A Grid Authorization Mechanism with Dynamic Role Based on Trust Model

Linna FAN*, Jun LIU, Ge LI, Zhaofeng WU, Jibin GUO

Institution of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China

Abstract

Because of the disadvantages of RBAC authorization mechanism in grid, paper designed a grid authorization model with dynamic role based on trust model and workflow management system. The mechanism is service-oriented and service is the access control object. Subject accessing services is under control of workflow management system. Trust Value Database records trust value of services after each invoking and update trust value of subject who owns these services. Subject’s role can vary with the variety of trust value. This policy encourages user in grid provide honest services. Simulation shows that the mechanism can increase the rate of success interaction and restrain dishonest subject as well as their services.

Keywords: Grid; Access Control; Trust Model; Role; Service-oriented

1 Introduction

Grid, as an increasingly flourishing technology, features a connection of putting all the independent computers, scattered in the geographical sense, into a share of resources [1]. The Globus Toolkit has emerged as the dominant middleware for Grid deployments worldwide. The Grid Security Infrastructure (GSI) is the portion of the Globus Toolkit that provides the fundamental security services needed to support Grids [2]. GSI uses Community Authorization Service (CAS) for authorization. Resource provider grants its coarse-grained privileges to CAS. Then CAS distributes fine-grained privileges [3].

Using RBAC in CAS can make resource management and authorization convenient. RBAC is one of the most popular access control technology, which is widely used in enterprises, cooperative authorization between organizations, information system of medical treatment and so on.

RBAC is a static access control method. Traditional static access control technology can not meet the grid requirement of share and dynamic. Grid is like human society. When a user requests
a resource, even we can authenticate the resource and it behaved well before, we are not sure that
the resource will be safe and do not harm users later.

The concept of trust, from the perspective of information security, will correspond to a set of
relations among entities that participate in a behavioral process [4]. Security is the key problem
of the Grid, and trust problem is the core issue which we must face in the solution of security
problem. Hence it is necessary to research on trust problem and propose effective trust model [5].

2 Current Research of Trust Model

Beth’s model [6] first quantized trust and divided it into direct trust and recommendation trust.
It decided probability entity finishing task through positive experience and negative experience
give the method computing direct trust and recommendation trust.

Jøsang’s model [7] use evidence space and concept space to descript and quantize trust rela-
tionship. It did not distinguish direct trust from recommendation trust. These two models don’t
have too much consideration and can not resist colluded cheat and repeated swing of node. A
dishonest node accumulates high trust value for a long time and then do harm to its requester
suddenly. This decreases its trust value. Then the dishonest node increases its trust value through
normal behavior and repeats this phenomenon which is called repeated swing of node.

F. Azzedin and M. Maheswaran [8] first integrated trust into grid resource management and
computed trust value between two grid entities according to direct trust value and recommenda-
tion value between two domains of the entities. The disadvantage is that he thinks all entities in
a domain have same trust value.

Reference [9] divided trust relationship between two grid entities into trust within a domain
and between domains. Each grid domain has an information node to manage the domain. Each
entities of domain maintain a table recording interaction with other entities. This model intro-
duced time attenuation function to accurate trust value. But it can not resolve the repeated
swing of dishonest node.

Reference [10] proposed a dynamic role-based access control based on trust mechanism in grid
environment. In this model computation of trust value need to refer to all subjects who interact
with the object and colligate all subjects’ mark to obtain the object’s trust value. This method
is not suitable to dynamic feature of grid. In grid, entities engage and quit dynamically. The
subject marking the object last time may quit grid next time. And too many subjects marking in
a large scale grid may bring heavy burden to grid. Moreover, some subjects are dishonest, which
can not contribute to trust value computation.

Paper proposed a workflow management system (WFMS) based trust model considering grid
need, features and disadvantages of current trust model. In this model, service is the object
in access control. Computation of service’s trust value only relates with WFMS’s estimate and
introduces time attenuation function as well as increase/decrease factor.

3 WFMS-based Trust Model (WFMSTM)

Paper’s trust model is built in VOs. A virtual organization (VO) is formed from different real
entities (e.g., medical centers, hospitals, governmental centers), and probably also from different
communities [11]. VO can start CAS service for authentication and authorization. To simplify
CAS’s authorization, paper designed role-based CAS. The role is different from role in RBAC. It does not have the privilege to access service and only can have privileges under control of WFMS. Trust model is built in follow frame, which can be seen in Fig. 1:

![WFMS-based trust model](image)

In Figure 1, CAS distributes roles to each subject. This model is service-oriented and service is the object of access control. Service-oriented architecture has many advantages like stability of service. User invokes service through interface but not the relative objects. So service can be same when object vary, which is good for access control management.

In this paper, WFMS has fully distributed architecture, in which each server has equal status and responsible for one part of the workflow [9]. CAS provides information of role and privilege to WFMS. It plays a role of attribute centre in WFMS. TVDB is a database stores each subject/service’s trust value. When finish a work, WFMS will value each service’s trust value and update them. Then compute subject’s trust value of these services. CAS will query TVDB for subject’s trust value period and adjust the subject’s role.

### 3.1 Symbols in the model

In order to descript trust value computation, symbols used is as Table 1:

### 3.2 WFMSTM working process

- **Initialize**: TVDB give initial trust value to services and subjects. Initial trust value is 0.5. When a new node engage, its initial trust value is also 0.5.

After initialization, WFMSTM run according to the following 6 steps:

1) When subject A in VO1 submit request W to WFMS, WFMS will divide W to different tasks T logically. Each T may need to invoke one or several services;
Table 1: Meaning of symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TV</td>
<td>Trust Value of services or subjects</td>
</tr>
<tr>
<td>$f_S$</td>
<td>Time attenuation function</td>
</tr>
<tr>
<td>$TL_i$</td>
<td>The level of service $i$</td>
</tr>
<tr>
<td>$TL_{max}$</td>
<td>The highest level of service</td>
</tr>
<tr>
<td>$\rho$</td>
<td>Time attenuation factor</td>
</tr>
<tr>
<td>$FQ_i$</td>
<td>Quality of service $i$ in an invoking</td>
</tr>
<tr>
<td>$FQ_{max}$</td>
<td>Max of quality of service</td>
</tr>
<tr>
<td>$v_S$</td>
<td>Increase/decrease extent of trust value</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Increasing or decreasing rate</td>
</tr>
</tbody>
</table>

2) When choosing services, WFMS can refer to service’s trust value in TVDB. If load permit, WFMS will choose the service with the highest trust value;

3) WFMS invokes and watch execution of services. Then WFMS mark service $S$ and transmit the trust value of this interaction to TVDB;

4) TVDB updates trust value of $S$ according to former trust value and this interaction;

5) TVDB updates subject’s trust value who owns $S$;

6) CAS queries each subject’s trust value in TVDB and adjusts their role.

3.3 Trust value computation of service

In WFMSTM, service is the object of access control and its value should attenuate with time elapsing according to its importance. To avoid sudden malicious behavior, the extent trust value increase and decrease is different.

3.3.1 Time attenuation function

Trust value should attenuate with time elapsing, which is accord with people’s comprehension about trust. For example, A has just interacted with B and thought B is trustworthy. After a long period, the degree of trust A toward B will be weakening. So we introduce Time attenuation function:

$$f_S(x) = \rho^{\Delta t} x, \quad (0 \leq \rho \leq 1)$$

In the function above, $\Delta t$ is time interval from last invoking to now of service. $\rho$ is time attenuation factor which can be adjusted according to environment.

3.3.2 Service level

Increase/decrease extent of service’s trust value is different. The higher of the service level, the larger of the increase/decrease extent. We use SL to symbol service level, which is often related with security, storage, bandwidth, emergency and so on.
3.3.3 Increase/decrease factor and extent

In order to prevent repeated swing of node, we introduce increase/decrease factor $\alpha$ and increase/decrease extent $v_S$. $\alpha$ is related with service level $TL$ and service quality $FQ$. Service be revoked successfully or not has different increase/decrease extent $v_S$. In the following formula, success=1 donate invoking service successfully, success=0 is to say invoking service abnormally.

$$\alpha' = \begin{cases} 
\alpha_i, & \text{if } success = 1 \\
\alpha_i - \frac{0.8SL_i|FQ|}{SL_{max}FQ_{max}}, & \text{if } success = 0
\end{cases}$$

The formula above is the computation method of $\alpha$. $\alpha$ is in the range of $[0,1]$. If $\alpha$ is bigger or smaller than 1 or 0, we set its value as 1 or 0. $FQ_i$ is the service quality of the service. $FQ > 0$ donates normal service. The higher of $FQ$ are, the better of the service quality is. $FQ < 0$ donates the requester has been attacked in having service of the subject. The lower of $FQ$ are, the worse of the attack is. $\alpha$’s initial value is 0.5. When the subject provide normal service, $\alpha$ maintain its former value, which control the increase of the trust value. When the subject provide abnormal service to requester, $\alpha$ decreases. And the decrease extent $v_S$ is related with service quality and service level. High service level is to say the service is important. If a service with high SL behaves abnormally, its increase/decrease factor will decrease largely.

Extent $v_S$ of normal service and abnormal service is different:

$$v_S = \begin{cases} 
v_1, & \text{if } success = 1 \\
v_2, & \text{if } success = 0
\end{cases}$$

In the expression above, $|v_1| < |v_2|$, $v_1 > 0$, $v_2 < 0$. That is to say, the decrease extent is larger than increase extent, which can prevent repeated swing of node effectively.

3.3.4 Computation of trust value for service

TV stands for trust value of a service. Then TV can be computed in the following formula:

$$TV = \rho^{\Delta t} \sum_{i=1}^{n} SL_i l(\alpha_i)v_i$$

$$l(\alpha_i) = \begin{cases} 
\alpha_i, & \text{if } success = 1 \\
1.1 - \alpha_i, & \text{if } success = 0
\end{cases}$$

$n$ stands for the service has been invoked $n$ times. $TL_S$, $\alpha_i$, $v_i$ are service level, increase/decrease factor of ith invoking and increase/decrease extent respectively.

3.3.5 Update of trust value

When a service finished its task, WFMS update trust value of the service in the following formula:

$$TV' = f_n(TV) + \frac{SL_i l(\alpha_i)v_i}{SL_{max}}$$

TV is controlled in range of $[-2, 2]$. 
3.4 Computation of trust value for subject

Subject’s trust value is related with services he owns. We assume subject A is the owner of services \( \{S_1, S_2, \ldots, S_i\} \). Trust value of \( S_1, S_2, \ldots, S_i \) is \( TV_1, TV_2, \ldots, TV_i \) which are stored in TVDB. Then the trust value of A is:

\[
TV_A = \frac{1}{i} \sum_{n=1}^{i} TV_n
\]  

(4)

3.4.1 Dynamic change of role

Subject’s role is related with its trust value:

\[
R_x = F(TV_X) = \begin{cases} 
R_1 & (-1 \leq TV_x < 1) \\
R_2 & (1 \leq TV_x < k) \\
... \\
R_m & (p \leq TV_x < 1) 
\end{cases}
\]

CAS will query TVDB regularly, and then adjusts roles according to its trust value. This policy will encourage subject to upload more normal service in order to increase trust value and get role with more privileges. In opposition, if a subject do harm to others when service invoking, trust value will be decreased and the subject can only get role with less privileges.

4 Simulation and its Results

![Fig. 2: WFMS-based trust model](image)

In simulation model, we assume there are 100 services. The max service level is 7. The max service quality is 8. Increase extent \( v_1 = 1 \). Decrease extent \( v_2 = -2 \). Increase/decrease factor of each
service is 0.5. SL and FQ are generated randomly. Fig. 2 shows the probability of success when trust model exists or not. In two circumstances, we assume abnormal service of dishonest subject provides normal services to requester in probability of 50% and attacks requester in probability of 50%. Results of simulation can be seen as follows:

From Fig. 2, we can see that in circumstance of no trust model, probability of success is the curve of linear decrease. When all services have dishonest subjects, probability of success is about 50%, which is equal to probability abnormal service behaving normally. In circumstance of trust model, probability of success is close to 100% when there are 0% to 90% abnormal services. From the data above, we can conclude that trust model increase probability of success largely.

Fig. 3 is the change of trust value and increase/decrease factor of a service with time.

![WFMS-based trust model](image)

The abnormal service behaves normally in probability of 70%. In the start period, it behaved normally and its increase/decrease factor maintained the initial value 0.5, which controlled the increase speed of trust value. When the service behaved maliciously, trust value decreased suddenly from 0.774853 to -0.38229. At the same time, its increase/decrease factor decreased to 0.328571. The service paid high cost for its malicious behavior. After that, if the service wants to accumulate trust value through normal behavior will need more time and the increase speed is lower.

Simulation result shows that the trust model designed in the paper can increase probability of successful interaction and restrain dishonest subject.

5 Conclusions

Dynamic change of role of authorization based on WFMS and trust model designed in the paper uses service as access control object. Subject accessing service is under control of WFMS. TVDB
records each service’s trust value and update it. Subject’s trust value is related with trust value of its services and can affect its role to encourage it to provide normal service. Simulation shows that the mechanism can increase probability of successful interaction and restrain dishonest subject.

References


