Access Control Mechanism Based on Trust Quantification

Shunan Ma¹ Jingsha He² Xunbo Shuai³ Zhao Wang²

¹College of Computer Science and Technology
Beijing University of Technology
Beijing, China
mashunan@emails.bjut.edu.cn

²School of Software Engineering
Beijing University of Technology
Beijing, China
jhe@bjut.edu.cn

³Research Institute of Petroleum Exploration & Development
PetroChina
Beijing, China
shuaixb69@petrochina.com.cn

Abstract—In an open distributed environment, protection of sensitive files and data becomes more difficult. Traditional access control mechanisms are not suitable for such dynamic environment. Trust can be an effective approach to solve the access control problem. In this paper, by considering fuzziness and uncertainty of trust, we propose a trust quantification algorithm based on grey fuzzy comprehensive evaluation method. Then we present an access control model based on trust quantification. Simulation results show that our mechanism is suitable for dynamic access control in distributed environment.

Keywords—access control; trust quantification; grey fuzzy theory

I. INTRODUCTION

In large-scale distributed network applications, not every resource requestor can be known beforehand by the resource owners because of the open property [1]. Access control, which is used to restrict the use of resources, is an important safeguard in network security. Traditional access control methods are well suited for the centralized and relatively static environment in which subjects and objects are known and relatively static and the permissions that are granted for subjects to access objects are rarely changed.

Traditional access control methods face some new challenges in open and distributed environments and they can hardly meet the open and dynamic requirements. Access control in distributed environments must dynamically adapt to dynamic addition and deletion of entities.

Trust is a part of our daily life and thus can be used as a tool to reduce the complexity of making access decisions, which can be accomplished by using trust to provide security [2]. In recent years, many researchers have applied trust to the distributed environments. However, trust may be difficult express using the traditional math theory because it can be subjective and uncertain. Fuzzy theory can thus be used to solve uncertain problems such as trust.

In this paper, we propose a new access control mechanism in distributed environments based on trust quantification. In our mechanism in which we use grey fuzzy comprehensive evaluation method to quantify trust. We also propose an access control model based on trust quantification.

The rest of the paper is organized as follows. In Section 2, we briefly review related works. In Section 3, we propose a trust quantification algorithm based on grey fuzzy comprehensive evaluation method. In Section 4, we present an access control model based on trust quantification. In Section 5, we present some simulation results. Finally, in Section 6, we conclude this paper in which we also discuss our future work.

II. RELATED WORK

Access control is an important security service, which can limit user access to resources and prevent users from making illegal access. There are at least three traditional methods for access control: discretionary access control (DAC)[3], mandatory access control (MAC) and role-based access control (RBAC)[4]. However, none of them is suitable for
the dynamic and open environments due to the lack of flexibility and efficiency.

Several novel access control models based on trust have been proposed in recent years. TrustBAC extends the conventional RBAC with the notion of trust level [5] in which users are assigned to trust levels instead of roles based on user identity, behavior history, recommendation, etc. When the trust level of a user changes, the role assigned to the user will change correspondingly. The authors in [6] proposed an access control framework using trust computing for peer-to-peer environments. A Role-based Trust management framework (RT) is described in [7] which integrates RBAC with trust management system and is thus suitable for credential based access control systems. In [8], the author presented a framework implementation for a trust and role based access control for secure interoperation. In all the work proposed above, although trust was introduced into access control models, no attempt has been made to quantify trust.

III. TRUST QUANTIFICATION

A. The Concept

In order to reflect the dynamism of trust in access control, we introduce several concepts here.

Trust quantification: a method of expressing the trust of an entity on another using a numerical value.

Credit: the evaluation result of the owner of an object on a subject based on some behavior information after an interaction between the subject and the object completes, which is denoted as C.

Reputation: degree of the trust of the owner of an object on a subject based on the credit values of several times, which is denoted as R.

Note that credit and reputation are dynamic expression of trust. In this paper, we use the following formula to compute credit and reputation.

\[ C = S \times T \]  

\[ R = \sum_{i=1}^{n} (S_i \times C_i) \quad \text{where} \quad \sum_{i=1}^{n} S_i = 1 \]  

In formula (1), T represents a trust value and S represents the satisfaction degree of the owner of an object on a subject in an interaction, and S \( \in [0,1] \).

In formula (2), n represents the number of credits. \( C_i \) is the credit value at \( i \)th time and \( S_i \) represents the weight of \( C_i \) for computing reputation.

For every request, the owner of a resource quantifies the trust of a subject. Then based on the interval to which the trust value belongs, access permissions can be determined.

B. Grey Fuzzy Comprehensive Evaluation

Grey fuzzy comprehensive evaluation method is a way of judging things and phenomena with fuzzy factors when information is not fully known. The method considers the grayness of expert evaluation information, uses grey theory to get grey statistics, then constructs fuzzy matrix and finally calculates comprehensive evaluation scores by using the fuzzy algorithm [9].

Due to the uncertainty of trust, there is normally some fuzzy information between a subject and an object for trust quantification. Consequently, we can use the grey fuzzy comprehensive evaluation method to quantify trust.

Following is the procedure for completing the grey fuzzy comprehensive evaluation:

1. Confirming the evaluation factor

   Suppose there is an evaluation factor set \( U = \{u_1, u_2, \ldots, u_n\} \) in which \( u_i \) (\( i = 1, 2, \ldots, n \)) denotes the \( i \)th factor.

   Let \( Z \) represent an evaluation set which is the degree of advantage and disadvantage of an evaluated object and \( Z = \{z_1, z_2, \ldots, z_m\} \) in which \( z_i \) denotes the \( i \)th evaluation grade, \( m \) denotes the number of evaluation grade.

   In this paper, we divide the evaluation set into four levels: {distrust, distrust but not certain, trust but not certain, trust} which corresponds to the intervals \( \{[0, 0.25), [0.25, 0.5), [0.5, 0.75), [0.75, 1]\} \), respectively.

2. Confirming the weight set

   The weight set can be viewed as a grey-fuzzy relationship between the evaluation target and the factor set. It can be expressed as:

   \[ \tilde{A} = \{(a_1, v_1), (a_2, v_2), \ldots, (a_m, v_m)\} \]
in which $\sum_{i=1}^{m} a_i = 1$ \hspace{1cm} (3)

If every factor’s weight is specified, then the weight set will be:

$A = \{(a_1, 0), (a_2, 0), \ldots, (a_m, 0)\}$ \hspace{1cm} (4)

(3) Establishing the grey fuzzy evaluation matrix

The evaluation matrix can be viewed as a relationship between the factor set and the evaluation set which can be expressed as $R$ below:

$R = \begin{pmatrix}
(\mu_{11}, v_1) & (\mu_{12}, v_2) & \cdots & (\mu_{1m}, v_m) \\
(\mu_{21}, v_1) & (\mu_{22}, v_2) & \cdots & (\mu_{2m}, v_m) \\
\vdots & \vdots & \ddots & \vdots \\
(\mu_{m1}, v_1) & (\mu_{m2}, v_2) & \cdots & (\mu_{mn}, v_m)
\end{pmatrix}$ \hspace{1cm} (5)

(4) Grey fuzzy comprehensive evaluation

The results of the grey fuzzy comprehensive evaluation can be expressed as follows:

$B_i = A_i \odot R_i = \left[ \left( \sum_{k=1}^{m} (a_k \cdot \mu_{ik}) \right) \left( \sum_{l=1}^{n} (v_l + v_{il}) \right) \right]_{ij}$ \hspace{1cm} (6)

(5) Using the evaluation results

According to the maximum subjection principle and minimum grayness principle, we select the interval which maximum subjection scale and the minimum grayness correspond to.

C. Trust Quantification Algorithm

We now use the grey fuzzy comprehensive evaluation method to quantify trust. The evaluation factors of object evaluating subject are credit and reputation. Namely, the evaluation factor set $U=\{\text{credit, reputation}\}$ and the evaluation set $V=\{\text{distrust, distrust but not certain, trust but not certain, trust}\}$. For each access request, we select the object and its neighboring nodes that interacted with the subject as the experts.

The trust quantification algorithm can be described as follows:

Step 1: Select $n$ neighboring nodes that interacted with the subject and get the most recent Credit and Reputation values from them for the subject, which can be denoted as $Credit_i$ and $Reputation_i$. If the object has no interaction history with the subject, then both of the Credit and Reputation values are 0. Namely, $Credit_i=0$ and $Reputation_i=0$.

Step 2: Using the weight of an expert $W_i$ where $W_i = \frac{Credit_i}{Credit_i + Reputation_i}$ and the weight of Reputation $RW_i = 1 - CW_i$.

Step 3: The following formula is used to compute the grayness of credit and reputation.

$CV_i = Credit_i \times (1 - Reputation_i)$ \hspace{1cm} (7)

$RV_i = Reputation_i \times (1 - Credit_i)$ \hspace{1cm} (8)

Step 4: According to every node’s Credit and Reputation values on the subject, we can determine to which evaluation level it belongs.

Step 5: Carry out grey fuzzy comprehensive evaluation.

$B = \left[ \left( \mu_{11}, v_1 \right), \left( \mu_{21}, v_2 \right), \ldots, \left( \mu_{m1}, v_m \right) \right]$ \hspace{1cm} (9)

Step 6: According to the principles of maximum subjection and minimum grayness, we select the interval $[a, b]$ which corresponds to $\min(v_j / \mu_j)$.

Step 7: The trust quantification value is thus

$Trust = a + (b - a) \times \mu_j$ \hspace{1cm} (10)

IV. ACCESS CONTROL BASED ON TRUST QUANTIFICATION

A. Dynamic Mapping between Trust and Permission

In this section, we describe how a quantized trust value is mapped to access permissions for providing fine-grained access control over sensitive resources. Meanwhile, access permissions can be dynamically adjusted based on the change of the trust quantification values.

Assume that an object’s permission set is $P$. We divide the trust of object’s owner on a subject into $k$ intervals, namely, $T = \{T_1, T_2, \ldots, T_k\}$. Then, access permission set $AP$ can be represented as $AP = \{\emptyset, \{read\}, \{read, write\}, \ldots, \{read, write, app, exe\}\}$ in which the number of elements of $AP$ is $k$, which is
equal to the number of trust intervals and each trust interval corresponds to an access permission set. For instance, if trust interval $[0, 0.25]$ corresponds to $\phi$, subjects whose trust quantification value belong to $[0, 0.25]$ would have no access permission to the object. If trust interval $[0.5, 0.75]$ corresponds to $\{\text{read, write}\}$, subjects whose trust quantification value belong to $[0.5, 0.75]$ would have the read and write permissions to the object.

In a distributed environment, a subject’s permission is dynamic with the change of its trust quantification value. When there is deception, the owner of the resource can modify mapping relationship between the access permission set and the trust intervals.

B Trust Quantification based Access Control Model (TQBAC)

The mapping method mentioned above is used for access control and a Trust Quantification Based Access Control Model (TQBAC) is thus proposed. The TQBAC model includes three layers: request management, access control management and access feedback management. The model also includes six modules: subject request, trust management, trust quantification, access permission mapping, access permission management and access feedback. The TQBAC model is shown in Figure 1.

The request management layer is mainly responsible for access request scheduling.

The main function of the trust management module is to divide trust interval. Based on access feedback information, it would compute the new credit of a subject and dynamically update the reputation of the subject. In addition, it will store other information of the subject in its trust evaluation table.

In the trust quantification module, grey fuzzy comprehensive evaluation method is used to quantify trust based on history information.

The permission mapping module reads the mapping table between a subject’s trust quantification value and access permissions and assigns corresponding permissions to the subject.

In the access feedback module, the feedback information from access behavior is sent to the trust management module, which can be referenced for the next access control.

Every object node will maintain a subject access record table that could include access sequence, time, IP address of subject, resource accessed, trust value, feedback satisfaction degree. Only the node itself can read and write the access record table. Subject’s trust evaluation table is related to the access record table.

A node interaction table is created to easily select “experts” in trust quantification. The table records interactions between nodes, which include at least four fields: sequence number, time, subject and object. To deal with malicious nodes, random selection method can be used in the selection of neighboring nodes for evaluation.

V. Simulation Results

In order to verify the validity of TQBAC model, a simulation is developed using Java program. Assume that there are 2 subjects and 10 objects.

In the experiment, we assume that every honest subject’s trust quantification value is randomly initialized to a value between 0.5 and 1, and hostile subject’s trust quantification value is randomly initialized to a value between 0.9 and 1. The mapping relation between trust interval and permission set is shown in TABLE I.
### TABLE 1. PERMISSION MAPPING

<table>
<thead>
<tr>
<th>Trust interval</th>
<th>0</th>
<th>0.25</th>
<th>0.4</th>
<th>0.6</th>
<th>0.8</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission set</td>
<td>$\emptyset$</td>
<td>read</td>
<td>read</td>
<td>write</td>
<td>write</td>
<td>app</td>
</tr>
<tr>
<td></td>
<td>read</td>
<td>write</td>
<td>app</td>
<td>exe</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Suppose there are two subjects, one is honest and the other is hostile. After each access, the satisfaction degree of the object to the honest subject is $S \in [0.85, 1]$ and that of the object to the hostile subject is $S' \in [0, 0.4]$. We select the most recent four credit values to compute reputation. The weight in formula (2) is then $S_1=0.5$, $S_2=0.25$, $S_3=0.125$, $S_4=0.125$, respectively.

The number of “experts” who participate in subject evaluation is four. After every access, satisfaction degree is randomly created in the satisfaction degree interval. Every subject randomly accesses object nodes 30 times. The experiment executes 50 times and we randomly extract one of them. The changes of the honest subject’s trust quantification value and access permissions are shown in Figure 2 and Figure 3, respectively and those of the hostile subject’s trust quantification values and access permissions are shown in Figure 4 and Figure 5, respectively.

In Figures 3 and 5, permission sets 0, 1, 2, 3 and 4 represent $\emptyset$, \{read\}, \{read, write\}, \{read, write, app\}, \{read, write, pp, exe\}, respectively.

We can see from Figures 2 and 4 that, since the honest node has good behavior, its trust quantification value is gradually increasing while, as the hostile node’s behavior is malicious, its trust quantification value drops very fast. In Figures 4 and 5, there are some rebounds in the decline process of the hostile node's trust values and permissions. The reason is that some nodes in “experts” have not interacted with the hostile node recently, so their evaluation of the hostile node remains same as earlier.

### VI. CONCLUSION AND FUTURE WORK

Trust management is an effective tool to solve access control problems in distributed environments. By considering subjectivity and uncertainty of trust, we selected the grey fuzzy comprehensive evaluation method to quantify trust. We then proposed a trust quantification algorithm based on the grey fuzzy comprehensive evaluation method and described how quantified trust values can be mapped to access permissions. We also designed a trust quantification based access control model (TQBAC) and performed
some simulation to show the effectiveness of our method. As the future work, we will improve the TQBAC model to make it suitable for specific distributed environment.

ACKNOWLEDGEMENT

This work has been supported by Beijing Education Commission Science and Technology Development Fund #KM201010005027.

REFERENCES


