An Intro-Domain Entity Trust Model Design of Computing Grid

Li Guo-ping

Department of Modern Education and Technology, Pingxiang College, Pingxiang 337000, Jiangxi, China

Yang Zhang-wei

Department of Modern Education and Technology, Pingxiang College, Pingxiang 337000, Jiangxi, China

Abstract

A conventional trust domain-based grid trust model uses the number of entities within the autonomous domain as a unique parameter of trust-value computing complexity, thus providing a low degree of safety. Therefore, an improved entity trust model within autonomous domain is introduced, being based on the existing computing grid trust model. Additionally, the time attenuation and penalty factor are introduced into the model to establish a GSP model that computers the user's direct trust and recommended trust. Through examination based on simulation, it is verified that the model thus introduced features higher resistance to whitewashing attack.

Key words: COMPUTING GRID, TRUST MODEL, USER TRUST AGENT, GRID SERVICE PROVIDER, WHITEWASHING ATTACK

1. Introduction

The grid computation is committed to sharing high-performance computing capacity. As opposed to cloud computation, which provides commercialized data processing service, grid computation is widely applied for scientific research and other specific fields [1]. In order to make grid computation safer and more attractive and to allow more convenient commutation among grid entities, trust among user entities is particularly important.

Trust is an important aspect of grid security, being important as a means to ensure grid security. Trust among entities is strongly independent but highly dependent on the past behavior of the given entity; moreover, it varies dynamically with changes in the behavior of the entity [2]. In the grid-computation environment, a good trust relationship should be established among nodes. The existing high-performance computing system is basically opened to the user for operation based on a trust mechanism. Among grid nodes, the mutual trust relationship may be adjusted in a timely, dynamic way according to the contact experience of past direct or indirect behaviors with respect to one another. Thus the manner in which to accurately compute entity trust value within an autonomous domain and establish a reasonable mechanism for updating trust value is integral to solving the problem of grid security.

It is necessary to know the trust relationship between the grid entities when they conduct a transac-

tion, given the dynamic performance and uncertainty of the grid environment. Reference 4 brings forward the design idea of a trust model based on the trust domain, whereby the grid is divided into several management domains. The trust relationship among nodes includes the intra-domain trust relationship and inter-domain trust relationship, each of which is managed through a particular strategy. Moreover, the intra-domain trust-value computing complexity is dependent only on the number of intra-domain nodes while the inter-domain computing domain is dependent only on the number of domains. This model uses the number of entities within the autonomous domain as a unique parameter of trust-value computing complexity. It offers the advantage of a low-complexity algorithm. However, it has disadvantages: No consideration is given to the transaction context, of which the environment is often necessary as a determinant of trust; there is no method for establishing the initial mechanism of the trust relationship, nor is there a mechanism for the updating of trust value. No consideration is given to the influence of time attenuation on trust value, which influences the accuracy of trust value; nor is consideration given to the penalization of malicious nodes, which reduce trust security.

2. Analysis of Several Trust Models

The concept for the design of the trust domain-based trust model is that the grid is divided into several management domains, that the trust relationship among nodes includes an intra-domain trust relationship and inter-domain trust relationship, and that they are handled through different strategies [3]. Moreover, the intra-domain trust value's computing complexity depends only on the number of intra-domain nodes while the inter-domain computing domain depends only on the number of domains.

A conventional trust domain-based grid trust model uses the number of entities within the autonomous domain as a unique parameter of trust-value computing complexity, featuring low safety. However, while it features the advantage of low complexity of algorithm, it also has some disadvantages:

(1) There is no consideration of the transaction context in which environment is often an essential factor in determining trust; (2) there is no method for establishing the initial mechanism of trust relationship, nor is there a mechanism for trust-value updating; (3) there is no consideration of the influence of time attenuation on trust value and, in turn, the accuracy of trust value; and (4) there is no consideration of penalty to malicious nodes, thereby reducing trust security. Consequently, in regard to the defects of the conventional computing grid trust model, the following trust models are established to improve them:

(1) Trust model based on the Dempster-Shafer (D-S) evidence theory [4]. By establishing corresponding rules, the trust degree is rated (as trusted, not trusted and uncertain) and evaluated to describe subjective trust degree;

(2) Fuzzy set-based trust relationship [5]. The trust relationship is rated in order to establish the membership function of the trust set.

(3) Probabilistic statistics-based trust relationship [6]. The statistical number of interactive successes and interactive failures is used to classify the trust rank.

(4) Behavior-based grid trust model: First proposed by F. Azzedin, it uses trust and prestige as measurements and introduces a trust-attenuation function to reflect the characteristics of trust, which vary with time.

Additionally, the D-S evidence theory-based trust model uses a basic belief function to evaluate the trust degree. Because this function is based on the classic probabilistic design, it ignores the influence of different trust evidence on trust value. The fuzzy set and probabilistic statistics-based trust models use probability to represent trust uncertainty, which must be established based on the random, probabilistic distribution of knowledge and is therefore not applicable to the computation of uncertainty information in a complex grid environment. Based on the Direct Trust Table (DTT) and the Recommended Trust Table (RTT), the behavior-based grid trust model proposed by F. Azzedin introduces trust degree and prestige, adds the time-attenuation factor and uses fuzzy logic to judge trust behavior. However, its trust relationship of inter-nodes of maintenance is overly complicated and does not readily accommodate an appropriate time-attenuation function.

Because the computing grid is open and dynamic, etc., the existing trust model, when applied to the grid, will face the whitewashing attacks initiated by malicious users and will thus be at risk. Therefore, improvement of the existing trust model and the assured accuracy of user-trust degree evaluation are important guarantees for grid security.

3. Improving Trust Model

3.1. Framework of Hierarchical Trust Evaluation

Because the grid is distributed, heterogeneous and highly dynamic, the computing grid cannot provide a single, united trust evaluation value. Moreover, a means of distributed trust management must be used. However, the grid consists of many autonomous domains in range of sizes. Although grid users and re-

sources are dynamic, they are more stable in comparison to the autonomous domain. Therefore, it is necessary to redesign the trust management of the computing grid so as to add an autonomous domain user trust agent (UTA) and avoid any grid service proxy (GSP) that is directly in contact with the user.

When the user-trust degree is evaluated, the autonomous domain UTA is responsible for evaluating and managing the user's direct trust degree within its domain. Additionally, the grid users within the autonomous domain evaluate the GSP trust degree through UTA, the hierarchical structure of which is shown in Figure 1.

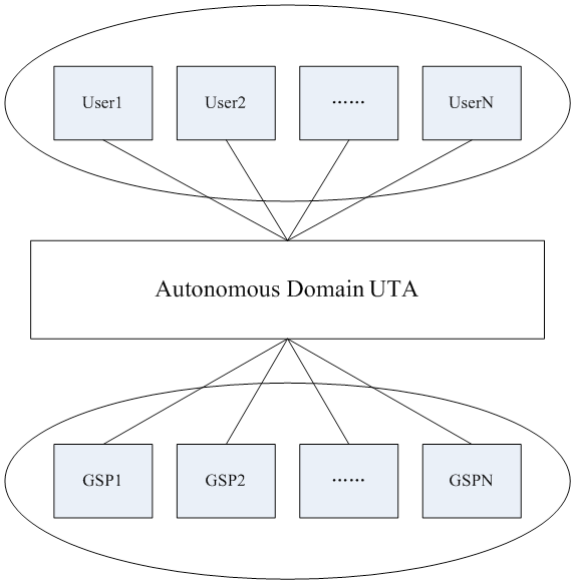

Figure 1. Framework of the Hierarchical Trust Model

After the above-mentioned trust management model is used, when users need apply computing grid service, the executive flow of such model is as follows:

a) The user makes an application from the autonomous domain UTA and inquires as to whether the GSP trust conditions are met.

b) According to the traction records between the user and the GSP within its domain, UTA evaluates the trust degree of the GSP and returns the results of evaluation to the user.

c) Once the user has chosen the GSP that meets the requirements, it applies for CA certification from the autonomous domain UTA. The certification includes the user's trust degree in the autonomous domain. The user will submit this certificate when applying services from the GSP so that the GSP can understand the user's identity and trust degree. GSP verifies the user certificate and determines the provision of services depending on the user-trust degree and trust degree to UTA contained in the certificate.

d) If GSP refuses to provide services, the user fails to apply.

e) If GSP provides services, it will update the trust degree to such autonomous domain UTA according to success of service after the end of service. Moreover, UTA updates the trust degree of such user within the autonomous domain.

Use hierarchical trust evaluation framework to perform transaction. Because GSP only needs to process UTA trust degree, the GSP processing efficiency may be increased, and, the UTA trust evaluation to the user within autonomous domain is more accurate. However, the hierarchical trust evaluation framework model makes the trust relationship become more complicated. It is necessary to consider GSP evaluating UTA trust.

3.2. Computing Direct Trust Degree

3.2.1. Evaluating Direct Trust Degree

GSP evaluates the trust of certain autonomous domain UTA based on the results of transaction with users within such autonomous domain and determines by the number of successfully and failed transactions. UTA is able to record the number of successfully and failed transactions of each user because GSP must transact with grid user each time through UTA. Given Ns and Nf respectively representing the transaction the number of successes and failures of GSP with the user within such autonomous domain, the direct trust degree (T) of such user may be attained according to Bayesian formula of probabilistic verification:

$$T = \frac{Ns+1}{Ns+Nf+c} \quad (1)$$

Where c is a constant, used to ensure accurate results of evaluation when there are fewer transactions. c is taken by 2 to 6, depending on the number of transactions.

The trust of GSP to UTA depends on the accuracy that the UTA evaluates the user-trust degree of such autonomous domain. Therefore, UTA trust degree may be expressed by a triple (T,D,S). Where T is the direct trust degree of the user within each domain, as obtained through Formula 3-1; D is the sum of the trust deviations of all the transactions, as obtained from the following Figure 1; S is the variance of transaction trust degree of deviation, as obtained from the following Figure 3.

Definition of 3-1: The transaction trust deviation (D) is defined as the deviation of the user-trust degree within autonomous domain from the total trust degree or total distrust. The «D» may be calculated according to Formula 2.

$$\begin{cases} Di = 1 - ti, & successful \\ Di = 0 - ti, & fail \end{cases} \quad (2)$$

Where Di is the trust deviation of the i^{th} transaction; ti is the direct trust degree of the user when GSP transacts with such user for the i^{th} time.

Definition 3-2: The variance (S) transaction trust degree of deviation is the mean of the square of all the transaction degrees of deviation divided by the mean of the square of reference degree of deviation. The «S» may be calculated according to Formula 3.

$$S = \frac{1}{n} * \sum_{i=1}^{n} \frac{Di^2}{Ds^2} \quad (3)$$

Where n is the total number of GSP transactions with such user; Ds is the reference degree of deviation.

3.2.2. Adding the penalty factor

When GSP transacts with the user, malicious transaction is inevitable. In order to prevent the grid security from adversely affected by malicious transaction, penalty factor may be added. After the user within autonomous domain presents malicious transaction, UTA will quickly lower the trust degree of such user so that it should be restricted for next resource application. Therefore, Formula 1 may be improved. With addition of penalty factor λ, the trust degree (T) may be calculated according to the following formula:

$$T = \frac{Ns+1}{\lambda(Ns+Nf)+c} \quad (4)$$

Where the penalty factor λ is taken by $\lambda \in [1, \infty)$. If λ is 0, there will be no penalty. The higher λ is, the higher of speed lowering trust degree of such user is, and the stronger the penalty to such user is.

In order to define whether the value of penalty factor during a specific transaction may quickly lower the trust degree to malicious user, it is necessary to define a reference value of evaluation to be used as the reference for λ value.

Definition 3-3: The reference values of evaluation C1 to C5 are respectively converted values under five different conditions that the malicious transaction rates are 0, 10%, 20%, 50% and 100% when GSP normally transacts with the user. The values of C1 to C5 are as shown the following Table 1.

Table 1. Reference Values of Evaluation

Reference of Evaluation	Proportion of malicious transaction	λ value
C1	0	1
C2	10%	(Ns+Nf)
C3	20%	(Ns+Nf)^2
C4	50%	(Ns+Nf)^5
C5	100%	(Ns+Nf)^10

According to the reference values of evaluation taken under different malicious transaction conditions, when the user has no malicious transaction, the trust degree T is the direct trust degree of such user obtained from the Bayesian formula of probabilistic verification. With increased malicious transactions, the value of trust degree (T) will be reduced in form of exponent; when malicious transactions reach 100%, the value of T approaches to 0, as a result, the user will be unable to perform further transaction.

3.2.3. Introducing time-attenuation processing mechanism

If there are many transactions between GSP and the user, relative to old transaction, the results of latest transaction will more easily reflect the current trust degree of such user. Therefore, when the user's direct trust degree is calculated, it is necessary to consider the influence of time attenuation on the trust value. At present, many trust models dynamically update the trust value with time attenuation in a weighted way. In order to more conveniently realize models, in this article, the weighted function is realized with logarithm. As shown in above Formulas 1 and 3, the direct trust degree is obtained with the transaction number of successes and failures as parameter. Because the latest transaction will more easily reflect the current trust degree of user, when the direct trust degree is calculated, use the results of M latest transaction in Formula 1:

$$M = Log_n(N_s + N_f) \quad (5)$$

$$T = \frac{Ns+1}{\lambda M+c} \quad (6)$$

Where $n \in [1,10]$ and its value is increased with increased total number of transactions between GSP and user. Therefore, relative to earlier malicious transactions, the latest malicious transactions are able to more quickly lower the user's trust degree.

3.3. Calculating the Recommended Trust Degree

For recommended trust, a path which may access the target entity will be sought through the entity transacting with the user. The recommended trust degree of the target entity is obtained from this path. If a GSP needs to obtain the recommended trust degree of the target user, the following process is used:

a) This GSP sends request to all GSPs via broadcast.

b) GSP will forward request after receiving. Moreover, it will check whether its own transaction with the target user can be found. If yes, it will send the direct trust degree (T) to the requester.

c) With data of direct trust degree (T) through many GSPs, GSP may attain the recommended trust

data of such user.

Because the recommended trust pertains to many users transacting with the target user, one trust proxy will be added in the grid for each user in order to ensure the reliability of recommended trust. The proxy functions to acquire the GSP trust value for user. If the user needs the trust information of the target of the target object, the value is provided by the trust proxy of such object. Generally, there are many proxy trust data during the calculation of recommended trust. The recommended trust value of the target user may be obtained after these data are calculated according to Formula 7.

$$T = \sum \frac{Xi \cdot Ni \cdot Ri \cdot Fi}{\sum Xi \cdot Ni \cdot Fi} \quad (7)$$

Where X_i, N_i and R_i are the trust value, recommended number and target user recommended trust value of the corresponding proxy of user i, respectively, F_i is a time parameter that is reduced with the increase in recommended time for the last time.

Additionally, because the recommended trust and entity prestige are fuzzy to a certain extent, the fuzziness can barely be represented by using one accurate value to express the recommended trust degree. Therefore, in this article a recommended trust reference is designed, and the trust degree is divided into five grades according to the range of values. The range of trust value is defined as [0,1], while the reference set is RTS={RTS_1(0.9,0.05,0.02), RTS_2(0.7,0.05,0.02), RTS_3(0.5,0.05,0.02), RTS_4(0.3,0.05,0.02), RTS_5(0.1,0.05,0.02)}, as shown in Figure 2.

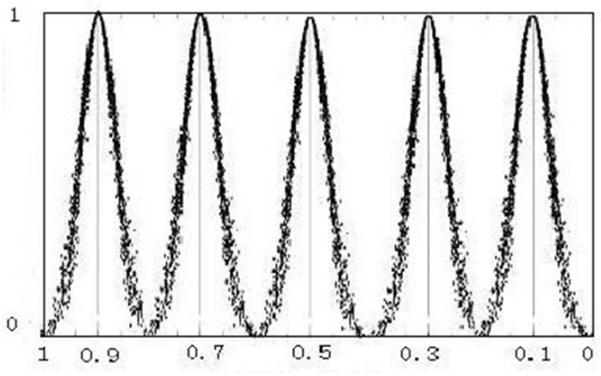

Figure 2. Reference Set of Recommended Trust

In a specific computing grid environment, the reference set of recommended trust is rated according to the trust rank. In this article, given the ratings «very trustable» to «untrustable,» the trust ranks may be set as RTS1 to RTS5.

3.4. Simulation Experiment and Analysis

In order to verify the effectiveness of the computing grid trust model, in this article a medium-scale computing grid simulation experiment environment is designed. This environment includes 10 user autonomous domains and GSPs. All the GSPs fully provide the same computation services. Each autonomous domain contains several hundred grid users and a small quantity of malicious users. The experimental processes are realized with three scenarios. Scenario 1 uses no autonomous domain UTA to manage trust degree, with user trust directly managed by the GSP; Scenario 2 manages trust degree through UTA; Scenario 3 uses the trust model described herein to manage trust degree. When the user requests computation service from GSP and with malicious user whitewashing attack, the number of successes attacked of three scenarios is as shown in Figure 3.

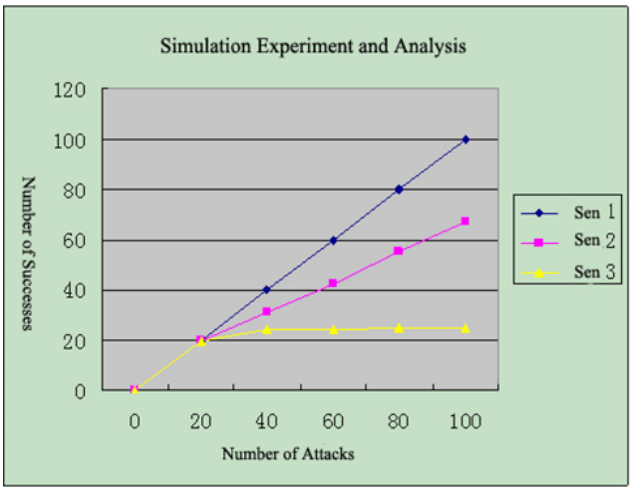

Figure 3. Simulation Experiment and Analysis

The simulation results show that, in the above three scenarios, Scenario 1 allows the malicious user to request services and is unable to prevent whitewashing attack, but that scenarios 2 and 3 use the UTA trust model. Because time attenuation and penalty factor are added to Scenario 3, after GSP receives one whitewashing attack, it will quickly lower the trust degree of such user so that it is unable to re-request services provided by the GSP, resulting in better resistance to attack.

4. Conclusions

Based on the existing trust model, the UTA hierarchical management mechanism is introduced. Moreover, time attenuation and the processing of malicious recommendation are introduced into the model to establish the computation model of direct trust degree and recommended trust degree. The results of the simulation experiment show that, by quickly lowering the trust degree of a malicious user, this improved trust model is able to prevent the malicious user's request of trust service, thereby resulting in higher GSP

resistance to whitewashing attack within the computation grid

Acknowledgements

This work was supported by Natural Science Foundation of Jiangxi Province (20144BAB2020010), Soft Science Program of Science and Technology Department of Jiangxi Province (20122BBA10094), Science and Technology Program of Education Department of Jiangxi Province (GJJ14789), and Scientific and Technological Guidance Plan of Pingxiang Municipal.

References

1. Yang Zhangwei (2011) Research on trust model in autonomous domain of campus grid. *Proceedings of 2011 International Conference on Computer Science and Service System*, p.p.521-530.
2. Rahman A A, Hailes S. (2000) Supporting Trust in Virtual Communities. *Proceedings of the 33rd Hawaii International Conference on System Sciences*, p.p. 6007-6016.
3. Ma Li, Zheng Weimin (2009) Synthesize trust degree valuting model for an information grid environment. *Tsinghua Science and Technology*, 2009(4), p.p.521-530.
4. A.Josang, S.J.Knapskog (1998) A metric for trusted systems. *Proceedings of the 21st National Security Conference*, p.p.1011-1023.
5. Azzedin F, Muthucumaru Maheswaran (2002) Towards Trust-Aware Resource Management in Grid Computing Systems. *Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid*, p.p.1-6.
6. A.Josang, S.Hird, E.Faccer (2003) Simulating the Effect of Reputation Systems on e-Markets. *Proceedings of the First International Conference on Trust Management*, pp.179-194.