with spatial trajectories. Springer Science and Business Media, 2011.